

Fundamentos de Routing e-book

Eduardo Collado Cabeza
<http://eduardocollado.com>
ISBN: 978-1409284635

29 de julio de 2009

Índice general

| | |
|--|-----------|
| 1. Prefacio | 7 |
| 2. Introducción | 9 |
| 2.1. Introducción al routing IP | 9 |
| 2.2. Tipos de protocolos de routing | 11 |
| 2.3. La tabla de routing | 15 |
| 2.4. Métodos de introducir rutas | 19 |
| 2.5. Routing y switching | 23 |
| 3. Direccionamiento IP | 27 |
| 3.1. Subnetting IP | 27 |
| 3.2. Prefijo de routing/CIDR | 33 |
| 3.3. VLSM – Variable-Length Subnet Masks | 36 |
| 3.4. Sumarización | 42 |
| 4. Diseño de redes IP | 47 |
| 4.1. Criterios de diseño de redes IP | 47 |
| 4.2. Direccionamiento privado | 56 |
| 4.3. Network address translation | 58 |
| 4.4. Introducción a IPv6 | 60 |

| | |
|---|------------|
| 5. Protocolos vector distancia | 71 |
| 5.1. Presentación | 71 |
| 5.2. RIP | 73 |
| 5.3. IGRP | 81 |
| 5.4. EIGRP | 82 |
| 5.5. Seleccionar protocolos de routing | 83 |
| 6. Protocolos estado del enlace | 89 |
| 6.1. OSPF | 92 |
| 6.2. IS-IS | 102 |
| 6.3. BGP-4 | 103 |
| 7. OSPF | 109 |
| 7.1. Fundamentos | 109 |
| 7.2. Características de OSPF | 112 |
| 7.3. Operación en un área | 119 |
| 7.4. Topologías de OSPF | 126 |
| 7.5. Configuración de OSPF en un único área | 131 |
| 7.6. Configuración de OSPF en topologías NBMA | 139 |
| 8. OSPF en múltiples áreas | 151 |
| 8.1. El propósito de OSPF en múltiples áreas | 151 |
| 8.2. Características de múltiples áreas en OSPF | 152 |
| 8.3. Operación de OSPF en múltiples áreas | 156 |
| 8.4. Configuración en OSPF multiárea | 162 |
| 8.5. Configuración opcional de OSPF multiárea | 163 |
| 8.6. Verificación OSPF multiárea | 171 |
| 8.7. Troubleshooting OSPF multiárea | 176 |

| | |
|---|------------|
| 9. Fundamentos de IS-IS | 179 |
| 9.1. Introducción a IS-IS | 179 |
| 9.2. Comparativa con OSPF | 184 |
| 9.3. Direccionamiento para IS-IS | 189 |
| 9.4. Estructura jerárquica de IS-IS | 194 |
| 9.5. Principios básicos de routing de área | 196 |
| 9.6. Redes e interfaces de IS-IS | 198 |
| 9.7. Operación de IS-IS | 209 |
| 9.8. Consideraciones de diseño de IS-IS | 214 |
| 9.9. Configuración básica de IS-IS | 215 |
| 9.10. Comandos opcionales de IS-IS | 216 |
| 9.11. Verificación de la operación de IS-IS | 221 |
| 9.12. Troubleshooting de la operación de IS-IS | 226 |
| 10.EIGRP | 229 |
| 10.1. Introducción a EIGRP | 229 |
| 10.2. Operación de EIGRP | 236 |
| 10.3. Diseño de una red EIGRP | 247 |
| 10.4. Configuración de EIGRP | 249 |
| 10.5. Verificación de la configuración de EIGRP | 257 |
| 10.6. Troubleshooting de la operación de EIGRP | 259 |
| 11.BGP | 261 |
| 11.1. Introducción a BGP | 261 |
| 11.2. Introducción a la operación de BGP | 267 |
| 11.3. Atributos de BGP | 271 |
| 11.4. Configuración básica de BGP | 284 |
| 11.5. Comandos opcionales de BGP | 286 |
| 11.6. Gestionar y verificar BGP | 290 |

| | |
|---|-----|
| 11.7. Diseño y configuración de iBGP | 299 |
| 11.8. Verificación de iBGP | 306 |
| 11.9. Controlar el tráfico de BGP | 307 |
| 11.10 Conectar a Internet con BGP | 313 |
| 11.11 Determinar el path de BGP modificando atributos . . | 317 |
| 11.12 Redistribución entre IGP y BGP | 319 |

Capítulo 1

Prefacio

Hoy, 15 de Mayo de 2009 por fin está el libro terminado, y listo para ser aprovechado por cualquier persona que tenga interés en la materia.

Todo empezó en el año 1999, un router cayó en mis manos, un pequeño Zyxel cuya función era crear un punto a punto entre dos oficinas con un enlace de 64kbps, desde entonces muchas cosas han cambiado, el ver un router ya no es algo extraño y minoritario.

Hoy en día tener un router en casa es algo de lo más habitual, pero hay cosas que no han cambiado, no existe documentación en español y el dominio del inglés es algo totalmente necesario.

Con este libro pretendo aportar mi pequeño granito de arena para que cualquier persona hispano parlante pueda empezar a comprender como funcionan los protocolos de routing más importantes como OSPF o BGP.

La redacción de este libro comenzó hace ya 6 años, el material de este libro se empezó a generar con unas diapositivas para un curso de routing con routers Cisco que impartía por aquella época en una academia en la ciudad de Madrid.

Espero que este material pueda serle útil al lector porque está

generado desde el punto de vista de la persona que quiere aprender dando información directa, sin demasiados rodeos y con un buen número de ejemplos.

El libro está publicado en dos formatos, en formato escrito y en formato online totalmente gratuito en <http://eduangi.com> porque entiendo que el coste de un libro no debe de ser impedimento para que la información pueda llegar a aquellas personas que la precisen.

Por supuesto no quiero dejar de agradecer a mi mujer Ángeles por su amor, su paciencia, y por todo el tiempo que no le he podido dedicar a ella por dedicárselo a esta profesión, tan esclava como satisfactoria a veces, y también quiero dejar este libro a mi hijo Eduardo que ya pertenece a una generación que no tendrá que preguntarse qué es Internet o qué es un router, de igual forma que nosotros no tuvimos que preguntarnos qué era la televisión porque siempre ha estado ahí.

Capítulo 2

Introducción

2.1. Introducción al routing IP

Protocolo: Acuerdo de un conjunto de reglas que determinan cómo va a operar algo.

Protocolo de Routing: Conjunto de Reglas que definen como los dispositivos de routing de nivel 3 envían actualizaciones entre todos los que están disponibles en la red. Si existiera más de un camino a la red de destino, sería el protocolo de routing el que decidiera qué camino es el mejor para la red remota.

También podemos definir Protocolo de Routing como mecanismo utilizado para enviar actualizaciones entre los dispositivos de routing de nivel 3.

El proceso de routing proporciona tres pasos envueltos en la creación, mantenimiento y utilización de la tabla de routing:

- El protocolo de routing envía información sobre las rutas o redes en el sistema autónomo (RIP, IGRP, EIGRP, OSPF) y entre sistemas autónomos (BGP).

- La tabla de routing recibe actualizaciones del protocolo de routing y proporciona el proceso de forwarding con información en una petición.
- El proceso de forwarding determina el camino seleccionado por la tabla de routing para reenviar un datagrama.

Es importante resaltar que vamos a llamar a partir de ahora a la PDU de nivel 3 datagrama y no paquete, ya que los datagramas son sin conexión tanto en IP como en IPX principalmente.

Para tomar las decisiones de reenvío tomaremos en cuenta tres puntos:

- **Métrica:** Los protocolos de routing utilizan la métrica para calcular cual es el mejor camino a una red remota. Hemos de tener en cuenta que muchos protocolos de routing IP tienen métricas completamente distintas, con lo que el intercambio de información es muy complejo.
- **Distancia Administrativa:** Si conviven varios protocolos de routing en un mismo router tenemos que tener una forma de diferenciar qué protocolo es el que está actualizando la tabla de routing. Esta información está basada en qué protocolo de routing se considera la fuente más fiable de información.
- **Longitud del Prefijo:** El proceso de forwarding utiliza la red más restrictiva para reenviar la información. La red más restrictiva se corresponde con la red que nos proporcione el prefijo (máscara) más larga.

Protocolo Enrutado (Routed): Protocolo de nivel 3 utilizado para transferir información desde un dispositivo a otro a través de la red. El protocolo enrutado es el datagrama de nivel 3 que lleva información de la aplicación además de información de los niveles superiores.

Protocolo de Routing: Protocolo utilizado para enviar actualizaciones entre los routers de la red. Además es el que determina el camino para el datagrama a través de la red.

| Protocolo Enrutado | Protocolo de Routing de Pasarela Interna |
|--------------------|--|
| Appletalk | RTMP, AURP, EIGRP |
| IPX | RIP, NLSP, EIGRP |
| Vines | RTP |

La lista de los protocolos no tan extendidos son:

RTMP: Routing Table Maintenance Protocol. Propietario de Apple Computer.

AURP: Appletalk Update-Based Routing Protocol. Método de encapsular el tráfico Appletalk en la cabecera de otro protocolo.

NLSP: Net-Ware Link Services Protocol. Protocolo de estado del enlace basado en IS-IS.

RTP: Routing Table Protocol. Protocolo de routing de VINES basado en RIP.

DECnet: Protocolo propietario de Digital Equipment Corporation (Fase I), en la Fase 5 completó su transición a los protocolos de routing de OSI (IS-IS y ES-IS).

2.2. Tipos de protocolos de routing

La primera distinción que vamos a hacer entre los protocolos de routing va a ser qué protocolos de routing envían su máscara de red y qué protocolos de routing no lo hacen, es decir:

- Routing Classless.
- Routing Classful.

Los protocolos de routing son esencialmente aplicaciones en el router. Su propósito es asegurar el correcto intercambio de información y en un tiempo adecuado entre los routers de la red, para que los routers de la red puedan realizar adecuadamente la función de routing y la de switching.

Los protocolos de routing classful no envían su máscara de red en las actualizaciones. Esto limita el diseño de las redes.

Características:

- La sumarización se realiza en el límite de la red.
- Los routers que intercambian información con redes remotas sumarizan en el límite de la red a direcciones classful de IANA.
- Dentro de la misma red (IANA Classful) se intercambia la información sin máscaras.
- La máscara de subred se supone consistente a las definidas como clase por IANA, así que todos los interfaces de todos los routers tienen que compartir la misma máscara.

En este tipo de protocolos el router toma las decisiones basándose en las reglas del classful, aunque si existe en la tabla de routing una entrada a una ruta más específica a una red, ésta será reenviada a esa red más específica.

Si la red es desconocida el datagrama será descartado.

Si existe una ruta por defecto y la red de destino es desconocida, el datagrama será enviado por la ruta por defecto.

Si existe una red mayor a la solicitada, pero la más restrictiva no existe el paquete será descartado aunque exista una ruta por defecto.

En cuanto al forwarding en protocolos classful:

- Se envía el datagrama a la subred si existe una entrada en la tabla de routing.
- Si no existe la entrada en la tabla de routing, se descarta el datagrama.
- Si existe una entrada para la red mayor, pero no para la subred específica, se descarta el datagrama.

- Si existe una entrada para la red mayor, pero no para la subred específica, no tendremos en cuenta la ruta por defecto, y descartaremos el datagrama.
- Si no existe una entrada para la red mayor o subred del destino del datagrama, se reenviará el datagrama a la ruta por defecto.

Routing Classless:

- Los protocolos de routing classless fueron creados para evitar las limitaciones de los protocolos classful.
- Las características de los protocolos de routing classless son las siguientes:
 - Los interfaces de los routers de la misma red pueden tener diferentes máscaras de subred (VLSM).
 - Los protocolos de routing classless soportan el uso de CIDR.
 - Las rutas pueden ser sumariadas más allá de los límites de las clases de IANA.

Las limitaciones que quedan patentes en los protocolos classful son:

- Utilización ineficiente del espacio de direccionamiento.
- No es posible la utilización de VLSM.
- La no utilización de VLSM provoca que no sea posible cargar tablas de routing muy grandes, ya que saturarían el tráfico de las redes.

Los protocolos de routing classless son:

- OSPF.
- EIGRP.

- RIPv2.
- IS-IS.
- BGP4.

Es interesante tener en este punto el comando `ip classless` de Cisco

- El comando `ip classless` cambia las decisiones que se hacen de forwarding de las entradas de la tabla de routing, no cambia la forma de hacer la tabla, pero si cambia en la forma en la que se realiza el proceso de routing.
- El comando `ip classless` viene en la configuración por defecto de los routers Cisco desde la versión de IOS 12.0, para deshabilitarlo utilizaremos el comando `no ip classless`.
- También tenemos que tener en cuenta en las rutas aprendidas a través de IS-IS u OSPF ignorarán el comando `no ip classless`.

La regla fundamental para trabajar con VLSM es recordar que la finalidad es conseguir un esquema jerárquico para conseguir una estructura lógica estable y sin fallos.

VLSM hace del espacio de direccionamiento eficiente y fuerza una correcta jerarquización, permitiendo sumarización.

2.3. La tabla de routing

```

rou-mad1.acens.net#sh ip route
Codes: 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, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
ia - IS-IS inter area, * - candidate default, U - per-user
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
B 216.221.5.0/24 [200/200000] via 213.11.14.19, 1w5d
B 216.187.99.0/24 [200/200000] via 213.11.14.19, 3d03h
B 210.51.225.0/24 [200/200000] via 213.11.14.19, 3d03h
B 210.17.195.0/24 [200/200000] via 213.11.14.19, 1w5d
B 209.136.89.0/24 [200/200000] via 213.11.14.19, 1w5d

```

En este ejemplo podemos encontrar varios campos, pero los más importante son Red, Interfaz de salida, Métrica y Siguiente salto, por ejemplo, en el caso de la línea:

```
B 210.51.225.0/24 [200/200000] via 213.11.14.19, 3d03h
```

Aquí podemos ver que la Red 210.51.225.0/25 tiene una métrica de 200000, el siguiente salto es 213.11.14.19 y el siguiente salto sería la IP por la que se llega a ese interfaz, en este caso, si hicieramos un show ip route 213.11.14.19 veríamos que es el interfaz fa0/1.

Es muy útil leer la tabla de routing de un router, para ello tendremos que conocer el significado de los campos:

- Red
- Interfaz de Salida
- Métrica
- Siguiente Salto

2.3.1. El campo Red

En cuanto al campo Red podemos decir lo siguiente:

- Este campo contiene las redes que el router conoce.
- Estas redes las ha podido aprender por un proceso estático o dinámico.
- Para poder reenviar un datagrama a la red de destino el router primero tiene que asegurarse que la red existe, esto lo hace comprobando la tabla de routing.
- En la tabla de routing sólo se almacena la porción de la dirección que hace referencia a la red.
- El proceso de routing tomará una decisión basándose en el prefijo más grande encontrado en la tabla de routing.
- La tabla de routing de los routers se mantienen ordenadas, con lo cual se ahorra en el tiempo de búsqueda de información.

Las rutas estáticas son introducidas de forma manual por la persona encargada de configurar el router y las rutas dinámicas son aprendidas de otros routers mediante protocolos de routing.

La ruta por defecto puede ser aprendida por un protocolo de routing o puede haber sido configurada por el administrador de red.

2.3.2. El campo Interfaz

El Campo Interfaz de Salida indica lo siguiente:

- Por qué interfaz será enviado el datagrama.
- A través de qué interfaz se recibe la actualización de routing.

Este campo ayudará al administrador de la red, ya que gracias a él puede saber entre otras cosas por dónde ha venido la actualización de routing y qué interfaz del router es el más próximo a la red en cuestión.

2.3.3. El campo Métrica

- La Métrica es el valor asignado a cada camino basándose en los criterios específicos de cada protocolo de routing y determina el mejor/es camino/s para un destino remoto.
- Por defecto en los routers Cisco si existen varios caminos con la misma métrica se pueden utilizar para balancear la carga utilizando round-robin entre todos. Hasta 6 caminos en paralelo.

Métricas de los Protocolos de Routing:

| Protocolo | Calculo de la Metrica |
|-----------|--|
| RIPv1 | Conteo de saltos |
| RIPv2 | Conteo de saltos |
| IGRP | Ancho de banda, retardo, carga, fiabilidad |
| EIGRP | Ancho de banda, retardo, carga, fiabilidad |
| OSPF | Coste (El estándar no define el coste, pero Cisco utiliza como coste la inversa proporcional al ancho de banda del interfaz) |
| IS-IS | Coste (El estándar no define el coste, pero Cisco utiliza como coste 10 sin tener en cuenta el ancho de banda) |

2.3.4. El campo Siguiente Salto

El siguiente salto indica la dirección del siguiente router del camino. Esta dirección debe de estar en la misma subred que el interfaz de salida, aunque existen excepciones, por ejemplo el siguiente salto en iBGP.

Al identificar el siguiente salto podemos deducir que este salto estará conectado con una trama de capa 2 a nuestro router, lo cual nos permite añadir funcionalidades de troubleshooting.

2.3.5. Cómo mantener la tabla de routing actualizada y precisa

- Dentro de cada router de un sistema autónomo las tablas de routing tienen que estar actualizadas y ser precisas.
- Para ello tenemos que tener en cuenta los tiempos de actualización de cada protocolo (p.e. RIP y OSPF).
- La precisión de la tabla de routing depende de cómo de rápido responda el router a los cambios en la red.
 - Aprendizaje de nuevas redes.
 - Aprendizaje de mejores caminos a redes existentes.
 - Aprendizaje de redes que ya no están disponibles.
 - Aprendizaje de rutas alternativas a una red.

Mientras que RIP v1 envía actualizaciones de su tabla de routing cada 30 segundos a la dirección de broadcast, OSPF lo hace cada vez que sucede un evento a la dirección de multicast.

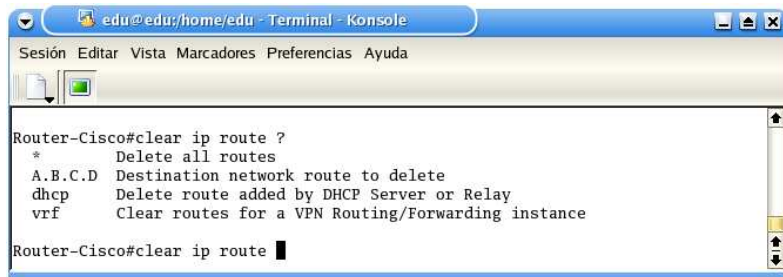
2.3.6. Troubleshooting de las tablas de routing

Para borrar la tabla de routing y obligar al router a volver a aprenderla se utilizan los comandos:

```
Router# clear ip route *
```

O bien

```
Router# clear ip route {red [máscara] | *}
```



```
edu@edu:/home/edu - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

Router-Cisco#clear ip route ?
*          Delete all routes
A.B.C.D    Destination network route to delete
dhcp       Delete route added by DHCP Server or Relay
vrf        Clear routes for a VPN Routing/Forwarding instance

Router-Cisco#clear ip route █
```

El comando `clear ip route` nos permite borrar la tabla de routing completa o de una sola entrada, de modo que obligamos al router a volver a aprender la tabla, y de esta manera podemos comprobar que el funcionamiento es correcto.

Esta prueba dejará al router sin conectividad con las redes remotas durante un lapso de tiempo, con lo que no se puede realizar a la ligera sin conocer los posibles efectos no deseados.

2.4. Métodos de introducir rutas

La forma más simple de mantener una tabla de routing consiste en la utilización de un protocolo de routing.

Pero en el caso que estemos en una red stub o que nuestro router disponga de pocos recursos existen otras posibilidades:

- Rutas Estáticas.
- Rutas Estáticas por Defecto.
- On Demand Routing (ODR).
- Rutas Estáticas Flotantes (Floating Static Routes).

2.4.1. Rutas estáticas

La configuración manual de la tabla de routing significa la utilización de rutas estáticas.

Las ventajas de las rutas estáticas son:

- Conservación de los recursos del router.
- Conservación de los recursos de la red.

La desventaja es:

- Es necesario mucho trabajo por parte del administrador. Si ocurre un cambio en la topología, es el administrador el encargado de solucionar el problema.

La convergencia en este tipo de redes es obviamente lenta y depende del tiempo que tarde el administrador de red en reconfigurar los routers.

Este tipo de routing se suele utilizar en redes especiales.

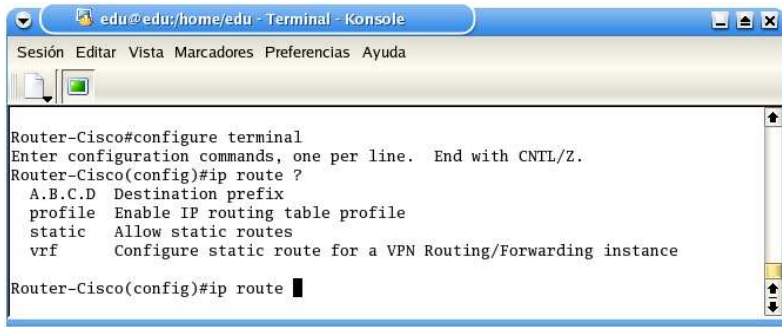
El routing a base de rutas estáticas se suele configurar en redes donde:

- Enlaces con poco ancho de banda (RTC, RDSI).
- El administrador necesita un control total de la red.
- El enlace es un backup de la línea principal.
- Sólo hay un camino al destino, como las redes stub.
- El router tiene los recursos muy limitados y no puede ejecutar un protocolo de routing.
- El administrador necesita permitir redes classful y classless.

2.4.1.1. Comando ip route

Este comando se utiliza para configurar una ruta estática en los routers Cisco comando se utiliza para configurar una ruta estática en los routers Cisco, la sintaxis es la siguiente:

```
ip route prefijo máscara {dirección_ip |  
tipo_de_interfaz número_de_interfaz}  
[distancia] [tag etiqueta] [permanent]
```

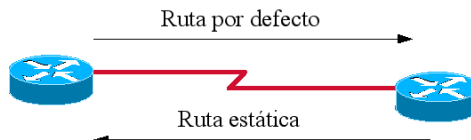


2.4.2. Rutas estáticas por defecto

Una Ruta por Defecto es una ruta que se utiliza si no existe una entrada para un destino específico en la tabla de routing.

Utilizaciones más comunes:

- Conectar una red stub a un sistema autónomo.
- Una conexión a Internet.



Ejemplo de configuración:

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Hemos de tener en cuenta que si ponemos una ruta estática a un router para llegar al otro, el otro tiene que saber volver.

En la ilustración podemos ver un esquema en el cual podemos ver que un router tiene una ruta estática a otro router. El otro router va a tener que tener que conocer lo que hay detrás del router de la izquierda ya sea mediante direccionamiento estático o dinámico, porque si no es así, las peticiones del router de la izquierda le llegarán al router de la derecha, pero no sabrán volver. Es decir, necesitamos un ruta recíproca.

2.4.3. ODR – On Demand Routing

Utilizaremos ODR en una red que dispone de una topología grande y distribuida, donde no es adecuado el routing dinámico, pero tampoco el estático, y en una red que tampoco dispone de mucho ancho de banda disponible.

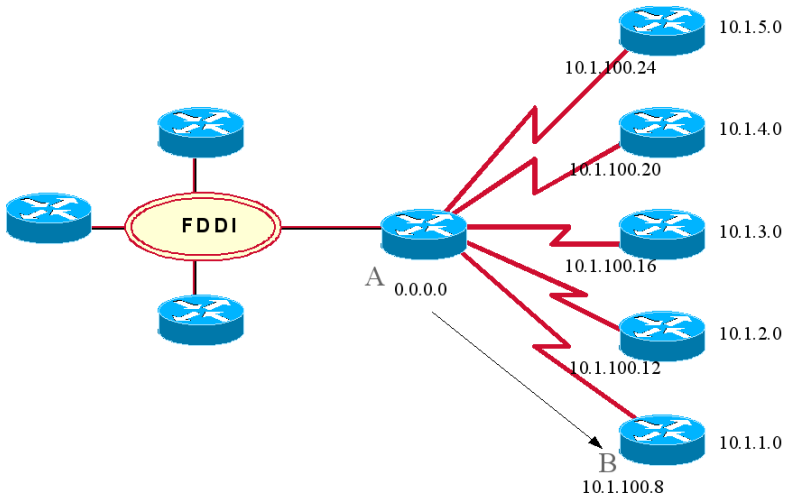
En ODR utilizaremos una topología hub-and-spoke, donde todos los routers spoke tienen una configuración idéntica (obviamente la IP es distinta en cada router).

ODR utiliza CDP para enviar los prefijos de las redes conectadas desde los routers spoke al router hub o central. El router central envía la dirección de su interfaz del enlace compartido como ruta por defecto para el router stub.

ODR permite VLSM y envía sus actualizaciones cada 60 segundos.

Como ODR funciona sobre CDP tenemos que tener habilitado el CDP en nuestros routers, recordemos que para habilitar el CDP es necesario utilizar el comando `cdp enable`.

En la siguiente imagen vemos un ejemplo donde podría resultar utilizar ODR:



2.5. Routing y switching

2.5.1. La función de routing

La función de routing es responsable de aprender la topología lógica de la red y tomar decisiones basadas en ese conocimiento.

Las decisiones determinan si el datagrama entrante puede ser enrutado, y si es así, cómo.

Los pasos para enrutar un datagrama se resumen en las siguientes preguntas:

- ¿Está configurado el protocolo de routing y la pila de protocolos?
- Si está la pila de protocolos, ¿hay alguna entrada para la red remota?
- Si no hay entrada para la red, ¿existe una ruta por defecto?

- Si existe una ruta estática o dinámica, ¿la red está alcanzable?
- ¿Cual es el mejor camino para esa red?
- ¿Hay caminos diferentes con el mismo coste?
- Si existen caminos diferentes con el mismo coste, ¿en que interfaz de salida tiene que ser encolados los datagramas?

Como resumen es conveniente recordar que la función de routing consiste en la determinación de la ruta al destino.

2.5.2. La función de switching

La función de switching se refiere al movimiento de datos dentro del router.

El switching se produce después de la función de routing.

La función de switching realiza las siguientes operaciones:

- Comprueba la validez de la trama entrante.
- Comprueba si la trama ha sido direccionada (capa 2) para el router.
- Comprueba que la trama está dentro del ámbito del entramado.
- Comprueba el FCS (CRC) de la trama.
- Extrae la cabecera y la cola de la trama de capa 2 y comprueba la dirección de destino en la caché.
- Crea una cabecera y cola apropiada y reenvía la trama a la cola del interfaz de salida del router, si es que el destino está en la caché.

La función de routing si ha encontrado que es posible reenviar el datagrama deja el resultado en la caché, y posteriormente la función de switching comprueba en la caché para ver si es posible realizar el switching.

2.5.3. Relación entre la función de routing y la de switching en un router Cisco

Un datagrama es aceptado en el router si la dirección de capa 2 corresponde con alguno de los interfaces.

Si el CRC es correcto, la trama se introduce en el buffer (en memoria principal).

Si la las direcciones de origen y destino de nivel 3 no han sido vistas antes se procederá al proceso de switching o routing:

- Se toma la decisión de reenviar este datagrama.
- El datagrama se encapsula.
- Si está habilitado el Fast Switching se examinará de nuevo y se introducirá en la cache.

La entrada en la caché consiste en:

- Prefijo IP.
- El interfaz de salida.
- La cabecera de nivel de enlace para ser utilizado en la trama saliente.

Si se volviera a encontrar datagramas que coincidieran con el prefijo encontrado se utilizará esta información:

- Tipos de caché en Cisco:
 - Fast switching
 - Autonomous switching
 - Silicon switching
 - Cisco Express Forwarding (CEF)

Capítulo 3

Direccionamiento IP

3.1. Subnetting IP

El subnetting IP hace referencia a cómo están direccionadas las redes IP.

El subnetting también hace referencia a como una gran red de nivel 3 se divide en varias pequeñas de nivel 3.

3.1.1. La necesidad de direccionamiento de nivel 3

- Una dirección de nivel 3 es una dirección lógica situada en la parte superior de la estructura de una red física.
- El direccionamiento de nivel 3 permite direccionar tráfico directamente hacia el destino.
- Este direccionamiento permite encontrar los destinos, ya que la localización se produce ya que el direccionamiento de nivel 3 es jerárquico.

La estructura física y lógica de la red debe de permitir el flujo de datos de la empresa.

Tenemos que tener en cuenta que la estructura tanto física como lógica de la red debe de permitir el flujo de información en la empresa. Esta estructura debe de reflejar el flujo de información de la empresa.

De esta forma los servidores deberían de ser adyacentes en la red física y pertenecer a la misma red lógica que los equipos. Esto hace que la red sea accesible y con un buen rendimiento.

Es muy importante entender el término red en su sentido en el nivel 3.

Una dirección de nivel 3 tiene dos partes:

- Porción de Red: Identifica un grupo de dispositivos individuales.
- Porción de Host: Identifica los dispositivos individuales en un grupo.

El switching de capa 3 y las VLANs son tecnologías de switching que distinguen entre distintas redes lógicas de capa 3.

3.1.2. Posibles definiciones de red

- El trozo de cable o medio físico en el cual están conectados los dispositivos. Esta definición es más precisa que la de segmento.
- Una red de nivel 3.
- La LAN.
- La red organizacional o corporativa.

Las tecnologías de switching de capa 3 nos permiten transferir datos a gran velocidad ya que las decisiones se realizan por hardware.

Si es necesario transferir entre distintas redes lógicas es necesario realizar una decisión de routing, la cual nos llevará más tiempo.

3.1.3. Características de redes de nivel 3

- El número de red define un grupo de dispositivos finales o hosts y etiqueta el grupo con el número de red.
- La dirección es jerárquica, lo cual permite que las decisiones se hagan por grupos de dispositivos.
- Los routers no reenvían broadcast.
- La dirección del grupo se combina con una una que identifica el dispositivo final. Esta es la parte de host.
- El identificador del dispositivo no tiene porque ser único para la organización, tiene que ser único en la red.
- Si el esquema de direccionamiento se realiza adecuadamente, los grupos pueden ser consolidados.
- Las redes gestionadas por un único administrador, ya sea personal física o entidad se llaman Sistemas Autónomos.

En el diseño de redes tenemos que tener especial cuidado con el diseño de los límites de la red, aunque es posible rediseñar los límites de las redes.

Con el uso de VLANs es muy fácil rediseñar los límites de las redes.

3.1.4. Conversión de nivel 3 a nivel 2

- Cuando un sistema final desea comunicarse con otro, la aplicación genera los datos y van bajando por la pila OSI hasta llegar al nivel 3.
- En el nivel 3 se le añade una cabecera con un direccionamiento.
- Acto seguido se le añade un encabezado de nivel 2 con su direccionamiento propio. El direccionamiento de nivel 2 no tiene que ser jerárquico porque se va a encontrar al destinatario en el mismo medio o tecnología.

- El nivel 2 envía a su vez la trama al nivel 1 donde se realiza la transmisión por el medio.
- Al llegar al destino el receptor en el nivel 2 tendrá que hacer las comprobaciones de dicho nivel y posteriormente subir al nivel 3 donde se realizarán las comprobaciones de nivel 3.

Comprobaciones de nivel 2:

- ¿La trama es valida?
- ¿El CRC es correcto?
- ¿El tamaño es adecuado?
- ¿La trama está dirigida a este dispositivo?
- ¿A que protocolo de nivel 3 hay que pasar la información? (IP, IPX ...).
- ¿El nivel 3 se ejecuta en este dispositivo?
- Desempaquetar la trama.
- Pasar la trama al nivel 3.

Comprobaciones de nivel 3:

- ¿El datagrama está destinado a este dispositivo?
- Si es así, se desencapsula el datagrama y se pasa a la capa superior.
- Si la trama no es valida se descarta la trama.
- Si el paquete no está destinado a este equipo y este equipo es un router, se envía al proceso de routing o switching que corresponda.
- El router mirará si la entrada existe en la caché, si existe se realizará el switching, si no se realizará el proceso de routing.

3.1.5. La dirección IP

IP es único porque no tiene ninguna parte de su direccionamiento de nivel 3 fijo como en IPX o AppleTalk.

La dirección IP sólo tiene sentido en conjunción con la máscara de subred.

Las direcciones IP originales están gestionadas por IANA, estas redes pueden ser subdivididas en rangos llamados subredes y se consiguen recolocando los bits de host y de red dependiendo de las necesidades concretas de cada caso.

El término Classful también será designado como Dirección de IANA.

IANA: Internet Assigned Numbers Authority (<http://www.iana.org>).

Terminología utilizada en el direccionamiento IP:

- Dirección proporcionada por IANA.
- Dirección Classful.
- Dirección de Supernet.
- Dirección de Internet.
- Dirección de Red. (Por defecto todas las direcciones son lo que se llamaba en el CCNA Classless).
- Redes Mayores.

3.1.6. Clases de direcciones

| Clase | Primer Octeto | Hosts por red |
|---------|---------------|----------------|
| Clase A | 001 a 127 | 16,77 millones |
| Clase B | 128 a 191 | 65534 |
| Clase C | 192 a 223 | 254 |
| Clase D | 224 a 239 | n/a |
| Clase E | 240 a 255 | n/a |

También podemos decir que:

El primer octeto de las direcciones de clase A comienzan por 0.

El primer octeto de las direcciones de clase B comienzan por 10.

El primer octeto de las direcciones de clase C comienzan por 110.

El primer octeto de las direcciones de clase D comienzan por 1110.

El primer octeto de las direcciones de clase E comienzan por 1111.

3.1.7. Los cuerpos administrativos de Internet

Registradores Regionales:

- Asia-Pacific Network Information Center (APNIC), <http://www.apnic.net>
- American Registry for Internet Networks (ARIN), <http://www.arin.net>
- Réseaux IP Européens (RIPE), <http://www.ripe.net>

Registro de Dominios:

- InterNIC, <http://www.internic.net>

La disposición del límite de la red es una tarea de la organización de la Clase para conseguir el máximo provecho del direccionamiento existente.

Ejemplo de colocación de bits en una dirección de red.

Tenemos lo siguiente:

- 10 bits para la parte de red.
- 22 bits para la parte de host.

10 bits representan: 1024 entradas distintas

22 bits representan 4194304 entradas distintas

Entonces disponemos de:

$1024 * 4194304 = 4294967296$ posibles hosts distintos

3.1.8. La máscara de subred

Para calcular la parte de red utilizaremos la función AND.

La función AND:

```

AND | 1 0
-----
1  | 1 0
0  | 0 0

```

Un ejemplo podría ser este:

```

Direccion IP      144.100.16.8
Máscara subred    255.255.255.0
Binario IP        10010000.01100100.00010000|00001000
Binario Máscara   11111111.11111111.11111111|00000000
-----|-----
Resultado AND     10010000.01100100.00010000|00000000

```

El protocolo ha seguir para el funcionamiento con máscaras de subred se puede encontrar detalladamente explicado en la RFC950 “Internet Standard Subnetting Procedure”.

En el ejemplo se puede ver que la dirección 144.100.16.8 forma parte de la red 144.100.16.8/24.

3.2. Prefijo de routing/CIDR

El subnetting IP hace referencia a cómo están direccionadas las redes IP.

El subnetting también hace referencia a como una gran red de nivel 3 se divide en varias pequeñas de nivel 3.

3.2.1. Definición de: prefijo de routing/CIDR

CIDR es posible gracias a que existen nuevos protocolos de routing que permiten el envío de máscaras de subred.

Prefijo de routing significa que Internet identifica únicamente la organización con los 32-bits de direccionamiento IP. El prefijo establece los límites del grupo de direcciones que forman la red.

CIDR viene definido por los siguientes RFCs:

- 1517: Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR).
- 1518: An Architecture for IP Address Allocation with CIDR.
- 1519: Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy.
- 1520: Exchanging Routing Information Across Provider Boundaries in the CIDR Environment.

3.2.2. Problemas con el direccionamiento IP e Internet

Con el direccionamiento classful existe el problema de la poca granularidad que nos proporciona por lo que se produce un gran desperdicio de direccionamiento público.

La RFC 1466 “Guideliness for Management of IP Address Space” discute el problema que existía con las pocas direcciones asignadas y la gran cantidad de rangos asignados.

El CIDR soluciona estos problemas.

Si una empresa necesita 50 direcciones utilizando classful se le tenía que asignar una clase C.

Si una empresa necesitaba 300 direcciones se le tenía que asignar una clase B.

Todo esto provocaba un enorme gasto innecesario de direccionamiento público.

3.2.3. CIDR como solución

Si una empresa necesita múltiples clases C consecutivas se asignarán sin necesidad de utilizar una clase B y se utilizará como una única red.

| Prefijo | Máscara | Espacio Direccionamiento |
|---------|-----------------|--------------------------|
| /27 | 255.255.255.224 | 12 % clase C, 30 hosts |
| /26 | 255.255.255.192 | 24 % clase C, 62 hosts |
| /25 | 255.255.255.128 | 50 % clase C, 126 hosts |
| /23 | 255.255.254.0 | 2 clases C, 510 hosts |
| /22 | 255.255.252.0 | 4 clases C, 1022 hosts |
| /21 | 255.255.248.0 | 8 clases C, 2046 hosts |
| /20 | 255.255.240.0 | 16 clases C, 4094 hosts |

ARIN, RIPE y APNIC procuran asignar espacios consecutivos a los ISPs, de forma que esto reduzca las tablas de routing de Internet.

Tenemos que tener en cuenta que si una empresa cambia de ISP cambiará también de espacio de direccionamiento IP.

Para tener un ahora de direcciones tenemos que utilizar también otro tipo de técnicas como el NAT, ya que sólo deben de tener direcciones públicas aquellas máquinas que estén en Internet por algún motivo concreto.

3.2.4. Ventajas de prefijo de routing/CIDR

El prefijo de routing se utiliza para reducir el tamaño de las tablas de routing.

Esta técnica permite que los routers de Internet tengan sólo 240.000 entradas para definir el total de Internet y consiste en agrupar las redes a la máscara menos restrictiva posible.

A esta técnica se le llama también sumarización.

Ventajas:

- Reducción del tamaño de las tablas de routing.

- Menos sobrecarga en términos de tráfico, CPU y memoria.
- Mayor flexibilidad en el direccionamiento de las redes.

3.3. VLSM – Variable-Length Subnet Masks

El subnetting IP hace referencia a cómo están direccionadas las redes IP.

El subnetting también hace referencia a como una gran red de nivel 3 se divide en varias pequeñas de nivel 3.

3.3.1. Introducción a VLSM

VLSM es utilizado dentro de la organización, sin embargo CIDR se utiliza fuera de la organización.

La utilización de VLSM dentro de las redes de la organización responde a que rara vez las organizaciones tienen repartidos de forma uniforme los hosts, entonces utilizan VLSM para adecuar la estructura de su red a las necesidades de la empresa.

VLSM hace referencia a la utilización de máscaras de subred de tamaño variable.

Los protocolos de routing que soportan VLSM son:

- RIP v2
- OSPF
- IS-IS
- EIGRP
- BGP-4

Las rutas estáticas también soportarán VLSM.

Los protocolos de routing que no soportan VLSM son:

- RIP v1
- IGRP
- EGP

3.3.2. Reglas para VLSM

Una subred puede ser utilizada como dirección de host o hacer subnetting.

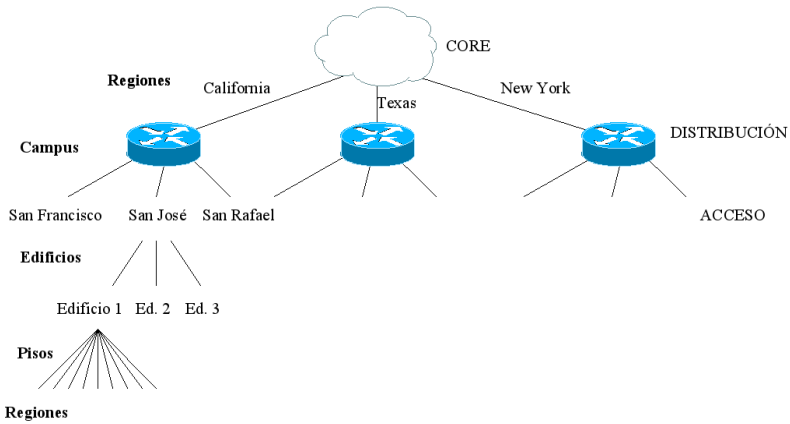
Originalmente no se podían utilizar porciones de subred todo 1s o todo 0s, para poderlas utilizar hay que utilizar el comando `ip subnet-zero`, que se encuentra por defecto a partir de la versión 12.0 de IOS.

El protocolo de routing debe de llevar la máscara en sus actualizaciones.

Múltiples subredes que se quieran sumarizar deben de tener los mismos bits de mayor peso.

Las decisiones de routing se realizan para la subred completa, el router escoge de la máscara más restrictiva a la menos restrictiva para realizar sus decisiones.

3.3.3. Ejemplo: direccionamiento de una red



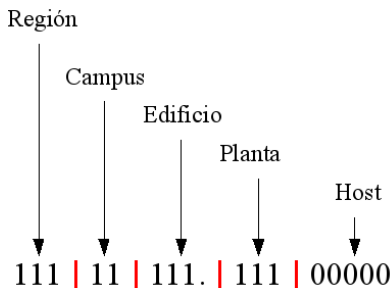
Para el direccionamiento de este caso de estudio tenemos que realizar las siguientes tareas:

- Determinar el número de regiones
- Determinar el número de campus
- Determinar el número de edificios
- Determinar el número de pisos
- Determinar el número de hosts

Para este ejemplo:

- La empresa tiene tres regiones, pero tiene previsto expandirse a no más de 8.
- En cada región no habrá más de 3 campus.
- Cada campus no tiene más que cuatro edificios a lo sumo.
- Los edificios son como mucho de 3 plantas.
- Cada planta no tiene más de 30 PCs.

Según los requerimientos del problema podemos llegar a la siguiente conclusión:



Es decir, la máscara para cada subred de hosts será

/27, es decir, 255.255.255.224.

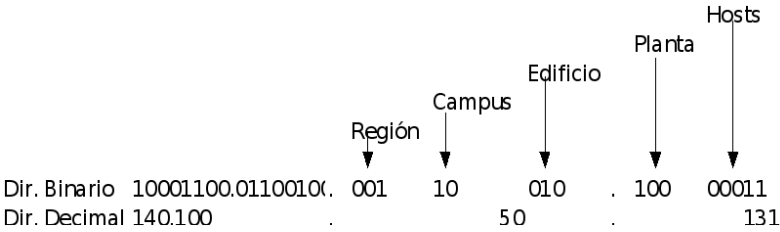
La máscara necesaria para toda la red es una /16.

Hemos de recordar que el número de host de una red es $2^n - 2$, ya que le hemos de restar la dirección de red y la dirección de broadcast.

Distribución de direcciones:

- Región:
 - California: 001
 - Texas: 010
- Campus:
 - San Francisco: 01
 - San José: 10
 - San Rafael: 11
- Edificios:
 - Edificio 1: 0001

- Edificio 2: 010
- Edificio 3: 011
- Edificio 4: 100
- Plantas:
 - Planta 1: 001
 - Planta 2: 010
 - Planta 3: 011
 - Planta 4: 100
 - Planta 5: 101
- Hosts;
 - 1-30



En este gráfico podemos ver que la máquina 140.100.50.131/27 se encuentra en la región de California, campus de San José, Edificio 2, planta 4, y es el segundo host del rango (acordémonos de la dirección de red).

Este esquema jerárquico nos permite sólo con ver la dirección del host saber su situación física exacta.

3.3.4. Optimizando el espacio de direccionamiento IP

- En la conexión de enlaces WAN punto a punto la utilización de las subredes que hemos definido resulta un tanto malgastadora.
- En los enlaces WAN no es conveniente utilizar rangos extensos, sino utilizar rangos más pequeños.

Para este caso en particular la asignación de subredes IP para conexiones WAN podría hacerse de la siguiente manera:

- Utilizamos redes en las cuales la parte de Región, Campus y Edificio es 0, con los que nos quedarán direcciones del tipo 140.100.0...
- El último octeto estaría disponible para hacer VLSM.
- Las subredes de conexión WAN se realizarán utilizando 30 bits para la máscara. Esto nos permite sólo 2 hosts por red, ideal para conexiones punto a punto.
- Entre los edificios de California:
 - 140.100.0.64/27 (30 hosts en Ethernet o FDDI)
- Entre los edificios y los campus en California:
 - 140.100.0.32/30, 140.100.0.28/30, 140.100.0.24/30, 140.100.0.20/30
- Entre los campus y las regiones:
 - 140.100.0.48/30, 140.100.0.4/30, 140.100.0.12/30
- Entre las regiones:
 - 140.100.0.96/30, 140.100.0.16/30, 140.100.0.8/30

Obviamente esta es una forma de hacerlo expuesta como ejemplo, no es la única, llegados a este punto el alumno debería ser capaz de proponer otro esquema de direccionamiento que sea lo más jerárquico posible.

3.4. Sumarización

El subnetting IP hace referencia a cómo están direccionadas las redes IP.

El subnetting también hace referencia a como una gran red de nivel 3 se divide en varias pequeñas de nivel 3.

3.4.1. Introducción a la sumarización

Si se ha realizado correctamente una asignación de direcciones jerárquica resultará muy sencillo realizar una sumarización que permite anunciar las menores rutas posibles o incluso una única ruta, lo que provocará una tabla de routing menor y menor tráfico de actualizaciones.

En el caso de nuestro ejemplo anterior al sumarizar en el límite de la red únicamente se anunciará la red 140.100.0.0/16, con lo que hemos reducido todas las redes en una única sumarizada.

La sumarización forma parte del CIDR y es la extensión del mismo al nivel de la organización.

La sumarización que se produce en la parte superior de la red también se suele designar con el nombre de supernets.

3.4.2. Ventajas de la sumarización

Reducen el tamaño de la tabla de routing.

- Al agregar una única ruta en vez de todas las existentes se consigue reducir el tamaño de la tabla de routing. También se reduce el ancho de banda de las actualizaciones y la carga de CPU y memoria.

Simplifican la recalculación de la red.

- Al ejecutar el algoritmo de routing en un router con una única entrada para la red resulta muy sencillo realizar los cálculos.

Oculto los cambios de la red.

- Al ser vista únicamente una ruta los cambios internos no se ven y quedan ocultos, esto provoca que si se envía un datagrama a una subred inexistente este datagrama nunca llegue y atraviese parte de la red, pero compensa con las ventajas que se obtienen en el routing.

Permite a la red crecer.

- Como la tabla de routing va a consumir menos recursos en los routers, estos serán capaces de agregar más redes con los mismos recursos.

Como resumen tenemos que tener en cuenta que al trabajar con prefijos más pequeños (p.e. /16) se enviarán menos actualizaciones de routing, la ruta será más fácil de calcular y se necesitará menos ciclos de CPU y cantidad memoria principal.

Al consumir menos memoria y CPU permitirá a los routers ser capaces de gestionar redes más grandes con los mismos recursos.

3.4.3. Otras soluciones al agotamiento de direcciones IP

El CIDR y el VLSM ayudan a no gastar innecesariamente direcciones IP, pero existen más métodos.

La utilización de `ip unnumbered`, es útil en enlaces punto a punto porque permite no utilizar una red en este tipo de enlaces.

Cuando utilizamos el comando `ip unnumbered`, el interfaz tomará prestada la dirección IP de otro interfaz

3.4.4. Configuración de la sumarización

En los protocolos más modernos de routing se debe de configurar la sumarización de forma manual, esto proporciona más control sobre la red.

Es muy importante recalcar que tanto BGP como EIGRP realizan la sumarización de forma automática por defecto, de todos modos más adelante se profundizará sobre este aspecto.

3.4.5. Sumarización automática

Los protocolos de routing antiguos como RIP o IGRP sumarian de forma automática a la clase en el límite de la red. Esto lo hacen porque no son capaces de transportar la máscara.

La sumarización automática utiliza la regla del primer octeto.

La regla del primer octeto hace referencia a que los primeros bits de la dirección IP nos indican a qué clase pertenece:

- 0: Clase A
- 10: Clase B
- 110: Clase C
- 1110: Clase D
- 1111: Clase E

3.4.6. Sumarización manual

EIGRP, IS-IS, RIP v2 y BGP permiten VLSM y sumarización manual, esto permite:

- Granularidad del diseño jerárquico.
 - Permite conocer con mayor precisión una red grande.
- Sumarización manual.
 - La sumarización se realiza bajo configuración.
- Redes discontinuas.

- Una red dividida por otra red diferente en el medio.

La sumarización manual permite un control mayor sobre la red y solucionar problemas como el de las redes discontinuas que no pueden ser tratados ni con RIP v1, ni con IGRP.

3.4.7. Redes discontinuas

Como redes discontinuas entendemos a una red que está dividida por otra red clasful que divide las dos partes de la misma red clasful.



En el caso de un router que esté ejecutando un protocolo de routing clasful no va a saber por qué camino enviar el datagrama y es probable que balancee el tráfico, como resultado, la mitad de los datagramas se perderán.

Este caso se puede dar por un diseño intencionado o por un error en la topología de la red, pero en cualquier caso en el supuesto de utilizar un protocolo de routing clasful tendremos un problema.

3.4.8. Consideraciones de sumarización para redes discontinuas

Las redes discontinuas no son un problema para los protocolos de routing que permiten VLSM, pero sí lo es si se realiza una sumarización automática.

En estos casos no podemos permitir que se produzca la sumarización automática y tenemos que utilizar la sumarización manual que le permitirá al administrador evitar este tipo de problemas, y le dará mayor granularidad a la red.

Tenemos que tener cuidado con EIGRP que aunque es un protocolo VLSM por defecto realizará una sumarización a la clase en el borde de la red. Para evitar esta situación EIGRP tiene la posibilidad de sumarizar a nivel de interfaz y decidir que interfaces no queremos que se sumaricen.

La clave para entender cuando una red es sumarizable es observar si existen bits comunes de mayor orden.

Si la sumarización no es posible, tenemos dos opciones:

- No sumarizar, pero entender que la red tendrá limitaciones de escalabilidad.
- Rehacer el diseño de la red para hacerla sumarizable.

Capítulo 4

Diseño de redes IP

4.1. Criterios de diseño de redes IP

El subnetting IP hace referencia a cómo están direccionadas las redes IP.

El subnetting también hace referencia a como una gran red de nivel 3 se divide en varias pequeñas de nivel 3.

4.1.1. El diseño jerárquico de Cisco

La clave del diseño es hacerlo jerárquico, con una división de la funcionalidad entre niveles de la jerarquía.

En el diseño de red jerárquico, cada nivel actúa como filtro para el segundo nivel, esto hace que la red sea escalable ya que se limita la cantidad de tráfico que puede pasar a través de los niveles.

Sólo los datos e información global necesitan salir del dominio inmediato o nivel.

Cisco propone el modelo en capas para conseguir una red estable y fiable.

Cisco proporciona un modelo jerárquico de diseño que simplifica la gestión de red y permite que la red pueda crecer

Se consigue una red estable y fiable porque se mantiene el tráfico local dentro del área, con lo cual este no tiene que traspasar al resto de los niveles de la jerarquía.

El número de niveles que se va a implementar en cada red difiere de las aplicaciones que se vayan a ejecutar, pero Cisco sugiere que con tres niveles tendríamos suficiente para una red de grandes dimensiones.

4.1.2. Funciones de cada nivel

Cada nivel del modo jerárquico es responsable de prevenir tráfico innecesario de ser reenviado a los niveles superiores.

Los tres niveles son:

- El nivel de acceso.
- El nivel de distribución.
- El nivel de core o núcleo.

4.1.2.1. Nivel de acceso

Nivel donde se conectan los dispositivos finales. Los dispositivos de nivel 3 de este nivel son los encargados de controlar que el tráfico local no pase a los niveles superiores.

La clasificación de QoS se proporciona aquí.

Los filtros SAP de Novell y las listas de zona de Appletalk también se aplican en este nivel.

4.1.2.2. Nivel de distribución

Proporciona conectividad entre muchas partes del nivel de acceso.

En este nivel de configuran access-lists, no como filtros, sino como primer nivel de una rudimentaria seguridad.

En este nivel se proporciona acceso a Internet, el cual requerirá de un firewall o de una seguridad más sofisticada.

4.1.2.3. Nivel de core o núcleo

La responsabilidad principal del nivel de core es interconectar la empresa entera, esto lo hace interconectando los dispositivos del nivel de distribución.

Para asegurar una continuidad de este nivel el nivel de core tiene que ser altamente redundante.

En el nivel de core la información tiene que estar lo menos posible, la información tiene que discurrir tan rápido como sea posible.

Ya que la toma de decisiones requiere un tiempo, esto producirá latencia, y por tanto todo este tipo de trabajo no se realizará en el nivel de core.

Aunque muchas implementaciones la QoS se implementa en este nivel de la jerarquía.

Es muy importante recalcar que el nivel de core tiene que ser altamente redundante, ya que un corte en este nivel podría dejar a gran parte de la organización sin conectividad.

4.1.3. Access-list IP

4.1.3.1. Seguridad con access-lists

Cisco recomienda utilizar métodos alternativos a los access lists para seguridad.

Algunas tareas simples de seguridad pueden ser realizadas con access lists, pero los access lists no constituyen una seguridad compleja y completa.

El procesado de la seguridad es preferible que sea realizado por un firewall, ya que estos dispositivos están pensados para llevar esta carga.

Si existe la posibilidad de balancear entre dispositivos, esto debería ser tópico de un proyecto de plan de capacidad.

Como resumen podemos decir que los access list no son herramientas de seguridad y que esta es preferible delegarla en firewalls.

Ejemplo de Access List:

```
Router(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 any eq 23
Router(config)# access-list 101 permit ip any any
(deny implícito)
Router(config)#interface ethernet 0
Router(config-if)#ip access-group 101 out
```

4.1.3.2. Controlando el acceso al terminal

Para controlar el tráfico por telnet en el cual el router es el dispositivo final, se puede situar un access list para esta función.

Por defecto se encuentran disponibles 5 sesiones de terminal (vty 0 .. vty 4).

Ya que es complicado predecir cual va a ser la sesión utilizada, el control generalmente se realiza de forma uniforme.

Sin embargo existen equipos que tienen limitaciones diferentes en cuanto al número de interfaces vty que pueden ser creados.

La configuración de los access lists es preferible aplicarlos juntos como único access-class:

Ejemplo de Access List para el telnet:

```
access-list 12 permit 192.168.1.0 0.0.0.255
(deny implícito)
!
line vty 0 4
access-class 12 in
```

4.1.4. Controlar el tráfico a través de las actualizaciones de routing.

4.1.4.1. Distribute lists

Definimos distribute lists como los access lists aplicados a los protocolos de routing para restringir la información enviada en las actualizaciones.

Se utilizan distribute lists para:

- Ocultar redes (investigación, test o simplemente privadas).
- Reducir el tráfico en las actualizaciones de routing.
- Prevenir bucles causados en la redistribución de múltiples protocolos de routing.

La gestión del tráfico es más sencilla de configurar a nivel 3. Sin embargo hay que tener cuidado, ya que, limitando el tráfico también se limita la conectividad.

Este caso requiere tener cuidado con el diseño y la documentación.

4.1.4.2. Otras soluciones para controlar el tráfico

Modificar los temporizadores de los protocolos de routing.

En los enlaces WAN podría ser ventajosa utilizar routing estático.

Snapshot routing: esta podría ser una solución para enlaces WAN bajo demanda.

Realizar un diseño de direccionamiento IP adecuado y jerárquico, sobre todo si se tienen que ejecutar aplicaciones cliente/servidor, es decir, una ingeniería de red adecuada.

La modificación de los temporizadores de los protocolos de routing en los routers hace que los protocolos hagan los anuncios con otra frecuencia, el problema es que también van a esperar esos anuncios con otra frecuencia, así que es necesario modificar los temporizadores

en todos los routers afectados, si no se hiciera así las tablas de routing acabarían por estar desincronizadas.

En el caso de utilizar routing estático hemos de tener en cuenta que existen protocolos como EIGRP y OSPF que se actualizan por disparos y de forma incremental, con lo que podría ser una solución.

El snapshot routing permite que sus actualizaciones sean realizadas de forma periódica o cuando el enlace esté arriba.

4.1.5. Priorización

Los access lists no se utilizan para determinar que paquetes son reenviados a un destino, sino para determinar el orden en el cual el tráfico está pensado en abandonar el interfaz.

Se encuentran disponibles varios tipos de priorización, también llamados «queuing techniques».

Es importante basar el plan de priorización en el conocimiento de la red, de forma que el tráfico más sensible sea enviado antes.

4.1.6. WFQ – Weighted Fair Queuing

Es la técnica de priorización por defecto en las versiones más modernas de IOS.

- Reemplaza el antiguo modo de priorización FIFO.
- WFQ analiza los patrones de tráfico del enlace, basándose en el tamaño de los paquetes y la naturaleza del tráfico, para distinguir tráfico interactivo de transferencia de ficheros.

4.1.7. Técnicas de queuing

Estas técnicas de priorización son configuradas de forma manual utilizando access lists.

4.1.7.1. Priority queuing

Divide el buffer del interfaz de salida en cuatro colas virtuales.

Los rangos de importancia o prioridad asignan el tráfico en cada cola.

Se asegura que en enlaces lentos o congestionados el tráfico sensible se procese antes.

4.1.7.2. Custom queuing

Divide el buffer del interfaz de salida en varias subcolas virtuales.

Cada cola tiene un umbral con un número de bytes o datagramas a ser enviados antes de pasar a la siguiente cola.

Para asignar el tráfico en una cola se utilizan ACLs.

4.1.7.3. Class-based Weighted Fair Queuing (CBWFQ)

Método extendido del WFQ para proporcionar clases de tráfico por usuario definido.

Los datagramas se van encolando mediante ACLs.

4.1.7.4. Low-latency queuing (LLQ)

Esta característica aplica una cola estricta de prioridad a CBWFQ.

Con el comando `priority` se asigna a las colas de datos sensibles al retardo (p.e. VoIP)

Si la cola está vacía se puede enviar otro tipo de tráfico.

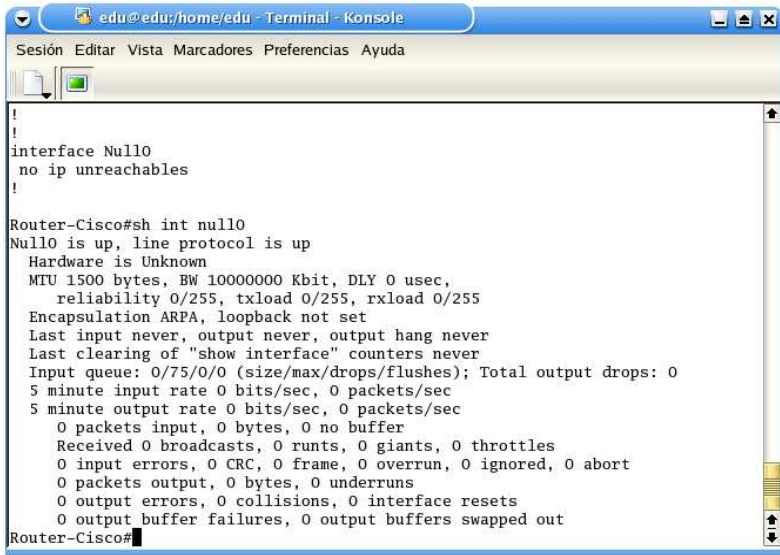
4.1.8. Reduciendo el tráfico de la red: alternativas a los ACLs

Los ACLs requieren una gran cantidad de recursos se tiene que buscar alternativas.

Interface `null0`:

- Una solución puede ser la creación de un interfaz que sólo exista en el sistema operativo.
- Este interfaz responderá a ping con un mensaje de Unreacheable al origen, para deshabilitar el envío de Unreacheable, configuraremos en el interfaz.

```
Router(config-if)#no ip unreachable
```



```
edu@edu:/home/edu - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

!
!
interface Null0
no ip unreachable
!

Router-Cisco#sh int null0
Null0 is up, line protocol is up
  Hardware is Unknown
  MTU 1500 bytes, BW 10000000 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation ARPA, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
Router-Cisco#
```

4.1.9. Puntos importantes a recordar al diseñar una red IP

1. Identificar hosts y subredes necesarias ahora y en un futuro, así como interconexión de departamentos, crecimiento de personal y presupuesto para el crecimiento de la red.

2. El diseño debe tener en cuenta los equipos de red disponibles y los posibles proveedores.
3. Para ofrecer sumarización (agregación de rutas), asignación de direcciones de acuerdo con la topología.
4. Si se utiliza VLSM, el protocolo de routing debe incorporar el envío de máscaras en las actualizaciones.
5. Si se utiliza VLSM, el protocolo de routing debe seleccionar las rutas con el prefijo más largo.
6. Comprobar que se han asignados los bits suficientes a cada nivel de la topología.

Al diseñar una red tenemos que tener en cuenta si se trata de adaptar una red existente o crear una desde cero.

También tenemos que tener en cuenta todos los puntos que hemos visto hasta ahora.

4.1.10. Diseño IP para una red existente

Cualquier diseño de red requiere un análisis muy cuidadoso de la red actual y un conocimiento muy claro de los planes futuros de la organización en cuanto a expansión de la red.

Lo primero que tenemos que determinar es si es posible la sumarización, para ello tenemos que tener en cuenta:

- El esquema de direccionamiento debe reflejar la topología física de la red.
- La topología tanto física como lógica debe respetar el diseño jerárquico.
- El esquema de direccionamiento debe permitir sumarización.
- La naturaleza debe reflejar el diseño jerárquico.
- El protocolo a utilizar debe permitir VLSM.

4.1.11. Tendencias en el diseño IP

Para mayor flexibilidad de la red muchas empresas utilizan en el diseño de la red servidores de DHCP y de DNS.

Naturaleza del tráfico basado en aplicaciones cliente / servidor.

Utilización de VLSM, ya que permite evitar las limitaciones del direccionamiento clasful de IANA.

Utilización de direccionamiento privado.

4.2. Direccionamiento privado

El subnetting IP hace referencia a cómo están direccionadas las redes IP.

El subnetting también hace referencia a como una gran red de nivel 3 se divide en varias pequeñas de nivel 3.

El direccionamiento público no es requerido si la compañía no tiene sus máquinas dentro de Internet.

Una de las ventajas del direccionamiento privado es que los routers en Internet no entienden este tipo de direccionamiento.

El direccionamiento privado junto con Ipv6, CIDR y VLSM son las soluciones propuestas por la comunidad de Internet para evitar el agotamiento de direcciones IP públicas de versión 4.

El direccionamiento privado viene descrito en las RFCs 1597 y 1918.

Las direcciones privadas (RFC 1918) no pueden ser enrutadas en Internet y serán descartadas.

Este direccionamiento permite que sea utilizado en las redes internas de las organizaciones, y que muchas organizaciones tengan el mismo direccionamiento privado idéntico.

Direccionamiento Privado descrito en la RFC 1918

| Rango de Direcciones | Prefijo | Redes Classful |
|-------------------------------|---------|----------------|
| 10.0.0.0 a 10.255.255.255 | /8 | 1 Clase A |
| 172.16.0.0 a 172.31.255.255 | /16 | 16 Clases B |
| 192.168.0.0 a 192.168.255.255 | /24 | 256 Clases C |

El uso de direcciones IP privadas en las LAN de las empresas se ha extendido gracias al NAT.

El uso de direccionamiento privado se ha extendido enormemente, esto significa que una empresa no tiene que solicitar direcciones públicas a IANA.

Las direcciones privadas no tienen significado global, esto significa que para salir a Internet es necesario utilizar un gateway que pueda hacer la traducción a dirección globalmente válida, esto se hace con NAT – Network Address Translation.

4.2.1. Razones para utilizar direccionamiento privado

El direccionamiento privado es muy útil por los siguientes motivos:

- Ordenación del direccionamiento dentro de la organización.
- Seguridad.
- Si existe un cambio de ISP el direccionamiento se mantiene.

El direccionamiento privado proporciona seguridad a la empresa porque la red interna no es visible desde Internet.

Recordemos que el direccionamiento público va a venir dado por el ISP, si cambiamos de ISP cambiará el direccionamiento, por lo que es interesante tener en cuenta que como el direccionamiento privado no depende de ningún ISP podremos mantener el direccionamiento interno de la organización.

4.2.2. Conceptos al tener en cuenta al utilizar direccionamiento privado

Si los hosts internos necesitan conexión con el exterior necesitaremos alguna forma de traducción de direcciones.

Como el direccionamiento privado no tiene significado global no se propagarán las rutas por Internet.

El futuro es posible que nuestra empresa se fusione con otra con el mismo direccionamiento.

NAT no permite siempre seguridad y encriptación IP.

Si las rutas privadas no se transportan por Internet y queremos unir varias oficinas por Internet tendremos que buscar alguna solución alternativa.

4.3. Network address translation

4.3.1. Conexión con Internet mediante NAT

Para poder salir a Internet es necesario utilizar traslación de direcciones o utilizar direccionamiento público proporcionado por el ISP.

NAT es el método de traducir una dirección de una red en otra de otra red cuando la dirección de origen está en una red ilegal o no válida en la red de destino.

El RFC que define el NAT es el RFC 1631 “The IP Network Address Translator”.

NAT se ejecuta en un dispositivo o router de nivel 3 ya que realiza traslación de direcciones de capa 3.

NAT muchas veces se ejecuta en firewalls, ya que la posición de los firewalls es una excelente elección para organizaciones que utilicen direccionamiento definido en la RFC 1918.

4.3.2. Utilidades de NAT

Organizaciones que utilizan direcciones asignadas a otras empresas.

Organizaciones que utilizan direccionamiento RFC1918 y quieren conectarse a Internet.

Para interconectar dos organizaciones que utilizan el mismo direccionamiento.

Organizaciones que desean ocultar su IP tras un firewall como política de seguridad.

Cisco soporta NAT en la mayoría de sus plataformas, incluyendo los firewalls PIX - ASA.

A partir de la versión de IOS 11.2 había que comprar el software extra para poder ofrecer NAT.

A partir de la versión de IOS 12.0 NAT venía ya incorporado dentro del software estándar.

4.3.3. Características de NAT

Direccionamiento estático: Traducción uno a uno configurada de forma manual.

Traducción de direcciones de origen dinámicas: Se define un rango de direcciones, estas direcciones son las que se traducen.

Port Address Translation – PAT: Diferentes direcciones dentro de una organización son traducidas a una única dirección pública. El identificador de puerto TCP o UDP es el que identifica a cada una de las estaciones. Se identifican las direcciones locales a través de los puertos.

Traducción rotatoria de la dirección de destino (Destination Address Rotary Translation): Definido para tráfico entrante en la red. La dirección foránea se mapea con un ACL con una dirección interna. Este tipo de traducción sólo se puede realizar con TCP. Direccionamiento estático.

4.3.4. Funciones principales de NAT

Para traducir de una dirección de una red a otra, el proceso debe diferenciar entre la funcionalidad de las direcciones que van a ser traducidas.

Inside Global: Direcciones que conectan la organización con Internet, proporcionadas por el ISP. Estas direcciones se propagan por Internet. Estas direcciones son las que explican como las direcciones inside son vistas globally por el exterior.

Inside Local: Direcciones que permiten a los dispositivos de la organización comunicarse entre sí. Pueden ser direcciones RFC1918. Son direcciones inside que son vistas locally por el resto de los equipos de la organización.

Outside Global: Son direcciones de Internet. Son direcciones que están outside y aparecen como globally en Internet.

Outside Local: Son direcciones no RFC1918 que se utilizan dentro de la organización, entonces estas direcciones existen outside, pero en nuestra red se ven locally.

4.4. Introducción a IPv6

IPv6 es la solución para muchas de las limitaciones de direccionamiento existentes en IPv4.

IPv6 cuadruplica la dirección, pasando de 32 a 128 bits.

Este tamaño de dirección permite unas 1030 direcciones por cada persona del planeta.

En IPv6 se encuentran implementadas soluciones más eficientes para:

- QoS.
- Seguridad.

4.4.1. Beneficios y características de IPv6

- Espacio de direccionamiento mayor.
- Direccionamiento Unicast y Multicast.
- Agregación de Direcciones.
- Autoconfiguración.
- Renumeración.
- Cabecera simple y eficiente.
- Seguridad.
- Movilidad.
- Opciones de transición de IPv4 a IPv6.
- Protocolos de Routing.

4.4.2. Formato de direcciones IPv6

Direcciones de 128 bits, en vez de 32.

Notación hexadecimal, se separan por dos puntos (:) campos de 16 bits.

- Ejemplo de Dirección IPv6

4021:0000:240E:0000:0000:0AC0:3428:121C

Las direcciones de IPv6 pueden simplificarse utilizando las pautas de la RFC 2373 “IP Version 6 Addressing Structure”.

Para evitar confusiones se han establecido una serie de reglas que simplifican el uso de las direcciones IPv6.

- Los números hexadecimales no son case sensitive, para prevenir errores del operador.

- Los 0s de la izquierda pueden ser eliminados y simplemente poner los (:).
- Un par de dos puntos (::) indican existen grupos de 16 bits que son ceros, pero sólo puedo poerlo una vez.
- En cada dirección sólo se permite un par de dos puntos (:), es decir:
 - 4021:0000:0000:0000:0000:0000:AC21:BCD
 - 4021::AC21:BCDE

4.4.3. Direcciones de IPv6 de unicast

Las direcciones de unicast de IPv6 están divididas de acuerdo a su funcionalidad.

Una dirección de unicast es una dirección que especifica a un nodo de forma única.

Tipos de direcciones Unicast:

- **Link Local:** Dirección en la cual el destino se encuentra en mismo medio físico. Aquí se incluyen protocolos de descubrimiento, de routing, y otros protocolos de control. El prefijo de estas direcciones es FE80::/10.
- **Site Local:** Este es un sistema que se encuentra en el el mismo sitio, pero en redes diferentes, no requiere conexión a Internet, por lo que el direccionamiento no tiene que ser único.
- **Aggregate Global Unicast:** Dirección de Internet globalmente única.
- **Unspecified and Loopback:** Dirección de loopback. Estación es ::1. Se utiliza para testear el hardware.

4.4.4. Direcciones IPv6 de multicast

Una dirección de multicast es una dirección que identifica un grupo de interfaces, por lo que para ciertas tareas es mucho más eficiente que una dirección de broadcast.

Teóricamente los routers no deberían de propagar multicast ya que no propagan datagramas con direcciones desconocidas, pero en tecnologías LAN se pueden propagar estos broadcast.

IPv6 no utiliza broadcast: RFC 2365 “Administratively Scoped IP Multicast”.

El prefijo de las direcciones de multicast en IPv6 se encuentran en el rango FF00::/8 – FFFF::/8.

El segundo octeto seguido de FF identifica el ámbito y el tiempo de vida de la dirección de Multicast.

Si un sistema que recibe un multicast no forma parte del grupo de multicast descartará el datagrama a nivel 2.

4.4.5. Agregación de rutas en IPv6

La sumarización es crucial en Internet sea cual sea el protocolo de capa 3 enrutado.

Como IPv6 permite un número casi infinito de direcciones la sumarización y el modelo jerárquico es fundamental.

Los primeros 48 bits de la dirección son utilizados para routing externo de IANA, y así crear lo que se llama el “Aggregate Global Unicast”.

Los últimos 3 bits anteriores son fijos 001 y se utilizan para indicar que es una dirección global.

El Site Level Aggregator (SLA) es la dirección utilizada para el routing dentro del sistema autónomo y funciona de una forma similar al direccionamiento privado de IPv4.

La dirección del interfaz se suele autoconfigurar utilizando la dirección MAC del interfaz.

La dirección IPv6 que es única en Internet se llama Agregate Global Unicast.

| | |
|-----------------------------|---------|
| Prefijo de IANA | 45 bits |
| Prefijo fijo 001 | 3 bits |
| Site Level Aggregator (SLA) | 16 bits |
| Interfaz | 64 bits |

4.4.6. Autoconfiguración

El router local o directamente conectado envía su prefijo y la ruta por defecto que tenga. Esto se envía por el cable, permitiendo que los routers vecinos configuren automáticamente su dirección IPv6.

- El router local proporciona el prefijo global de 48 bits y el SLA (Site Level Aggregator) a cada uno de los sistemas finales.
- El sistema final simplemente añade su dirección de nivel 2, utilizando la MAC.

Esta capacidad de IPv6 de asignar direcciones sin necesidad de ningún servidor de DHCP hace que Internet llegue a ser plug-and-play.

4.4.7. Renumeración

Mientras que en IPv4 tenemos que establecer una gran cantidad de tiempo en hacer el plan de direccionamiento de la red con IPv6 como acabamos de ver no es necesario.

La autoconfiguración permite la renumeración de las direcciones de la red en caso de cambio.

4.4.8. Cabecera simple y eficiente

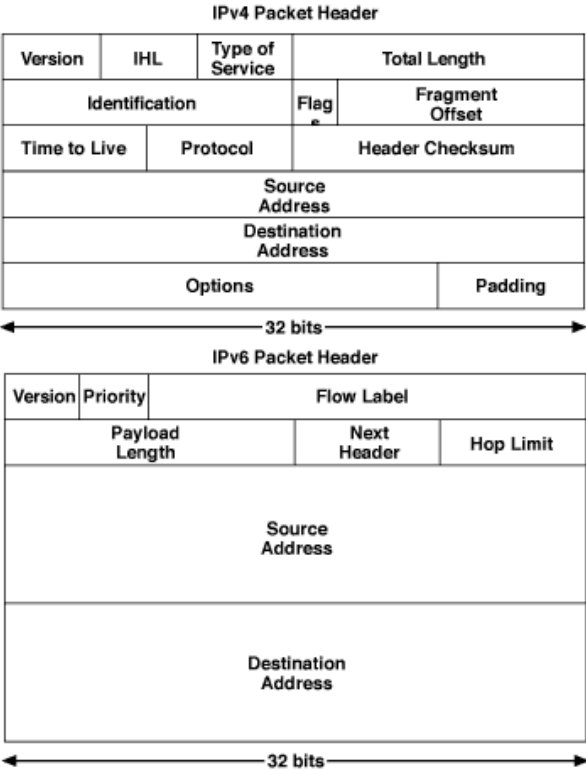
La cabecera de IPv6 ha simplificado el proceso necesario para que el router trabaje con ella, aumentando el rendimiento y la eficiencia del router, debido a:

- Menos campos en la cabecera.
- Los campos se alinean a 64 bits.
- La suma de comprobación ha sido eliminada.

Los microprocesadores actuales funcionan con palabras de 64 bits, esto hace que los campos tengan la medida atómica, el único problema es la dirección que ocupa 2 palabras de memoria.

La eliminación de la suma de comprobación también ha ayudado al aumento del rendimiento en los routers.

4.4.9. Cabeceras de IPv4 e IPv6



4.4.10. Campos de extensión de la cabecera IPv6

En IPv6 desaparece el campo de opciones, en su lugar vamos a utilizar el campo “Next Header”, en el que indicaremos si hay algo más por procesar, esto aumenta el proceso porque se pueden encadenar varios campos de extensión.

4.4.11. Seguridad en IPv6

La conexión directa entre extremos permite que la seguridad sea más realista, ya que la necesidad de NAT y firewalls decrece.

En IPv4 IPSec es opcional, sin embargo en IPv6 es mandatoria u obligatoria.

Los campos de extensión permiten una seguridad dedicada al protocolo extremo a extremo.

4.4.12. Movilidad en IPv6

La cabecera de routing de IPv6 permite cambiar su dirección IP si el host final utiliza una home address como origen de los datagramas.

La home address es estable y no cambia, permitiendo de esta manera la movilidad.

En IPv4 tenemos una cosa parecida llamada routing triangular, que consisten en hacer un túnel hasta la red anfitriona y desde allí enrutar hasta el destino.

4.4.13. Transición de IPv4 a IPv6

La llave para el éxito de IPv6 no reside en su funcionalidad y eficiencia, sino a la capacidad de transición de IPv4 a IPv6. La transición requiere:

- Nuevo direccionamiento.
- La instalación de una nueva pila de protocolos.
- Nuevas aplicaciones que puedan comunicarse con esta nueva pila.

Para hacer la transición tenemos que instaurar IPv6 en los bordes de la red e ir avanzando poco a poco hasta el core, pero al hacer esto pueden pasar tres cosas:

- IPv6 tenga que ser transportada sobre IPv4.
- IPv4 e IPv6 tengan que convivir en la red.
- Un protocolo tenga que ser traducido a otro.

4.4.14. Métodos de transición

- IOS dual stack:
 - Conviven las dos pilas de protocolos y es el DNS el que indica qué pila se debe de utilizar en cada caso.
- Túneles configurados:
 - Se configuran túneles estáticos para permitir la comunicación de IPv6 sobre IPv4.
- Tunneling 6to4:
 - A los routers que interconectan las redes IPv6 con la red IPv4 de paso se les configuran los interfaces con direcciones fácilmente traducidas a IPv4.
 - Se utiliza el prefijo 2002::/16 y se le añade una dirección IPv4.

4.4.15. Protocolos de routing de IPv6

A partir de la release 12.2T de IOS se permiten los protocolos de routing de IPv6:

- RIPng
- OSPF
- IS-IS
- BGP-4

Evidentemente para que los protocolos de routing puedan transportar direccionamiento IPv6 es necesario realizar unos cambios para adaptarlos a las nuevas necesidades.

Capítulo 5

Protocolos vector distancia

5.1. Presentación

Entendemos como protocolos de routing vector distancia a aquellos protocolos de routing que algoritmos de vector distancia (p.e. Bellman Ford).

- Classful: RIPv1 e IGRP.
- Classless: RIPv2 e IGRP.

Aunque IGRP y EIGRP no sean estrictamente protocolos podemos considerarlos como tal debido a sus características principales fundamentales.

5.1.1. Operación de los protocolos de routing vector distancia

Los protocolos de routing de vector distancia envían actualizaciones de rutas periódicas a los vecinos directamente conectados.

El temporizador se resetea justo después de realizar un envío.

Después de recibir la tabla de routing de un vecino, el router actualiza su tabla de routing envía su tabla modificada en las siguientes actualizaciones.

Los protocolos vector distancia son protocolos classful, entendiendo que sumarizan de forma natural en al límite de la red a la clase de IANA o al límite de la red mayor. Utilizan la regla del primer octeto.

Las actualizaciones incluyen la tabla de routing completa, excluyendo la red del interfaz por la que se ha aprendido esa ruta. (Horizonte Dividido)

En la implementación de la regla del horizonte dividido se utiliza para evitar tráfico innecesario en la red y para evitar bucles.

5.1.2. Técnicas para evitar bucles

Los protocolos de routing de vector distancia utilizan las siguientes técnicas para evitar bucles:

- Split Horizon.
- Poison Reverse.
- Holddown.
- Triggered Updates.
- Aging of Routes.

El conteo al infinito no se puede cosiderar una técnica.

5.1.3. Métricas de los protocolos de routing de vector distancia

La métrica utilizada por estos protocolos es el “conteo de saltos” o routers encontrados en el camino.

IGRP y EIGRP se consideran de Vector Distancia aunque sus métricas no sean saltos. Tenemos que tener en cuenta que ni IGRP ni EIGRP utilizan saltos como métricas, y EIGRP además utiliza el algoritmo DUAL.

5.2. RIP

5.2.1. Introducción histórica

Uno de los protocolos de routing más antiguos es el Routing Information Protocol o más comúnmente llamado RIP. RIP utiliza algoritmos de vector distancia para calcular sus rutas. Este tipo de algoritmos para calcular rutas fueron utilizados durante décadas en sus distintas variantes. De hecho los algoritmos de vector distancia utilizados por RIP están basados en aquellos algoritmos utilizados por ARPANET en el año 1969.

Los protocolos vector distancia fueron descritos académicamente por: R.E. Bellman, L.R. Ford Jr y D.R. Fulkerson.

La primera organización que implementó un protocolo de vector distancia fue la compañía Xerox en su protocolo GIP (Gateway Information Protocol), este protocolo estaba incluido dentro de la arquitectura XNS (Xerox Network Systems). GIP se utilizaba para intercambiar información de routing entre redes o sistemas autónomos no adyacentes. Pero claro, Xerox había implementado su propio protocolo propietario.

Poco después la University of California en Berkeley creo una variante llamada “routed”, esta variante del GIP introdujo novedades como modificación del campo de direccionamiento, que se consiguió más flexible, también se añadió un temporizador que limitaba a 30

segundos el tiempo máximo de actualización, es decir, el tiempo máximo permitido sin saber la información de los vecinos, y por supuesto se integró dentro de UNIX, con lo cual pasó a ser abierto.

El protocolo RIP, tal cual lo conocemos actualmente, fue descrito por primera vez en el RFC 1058 (<http://www.rfc-editor.org/rfc/rfc1058.txt>) por C. Hedrick de la Rutgers University en Junio de 1988, y posteriormente fue mejorado en la RFC 2453 (<http://www.rfc-editor.org/rfc/rfc2453.txt>) por G. Malkin de la compañía Bay Networks en Noviembre de 1998.

Desde el año 1998 el protocolo RIP se ha mantenido estable, aunque posteriormente salió la versión para Ipv6.

5.2.2. Introducción técnica

RIP es un protocolo de routing de vector distancia muy extendido en todo el Mundo por su simplicidad en comparación a otros protocolos como podrían ser OSPF, IS-IS o BGP. RIP se trata de un protocolo abierto a diferencia de otros protocolos de routing como por ejemplo IGRP y EIGRP propietarios de Cisco Systems o VNN propietario de Lucent Technologies.

RIP está basado en el algoritmo de Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada router atravesado para llegar a su destino es un salto.

RIP, al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos tales como por ejemplo ancho de banda o congestión del enlace.

5.2.3. RIPv1

Protocolo simple que funciona bien en una red pequeña que no vaya a crecer mucho.

Envía actualizaciones cada 30 segundos que contienen la tabla de routing completa.

Las siguientes características son de RIPv1 y de cualquier protocolo de vector distancia:

- Cuenta al infinito: Al crearse un bucle RIP permite que el datagrama siga vagando hasta que llegue al infinito (en este caso infinito=16 saltos).
- Horizonte Dividido: El proceso de routing no anunciará rutas por el mismo interfaz que por el que las ha recibido.
- Horizonte Dividido con Inversa Envenenada: El proceso de routing no anunciará rutas por el mismo interfaz que por el que las ha recibido, pero en el caso de que la red en cuestión haya caído sí se anunciará por el interfaz pero con un coste inaccesible (en RIPv1 será 16).
- Holddown: Después de ver que una ruta es inaccesible se marca como tal y se espera tres actualizaciones antes de borrarla de la tabla de routing.
- Actualizaciones por disparo (Triggered Updates): Tan pronto como se detecta que una red no es accesible se lanza una actualización en la cual se indica que la red es inaccesible.
- Balanceo de Carga: Si es posible enrutar la información por varios caminos con el mismo coste se balanceará el tráfico siguiendo la técnica de round-robin.

El problema de RIP se encuentra en los tiempos de convergencia, que son muy elevados para redes grandes, aunque RIP nunca se penso para redes grandes, sino todo lo contrario.

En Junio de 1988, C. Hedrick publicó el RFC 1058 correspondiente a RIP versión 1, y lo encabezó de la siguiente manera:

“This RFC describes an existing protocol for exchanging routing information among gateways and other hosts. It is intended to be used as a basis for developing gateway software for use in the Internet community. Distribution of this memo is unlimited.”

El protocolo RIPv1, al igual que sus antecesores propietarios es un protocolo de routing que fue diseñado para funcionar como protocolo vector distancia. RIPv1 fue diseñado para funcionar en redes pequeñas de pasarela interior. RIPv1 está basado según el autor del RFC en la versión 4.3 de la distribución de UNIX de Berkeley.

En cuanto al protocolo tenemos que tener en cuenta las tres limitaciones que C. Hedrick describe en la página 3 del RFC 1058:

- El protocolo no permite más de quince saltos, es decir, los dos routers más alejados de la red no pueden distar más de 15 saltos, si esto ocurriera no sería posible utilizar RIP en esta red.
- Problema del “conteo a infinito”. Este problema puede surgir en situaciones atípicas en las cuales se puedan producir bucles, ya que estos bucles pueden producir retardos e incluso congestión en redes en las cuales el ancho de banda sea limitado. El autor del RFC 1058 también comenta que en la realidad esto sólo puede ser un problema en redes lentas, pero el problema existe.
- El protocolo utiliza métricas fijas para comparar rutas alternativas, lo cual implica que este protocolo no es adecuado para escoger rutas que dependan de parámetros a tiempo real como por ejemplo retardos o carga del enlace.

Además de los problemas que cita el autor del protocolo tenemos que tener en cuenta que el protocolo RIPv1 es un protocolo classful⁶, con lo que existe el problema de la discontinuidad de redes. El problema de la discontinuidad de redes se produce en el momento que tenemos una red dividida en varias subredes y no pueden ser sumariadas en una misma ruta, ya que físicamente cada una de las subredes está ubicada en un lugar que depende de un interfaz distinto una subred de la otra. Pero claro, en la época en la que se escribió este RFC, que era en 1988 estos problemas no estaban contemplados y con el tiempo se detectó este problema, esta es una de las razones de la existencia de RIPv2. convergencia, que son muy elevados para redes

grandes, aunque RIP nunca se penso para redes grandes, sino todo lo contrario.

5.2.4. Tabla de routing de RIP

Si continuamos la lectura detallada del RFC1058, podemos ver que el autor nos dice que la base de datos de routing de cada uno de los hosts de la red que están utilizando el protocolo de routing RIP tiene los siguientes campos:

- Dirección de destino.
- Siguiente salto.
- Interfaz de salida del router.
- Métrica.
- Temporizador.

Para obtener esta tabla, el protocolo de routing RIP utiliza el siguiente procedimiento para mantener actualizada la tabla de routing de cada uno de los nodos o routers de la red:

1. Mantener una tabla con una entrada por cada posible destino en la red. La entrada debe contener la distancia D al destino, y el siguiente salto S del router a esa red. Conceptualmente también debería de existir una entrada para el router mismo con métrica 0, pero esta entrada no existirá.
2. Periódicamente se enviará una actualización de la tabla a cada uno de los vecinos del router mediante la dirección de broadcast. Esta actualización contendrá toda la tabla de routing.
3. Cuando llegue una actualización desde un vecino S , se añadirá el coste asociado a la red de S , y el resultado será la distancia D' . Se comparará la distancia D' y si es menor que el valor actual de D a esa red entonces se sustituirá D por D' .

El protocolo de routing RIP como ya hemos dicho mantiene una tabla de routing, como cualquier protocolo de routing, seguidamente pasamos a comentar cada uno de los campos de la tabla.

5.2.4.1. Dirección de destino

La dirección de destino en la tabla de routing de RIP será la red de destino, es decir, la red final a la que deseamos acceder, esta red en la versión 1 del protocolo RIP tendrá que ser obligatoriamente clasfull, es decir tendrá que tener en cuenta la clase, es decir, no se permite el subneting en RIP versión 1, por ejemplo si la red de destino es la 192.168.4.0, sabemos que al ser RIP classful la red de destino tiene 256 direcciones, de las cuales 254 son útiles, una vez descontada la dirección de red y la dirección de broadcast, ya que la red 192.168.4.0 es de clase C, es decir que los 24 primeros bits de la dirección IP identifican la red y los 8 últimos identifican los hosts de dentro de la red.

5.2.4.2. Siguiente salto

El siguiente salto lo definimos como el siguiente router por el que nuestro paquete va a pasar para llegar a su destino, este siguiente salto será necesariamente un router vecino del router origen.

5.2.4.3. Interfaz de salida del router

Entendemos por interfaz de salida del router al interfaz al cual está conectado su siguiente salto.

5.2.4.4. Métrica

La métrica utilizada por RIP como ya hemos comentado consiste en el conteo de saltos, como métrica se considera cada salto como una única unidad, independientemente de otros factores como tipo de interfaz o congestión de la línea. La métrica total consiste en el

total de saltos desde el router origen hasta el router destino, con la limitación que 16 saltos se considera destino inaccesible, esto limita el tamaño máximo de la red.

5.2.4.5. Temporizador

El temporizador nos indica el tiempo transcurrido desde que se ha recibido la última actualización de esa ruta. RIP utiliza dos tiempos importantes, el tiempo de actualización que se establece en 30 segundos, el tiempo de desactivación que se establece en 180 segundos y el tiempo de borrado se establece en 300 segundos.

El tiempo de actualización se considera al tiempo máximo a transcurrir entre el envío de los mensajes de actualización de los vecinos.

El tiempo de desactivación se considera al tiempo máximo que puede esperar un router sin recibir actualizaciones de vecino, una vez pasado este tiempo, el vecino que no ha enviado la actualización se considera que ha caído y con lo cual el router no está activo en la red, se establece la métrica a valor 16, es decir destino inalcanzable.

El tiempo de borrado implica que una vez transcurrido ese tiempo todas las rutas de ese router supuestamente caído son eliminadas de la tabla de routing.

5.2.5. RIPv2

Diez años después de que se publicara la versión 1 de RIP se publicó la versión 2, por G.Malkin de la compañía Bay Networks en Noviembre de 1998 en el RFC 2453.

RIPv2 establece una serie de mejoras muy importantes con su antecesor que son las siguientes:

- Autenticación para la transmisión de información de RIP entre vecinos.

- Utilización de mascarar de red, con lo que ya es posible utilizar VLSM.
- Utilización de máscaras de red en la elección del siguiente salto, lo cual nos puede permitir la utilización de arquitecturas de red discontinuas.
- Envío de actualizaciones de tablas de RIP mediante la dirección de multicast 224.0.0.9.
- Inclusión de RIPv2 en los bloques de información de gestión (MIB).

Por supuesto además de estas mejoras RIPv2 nos permite la redistribución de rutas externas aprendidas por otros protocolos de routing.

Pero RIPv2 aunque haya tenido una serie de mejoras muy importantes desde la versión 1 del protocolo sigue teniendo una serie de carencias muy importantes como:

- Limitación en el tamaño máximo de la red. Con RIPv2 sigue existiendo la limitación de 15 saltos como tamaño máximo de la red, lo cual implica que no nos permite la utilización de RIPv2 en redes de un tamaño más grande.
- Conteo a infinito, RIPv2 sigue sin solucionar el problema del conteo hasta el infinito si se forman bucles, aunque existen técnicas externas al protocolo como pueden ser la inversa envenenada y el horizonte dividido, técnicas brevemente descritas por William Stallings en su libro “Comunicaciones y Redes de Computadoras”, las cuales consisten básicamente en no anunciar una ruta por el interfaz por el que se ha recibido en algún momento.
- Métricas estáticas que pueden ser cambiadas por el administrador de la red, pero que no nos dan ninguna información del estado de la red.

- RIPv2 sólo permite al igual que su antecesor una ruta por cada destino, lo cual implica la imposibilidad de realizar balanceos de carga por ejemplo, lo que redundaba en una pobre y poco óptima utilización de los enlaces.
- RIPv2 es un protocolo que al igual que su antecesor genera muchísimo tráfico al enviar toda la tabla de routing en cada actualización, con la carga de tráfico que ello conlleva.

5.3. IGRP

Interior Gateway Routing Protocol es un protocolo propietario de Cisco Systems creado a mediados de los 80s.

Supera las limitaciones de RIPv1, incluyendo:

- Actualizaciones incrementales.
- Métrica más eficiente y compleja.
- No tiene limitación del diámetro de la red de 16 saltos.

5.3.1. Características de IGRP

Actualizaciones Periódicas: Cada 90 segundos por defecto, RIPv1 era cada 30. La actualización es un sumario de las rutas, sólo se intercambia con los routers vecinos.

Actualizaciones por Broadcast: Las actualizaciones se envían por broadcast. Protocolos posteriores como RIPv2 ya utilizaban multicast.

Actualizaciones completas de routing: Además de las actualizaciones por disparo IGRP cada 90 segundos realiza una sincronización con los vecinos de toda la tabla de routing enviando las cabeceras.

Conteo al Infinito: Como los demás protocolos de routing de vector distancia IGRP utiliza un conteo al infinito para evitar bucles.

Horizonte Dividido: IGRP utiliza Horizonte Dividido como ayuda para prevenir los bucles de la red.

Actualizaciones de Disparo con Ruta Envenenada: IGRP envía las actualizaciones tan rápido como puede para minimizar el tiempo de convergencia, si una ruta no es valida entonces envía su actualización.

Balanceo de Carga en Caminos Iguales: Hasta 4 por defecto. Lo utiliza para mejorar la carga de los enlaces.

Rutas por Defecto: Acepta como candidato al router del borde de la red.

Algoritmo de Routing Bellman Ford: Utiliza una métrica compuesta y la varianza para modificar los parámetros del balanceo de carga.

5.3.2. Diferencias de IGRP con RIPv1

IGRP tiene una métrica compuesta por ancho de banda, retardo, carga, fiabilidad y MTU, aunque en la configuración por defecto sólo utilice ancho de banda y retardo.

IGRP tiene un máximo de saltos de 100 configurable hasta 255. Esto vale sólo para el conteo al infinito, no para la métrica.

Las actualizaciones en IGRP son cada 90 segundos en vez de cada 30 en RIPv1.

Permite el balanceo de carga entre enlaces con coste no igual.

IGRP utiliza una estructura del paquete más eficiente.

Los Sistemas Autónomos se utilizan para poder ejecutar varios procesos de IGRP, esto permite escalar la red.

5.4. EIGRP

Enhanced Interior Gateway Routing Protocol. Protocolo propietario de Cisco Systems. Muchas veces referido como Protocolo de Vector Distancia Avanzado o Protocolo Híbrido Equilibrado.

Las características de EIGRP son:

- En una red estable EIGRP utiliza muy pocos recursos.
- Los cambios en la topología son enviados cada 30 segundos.
- La actualización inicial de EIGRP es la tabla completa, a partir de ahí sólo se envían las modificaciones.
- Utiliza el algoritmo DUAL (Diffused Update Algorithm).
- En vez de tener que esperar actualizaciones, tan pronto como una ruta se viene abajo, EIGRP examina la tabla topológica para buscar una ruta alternativa, si se encuentra se sustituye inmediatamente.
- EIGRP utiliza sólo paquetes hello para mantener las bases de datos de routing.
- La tabla de vecinos se construye con paquetes hello, si uno de los vecinos no responde con su ACK correspondiente entonces se anuncia a los vecinos que el router vecino está abajo. Que el routing es fiable significa que no se tiene que reenviar actualizaciones cada 30 segundos.
- Si una ruta se cae EIGRP intentará buscar rutas alternativas en la tabla de topología, si no encuentra entrada alternativa, entonces preguntará a los demás routers.

5.5. Seleccionar protocolos de routing

Existen muchos protocolos de routing para escoger, pero escoger un único protocolo es toda la red es mejor porque permite una consistencia en la red.

Si existe más de un protocolo de routing en la red las decisiones se realizarán basándose en la distancia administrativa.

Para solventar este problema utilizaremos la redistribución de rutas.

La distancia administrativa selecciona uno o más caminos para elegir la ruta basándose en el protocolo.

5.5.1. La distancia administrativa

La Distancia Administrativa es un conjunto de valores arbitrarios elegidos para las diferentes fuentes de información. Es posible cambiar estos valores, pero con cuidado.

La distancia administrativa menor es preferida sin contar con la métrica.

En la siguiente tabla se pueden observar las distintas distancias administrativas por origen del routing.

| Fuente del routing | Distancia Administrativa |
|--|--------------------------|
| Interfaz conectado directamente o ruta estática que identifica el interfaz de salida en vez del siguiente salto. | 0 |
| Ruta estática. Contamos el siguiente salto | 1 |
| Ruta EIGRP sumarizada | 5 |
| BGP Externo | 20 |
| EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| RIP | 120 |
| ODR | 160 |
| EIGRP Externo | 170 |
| BGP Interno | 200 |
| Red desconocida | 255 o infinito |

La distancia administrativa es fija e independiente de la métrica, lo cual redundante en una pobre elección de la ruta.

En el caso que tengamos una ruta principal por un E3 utilizando OSPF, esta tendrá una distancia administrativa de 110, si embarlo

la ruta estática por RDSI tendrá una distancia administrativa de 1, así que el router elegirá siempre la ruta estática por RDSI, para evitar este tipo de cosas utilizaremos las rutas estáticas flotantes.

5.5.2. Convergencia

La convergencia ocurre cuando todos los routers del dominio están de acuerdo en las rutas que se encuentran disponibles.

El tiempo de convergencia es el tiempo que necesita cada router para sincronizar su tabla de routing después de que se haya producido un cambio en la topología de la red.

El tiempo de convergencia tiene que ser el más corto posible, ya que mientras tanto los router no están de acuerdo en las redes disponibles y no pueden enrutar de forma correcta y eficiente.

Cada protocolo de routing tiene un método diferente de actualizar su tabla de routing, esto afecta al tiempo de convergencia.

5.5.3. Convergencia en RIPv1 y RIPv2

Los pasos son los siguientes:

1. Cuando un router ve que ha desaparecido una ruta directamente conectada, envía una actualización (flash update) y borra esa entrada de su tabla de routing. Esto se llama inversa envenenada con actualización de disparo.
2. El router receptor envía la actualización y deja la ruta en holddown.
3. El router inicial solicita a sus vecinos una ruta alternativa, si el vecino la tiene se la envía, si no envía una inversa envenenada.
4. El router original instala la nueva ruta y borra la anterior.
5. Los routers en holddown ignoran la ruta alternativa, la aceptarán cuando salgan del holddown.

6. Se obtiene la convergencia.

5.5.4. Convergencia en IGRP

Los pasos son los siguientes:

1. Cuando un router ve que ha desaparecido una ruta directamente conectada, envía una actualización (flash update) y borra esa entrada de su tabla de routing. Esto se llama inversa envenenada con actualización de disparo.
2. El router receptor envía la actualización y deja la ruta en holddown.
3. El router inicial solicita a sus vecinos una ruta alternativa, si el vecino la tiene se la envía, si no envía una inversa envenenada.
4. El router original instala la mejor ruta alternativa y borra la anterior. Envía una actualización (flash update).
5. Los routers que están en holddown ignoran la nueva actualización.
6. Cuando los routers salen de holddown aceptan la nueva ruta.
7. El router original pregunta a sus vecinos por rutas alternativas, y recibe los acknowledges de los routers.

Como se puede observar los tres primeros pasos son exactamente iguales a los de RIP.

El tiempo de convergencia consta de detección, holddown más el número de actualizaciones (igual al diámetro en saltos de la red) de 90 segundos. El tiempo de actualización es muy elevado.

5.5.5. Convergencia en EIGRP

Los pasos son los siguientes:

1. Cuando el router local ve que una ruta conectada desaparece, comprueba la tabla topológica buscando un feasible successor, si no lo encuentra, pasa a estado activo.
2. El router original pregunta a sus vecinos por rutas alternativas, y recibe los acknowledges de los routers.
3. Si existe una ruta alternativa, la información se envía al querying router.
4. Si existe un successor aceptable, lo añade a su tabla de routing.
5. El router envía una flash update del camino con la métrica mayor.
6. El router receptor envía el ACK de la actualización.

La convergencia es muy rápida porque es el tiempo de detección + el tiempo de consulta (query) + tiempo de respuesta + tiempo de actualización.

Si existe un feasible successor, la convergencia es casi instantánea.

5.5.6. Protocolos IGP y EGP

Los protocolos que operan dentro de la organización son conocidos como IGP (Interior Gateway routing Protocols).

- RIPv1.
- RIPv2.
- IGRP.
- EIGRP.

- OSPF.
- IS-IS.

Los límites de la organización delimitan el AS (Autonomous System). Los protocolos que intercambian información de routing entre las organizaciones son llamados EGP (Exterior Gateway routing Protocols). Este tipo de protocolos necesitan determinar políticas de routing entre organizaciones debido a su complejidad:

- BGP-4

Los sistemas autónomos disponen de un identificador único asignado.

- AS públicos: 1 – 64511
- AS privados: 64512 - 65535

Tenemos que tener en cuenta que a partir del 1 de Enero de 2009 los ASs son de 32 bits como primera opción utilizando la notación asplain definida en la RFC 5396.

Capítulo 6

Protocolos estado del enlace

Los protocolos de routing de estado del enlace están pensados para mantener las tablas de routing libres de bucles y precisas.

Este tipo de protocolos envían sus actualizaciones de forma incremental y mediante multicast.

Muchos protocolos además de enviar las tablas de forma incremental envían la tabla completa, pero cada 30 minutos y mediante multicast.

El Significado de Estado del Enlace:

- Enlace se refiere a la conexión entre los routers (conexión física).
- Un protocolo de estado del enlace es un protocolo que envía información sobre los enlaces entre los routers.
- La información enviada sólo es de los enlaces conectados localmente.
- Sin embargo este tipo de protocolos mantienen una imagen de la red completa, creada a partir de las actualizaciones.

- Enviar información sobre los enlaces es más eficiente que sobre las rutas, ya que los enlaces afectan a las rutas.
- Los recursos utilizados son de CPU, aunque se gastan menos recursos de ancho de banda que en los de vector distancia.

Aprendizaje de la Red:

- El protocolo de routing desarrolla y mantiene la relación entre vecinos enviando mensajes hello por el medio.
- Después de sincronizar sus tablas de routing intercambiando actualizaciones se dice que los routers son adyacentes.
- Como la relación de adyacencia se mantiene con paquetes Hello, la actualización de routing es muy rápida y eficiente.
- Un router sabe que su vecino se ha caído cuando deja de recibir paquetes Hello.
- Una vez que el router identifica el problema envía una actualización por disparo (triggered update), y lo hace de forma incremental y por multicast, reduciendo el tráfico de routing y permitiendo más ancho de banda para la información.

Reducción del ancho de banda de información de routing por los protocolos de estado del enlace:

- Los protocolos de estado del enlace son adecuados para ser utilizados en redes grandes, ya que minimizan la utilización del ancho de banda para actualizaciones de routing de la siguiente manera.
 - Utilizando direccionamiento de multicast
 - Enviando actualizaciones por disparo
 - Enviando resumen de la tabla de routing de forma esporádica, si es que es necesario.

- Utilizando paquetes pequeños desde los que cada router describe su conectividad local, en vez de enviar la tabla de routing completa.

Actualización de las Tablas de Routing Locales:

- Los protocolos de estado del enlace utilizan tablas topológicas en las cuales incorporan todos los cambios que se van produciendo en la red. Esto lo hacen con las actualizaciones incrementales que van recibiendo.
- Una vez que se tiene completa la tabla topológica se procede a ejecutar el algoritmo de Dijkstra para obtener la tabla de routing.
- Una vez realizados estos pasos la tabla de routing quedará actualizada.

Selección del Camino:

- El protocolo de routing selecciona el mejor camino utilizando la métrica para ello.
- La métrica en algunos protocolos de routing de este estilo, como por ejemplo OSPF no viene especificada en el estándar y es el fabricante el que establece la métrica. En el caso de OSPF Cisco utiliza como métrica $\frac{10^8}{\text{ancho de banda}}$.

Ejemplos de protocolos de estado del enlace para IP son:

- OSPF.
- IS-IS.

6.1. OSPF

6.1.1. Introducción

Open Shortest Path First (OSPF), es un protocolo de routing de estado del enlace basado en un estándar abierto. OSPF ha sido descrito en varios RFCs, pero el estándar de OSPF v.2 está descrito por John J. Moy en el RFC2328 y en el libro “OSPF Anatomy of an Internet Routing Protocol”, escrito por el mismo autor, y publicado por la editorial Addison-Wesley.

El término Open en el nombre del protocolo hace referencia a que es un protocolo abierto al público y no propietario de ninguna compañía. De entre los protocolos abiertos existen varios como RIPv1, RIPv2 u OSPF entre otros, pero entre RIP y OSPF para redes de tamaño medio-grande es preferible, ya que OSPF permite una escalabilidad muy remarcable, entre otras características podemos decir que OSPF no tiene el problema de la limitación de los 15 saltos de RIP, además los tiempos de convergencia de OSPF son muchísimo mejores en todos los casos y además OSPF para el calculo de costes y rutas óptimas tiene en cuenta factores tales como el ancho de banda, lo cual permite elegir un camino supuestamente más lento si el camino que supuestamente es más rápido tiene menor ancho de banda, lo cual provocaría más lentitud de la transmisión.

OSPF es uno de los protocolos que sin duda están preparados para las redes actuales. OSPF también considera la capacidad de escalabilidad de la red a través de la escalabilidad que permite un modelo jerárquico que es posible conseguir mediante la utilización de distintas áreas.

OSPF utiliza la tecnología de estado del enlace, de forma opuesta a RIP que utiliza tecnología de vector distancia. Los router de estado del enlace mantienen una imagen común de la red e intercambian su información de enlaces desde un descubrimiento inicial hasta los cambios de la red. Los routers de estado del enlace no realizan broadcast de sus rutas periódicamente como los routers que utilizan vector distancia. OSPF tiene las siguientes características.

- **Velocidad de convergencia:** En redes grandes, la convergencia utilizando RIP puede alargarse varios minutos, hasta que la tabla completa de routing de los routers de la red se completa y se estabiliza. En OSPF el tiempo de convergencia es muchísimo menor ya que sólo se actualizan las rutas que han sido modificadas y éstas son distribuidas por la red de forma rápida.
- **Soporte de VLSM:** RIPv1 es un protocolo de los denominados clasful, y como tal no soporta VLSM, sin embargo tenemos que recordad que RIPv2 sí soporta VLSM.
- **Tamaño de la red:** En un entorno RIP una red con más de 15 saltos no es viable, ya que más de 15 saltos se considera inalcanzable. Sin embargo en un entorno de routing basado en OSPF no tenemos este tipo de limitación, ya que teóricamente no tenemos esta limitación de tamaño, aunque si seguimos las especificaciones de los fabricantes de routers Cisco o Lucent Technologies nos recomiendan redes en las cuales no haya más de 400 routers por área, obviamente pueden existir más áreas, pero la única limitación física, que no de protocolo sería la de los 400 routers por área. Esta característica hace de OSPF ideal para redes medianas y grandes.
- **Utilización de ancho de banda:** Si utilizamos RIP estamos realizando broadcast a la red de la tabla de routing completa cada 30 segundos. Esta característica puede ser especialmente problemática sobre lentos enlaces WAN. Sin embargo OSPF utiliza multicast y sólo envía actualizaciones cuando se produce un cambio en la red.
- **Selección de camino:** RIP selecciona el camino óptimo contando saltos, o distancia a otros routers. Dentro de la elección de ruta óptima no entran en consideración factores como el ancho de banda restante o los retardos en la red. Sin embargo OSPF utiliza una métrica basada en ancho de banda y retardos.

- **Agrupación de miembros:** RIP utiliza una topología plana en la cual todos los routers forman parte de la misma red. Esta característica provoca que la comunicación entre routers tenga que navegar por la totalidad de la red, de esta forma cada cambio en un router individual afectaría al resto de los equipos de la red. Sin embargo con OSPF se introduce el concepto de “áreas”, lo que permite la segmentación de la red en segmentos más pequeños. Al dividir la red en áreas se tiene que introducir el concepto de comunicación entre áreas, pero gracias a la división de la red los cambios producidos en un router de un área no afectan a la totalidad de la red, sino que sólo afecta a los routers de un área.

Ya que OSPF fue pensado y descrito para redes de un tamaño considerable al crear una red con más de 50 routers hay que tener un cuidado especial con el diseño y la planificación de la red con tal de minimizar tráfico y el montante de intercambio de información de routing.

Como protocolo de estado del enlace, OSPF opera de forma distinta a los protocolos de vector distancia como podrían ser RIP.

La información proporcionada por OSPF a los vecinos no es la tabla de routing completa. Sin embargo, los routers que utilizan OSPF le informan a sus vecinos sobre el estado de sus conexiones o enlaces. En otras palabras los routers OSPF anuncian el estado de sus enlaces. Los routers procesan esta información y generan la base de datos de estado del enlace, la cual es esencial para poder dibujar un esquema de quien está conectado con quien. Todos los routers en un mismo área tienen que tener una base de datos del enlace idéntica. Cada router ejecuta independientemente el algoritmo SPF, también conocido como algoritmo de Dijkstra, en la base de datos del enlace con tal de determinar las mejores rutas a los destinos. El algoritmo SPF añade el coste (el cual está normalmente basado en el ancho de banda) a cada uno de los enlaces entre el router origen y el destino. Entonces el router escoge el camino con coste más bajo y añade el camino a su tabla de routing también conocida como base de datos

de forwarding.

Los routers que utilizan OSPF mantienen información de sus vecinos y de sus bases de datos de adyacencia. Para simplificar el intercambio de información de routing sobre varios vecinos en la misma red, los routers que ejecutan OSPF tienen que escoger el Router Designado (DR) y el Router Designado de Backup (BDR) para servir de punto central para la actualización de rutas.

Los routers que ejecutan OSPF establecen relaciones, o estados, con sus vecinos para un intercambio de información de estado más eficiente. En contraste con los protocolos de vector distancia, como RIP, los cuales realizan broadcast o multicast de su tabla de routing completa por cada interfaz, esperando que los demás routers la reciban. RIP por defecto envía cada 30 segundos sólo un único tipo de mensaje, su tabla completa de routing. Sin embargo, los routers que ejecutan OSPF disponen de cinco tipos de paquetes distintos a enviar a sus vecinos para actualizar la información de estado del enlace.

Estos cinco tipos de mensajes hacen de OSPF un protocolo adecuado para comunicaciones sofisticadas y complejas.

OSPF se relaciona con sus vecinos mediante siete estados distintos.

6.1.2. Topologías de OSPF

En OSPF podemos encontrar distintos tipos de topologías según el RFC2328, pero sin embargo ya se ha empezado a desarrollar soporte para otro tipo de topologías de forma propietaria.

6.1.2.1. Topología de broadcast

Este tipo de topología se puede utilizar en entornos donde es posible que los routers tengan en común una red de broadcast, como podría ser una red Ethernet, Token Ring o FDDI. En este tipo de topologías los routers tienen en común una red que permite tráfico de multicast del DR con el resto de los routers.



6.1.2.2. Topología punto a punto

Este tipo de topologías son las más simples, ya que en ella sólo entran dos routers conectados de forma directa formando un único enlace.

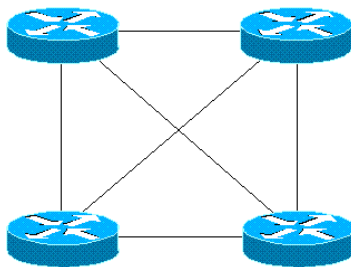


En este tipo de topologías no es necesario la elección de DB y BDR ya que sólo hay dos routers.

6.1.2.3. Topología NBMA

En este tipo de topologías que no son de Broadcast, recordemos que NBMA son las siglas de “NonBroadcast MultiAccess networks”. En este tipo de topologías nos encontramos con un problema adicional, ¿Cómo enviamos mensajes de multicast en este tipo de redes?, pues bien, esta pregunta sólo tiene una contestación posible, es decir, la contestación consiste en realizar una emulación de una red de broadcast.

La emulación de una red de broadcast en una red que no lo es sólo se puede hacer mediante la replicación de mensajes. Una red NBMA totalmente mallada, en la cual todos los routers están conectados con todos los routers tenemos que replicar un mensaje de multicast en muchos mensajes de unicast, es decir, en vez de enviar un único mensaje a la red a la dirección de multicast 224.0.0.5 tenemos que enviar el mismo mensaje por cada uno de los enlaces que tiene el router con los demás routers de la red, es decir, estamos realizando una topología que emula a una red de broadcast mediante un conjunto de redes punto a punto.



6.1.3. Estados de OSPF

Para una comprensión más profunda de OSPF es necesario comprender las relaciones o estados que tienen entre si los routers que utilizan OSPF.

1. **Estado Down:** En el estado Down, el proceso OSPF no ha empezado a intercambiar información con ningún vecino. OSPF está esperando a entrar en el siguiente estado.
2. **Estado Init:** Los routers que utilizan OSPF envían paquetes de tipo 1 (Hello) en intervalos regulares (por defecto 10 segundos en Quagga y en Cisco) para establecer relación con sus routers vecinos, cuando un interfaz recibe su primer paquete Hello entonces decimos que el router ha entrado en estado Init y está preparado para entrar en el siguiente estado.
3. **Estado Two-Way:** Utilizando paquetes Hello, cada router OSPF intenta establecer una comunicación bidireccional con cada router vecino que está ubicado en la misma red IP. Un router entra en estado two-way en el momento que se ve en una de las actualizaciones de uno de sus vecinos. El estado two-way es la relación más básica que pueden tener los routers OSPF, pero la información de routing no se intercambia en este estado. Para aprender sobre enlaces de otros routers el router tiene que tener al menos una adyacencia completa.

4. **Estado ExStart:** Técnicamente, cuando un router y su vecino entran en estado ExStart, su conversación se caracteriza por una adyacencia, pero los routers todavía no tienen una adyacencia completa. El estado ExStart se establece utilizando paquetes de tipo 2. Entre los dos routers se utilizan paquetes hello para determinar cual de los dos es el maestro y cual es el esclavo en su relación y se intercambian paquetes de tipo 2.
5. **Estado Exchange:** En el estado exchange se utilizan paquetes de tipo 2 para enviar al otro router su información de estado del enlace. En otras palabras, los routers describen sus bases de datos de estado del enlace al otro router. Si alguna de las rutas no está en la base de datos del enlace del router receptor de la información, este solicita una actualización completa, la cual se realiza en el estado Loading.
6. **Estado Loading:** Después de que todas las bases de datos han sido descritas a cada router, se tiene que solicitar una información que es más completa utilizando paquetes de tipo 3. Cuando un router recibe un paquete de tipo 3, este responde con una actualización mediante un paquete de tipo 4. Los paquetes de tipo 4 describen la información de estado del enlace que es el corazón de los protocolos de routing de estado del enlace. Los paquetes de tipo 4 con respondidos con paquetes de tipo 5.
7. **Adyacencia Completa:** Cuando termina el estado Loading, los routers están en una adyacencia completa. Cada router mantiene una lista de sus vecinos adyacentes, llamada base de datos de adyacencia. Es preciso no confundir la base de datos de adyacencia con la base de datos de estado del enlace o con la base de datos de forwarding.

Ya que la adyacencia es necesaria para que los routers que utilizan OSPF puedan compartir su información de routing, un router tiene que estar adyacente con al menos otro router en la red IP a la que esté conectado. Si hay o no adyacencia depende del tipo de red que

se esté utilizando, es decir, de qué tipo de red esté conectado los routers.

Los interfaces de un router que estén ejecutando OSPF tiene que reconocer tres tipos de redes: redes de broadcast (p.e. ethernet), NBMA (p.e. frame relay totalmente mallada) y redes punto a punto (sólo dos routers). Un administrador de red podría configurar un cuarto tipo de red:

- red punto a multipunto.

El tipo de red en la que esté trabajando OSPF dictará el funcionamiento del protocolo, y este a su vez puede ser optimizado por el administrador de la red.

Muchas redes se definen como redes de multiacceso porque no es posible predecir cuantos routers van a haber conectados.

6.1.4. Routers OSPF

Debido a que en redes de multiacceso pueden existir un número significativo de routers, OSPF utiliza un método para evitar la sobrecarga de información de routing en la red, de este modo la información se centraliza en dos routers:

- **Router Designado (DR – Designated Router):** Para todas las redes de multiacceso IP se debe de elegir un DR. Este DR tiene dos funciones principales:
 - Mantener adyacencia con todos los demás routers de la red.
 - Actuar de portavoz de todos los demás routers de la red y anunciar los cambios a las otras redes, por supuesto es el encargado de mantener la información centralizada del estado de su red.
- **Router Designado de Backup (BDR – Backup Designated Router):** El DR puede representar un único punto de

fallo, así que se elige un BDR para proporcionar tolerancia a fallos, es decir una redundancia. Así pues el BDR también tiene que ser adyacente a todos los demás routers de la red y tiene que estar sincronizado con el DR para que en caso de caída del DR pueda este asumir la responsabilidad de la red:

- En redes punto a punto, en las cuales sólo existen dos nodos no tiene mucho sentido el que exista ni DR ni BDR, así que en este caso ambos routers funcionan peer-to-peer.
- **Routers Internos (IR):** Los routers internos tienen todos sus interfaces en una misma área. Todos los routers del mismo área tienen las mismas bases de datos de enlaces, es decir los routers internos del mismo área al ejecutar el algoritmo SPF utilizan los mismos routers como datos.
- **Backbone Routers (BR):** Los routers de backbone están situados en los límites del área de backbone y tienen al menos un interfaz conectado al área 0.
- **Area Border Routers (ABR):** Estos routers como indica su nombre son los routers que tienen enlaces a distintas áreas, estos routers mantienen bases de datos del enlace separadas por áreas, es decir, tienen una base de datos independiente por área y ejecutan un SPF independiente por área.
- **Autonomous System Boundary Routers (ASBR):** Estos routers en castellano serían denominados Routers Frontera del Sistema Autónomo, y tienen al menos un interfaz con un AS (Sistema Autónomo) distinto. El AS distinto no tiene porque utilizar OSPF. Los ASBR distribuyen información no OSPF a la red OSPF y viceversa cuando es necesario.

Por supuesto un routers puede ser de varios tipos a la vez.

6.1.5. Tipos de LSA (Link State Advertisement)

Los LSAs describen el estado de una red o de un router. Esta descripción cubre el estado de todos los interfaces de los routers y sus adyacencias.

En OSPF utilizamos 4 tipos de LSAs:

- **Tipo 1:** Son llamados router link, estos LSAs describen el estado y el coste de los enlaces entre routers de área. Estos LSAs sólo se propagan dentro de un mismo área, no en todo el Sistema Autónomo.
- **Tipo 2:** Son llamados network links, estos LSAs describen todos los routers que hay en una red en particular. Estos LSAs se propagan dentro del área que contiene la red.
- **Tipo 3 / 4:** Esos son los summary links. Estos LSAs se generan por los ABRs, y describen los enlaces entre los ABRs y los Irs del área local. Los summary links se propagan a través del área 0 o backbone a otras áreas a través de los ABRs del AS. Los LSAs de tipo 3 y de tipo 4 tienen diferencias. Los LSAs de tipo 3 describen las rutas a las redes a través del AS y se envían por el área 0. Sin embargo los LSAs de tipo 4 describen la localización de los ASBR.
- **Tipo 5:** Son también conocidos como external links, los cuales se crean en los ASBRs. Estos LSAs describen las rutas a destinos fuera del AS. Estos LSAs van por las áreas estándar y por la backbone. Existen dos tipos de external links:
 - External link type 1: Este se calcula añadiendo al coste externo el coste interno para alcanzar el destino.
 - External link type 2: Es el coste externo sin tener en cuenta el coste interno.

Tal y como se puede observar en la descripción de los tipos de área, ningún tipo de LSA atraviesa las áreas totally stubby.

6.1.6. Funcionamiento de OSPF en un único Área

Cuando un router arranca el proceso de routing OSPF en uno de sus interfaces, éste envía un paquete hello y continua enviando paquetes hello en intervalos regulares.

En el nivel 3 del modelo de referencia OSI, los paquetes hello son enviados a la dirección de multicast 224.0.0.5. Esta dirección tiene el significado de “todos los routers”. Los routers que están ejecutando OSPF envían periódicamente paquetes hello para iniciar y mantener su adyacencia y para asegurarse que las adyacencias con sus vecinos no desaparecen. Los tiempos de actualización para el envío de paquetes hello son configurables, y por ejemplo fabricantes como Cisco envían por defecto paquetes hello en redes de broadcast cada 10 segundos, sin embargo en redes NBMA envían los paquetes cada 30 segundos, este sería el caso de redes Frame-Relay que utilizan OSPF como protocolo de encaminamiento.

6.2. IS-IS

IS-IS es un protocolo de routing que utiliza el algoritmo SPF.

Ofrece convergencia rápida, flexibilidad, evita bucles y soporta redes muy grandes.

IS-IS es un protocolo integrado. Diseñado por Digital Equipment Corp. para DECnet fase V y ratificado como estándar por la ISO.

El espacio para direccionamiento es muy grande permitiendo ser utilizado por redes muy grandes.

El protocolo tiene un diseño jerárquico.

La estructura del paquete le permite incorporar mejoras, haciéndolo muy flexible.

IS-IS es el protocolo utilizado por el Gobierno de los EEUU, incluyendo las fuerzas armadas de ese País.

6.2.1. Características de IS-IS

Enruta tráfico CLNP¹, definido en el estándar ISO 10589.

Enruta tráfico IP, definido en el estándar RFC 1195.

Protocolo de Routing Classless.

Utiliza VLSM y summarización manual y automática a IANA en los límites de la red.

Utiliza el diseño en áreas para limitar la utilización intensiva de CPU.

El coste definido por Cisco es 10 para cualquier medio.

Asigna funcionalidad a los routers. Los routers Level 1 operan dentro del área, mientras que los routers de Level 2² operan entre áreas.

Envían actualizaciones incrementales, a través de los medios de broadcast, sincronizan las rutas completas cada 10 minutos.

Mantienen la relación entre vecinos mediante paquetes Hello cada 10 segundos.

Considera que el vecino ha muerto tras 30 segundos de silencio.

Opera como protocolo IGP dentro del AS.

6.3. BGP-4

BGP-4 estrictamente hablando no es un protocolo de estado del enlace, sino un protocolo de path vector, aunque mantiene muchas características comunes con los de vector distancia.

Es un protocolo EGP, con lo que es un protocolo totalmente diferente a los vistos hasta ahora.

Path Vector hace referencia a la lista de números de AS que son enviados en las actualizaciones de BGP-4. El vector indica la dirección de la red remota.

¹CLNP: ConnectionLess Network Protocol. El nivel 3 de OSI no requiere que se establezca un circuito antes de transmitir el datagrama.

²No hemos de confundir los routers de Layer 1 o de Layer 2 con los niveles de OSI, lo único que tienen en común es el nombre.

BGP-4 se utiliza principalmente en las conexiones en Internet y entre los ISPs.

6.3.1. Tipos de BGP

eBGP: BGP Externo (External Border Gateway Protocol). Básicamente BGP es un protocolo que interconecta AS y nos referiremos a el como eBGP.

iBGP: BGP Interno (Internal Border Gateway Protocol).

- También existe el iBGP que se utiliza para enviar la información dentro de un AS, utilizado como área de tránsito para otro AS.
- iBGP necesita que sus routers estén en una topología totalmente mallada, aunque no es necesario que estén directamente conectados.

BGP se define en la RFC1771.

BGP envía muy poca información en sus actualizaciones, y sólo cuando hay cambios en la red.

Uno de los mayores logros de BGP es que se permite determinar un camino diferente dependiendo de los tipos de tráfico.

Permite la interconexión de redes muy amplias.

6.3.2. Características de BGP-4

Protocolo de Routing Classless.

Utiliza VLSM y sumarización manual y automática a IANA en los límites de la red.

Envía las rutas completas al inicio de la sesión.

Después del inicio sólo envía actualizaciones por disparo.

La relación entre routers BGP se mantiene con paquetes Hello³ cada 60 segundos. Tras 180 segundos se considera que el vecino está caído.

Utiliza una estructura jerárquica de AS.

Tiene una métrica compleja basada en atributos, con los cuales se puede manipular los diferentes caminos (paths).

6.3.3. Convergencia OSPF

Los pasos para la convergencia de OSPF son:

1. Cuando el router detecta un fallo en un enlace, envía un LSA a los vecinos. Si el router está en un enlace de multiacceso envía la actualización al DR y al BDR.
2. La ruta se borra de la tabla de routing del router.
3. El receptor del LSA actualiza su tabla topológica e inunda los demás interfaces con el LSA.
4. Se ejecuta el SPF y se reconstruye la tabla de routing.

La convergencia en OSPF se produce después del tiempo de detección, la inundación de LSA y a esto le añadiremos 5 segundos antes de recomputar la tabla de routing.

6.3.4. Convergencia en IS-IS

Los pasos para la convergencia de IS-IS son:

1. Cuando el router detecta un fallo en un enlace, se envía un LSP a sus vecinos o en entornos multiacceso al DIS.
2. El camino borrado será eliminado de las tablas del sistema emisor.

³El protocolo Hello es orientado a la conexión y el paquete irá sobre el puerto 179/TCP.

3. El router receptor del LSP actualizará su table de topología e inundará el LSP por todos los interfaces excepto por el que lo recibió.
4. Se ejecutará el algoritmo de Dijkstra.

La convergencia en IS-IS se produce después del tiempo de detección y la inundación de LSP⁴.

6.3.5. Convergencia en BGP-4

La convergencia será distinta en eBGP que en iBGP.

Cuando un vecino no es accesible se intenta reconectar con el, si esto falla se borra la información con este vecino del router, entonces se envía una actualización a todos los demás vecinos.

En eBGP la fiabilidad es muy importante, sin embargo en iBGP es más importante el tiempo e convergencia, esto hace diferenciar la convergencia en estos dos protocolos.

6.3.6. Protocolos y tiempos de actualización

| Protocolo | Tiempo de actualización | Tecnología |
|-----------|---|------------------|
| RIPv1 | Cada 30 segundos la tabla de routing completa | Vector Distancia |
| RIPv2 | Cada 30 segundos la tabla de routing completa | Vector Distancia |

⁴LSP: Link State Packet. En entornos de multiacceso se enviará para avisar a los demás routers a los DIS (Designated Intermediate System), no a los vecinos. (DIS en IS-IS = DR en OSPF).

| Protocolo | Tiempo de actualización | Tecnología |
|-----------|---|--|
| OSPF | Incremental con sólo los cambios de la red. Sin embargo cada 30 minutos se propaga una versión comprimida de la tabla | Estado del Enlace |
| EIGRP | Incremental con sólo los cambios de la red | Vector Distancia Avanzado, también llamado Híbrido Equilibrado |
| IGRP | Actualizaciones cada 90 segundos con actualizaciones incrementales | Vector Distancia |
| BGP-4 | Incremental con sólo los cambios de la red | Path Vector, también llamado como un tipo de protocolo de vector distancia |

6.3.7. Vector distancia Vs. estado del enlace

| | |
|--|---|
| Utilizan métrica basada en cómo de distante está el destino (IGRP no lo hace así) | Utilizan métricas complejas |
| Vector Distancia | Estado del Enlace |
| Envía la tabla de routing completa en intervalos regulares. Envía actualizaciones por disparo para reflejar cambios en la red. | Envía actualizaciones incrementales cuando se produce un cambio. OSPF envía información sumariada cada 30 minutos, además de las actualizaciones incrementales. |
| Típicamente envía las actualizaciones por broadcast | Las actualizaciones son enviadas a los routers que participan en el dominio del protocolo de routing, vía dirección de multicast. |
| El conocimiento de la red está basado en la información aprendida de los vecinos. | Su conocimiento se basa en todos los routers del área. |
| La tabla de routing tiene la perspectiva del router. | La tabla topológica es igual para todos los routers del área. |
| Algoritmo de Bellman Ford | Algoritmo de Dijkstra |
| No consume muchos recursos de CPU, pero sí de ancho de banda | Consume mucha CPU, pero poco ancho de banda |
| Mantiene un dominio con todos los routers que conoce. | Utiliza un diseño jerárquico basado en áreas que permite una sumariación más efectiva. |
| No está restringido por el esquema de direccionamiento. | Para uso efectivo, el esquema de direccionamiento tiene que representar el diseño jerárquico de la red. |
| Convergencia Lenta. | Convergencia muy rápida. |

Capítulo 7

OSPF

7.1. Fundamentos

OSPF es un estándar abierto que utiliza el algoritmo SPF.

Es un protocolo de estado del enlace.

Estándar Abierto significa que cualquier puede leer las especificaciones y crear aplicaciones.

Muy buena solución para conectar varias tecnologías y varios fabricantes.

El propósito de OSPF es intercambiar información de routing entre los routers de la red.

La tecnología de estado del enlace está diseñada para ser muy eficiente a la hora de propagar las actualizaciones, permitiendo a la red crecer y ser escalable.

7.1.1. Terminología OSPF

Adyacencia: Se forma cuando dos routers vecinos han intercambiado información de routing y han sincronizado sus tablas. Ambos routers están en la misma red.

Área: Grupo de routers con el mismo ID de área. Los routers en un área comparten la misma tabla topológica. El área se describe por interfaz en base a la configuración.

Sistema Autónomo: Formado por routers que comparten el mismo protocolo de routing en la organización.

Backup Designated Router (BDR): En caso que falle el DR, el BDR tomará sus funciones.

Coste: No definido en el estándar, Cisco propone por defecto la siguiente. Se puede modificar.

Descriptor de la Base de Datos: Descrito como DBD (Data Base Descriptor) o como DDPs (Database Description Packets). Estos paquetes son intercambiados entre vecinos durante el estado exchange. Los DDPs contienen LSAs parciales, que suman los enlaces entre cada router de la topología del vecino.

Designated Router (DR): Router responsable de establecer las adyacencias entre todos los vecinos de una red de multiacceso. El DR se asegura que todos los routers tienen idéntica base de datos topológica.

Algoritmo de Dijkstra: Algoritmo complejo utilizado por los routers que utilizan protocolos de routing de estado del enlace, para encontrar el camino más corto al destino.

Estado Exchange: Estado en el cual dos vecinos descubren el mapa de la red. Cuando estos routers sean adyacentes, intercambiarán DDPs para asegurarse que tienen la misma base de datos topológica.

Estado Exstart: Estado en el cual dos vecinos determinan los números de secuencia de los DDPs y establecen su relación maestro/esclavo.

Inundación (Flood): La información de la red se manda a todos los dispositivos del dominio por inundación.

Adyacencia Completa (Fully Adyacency): Se produce en el momento que dos vecinos tienen totalmente sincronizadas la visión de la red (tienen exactamente la misma visión de la red).

Estado Init: Estado en el cual se ha enviado un paquete Hello y se

está esperando una respuesta para entrar en comunicación two-way.
Router Interno: Router que tiene todos los interfaces en el mismo área.

Link-State Advertisement (LSA): Paquete que describe los enlaces del router. Existen diferentes tipos de LSAs.

Link-State Database: También conocido como mapa topológico. Mapa con todos los routers, sus enlaces y estado de sus enlaces.

Link-State Request (LSR): Cuando un router recibe la DDP completa con LSAs parciales los compara la base de datos topológica, si encuentra algún LSA que no esté presente o con una entrada más antigua que la de la DDP, envía una petición (LSR) con más información.

Link-State Update (LSU): Respuesta a un LSR. Es un LSA con la información solicitada.

Estado Loading: Estado en el cual el router receptor solicita más información durante el proceso en el cual dos routers están creando la adyacencia. Si se necesita más información se enviará un LSR al que se responderá con un LSU.

Vecino: Router en el mismo enlace físico con el que se comparte información de routing.

Tabla de Vecinos: Tabla construida con paquetes Hello. Los paquetes Hello también portan información sobre los vecinos.

Prioridad: Herramienta de Cisco con la cual se puede escoger el DR, o incluso decidir que router nunca llegará a ser DR o BDR.

Shortest Path First (SPF): Es básicamente el algoritmo de Dijkstra, utilizado para decidir la(s) mejor(es) ruta(s).

Árbol SPF: Árbol de la red topológica. El algoritmo elimina del árbol aquellos enlaces alternativos que pueden crear bucles. Cada router es el punto central de la red.

Tabla Topológica: Lo mismo que la Base de Datos de Estado del Enlace.

Estado Two-Way: Estado durante el proceso de crear la adyacencia. El router ve su propio ID en un paquete Hello recibido de otro

router. Este es el punto anterior a que la información de routing sea intercambiada.

7.2. Características de OSPF

7.2.1. Vecinos OSPF

Un vecino OSPF es un router que comparte el mismo enlace de red en el mismo segmento físico.

Los vecinos se descubren enviando paquetes Hello.

Los mensajes Hello se envían cada 10 segundos, y en este caso se harán a la dirección de multicast 224.0.0.5 (AllSPFRouters).

Todos los routers ejecutando OSPF escuchan el protocolo y envían sus actualizaciones con paquetes Hello de forma periódica.

7.2.2. Vecinos OSPF Adyacentes

Una vez se ha establecido la comunicación entre vecinos se intercambian actualizaciones de routing.

Estas actualizaciones se introducen en la tabla topológica.

Posteriormente se calculan los mejores caminos en la tabla topológica y se construye la tabla de routing.

En el momento que las bases de datos topológicas de los routers son iguales se produce la adyacencia completa (fully adjacency).

Para asegurar la adyacencia se continúan enviando paquetes Hello.

Se continúan enviando paquetes Hello para asegurar que las bases de datos son precisas y se encuentran actualizadas.

Crear relaciones entre vecinos tiene una serie de ventajas:

- Mecanismo para detectar que un vecino se ha caído. Se detecta cuando el vecino deja de enviar paquetes Hello.

- Ya que los routers están sincronizados en el momento que haya un cambio se lo comunicarán automáticamente, así como cada 30 minutos.
- Las adyacencias creadas entre los vecinos controlan la distribución de los paquetes de los protocolos de routing.

El uso de adyacencias ayuda a una rápida convergencia, debido a que entre los vecinos existe una comunicación permanente.

7.2.3. El DR

Un router del segmento es asignado a la tarea de mantener las adyacencias con los demás routers del segmento. Este router se llama Designated Router (DR).

La elección del DR se hace mediante paquetes Hello, y se elige el que tenga la dirección más alta o mediante el siguiente comando:

```
Router(config-if)#ip ospf priority número
```

Todos los routers tienen que ser adyacentes con el DR.

El DR se establece en una red de multiacceso, esto implica que como todos los routers tienen que tener adyacencia con el DR, el DR y el BDR tienen que estar conectados con todos los demás.

La prioridad puede estar entre 0 y 255, donde cuanto más prioridad tenga, más probable será que llegue a ser DR.

7.2.4. El BDR

El Backup Designated Router (BDR), es el router que se queda como DR en caso de que el DR caiga.

Todos los routers del área tienen adyacencia con el DR y con el BDR, a su vez el BDR es adyacente con el DR.

Si el DR cae, automáticamente el BDR se convertirá en DR.

OSPF permite que el router principal, el DR, sea redundado con el BDR, de esta manera aseguramos que aunque caiga el DR, el protocolo siga funcionando correctamente.

7.2.5. Elección del DR y del BDR

El DR y el BDR pueden ser seleccionados de forma manual o dinámica.

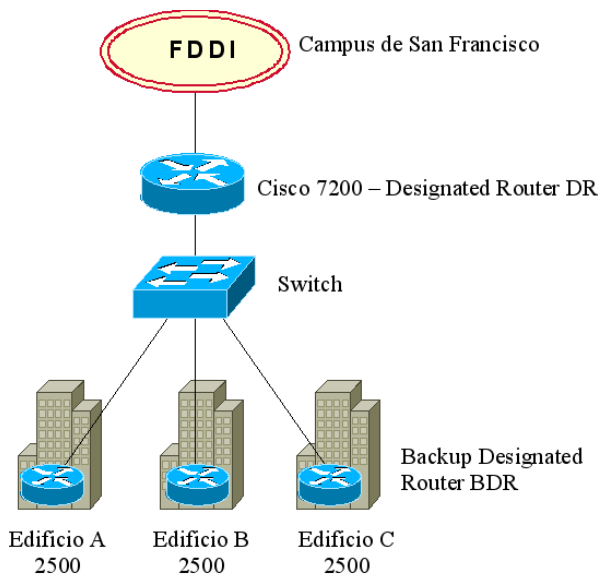
Elección Dinámica del DR.

- La selección se realiza en base al router ID más alto o a la dirección más grande. Esto puede no ser lo más óptimo.

Configuración Manual del DR.

- Para determinar qué router es el DR de forma manual lo haremos mediante la prioridad de OSPF.
- La prioridad por defecto en los routers Cisco es 1.

7.2.6. Ejemplo de DR y BDR



En este ejemplo hemos elegido el router Cisco 7200 como DR de forma manual, ya que es el router más potente de la red. De esta forma ya no dependemos que la dirección IP que tengamos. Además el 7200 será el responsable de las redes FDDI y la ethernet de abajo.

7.2.7. La Elección del DR

El proceso de elección de DR es el siguiente, suponemos que todos los routers tienen prioridad ≥ 1 :

1. El vecino con mayor prioridad es elegido como BDR.
2. Si no hay DR, el BDR es promocionado a DR.
3. Para el resto de los routers, el de mayor prioridad será elegido BDR.

- 4. Si no se ha configurado la prioridad habrá un empate, porque por defecto todos los routers tienen prioridad 1.
- 5. Si hay un empate, el router con mayor ID será elegido.

7.2.8. Cabeceras de OSPF y del paquete Hello

7.2.8.1. Cabecera OSPF

| |
|-------------------------------|
| Version (8 bits) |
| Type (8 bits) |
| Packet Lenght (16bits) |
| Router ID (32 bits) |
| Area ID (32 bits) |
| Checksum (16 bits) |
| Authentication Type (16 bits) |
| Authentication (16 bits) |

| Campo | Características | Función |
|------------------------|---|---|
| Cabecera Común de OSPF | | |
| Version | La versión de OSPF, actualmente estamos en la versión 2 | Asegurar que la versión de OSPF es compatible |
| Type | Tipo de paquete OSPF | p.e. El tipo 1 es un paquete Hello |
| Packet Lenght | Longitud del paquete OSPF, incluyendo cabecera | Se utiliza para identificar la longitud |

| | | |
|---------------------|---|---|
| Router ID | Número de 32 bits. La dirección IP más alta del router se utiliza como router ID. También se pueden utilizar direcciones de loopback. | Este campo identifica el router dentro del sistema autónomo |
| Area ID | Es el Area ID para el interfaz del router que origina el paquete | El paquete Hello tiene que venir de un router dentro del mismo área |
| Checksum | Suma de comprobación de todo el paquete OSPF excluyendo el campo de autenticación | Se utiliza para comprobar la integridad del paquete. |
| Authentication Type | Tipo de autenticación utilizada | Asegura la misma autenticación en ambos extremos |
| Authentication | Autenticación de 64 bits | Utilizado para seguridad entre sistemas. |

7.2.8.2. Cabecera Hello

| |
|-----------------------------|
| OSPF Header (192 bits) |
| Network Mask (32 bits) |
| Hello Interval (16 bits) |
| Options (8 bits) |
| Router Priority (8 bits) |
| Dead Interval (32 bits) |
| Designated Router (32 bits) |
| Backup Router (32 bits) |
| Neighbor (32 bits) |
| etc... |

| Campo | Características | Función |
|---------------------------|---|--|
| Formato del Paquete Hello | | |
| Network Mask | La máscara de red para el interfaz transmisor | Debe de coincidir con la máscara del interfaz receptor |
| Hello Interval | Utilizado en broadcast y redes de multiacceso: Dead interval = 40 Hello=10 sec | Hello mantiene la presencia del router en las bases de datos de sus vecinos, funciona como si fuera un keepalive |
| Options | Utilizado en redes de nonmultiaccess: Dead interval = 120 Hello=30 sec | |
| Router Dead interval | | El Dead Interval es el tiempo antes de determinar que el router vecino ha caído. Normalmente son 4 mensajes Hello. |

| Campo | Características | Función |
|--------------------------|---|--|
| Neighbor | Es el router ID del vecino, cuando hay comunicación two-way | Vecino es aquel que intercambia datos de routing con el 1er router y que sincroniza sus BBDD |
| Rtr Pri | Prioridad del router | Para escoger el DR y el BDR de forma manual |
| Designated Router | Dirección del DR existente | Para crear tráfico de Unicast con el DR |
| Backup Designated Router | Dirección del BDR existente | Para crear tráfico de Unicast con el BDR |
| Authentication | Especifica el tipo de encriptación | Utilizado por seguridad |

7.3. Operación en un área

7.3.1. Creación y mantenimiento de la tabla de routing de OSPF

Después de descubrir un vecino se tiene que crear la adyacencia.

La tabla de routing se crea de diferentes formas, ya que puede ser se tenga que ajustar las bases de datos o que un router nuevo haya que añadirlo a la red.

La diferencia entre estas dos técnicas es la siguiente:

- Si se conecta un nuevo router a la red, se intercambiarán paquetes Hello y se intercambiará información de routing.

- Si ocurre un cambio en la topología, el router verá el cambio y este será inundado por toda la red. **Link-State Acknowledgement**

Es necesario saber la diferenciar las dos técnicas para poder comprender el funcionamiento de OSPF.

7.3.2. Cómo construir la tabla de routing en un router nuevo

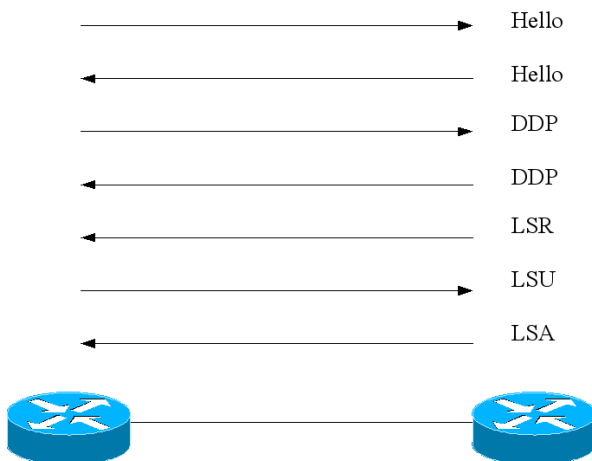
Al añadir un nuevo router a la red, se construye una tabla de routing escuchando los routers y completando las tablas de routing.

Se definen 5 tipos de paquetes para construir la tabla de routing la primera vez:

- **Protocolo Hello:** Utilizado para encontrar vecinos y determinar el DR y el BDR. La propagación continua del protocolo Hello mantiene al router actualizado.
- **Descriptor de la Base de Datos:** Envía información sumariada a los vecinos para sincronizar sus bases de datos topológicas.
- **LSR:** Link State Request. Solicita información más detallada sobre una ruta.
- **LSU:** Link State Update. Respuesta a una petición LSR.
- **Link-State Acknowledgement:** Acepta el LSU

Cada router en el área tendrá la misma base de datos y tendrá el mismo conocimiento de la red o área.

7.3.3. Creación de la tabla de routing



En la imagen se puede ver el intercambio de paquetes entre los dos routers explicado en el punto anterior.

7.3.4. Encontrar los vecinos en el proceso de intercambio

En el momento de conectar un nuevo router funcionando con OSPF a la red, este debe de aprender la red de los sistemas que están funcionando correctamente.

Para comprobar el estado del proceso utilizaremos los comandos:

```
show ip ospf neighbor
debug ip ospf adjacency
```

Hay que tener cuidado al utilizar los comandos de debug, ya que este tipo de comandos hacen un uso intensivo de la CPU.

7.3.5. Establecimiento de vecindad

Las diferentes fases por las que pasan los routers en el proceso de establecer la vecindad son:

- **Estado Down:** El router envía paquetes Hello para presentarse a sus vecinos. Estos paquetes se envían a la dirección de multicast 224.0.0.5 (AllSPFRouters), en este paquete el DR y el BDR tienen un ID de 0.0.0.0.
- **Estado Init:** El router espera una respuesta de un DR o de un BDR, normalmente es de 4 veces el tiempo del envío de paquetes Hello.
- **Estado Two-Way:** En este punto el router ve en un mensaje de un vecino su propio ID, en ese momento el router ha establecido una relación con ese vecino.

Descubrimiento de Rutas:

- Una vez que se establece la vecindad hay que empezar a intercambiar rutas.

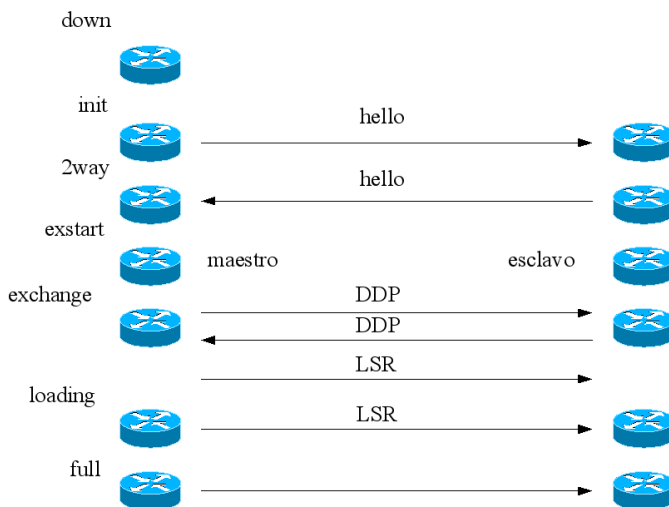
Fases del descubrimiento de rutas:

- **Estado Exstart:** En este estado se establece una relación maestro / esclavo. El maestro será el que tenga la IP más alta, esta relación no significa nada, sólo determina quien empieza a hablar.
- **Estado Exchange:** Ambos routers se se envían sus DDPs. Se envían sus interfaces ID del interfaz saliente, el link ID, y la métrica. Cuando el router recibe los DDPs, los compara con lo que tiene en la base de datos topológica. Si existen diferencias entonces las comunica a los demás routers.
- **Estado Loading:** Si el router receptor necesita más información de la que ha recibido por los DDPs entonces solicitará más

mediante un LSR, a lo que el primer router contestará con un LSU.

- **Estado Full (full state):** Cuando se ha solicitado todos los LSR y se han sincronizado las bases de datos entonces los vecinos son totalmente adyacentes.

Cuadro resumen de los Estados:



7.3.6. La base de datos topológica

La base de datos topológica es la visión del router dentro del área, incluye todos los routers OSPF con todas sus redes directamente conectadas.

Esta base de datos se actualiza mediante LSAs.

La base de datos topológica es idéntica en todos los routers del área.

La sincronización de los mapas topológicos se realiza con un orden muy meticuloso de los números de las cabeceras de los LSAs.

De los mapas topológicos se obtiene la base de datos de routing.

A la base de datos de routing se le aplica el SPF para obtener la tabla de routing.

En el caso de que se produzca flapping OSPF implementa unos temporizadores.

La RFC2328 no define un número máximo de enlaces máximos para balancear el tráfico, sin embargo Cisco define que el máximo será 6 y que por defecto se habilita la posibilidad de poner 4 caminos en paralelo.

7.3.7. Mantenimiento de la base de datos topológica y la tabla de routing

En el momento que el router tiene constancia de que se ha producido un cambio en la topología, este es responsable de propagar el cambio. El cambio ha sido producido por las siguientes razones:

- El router pierde el enlace físico o de enlace a una red: El router propaga un LSU al DR en redes de multiacceso o al vecino en redes punto a punto.
- El router no ha recibido paquetes OSPF Hello: El router propaga un LSU al DR en redes de multiacceso o al vecino en redes punto a punto.
- El router recibe una actualización LSA de un vecino adyacente, infomándole de un cambio en la topología: El LSU es aceptado e inundado por los demás interfaces.

Si ocurre alguna de estas cosas el router es responsable de transmitir esta información a los demás.

7.3.8. Aprendizaje de nueva ruta.

En el caso de recibir una nueva ruta mediante un LSA tendremos que tener el cuenta:

- Si el LSA es más moderno que el que teníamos.
- Reenviaremos el LSA por todos los interfaces excepto por el que ha llegado.
- Si hay que procesar la entrada del LSA se espera el tiempo para realizar la actualización necesario.
- Además de realizar este aprendizaje cada 30 minutos se sincronizarán las BBDD aunque no haya actualizaciones para asegurar la coherencia.

Para comprobar si el LSA es más moderno compararemos número de LSA, si es igual compararemos la checksum, si es igual miraremos el campo MaxAge, y nos quedaremos con el mayor.

7.3.9. Escoger el camino más corto para construir la tabla de routing

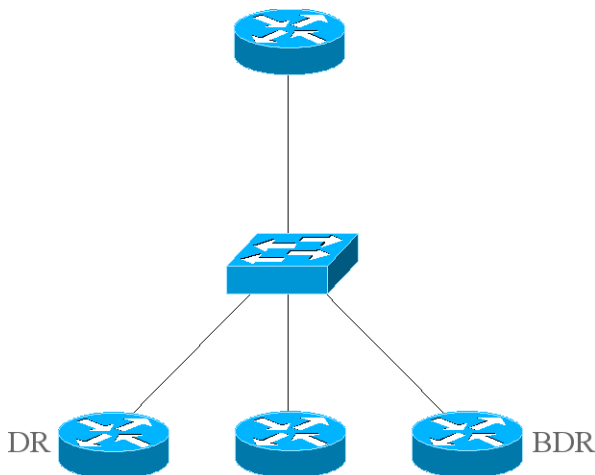
Métrica: La decisión de qué camino tomar se basa en la métrica. Si la CPU y la memoria es lenta entonces se producirá latencia. En OSPF no está definido el coste y este está en función de la implementación del protocolo, y por supuesto, el administrador puede cambiar el coste. Si es posible utilizar varios caminos para un mismo destino, entonces hablamos de **multiple equal-cost paths**. El coste se aplica al interfaz saliente y el proceso de routing escogerá la ruta basándose en el camino con menor coste acumulado.

Información Necesaria para la Tabla de Routing: Una vez determinado el camino más corto, el proceso de routing necesita proporcionar información adicional: siguiente salto lógico, interfaz de salida. Esta información la requiere la tabla de routing o forwarding database.

7.4. Topologías de OSPF

7.4.1. Broadcast multiaccess

Las redes de multiacceso son cualquier LAN, como Ethernet, Token Ring o FDDI. En este entorno OSPF envía tráfico de multicast. Se elige un DR y un BDR.



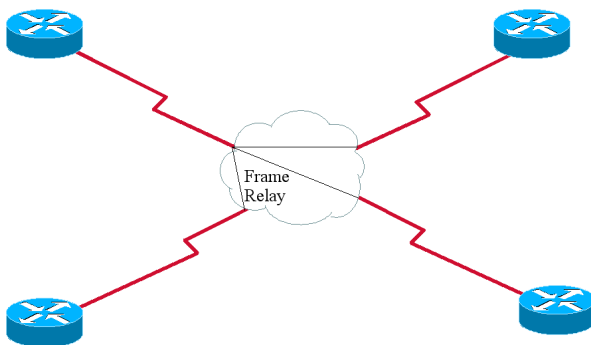
7.4.2. Punto a punto

Este tipo de topología se utiliza cuando un router está directamente conectado a otro. Un ejemplo típico una conexión serie.



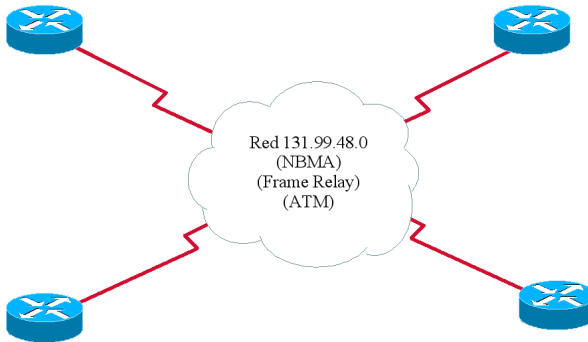
7.4.3. Punto a multipunto

En este tipo de topologías un interfaz se conecta con múltiples interfaces, tratándolo como múltiples circuitos punto a punto. No existe elección de DR y de BDR.



7.4.4. NBMA - Non Broadcast Multiaccess

Físicamente, varias punto-multipunto no pueden soportar multicast o tráfico de broadcast. En una topología NBMA se requiere una configuración especial. NBMA físicamente requiere enlaces punto a punto, de forma total o parcialmente mallada. OSPF envía un broadcast por cada uno de los enlaces. Se requiere una configuración manual del DR, del BDR y de los vecinos. El DR es pues el encargado de generar los LSAs para los nodos de la red.



7.4.5. Virtual-links

Un virtual-link es una conexión virtual a un área remota que no tiene ninguna conexión con el área de backbone.

Sin embargo OSPF va a tratar a estos enlaces como directamente conectados al área 0, ya que se crearán túneles a través del enlace virtual.

El tráfico de OSPF de la red será enviado como datagramas unicast a través de estos enlaces.

7.4.6. OSPF a través de redes NBMA

Una red NBMA es aquella red que no permite el envío de tráfico a múltiples destinos.

Como OSPF trabaja con tráfico de multicast es necesario solventar este problema y esto lo haremos utilizando una de las dos posibles tecnologías.

- Punto a punto
- NBMA

Existen dos categorías que subdividen las tecnologías NBMA:

- RFC-Compliant: Solución Independiente a la plataforma.
 - NBMA.
 - Point-to-multipoint.
- Cisco-Specific. Solución específica de Cisco Systems.
 - Point-to-multipoint nonbroadcast.
 - Broadcast.
 - Point-to-point.

La selección de la tecnología a utilizar depende de la topología de la red.

Las topologías Frame Relay incluyen lo siguiente:

- Totalmente Mallada: Todos los routers están conectados entre ellos, todos con todos. Esta solución proporciona redundancia y balanceo de carga. Es la solución más cara.
- Parcialmente Mallada: Varios routers conectados con varios routers.
- Estrella o hub-and-spoke: Un router está conectados con todos los demás. Esta es la solución más económica, ya que requiere el mínimo número de PVCs.

7.4.7. Escogiendo una topología

- Circuito point-to-point:
 - No se requiere BR o BDR.
 - En cada circuito existe una adyacencia.
- Entorno NBMA:

- Se requiere BR y BDR, a no ser que la tecnología subyacente sea punto a punto.
- Cada router establece dos adyacencias, una con el DR y otra con el BDR.
- Requiere mucha administración en términos de configuración.

7.4.8. OSPF sobre NBMA

| | Point-to-point nonbroadcast | Point-to-point | Broadcast | NBMA | Point-to-multipoint |
|-------------------------------------|--------------------------------|---|--------------------|------------------------------|--------------------------------|
| Direccionamiento | Unicast | Multicast | Multicast | Unicast | Multicast |
| DR/BDR | No | No | Sí | Manual Sí | No |
| Configuración manual de los vecinos | Sí | No | No | Sí | No |
| Hello | 30 Seg, Dead=120 segundos | 10 seg. Dead=40 | 10 seg. Dead=40 | 30 Seg, Dead=120 segundos | 30 Seg, Dead=120 segundos |
| RFC/Cisco | Cisco | Cisco | Cisco | RFC2328 | RFC2328 |
| Redes soportadas | Estrella, parcialmente mallada | Estrella, parcialmente mallada, subinterfaces | Totalmente mallada | Totalmente mallada | Estrella, parcialmente mallada |

| | Point-to-point nonbroadcast | Point-to-point | Broadcast | NBMA | Point-to-multipoint |
|-------------------------|--------------------------------|----------------------------|-----------|------|---------------------|
| Replicación de paquetes | Sí | Sí | Sí | Sí | Sí |
| Número de Subredes | 1 | Muchas (1 por circuito) | 1 | 1 | 1 |

Para interfaces serie HDLC. Point-to-point (hello 10, dead 40).

Para interfaces Frame Relay. Nonbroadcast (hello 30, dead 120).

Para interfaces Frame Relay con subinterfaces point-to-point. Point-to-point (hello 10, dead 40).

Para interfaces Frame Relay con subinterfaces point-to-multipoint. Nonbroadcast (hello 30, dead 120).

7.5. Configuración de OSPF en un único área

7.5.1. Comandos de configuración requeridos

Para configurar un router Cisco y hacerle entender que tiene que participar en una red OSPF hay que indicarle al menos:

- **El proceso OSPF:** Es necesario arrancar el proceso de routing en el router. OJO, no en todos los routers hay que configurar el proceso, p.e. En un router Quagga no hay que configurarlo, ya que Quagga sólo soporta un proceso OSPF.
- **Interfaces del router que participan en OSPF:** Es de esperar que no todos los interfaces del router participen en el

protocolo de routing, para ello definiremos los interfaces que van a entrar definiendo sus redes.

- **Identificación del área:** Se define en el área que van a participar cada uno de sus interfaces.
- **Router ID (RID):** Esto permite que el router pueda ser identificado por los demás routers de la red y pueda ser el siguiente salto.

Para habilitar el OSPF en un único router tendremos que habilitar lo siguiente.

```
router ospf número de proceso  
network número de red
```

7.5.2. Habilitar el protocolo de routing OSPF

```
Router(config)#router ospf número-de-proceso
```

En este comando el *número-de-proceso* es de significado local, es decir, no tiene que ser el mismo en todos los routers.

El *número-de-proceso* identifica el proceso del OSPF, puede haber más de un proceso, pero no es recomendado por el gasto que hace de recursos.

Un escenario posible para la utilización de varios procesos OSPF sería un proveedor de servicios que quiere separar su dominio de OSPF del resto.

No es necesario que todos los routers ejecuten el mismo número de proceso, sin embargo es recomendado por razones de coherencia en los equipos de la red.

7.5.3. Habilitar la red con OSPF

```
Router(config)#network número-de-red máscara-wildcard  
area número-de-área
```

Una vez arrancado el OSPF tenemos que decirle que tiene que tiene que operar con alguna red, para ello utilizaremos el comando de arriba.

El comando **network** es muy similar al network de RIP, la diferencia es el grado de granularidad.

Hemos de tener en cuenta que en OSPF no utilizamos la máscara de red en el comando **network**, sino la wildcard.

La wildcard es la máscara de red invertida.

```

255.255.255.255
- 255.255.255.000  ->  Máscara original
-----
000.000.000.255  ->  Wildcard resultante

```

La wildcard se calcularía de esta manera.

7.5.4. ¿Qué hace el comando **network**?

Después de que se haya introducido el comando **network**, OSPF identifica los interfaces que van a participar en la red OSPF.

Las direcciones de los interfaces a participar se fijan a través de la wildcard.

Tras identificar los interfaces que van a participar en OSPF sucede lo siguiente:

- Las actualizaciones serán recibidas en el interfaz.
- Las actualizaciones serán enviadas desde el interfaz.
- Los interfaces estarán definidos dentro de un área.
- Dependiendo del tipo de interfaz serán propagados paquetes Hello.

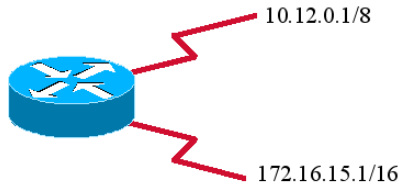
Si existen áreas stub podría ser útil realizar una redistribución de las redes conectadas directamente mediante el comando:

```
Router(config-router)#redistribute connected subnets
```

El comando **network** funciona de una forma similar a los ACLs. La wildcard mask tiene el mismo formato y permite habilitar un grupo de interfaces en un área.

El comando **redistribute connected subnets** permite anunciar por el proceso de OSPF los interfaces directamente conectados que forman parte de la red OSPF.

7.5.5. Ejemplos de configuración



Si queremos anunciar todas las redes en OSPF:

```
Router(config-router)#network 0.0.0.0 255.255.255.255  
area 0
```

Si queremos anunciar sólo la 10.0.0.0/8:

```
Router(config-router)#network 10.0.0.0 0.255.255.255  
area 0
```

Si queremos anunciar sólo los interfaces:

```
Router(config-router)#network 10.12.0.1 0.0.0.0  
area 0  
Router(config-router)#network 172.16.15.1 0.0.0.0  
area 0
```

7.5.6. Complejidad del comando `network` en OSPF

El comando `network` es más complejo en OSPF que en RIP o IGRP ya que OSPF permite que un router esté ejecutando varias áreas a la vez y además OSPF permite una precisión a la hora de describir las redes que no nos permite ni RIP ni IGRP.

7.5.7. Opciones de configuración en un router interno (IR)

Las siguientes opciones no son necesarias para el correcto funcionamiento de OSPF, pero pueden ser útiles en los diseños de red:

- Interfaz de Loopback.
- El comando `cost`.
- El comando `priority`.
- El RID (Router ID).

7.5.8. El interfaz de loopback y el router ID

El router necesita un ID para participar en el dominio de OSPF.

El RID es el identificador que va a tener el router dentro del dominio de OSPF y va a ser cómo lo van a ver los vecinos.

El RID también es el identificador que se utiliza para la elección del DR y el BDR, el RID mayor será el que sea el DR si todos tienen la misma prioridad.

El RID se utiliza para identificar el origen de las actualizaciones LSA y mostrarlos en la base de datos.

El ID se coge de una dirección IP, y recordemos que el RID es utilizado para la elección de DR y del BDR, así que es posible definir una interfaz de loopback, la cual nunca se va a caer, con una IP mayor para que sea el RID del router.

Selección Automática del RID:

- La realiza el router automáticamente y es la IP más grande de los interfaces del router.

Selección Manual del RID:

- Se configura mediante el comando `router-id`.

7.5.9. Configuración del interfaz de loopback y del RID

Para configurar la interfaz de loopback:

```
Router(config)#interface loopback número-de-interfaz
Router(config-if)#ip address dirección-ip máscara-de-
subred
```

Para configurar el RID:

```
Router(config)#router ospf número-de-proceso
Router(config-router)#router-id dirección-ip
```

En el caso del comando `router-id` la dirección IP representa el identificador del router que se lo indicamos con un IP, esa dirección IP no tiene porque ser una dirección IP del router.

Es muy útil definir diferentes rangos para las direcciones de loopback, ya que de esta forma serán fácilmente diferenciables del resto.

Estas son las dos formas que tenemos de utilizar una dirección IP en un router de forma que se identifiquen en el dominio de OSPF con otra IP a la de los interfaces “reales”.

7.5.10. Cambiar la métrica por defecto utilizando el comando `cost`

Otro comando muy útil es `cost`, ya que nos permite modificar la métrica asignada por el protocolo a un enlace, se configura pues en el interfaz.

El valor por defecto se calcula con el comando `bandwidth` del interfaz:

```
Router(config-if)#ip ospf cost coste
```

También es posible controlar como OSPF calcula sus métricas por defecto con el comando:

```
Router(config-router)#ospf auto-cost reference-  
bandwidth bandwidth-de-referencia
```

En el comando `ip ospf cost` el `coste` está comprendido entre 1 y 65535, y se refiere al ancho de banda. Recordemos que el `coste` por defecto es:

$$\frac{10^8}{\text{ancho de banda}}$$

Costes por defecto en OSPF:

| Tipo de Enlace | Coste por Defecto |
|---------------------|-------------------|
| 56 kbps | 1785 |
| T1 (1,544 Mbps) | 64 |
| ethernet (10Mbps) | 10 |
| token ring (16Mbps) | 16 |
| FDDI (100Mbps) | 1 |

En el comando `ospf auto-cost reference-bandwidth reference-bandwidth`, `reference-bandwidth` hace referencia al punto de referencia tomado para calcular la métrica. Por defecto es 100, esto significa que $1=100\text{Mbps}$ y $10=100/10=10\text{Mbps}$, si quisiéramos considerar Gigabit Ethernet podríamos de `reference-bandwidth` el valor 1000.

Actualmente `ospf auto-cost` se escribe como `auto-cost`, para comprobarlo es mejor ir directamente a la referencia de IOS.

Hemos de tener en cuenta que no se puede modificar el coste de OSPF así por las buenas, para poderlo hacer tenemos que documentar las razones.

Si modificamos el coste:

- Puede que nuestros routers no puedan interoperar con otros de otros fabricantes.
- Puede ser que cambien las rutas.

7.5.11. Determinar el DR con el comando `priority`

El último comando operacional a considerar es `priority`.

Este comando se utilizará para determinar el DR y el BDR

Las razones para modificar la prioridad del router son:

- El router es que dispone de más memoria y CPU.
- El router es el más fiable de la red.
- Todos los demás routers de la LAN están conectados a áreas stub, es decir, pertenecen al nivel de acceso.
- Existe una topología NBMA de punto-multipunto y el router se elige como DR ya que actúa como una “especie” de hub.
- El router es ABR y no queremos que tenga más carga al convertirse en DR, así que le disminuimos la prioridad.

```
Router(config-if)#ip ospf priority prioridad
```

La prioridad se utiliza para escoger el DR y el BDR de la red y va desde 1 hasta 255.

7.5.12. Ejemplo de configuración de OSPF

```
Router(config)#router ospf 100
Router(config-router)#network 192.168.1.0 0.0.0.248 area 0
Router(config-router)#interface ethernet 0
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#ip ospf priority 100
Router(config-if)#no shutdown
Router(config-if)#interface ethernet 1
Router(config-if)#ip address 192.168.1.5 255.255.255.252
Router(config-if)#ip ospf cost 10
Router(config-if)#no shutdown
```

7.6. Configuración de OSPF en topologías NBMA

7.6.1. Consideraciones de diseño de OSPF en topologías NBMA

Las elecciones de configuración en este tipo de topologías es muy delicado y puede afectar a la funcionabilidad de la red.

En topologías parcialmente malladas, la elección de punto a punto gasta más direcciones que en una punto multipunto, pero si se utiliza direccionamiento privado, esto no es un problema.

La elección se hace con el comando:

```
Router(config-if)#ip ospf network {broadcast /
    non-broadcast / {point-to-multipoint
    [non-broadcast]}}
```

¹

El comando `ip ospf network`:

| Opción | Descripción |
|---------------------|---|
| Broadcast | Configura la red en modo de broadcast. |
| Non-broadcast | Configura la red en modo de NBMA. Este es el modo por defecto para interfaces frame-relay y subinterfaces punto-multipunto. |
| Point-to-multipoint | Configura la red en modo de nonbroadcast punto multipunto. |

7.6.2. Configuración de OSPF en modo NBMA

En el modo NBMA, las consideraciones de diseño son imperativas, ya que se debe de asegurar la conexión física con el DR y el BDR.

Este es un entorno de nonbroadcast, por lo tanto hay que configurar una lista estática con los vecinos. Esto se consigue con el comando `neighbor`.

```
Router(config-if)#neighbor dirección-ip [priority número]
[poll-interval segundos] [cost número]
```

```
Router-Cisco(config-if)#ip ospf network ?
broadcast Specify OSPF broadcast multi-access network
non-broadcast Specify OSPF NBMA network
point-to-multipoint Specify OSPF point-to-multipoint network
point-to-point Specify OSPF point-to-point network
```

7.6. CONFIGURACIÓN DE OSPF EN TOPOLOGÍAS NBMA141

| Sintaxis | Descripción |
|--------------------------------------|--|
| Dirección-ip | Dirección IP del interfaz del vecino. |
| Priority número (Opcional) | Número de 8 bits que indica la probabilidad de que el vecino sea elegido DR o BDR. Por defecto es 0. Obviamente esto no aplica en interfaces punto a punto ya que no necesitan ni DR ni BDR. Esta es otra forma de aplicar el ip ospf priority. |
| Poll-interval segundos (Opcional) | Intervalo de consulta, según la RFC1247, este tiempo tiene que ser muy superior al tiempo de Hello. Por defecto 120 segundos. Este comando no se aplica a topologías punto-multipunto. Este es el tiempo que hay que esperar antes de enviar un paquete para comprobar que el vecino sigue vivo. |
| Cost número (Opcional) | Valor asignado a la métrica. Esta es la otra forma de aplicar el el ip ospf cost. |

7.6.3. El comando neighbor

```
Router(config)#interface Serial0
Router(config-if)#ip address 131.144.10.100
255.255.255.0
Router(config-if)#encapsulation frame-relayEstablecimiento de
Router(config-if)#ip ospf network non-broadcast
Router(config)#router ospf 1
Router(config-router)#network 131.144.10.0
0.0.0.255 area 0
```

```
Router(config-router)#neighbor 131.144.10.2
Router(config-router)#neighbor 131.144.10.3
Router(config-router)#neighbor 131.144.10.5
```

NBMA es el modo por defecto en entornos de acceso de multiacceso sin broadcast, por eso no hay necesidad del comando `ip ospf network non-broadcast`.

Sin embargo el comando `neighbor` es necesario.

7.6.4. Configurar OSPF en modo point-to-multipoint

Un interfaz OSPF point-to-multipoint es visto como un interfaz point-to-point con uno o más vecinos.

Se pueden especificar los vecinos con el comando `neighbor`, en cual case tendremos que especificar un coste a cada vecino.

No es necesario establecer una topología totalmente mallada.

Para cambiar la topología NBMA por defecto por point-to-multipoint podemos utilizar el comando:

```
Router(config-if)#ip ospf network point-to-multipoint
```

Y cambiar a nonbroadcast point-to-point

```
Router(config-if)#ip ospf network point-to-multipoint
non-broadcast
```

Por defecto una red es consideada como una serie de interfaces punto a punto.

No es necesaria la elección de DR o de BDR.

En point-to-multipoint la adyacencia se produce automáticamente en cada PVC, lo cual crea más sobrecarga, pero es más resistente que NBMA.

7.6. CONFIGURACIÓN DE OSPF EN TOPOLOGÍAS NBMA143

La topología point-to-point se considera una topología de broadcast, con lo cual al utilizar non-broadcast es imprescindible utilizar el comando neighbor.

7.6.5. Ejemplo topología point-to-multipoint

```
Router(config)#interface Serial0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#encapsulation frame-relay
Router(config-if)#ip ospf network point-to-multipoint
Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.0.0.255 area 0
```

7.6.6. Configuración de OSPF en modo broadcast

El modo de broadcast funciona en una red totalmente mallada.

No es necesario utilizar el comando neighbor.

Ejemplo de Configuración de OSPF en Modo Broadcast:

```
Router(config)#interface Serial0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#encapsulation frame-relay
Router(config-if)#ip ospf network point-to-multipoint
Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.0.0.255 area 0
```

7.6.7. Configuración de OSPF en modo point-to-point en subinterfaces frame relay

En modo point-to-point, la adyacencia creada entre los routers es automática, ya que cada subinterfaz se comporta como una red física point-to-point.

Los pasos que explican como configurar OSPF en modo point-to-point en subinterfaces son los siguientes:

- Configurar la encapsulación Frame Relay en el Interfaz.
- En el nivel de Interfaz crear el subinterfaz. Es recomendable eliminar cualquier direccionamiento de nivel 3 del interfaz.
- Configurar las direcciones de nivel 3 y de nivel 2 (DLCI) en el subinterfaz
- El modo point-to-point es el por defecto en subinterfaces OSPF, así que no es necesaria más configuración.

7.6.8. Ejemplo de configuración de OSPF en modo point-to-point en subinterfaces frame relay

```
Router(config)#interface Serial0
Router(config-if)#no ip address
Router(config-if)#encapsulation frame-relay
Router(config)#interface Serial0.1 point-to-point
Router(config-subif)#ip address 10.1.1.1 255.255.255.0
Router(config-subif)#frame-relay interface-dlci 51
Router(config)#interface Serial0.2 point-to-point
Router(config-subif)#ip address 10.1.2.1 255.255.255.0
Router(config-subif)#frame-relay interface-dlci 52
```

Hasta aquí sería la configuración de los subinterfaces:

```
Router(config)#router ospf 1
Router(config-router)#network 10.1.0.0 0.0.255.255
```

7.6.9. Comprobar la configuración de OSPF en un único router

`show ip ospf`

- Muestra el proceso y sus detalles, como por ejemplo, cuantas veces se ha ejecutado el SPF.

7.6. CONFIGURACIÓN DE OSPF EN TOPOLOGÍAS NBMA145

`show ip ospf database`

- Muestra los contenidos de la base de datos topológica

`show ip ospf interface`

- Muestra información sobre cómo ha sido configurado OSPF en cada interfaz, etc.

`show ip ospf neighbor`

- Muestra toda la información sobre la relación que el router tiene con sus vecinos.

`show ip protocols`

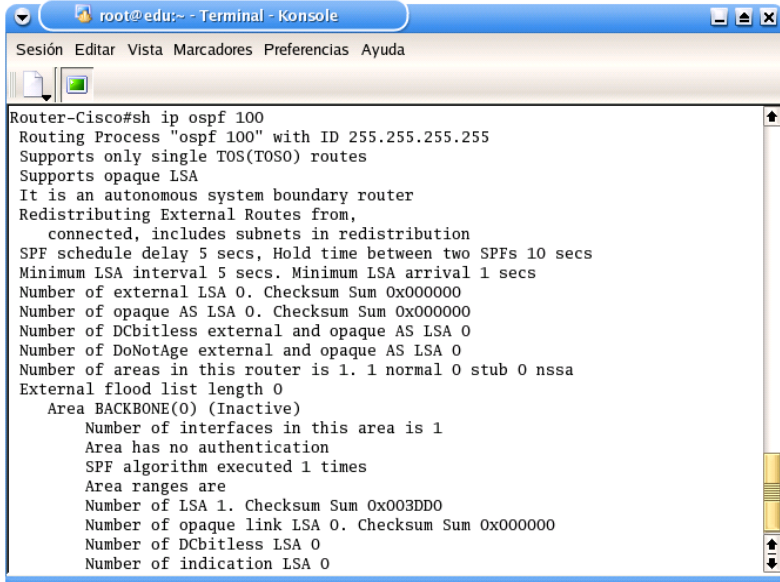
- Habilita la vista de vista de los protocolos de routing IP en el router.

`show ip route`

- Muestra información detallada sobre la tabla de routing.

7.6.9.1. El comando show ip ospf

Router#show ip ospf [ID-del-proceso]



```
root@edu:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

Router-Cisco#sh ip ospf 100
Routing Process "ospf 100" with ID 255.255.255.255
Supports only single TOS(TOS0) routes
Supports opaque LSA
It is an autonomous system boundary router
Redistributing External Routes from,
connected, includes subnets in redistribution
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0) (Inactive)
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 1 times
    Area ranges are
      Number of LSA 1. Checksum Sum 0x003DD0
      Number of opaque link LSA 0. Checksum Sum 0x000000
      Number of DCbitless LSA 0
      Number of indication LSA 0
```

Este comando es muy útil ya que muestra como está corriendo el protocolo de routing OSPF en un router particular. Incluyendo el número de veces que se ha ejecutado el algoritmo SPF, el cual muestra la estabilidad de la red.

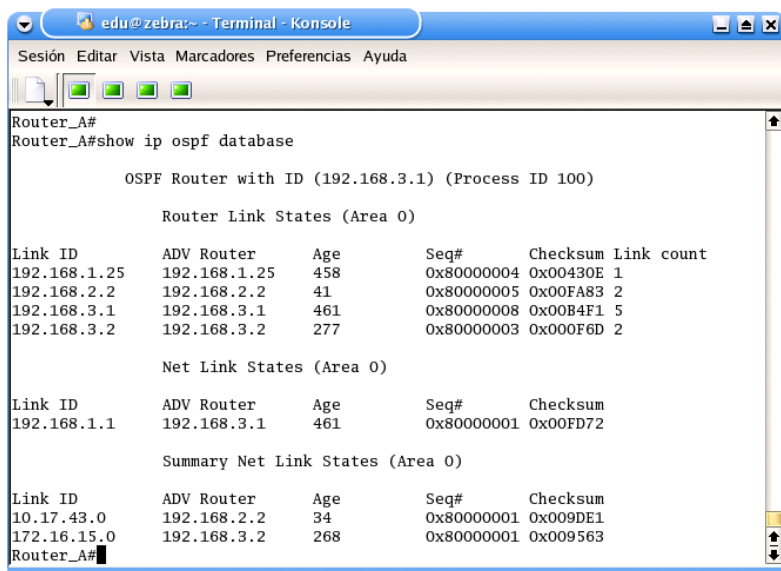
- Routing Process “ospf 100” with ID ...: Indica el RID y el proceso.
- Supports only single ToS (TOS0) routes: OSPF es capaz de llevar información sobre el tipo de servicio que el datagrama solicita. Esto lo soporta Cisco de acuerdo con el RFC.
- This is an autonomous boundary router: Especifica el tipo de router.

7.6. CONFIGURACIÓN DE OSPF EN TOPOLOGÍAS NBMA147

- SPF schedule delay: Especifica el tiempo a esperar para calcular el SPF y prevenir flapping.
- Hold time between two SPFs: Especifica el tiempo mínimo entre cálculo de SPFs.
- Number of Dcbitless external LSA: Utilizado para cicuitos OSPF bajo demanda.
- Number of DoNotAge external LSA: Utilizado para cicuitos OSPF bajo demanda.

7.6.9.2. El comando show ip ospf database

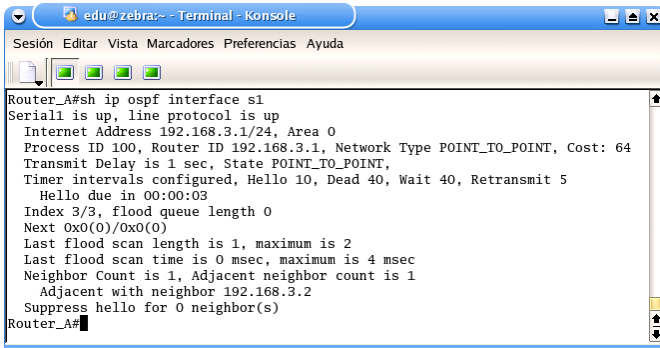
Router#show ip ospf database



```
Router_A#  
Router_A#show ip ospf database  
  
        OSPF Router with ID (192.168.3.1) (Process ID 100)  
  
        Router Link States (Area 0)  
  
Link ID        ADV Router    Age         Seq#          Checksum Link count  
192.168.1.25   192.168.1.25  458        0x80000004   0x00430E  1  
192.168.2.2    192.168.2.2   41         0x80000005   0x00FA83  2  
192.168.3.1    192.168.3.1   461        0x80000008   0x00B4F1  5  
192.168.3.2    192.168.3.2   277        0x80000003   0x000F6D  2  
  
        Net Link States (Area 0)  
  
Link ID        ADV Router    Age         Seq#          Checksum  
192.168.1.1    192.168.3.1   461        0x80000001   0x00FD72  
  
        Summary Net Link States (Area 0)  
  
Link ID        ADV Router    Age         Seq#          Checksum  
10.17.43.0     192.168.2.2   34         0x80000001   0x009DE1  
172.16.15.0    192.168.3.2   268        0x80000001   0x009563  
Router_A#
```

7.6.9.3. El comando show ip ospf interface

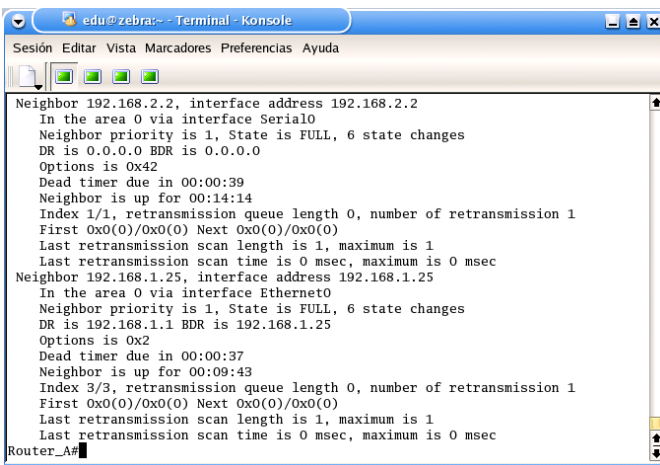
Router#show ip ospf interface[interfaz]



```
Router_A#sh ip ospf interface s1
Serial1 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0
  Process ID 100, Router ID 192.168.3.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.3.2
  Suppress hello for 0 neighbor(s)
Router_A#
```

7.6.9.4. El comando show ip ospf neighbor

Router#show ip ospf neighbor detail

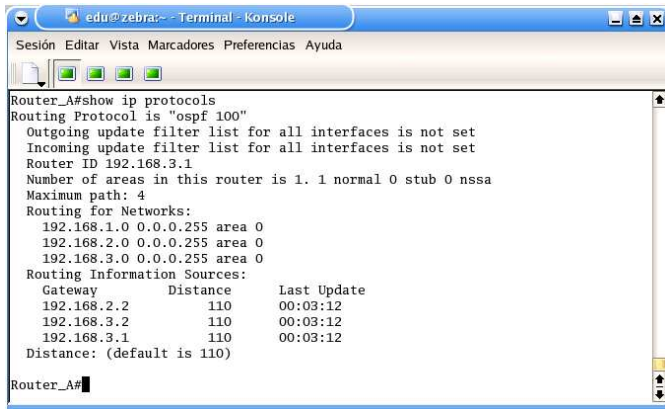


```
Neighbor 192.168.2.2, interface address 192.168.2.2
  In the area 0 via interface Serial0
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 0.0.0.0 BDR is 0.0.0.0
  Options is 0x42
  Dead timer due in 00:00:39
  Neighbor is up for 00:14:14
  Index 1/1, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 192.168.1.25, interface address 192.168.1.25
  In the area 0 via interface Ethernet0
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 192.168.1.1 BDR is 192.168.1.25
  Options is 0x2
  Dead timer due in 00:00:37
  Neighbor is up for 00:09:43
  Index 3/3, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
Router_A#
```

7.6. CONFIGURACIÓN DE OSPF EN TOPOLOGÍAS NBMA149

7.6.9.5. El comando show ip protocols

Router#show ip protocols



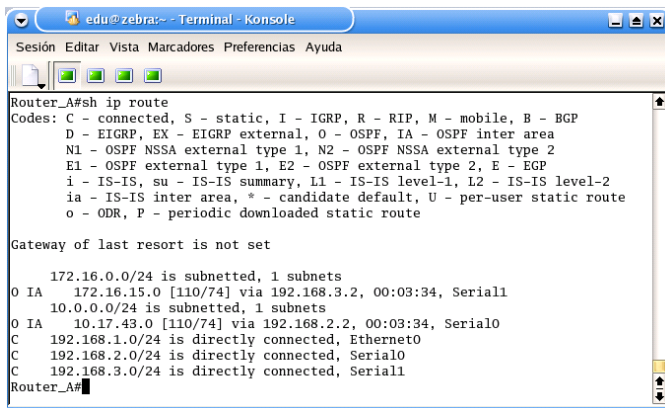
```
edu@zebra:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

Router_A#show ip protocols
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.3.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.2.0 0.0.0.255 area 0
    192.168.3.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2             110          00:03:12
    192.168.3.2             110          00:03:12
    192.168.3.1             110          00:03:12
  Distance: (default is 110)

Router_A#
```

7.6.9.6. El comando show ip route

Router#show ip route



```
edu@zebra:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

Router_A#sh ip route
Codes: C - connected, S - static, I - IGRP, 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, su - IS-IS summary, 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

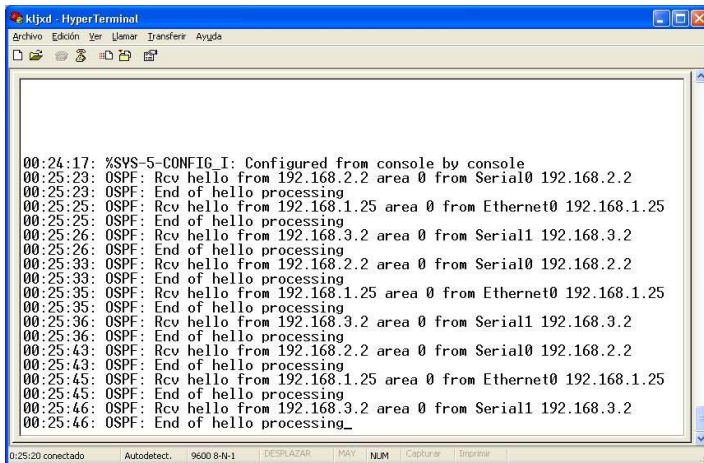
Gateway of last resort is not set

    172.16.0.0/24 is subnetted, 1 subnets
O IA   172.16.15.0 [110/74] via 192.168.3.2, 00:03:34, Serial1
    10.0.0/24 is subnetted, 1 subnets
O IA   10.17.43.0 [110/74] via 192.168.2.2, 00:03:34, Serial0
C       192.168.1.0/24 is directly connected, Ethernet0
C       192.168.2.0/24 is directly connected, Serial0
C       192.168.3.0/24 is directly connected, Serial1

Router_A#
```

7.6.9.7. Los comandos de debug

Router#debug ip ospf events



```

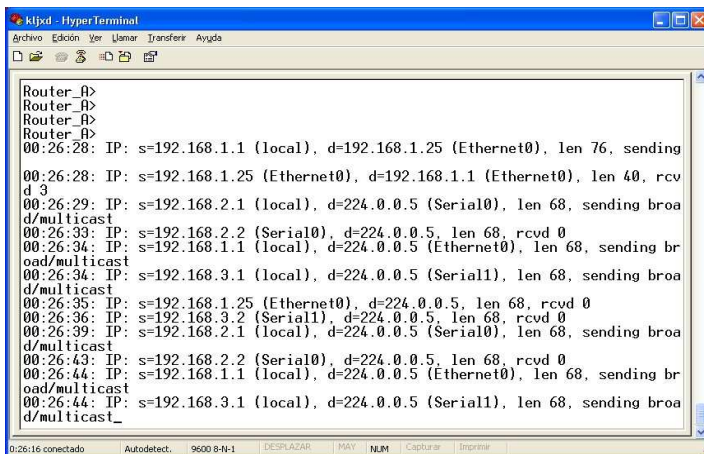
kljxd - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda

00:24:17: %SYS-5-CONFIG_I: Configured from console by console
00:25:23: OSPF: Rcv hello from 192.168.2.2 area 0 from Serial0 192.168.2.2
00:25:23: OSPF: End of hello processing
00:25:25: OSPF: Rcv hello from 192.168.1.25 area 0 from Ethernet0 192.168.1.25
00:25:25: OSPF: End of hello processing
00:25:26: OSPF: Rcv hello from 192.168.3.2 area 0 from Serial1 192.168.3.2
00:25:26: OSPF: End of hello processing
00:25:33: OSPF: Rcv hello from 192.168.2.2 area 0 from Serial0 192.168.2.2
00:25:33: OSPF: End of hello processing
00:25:35: OSPF: Rcv hello from 192.168.1.25 area 0 from Ethernet0 192.168.1.25
00:25:35: OSPF: End of hello processing
00:25:36: OSPF: Rcv hello from 192.168.3.2 area 0 from Serial1 192.168.3.2
00:25:36: OSPF: End of hello processing
00:25:43: OSPF: Rcv hello from 192.168.2.2 area 0 from Serial0 192.168.2.2
00:25:43: OSPF: End of hello processing
00:25:45: OSPF: Rcv hello from 192.168.1.25 area 0 from Ethernet0 192.168.1.25
00:25:45: OSPF: End of hello processing
00:25:46: OSPF: Rcv hello from 192.168.3.2 area 0 from Serial1 192.168.3.2
00:25:46: OSPF: End of hello processing_

0:25:20 conectado Autodetect. 9600 8-N-1 DESPLAZAR MAY NUM Capture Imprimir

```

Router#debug ip ospf packets



```

kljxd - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda

Router_0>
Router_0>
Router_0>
Router_0>
00:26:28: IP: s=192.168.1.1 (local), d=192.168.1.25 (Ethernet0), len 76, sending
00:26:28: IP: s=192.168.1.25 (Ethernet0), d=192.168.1.1 (Ethernet0), len 40, rcv
d 3
00:26:29: IP: s=192.168.2.1 (local), d=224.0.0.5 (Serial0), len 68, sending broa
d/multicast
00:26:33: IP: s=192.168.2.2 (Serial0), d=224.0.0.5, len 68, rcvd 0
00:26:34: IP: s=192.168.1.1 (local), d=224.0.0.5 (Ethernet0), len 68, sending br
oad/multicast
00:26:34: IP: s=192.168.3.1 (local), d=224.0.0.5 (Serial1), len 68, sending broa
d/multicast
00:26:35: IP: s=192.168.1.25 (Ethernet0), d=224.0.0.5, len 68, rcvd 0
00:26:36: IP: s=192.168.3.2 (Serial1), d=224.0.0.5, len 68, rcvd 0
00:26:39: IP: s=192.168.2.1 (local), d=224.0.0.5 (Serial0), len 68, sending broa
d/multicast
00:26:43: IP: s=192.168.2.2 (Serial0), d=224.0.0.5, len 68, rcvd 0
00:26:44: IP: s=192.168.1.1 (local), d=224.0.0.5 (Ethernet0), len 68, sending br
oad/multicast
00:26:44: IP: s=192.168.3.1 (local), d=224.0.0.5 (Serial1), len 68, sending broa
d/multicast_

0:26:16 conectado Autodetect. 9600 8-N-1 DESPLAZAR MAY NUM Capture Imprimir

```

Capítulo 8

OSPF en múltiples áreas

8.1. El propósito de OSPF en múltiples áreas

Múltiples áreas en OSPF proporcionan una de las principales características que distinguen los protocolos de vector distancia con OSPF (estado del enlace).

Un área de OSPF es una agrupación lógica de routers que ejecutan OSPF con una base de datos topológica idéntica.

Un área es una subdivisión del dominio de OSPF, a veces llamado sistema autónomo.

La división del sistema autónomo en áreas permite a los routers de cada área limitar el tamaño de sus bases de datos topológicas, sumarizar y asegurar la conectividad entre áreas y redes fuera del sistema autónomo.

8.1.1. Problemas con OSPF en un único área

Cuanto más grande es el área es más probable que haya que ejecutar el SPF, si la dividimos en diferentes áreas esta probabilidad baja.

Cuanto más grande es el área, más grande es la tabla de routing. Incrementan las necesidades de memoria y CPU para calcularla.

La base de datos topológica incrementa el tamaño y puede llegar a convertirse en inmanejable

8.1.2. Comandos relacionados

Para comprobar la utilización de CPU:

```
Router#show processes cpu
```

Para comprobar la utilización de memoria:

```
Router#show memory free
```

8.1.3. Cómo determinar los límites del área

Para determinar si es necesaria la utilización de varias áreas se tienen que cumplir las siguientes cuestiones:

El crecimiento de un único área se convierte en inmanejable.

El diseño con múltiples áreas pequeñas, para que en un futuro estas puedan ir creciendo cómodamente.

8.2. Características de múltiples áreas en OSPF

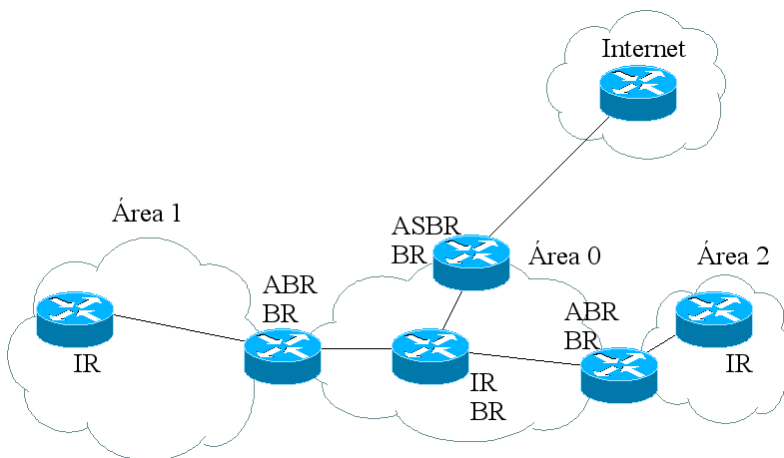
8.2.1. OSPF en un área

Uno de los puntos fuertes de OSPF es la capacidad de soportar grandes redes. Esto se consigue dividiendo la red en múltiples áreas.

8.2. CARACTERÍSTICAS DE MÚLTIPLES ÁREAS EN OSPF153

Sin embargo si mantenemos una gran red en un único área el proceso será intensivo de CPU y de memoria.

8.2.2. Tipos de routers



- **Internal Router (IR):** Es responsable de mantener la base de datos del área actualizada y optimizada de cada subred del área. Todos sus interfaces se encuentran en el mismo área. El otro router que funciona en un único área es el ASBR.
- **Backbone Router (BR):** OSPF requiere que todas las áreas estén conectadas al área 0 o de backbone. Un router en este área es un BR. En un Área 0 también pueden estar IR, ABR y ASBR.
- **Area Border Router (ABR):** Este router es el responsable de unir varias áreas. Mantiene una base de datos topológica de cada área. Realiza la sumarización del área y es el responsable de reenviar los LSAs entre áreas.

- **Autonomous System Boundary Router (ASBR):** Es el responsable de conectar la red OSPF con una red externa con un protocolo EGP.

8.2.2.1. Link-State Advertisements (LSAs)

- **Router Link LSA:** LSA generado para cada área a la que el router pertenece. Este LSA da información de los enlaces dentro del área. Se inunda por el área. Es conocido como LSA de tipo 1.
- **Network Link LSA:** LSA generado por un DR y dirigido a los routers del área. También conocido como LSA de tipo 2.
- **Network Summary Link LSA:** LSA enviado entre áreas que resume las redes IP. Son generados por los ABR. También conocidos como LSA de tipo 3.
- **AS external ASBR Summary Link LSA:** LSA enviado a un ASBR por un ABR. El LSA contiene la métrica del ABR al ASBR. También conocidos LSA de tipo 4.
- **External Link LSA:** LSA generado por el ASBR que es inundado por el AS. Cada LSA de este tipo describe la ruta a un destino fuera del AS. Las rutas por defecto del AS también son descritas como External Link LSA. También conocidos como LSA de tipo 5.
- **NSSA External LSA:** Son creados por los ASBR cuando residen en áreas NSSA. Similares a los LSA de tipo 5, excepto porque estos LSA se generan desde un área NSSA y no pueden ser propagados, entonces el ABR lo transformará en LSA de tipo 5.

8.2.3. Tipos de áreas OSPF

- **Área Estándar:** Este tipo de área se conecta a la de backbone o Área 0. Todos los routers del área conocen los demás routers

del área y tiene la misma base de datos topológica. Sin embargo cada router tiene su propia tabla de routing.

- **Área Stub:** Este tipo de áreas no acepta LSAs de tipo 5. Sólo existe una forma de ver fuera el AS es mediante una ruta por defecto. Suele ser una topología hub-and-spoke.
- **Área Totally Stub:** Este tipo de áreas no acepta LSAs de tipo 3, 4 y 5. La única forma de salir del área es mediante una ruta por defecto. Este tipo de área es muy útil para sitios remotos con pocas redes y conectividad limitada con el resto de la empresa. Esta es una solución propietaria de Cisco Systems.
- **Área NSSA:** Este tipo de áreas se suelen utilizar para conectar a un ISP o cuando se requiere una redistribución. No se permiten LSAs de tipo 4 y 5. NSSA se ven como áreas stub, pero que pueden recibir rutas externas, pero que no pueden propagarlas hacia el área de backbone y por tanto al resto del dominio de OSPF. En estas áreas se crean los LSA de tipo 7 que son transformados a LSA de tipo 5 por el ABR del NSSA, de esta forma se puede propagar al resto del dominio OSPF. Las áreas NSSA se diseñaron como áreas stub especiales para aplicaciones como en un área con pocas áreas stub pero inteconectadas con un router ejecutando RIP, o como área con su propia conexión a Internet.
- **Área de Backbone:** Conocida como Área 0, interconecta todas las demás áreas. No puede propagar LSA de tipo 7, estos son traducidos a LSA de tipo 5 por el ABR.

8.2.4. Restricciones de las áreas totally stub

Las áreas Totally Stub tienen unas características que las diferencian del resto y que tenemos que tener muy en cuenta cuando trabajemos con ellas.

- No están permitidas las rutas externas.

- No están permitidos los virtual-links.
- No se permite la redistribución.
- No están permitidos los router ASBR.
- Este tipo de área no puede ser área de backbone.
- Todos los routers están configurados como routers stub.

8.3. Operación de OSPF en múltiples áreas

8.3.1. Propagación de LSAs por los ABR y los ASBR

Un ABR genera LSAs sumariadas y las inunda por el área de backbone.

Las rutas generadas internamente son de Tipo 1 y 2.

Las rutas inyectadas son de Tipo 3.

Las rutas de Tipo 3 ó 4 son recibidas desde el área 0 y reenviadas al área por el ABR.

Ciertas condiciones tienen que existir antes de que los LSAs sean inundados por los interfaces.

- El LSA no se haya recibido por ese interfaz.
- El interfaz esté en estado exchange o full adjacency.
- El interfaz no esté conectado a un área Stub. (LSA Tipo 5 no se propagarán).
- El interfaz no esté conectado aun área totally stubby (LSAs Tipo 3,4 ó 5 no se propagarán).

8.3.2. Sección del camino OSPF entre Áreas

La tabla de routing que existe en un router depende de los siguientes factores:

- La posición del router en el área y el estado de la red.
- El tipo de área en la que el router está localizado.
- Si existen múltiples áreas en el dominio.
- Si existe comunicación fuera del AS.

8.3.3. Procesamiento de LSAs

Hay que recordar que cuando el router recibe un LSA construye la base de datos topológica, entonces ejecuta el algoritmo de Dijkstra, obtiene el árbol SPF y genera la tabla de routing.

Los diferentes LSA tienen pesos diferentes en el proceso de selección. Es preferible utilizar una ruta interna a una remota, además de esta forma nos ahorramos la posibilidad de crear bucles innecesarios en la red.

El Router va a procesar los LSAs según este orden:

- LSAs internos (Tipos 1 y 2).
- LSAs del AS (Tipos 3 y 4), si existe una ruta más cercana utilizaremos los LSAs de tipo 1 y 2.
- LSAs externos de Tipo 7.

8.3.4. Calculando el coste del camino a otro área

El camino a otras áreas se calcula como el más corto al ABR, añadido al coste del backbone.

Las rutas externas son rutas pasadas entre los routers del dominio de OSPF y el router en otro AS o dominio. Estas rutas se calculan de dos formas:

- E1: El coste del camino al ASBR es añadido al coste externo.
- E2: El coste externo es el coste desde el ASBR al extremo.

Si disponemos de rutas E1 y E2, por defecto se prefiere E1.

8.3.5. Códigos asociados en la tabla de routing a los LSAs

| Tipo de LSA | Entrada en la Tabla de Routing |
|-------------|--------------------------------|
| 1 | O |
| 2 | O |
| 3 ó 4 | O IA |
| 5 | O E1 u O E2 |

8.3.6. Consideraciones de diseño en múltiples áreas OSPF

Las principal consideración de diseño en OSPF consiste en dividir la red en áreas. Esto es muy importante ya que afecta a cómo se va a decidir el esquema de direccionamiento IP.

OSPF funciona mejor con direccionamiento jerárquico, en el cual el movimiento de datos de un área a otra compromete únicamente a una subred específica. Es muy importante la sumarización.

Hay que tener en cuenta la utilización de recursos.

En un buen diseño de red hay que tener previsto la posibilidad de transiciones o cortes en la red (virtual-links).

Es muy importante también especificar el tipo de topología a utilizar, ya que no todas funcionan igual.

También es importante recordar que el tráfico generado por un área será diseminado por el área 0.

Los virtual-links permiten a redes no conectadas directamente funcionar en el dominio de OSPF.

8.3.7. Planificando la Capacidad en OSPF

Las recomendaciones “ideales” de Cisco son:

- 50 Routers por Área.
- 60 Vecinos por Router.
- 3 Áreas por Router.
- Un router no debe ser DR ni BDR para más de un área.

Sin embargo estas normas no son tajantes, ya que depende de las características de cada router y del área en el cual esté ese router trabajando.

Número de Vecinos por Router:

- Incrementar el número de vecinos incrementa el consumo de recursos que el router.

Número de Áreas por ABR:

- Para cada área a la cual está conectado el ABR debe de tener una base de datos topológica, lo cual incrementa la necesidad de CPU y memoria.

No es lo mismo ejecutar OSPF en un 2600 que en un 7600.

Varios de los factores que influyen en el número de router por área incluyen los siguientes:

- Qué tipo de área es (stub, totally stub, backbone).
- Qué necesidad de cómputo existe.
- Qué tipo de medio hay.
- Cómo de estable es la red.
- El área está en una NBMA o en una totalmente mallada.

- La red tiene conexiones externas.
- Existe un diseño jerárquico con sumarización.

La memoria recomendada es:

- Si la tabla tiene menos de 500 kb en una RAM de 2 a 4 Mb.
- Si la tabla tiene más de 500 kb en una RAM 8, 16, 32 o 64 Mb.

8.3.8. Sumarización

Uno de los puntos fuertes de OSPF es su escalabilidad.

En OSPF disponemos de dos tipos de sumarización:

- Sumarización Interárea: La proporciona el ABR y crea LSAs de tipo 3 y tipo 4.
- Sumarización Externa: La proporciona el ASBR y crea LSA de tipo 5.

Por supuesto ambas sumarizaciones pueden suceder si se ha realizado un esquema de direccionamiento correcto.

8.3.9. El virtual-link

Para conectar un área que no está directamente conectada al área 0 se crea un túnel al ABR, de forma que desde el punto de vista de OSPF existe una conexión directa.

Esta situación puede ocurrir en los siguientes casos:

- No existe conexión física al área 0 (p.e. Fusión empresarial o fallo en red).
- Existen dos áreas 0, entonces las conectaremos con otro área. (p.e. Fusión empresarial).

- El área es crucial para la empresa y tiene una conexión de backup para redundancia.

El dictado principal de OSPF es que si existen múltiples áreas, estas deben conectarse al backbone directamente, mediante un ABR, el cual reside en las dos áreas.

Sin embargo para los caso en los que esto no pueda suceder OSPF tiene una solución llamada virtual-link.

No es recomendado utilizar virtual-link de forma predeterminada aunque sea una solución muy potente. Además, antes de crear un virtual-link debemos observar lo siguiente:

- Ambos routers deben compartir el mismo área.
- Las áreas que conectan no pueden ser áreas stub.
- Uno de los routers tiene que estar conectado al área 0.

8.3.10. Múltiples áreas sobre redes NBMA

Existen dos consideraciones de diseño para las redes NBMA como parte del dominio de OSPF:

- Red NBMA definida como área 0: Es utilizada para conectar a todos los sitios remotos, entonces todo el tráfico atravesará la red. Esto funcionará bien siempre que la topología de la red NBMA sea totalmente mallada.
- Red hub-and-spoke como área 0: Se mantendrá un tráfico mínimo en el área 0, pero no en el router central, dependiendo del tamaño de la red, en las áreas podemos utilizar redes NBMA.

8.4. Configuración en OSPF multiárea

8.4.1. Comandos de configuración requerida para redes OSPF multiárea

Antes de empezar a trabajar con OSPF lo primero que debemos que hacer es conocer el funcionamiento.

Prerequisitos:

- Interfaces del router participantes: Es importante identificar los interfaces que van a participar dentro del dominio de OSPF.
- Identificación del área: Es imprescindible identificar el área en la cual participa cada interfaz.
- Router ID: Este es el identificador único del router.
- Comando de OSPF `router ospf`.
- Comando de OSPF `network`.

8.4.2. Habilitando el protocolo de routing OSPF

Cuando se configura por primera vez un router no se encuentra configurado el protocolo de routing:

```
Router(config)#router ospf ID-Proceso
```

Tenemos que tener en cuenta que el número del proceso es de significancia local, es decir, podemos tener varios procesos en el router, y cada router puede ejecutar procesos distintos, aunque se suele configurar el mismo número de proceso por coherencia en el diseño.

8.4.3. Habilitando el comando `network`

El comando `network` habilita el OSPF en un interfaz concreto y lo asocia a un área:

```
Router(config-router)#network red wildcard area
                             número-de-área
```

Este comando es un prerequisite ya que es el responsable de establecer la pertenencia a las áreas por parte de los interfaces de los routers.

8.5. Configuración opcional de OSPF multiárea

Comandos opcionales de OSPF significa que sin estos comandos OSPF va a funcionar de forma eficiente, pero que con estos comandos se consigue aumentar las cualidades de mantenimiento de una red eficiente.

- Comando `area range`: Configurado en el ABR.
- Comando `summary-address`: Configurado en el ASBR.
- Comando `area [ID-área] stub`: Comando para definir el área Stub.
- Comando `area [ID-área] stub no-summary`: Comando para definir el área Totally Stubby.
- Comando `area default-cost`: Comando para determinar el coste de las rutas por defecto que entran en el área.
- Comando `area virtual-link`: Comando utilizado para crear un virtual-link.

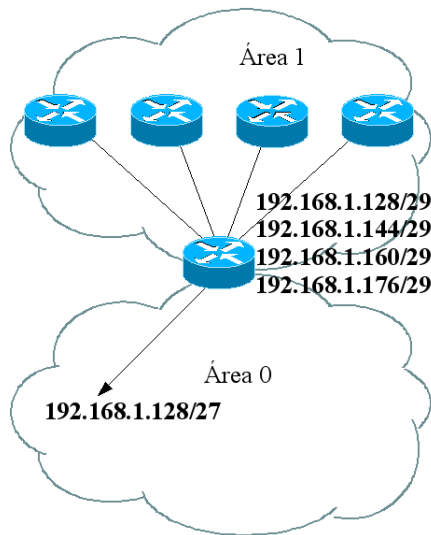
8.5.1. Comando area range

El comando `area range` se configura en el ABR ya que este es el router que controla las redes que son anunciadas en el área.

El comando `area` con la palabra clave `range` consolida y resume las rutas en el borde del área. Esto reduce el tamaño de las bases de datos y es muy útil sobre todo en el área de backbone.

```
Router(config-router)#area área-id range dirección  
                               máscara
```

8.5.1.1. Ejemplo de comando area range



```
Router(config-router)#network 192.168.1.128 0.0.0.7 area 1  
Router(config-router)#network 192.168.1.144 0.0.0.7 area 1
```

8.5. CONFIGURACIÓN OPCIONAL DE OSPF MULTIÁREA165

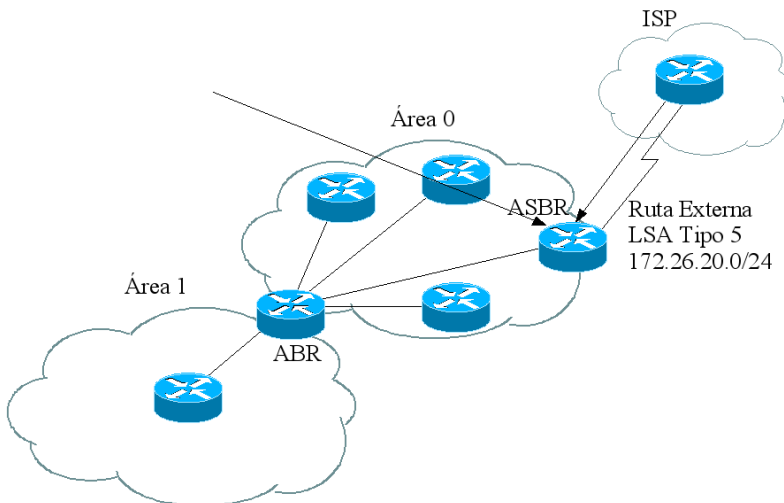
```
Router(config-router)#network 192.168.1.160 0.0.0.7 area 1
Router(config-router)#network 192.168.1.176 0.0.0.7 area 1
[...]
Router(config-router)#area 1 range 192.168.1.128
255.255.255.192
[...]
```

8.5.2. Comando summary-address

El comando `summary-address` es utilizado en el ASBR para sumarizar las redes que son anunciadas desde fuera del AS. Estas rutas son redistribuidas dentro del dominio de OSPF desde otros protocolos de routing:

```
Router(config-router)# summary-address dirección
máscara [not-advertise] [tag etiqueta]
```

8.5.2.1. Ejemplo del comando summary-address



```
Router(config)#router ospf 100
Router(config-router)#network 172.26.20.4 0.0.0.3
    area 0
Router(config-router)#summary-address 172.26.20.0
    255.255.255.0
```

8.5.3. El comando area area-id stub

Una vez diseñado el esquema de direccionamiento es necesario determinar los candidatos para áreas stub, totally stubby y NSSA.

La sintaxis para configurar un área como stub:

```
Router(config-router)#area área-id stub
```

Todos los routers dentro del área stub de OSPF deben estar configurados como routers stub para que puedan empezar a intercambiar paquetes Hello.

Para indicar que el interfaz pertenece a un área stub se utiliza un flag en el paquete Hello llamado E que se pone a 0. Todos los routers de este área tienen que estar de acuerdo en este flag.

Las áreas stub no aceptan LSAs de tipo 5.

8.5.3.1. Ejemplo de configuración

```
Router(config)#router ospf 100
Router(config-router)#network 172.16.20.128 0.0.0.7
    area 0
Router(config-router)#network 172.16.20.8 0.0.0.7
    area 0
Router(config-router)#area 0 range 172.168.20.128
    255.255.255.192
Router(config-router)#area 1 stub
```

8.5.4. El comando `area area-id stub no-summary`

La sintaxis para este tipo de áreas es:

```
Router(config-router)#area area-id stub no-summary
```

En este tipo de áreas el ABR no envía actualizaciones sumarizadas desde otras áreas al área.

Este comando se configura en el ABR.

Este comando sólo puede ser configurado en routers Cisco ya que es una solución propietaria.

Las demás rutas son configuradas como áreas internas del área stub.

En este tipo de áreas las rutas externas no son propagadas dentro del área.

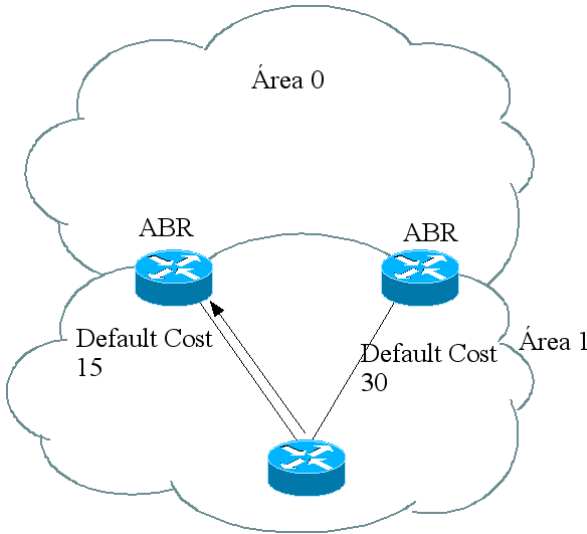
8.5.5. El comando `area default cost`

La sintaxis de este comando es:

```
Router(config-router)#area area-id default-cost coste
```

Para definir el coste de la ruta por defecto utilizaremos este comando.

El ABR conectado al área stub automáticamente genera y anuncia una ruta por defecto con destino 0.0.0.0 en el área stub.



Este comando es muy útil cuando el stub área tiene más de un ABR, entonces definiremos costes distintos para decidir el ABR por el cual queremos salir.

8.5.6. El comando `area virtual-link`

La sintaxis de este comando es:

```
Router(config-router)#area área-id virtual-link  
                        router-id
```

Donde *área-id* es el ID asignado al área de tránsito para el virtual-link y donde *router-id* es el ID del router vecino del virtual-link.

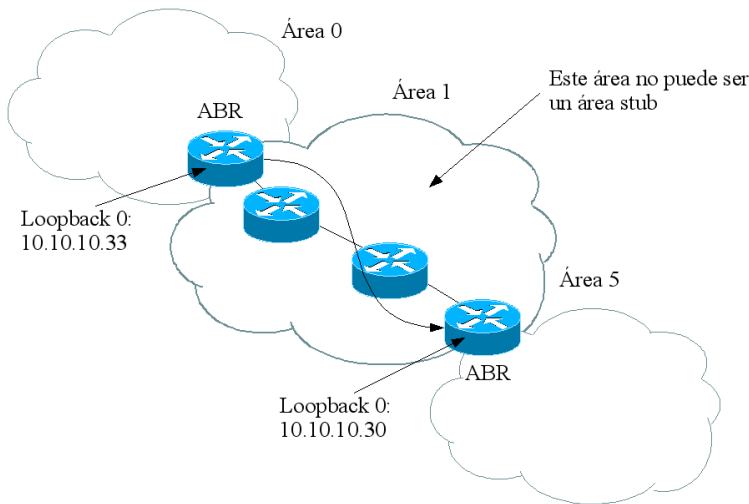
Para definir el coste de la ruta por defecto utilizaremos este comando.

Cuando no es posible conectar un área al área 0 directamente, existe una solución consistente en crear un túnel llamado virtual-link.

8.5. CONFIGURACIÓN OPCIONAL DE OSPF MULTIÁREA169

El comando `area virtual-link` se configura entre los ABRs que comparten un área común, al menos uno de los ABRs tiene que estar en el área 0.

El comando debe configurarse en ambos routers.



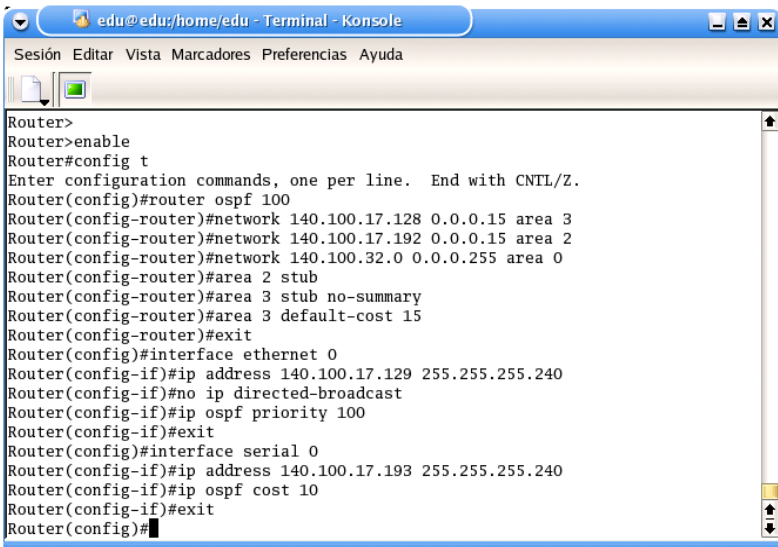
```
edu@edu:/home/edu - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface loopback 0
Router(config-if)#ip address 10.10.10.33 255.255.255.255
Router(config-if)#exit
Router(config)#router ospf 100
Router(config-router)#network 172.15.20.128 0.0.0.7 area 0
Router(config-router)#network 10.10.10.33 0.0.0.0 area 0
Router(config-router)#area 0 range 172.16.20.128 255.255.255.192
Router(config-router)#area 1 default-cost 15
Router(config-router)#area 1 virtual-link 10.10.10.30
Router(config-router)#
```

Es importante observar que en el comando `area 1 virtual-link 10.10.10.30` hace referencia al vecino, y en el vecino tendremos configurado `area 1 virtual-link 10.10.10.33`.

8.5.7. Configuración funcional de OSPF multi-área

En el ejemplo de la ilustración se puede observar una configuración funcional de OSPF multiárea.

A screenshot of a terminal window titled "edu@edu:/home/edu - Terminal - Konsole". The window has a menu bar with "Sesión", "Editar", "Vista", "Marcadores", "Preferencias", and "Ayuda". Below the menu bar is a toolbar with icons for file operations. The terminal displays the following commands and their outputs:

```
Router>
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 100
Router(config-router)#network 140.100.17.128 0.0.0.15 area 3
Router(config-router)#network 140.100.17.192 0.0.0.15 area 2
Router(config-router)#network 140.100.32.0 0.0.0.255 area 0
Router(config-router)#area 2 stub
Router(config-router)#area 3 stub no-summary
Router(config-router)#area 3 default-cost 15
Router(config-router)#exit
Router(config)#interface ethernet 0
Router(config-if)#ip address 140.100.17.129 255.255.255.240
Router(config-if)#no ip directed-broadcast
Router(config-if)#ip ospf priority 100
Router(config-if)#exit
Router(config)#interface serial 0
Router(config-if)#ip address 140.100.17.193 255.255.255.240
Router(config-if)#ip ospf cost 10
Router(config-if)#exit
Router(config)#
```

El comando `no ip directed-broadcast` sirve para enviar broadcast como mensajes unicast, con lo cual es interesante desactivar esta característica si es posible.

8.6. Verificación OSPF multiárea

Esta sección se refiere a los comandos show utilizados en una Red OSPF Multiárea:

Los siguientes comandos se pueden utilizar en conjunción con los comandos de área única para verificar la operación de OSPF en un área multiárea:

- Comando show ip ospf border-routers.
- Comando show ip route.
- Comando show ip ospf database.
- Comando show ip ospf virtual-circuits.

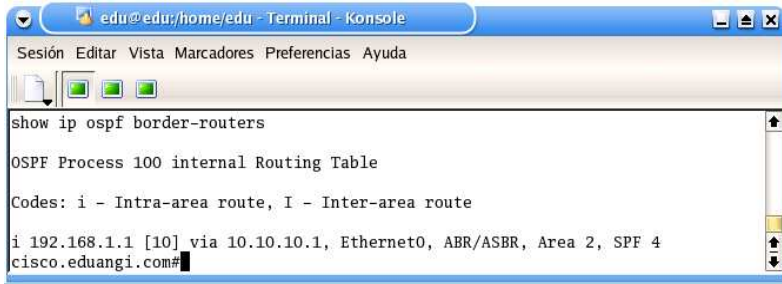
Hay que recordar que los comandos utilizados en un único área son:

- show ip ospf.
- show ip ospf database.
- show ip ospf neighbor.
- show ip protocols.
- show ip route.

8.6.1. Comando show ip ospf border-routers

La sintaxis del comando es:

```
Router#show ip ospf border-routers
```



```
edu@edu:/home/edu - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
show ip ospf border-routers
OSPF Process 100 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 192.168.1.1 [10] via 10.10.10.1, Ethernet0, ABR/ASBR, Area 2, SPF 4
cisco.eduangi.com#
```

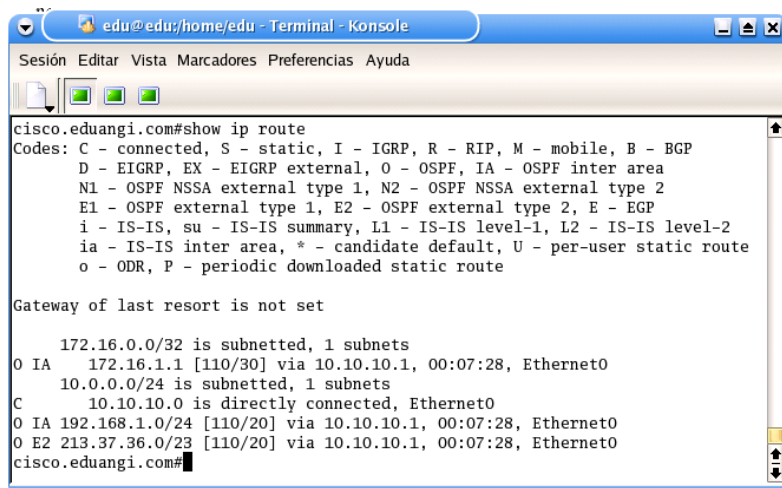
Este comando muestra los ABRs y los ASBRs para los cuales el IR tiene entradas en su tabla de routing.

Este comando es estupendo para detectar errores en la configuración y entender como la red comunica sus rutas.

8.6.2. Comando show ip route

La sintaxis del comando es:

```
Router#show ip route
```



```

edu@edu:/home/edu - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

cisco.eduangi.com#show ip route
Codes: C - connected, S - static, I - IGRP, 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, su - IS-IS summary, 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

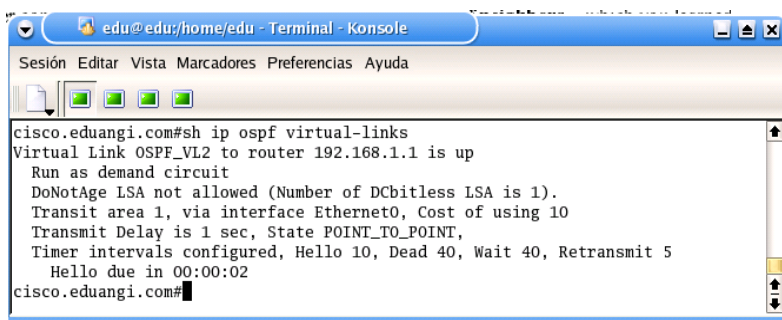
    172.16.0.0/32 is subnetted, 1 subnets
O IA   172.16.1.1 [110/30] via 10.10.10.1, 00:07:28, Ethernet0
    10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Ethernet0
O IA   192.168.1.0/24 [110/20] via 10.10.10.1, 00:07:28, Ethernet0
O E2   213.37.36.0/23 [110/20] via 10.10.10.1, 00:07:28, Ethernet0
cisco.eduangi.com#

```

8.6.3. Comando show ip ospf virtual-link

La sintaxis del comando es:

```
Router#show ip ospf virtual-link
```



```

edu@edu:/home/edu - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

cisco.eduangi.com#sh ip ospf virtual-links
Virtual Link OSPF_VL2 to router 192.168.1.1 is up
  Run as demand circuit
  DoNotAge LSA not allowed (Number of DCbitless LSA is 1).
  Transit area 1, via interface Ethernet0, Cost of using 10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
cisco.eduangi.com#

```

Es comando es útil utilizarlo en conjunción con el comando show ip ospf neighbors.

Este comando nos indica:

- El ID del router final del virtual-link.
- El área de transito.
- A través de qué interfaz se conecta.
- El coste.
- El tiempo que tarda en transmitir LSA (Delay).
- El Estado del router remoto, qué tipo de router es, DROTHER significa que no es ni DR ni BDR.
- Los tiempos de Hello y Dead.
- El tiempo que esperará una respuesta antes de retransmitir el LSA (Retransmit).
- El tipo de Adyacencia:

```
Router#show ip ospf database [router | network | summary | asbr-s
```

8.6.4. Comando show ip ospf database

La sintaxis del comando es:

```
Router#show ip ospf database [router | network |  
    summary | asbr-summary | nssa-external | external |  
    database-summary]
```

Este comando muestra todas las entradas en la base de datos de estado del enlace e información recibida por los LSAs.

Este comando se puede utilizar en conjunción con `show ip ospf neighbors`.

```

edu@edu:/home/edu - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

cisco.eduangi.com#show ip ospf database

        OSPF Router with ID (172.16.1.1) (Process ID 100)

        Router Link States (Area 0)

Link ID        ADV Router    Age          Seq#           Checksum Link count
172.16.1.1     172.16.1.1   216          0x80000001    0x00665E 0

        Summary Net Link States (Area 0)

Link ID        ADV Router    Age          Seq#           Checksum
10.10.10.0     172.16.1.1   216          0x80000001    0x00E471

        Summary ASB Link States (Area 0)

Link ID        ADV Router    Age          Seq#           Checksum
172.16.1.1     172.16.1.1   216          0x80000001    0x0023BB

        Router Link States (Area 1)

Link ID        ADV Router    Age          Seq#           Checksum Link count
10.10.10.1     10.10.10.1   1255         0x80000002    0x0004E7 1
172.16.1.1     172.16.1.1   216          0x80000005    0x00CF98 1
--More--
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 2.00.0 | VT102 | Desconectado

```

Este comando nos muestra:

- **LINK ID:** ID del router.Verificación OSPF Multiárea.
- **ADV Router:** ID del router que anuncia la ruta.
- **Age:** Edad del estado del enlace.
- **Seq#:** Número de secuencia del LSA, para detectar LSAs antiguos.
- **Checksum:** Suma de comprobación del LSA.
- **Link count:** Número de interfaces detectados por router.

8.7. Troubleshooting OSPF multiárea

El troubleshooting de OSPF a través de múltiples áreas es obviamente más complicado que el troubleshooting en un único área. Es necesario seguir las siguientes pautas para poder desarrollar el troubleshooting de la mejor forma:

- Mantener los mapas de topología de la red claros.
- Disponer de copias recientes de las configuraciones de todos los routers.
- Documentar todos los cambios que puedan suceder en la red.

Esta sección cubre el comando `log-adjacency-changes` y varios de los comandos de debug.

8.7.1. Comando `log-adjacency-changes`

Este comando tiene una función similar a los comandos de debug, pero requiere menos recursos.

Los comandos de debug proporcionan mucha más información, pero es posible sobrecargar los buffers de los routers.

Sintaxis:

```
Router(config-ospf)#log-adjacency-changes
```

8.7.2. Comandos comunes de debug

Los comandos de debug se utilizan para conseguir información adicional en la consola, es importante recordar que estos comandos se introducen en modo privilegiado.

Los comandos de debug más importantes son:

8.7.2.1. Comando debug ip packet.

Este comando es útil para analizar los mensajes que están viajando entre los hosts local y remoto. Entre la información que proporciona el debug se incluyen los paquetes recibidos, generados y reenviados.

8.7.2.2. Comando debug ip ospf events.

Este comando muestra información relativa a eventos OSPF, así como adyacencias, información de inundación, selección del DR, y cálculo del SPF.

8.7.3. Problemas comunes de las adyacencias

Muchos problemas de adyacencias se basan en discrepancias con los vecinos.

Si al configurar OSPF no se ven los vecinos se pueden realizar los siguientes pasos:

- Comprobar que ambos routers tienen la misma máscara IP, MTU, temporizador de Hello en el interfaz, temporizador de Hello de OSPF, intervalo dead de OSPF.
- Comprobar que ambos extremos pertenecen a la misma área.
- Utilizar comandos debug y show para ampliar información sobre el problema.

Capítulo 9

Fundamentos de IS-IS

9.1. Introducción a IS-IS

IS-IS es un protocolo IGP desarrollado por DEC, y suscrito por la ISO en los años 80 como protocolo de routing para OSI.

El desarrollo de IS-IS fue motivado por la necesidad de:

- Protocolo no propietario.
- Esquema de direccionamiento grande.
- Esquema de direccionamiento jerárquico.
- Protocolo eficiente, permitiendo una convergencia rápida y precisa y poca sobrecarga en la red.

IS-IS es utilizado por el gobierno de los EEUU y actualmente está emergiendo.

El nuevo interés se basa en que IS-IS es un estándar que proporciona independencia del protocolo, capacidad de escalado y capacidad de definir routing basado en ToS.

9.1.1. Terminología de IS-IS

- **Adyacencia:** Información de routing local que muestra la alcanzabilidad de los ES e IS conectados directamente. Una adyacencia separada se crea para cada vecino en un circuito, y por cada nivel de routing en un circuito de broadcast.
- **Dominio Administrativo:** Conjunto de routers que comparten el mismo protocolo de routing en una organización.
- **Área:** Subdominio en un Dominio Administrativo. Los routers en el área mantienen información de routing detallada de la composición interna del área. Los routers también mantienen información de routing que les permite alcanzar otras áreas. Las direcciones de las áreas están contenidas en las direcciones NET y NSAP.
- **Circuito:** Información de routing local para una Single subNet Point of Attachment (SNPA).
- **Code/Lengh/Value (CLV):** Direccionamiento OSI para IS-IS. Estos son los campos variables en la PDU. El campo code especifica la información en el campo Content como un número. El campo Lengh determina el tamaño del campo Value. El campo Value contiene la información.
- **Complete Secuence Number Packet (CSNP):** CSNP describe cada enlace en la BD de estado del enlace. Los CSNP se envían en enlaces punto a punto cuando el enlace se levanta para sincronizar las BD de estado del enlace. El Router Designado (DR), o el Sistema Intermedio Designado (DIS), en redes multicast envían el CSNP cada 10 segundos.
- **ConnectionLess Network Protocol (CLNP):** Protocolo utilizado por OSI para transportar datos e indicación de errores en el nivel de red. CLNP es similar a IP y no proporciona detección de errores en la transmisión de datos, delega en el nivel transporte esta función.

- **ConnectionLess Network Service (CLNS):** CLNS utiliza un servicio de datagramas para transportar la información y no requiere que el circuito haya sido establecido antes de transmitir. Mientras que CLNP define el protocolo actual, CLNS describe el servicio no orientado a la conexión proporcionado para el nivel de transporte.
- **Designated Intermediate System (DIS):** El router (IS) en una LAN que es designado para otras tareas. En particular, el DIS genera PDUs de estado del enlace en nombre de la LAN, tratándola como si fuera un pseudonodo.
- **Dual IS-IS:** IS-IS soporta routing OSI e IP. Las áreas en el AS pueden ejecutar OSI, IP, o ambos. Sin embargo la configuración escogida debe de ser consistente en toda la red.
- **End System (ES):** El host, el cual tiene capacidades de routing limitadas. El ES tiene un protocolo de nivel 3 OSI o IP ejecutándose y puede enviar y recibir información.
- **End System-to-Intermediate System (ES-IS):** Protocolo con el cual los OSI ES se comunican con los IS para aprender dinámicamente las adyacencias de Nivel 2.
- **Hello:** Los paquetes Hello son utilizados para descubrir y mantener las adyacencias.
- **Dirección de Host:** Subconjunto de dirección NET, que incluye dominio, área y system ID.
- **IS-IS:** Otro término utilizado para Dual IS-IS. Indica que IS-IS puede ser utilizado para soportar protocolos de routing de IP y CLNP en la red de forma simultánea.
- **Intermediate System (IS):** Un router. El IS es un dispositivo capaz de direccionar tráfico a destinos remotos.
- **Intermediate System-to-Intermediate System (IS-IS):** Protocolo de routing OSI que aprende la localización de las redes en el AS para poder realizar el reenvío de información.

- **Dominio IS-IS:** Grupo de routers ejecutando IS-IS para intercambiar información de routing.
- **Nivel 1 – Level 1(L1):** Estos routers son internos al área, lo cual significa que sólo reciben información de routing de su área y no tienen conocimiento de las demás áreas de la red. Para comunicarse con otras áreas los Routers L1 tiene que tener una ruta por defecto al Router L2 más cercano.
- **Nivel 1-2 – Level 1-2(L1-2):** Routers que conectan áreas. Estos routers conectan áreas L1 con el backbone L2. Tienen una tabla de routing L1 para enrutar los ES e IS en su propio área con el system ID. Mantienen una tabla de prefijos L2 de rutas a otras áreas.
- **Nivel 2 – Level 2(L2):** Estos routers están conectados sólo al backbone y proporcionan tráfico de tránsito entre áreas.
- **Enlace – Link:** Conexión física a un vecino. Este enlace es transmitido a todos los demás routers del área via LSP.
- **Link State Packet (LSP):** Paquete que describe los enlaces de los routers. Existen LSPs separados de nivel 1 y de nivel 2.
- **Vecino:** Un router en el mismo enlace con el cual se ha formado una adyacencia y se intercambia información de routing.
- **Network Entity Tittle (NET):** Parte de la dirección OSI. NET describe el área y el system ID del sistema en una red IS-IS, pero excluye el NSEL, el cual define la dirección NSAP del sistema.
- **Network Protocol Data Unit (NPDU):** Igual que PDU – Protocol Data Unit.
- **Network SElector (NSEL):** También referido como el campo SEL. Este campo describe el servicio en el nivel de red para cada paquete a enviar. NSEL es similar al campo protocolo de IP.

- **Network Service Access Point (NSAP):** Describe un servicio en el nivel de red al cual se tienen que enviar los paquetes. El NSAP es la dirección NET con el campo SET fiado a un valor distinto a 0x00.
- **Bit Overload (OL):** El OL se configura en el LSP si el router no puede almacenar la BD de estado del enlace completa. Los otros routers no enviarán ningún tráfico de tránsito por miedo a que su tabla de routing esté incompleta. (Se pueden producir bucles)
- **Partial Sequence Number Packet (PSNP):** Los PSNP se envían en enlaces punto a punto para realizar un ACK explícito de cada LSP que recibe el router. Un router en una subred de broadcast envía una petición PSNP solicitando el LSP necesita sincronizar su BD de estado del enlace.
- **Protocol Data Unit (PDU):** Unidad de datos pasada de un nivel del modelo OSI al mismo nivel del modelo OSI en otro nodo. En el nivel de red tendremos NPDU y en el nivel de enlace tendremos DLPDU.
- **Pseudonode:** El identificador de LAN para subredes de broadcast. El pseudonode hace que el medio de broadcast aparezca como un router virtual y que los routers aparezcan como interfaces conectados. Los routers mantienen adyacencias con el pseudonode, las cuales son gestionadas por el DIS.
- **Routing Domain:** Es lo mismo que el Dominio Administrativo. Define los límites del AS.
- **Sequence Number PDU (SNP):** Los SNPs se utilizan para aceptar la recepción de LSPs y sincronizar las BD del enlace.
- **Subnetwork:** El nivel de enlace de datos.
- **Subnetwork Dependent Layer:** Este subnivel transmite y recibe PDUs de la Subnetwork, traduce los DLPDU a NPDU,

y los maneja con el proceso OSI apropiado. El Subnetwork Dependent Layer también es responsable de crear y mantener las adyacencias a través del intercambio de PDUs Hello de IS-IS.

- **Subnetwork Independent Layer:** Describe como CLNS crea y mantiene el conocimiento de la red intercambiando y procesando información de routing, para que la información pueda ser transmitida al destino remoto y manejada por el nivel de transporte.
- **Subnetwork Point of Attachment (SNPA):** El SNPA se refiere a los servicios ofrecidos por el nivel de enlace al nivel físico y al de red. La dirección SNPA es la dirección física.
- **Type/Lenght/Value (TLV):** Es lo mismo que CLV.

9.2. Comparativa con OSPF

9.2.1. Similitudes de OSPF con IS-IS

Ambos son protocolos de routing de estado del enlace.

Ambos están basados en el algoritmo SPF basado a su vez en el algoritmo de Dijkstra.

Ambos tienen dos niveles de jerarquía.

9.2.2. Lugares de utilización

OSPF se utiliza como solución empresarial.

IS-IS se utiliza como solución para ISPs.

9.2.3. Terminología

| Terminología IS-IS | Terminología OSPF |
|--|---|
| Área | Area Stub |
| Area ID | Area ID |
| Área de Backbone | Área de Backbone |
| DIS - Designated Intermediate System | DR - Designated Router |
| Domain | Network |
| ES (End System) | Host |
| ES-IS (End System - Intermediate System) | ARP (Address Resolution Protocol) |
| IS (Intermediate System) | Router |
| ISO Routing Domain | Autonomous Domain |
| Level 1 | Internal nonbackbone área |
| Level 1-2 | Area Border Router (ABR) |
| Level 2 | Backbone Router |
| LSP (Link State Packet) | LSA (Link State Advertisement) |
| CSNP y PSNP | Link State AcknowledgePacket |
| PDU (Protocol Data Unit) | Packet |
| NET (network Entity Title) | IP Destination Address |
| NSAP (Network Service Access Point) | IP destination address + IP protocol number |
| SNPA (Subnetwork Point of Attachment) | Layer 2 Address. MAC, DLCI ... |
| System ID | Dirección de un host en la red, puede ser un Router ID. |
| virtual-link (NO SOPORTADO) | virtual-link |

9.2.4. Diferencias de OSPF con IS-IS

Los protocolos difieren en cómo se asigna el direccionamiento del área.

En IS-IS el área y el ID del host son asignados al router completo, no al interfaz como en OSPF.

En IS-IS un router se encuentra en un único área, mientras que en OSPF un router puede estar en varias áreas, pero esto no significa que IS-IS no permita múltiples áreas.

Todos los routers Level 1 de IS-IS se encuentran en el mismo área.

Los routers Level 1-2 conectan áreas y se encuentran en el mismo área que los routers Level 1. Los routers Level 1-2 pueden ver el resto del AS y se ofrecen como ruta por defecto a los routers Level 1, de forma análoga a las áreas stub de OSPF.

Los routers Level 2 envían actualizaciones Level 2 a otras áreas, o rutas de prefijo, de forma análoga a los ABR de OSPF.

El DIS de IS-IS existe para Level 1 y para Level 2 en redes de multiacceso, pero no existe BDR.

En OSPF el DR se escoge de por vida, sin embargo en IS-IS si aparece un Router con mayor prioridad que el DIS, este dejará de ser el DIS.

En cuanto a las adyacencias en IS-IS, son mayor cantidad que en OSPF, ya que en IS-IS es necesario crear adyacencias con cada uno de los routers.

En IS-IS los LSPs son enviados únicamente por el DIS en nombre del pseudonode.

La mayor diferencia estriba en la encapsulación de los protocolos. IS-IS es independiente al protocolo porque funciona directamente en la parte superior de la capa 2.

La fragmentación es responsabilidad de IS-IS, esto permite que el protocolo evolucione muy fácilmente ya que no depende de un tercero.

OSPF depende de IP porque se encapsula dentro de IP.

El tratamiento de los LSPs por parte de IS-IS es un poco distinto al tratamiento de los LSAs por parte de OSPF.

9.2.5. Diferencias técnicas de IS-IS con OSPF

9.2.5.1. Áreas

Mientras que en IS-IS los límites son establecidos por el enlace en OSPF los límites son establecidos por el router.

Un router en IS-IS está únicamente en un área, sin embargo en OSPF un router puede pertenecer a más de un área.

9.2.5.2. Designated Router (DR) vs Designated Intermediate System (DIS)

En IS-IS si aparece un router activo con mayor prioridad que el DIS pasará a ser el DIS inmediatamente, en OSPF no.

Si existen varios routers con la misma prioridad en IS-IS, entonces elegiremos el que tenga la mayor MAC, en OSPF si existe empate utilizaremos la dirección IP mayor.

Las adyacencias en IS-IS se crean con todos los IS del medio de broadcast, en OSPF sólo se forman con el DR y el BDR.

En IS-IS cada IS envía los LSPs a todos los IS del medio mediante multicast y no se aceptan, en OSPF los LSAs se aceptan.

9.2.5.3. Encapsulación

Mientras que IS-IS opera en la parte superior de la capa 2, OSPF opera en la capa 3.

IS-IS es un protocolo con su propio paquete de capa 3, mientras que OSPF utiliza un paquete IP.

La Fragmentación es responsabilidad de IS-IS, sin embargo en OSPF la fragmentación es responsabilidad de IP.

9.2.5.4. Inundación de LSAs

En una red de broadcast todos los IS de IS-IS mantienen adyacencia entre ellos, sin embargo en OSPF sólo se mantiene adyacencia entre el DR y BDR con los demás routers.

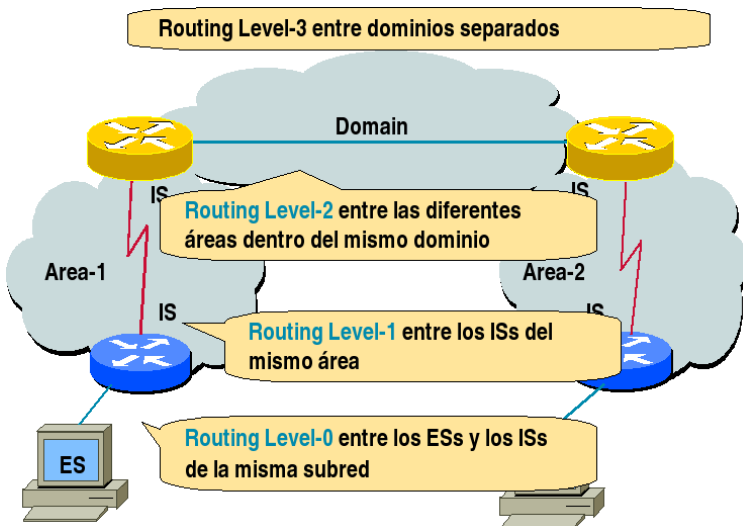
El DIS envía CNSPs a los demás IS. En OSPF, los acks se envían desde el DR en forma de Unicasts.

En IS-IS se envían de forma periódica CSNPs para asegurar que las bases de datos están sincronizadas.

9.2.5.5. LSAs

En IS-IS existen dos tipos de LSPs mientras que en OSPF existen siete tipos de LSA.

9.2.6. Servicios de red OSI – Operación de routing OSI



9.3. Direccionamiento para IS-IS

Cuando IS-IS encamina tráfico IP, la información de routing se lleva en actualizaciones IS-IS, pero los routers participantes necesitan una dirección ISO.

Una dirección ISO puede ser de dos formas (dirección NSAP o NET). Las direcciones ISO son de tamaño variable, de 8 a 20 bytes de longitud.

Una dirección ISO está dividida en tres partes (Area, ID y SEL) tal y como viene descrito en la norma ISO 10589:

| AREA | ID | SEL |
|------|----|-----|
|------|----|-----|

Como IS-IS es un producto de un comité, parece que es una solución académica para resolver cualquier eventualidad. Su esquema de direccionamiento es global y no local.

Una de las características de IS-IS que le están haciendo tan popular es la longitud de su espacio de direccionamiento.

Los campos de la dirección ISO son:

- Área: Se utiliza para enrutar entre áreas utilizando routing Level 2.
- ID: Se utiliza para enrutar a un host o router dentro del área utilizando routing Level 1.
- SEL: Se utiliza para enrutar a una entidad en el host o en el ES.

El direccionamiento IS-IS es complicado ya que los tres campos se subdividen para permitir mayor granularidad en el routing.

Las tres partes de la dirección describen como llegar al área, como encontrar el host y como encontrar la aplicación dentro del host.

Los dos primeros campos son utilizados para encontrar el host de destino, la última parte se utiliza para después de haber encontrado el host.

Por tanto, IS-IS tiene dos niveles de jerarquía:

- Cómo llegar al área
- Cómo llegar al host

9.3.1. Dirección OSI

Una dirección OSI se divide básicamente en dos partes, la IDP (Initial Domain Part) y la DSP (Domain Specific Part).

De hecho las direcciones OSI pueden tener muchas formas y esto puede causar confusión, pero hay que recordar que OSI utiliza sólo dos niveles de jerarquía.

| IDP | | DSP | | |
|----------------|-----|----------------|-------------------------|-----------------|
| AFI (1 octeto) | IDI | High Order DSP | System ID (1-8 octetos) | NSEL (1 octeto) |
| AREA | | | ID | SEL |

9.3.1.1. Initial domain part (IDP)

Routing Externo. Utilizado para enrutar el dominio o el AS. El IDP es otorgado por ISO e identifica la organización, la cual es responsable del resto de la estructura del direccionamiento.

Authority and Format Identifier (AFI): Es el primer octeto.

Initial Domain Identifier (IDI): Es la subrogación del AFI.

9.3.1.2. Domain specific part (DSP)

Utilizado para enrutar dentro del AS.

High Order DSP: Es normalmente el área dentro del AS.

System ID: Puede tener un valor de entre 1 y 8 octetos. Cisco utiliza seis octetos como solución común, ya que permite utilizar la dirección MAC para autoconfigurar el sistema.

NSEL: Un byte que identifica el servicio particular en el nivel de red que debe de manejar el paquete.

9.3.2. NETs y NSAP

Una dirección NET es la dirección de un host, donde el valor del campo NSEL es fijo a 0x00, es decir, que no tiene ningún protocolo de capa superior identificado. Estas direcciones son transitorias de IS.

Las direcciones NET son básicamente direcciones NSAP con el campo NSEL a 0x00.

Sin embargo las direcciones NSAP son direcciones ISO completas, y no sólo describe el área y el host, sino también a quien enviar la información una vez llegado al host destino.

El campo NSEL de ISO especifica el protocolo de capa superior, de forma análogo al campo Protocolo de la cabecera IP.

Tanto NET como NSAP son direcciones ISO, la diferencia entre ellas es sutil, la diferencia estriba en el valor del campo NSEL:

- NSEL=0x00 -> Dirección NET.
- NSEL≠0x00 -> Dirección NSAP.

9.3.3. Reglas del direccionamiento ISO

El direccionamiento ISO tiene las siguientes reglas:

- La dirección ISO es asignada al sistema, no al interfaz.
- El router tiene una dirección NET. El límite es de 3 direcciones NET por área y/o router. Durante las transiciones se utilizan múltiples direcciones.
- Si existen múltiples NET en un router, todas deben de tener el mismo System ID.

- La dirección del Área tiene que ser la misma para todos los routers del área.
- Todos los routers de nivel 2 deben tener el mismo System ID, y tiene que ser único para todo el dominio.
- Todos los routers de nivel 1 de un área tendrán el mismo System ID.
- El System ID tiene que ser de la misma longitud para todos los IS y ES del dominio de routing.

9.3.4. Ejemplos de una dirección NET

9.3.4.1. Ejemplo utilizando la dirección MAC como System ID

MAC: aa:00:03:01:16:cd

| IDP | | DSP | | |
|----------------|-----|----------------|-------------------------|-----------------|
| AFI (1 octeto) | IDI | High Order DSP | System ID (1-8 octetos) | NSEL (1 octeto) |
| 47. | | 0005. | aa00.0301.16cd | 0 |
| AREA | | | ID | SEL |

9.3.4.2. Ejemplo utilizando la dirección IP como System ID

IP: 144.132.16.19

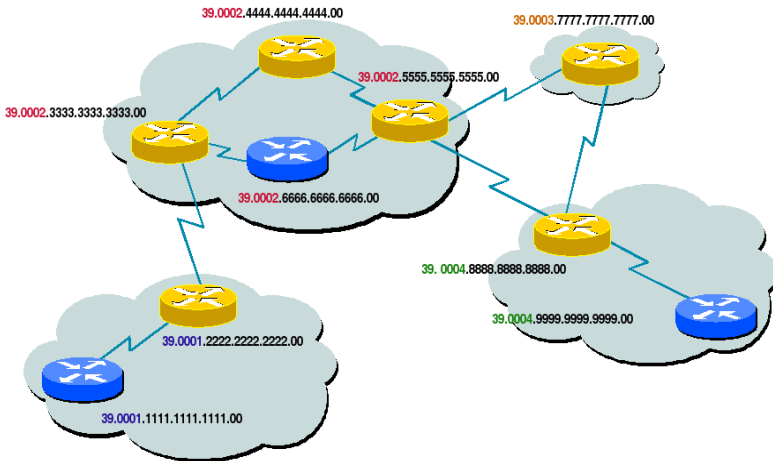
| IDP | | DSP | | |
|----------------|-----|----------------|-------------------------|-----------------|
| AFI (1 octeto) | IDI | High Order DSP | System ID (1-8 octetos) | NSEL (1 octeto) |
| 47. | | 0001. | 0001.1441.3201.6019. | 0 |
| AREA | | ID | | SEL |

9.3.4.3. Ejemplo de dirección GOSIP¹ versión 2

| IDP | | DSP | | |
|----------------|----------------------|----------------|-------------------------|-----------------|
| AFI (1 octeto) | IDI | High Order DSP | System ID (1-8 octetos) | NSEL (1 octeto) |
| 47. | 0005.80ff.f800.0000. | 0001. | 0000.0c00.1234. | 0 |
| AREA | | ID | | SEL |

¹GOSIP; Government OSI Profile. Procedimiento del Gobierno de los EEUU para los protocolos OSI. A través del GOSIP el gobierno de los EEUU ordenó a sus agencias federales estandarizar OSI e implementarlo en sus sistemas y hacerlo comercialmente disponible.

9.3.5. Ejemplo de direccionamiento



9.4. Estructura jerárquica de IS-IS

El esquema de direccionamiento permitiría numerosos niveles de jerarquía, sin embargo en IS-IS sólo existen dos niveles.

Para acomodar los niveles de jerarquía existen dos tipos de routers

- Router Level 1: Este tipo de routers son de primer nivel y sólo trabajan dentro del área para encontrar sus rutas.
- Router Level 2: Este tipo de routers trabajan en el segundo nivel y buscan el área a la cual pertenece un IS o ES de destino.

Para que los Routers de Level 1 y los de Level 2 puedan comunicarse es necesaria la utilización de Routers Level 1-2.

- Router Level 1-2: Estos routers ejecutan procesos de Level 1 y de Level 2 y pueden ser vistos como routers de una tercera clase.

9.4.1. Router Level 1

El Router Level 1 localiza el host de destino dentro del área, esto es conocido como intra-area routing.

El conocimiento de la red de un Router Level 1 está limitado al área a la cual pertenece, utilizando una ruta por defecto al router Level 2 más cercano para enrutar hacia fuera del área.

Cada Router Level 1 tiene una base de datos de topología con la información de su área, y todos los Routers Level 1 del área tienen la misma información.

Obviamente para que un Router Level 1 pueda comunicarse con otro, ambos deben pertenecer al mismo área.

En medio LAN se elige un DIS.

9.4.2. Router Level 2

Para enrutar tráfico entre áreas es necesario un Router Level 2. Este tipo de routing se llama interarea routing.

Al igual que en OSPF el backbone tiene que ser continuo.

Los Routers Level 2 intercambian información utilizando paquetes Hello que son entendidos sólo por otros Routers Level 2.

Al igual que los Routers Level 1, la base de datos del enlace es idéntica en todos los Routers Level 2.

La base de datos contiene los prefijos de direcciones en otras áreas.

9.4.3. Router Level 1-2

EL Router Level 1-2 es tanto *intra-area* como *interarea*.

Sus características son similares a los ABR de OSPF.

Este tipo de routers tiene vecinos tanto de Level 1 como de Level 2, y se comunica con todos.

Los Routers Level 1-2 tiene bases de datos Level 1 y Level 2.

Estos routers pueden informar a los Routers Level 2 de las áreas a las que está conectado y a los Routers Level 1 de que pueden utilizarlo para reenviar el tráfico a otras áreas.

El consumo de estos routers en cuanto a CPU y memoria es superior a los demás.

Este es el tipo de routers por defecto en Cisco.

9.5. Principios básicos de routing de área

Proceso de decisión de routing en routing de área:

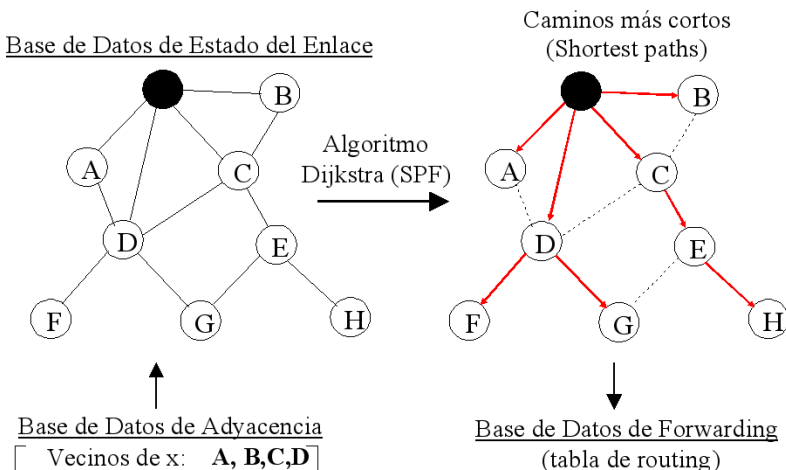
- Cuando un router recibe tráfico con destino otra red, lo primero que se hace es una búsqueda en la tabla de routing.
- El router extrae en la dirección OSI el System ID y el SEL para diferenciarlos de la porción de Área. Si el área es la misma se enruta el paquete al host de destino utilizando la base de datos Level 1.
- Si las Áreas son diferentes entonces:
 - Si el router es un Router Level 1, se envía al Router Level 2 más cercano.
 - Si el router es un Router Level 2, se busca la ruta en la base de datos de forwarding.
 - Se busca el prefijo más genérico posible para reenviar el paquete (sumarización).

Este proceso se describe basándonos en la dirección de destino OSI del paquete entrante.

Las áreas en IS-IS se definen en el enlace, lo cual significa que el router completo es el que está en el área y no el interfaz como en OSPF.

Para que las actualizaciones de Level 2 puedan intercambiarse, todos los Routers Level 2 tienen que ser contiguos.

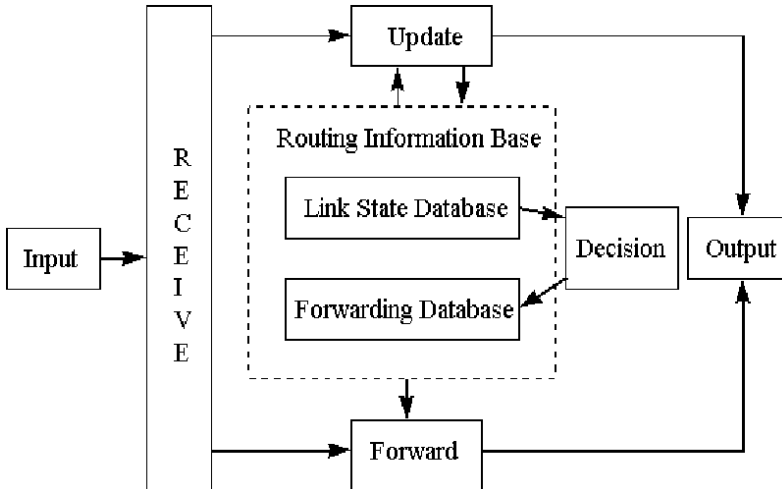
9.5.1. Entorno de estado del enlace



9.5.2. Ejemplos de protocolos estado del enlace

- OSPF (Open Shortest Path First), soporta únicamente IP; RFC 2328.
- DECnet Phase V, soporta Decnet/OSI.
- IS-IS (soporta CLNP); estándar ISO.
- IS-IS (soporta CLNS and IP); RFC 1195.
- NLSP (Netware Link Services Protocol), soporta únicamente IPX, basado en IS-IS.
- PNNI (Private Network to Network Interface)— utilizado en “routing” ATM.

9.5.3. Proceso de estado del enlace



9.6. Redes e interfaces de IS-IS

Los Routers comparten un nivel de enlace común pasan a ser vecinos de IS-IS siempre que los paquetes Hello intercambien información para formar la adyacencia.

Cada Hello informa de las capacidades del interfaz emisor, si estas capacidades concuerdan entonces se forma la adyacencia y los vecinos intercambian información de Routing en forma de LSPs.

Para que se pueda producir la adyacencia se tiene que cumplir:

- La MTU (Maximum Packet Size) tiene que ser idéntico en cada interfaz.
- Cada router tiene que estar configurado en el mismo nivel.
- Si se trata de Routers Level 1 tiene que estar en el mismo área.

- El System ID tiene que ser único en cada router.
- Si se configura autenticación tiene que ser igual en ambos extremos.
- Los temporizadores de Hello deben de coincidir.

El encontrar un vecino difiere sutilmente del medio.

Un Router Level 1 creará adyacencia con otro Router Level 1.

Un Router Level 2 creará adyacencia con otro Router Level 2.

Para que un Router Level 1 pueda comunicarse con un Router Level 2 uno de ellos tiene que estar configurado como Router 1-2.

Para conectar con otro área al menos debe de existir un Router Level 1-2.

9.6.1. Tipos de redes en IS-IS

- Point-to-point.
- Broadcast link.
- NBMA link.

9.6.2. Establecimiento de adyacencias en punto a punto

Un enlace de punto a punto conecta dos routers.

Después de que el paquete Hello haya sido recibido, ambos extremos declaran el otro extremo como alcanzable.

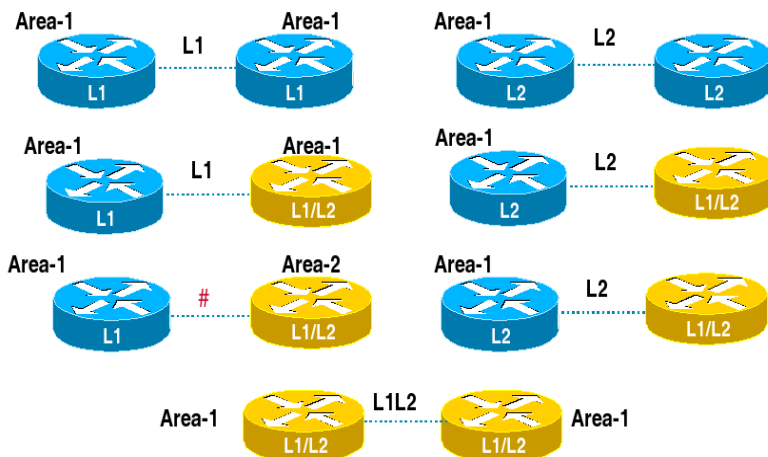
En ese momento los routers son adyacentes.

Una vez son adyacentes se envían CSNP².

Periódicamente se envían Hello para mantener la adyacencia.

²Complete Sequence Number Packet (CSNP): CSNP describe cada enlace en la BD de estado del enlace. Los CSNP se envían en enlaces punto a punto cuando el enlace se levanta para sincronizar las BD de estado del enlace. El Router

9.6.3. Adyacencias punto a punto



9.6.4. Establecimiento de adyacencias en enlace broadcast

En enlaces de broadcast, todos los routers ejecutando IS-IS reciben paquetes Hello del DIS.

El DIS tiene la responsabilidad de inundar los LSPs a todos los sistemas conectados ejecutando IS-IS, es decir, el DIS inunda los LSPs al pseudonode.

El pseudonode inunda con un nuevo pseudonode LSP cuando existe un cambio en sus conexiones.

Las adyacencias con los demás routers se mantienen por el DIS cada 3,3 segundos

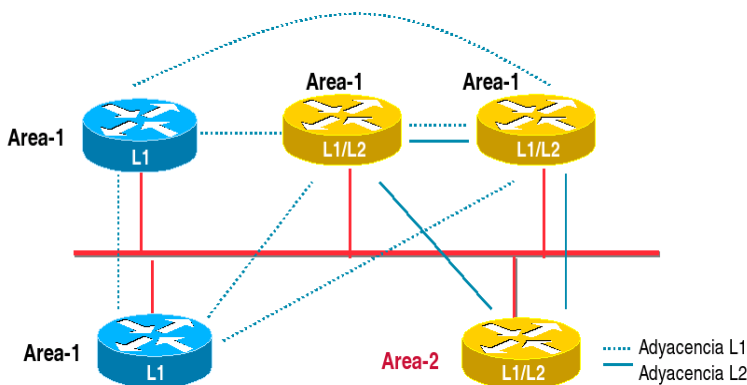
Designado (DR), o el Sistema Intermedio Designado (DIS), en redes multicast envían el CSNP cada 10 segundos.

El CSNP consiste en una lista de enlaces que existen en la BBDD del enlace. Si un router no escucha el Hello del adyacente, al llegar al holtime (30 segundos) , entonces se borrará el router de la BBDD del enlace.

Si existiera un problema con el DIS u otro router tuviera más prioridad entonces se cambiaría automáticamente el DIS.

La elección del DIS se basa en el valor más alto para el SNPA³.

9.6.5. Adyacencias de broadcast



9.6.6. Establecimiento de adyacencias en NBMA

NBMA no es ni broadcast ni punto a punto, sino un poco de cada.

IS-IS soporta como medio la LAN y por tanto necesita capacidades de broadcast, sin embargo una WAN se puede considerar una LAN si se consigue emular.

Para evitar complejidades Cisco recomienda configurar la red NBMA como un conjunto de enlaces punto a punto.

³Sunetwork Point of Attachment (SNPA): El SNPA se refiere a los servicios ofrecidos por el nivel de enlace al nivel físico y al de red. La dirección SNPA es la dirección física.

9.6.7. Protocolos de capa 3 utilizados en IS-IS

La PDU se crea en el nivel de red y se encapsula directamente en la trama de capa 2.

Después de la cabecera fija, existen unos campos opcionales de tamaño variable que contienen información de routing específica. Estos campos son llamados TLV y CLV.

| Campo | Longitud del campo en octetos | Descripción |
|------------------------------|-------------------------------|--|
| Intradomain Routing Protocol | 1 | Todas las PDUS de IS-IS tienen el valor 0x83. |
| Length Indication | 1 | Longitud de la cabecera. |
| Version / Protocol ID | 1 | Configurado a 1 |
| ID Length | 1 | El tamaño del System ID en el NSAP. uede ser un entero de 1 a 8. En Cisco por defecto es 6, pero se representa con un 0 para indicar que no ha cambiado. |

| Campo | Longitud del campo en octetos | Descripción |
|------------------------|-------------------------------|--|
| Reserved / Packet Type | 1 | Los 3 primeros bits están reservados, configurados a 0 e ignorados. El Packet Type identifica si es un Hello, LSP o SNP. |
| Version | 1 | Configurado a 1 |
| Reserved | 1 | Configurado a 0 e ignorado |
| Maximim Area Addresses | 1 | Indica el máximo número de direcciones de área permitidas. En Cisco el tamaño máximo es 3, y se representa por 0. |

9.6.8. Tipos de paquetes en IS-IS

Hello: Estos paquetes crean y mantienen las adyacencias y relaciones entre vecinos.

- LAN Level 1: Generados por los Routers Level 1 y Routers Level 1-2.
- LAN Level 2: Generados por los Routers Level 2 y Routers Level 1-2.

Point-to-Point: Generados por todos los routers.

LSP: Mantienen información de los vecinos conectados directamente al router.

- Level 1: Generados por los Routers Level 1 y Routers Level 1-2.
- Level 2: Generados por los Routers Level 2 y Routers Level 1-2.

Sequence Number Packet (SNP): Este tipo de paquetes no se inundan y se envían directamente al vecino. Se aseguran que las BBDD están sincronizadas entre vecinos:

- Distribuyendo grupos de LSPs en la LAN sin ACKs individuales explícitos.
- Realizando ACKs de LSPs individuales.
- Solicitando LSPs al inicio.

Existen dos tipos de SNPs para cada nivel de routing.

Complete SNP (CSNP): Incluye todos los LSPs de la BBDD:

- Level 1.
- Level 2.

Partial SNP (PSNP): Incluye un subconjunto de LSPs, bajo petición:

- Level 1.
- Level 2.

9.6.9. Formato del paquete Hello

Punto a punto y broadcast funcionan de forma diferente, por eso existen dos tipos bien diferenciados de paquetes hello.

Consideraciones en punto a punto:

- Una vez que se establece el nivel de routing pueden ser enviadas las actualizaciones.

Consideraciones en Broadcast:

- Disponemos de dos tipos, los de Level 1 y los de Level 2.

9.6.10. Hello punto a punto

| Campo | Longitud (en bytes) | Descripción |
|------------------------|---------------------|---|
| Holding Time | 2 | El tiempo a esperar sin recibir Hellos del vecino antes de determinar que ha caído |
| Cabecera fija de IS-IS | 8 | Común en todas las PDUs de IS-IS |
| Circuit type | 1 | Establece si el transmisor es Level 1 ó 2, o si es Level 1-2 y permite ambos tipos de Hello |
| Source ID | ID length | El System ID del NSAP del router transmisor |
| Packet Length | 2 | La longitud del paquete Hello en bytes |
| Local Circuit ID | 1 | Identificador del interfaz transmisor. |

9.6.11. Hello lan

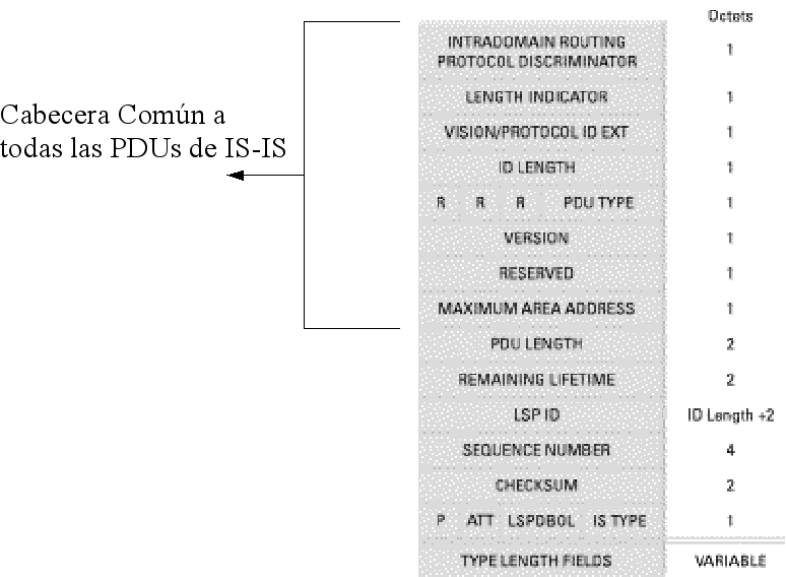
| Campo | Longitud (en bytes) | Descripción |
|------------------------|---------------------|---|
| Cabecera fija de IS-IS | 8 | Común en todas las PDUs de IS-IS |
| Circuit type | 1 | Establece si el transmisor es Level 1 ó 2, o si es Level 1-2 y permite ambos tipos de Hello |
| Source ID | ID length | El System ID del NSAP del router transmisor |
| Holding Time | 2 | El tiempo a esperar sin recibir Hellos del vecino antes de determinar que ha caído |
| Packet Length | 2 | La longitud del paquete Hello en bytes |
| Priority | 2 | Utilizado en la elección del DIS |
| LAN ID | ID length + 1 | El DIS utiliza su System ID y un octeto adicional para identificar la LAN. |

9.6.12. Formato del LSP

El LSP de un Router Level 1 se inunda a los demás routers en el área. El LSP contiene una lista con todas las adyacencias.

El LSP de un Router Level 2 inunda los LSPs a los otros Router Level 2 del dominio. Este tipo de LSPs contienen la lista de adyacencias a los otros Routers Level 2 y a las áreas que los routers son capaces de acceder.

El TLV⁴ mantiene la información de Level 1 y Level 2, permitiendo que el formato del LSP sea el mismo para Level 1 y Level 2.



Packet Length: Longitud total del LSP

⁴TLV es lo mismo que CLV Code/Lengh/Value (CLV): Estos son los campos vartiables en la PDU. El campo code especifica la información en el campo Content como un número. El campo Lengh determina el tamaño del campo Value. El campo Value contiene la información.

Remaining Lifetime: El tiempo en segundos hasta que el LSP sea borrado de la BBDD.

LSP ID: System ID o Pseudonode ID.

Sequence Number: Para determinar la última versión del LSP.

Checksum: Suma de comprobación de los contenidos del LSP.

P: Partition Bit. Los Routers Level 2 identifican si está disponible la reparación de partición. NO soportado por Cisco.

ATT: Attached Bit. Utilizado por los LSPs Level 1 generados por los Routers Level 1-2. Muestra a los Routers Level 1 la salida del área más próxima.

OL: Overload Bit. Muestra que el Router está sin memoria en su BBDD del Enlace.

IS Type: Indica si el Router es Level 1 o Level 2.

9.6.13. Formato del SNP

| Campo | Longitud (en bytes) | Descripción |
|------------------------|---------------------|---|
| Cabecera fija de IS-IS | 8 | Común en todas las PDUs de IS-IS |
| Packet Length | 2 | La longitud del LSP completo |
| Source ID | ID length + 2 | El System ID del NSAP del router transmisor |
| Start LSP ID | ID length + 2 | System ID o Pseudonode ID del emisor |
| End LSP ID | ID length + 2 | System ID o Pseudonode ID del receptor |

9.6.14. TLVs

Los TLVs también son llamados CLVs, y forman una de las características más importantes de IS-IS, ya que proporcionan flexibilidad y funcionabilidad extendida del protocolo.

La estructura de TLV:

- Type o Code: Identifica el TLV y las características a las que pertenece. TLV 128 define la capacidad de llevar rutas IP en IS-IS, es decir TLV 128 es IS-IS.
- Length: La longitud del siguiente campo que es de longitud variable.
- Value: La información que transporta.

Code/Length/Value (CLV): Estos son los campos variables en la PDU. El campo code especifica la información en el campo Content como un número. El campo Length determina el tamaño del campo Value. El campo Value contiene la información.

9.7. Operación de IS-IS

Los Routers envían la lista de todos sus interfaces de IS-IS para descubrir vecinos para formar adyacencias.

Los Routers que comparten un enlace de datos común serán adyacentes.

Los Routers construyen LSPs basados en los interfaces locales de IS-IS y prefijos aprendidos de los routers adyacentes.

Los Routers inundan los LSPs recibidos a todos los routers adyacentes, excepto a los vecinos mediante los cuales han recibido los LSPs.

Cuando se recibe LSPs diferentes de los que ya tiene el router, estos se añaden a la BD de estado del enlace.

El Router calcula el SPF para cada destino y construye el Shortest Path First Tree (SPT) y la BD de forwarding.

9.7.1. Pasos del proceso de operación de IS-IS

- Update (Actualización).
- Decision (Decisión).
- Forwarding (Reenvío).
- Receive (Recepción).

9.7.1.1. Update (actualización)

Los LSPs son generados si hay un cambio en la red, sin embargo, cualquiera de las siguientes causas dispararán un nuevo LSP:

- Una adyacencia se ha creado o ha caído.
- Un interfaz de un router cambia de estado o se le asigna una nueva métrica.
- Una ruta IP cambia.

Enviar y Recibir LSPs:

- En el momento de recibir un LSP, el router lo almacena en la BD de enlace y lo marca para su inundación.
- Si el LSP ya existe en la BD entonces lo acepta y lo ignora.
- Si no existe se inunda por la red hasta llegar a los límites de la red.
- Los Routers Level 1 y los Routers Level 2 disponen de LSPs distintos.

Propagación de LSPs en interfaces punto a punto:

- Cuando se crea la adyacencia, ambos lados envían un CSNP con información comprimida de sus BBDD del enlace.

- Si se recibe algún LSP que no está en el CSNP, se envía una copia al otro router.
- Si en la BD falta cualquier LSP recibido en el CSNP se solicita un LSP detallado.
- Los LSPs son solicitados, enviados y aceptados vía PSNP.
- Cuando se envía un LSP, el router establece un tiempo en el cual se espera su aceptación antes de ser reenviado. Este tiempo se llama `minimumLSPTransmission-interval`.

Propagación de LSPs en enlaces de broadcast:

- El enlace envía sus actualizaciones utilizando direcciones MAC de multicast a todos los Routers Level 1 y Level 2.
- Ya que el pseudonode es un router ficticio, un router real tiene que tomar su papel.
- El DIS (Designated Intermediate System) toma mucha de la responsabilidad de sincronización de las BBDD en lugar el pseudonode.

Determinar cuando el LSP de la BD es válido:

- El LSP tiene 3 campos que ayudan a determinar si el LSP recibido es más reciente que el existente en la BD y si está intacto o está corrupto.
 - **Remaining Lifetime:** Si un LSP está en la BD durante 20 minutos se asume que el router está caído. El tiempo por defecto para las actualizaciones es de 15 minutos.
 - **Sequence Number:** Número entero de 32 bits sin signo utilizado para numerar los LSP, se van incrementando de uno en uno.
 - **Checksum:** Si el router recibe un LSP y el checksum no es correcto entonces se tira y se solicita un reenvío del LSP.

9.7.1.2. Decision (Decisión)

Los pasos en mediante los cuales se construye la BD de forwarding son:

- El router se coloca como raíz en la tabla PATH.
- El SPF mira cada LSP de la BD de estado del enlace y selecciona la mejor considerando la métrica de cada camino, el que tenga menor métrica será elegido.
- El proceso de decisión busca un LSP para el nodo en la tabla PATH. El coste de la métrica al nodo se añade al coste del LSP. Este valor se introduce en TENT.
- Si la tabla TENT está vacía, entonces nos paramos.
- Si no está vacía la tabla TENT, encontrar la entrada con menor coste y moverla de la tabla PATH a la tabla TENT.
- Volver al inicio del proceso de decisión.

Si existe más de un camino para un destino:

- Si existe más de un camino con la métrica más baja, los equipos Cisco permiten hasta seis caminos en la tabla de routing. El número de rutas iguales permitidas por defecto en Cisco es de cuatro.
- Métricas opcionales son seleccionables antes que la métrica por defecto pero Cisco sólo soporta la de por defecto.
- Los caminos internos son preferidos antes de escoger los externos.
- Los caminos de Level 1 son preferidos a los otros.
- Escogeremos la ruta con mayor precisión (con más bits de red)
- Si hay ToS se prefiere a las rutas sin ToS.

- Si existen múltiples caminos con ToS, se escogerá la que tenga la ruta más corta.
- Si el ToS es el mismo, se permite hasta 6 entradas en la tabla de routing y balancear el tráfico.
- Si existe ruta se utiliza una ruta por defecto al Router Level 2 más cercano.

9.7.1.3. Métricas

- **Default:** También llamada coste. Cada router ejecutando IS-IS debe soportar esta métrica. Cisco configura como defecto en todos sus interfaces con coste 10.
- **Delay:** Retardo de transmisión.
- **Expense:** Coste monetario de la red.
- **Error:** Confiabilidad del enlace.

Las métricas de OSI se configuran en el interfaz de salida utilizando un valor entero de entre 0 y 63.

Un campo de 10 bits describe el camino total al destino, permitiendo un valor de 0 a 1023.

Sin embargo Cisco ha incrementado el campo de la métrica hasta 24 bits. En la configuración por defecto utiliza 6 bits para la narrow metric.

9.7.1.4. Forwarding (Reenvío) y Receive (Recepción)

Después que se haya construido el SPT, la BD de forwarding puede ser creada.

La tabla de forwarding es una tabla de búsqueda de la entrada más concreta, donde el balanceo de carga ocurre en caminos iguales.

Si la trama es valida, el proceso receptor pasa los reportes de datos y errores al proceso de forwarding, donde la información de routing (Hellos, LSPs, SNPs) se envía al proceso de update.

9.8. Consideraciones de diseño de IS-IS

En IS-IS, las consideraciones fundamentales de diseño son áreas y direccionamiento.

Cuando se diseña una red, hay que comprometerse. Normalmente, el problema se encuentra entre fiabilidad y velocidad. Lo que sea preferible para nuestra red es una decisión corporativa a tener en cuenta.

- **Particionamiento del área:** Si no utilizamos áreas ante caso de fallo un área no queda aislada.
- **Perdida de Información:** Si el área se queda particionada se pierde Información.
- **Decisiones de Routing no óptimas:** Los Routers Level 1 no conocen más allá de su área y tienen una ruta por defecto para el Router Level 2 más cercano.

9.8.1. Diseño de área de routers IS-IS

Las consideraciones de diseño típicas son:

- Una red plana utiliza únicamente routing Level 1 (no escalable).
- Una red plana utiliza únicamente routing Level 2 (permite escalar conectando áreas con Routing Level 1).
- Una red plana utiliza únicamente routing Level 1-2 (por defecto de Cisco). Este tipo de diseño requiere más recursos para mantener las dos tablas de routing.
- Modelo jerárquico en el cual utilizamos un área principal con Level 2 y áreas adyacentes utilizando Level 1, para interconectarlas tenemos que utilizar Routers Level 1-2.

Por defecto Cisco utiliza Routers Level 1-2 por:

- Particionamiento del área.
- Pérdida de Información.
- Decisiones de Routing no óptimas.

9.8.2. Sumarización de rutas

Las reglas para la sumarización son las siguientes:

- Los Routers Level 1-2 pueden sumarizar rutas dentro de su área. Las rutas sumarizadas se propagan a los Routers Level 2. Este es un método eficiente para establecer el prefijo de routing a otras áreas. La sumarización se configura en el Router Level 1-2 en el límite de la red.
- Si un Router Level 1-2 tiene configurada la sumarización, se tiene que configurar la sumarización en los demás Routers Level 1-2 para inyectar las actualizaciones a los Routers Level 2.
- Los Routers Level 1 no pueden sumarizar dentro del área porque el protocolo no lo permite.

La sumarización reduce la necesidad de recursos en la red y oculta los problemas de la red en un área, reduce los recursos requeridos para los cálculos de SPF.

Cuanto más detalles tenga el router sobre la red, más recursos deberá de mantener para un buen conocimiento de la red.

La sumarización permite a las áreas gestionar el conocimiento interno de la red y sumarizar el conocimiento a través de los límites del área.

9.9. Configuración básica de IS-IS

Paso 1: Definir áreas, preparar el plan de direccionamiento (NETs) para los routers y determinar interfaces.

Paso 2: Habilitar IS-IS en el Router.

Paso 3: Configurar la NET (Network Entity Tittle).

Paso 4: Habilitar IS-IS en los interfaces – no olvidar interfaces a redes IP stub, como loopbacks.

```
Router(config)#router isis [tag]
```

Este comando habilita el proceso de IS-IS en el router, la etiqueta (tag) es el nombre del proceso.

```
Router(config-router)#net network-entity-tittle(NET)
```

Configura la red IS-IS para el proceso de routing.

```
Router(config-if)#ip router isis [tag]  
Router(config-if)#clns router isis [tag]
```

Configura el proceso de IS-IS en el interfaz (IP, CLNS o ambos).

9.10. Comandos opcionales de IS-IS

9.10.1. Cambiar la opción por defecto de Router Level 1-2

```
Router(config-router)#is-type {level-1 | level-1-2 |  
level-2}
```

Configura el nivel del router, por defecto es Router Level 1-2.

```
Router(config-if)#isis circuit-type {level-1 |  
level-2-only}
```


Configura el tipo de adyacencia del interfaz, por defecto es Level 1-2.

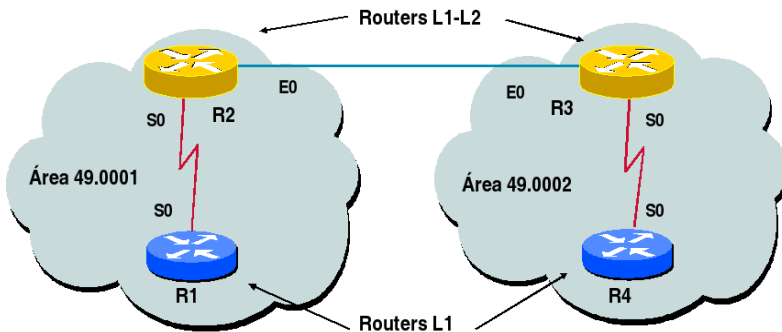
```
Router(config-if)#isis metric métrica-por-defecto
{level-1 | level-2}
```

Configura la métrica por defecto en el interfaz, por defecto la métrica es igual a 10.

9.10.2. Ejemplo de configuración de router IP Level 1-2

```
router isis
net 01.0001.0000.0000.0002.00
!
interface ethernet 0
ip address 10.1.1.1 255.255.255.0
ip route isis
!
interface serial 0
ip address 10.1.2.1 255.255.255.0
ip router isis
```

9.10.3. Ejemplo de estructura en dos niveles



9.10.3.1. Router R1, como router sólo Router L1

```
hostname R1
!  
interface Serial0  
    ip address 192.168.120.1 255.255.255.0  
    ip route isis  
!  
router isis  
    is-type level-1  
    net 49.0001.1921.6800.1005.00
```

9.10.3.2. Router R2, como router Router L1-L2

```
hostname R2  
!  
interface ethernet0  
    ip address 192.168.220.2 255.255.255.0  
    ip router isis  
    isis circuit-type level-2-only  
!  
interface serial0  
    ip address 192.168.120.2 255.255.255.0  
    ip router isis  
    isis circuit-type level-1  
!  
router isis  
    net 49.0001.1921.6800.1006.00
```

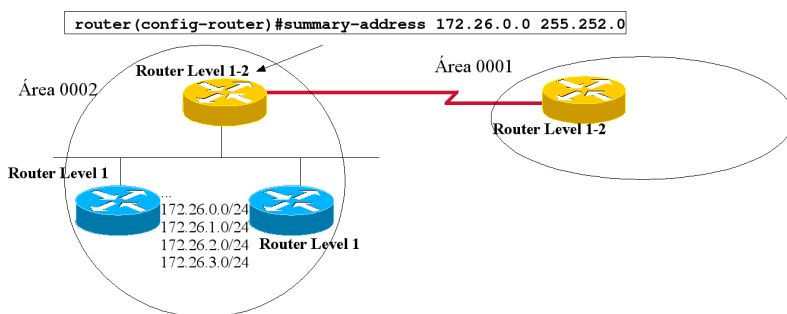
9.10.4. Configuración de la sumarización

Existen tres reglas en cuanto a la sumarización de rutas IP para IS-IS

- Las rutas internas no pueden ser sumarizadas dentro del área porque no lo permite el protocolo.

- Las rutas internas pueden ser sumarizadas entre áreas, desde un Router Level 1 a un Router Level 2 a través de un Router Level 1-2. La sumarización se configurará en el Router Level 1-2, el cual convertirá las rutas Level 1 en rutas Level 2.
- Si se utiliza sumarización, se tiene que configurar en todos los routers Level 1-2, ya que si no, existirá algún Router Level 1-2 con las rutas más específicas y entonces el protocolo de routing lo escogerá y provocará un problema en el routing.

Router(config-router)#summary-address red máscara⁵



9.10.5. Configuración de NBMA

IS-IS acepta dos tipos de topologías de red:

- Broadcast.
- Punto a Punto.

Si el enlace de red no es serie entonces IS-IS considera que es broadcast.

⁵Este comando realizará la sumarización de la red especificada.

Para interfaces WAN de multiacceso, es muy recomendable configurar la nube NBMA como un conjunto de subinterfaces punto a punto.

9.10.5.1. Configuración de broadcast sobre NBMA

Si la nube NBMA es totalmente mallada, la opción de broadcast es la que elegiremos.

En este tipo de configuraciones se elegirá el DIS y funcionará como una Ethernet.

El comando `frame-relay map ip` relaciona la dirección IP con el DLCI.

En IS-IS utilizaremos el comando `frame-relay map clns` en el proceso⁶.

9.10.5.2. Configuración point-to-point sobre NBMA

Para la configuración de point-to-point sobre NBMA es necesaria una subred IP por enlace. Esta es la configuración recomendada por Cisco.

Esta configuración es muy simple porque no requiere la utilización de los comandos `frame-relay map`.

En este tipo de configuraciones simplemente definimos que utilizamos IS-IS en el subinterfaz y definimos el dlci,

```
ip router isis
frame-relay interface-dlci 901
```

⁶Sin el comando `frame-relay map clns` no aparecerán las rutas IP en la tabla de routing ya que no se recibirá IS-IS y no se podrá actualizar la tabla.

9.11. Verificación de la operación de IS-IS

```
show clns neighbors
```

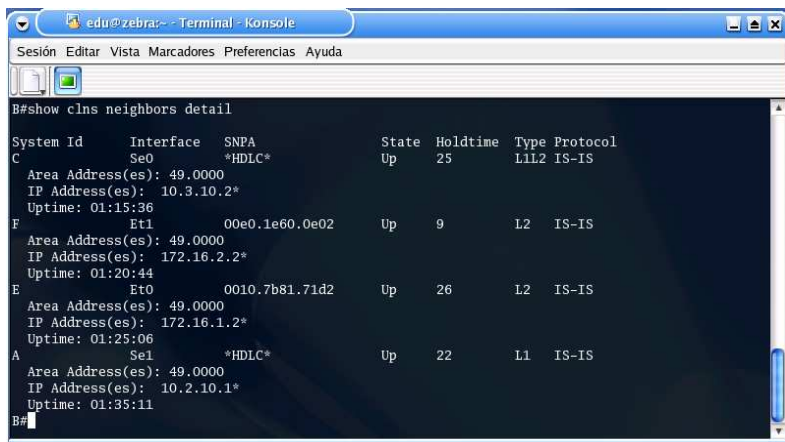


```
B#show clns neighbors
```

| System Id | Interface | SNPA | State | Holdtime | Type | Protoc |
|-----------|-----------|----------------|-------|----------|------|--------|
| C | Se0 | *HDLC* | Up | 27 | L1L2 | IS-IS |
| F | Et1 | 00e0.1e60.0e02 | Up | 7 | L2 | IS-IS |
| E | Et0 | 0010.7b81.71d2 | Up | 24 | L2 | IS-IS |
| A | Se1 | *HDLC* | Up | 22 | L1 | IS-IS |

```
B#
```

```
show clns neighbors detail
```

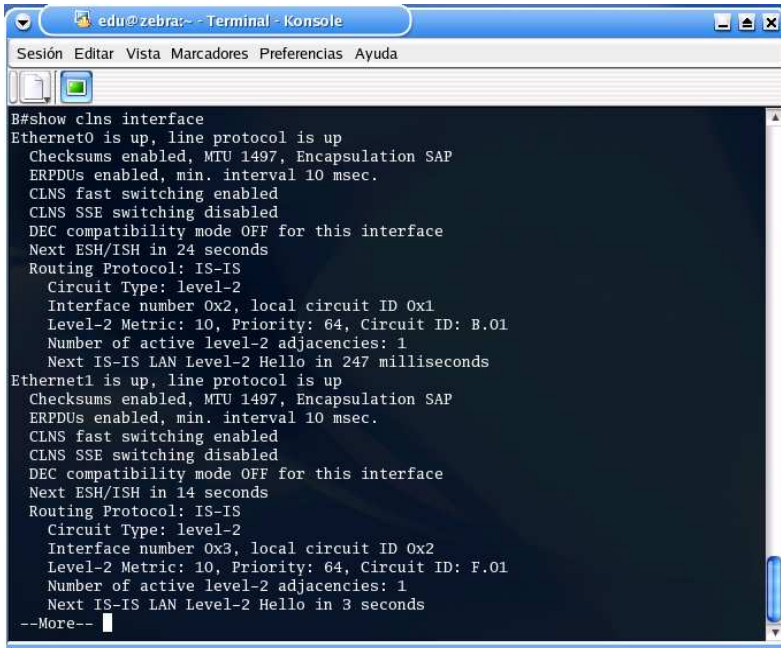


```
B#show clns neighbors detail
```

| System Id | Interface | SNPA | State | Holdtime | Type | Protocol |
|-----------------------------|-----------|----------------|-------|----------|------|----------|
| C | Se0 | *HDLC* | Up | 25 | L1L2 | IS-IS |
| Area Address(es): 49.0000 | | | | | | |
| IP Address(es): 10.3.10.2* | | | | | | |
| Uptime: 01:15:36 | | | | | | |
| F | Et1 | 00e0.1e60.0e02 | Up | 9 | L2 | IS-IS |
| Area Address(es): 49.0000 | | | | | | |
| IP Address(es): 172.16.2.2* | | | | | | |
| Uptime: 01:20:44 | | | | | | |
| E | Et0 | 0010.7b81.71d2 | Up | 26 | L2 | IS-IS |
| Area Address(es): 49.0000 | | | | | | |
| IP Address(es): 172.16.1.2* | | | | | | |
| Uptime: 01:25:06 | | | | | | |
| A | Se1 | *HDLC* | Up | 22 | L1 | IS-IS |
| Area Address(es): 49.0000 | | | | | | |
| IP Address(es): 10.2.10.1* | | | | | | |
| Uptime: 01:35:11 | | | | | | |

```
B#
```

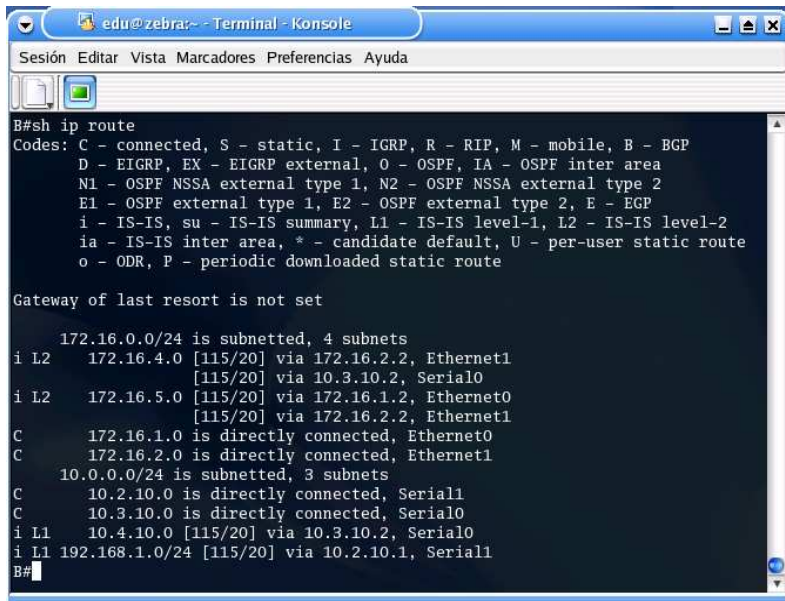
```
show clns interface
```



```
edu@zebrar:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

B#show clns interface
Ethernet0 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUS enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 24 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-2
    Interface number 0x2, local circuit ID 0x1
    Level-2 Metric: 10, Priority: 64, Circuit ID: B.01
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-2 Hello in 247 milliseconds
Ethernet1 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUS enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 14 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-2
    Interface number 0x3, local circuit ID 0x2
    Level-2 Metric: 10, Priority: 64, Circuit ID: F.01
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-2 Hello in 3 seconds
--More--
```

```
show ip route
```



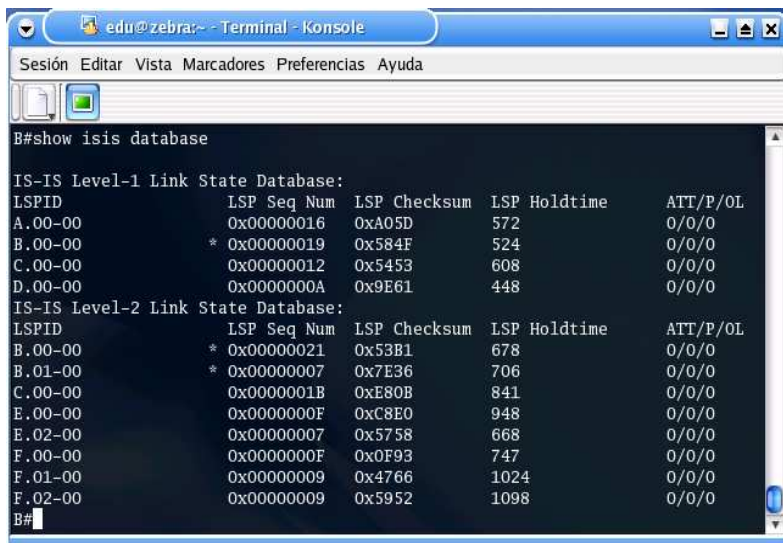
```
edu@zebra:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

B#sh ip route
Codes: C - connected, S - static, I - IGRP, 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, su - IS-IS summary, 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

    172.16.0.0/24 is subnetted, 4 subnets
i L2   172.16.4.0 [115/20] via 172.16.2.2, Ethernet1
        [115/20] via 10.3.10.2, Serial0
i L2   172.16.5.0 [115/20] via 172.16.1.2, Ethernet0
        [115/20] via 172.16.2.2, Ethernet1
C       172.16.1.0 is directly connected, Ethernet0
C       172.16.2.0 is directly connected, Ethernet1
    10.0.0.0/24 is subnetted, 3 subnets
C       10.2.10.0 is directly connected, Serial1
C       10.3.10.0 is directly connected, Serial0
i L1    10.4.10.0 [115/20] via 10.3.10.2, Serial0
i L1    192.168.1.0/24 [115/20] via 10.2.10.1, Serial1
B#
```

```
show isis database
```



```
edu@zebra:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

B#show isis database

IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
A.00-00        0x00000016   0xA05D        572           0/0/0
B.00-00        * 0x00000019   0x584F        524           0/0/0
C.00-00        0x00000012   0x5453        608           0/0/0
D.00-00        0x0000000A   0x9E61        448           0/0/0

IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
B.00-00        * 0x00000021   0x53B1        678           0/0/0
B.01-00        * 0x00000007   0x7E36        706           0/0/0
C.00-00        0x0000001B   0xE80B        841           0/0/0
E.00-00        0x0000000F   0xC8E0        948           0/0/0
E.02-00        0x00000007   0x5758        668           0/0/0
F.00-00        0x0000000F   0x0F93        747           0/0/0
F.01-00        0x00000009   0x4766        1024          0/0/0
F.02-00        0x00000009   0x5952        1098          0/0/0
B#
```



```
show isis database detail
```

```

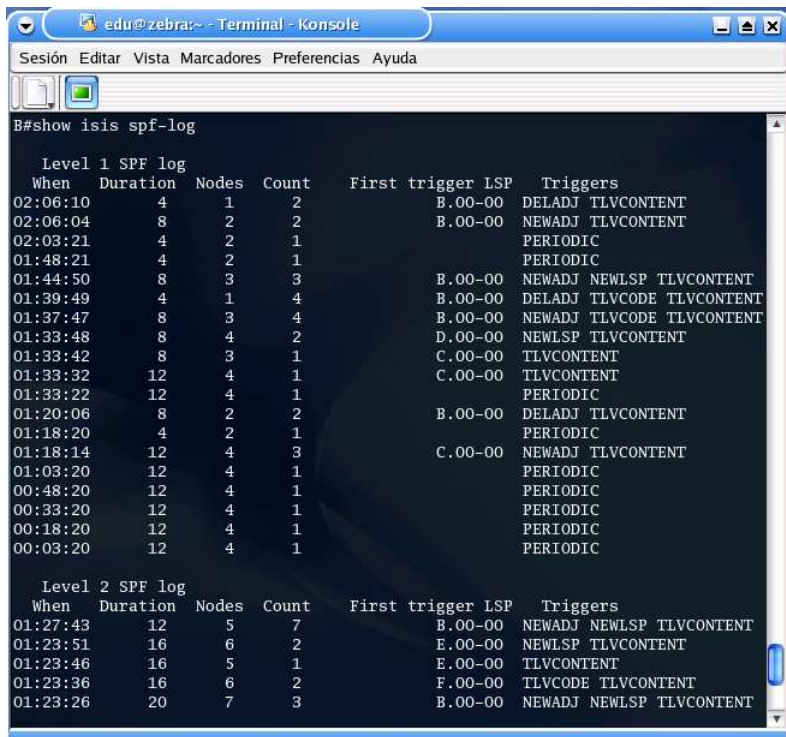
B#show isis database detail

IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
A.00-00        0x00000016   0xA05D        531           0/0/0
  Area Address: 49.0000
  NLPID:        0xCC
  Hostname: A
  IP Address:   10.2.10.1
  Metric: 10    IP 192.168.1.0 255.255.255.0
  Metric: 10    IP 10.2.10.0 255.255.255.0
  Metric: 10    IS B.00
B.00-00        * 0x00000019   0x584F        483           0/0/0
  Area Address: 49.0000
  NLPID:        0xCC
  Hostname: B
  IP Address:   10.2.10.2
  Metric: 10    IP 10.3.10.0 255.255.255.0
  Metric: 10    IP 10.2.10.0 255.255.255.0
  Metric: 10    IS C.00
  Metric: 10    IS A.00
C.00-00        0x00000012   0x5453        566           0/0/0
  Area Address: 49.0000
  NLPID:        0xCC
  Hostname: C
  IP Address:   10.3.10.2
  Metric: 10    IP 10.4.10.0 255.255.255.0
  Metric: 10    IP 10.3.10.0 255.255.255.0
  Metric: 10    IS B.00
  Metric: 10    IS D.00
--More--

```

9.12. Troubleshooting de la operación de IS-IS

```
show isis spf-log
```



```

B#show isis spf-log

Level 1 SPF log
When   Duration  Nodes  Count  First trigger LSP   Triggers
02:06:10      4      1      2      B.00-00 DELADJ TLVCONTENT
02:06:04      8      2      2      B.00-00 NEWADJ TLVCONTENT
02:03:21      4      2      1      PERIODIC
01:48:21      4      2      1      PERIODIC
01:44:50      8      3      3      B.00-00 NEWADJ NEWLSP TLVCONTENT
01:39:49      4      1      4      B.00-00 DELADJ TLVCODE TLVCONTENT
01:37:47      8      3      4      B.00-00 NEWADJ TLVCODE TLVCONTENT
01:33:48      8      4      2      D.00-00 NEWLSP TLVCONTENT
01:33:42      8      3      1      C.00-00 TLVCONTENT
01:33:32     12      4      1      C.00-00 TLVCONTENT
01:33:22     12      4      1      PERIODIC
01:20:06      8      2      2      B.00-00 DELADJ TLVCONTENT
01:18:20      4      2      1      PERIODIC
01:18:14     12      4      3      C.00-00 NEWADJ TLVCONTENT
01:03:20     12      4      1      PERIODIC
00:48:20     12      4      1      PERIODIC
00:33:20     12      4      1      PERIODIC
00:18:20     12      4      1      PERIODIC
00:03:20     12      4      1      PERIODIC

Level 2 SPF log
When   Duration  Nodes  Count  First trigger LSP   Triggers
01:27:43     12      5      7      B.00-00 NEWADJ NEWLSP TLVCONTENT
01:23:51     16      6      2      E.00-00 NEWLSP TLVCONTENT
01:23:46     16      5      1      E.00-00 TLVCONTENT
01:23:36     16      6      2      F.00-00 TLVCODE TLVCONTENT
01:23:26     20      7      3      B.00-00 NEWADJ NEWLSP TLVCONTENT
  
```

When: Hace cuanto que se calculó el SPF, se muestran las últimas 19 veces.

Duration: Número de milisegundos que costó calcularlo.

Nodes: Número de routers y pseudonodos calculados en la ejecución del SPF.

Count: Número de eventos que han sucedido antes de recalcular el SPF.

Last Triggered LSP: Si se ha tenido que recalcular el SPF debido a una actualización por disparo quien la ha causado, si han sido varios sólo se muestra el último.

Trigger: Lista con todos los eventos que han provocado el cálculo.

9.12.1. Comandos de debug en IS-IS

`debug isis adjacencies-packets`: Muestra información de todas las actividades relacionadas con las adyacencias.

`debug isis spf-statistics`: Muestra información sobre la construcción de rutas entre routers.

`debug isis update-packets`: Muestra SNPs (CSNPs y PSNPs) y los LSPs detectados por el router.

Capítulo 10

EIGRP

10.1. Introducción a EIGRP

EIGRP es la versión avanzada de IGRP.

EIGRP utiliza la misma tecnología de vector distancia que IGRP.

EIGRP es muchas veces llamado como Protocolo de Routing Híbrido Equilibrado, aunque Cisco prefiere llamarlo Protocolo de Routing Avanzado de Vector Distancia.

EIGRP es una solución eficiente, aunque propietaria para entornos de networking grandes, ya que es un protocolo con capacidad de escalabilidad.

Al igual que OSPF, EIGRP puede escalar dependiendo del diseño de la red.

10.1.1. Terminología de EIGRP

Vecino: Un router directamente conectado ejecutando EIGRP.

Neighbor Table: Lista con todos los vecinos. Esta tabla se construye con información de Hellos recibidos desde los routers adyacentes. Incluye la lista de vecinos con la siguiente información:

- Dirección IP.
- Interfaz saliente.
- Holdtime.
- Smooth Round-Trip Time (SRTT).
- Uptime.

El tiempo que hace que el vecino ha sido añadido a la tabla.

Tabla de Routing: Lista de las redes disponibles y los mejores caminos. La ruta se mueve desde la tabla topológica hasta la de routing cuando se identifica el feasible successor.

Tabla Topológica: Tabla que contiene todos los caminos anunciados por los vecinos a todas las redes conocidas. Lista de:

- Todos los successors.
- Feasible successors.
- Feasible distance.
- Advertised distance.
- Interfaz saliente.

DUAL actúa en la tabla topológica para determinar los successors y construir la tabla de routing.

Hello: Mensajes utilizados para encontrar y mantener vecinos en la tabla topológica.

Update: Paquete EIGRP que contiene información sobre los cambios de la red. Se envían únicamente cuando hay un cambio en la red que afecta a los routers.

Query: Enviado por el router cuando pierde el camino a una red. Si no existe una ruta alternativa (feasible successor), envía la query a los vecinos preguntando si tienen un feasible successor. Esto hace que la ruta pase a estado active.

Reply: Respuesta a una query, si el router no tiene información para devolver entonces pregunta a todos sus vecinos. El Reply se envía por unicast.

ACK: Paquete Hello sin datos. Se trata de una aceptación.

Holdtime: Valor configurado en el paquete Hello. Determina cuanto tiempo se va a esperar para recibir Hellos de un vecino antes de declararlo no disponible.

Smooth Round-Trip Time (SRTT): El tiempo que el router espera después de enviar un paquete para oír el acknowledge.

Retransmission Timeout (RTO): Tiempo calculado en referencia al SRTT. El RTO determina cuánto tiene que esperar el router el ACK antes de retransmitir el paquete.

Reliable Transport Protocol (RTP): Mecanismo utilizado para determinar los requerimientos de entrega de los paquetes, asegurando la entrega secuencial de los mismo.

Diffusing Update Algorithm (DUAL): Algoritmo que hace que la tabla topológica converja. Está basado en la detección en un tiempo finito de cambios en la topología por parte de los routers. Como el algoritmo se calcula simultáneamente, se asegura una red libre de bucles.

Advertised Distance (AD): El coste del camino a una red remota desde el vecino (i.e. La métrica del vecino).

Feasible Distance (FD): La métrica más baja a una red remota.

Feasible Condition (FC): Cuando un router una AD más pequeña que su FD.

Feasible Successor (FS): Si un vecino reporta una AD más pequeña que la FD, entonces el vecino se convierte en Feasible Successor.

Successor: El siguiente router que pasa la FC. Se escoge el que tenga la métrica más baja a un destino de los FS.

Stuck in Active (SIA): Estado de un router que ya ha enviado paquetes y está esperando los ACKs de sus vecinos.

Query Scoping: Diseño de red para limitar el ámbito del rango de peticiones, es decir, a qué distancia se permite que se busque un feasible successor. Esto es necesario para prevenir SIA, lo cual puede provocar problemas en la red.

Active: Estado de la ruta cuando hay un cambio en la red y no se encuentra un FS. La ruta se establece en modo Active, y el router pregunta por rutas alternativas.

Passive: Una ruta operacional es pasiva. Si no se ha perdido el camino, el router examina la tabla topológica en busca de un FS. Si existe un FS se añade a la tabla de routing, si no, el router pregunta a los vecinos y la ruta se queda en modo active.

10.1.2. Características y ventajas de EIGRP

EIGRP incrementa el crecimiento potencial de la red reduciendo el tiempo de convergencia. Esto se consigue con las siguientes características:

- DUAL.
- Redes libres de bucles.
- Actualizaciones incrementales.
- Direccionamiento de multicast para actualizaciones.
- Protocolo vector distancia avanzado.
- Tabla de routing libres de bucles.
- Soporte para diferentes tecnologías.
- Convergencia rápida.
- Utilización de ancho de banda reducido.
- Configuración sencilla.

- Utilización de métrica compuesta.
- Balanceo de carga entre enlaces de coste diferente.

DUAL: DUAL es una de las características principales de EIGRP. DUAL distribuye la computación de routing entre varios routers.

Redes Libres de Bucles: El algoritmo DUAL se utiliza para asegurar una red libre de bucles. El FS es escogido sólo porque tiene una métrica menor. Esto proporciona una red libre de bucles.

Actualizaciones Incrementales: EIGRP envía actualizaciones parciales no periódicas. Esto significa que cuando hay un cambio se envía la actualización con únicamente la información que ha sido modificada.

Direcciones Multicast para Actualizaciones: EIGRP utiliza RTP para garantizar la entrega, esencialmente cuando las actualizaciones de routing no son periódicas. Si el receptor no espera una actualización no puede saber si ha perdido alguna actualización. Las actualizaciones se realizan mediante multicast fiable a la 224.0.0.10. Cuando el receptor recibe una actualización devuelve un ACK.

Protocolo Avanzado de Vector Distancia: EIGRP ha solucionado muchos de los problemas de los protocolos vector distancia. EIGRP es un protocolo classless. Sin el uso de áreas EIGRP permite sumarización en cualquier punto de la red, lo cual implica un menor gasto de recursos. Por supuesto también soporta discontinuidad de redes y VLSM.

Tablas de Routing Libres de Bucles: El criterio para seleccionar las rutas primarias y de backup en la tabla topológica y en la tabla de routing aseguran que las rutas están libre de bucles. Las rutas están libres de bucles porque al escoger el Successor cogeremos el de menor métrica y el Feassible Successor será el de menor métrica del vecino.

Soporte para Diferentes Topologías: EIGRP es un protocolo moderno que permite la utilización de las más recientes topologías como por ejemplo NBMA.

Convergencia Rápida: El uso del algoritmo DUAL almacena la mejor ruta y las siguientes mejores, así en caso de fallo de la ruta se puede empezar a utilizar la ruta alternativa de forma automática.

Uso Reducido de Ancho de Banda: Utilizando direcciones de multicast y de unicast para enviar y aceptar las actualizaciones reduce el ancho de banda y la CPU. EIGRP utiliza únicamente actualizaciones incrementales, NO periódicas.

Independencia del Protocolo a Nivel 3: EIGRP funciona como protocolo de routing para IP, AppleTalk e IPX. Se utiliza una tabla de routing diferente por protocolo. EIGRP redistribuye de forma automática IPX RIP, AppleTalk RTMP e IP IGRP dentro del mismo AS.

Compatibilidad con IGRP: Como EIGRP descende del IGRP son totalmente compatibles, EIGRP redistribuye IGRP, esto permite que redes antiguas que no permitan EIGRP sigan utilizando IGRP sin problemas en una red EIGRP.

Configuración Sencilla: Ya que EIGRP fue diseñado para el hardware en el cual corre, la configuración del mismo es muy sencilla y requiere menos consideraciones de diseño que OSPF.

Utilización de Métrica Compuesta: EIGRP utiliza la misma métrica que IGRP, pero con un tamaño de 32 bits, permitiendo crecer a la red y permitiendo mayor granularidad.

Balanceo de Carga entre Enlaces de Coste Diferente: EIGRP permite el balanceo de carga entre enlaces de coste diferente, lo cual permite no saturar los enlaces más lentos.

10.1.3. Componentes de EIGRP

Cisco define cuatro componentes principales de EIGRP:

- Módulos Independientes del Protocolo.
- RTP.
- Descubrimiento y Recuperación de Vecinos.

- DUAL.

10.1.3.1. Módulos independientes del protocolo

Se mantiene una tabla de routing separada y un conjunto de funciones para cada protocolo de capa 3 que puede enrutar EIGRP:

- IP.
- AppleTalk.
- IPX.

10.1.3.2. RTP

EIGRP utiliza tanto direcciones unicast como multicast, y muchos de estos paquetes tienen que ser confiables utilizando RTP, es decir, tienen que ser aceptados.

Estos paquetes incluyen un número de secuencia.

No requieren confirmación:

- Hello.
- ACK.

Sí requieren confirmación:

- Update.
- Query.
- Reply.

Si no recibimos un hello de un vecino no consideraremos que está caído hasta que falle 16 veces.

10.1.3.3. Descubrimiento y recuperación de vecinos

Los vecinos comparten tablas de routing e información sobre los estados de sus conexiones.

EIGRP localiza toda la información posible, reduciendo el ancho de banda y los requerimientos de CPU de la red, haciéndola así más rápida la convergencia.

10.1.3.4. DUAL

EIGRP utiliza DUAL para mantener las bases de datos de la red.

Se selecciona el mejor camino a un destino y si es posible se guarda una ruta de backup.

Successor hace referencia al camino al destino.

Feasible Successors hacen referencia a rutas alternativas.

Si el Successor cae y tenemos Feasible Successor entonces este último se convertirá en Successor y entraremos en modo pasivo.

Si no tenemos Feasible Successor entraremos en modo activo y el router preguntará a los vecinos por un Feasible Successor.

10.2. Operación de EIGRP

Uno de los puntos fuertes de EIGRP es que limita el ámbito de la computación de la red, manteniendo todo el conocimiento todo lo local que se pueda.

EIGRP dispone de tres tablas principales:

- Tabla de Vecinos.
- Tabla de Topología.
- Tabla de Routing.

10.2.1. Creación de la tabla de vecinos

La tabla de vecinos se mantiene mediante el protocolo Hello.

El protocolo Hello informa a los vecinos que las conexiones están vivas y activas y mantiene el seguimiento de los paquetes enviados entre vecinos.

Hay que tener en cuenta que cada protocolo de capa 3 tiene su propia tabla de routing.

10.2.2. Contenidos de la tabla de vecinos

La tabla de vecinos comprende la siguiente información:

- **Dirección del vecino.**
- **El interfaz por el cual se ha recibido el hello del vecino.**
- **El holdtime:** Cuánto va a esperar en declarar al vecino muerto y borrarlo de la tabla. Su valor por defecto es de tres veces el tiempo de Hello.
- **El uptime:** Hace cuánto que se recibió el primer hello del vecino.
- **El número de secuencia:** Esta tabla hace un seguimiento de todos los paquetes que se envían entre vecinos. Su incremento es secuencial de uno en uno.
- **SRTT:** Tiempo que tarda en el paquete en enviarse al vecino y ser recibida su respuesta (en milisegundos).
- **RTO:** Calculado a partir del SRTT. Tiempo que el router esperará en un protocolo orientado a la conexión para reenviar el paquete.
- **El número de paquetes en la cola:** Con este parámetro el administrador puede controlar la congestión de la red.

10.2.3. Llegar a ser vecino

EIGRP utiliza una dirección de multicast 224.0.0.10 para que todos los routers puedan periódicamente enviar Hellos.

Si un Hello de un vecino conocido no se escucha dentro del tiempo predeterminado, entonces este pasa a holdtime¹, una vez pasado este tiempo se considera que el vecino está caído.

| | LAN | WAN |
|----------|--------|---------|
| Hello | 5 seg | 60 seg |
| Holdtime | 15 seg | 180 seg |

10.2.4. Condiciones para llegar a ser vecino

El router tiene que escuchar un paquete Hello o un ACK de su vecino.

El número de AS en la cabecera del paquete debe ser el mismo en los dos routers.

La configuración de la métrica debe ser la misma en los dos routers.

10.2.5. Creación de la tabla topológica

La tabla topológica tiene un registro con todas las rutas a las redes conocidas en la organización, no simplemente un conjunto de successors y feasible successors.

La tabla topológica incluye la siguiente información:

- Si la ruta es activa o pasiva.
- Que una actualización ha sido enviada a los vecinos.
- Que un paquete de query ha sido enviado a los vecinos. Si este campo es positivo, al menos una ruta se habrá marcado como active.

¹El Holdtime tiene un valor predeterminado de tres Hellos.

- Si se ha enviado un paquete de query, otro campo hará el seguimiento de si se han recibido respuestas de los vecinos.
- Que un paquete de respuesta se ha enviado como respuesta a un paquete de query de un vecino.
- Las redes remotas.
- El prefijo o máscara de la red remota.
- La métrica para la red remota, es decir, la FD.
- La métrica de la red remota anunciada por el siguiente salto lógico, el AD.
- El siguiente salto.
- El interfaz de salida pasa ser utilizado para alcanzar el siguiente salto lógico.
- Los successors, el camino a la red remota en saltos.

La tabla se construye con los paquetes de actualización que son intercambiados por los vecinos y las respuestas a las peticiones enviadas por el router.

Las peticiones y las respuestas utilizadas por DUAL de EIGRP se envían de forma confiable utilizando RTP.

Si un router no escucha un ACK dentro del tiempo determinado, se retransmite ese mismo paquete en unicast. Si no hay respuesta después de 16 intentos, el router marca al vecino como caído. Cada vez que el router envía un paquete, RTP incrementa el contador en una unidad. El router tiene que escuchar los ACKs de cada router antes de enviarle el siguiente paquete.

En el momento en el que el router tiene el conocimiento de la red, entonces se ejecuta DUAL.

10.2.6. Mantenimiento de la tabla topológica

Los siguientes aspectos hacen que la tabla topológica se recalcule.

El router escucha un cambio cuando una nueva red está disponible.

- La tabla topológica recibe una actualización que indica que existe una nueva red.
- Un interfaz directamente conectado a la red EIGRP se pone online.

El router cambia el successor en la tabla topológica y en la de routing.

- La tabla topológica recibe una respuesta a una petición de un vecino.
- Existe una configuración local de interfaces directamente conectados y ha cambiado el coste del enlace.

El router escucha un cambio de un vecino cuando la red pasa a no disponible.

- La tabla topológica recibe una petición, respuesta o actualización indicando que la red remota está caída.
- La de vecinos no recibe un hello tabladentro del holdtime.
- La red directamente conectada ha sufrido una pérdida de portado

La tabla topológica hace un seguimiento de los paquetes de EIGRP.

También identifica el estado de las redes en la tabla:

- Active: El router trata de encontrar otra ruta.
- Passive: El router no busca nada.

10.2.7. Añadir una red a la tabla topológica.

En el momento que el router pone una nueva red, esta empieza a enviar hellos por el nuevo interfaz. Aunque no haya vecinos la entrada se incluye porque es una nueva red.

EIGRP manda una actualización a sus vecinos informando de la nueva red, a la cual los vecinos contestan con el ACK correspondiente.

En el router receptor de la actualización: Actualiza el número de secuencia en la tabla de vecinos y añade la red a la tabla topológica. Calcula la FD y el successor para colocarlo en la tabla de routing. En ese momento envía la actualización a los vecinos.

10.2.8. Borrar una red de la tabla topológica

Si una red conectada a un router se desconecta, este router actualiza su tabla topológica y envía una actualización a sus vecinos.

Cuando el router receptor recibe la actualización, actualiza su tabla de vecinos y su tabla topológica.

Como este último router está programado para encontrar caminos alternativos, examina su tabla topológica para ello.

Si no encuentra un FS envía una petición a los vecinos. La ruta se marca como activa.

Se comienzan las queries y se actualizan las tablas de vecinos y topológica.

Se ejecuta DUAL tan pronto como el cambio de la red se registra.

Si no hay ruta alternativa, los vecinos contestan un reply de estado de query ya que no tienen camino alternativo.

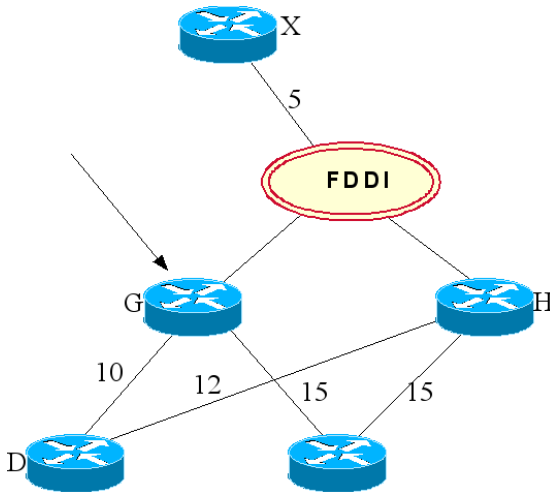
Llegados a este punto los vecinos empiezan a preguntar a sus vecinos para encontrar un FS.

Si ningún router tienen un FS entonces todos borran la entrada de la tabla de routing y de la de topología.

10.2.9. Encontrar un camino alternativo a una red remota

Ocasionalmente en enlaces lentos puede producirse que no se reciba una respuesta dentro del tiempo establecido. Esto hace que la ruta sea declarada SIA².

El vecino que ha fallado la respuesta de todas las queries se borra de la tabla de vecinos y DUAL asume que ha recibido una respuesta y le asigna un coste infinito.



Los siguientes puntos describen el proceso después de que G caiga.

- El Router D marca las rutas que no han llegado a G.
- El Router D busca en la tabla topológica, para determinar si existe una ruta alternativa, es decir, busca un FS.

²Stuck in Active (SIA): Estado de un router que ya ha enviado paquetes y está esperando los ACKs de sus vecinos.

- Se encuentra un FS. La tabla topológica tiene la AD y la FD para cada router.
- El Router D añade la ruta alternativa a Router X a través de Router H, sin poner la ruta en modo activo ya que la AD es menor que la FS. (AD=5, FS=15). Es necesario enviar actualización a los vecinos porque la métrica ha cambiado.
- Si el Router no tiene FS pondrá la ruta en modo activo mientras que se pregunta a otros routers por un camino alternativo.
- Después de mirar la tabla topológica, si se encuentra un FS, el vecino responde con el camino alternativo y se añade a la tabla topológica.
- En el último paso de DUAL la tabla de routing se actualiza.
- La red se vuelve a poner en estado pasivo hasta el próximo cambio en la red.
- Si un vecino al que se le ha preguntado no tiene camino alternativo o FS, colocará su red en modo activo y preguntará a sus vecinos.
- Si no existe respuesta, los mensajes se propagarán hasta el límite de la red.

10.2.10. Creación de la tabla de routing

La tabla de routing está construida desde la tabla topológica una vez se ha ejecutado DUAL.

La tabla topológica es donde se almacenan todas las rutas, y tras ejecutarse DUAL, las mejores pasan a la tabla de routing.

Una vez existe la tabla de routing ya se puede empezar a tomar decisiones de routing.

10.2.11. Métricas de EIGRP

Las métricas utilizadas en EIGRP son muy similares a las de IGRP. La diferencia principal es que EIGRP da el resultado en un campo de 32 bits.

Es posible utilizar hasta 6 caminos diferentes para un único camino. Existen tres tipos de caminos:

- Internal: Caminos internos al AS.
- Summary: Caminos internos que han sido sumarizados.
- External: Caminos externos al AS que han sido redistribuidos a EIGRP.

| Métrica | Valor de la Métrica | Valor por Defecto |
|---------|---------------------|-------------------|
| K1 | Bandwith | 1 |
| K2 | Loading | 0 |
| K3 | Delay | 1 |
| K4 | Reliability | 0 |
| K5 | MTU | 0 |

Si $K5=0$

$$métrica = K1 * bw + \frac{K2 * bw}{256 - load} + K3 * delay$$

Si $K \neq 5$

$$métrica = \frac{métrica * K5}{reliability + K4}$$

10.2.12. La tabla topológica y la máquina de estados finitos DUAL

DUAL es responsable del mantenimiento de la tabla de topología y de la creación de la tabla de routing.

El coste a una red de destino desde un router que la anuncia, más el coste a ese router es igual a la métrica hasta esa ruta.

La métrica o coste desde el vecino que la anuncia se llama AD (Advertised Distance).

La métrica desde el router local se llama FD (Feasible Distance).

Esto es fundamental para EIGRP porque si la $AD < FD$ significa que no hay bucles, ya que el siguiente salto está más cerca del destino.

10.2.13. Actualizando la tabla de routing en modo passive

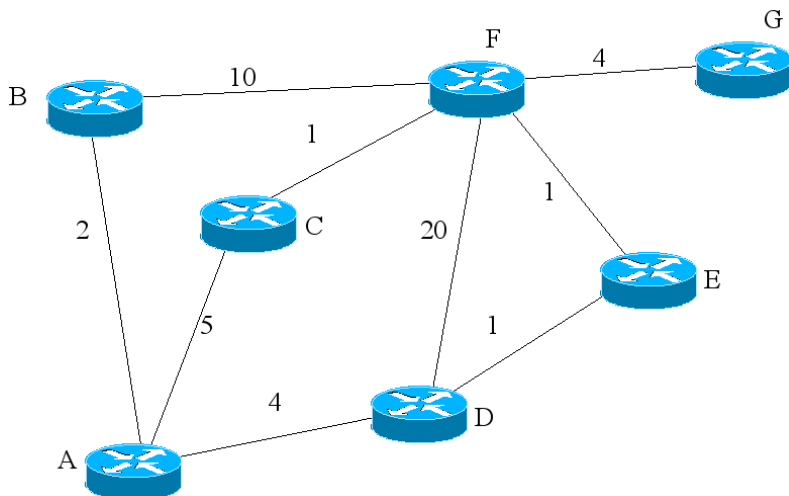
DUAL determina si existe una ruta aceptable en la tabla topológica para sustituir al camino en la tabla de routing.

Utilizando nomenclatura EIGRP: DUAL determina si es aceptable reemplazar un successor en la tabla de routing con un feasible successor de la tabla topológica.

Para que se produzca el cambio se tiene que cumplir:

- Que la $AD < FD$, a esto se la llama FC (Feasible Condition).
- Si se da la FC entonces la ruta pasa a ser FS (Feasible Successor).
- El FS con la menor métrica será el que reemplace a la ruta actual.

10.2.14. Feasible successor



Ejemplo de FS:

- Origen: A
- Destino: G
- Successor: C
- Feasible Successor: D

Ruta principal:

A – C – F – G

Ruta Secundaria:

A – D – E – F – G

Por B no se puede ir por que la AD a G que anuncia B=14 que es mayor que la FD de A = 10

Por D sí podría ir porque la AD a G que anuncia D=6 que es menor que la FD de A =10.

10.2.15. Actualizando la tabla de routing en modo activo

Cuando no se encuentra una ruta alternativa en la tabla de routing y todas las AD son mayores que la FD entonces no se cumple la FC y tenemos que entrar en modo active.

Una vez que está en active los routers vecinos ya pueden enviar sus AD y aunque sean mayores que la FD actual el router las aceptará.

Una vez aceptadas las rutas escogerá la de menor peso como successor.

Si existe otra que cumple la FC pasará a ser feasible successor.

10.2.16. Escoger un successor

Para determinar si el camino a una red remota es feasible, EIGRP considera la FC de la ruta.

Cada router mantiene una tabla de routing que contiene una lista de las redes disponibles y el mejor o más eficiente camino a cada una de ellas.

Un vecino puede llegar a ser FS para una ruta sólo si $AD < FD$, esto es uno de los conceptos fundamentales de DUAL para mantener la red libre de bucles.

Cuando un camino a una red remota se ha perdido, el router tiene que ser capaz de encontrar una ruta alternativa con un uso de recursos mínimos. Esto ayuda a una convergencia rápida.

10.3. Diseño de una red EIGRP

EIGRP está diseñado para trabajar en redes muy grandes. Sin embargo, al igual que OSPF, es sensible al diseño.

Los factores que pueden afectar a la escalabilidad de EIGRP son:

- La cantidad de información enviada entre vecinos.

- El número de routers que envían actualizaciones.
- Cómo de lejos están los routers que envían las actualizaciones.
- El número de caminos alternativos a redes remotas.

Si tenemos una red EIGRP que no puede escalar puede ser por:

- Una ruta es SIA.
- Congestión de red:
 - Delay.
 - Se ha perdido información de routing.
 - Rutas que están haciendo flapping.
 - Retransmisiones.
- El router se queda sin CPU o sin memoria disponible.
- Circuitos no confiables o unidireccionales.

10.3.1. Soluciones a los problemas de escalabilidad de EIGRP

Las direcciones tienen que ser contiguas para permitir la sumarización.

Utilizar un modelo jerárquico.

Los dispositivos de la red deben de tener suficientes recursos.

En los enlaces WAN tiene que haber suficiente ancho de banda.

La configuración de EIGRP en los enlaces WAN tiene que ser apropiada.

Se deben utilizar filtros.

Se debe de tener la red monitorizada en todo momento.

10.3.2. Consideraciones de diseño utilizando EIGRP

En enlaces lentos WAN, cuanto menos información de routing se envíe más capacidad quedará para tráfico para usuarios.

Sin embargo si se envía poca información de routing, los routers tendrán menos información para realizar decisiones de routing.

Estas dos consideraciones anteriores se tienen que sopesar.

EIGRP resume automáticamente en los límites de la red y en los límites de la red classful.

Para configurar sumariación manual primero es necesario deshabilitar la sumariación automática.

La sumariación se configura a nivel de interfaz.

Las queries limitarán la capacidad de crecimiento de EIGRP.

Para limitar el tráfico de queries se puede dividir el AS en varios AS.

Entre AS no se envían actualizaciones.

Muchas empresas utilizan los AS como si fueran áreas de OSPF redistribuyendo entre ellas, si se hace esto no se ha ganado nada.

La sumariación de rutas parará la propagación de ruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.

10.4. Configuración de EIGRP

EIGRP permite VLSM y sumariación, ya que la máscara se envía en el proceso de actualización.

EIGRP resume al límite de la red mayor.

Para sumarizar al número de IANA es necesario hacerlo manualmente.

EIGRP no sólo permite sumarizar en cada router sino que también permite sumarizar en cualquier interfaz.

10.4.1. Comandos requeridos en la configuración de EIGRP

El proceso de EIGRP: Es necesario arrancar el proceso de routing en el router.

El número del AS de EIGRP en el router: Todos los routers que compartan información de routing deben pertenecer al mismo AS.

Interfaces Participantes de los Routers: Como es posible que no queramos que todos los interfaces del router participen en EIGRP, entonces habilitaremos únicamente los interfaces que deseemos.

```
Router(config)#router eigrp número-de-AS
```

Habilita el protocolo de routing EIGRP e identifica el AS en el router.

```
Router(config-router)#network número-de-red [wildcard]
```

Habilita el interfaz deseado dentro de la red EIGRP.

En versiones anteriores a la 12.04(T) al escribir el número de red EIGRP lo mostraba como si se hubiera escrito la red classful.

El comando network identifica:

- Las actualizaciones se reciben por ese interfaz.
- Las actualizaciones se envían por ese interfaz.
- La red es anunciada por todos los interfaces EIGRP.
- Si es apropiado, el protocolo hello se propaga.

```
Router(config-router)#passive-interface interfaz
```

Previene que EIGRP reciba o transmita actualizaciones por el interfaz especificado.

10.4.2. Comandos opcionales en la configuración de EIGRP

- Sumarización en EIGRP.
- Routers Stub.
- Balanceo de Carga en EIGRP.
- Modificación del proceso de EIGRP.
- Modificación del intervalo de hello.
- Modificación del tiempo de espera de hello.
- Utilización del Ancho de Banda.
- Reglas para Configurar el Ancho de Banda en una Nube NBMA.
- Configuración de Ancho de Banda en una Red Punto Multipunto.
- Configuración de Ancho de Banda en una Red Multipunto Híbrida.
- Configuración en Punto en Punto.

10.4.2.1. Sumarización de EIGRP

La sumarización en EIGRP resuelve los problemas de escalabilidad. Con OSPF se diferencia en que OSPF sólo sumariza en el límite del área, EIGRP puede sumarizar en el interfaz.

Si no se configura sumarización EIGRP sumariza en al límite de la clase.

La sumarización reduce el monto de recursos necesarios por los routers en la red.

La sumarización también reduce las queries enviadas por el router.

Si se ha configurado sumarización, las queries encontrarán como límite el punto en el que ya no se vean.

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

Deshabilita la sumarización automática. El comando aplica a todo el router.

```
Router(config-if)#ip summary-address eigrp AS  
dirección máscara distancia-administrativa
```

Habilita la sumarización manual en un interfaz.

10.4.2.2. Routers Stub

Los Routers stub en redes EIGRP utilizan EIGRP para enviar información limitada entre los routers stub y el core.

Como en ODR, un router en la red EIGRP no tiene otros vecinos que no sea el de distribución.

Otra razón para configurar el router remoto como stub es aislar del resto de la red los SIA. Si hay una configuración stub, el router responde a las queries como inaccesible, de esta forma se evita que ocurra SIA.

```
Router(config-router)#eigrp stub [receive-only |  
connected | static | summary]
```

- **receive-only**: Sólo recibe actualizaciones del vecino.
- **connected**: Se anuncian las rutas directamente conectadas.
- **static**: Se anuncian las rutas estáticas.
- **summary**: Se anuncian las rutas sumarizadas.

10.4.3. Balanceo de carga en EIGRP

EIGRP automáticamente balancea la carga entre enlaces con el mismo coste.

Es posible configurar EIGRP para balancear el tráfico sobre enlaces con coste distinto utilizando el comando `variance`.

El comando `variance` permite al administrador identificar el ámbito de la métrica incluyendo caminos adicionales con el uso del parámetro `multiplicador`.

```
Router(config-router)#variance multiplicador
```

- El campo `multiplicador` por defecto es 1 y puede llegar a 128.
- Este campo identifica el ámbito en el cual se pueden utilizar las rutas, se multiplica el coste de la mejor ruta a un destino por el `multiplicador` y así obtenemos el umbral.

10.4.4. Modificación del proceso de EIGRP

Existen varias formas de modificar el comportamiento de una red, incluyendo balanceo de carga sobre varios caminos, sumarización de rutas, y reduciendo la frecuencia de actualización de los tiempos de actualización.

Cuanto menos hello se envíen más va a tardar en propagarse un error y aumentará el tiempo de convergencia.

Los Hello y los ACK utilizan RTP ya que se envían sólo modificaciones incrementales.

El proceso envía ruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.

Se puede configurar el temporizador de Hello y el Holdtimer, pero se debe de considerar la repercusión que esto tendrá en la red.

10.4.5. El temporizador de intervalo de Hello

Modificar el intervalo de Hello afecta a la disponibilidad de la red en cuanto a anunciar las modificaciones a los vecinos.

```
Router(config-if)#ip hello-interval eigrp AS segundos
```

Este comando se utiliza para decrementar el periodo de envío de hello en interfaces NBMA es muy útil, ya que en enlaces lentos (menos que un T1) se envían los Hello cada 60 segundos por defecto.

10.4.6. El temporizador de holdtime

Modificar el intervalo de Holdtime implica que se va a modificar el tiempo que puede esperar EIGRP sin recibir hello de sus vecinos.

Por defecto este tiempo es igual a 3 veces el tiempo de envío de Hello.

```
Router(config-if)#ip hold-time eigrp AS segundos
```

Este comando se utiliza para decrementar el periodo de envío de hello en interfaces NBMA es muy útil, ya que en enlaces lentos (menos que un T1) se envían los Hello cada 60 segundos por defecto.

10.4.7. Comandos opcionales sobre WANs

Los comandos `bandwidth` y `bandwidth-percent` son muy útiles para determinar la utilización de recursos de EIGRP al enviar sus actualizaciones.

Uno de los máximos beneficios de EIGRP y OSPF es su capacidad de enviar el mínimo tráfico posible.

Esta característica ayuda a decrementar el tiempo de convergencia.

10.4.8. Utilización de ancho de banda por EIGRP

EIGRP no utiliza más del 50 % del ancho de banda del enlace para información de routing.

El comando `bandwidth` utilizado en los routers Cisco permite establecer los valores de ancho de banda que utilizará el protocolo para sus cálculos.

El ancho de banda (`bandwidth`) es una construcción lógica que tiene implicaciones en la función del router. Esto no modifica el ancho de banda del router.

10.4.9. Reglas de configuración del `bandwidth` en nube NBMA

Cisco identifica tres reglas que se deben seguir cuando se configura EIGRP sobre una nube NBMA.

- El tráfico EIGRP no debe exceder la capacidad del Committed Information Rate (CIR) del Circuito Virtual (VC).
- El tráfico agregado de EIGRP sobre el VC no debe exceder la velocidad de la línea y/o del interfaz.
- El ancho de banda de EIGRP en cada VC debe ser el mismo en ambas direcciones.

10.4.10. Configuración del `bandwidth` sobre una red punto multipunto

La configuración del comando `bandwidth` en una nube NBMA depende del diseño de los VCs.

Si la línea serie tiene varios VCs en la configuración multipunto, EIGRP distribuirá su carga entre los VCs.

El comando `bandwidth` deberá pues reflejar la velocidad del enlace en la nube Frame Relay.

10.4.11. Configurar el ancho de banda en una red híbrida multipunto

Si la red multipunto tiene varias velocidades en los VCs es necesaria una solución más compleja:

Utilizar el CIR más pequeño y configurar el comando `bandwidth` en el interfaz. Esta solución no puede ser la más óptima.

Si es posible, es mucho más sencillo configurarlo utilizando subinterfaces, donde configuramos el `bandwidth` en cada subinterfaz.

```
Router(config)#interface interfaz subinterfaz
Router(config-subif)#bandwidth ancho-de-banda
```

10.4.12. Configurar una red pura punto a punto

Si hay varios VCs, tiene que haber suficiente ancho de banda para soportar el tráfico de EIGRP.

Los subruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.

En este caso el comando `ip bandwidth-percent eigrp` es adecuado.

El comando `ip bandwidth-percent eigrp` interactúa con el comando `bandwidth` del interfaz.

```
Router(config)#interface interfaz subinterfaz
Router(config-subif)#ip bandwidth-percent eigrp
    porcentaje-del-bandwidth
```


10.5. Verificación de la configuración de EIGRP

```
show ip eigrp neighbors
```



The screenshot shows a terminal window titled 'edu@zebra:~ - Terminal - Konsole'. The command 'routerA#show ip eigrp neighbors' has been executed, resulting in the following output:

```
routerA#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address           Interface    Hold Uptime    SRTT   RTT  Q   Seq Type
  Address           Interface    (sec)         (ms)      Cnt  Num
2   192.190.10.2       Se0.3        10 00:25:57    49    294  0   14
0   192.170.10.2       Se0.1        13 00:47:31   166    996  0   10
1   192.180.10.2       Se0.2        11 02:14:54    51    306  0    8
routerA#
```

Process: Muestra el AS en el cual está funcionando EIGRP.

Address: Dirección IP del vecino EIGRP.

Interface: Interfaz por el que se ha recibido el hello.

Holdtime: Tiempo en segundos que el router esperará para escuchar el siguiente hello.

Uptime: Tiempo transcurrido desde que se ha recibido el primer hello.

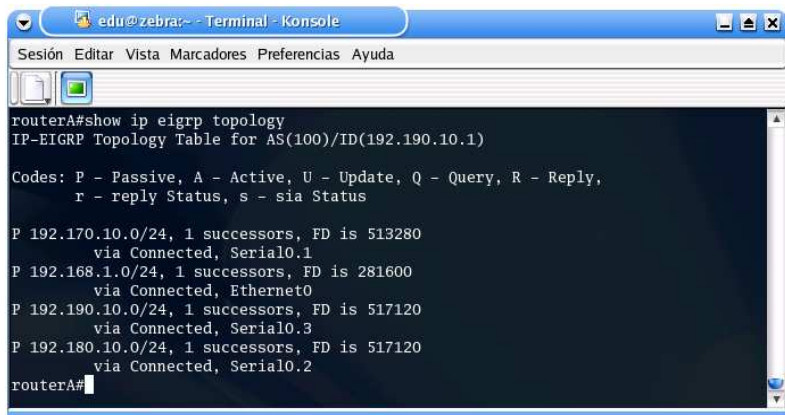
Q Count: Número de paquetes EIGRP que el router tiene encolados.

Seq Num: Número de secuencia del último paquete que se ha recibido.

SRTT: Smooth Round-Trip Time. Tiempo en milisegundos y medido desde el envío del paquete al receptor.

RTT: Retransmission TimeOut. Medido en milisegundos. Muestra cuanto esperará a recibir la respuesta antes de reenviar.

```
show ip eigrp topology
```



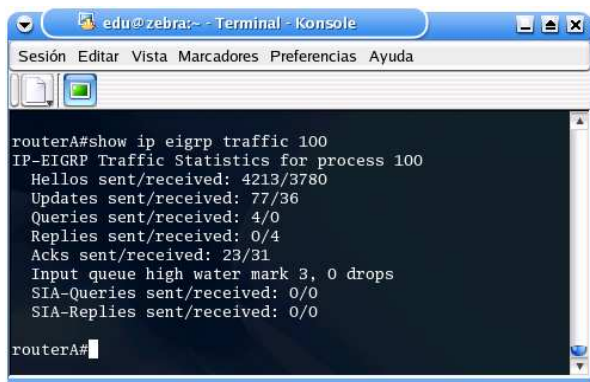
A terminal window titled 'edu@zebra:~ - Terminal - Konsole' with a menu bar (Sesión, Editar, Vista, Marcadores, Preferencias, Ayuda) and a toolbar. The terminal displays the output of the command 'routerA#show ip eigrp topology'. The output shows the IP-EIGRP Topology Table for AS(100)/ID(192.190.10.1) and lists four routes with their successors and FD values.

```
routerA#show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(192.190.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.170.10.0/24, 1 successors, FD is 513280
   via Connected, Serial0.1
P 192.168.1.0/24, 1 successors, FD is 281600
   via Connected, Ethernet0
P 192.190.10.0/24, 1 successors, FD is 517120
   via Connected, Serial0.3
P 192.180.10.0/24, 1 successors, FD is 517120
   via Connected, Serial0.2
routerA#
```

```
show ip eigrp traffic
```

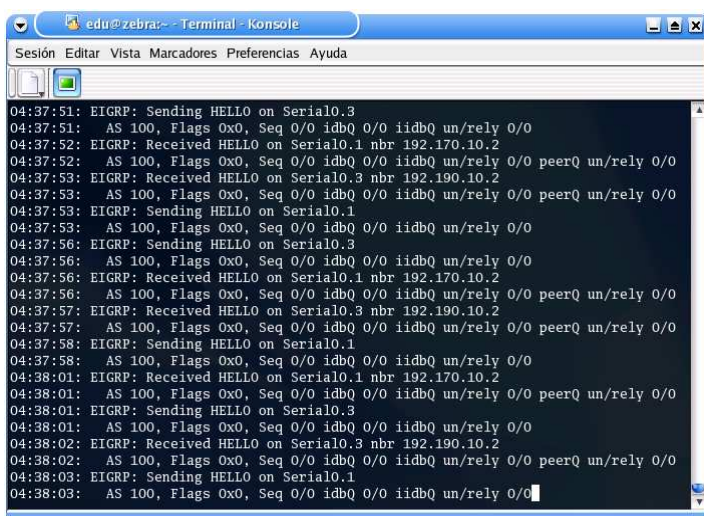


A terminal window titled 'edu@zebra:~ - Terminal - Konsole' with a menu bar (Sesión, Editar, Vista, Marcadores, Preferencias, Ayuda) and a toolbar. The terminal displays the output of the command 'routerA#show ip eigrp traffic 100'. The output shows IP-EIGRP Traffic Statistics for process 100, including counts for Hellos, Updates, Queries, Replies, Acks, and SIA-Queries/SIA-Replies sent and received.

```
routerA#show ip eigrp traffic 100
IP-EIGRP Traffic Statistics for process 100
  Hellos sent/received: 4213/3780
  Updates sent/received: 77/36
  Queries sent/received: 4/0
  Replies sent/received: 0/4
  Acks sent/received: 23/31
  Input queue high water mark 3, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
routerA#
```

10.6. Troubleshooting de la operación de EIGRP

- `debug eigrp packet`: Muestra los paquetes enviados y recibidos por el router. Se puede escoger el paquete que queremos monitorizar (existen 11).
- druta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.
- Un `predebug eigrp neighbors`: Muestra los paquetes hello enviados y recibidos por el router y los vecinos descubiertos en el proceso.
- `debug ip eigrp route`: Muestra los cambios que se van produciendo en la tabla de routing (activado por defecto).
- `debug ip eigrp summary`: Muestra el proceso tomado cuando la sumarización ha cambiado en el router.



```

04:37:51: EIGRP: Sending HELLO on Serial0.3
04:37:51: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0
04:37:52: EIGRP: Received HELLO on Serial0.1 nbr 192.170.10.2
04:37:52: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0 peerQ un/rely 0/0
04:37:53: EIGRP: Received HELLO on Serial0.3 nbr 192.190.10.2
04:37:53: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0 peerQ un/rely 0/0
04:37:53: EIGRP: Sending HELLO on Serial0.1
04:37:53: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0
04:37:56: EIGRP: Sending HELLO on Serial0.3
04:37:56: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0
04:37:56: EIGRP: Received HELLO on Serial0.1 nbr 192.170.10.2
04:37:56: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0 peerQ un/rely 0/0
04:37:57: EIGRP: Received HELLO on Serial0.3 nbr 192.190.10.2
04:37:57: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0 peerQ un/rely 0/0
04:37:58: EIGRP: Sending HELLO on Serial0.1
04:37:58: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0
04:38:01: EIGRP: Received HELLO on Serial0.1 nbr 192.170.10.2
04:38:01: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0 peerQ un/rely 0/0
04:38:01: EIGRP: Sending HELLO on Serial0.3
04:38:01: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0
04:38:02: EIGRP: Received HELLO on Serial0.3 nbr 192.190.10.2
04:38:02: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0 peerQ un/rely 0/0
04:38:03: EIGRP: Sending HELLO on Serial0.1
04:38:03: AS 100, Flags 0x0, Seq 0/0 idbq 0/0 iadbq un/rely 0/0

```


Capítulo 11

BGP

11.1. Introducción a BGP

BGP es un protocolo extremadamente complejo utilizado a través de Internet y dentro de empresas multinacionales.

La función de un protocolo de routing de pasarela externa, como BGP, no es encontrar una red específica, sino proporcionar información que permita encontrar el AS en el cual se encuentra dicha red.

El protocolo de routing de pasarela interna (RIP, IGRP, EIGRP, IS-IS, OSPF...) es el encargado de encontrar la red específica que se está buscando

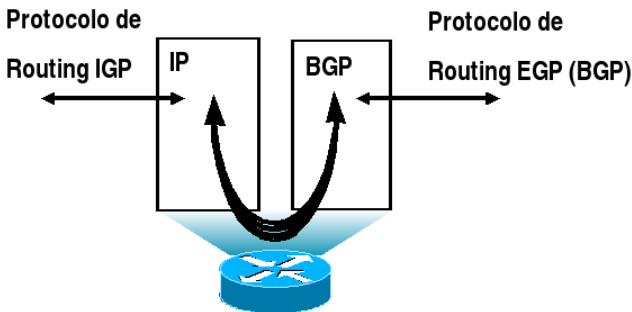
11.1.1. Características de BGP

Estas características demuestran por qué este protocolo es el mejor para routing exterior.

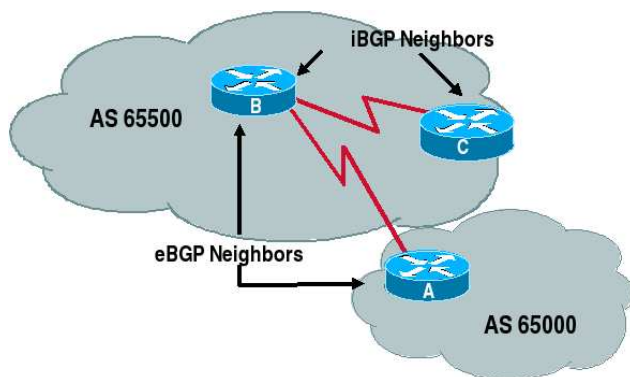
Las claves principales de BGP incluyen:

- Es un protocolo de routing path vector.

- BGP soporta VLSM, CIDR y sumarización.
- En el inicio de la sesión se envían actualizaciones completas; las actualizaciones por disparo se envían posteriormente.
- Se crean y mantienen las conexiones entre peers utilizando el puerto 179/TCP.
- La conexión se mantiene por keepalives periódicos.
- Cualquier cambio en la red resulta una actualización por disparo.
- Las métricas utilizadas por BGP, llamadas atributos, permiten gran granularidad en la selección del camino.
- El uso de direccionamiento jerárquico y la capacidad de manipular el flujo de tráfico son unas de las características que permiten al diseño de la red crecer.
- BGP tiene su propia tabla de routing, sin embargo es capaz de compartir y preguntar sobre la tabla de routing IP interior.
- Es posible manipular el flujo de tráfico utilizando atributos. Esto significa que una ruta no puede enviar tráfico si el siguiente salto no quiere.



- Una de las mayores caruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.
- Un prracterísticas distintivas de BGP son sus actualizaciones.
- A BGP no le interesa comunicar un conocimiento de cada subred de la organización, sólo le interesa utilizar suficiente información para encontrar un AS.
- Las actualizaciones de routing de BGP lleva la sumarización al extremo comunicando únicamente los números de los AS, prefijos de direcciones agregadas e información de routing basada en políticas.
- BGP asegura la fiabilidad del transporte llevando sus actualizaciones de routing y sincronizando las actualizaciones de routing.
- BGP puede ser implementado de diferentes formas:
 - Entre AS: En este momento actúa como un protocolo de pasarela exterior, entonces lo llamaremos eBGP.
 - Dentro de una AS: BGP se puede utilizar para llevar información exterior entre routers eBGP que residen en el mismo AS, entonces lo llamaremos iBGP.

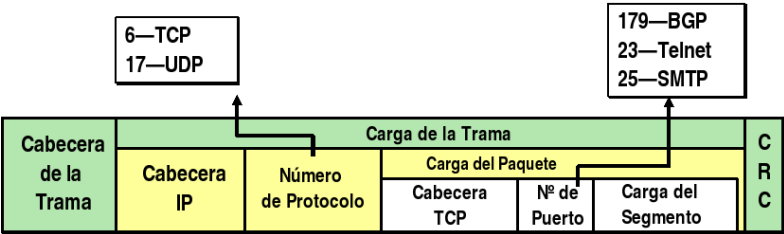


Comparativa de protocolos:

| Protocolo | Interior o Exterior | Vector Distancia o Estado del Enlace | Jerarquía Requerida | Métrica |
|-----------|---------------------|--------------------------------------|---------------------|--------------------------|
| OSPF | Interior | Estado del Enlace | Sí | Coste |
| EIGRP | Interior | VD Avanzado | No | Compuesta |
| BGP | Exterior | Vector Distancia | No | Path vectors o atributos |
| IS-IS | Interior | Estado del Enlace | Sí | Coste |

BGP es un protocolo de routing avanzado vector distancia.

- Utiliza TCP para gestión de la sesión fiable.
- Utiliza el puerto 179/TCP.



11.1.2. Terminología de BGP

Agregación: El término de BGP para sumarización.

Atributo: Similar a la métrica, define características del camino al destino. Estas características pueden ser utilizadas para tomar decisiones sobre el camino a tomar.

Sistema Autónomo: Definición de los límites de la red. El AS define todos los routers dentro del dominio administrativo, donde cada router tiene un conocimiento de las redes en el dominio. Si se utiliza BGP para interconectar AS, cada AS debe tener una numeración única asignada por las comunidades de direccionamiento de Internet.

Exterior Gateway Protocol (EGP): Término genérico para un protocolo que funciona entre diferentes AS.

Interior Gateway Protocol (IGP): Protocolo de routing que funciona dentro de un AS.

Internal BGP (iBGP): Cuando BGP se utiliza dentro de un AS. Para ser vecinos los routers no tienen por qué ser físicamente adyacentes. iBGP se utiliza entre routers eBGP del mismo AS.

Originator-ID: Atributo de BGP opcional no transitivo que se crea por los route reflectors. Este atributo contiene el router-ID del router que ha originado la actualización. El propósito de este atributo es prevenir bucles de routing. Si el router que lo ha originado recibe su actualización la ignorará.

Policy-based routing: Permite al administrador programar el protocolo de routing definiendo cómo se va a enrutar el tráfico. Es una forma de routing estático forzado por unos ACLs llamados route maps. El Policy-Based Routing (PBR) es independiente al protocolo y utiliza route mruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.

Prefix list: Los prefix list se utilizan como alternativa a los distribute list para controlar cómo BGP aprende las actualizaciones anunciadas. Los prefix list son más rápidos, más flexibles y menos intensivos de procesador que los distribute list.

Route reflector: Router que está configurado para reenviar rutas desde otros clientes identificados iBGP, esto elimina la necesidad de la red totalmente mallada iBGP, preservando los recursos de la red. Una red totalmente mallada tiene el problema de la sobrecarga y la dificultad de ser escalable.

Route reflector client: El cliente es un router que tiene sesiones TCP con su peer iBGP que actúa como route reflector. Reenvía rutas al route reflector, el cual propaga estas a los demás routers. El cliente no tiene otros peers.

Route reflector cluster: Un cluster es un grupo consistente de route reflector y clientes. Puede haber más de un route reflector.

Synchronization rule: Esta regla hace que un router no puede reenviar una ruta al peer eBGP a no ser que la ruta se encuentre en su tabla de routing IP local. Esto requiere que el routing IGP y BGP esté sincronizado, así se previene a BGP de anuncios de rutas dentro de AS que no puedan ser direccionadas directamente.

Si BGP está totalmente mallado no es necesario utilizar tablas IGP y la sincronización puede ser deshabilitada con el comando:

```
Router(config-router)#no synchronization
```

Transit Autonomous System: AS que se utiliza para transportar tráfico BGP a otro AS. No existe tráfico BGP destinado a este AS, simplemente este AS permite que el tráfico pase a través de el.

11.1.3. Cuándo utilizar BGP

Existen situaciones específicas en las que es necesario utilizar BGP:

- La organización se conecta a múltiples ISPs o ASs, se justifica el coste adicional utilizando estos enlaces reduciendo cuellos de botella y congestión. En este caso se necesitan decisiones de routing basadas en política basadas en el enlace.
- La política de routing del ISP y el de la organización difieren y es necesario que exista comunicación.

- El tráfico de la organización necesita diferenciar qué tráfico es de cada ISP.
- La organización es un ISP, y debido a la naturaleza del negocio es necesario que el tráfico de otros ASs circule por el AS de la organización, funcionando como AS de tránsito. ruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.

11.1.4. Cuándo no utilizar BGP

Una red simple es una red que es fácilmente gestionable y mantenible, lo cual es razón para evitar la utilización de BGP.

- El ISP y la organización tienen la misma política de routing.
- Aunque la organización tenga varias conexiones a Internet, no está previsto utilizar más de una simultáneamente.
- Existen recursos limitados, como CPU o memoria en los routers.
- El ancho de banda en el AS es bajo, y la utilización de información de routing adicional repercutirá en un ancho de banda disponible más bajo para tráfico de datos.

11.2. Introducción a la operación de BGP

BGP es un orientado a la conexión.

Cuando los vecinos “se ven”, se establece y se mantiene una sesión de peering BGP.

BGP envía keepalives periódicamente para mantener el enlace y la sesión.

Estos keepalives son la cabecera de 19 bytes de la cabecera de BGP utilizada en las actualizaciones.

Una vez que se ha establecido la sesión, las tablas de routing son intercambiadas y sincronizadas.

En ese momento los routers se envían actualizaciones incrementales sólo cuando hay cambios.

La actualización consiste en un único path y las redes que pueden ser alcanzadas por ese path.

Una vez corregida la tabla de routing, el proceso de BGP propaga los cambios a todos los vecinos, asegurándose que no hay bucles.

11.2.1. Mensajes utilizados en BGP

Open messages: Utilizados para establecer conexiones con peers.

Keepalives: Enviados periódicamente entre peers para mantener las conexiones y verificar los paths que el router tiene enviando el keepalive. Si el temporizador se configura a 0, esto igual a infinito, y no se envían keepalives.

Update messages: Contiene paths a redes de destino y los atributos del path. Hay un path por actualización, requiriendo muchas actualizaciones para múltiples paths. La información contenida en las actualizaciones incluyen los atributos del path como el origen, path del AS, vecino, o la métrica entre AS.

Notificación: Utilizado para informar al router receptor de los errores que causan que se cierre la conexión.

11.2.2. CIDR y agregación de rutas

BGP necesita comunicar mucha información entre los sistemas autónomos, pero no toda es necesaria. Si el diseño de la red permite sumarización se pueden reducir la necesidad de recursos (CPU, memoria) durante la actualización de rutas.

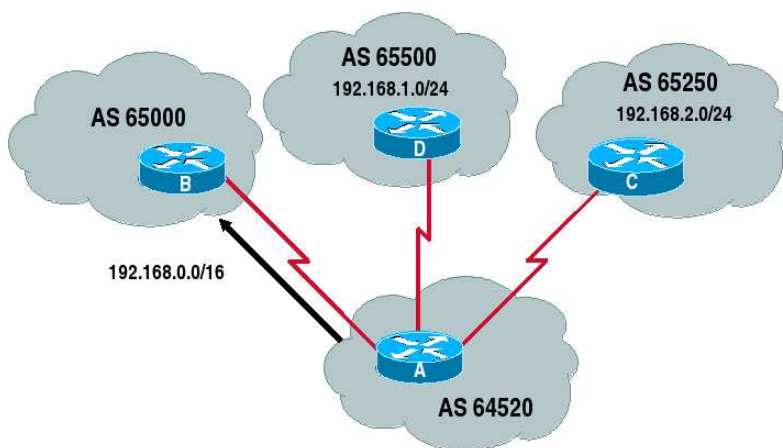
CIDR es una de las soluciones implementada en los últimos años, lo cual constituye un método de consolidar direcciones en unas pocas sumarizadas.

La sumarización reduce el número de bits de prefijo e incorpora otras redes que compartan ese prefijo en una única dirección.

BGP propaga el prefijo y la máscara, permitiendo un diseño jerárquico y reduciendo los recursos de la red.

Un router puede estar por defecto en el AS y una ruta estática es el AS del ISP o de la organización.

Un router puede enviar rutas agregadas, rutas que no hayan sido agregadas o ambas.



Las rutas pueden ser agregadas cuando pasan a través de un AS.

11.2.3. BGP y routing basado en políticas

Routing Basado en Políticas proporciona al administrador la capacidad de definir cómo será enrutado el tráfico a través del AS.

El Routing Basado en Políticas es un tipo de routing estático forzado por access lists, incluyendo route maps, distribute lists, prefix lists, y filter lists. Esta práctica influye en la tabla de routing tanto entrante como saliente.

Mediante muchas variables o atributos, en BGP se puede influir en el routing dinámico, al administrador se le proporciona un gran nivel de control.

Esta característica distingue a BGP del resto de los protocolos de routing.

11.2.4. Reglas del routing basado en políticas

BGP puede implementar alguna de las siguientes reglas asociadas con el paradigma hop-by-hop. Este paradigma tiene la capacidad de influir en como el router elige al next-hop. Esto afecta al path completo.

Las reglas son las siguientes:

- El tráfico puede ser dirigido basándose en la dirección de origen, la de destino o ambas.
- El Routing Basado en Políticas (PBR) afecta sólo al next-hop en el path al destino.
- El PBR no afecta al destino del paquete. Afecta al camino tomado al destino.
- El PBR no permite que el tráfico enviado a otro AS tome otro camino que el elegido por el AS.
- Es posible influir únicamente en como alcanzar al vecino, no cómo enrutarse por el AS.
- El PBR examina la dirección de origen, la cual se configura en el interfaz de entrada.

11.3. Atributos de BGP

La clave de BGP es su capacidad de desviar el tráfico basándose en criterios determinados por los arquitectos de la red. BGP tiene que ver con la capacidad de manipular el flujo de tráfico a través de la red.

Estas características pueden ser utilizadas para distinguir los paths (caminos) al utilizar PBR. Así que la PBR utiliza los atributos de BGP para tomar decisiones sofisticadas en la selección del path.

BGP direcciona el flujo de tráfico utilizando atributos.

El uso de atributos se refiere al uso de variables en la selección del mejor camino para el protocolo de ruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.

BGP utiliza atributos para seleccionar el mejor camino. Básicamente los atributos son la métrica de BGP.

Las variables describen características o atributos del camino al destino.

Mucha información transportada en los mensajes de actualización es más importante que otra.

Ya que la información de BGP en las actualizaciones varía en la red, la categorización es muy importante.

Los atributos se dividen en dos partes:

- Well-known: Atributos que su utilización es obligatoria
- Optional: Atributos opcionales.

Además cada una de las dos divisiones se dividen a su vez en dos más, permitiendo así una mayor granularidad.

11.3.1. Categorías de los atributos de BGP

Well-known

- **Mandatory:** Estos atributos son requeridos y deben ser reconocidos por todas las implementaciones de BGP.
- **Discretionary:** Estos atributos no son requeridos, pero en el caso de estar presentes todos los routers que ejecuten BGP tiene que reconocerlos y actuar en la información que contienen.

Optional

- **Transitive:** El router no debe de reconocer estos atributos, pero si este es el caso, marcará la actualización como parcial y enviará la actualización completa con los atributos, al siguiente router. Los atributos atraviesan el router sin ser cambiados, si no son reconocidos.
- **Nontransitive:** Estos atributos son eliminados si caen en un router que no entiende o reconoce los atributos. Estos atributos no serán propagados al peer BGP.

Los Atributos de BGP incluyen:

- AS-path *
- Next-hop *
- Local preference
- Multi-exit discriminator (MED)
- Origin *
- Community
- Weight **

- Atomic Aggregate *
- Aggregator
- Originator ID
- Cluster ID

* = Atributos Well-Known mandatory

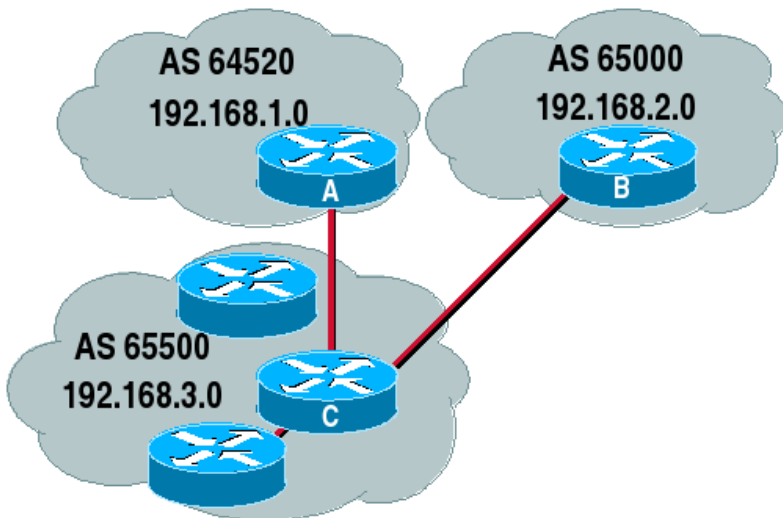
** = Propietario de Cisco Systems

11.3.2. Atributo AS_Path

Well-known, mandatory, código 2, preferencia el camino más corto.

Lista con todos los ASs que la ruta tiene que atravesar.

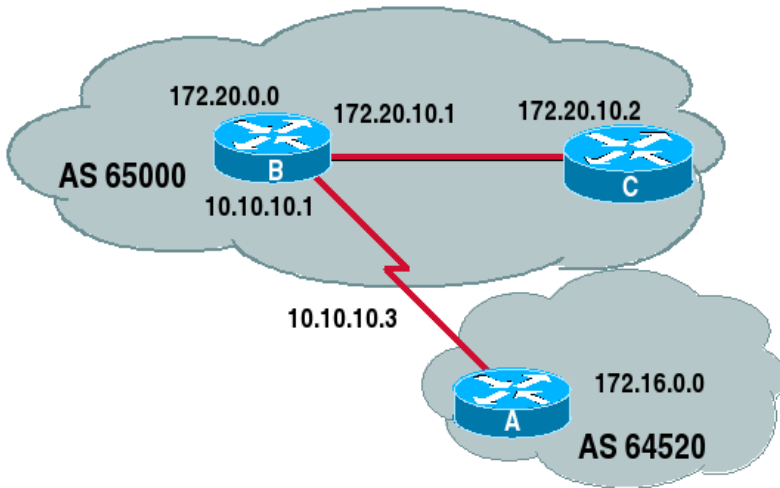
p.e. El Router B, el path a 192.168.10 es la secuencia de AS 65500 64520.



11.3.3. Atributo Next Hop

Well-known, mandatory, código 3, preferencia el camino más corto. Siguiente salto para alcanzar la red.

- El Router A anuncia la red 172.16.0.0 al router B en eBGP, con un next hop 10.10.10.3.
- El Router B anuncia 172.16.0.0 en iBGP al Router C, manteniendo 10.10.10.3 como la dirección del next hop.

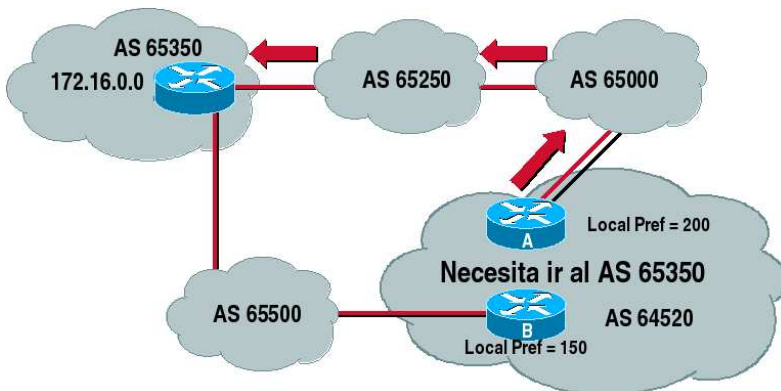


En eBGP, es la dirección que ha originado la actualización de routing del otro AS.

En iBGP, para las rutas originadas fuera del AS, se mantiene como next hop la dirección que ha originado la actualización del otro AS.

11.3.4. Atributo Local Preference

Well-known, discretionary, código 5, preferencia valor mayor.



Los Paths con el mayor valor de la preference son deseados.

Preference configurada en los routers.

Preference enviada únicamente a vecinos iBGP.

Este atributo se utiliza para decirle a los otros routers dentro del AS como salir del AS en caso que tengamos varias posibilidades.

Es el opuesto al atributo MED.

Este valor se pasa únicamente entre vecinos iBGP

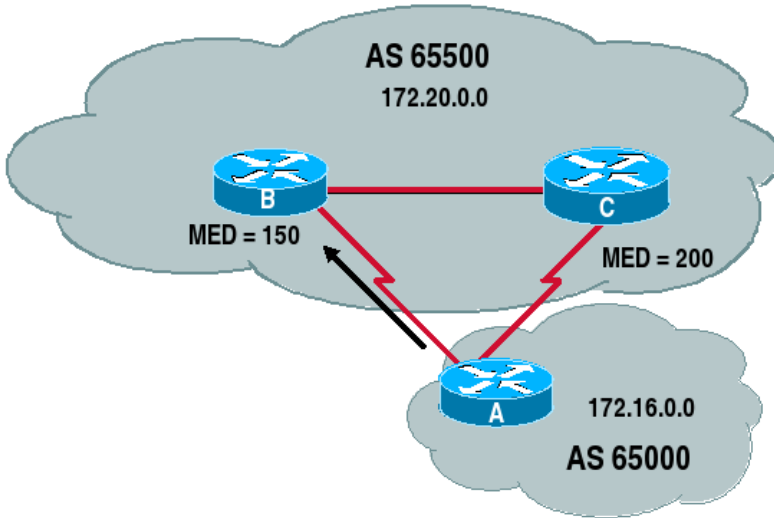
11.3.5. Atributo MED (Multiple Exit Discriminator)

Este atributo informa a los routers de fuera del AS que camino tomar para entrar en el AS.

El MED es conocido como la métrica externa de una ruta.

MED se pasa entre ASs, pero no se propagará a ASs terceros.

Optional, nontransitive, código 4, preferencia menor valor.



Paths con el MED (también llamado métrica) menor son deseables:

- El MED se configura en los routers.
- MED se envía únicamente a los vecinos eBGP.

11.3.6. Atributo Origin

Well-known, mandatory, código 1, preferencia código origen menor, donde $IGP < EGP < Incomplete$.

Identifica el origen de la actualización de routing.

IGP (i)

- Comando **network**.

EGP (e)

- Redistribuido desde EGP.

Incomplete (?)

- Redistribuido desde IGP o ruta estática.

El path se origina dentro del AS. Se crea con el comando de iBGP network. La ruta se marca en la tabla de routing BGP con una “i”. Si el origen es un protocolo de routing exterior, se marcará con una “e” en la tabla de routing de BGP.

La ruta puede haber sido redistribuida en BGP, por tanto tener información incompleta. La ruta se marcará como “?”.

11.3.7. Atributo Community

Optional, transitive, código 8, preferencia no existente porque no es utilizada en la selección del path.

Esta es la capacidad de etiquetar ciertas rutas que tiene algo en común.

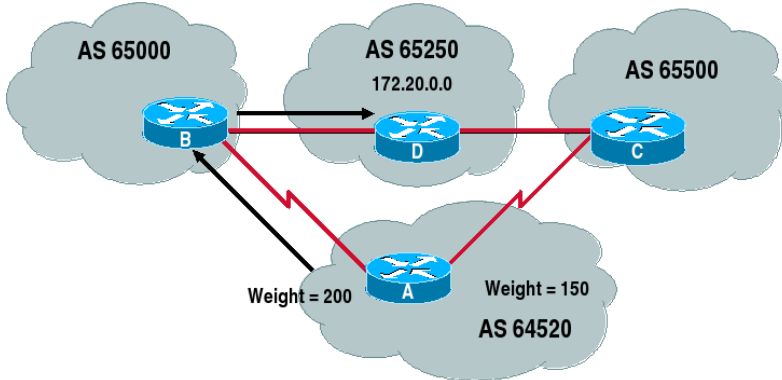
Se suele utilizar en conjunción con otros atributos que afecten a la selección de la ruta para la community.

Las communities no tienen límites geográficos o lógicos.

BGP puede filtrar en el interfaz de entrada o en el de salida las rutas para redistribución o selección de path.

11.3.8. Atributo Weight¹

Definido por Cisco, preferencia el valor mayor.



Paths con el valor del weight más alto serán deseables

El Weight se configura en los routers, basándose en el vecino

El Weight no se envía a ningún vecino BGP, así que no tiene código.

11.3.9. Atributo Atomic Aggregate

Well-known, discretionary, código 6, preferencia no existente porque no es utilizada en la selección del path.

El router que ha originado de la ruta agregada.

Útil porque muestra información que ha sido perdida al realizar la agregación de rutas.

11.3.10. Atributo Aggregator

Optional, nontransitive, código 7, preferencia no existente porque no es utilizada en la selección del path.

¹Propietario de Cisco Systems

Este atributo muestra el Router ID y el número de AS del router responsable de la agregación de la ruta.

Este atributo incluirá una lista de todos los ASs que las rutas agregadas han atravesado.

Muestra al receptor, en otro AS, el router que ha originado la ruta agregada.

11.3.11. Atributo Originator ID

Optional, nontransitive, código 9, preferencia no existente porque no es utilizada en la selección del path.

El route reflector añade este atributo.

Lleva el Router ID en el AS local.

Se utiliza para prevenir bucles.

11.3.12. Atributo Cluster ID

Optional, nontransitive, código 10, preferencia no existente porque no es utilizada en la selección del path.

Identifica a los routers envueltos en la route reflection.

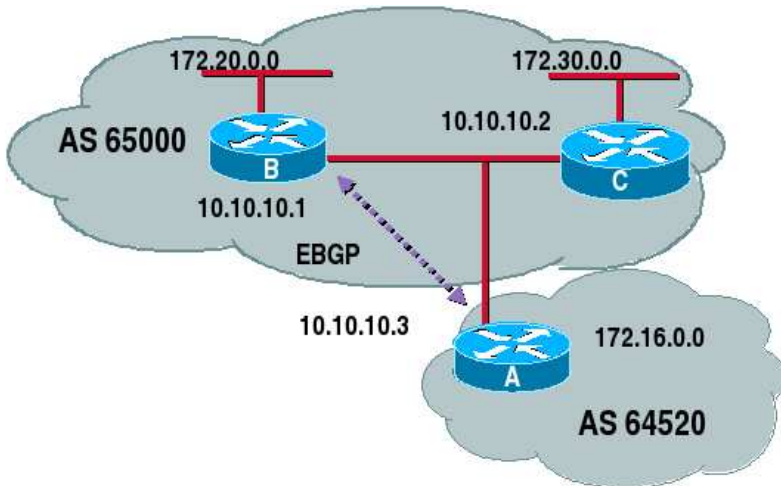
El cluster muestra el reflection path que se ha tomado.

Se utiliza para evitar errores de bucles.

11.3.13. Ejemplos

11.3.13.1. El atributo Next Hop en una red de broadcast multiacceso

En una red de broadcast multiacceso.



- El Router B anunciará la red 172.30.0.0 al Router A en eBGP, con el next hop de 10.10.10.2, no 10.10.10.1.
- Esto evita un salto innecesario.

En eBGP el next hop es la dirección IP del router que anuncia el AS. La dirección IP se especifica con el comando `network`.

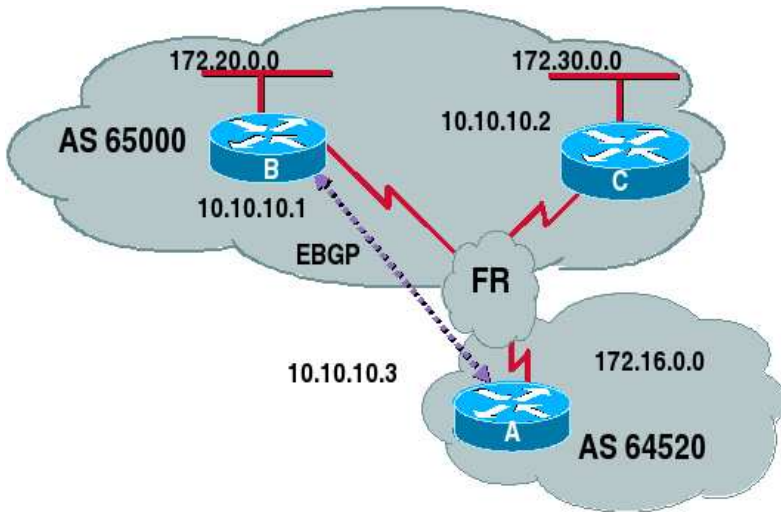
En un entorno de multiacceso si la ruta viene de otro router se puede anunciar el next hop con la dirección del otro router, esto evita que se den más vueltas de las necesarias.

La regla es: La dirección del route que originalmente envía la actualización en un entorno de multiacceso se mantiene como next hop.

11.3.13.2. El atributo Next Hop en una red NBMA

En NBMA se cumplen las mismas reglas que en entornos de mutliacceso broadcast.

Sin embargo si no existe conectividad directa entre los routers se puede evitar que el router anuncie el next hop con la dirección de otro router mediante comandos.



En una red NBMA:

- Por defecto, el Router B anunciará la red 172.30.0.0 al Router A en eBGP con un next hop de 10.10.10.2, no de 10.10.10.1.
- Puede ser sobrescrita.

11.3.14. Mensajes de BGP

BGP define los siguientes tipos de mensajes:

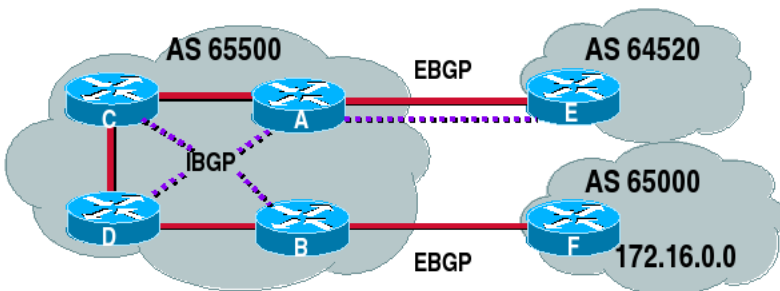
- Open:
 - Incluye el holdtime y el Router ID de BGP.
- Keepalive:

- Update
 - Información para un único path (puede tener varias redes).
 - Incluye los atributos del path y las redes.
- Notification
 - Cuando se detecta un error.
 - Conexión BGP cerrada después de enviar.

11.3.15. Sincronización de BGP

Regla de sincronización: No utilizar, o anunciar a un vecino externo, una ruta aprendida por iBGP, hasta que no se haya aprendido de IGP.

- Asegura consistencia de la información a través del AS.
- Evita agujeros negros en el AS.
- Es más seguro desactivar la sincronización cuando todos los routers del AS están ejecutando BGP porque todos los routers han aprendido esa ruta mediante IGP.



Todos los routers en el AS 6550 están ejecutando BGP; no encuentran rutas IGP.

Si la sincronización está activa (por defecto), entonces:

- Los Routers A, C, y D no utilizarán o anunciarán la ruta a 172.16.0.0 hasta que reciban la matching route vía un IGP.
- El Router E no sabrá de la existencia de 172.16.0.0.

Si la sincronización está desactivada, entonces:

- Los Routers A, C y D utilizarán y anunciarán la ruta que han recibido vía iBGP; El Router E conocerá la existencia de 172.16.0.0.
- Si el Router E envía tráfico para la red 172.16.0.0, los Routers A, C y D encaminarán los paquetes correctamente al Router B.

11.3.16. Proceso de selección de ruta

Considerando únicamente rutas sincronizadas sin bucles en el AS y con un next hop válido, entonces:

1. Se prefiere el weight mayor (local del router y propietario de Cisco).
2. Se prefiere la local preference mayor (global del AS).
3. Se prefiere la ruta originada por el router local.
4. Se preruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.
5. Se Prefiere el AS_Path más corto.
6. Se prefiere el Origin más pequeño (IGP < EGP < incomplete).

7. Se prefiere el MED más pequeño (desde otro AS).
8. Se prefiere el path eBGP sobre el path iBGP.
9. Se prefiere el path a través del vecino IGP más cercano.
10. Se prefiere la ruta más antigua de los paths eBGP.
11. Se prefiere el path con el vecino BGP que tenga el Router ID más bajo .
12. Se prefiere el camino con el vecino BGP que tenga la dirección IP más baja.

11.4. Configuración básica de BGP

11.4.1. Comandos requeridos de BGP

Para conectar con otros ASs, es necesario configurar los siguientes puntos:

```
routerA(config)#router bgp 64520
RouterA(config-router)#neighbor 10.1.1.1 remote-as 65000
RouterB(config)#router bgp 65000
RouterB(config-router)#neighbor 10.1.1.2 remote-as 64520
```

- Iniciar el proceso de routing.
- El vecino BGP con el cual el proceso de routing sincronizará las tablas de routing sobre una sesión TCP.

```
Router(config)#router bgp número-de-AS
```

Este comando configura el proceso de routing.

11.4.2. Identificar a los vecinos y definir el peer-group

Un peer group es un grupo de vecinos que comparten la misma política de actualizaciones.

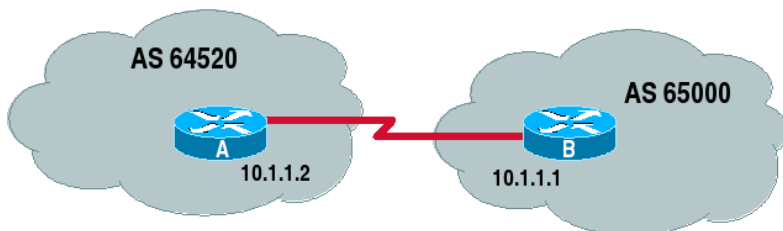
- Con este mecanismo se les agrupa para una configuración más simple.
- El peer group también reduce la carga de la red, ya que los routers iBGP² no necesitan estar totalmente mallados.
- El uso del nombre-del-peer-group permite la identificación del router como miembro del peer group.

```
Router(config-router)#neighbor nombre-del-peer-group  
peer-group
```

- Una vez que el peer group ha sido definido, es posible definir los vecinos para todos los miembros del peer group.

```
Router(config-router)#neighbor dirección-IP |  
nombre-del-peer-group remote-as número-de-AS
```

11.4.3. Ejemplo de configuración básica



²En iBGP, el número del AS remoto y el número de AS definido en el proceso de routing es el mismo, en eBGP son diferentes.

```
RouterA(config)#router bgp 64520
RouterA(config-router)#neighbor 10.1.1.1
    remote-as 65000
RouterB(config)#router bgp 65000
RouterB(config-router)#neighbor 10.1.1.2
    remote-as 64520
```

11.5. Comandos opcionales de BGP

Los comandos opcionales de BGP utilizados en la configuración básica realizan las siguientes funciones:

- Definen las redes que tiene que ser anunciadas.
- Fuerzan la dirección del next hop.
- Agregación de rutas.

11.5.1. Definir las redes a anunciar

Para definir las redes a anunciar por BGP se utiliza el siguiente comando:

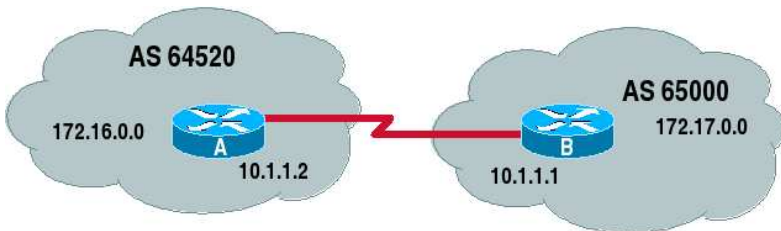
```
Router(config-router)#network dirección-de-red mask
    máscara-de-red
```

El comando `network` determina las redes que son originadas por el router.

Este comando no identifica los interfaces que participan en BGP, sino que indica que las redes serán anunciadas por BGP.

El comando `network` debe de incluir todas las redes que tienen que ser anunciadas en el AS, o simplemente las directamente conectadas al router.

11.5.1.1. Ejemplo con network



```
RouterA(config)#router bgp 64520
RouterA(config-router)#neighbor 10.1.1.1
    remote-as 65000
RouterA(config-router)#network 172.16.0.0
RouterB(config)#router bgp 65000
RouterB(config-router)#neighbor 10.1.1.2
    remote-as 64520
RouterB(config-router)#network 172.17.0.0
```

11.5.2. Forzar la dirección del next hop

En una red de multiacceso, la regla es que la dirección de origen es la del router que ha originado el paquete en la red.

Esto puede causar problemas en redes NBMA, donde puede que no haya conectividad con el router que lo ha originado y los paquetes sean descartados.

Para solucionar este problema se utiliza el comando:

```
Router(config-router)#neighbor {dirección-ip |
    peer-group} next-hop-self
```

Este comando fuerza que la ruta se anunciada con el next hop modificado.

11.5.3. Agregación de rutas

Para sumarizar o agregar rutas dentro del dominio de BGP, utilizaremos el siguiente comando:

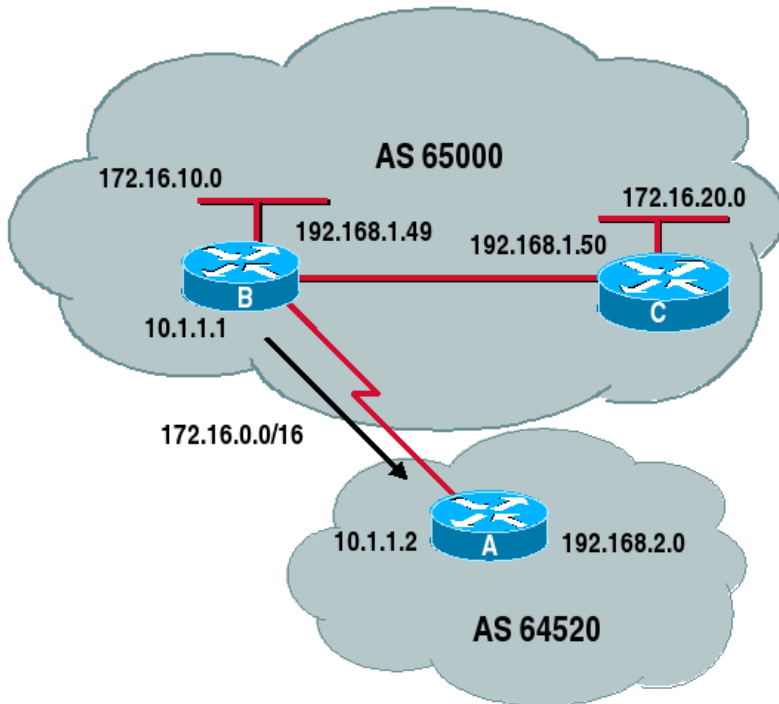
```
Router(config-router)#aggregate-address dirección-ip  
máscara [summary-only] [as-set]
```

Si se utiliza el parámetro `summary-only`, entonces las rutas específicas son suprimidas y sólo se propagará la sumariada.

Si se utiliza el parámetro `as-set`, entonces todos los ASs que atraviese serán almacenados en el mensaje de actualización.

Los atributos `AS_Path` de los prefijos se construirán con el agregado.

11.5.4. Ejemplo



```

RouterB(config)#router bgp 65000
RouterB(config-router)#neighbor 10.1.1.2 remote-as 64520
RouterB(config-router)#neighbor 192.168.1.50
                        remote-as 65000
RouterB(config-router)#network 172.16.10.0
                        mask 255.255.255.0
RouterB(config-router)#network 192.168.1.0
                        mask 255.255.255.0
RouterB(config-router)#no synchronization

```

```
RouterB(config-router)#neighbor 192.168.1.50
next-hop-self
RouterB(config-router)#aggregate-address 172.16.0.0
255.255.0.0 summary-only
```

11.6. Gestionar y verificar BGP

11.6.1. Resetear conexiones TCP entre vecinos

Después de cambios en la configuración de BGP, es necesario resetear las sesiones TCP entre vecinos:

```
Router#clear ip bgp {* | dirección} [soft [in | out]]
```

Este comando desconecta la sesión entre los vecinos y la restablece utilizando la nueva configuración que se ha introducido.

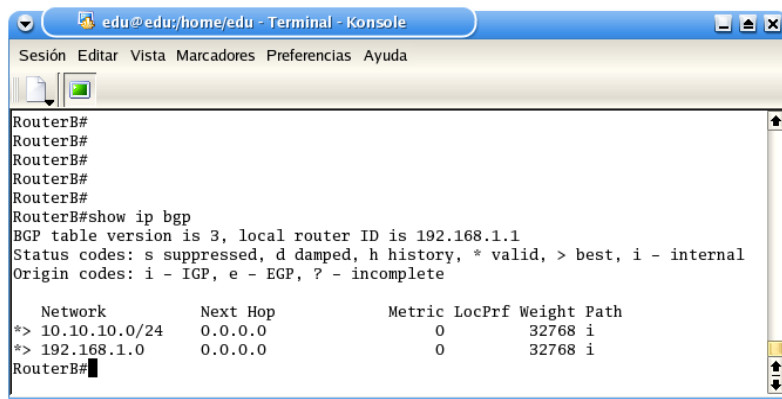
La opción `soft` no tira las sesiones, pero reenvía las actualizaciones.

Las opciones `in` y `out` permiten la configuración del interfaz entrante o saliente.

11.6.2. Comandos show relacionados con BGP

```
Router#show ip bgp
```

Muestra la tabla de routing BGP:



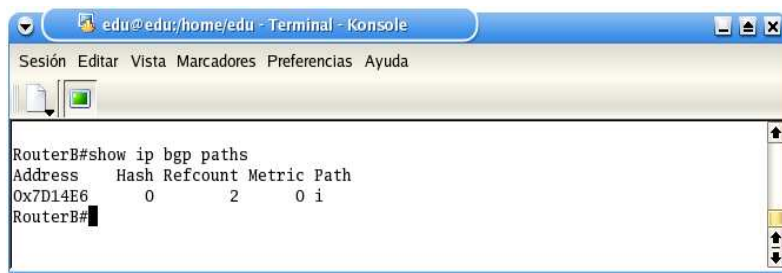
```
edu@edu:/home/edu - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

RouterB#
RouterB#
RouterB#
RouterB#
RouterB#
RouterB#show ip bgp
BGP table version is 3, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*> 10.10.10.0/24     0.0.0.0              0         32768 i
*> 192.168.1.0       0.0.0.0              0         32768 i
RouterB#
```

```
Router#show ip bgp paths
```

Muestra la tabla topológica:

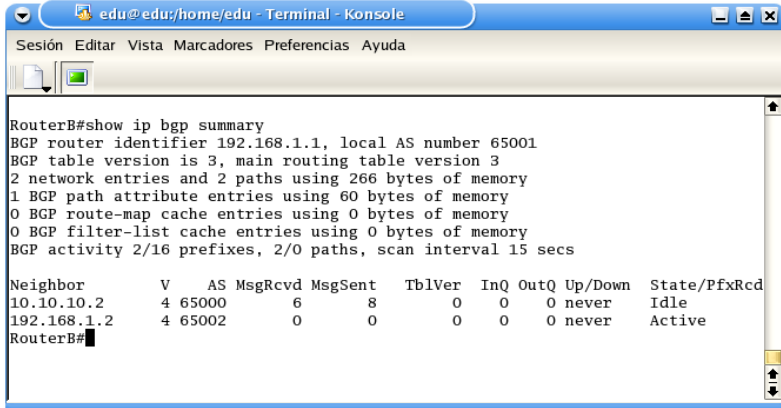


```
edu@edu:/home/edu - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

RouterB#show ip bgp paths
Address      Hash Refcount Metric Path
0x7D14E6    0      2      0 i
RouterB#
```

```
Router#show ip bgp summary
```

Muestra información sobre las sesiones TCP:

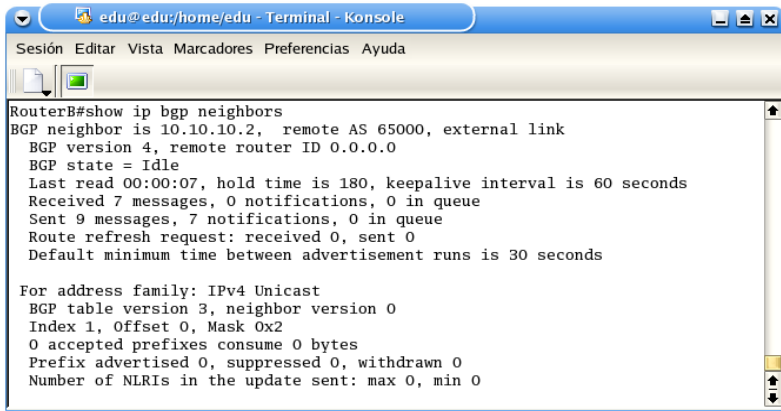


```
RouterB#show ip bgp summary
BGP router identifier 192.168.1.1, local AS number 65001
BGP table version is 3, main routing table version 3
2 network entries and 2 paths using 266 bytes of memory
1 BGP path attribute entries using 60 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 2/16 prefixes, 2/0 paths, scan interval 15 secs

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.2    4 65000      6      8       0    0    0 never    Idle
192.168.1.2   4 65002      0      0       0    0    0 never    Active
RouterB#
```

```
Router#show ip bgp neighbors
```

Muestra información sobre las conexiones TCP con los vecinos. Cuando se establece la conexión, los vecinos pueden intercambiar actualizaciones:



```
RouterB#show ip bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 65000, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 00:00:07, hold time is 180, keepalive interval is 60 seconds
  Received 7 messages, 0 notifications, 0 in queue
  Sent 9 messages, 7 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Default minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
  BGP table version 3, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes consume 0 bytes
  Prefix advertised 0, suppressed 0, withdrawn 0
  Number of NLRI in the update sent: max 0, min 0
```

```
Router#show processes cpu
```

Muestra los procesos activos en el router. Identifica los procesos que están consumiendo excesivos recursos:

```
RouterB#show processes cpu
CPU utilization for five seconds: 12%/0%; one minute: 4%; five minutes: 3%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 144 1465 98 0.00% 0.00% 0.00% 0 Load Meter
3 30964 1568 19747 0.00% 0.37% 0.38% 0 Check heaps
4 4 1 4000 0.00% 0.00% 0.00% 0 Chunk Manager
5 0 1 0 0.00% 0.00% 0.00% 0 Pool Manager
6 0 2 0 0.00% 0.00% 0.00% 0 Timers
7 88 7 12571 0.00% 0.00% 0.00% 0 Serial Background
8 4 127 31 0.00% 0.00% 0.00% 0 ARP Input
9 4 4 1000 0.00% 0.00% 0.00% 0 DDR Timers
10 0 2 0 0.00% 0.00% 0.00% 0 Dialer event
11 20 2 10000 0.00% 0.00% 0.00% 0 Entity MIB API
12 0 1 0 0.00% 0.00% 0.00% 0 SERIAL A'detect
13 4 1 4000 0.00% 0.00% 0.00% 0 Critical Bkgnd
14 1220 1745 699 0.00% 0.00% 0.00% 0 Net Background
15 20 35 571 0.00% 0.00% 0.00% 0 Logger
16 292 7310 39 0.08% 0.01% 0.00% 0 TTY Background
17 288 7346 39 0.00% 0.00% 0.00% 0 Per-Second Jobs
18 100 797 125 0.00% 0.00% 0.00% 0 Net Input
19 136 1466 92 0.00% 0.00% 0.00% 0 Compute load avg
20 8316 124 67064 0.00% 0.08% 0.07% 0 Per-minute Jobs
21 0 1 0 0.00% 0.00% 0.00% 0 AAA Dictionary R
22 1916 898 2133 0.49% 0.07% 0.01% 0 IP Input
--More--
```

11.6.3. Comandos debug de BGP

```
Router#debug ip bgp [dampening | events |
keepalives | updates]
```

Este comando muestra información a tiempo real de los eventos que van sucediendo.

Route dampening es un mecanismo para minimizar la inestabilidad causada por el flapping de rutas.

Los comandos de depuración en BGP no se tratan con la misma profundidad que otros protocolos en el BSCI ya que BGP no es un protocolo muy extendido en las empresas, aunque sí en los ISPs.

```

02:09:24: BGP: 192.168.1.2 went from Active to Idle
02:09:27: BGP: 10.10.10.2 passive open
02:09:27: BGP: 10.10.10.2 went from Idle to Connect
02:09:27: BGP: 10.10.10.2 rcv message type 1, length (excl. header) 26
02:09:27: BGP: 10.10.10.2 rcv OPEN, version 4
02:09:27: BGP: 10.10.10.2 went from Connect to OpenSent
02:09:27: BGP: 10.10.10.2 sending OPEN, version 4, my as: 65001
02:09:27: BGP: 10.10.10.2 rcv OPEN w/ OPTION parameter len: 16
02:09:27: BGP: 10.10.10.2 rcvd OPEN w/ optional parameter type 2 (Capability) 16
02:09:27: BGP: 10.10.10.2 OPEN has CAPABILITY code: 1, length 4
02:09:27: BGP: 10.10.10.2 OPEN has MP_EXT CAP for afi/safi: 1/1
02:09:27: BGP: 10.10.10.2 rcvd OPEN w/ optional parameter type 2 (Capability) 12
02:09:27: BGP: 10.10.10.2 OPEN has CAPABILITY code: 128, length 0
02:09:27: BGP: 10.10.10.2 OPEN has ROUTE-REFRESH capability(old) for all address
02:09:27: BGP: 10.10.10.2 rcvd OPEN w/ optional parameter type 2 (Capability) 12
02:09:27: BGP: 10.10.10.2 OPEN has CAPABILITY code: 2, length 0
02:09:27: BGP: 10.10.10.2 OPEN has ROUTE-REFRESH capability(new) for all address
02:09:27: BGP: 10.10.10.2 bad OPEN, remote AS is 6500, expected 65000
02:09:27: BGP: 10.10.10.2 went from OpenSent to Closing
02:09:27: %BGP-3-NOTIFICATION: sent to neighbor 10.10.10.2 2/2 (peer in wrong AS)
02:09:27: BGP: 10.10.10.2 send message type 3, length (incl. header) 23
02:09:27: BGP: 10.10.10.2 local error close, erroneous BGP update received
02:09:28: BGP: 10.10.10.2 went from Closing to Idle
02:09:28: BGP: 10.10.10.2 closing
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 2.00.0 | VT102 | Desconectado

```

11.6.4. Métodos alternativos para conectar con otros ASs

Si no es necesaria la utilización de BGP, hay que considerar otras opciones para conectar la red a otro AS.

Para ello tenemos dos opciones:

- Una ruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.
- Un protocolo de routing en el AS, haciendo el AS del ISP parte de nuestro AS. En este caso haremos redistribución dentro del

dominio, también podemos poner una pseudoseguridad como ACLs o un firewall.

El uso de rutas por defecto y estáticas es una alternativa a BGP que ha sido usado durante mucho tiempo, en redes satélite, redes conectadas a un enlace telefónico o incluso por residenciales para conectarse a Internet.

```
Router(config)#ip route prefijo máscara {interfaz |  
dirección-ip} [distancia]
```

11.6.5. Construyendo una red utilizando iBGP

Aunque BGP es un protocolo de routing exterior, dispone de dos comportamientos:

- Internal BGP (iBGP).
- External BGP (eBGP).

La diferencia depende de la función del protocolo de routing, es el router el que determinará si el será un vecino eBGP o iBGP comprobando el número de AS en las actualizaciones.

eBGP envía información de routing entre ASs.

iBGP se utiliza dentro de un único AS y se suele utilizar para comunicar dos routers eBGP situados en el mismo AS.

11.6.6. Requerimientos de red en iBGP

Para diseñar e implementar correctamente BGP es necesario tener en cuenta algunas características de BGP que es necesario entender:

- Los routers iBGP no tienen que estar directamente conectados.
- Los routers eBGP tienen que estar físicamente conectados.

11.6.7. Conexiones físicas y lógicas

Los routers iBGP no requieren estar conectados en el mismo medio físico, pero tienen que estar conectados utilizando el puerto 179/TCP, esto significa que iBGP tiene independencia de la topología.

La comunicación entre routers iBGP puede ser propagada con otro protocolo IGP ya que BGP no requiere una conexión física sino lógica.

BGP puede pasar la información de routing al protocolo IGP que esté en la red mediante redistribución.

Recordemos que la función de BGP es encontrar el AS que contiene la ruta, no encontrar al destinatario, de ello se encarga el protocolo IGP correspondiente.

11.6.8. Propagación de rutas entre routers iBGP

Un router iBGP propagará una ruta a un vecino BGP bajo las siguientes condiciones:

- Si la ruta ha sido generada por el router emisor:
 - Vía el comando network.
 - Redistribuyendo desde IGP.
 - Redistribuyendo rutas estáticas.
- Si la ruta anunciada es una ruta conectada:

Básicamente, si la ruta ha sido aprendida desde una actualización de un vecino BGP dentro del mismo AS no se propagará de forma interna, un router eBGP se la puede propagar únicamente a otro eBGP.

Como iBGP no reenvía actualizaciones lo aprende todo de sus vecinos iBGP, así que en iBGP la manera de que se puedan comunicar será con una red totalmente mallada.

11.6.9. Sincronización

Antes de poder propagar una ruta interna a otro AS es necesario que el protocolo de routing IGP esté sincronizado con BGP.

La sincronización se asegura que si el tráfico se envía al AS, el protocolo IGP conocerá su destino.

Esta regla está habilitada por defecto y sólo se puede desactivar en situaciones muy concretas, como p.e. que todos los routers de AS ejecuten BGP.

La sincronización es beneficiosa por:

- Preserva que el tráfico sea reenviado a destinos inalcanzables.
- Reduce tráfico innecesario.
- Asegura consistencia dentro del AS.

En ocasiones, es útil deshabilitar la sincronización:

- Si todos los routers en el AS ejecutan BGP.
- Si los routers dentro del AS están en una topología totalmente mallada.
- Cuando el AS no sea un AS de tránsito.

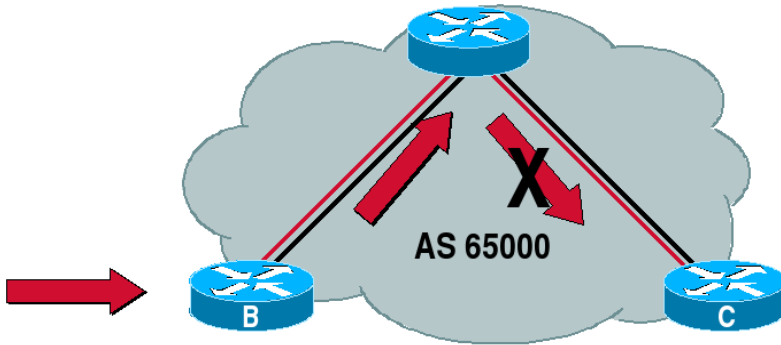
```
Router(config-router)#no synchronization
```

11.6.10. La red totalmente mallada

La regla del horizonte dividido de BGP indica que las rutas aprendidas por iBGP no serán propagadas nunca a otros peers iBGP.

El horizonte dividido al igual que en otros protocolos de routing es necesario para que evitar bucles de red empiecen en el AS.

Como resultado es necesaria una red totalmente mallada.



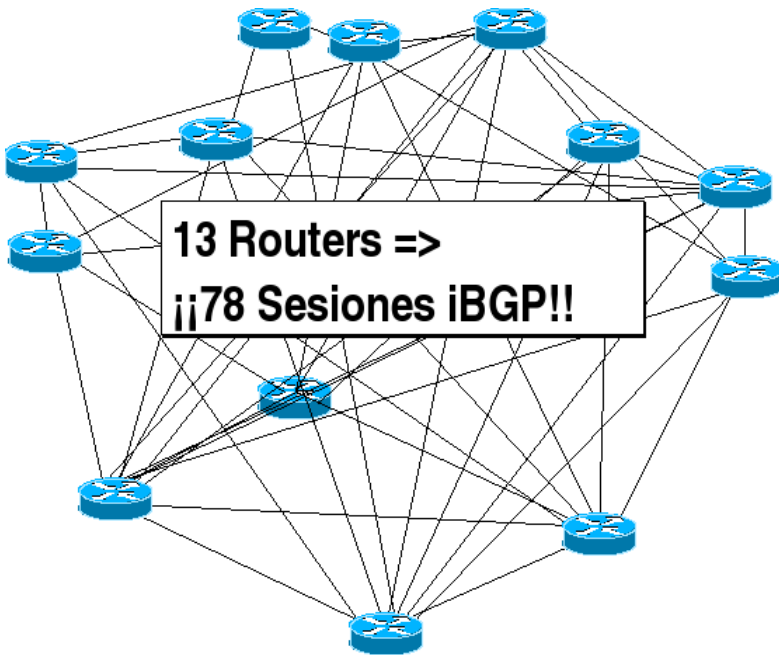
11.6.11. Recursos de una red totalmente mallada

BGP mantiene actualizada y precisa la información de routing enviando actualizaciones incrementales sobre conexiones TCP.

La ecuación para determinar el número de sesiones iBGP en una red totalmente mallada es:

Esta ecuación funciona bien en entornos donde se requieren pocas sesiones, sin embargo en entornos donde existen muchos routers no es factible.

$$n \frac{(n-1)}{2} = 13 \frac{(13-1)}{2} = 78 \text{ Sesiones}$$



11.7. Diseño y configuración de iBGP

Una red totalmente mallada iBGP evita bucles de routing.

Una red totalmente mallada no es escalable por:

- Demasiadas sesiones TCP.
- Se replica el tráfico de routing a través de todas las sesiones.

11.7.1. Route reflectors

Un Route Reflector es un router configurado para reenviar actualizaciones a sus vecinos o peers a través del mismo AS.

Estos peers iBGP necesitan identificarse como clientes en la configuración.

Cuando un cliente envía una actualización al route reflector, este la reenvía a sus otros clientes.

El Router Reflector lo que hace básicamente es modificar la regla del horizonte dividido de BGP.

El Router Reflector necesita un peering completo con sus clientes, aunque el peering entre vecinos no es necesario.

Los nonclients necesitan seguir en topología totalmente mallada con los Route Reflectors y el resto de nonclients.

Como solución a estos problemas se dispone de los route reflectors.

Un Route Reflector y sus clientes forman un cluster.

Cuando un Route Reflector reenvía actualizaciones se activa el atributo Originator-ID. Si el Route Reflector vuelve a recibir una actualización con su Originator-ID, la descartará, así evitará bucles.

Si existen múltiples Route Reflector se activará el atributo Cluster-ID, el cual también se utiliza para evitar bucles.

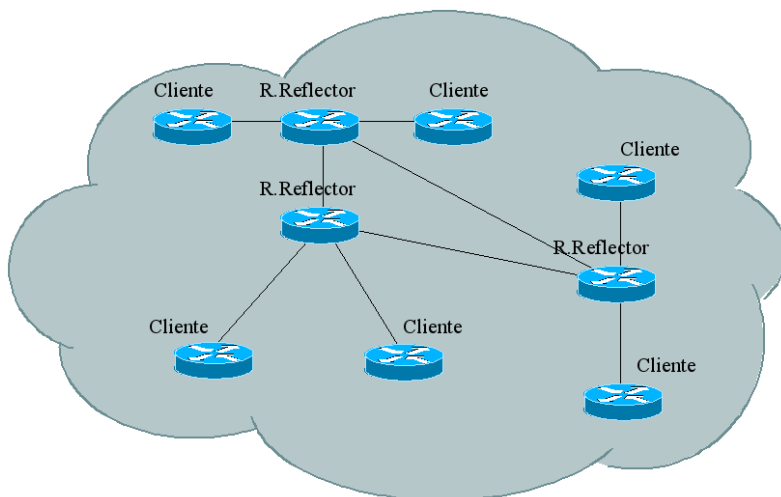
Es posible crear varios niveles de jerarquía de Route Reflector.

Los routers que no sean Route Reflector no se verán afectados por cambios en la topología, ya que siguen recibiendo las actualizaciones que necesitan de los Route Reflector.

Los Route Reflector tienen que estar en topología totalmente mallada.

Si creamos varios niveles de jerarquía de Route Reflector hemos de tener cuidado con el diseño ya que no tenemos protección ante bucles.

Un Route Reflector se comporta básicamente como un espejo que refleja las actualizaciones de sus clientes a los demás clientes sin necesidad de una red totalmente mallada.



11.7.2. Beneficios de los route reflector

Capacidad de Escalar la Red.

Fuerte Diseño Jerárquico.

Reducción de Tráfico en la Red.

Reducción de CPU necesaria para mantener las sesiones TCP entre peers iBGP.

Convergencia más rápida y red más sencilla ya que se implementan dos protocolos de routing:

- iBGP para información de routing externa que atraviesa el AS.
- IGP para rutas internas del AS.

Esta solución es muy buena para entornos iBGP amplios como redes de ISPs donde no es posible disponer de una red totalmente mallada.

11.7.3. Operación de los route reflector

El Route Reflector recibe una actualización de sus clientes y nonclientes.

Si la actualización es de un cliente, reenvía la actualización a sus cliente excepto al Originator y se le quita el Originator-ID.

Si existen varios paths el Route Reflector escogerá el mejor.

Si la actualización es de un nonclient, reenvía la actualización a todos sus clientes.

Si la actualización es de un peer eBGP, reenvía la actualización a todos sus clientes y nonclients.

11.7.4. Configuración de Route Reflectors

El comando para configurar un route reflector es:

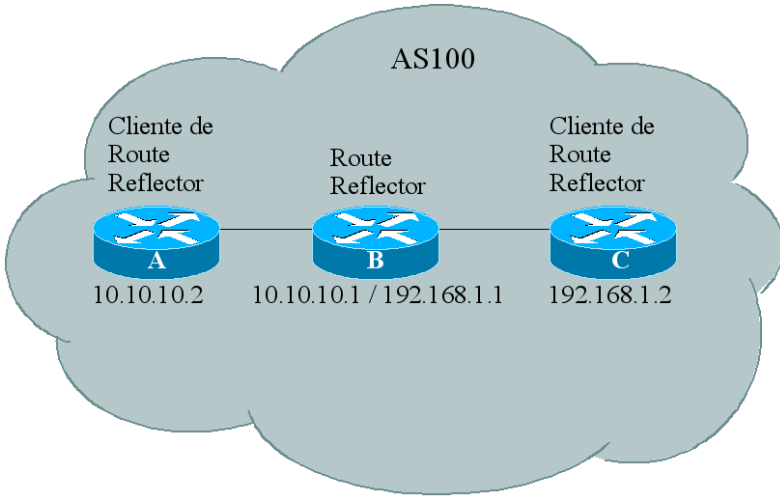
```
Router(config-router)#neighbor dirección-ip  
route-reflector-client
```

Para borrar un cliente:

```
Router(config-router)#no neighbor dirección-ip  
route-reflector-client
```

Si se eliminan todos los clientes, el route reflector pierde su estado y se convierte en un router iBGP estándar. Si esto ocurre, los routers iBGP tienen que estar en una topología totalmente mallada.

11.7.5. Ejemplo de configuración



Router B

```
router bgp 100
neighbor 10.10.10.2 remote-as 100
neighbor 10.10.10.2 route-reflector-client
neighbor 192.168.1.2 remote-as 100
neighbor 192.168.1.2 route-reflector-client
```

Router A

```
router bgp 100
network 10.10.10.0 mask 255.255.255.0
neighbor 10.10.10.1 remote-as 100
```

Router C

```

router bgp 100
network 192.168.1.0 mask 255.255.255.0
neighbor 192.168.1.1 remote-as 100

```

show ip bgp en Router C

```

RouterC#sh ip bgp
BGP table version is 2, local router ID is 192.168.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*  i10.10.10.0/24  10.10.10.2          0     100      0  i
*> 192.168.1.0    0.0.0.0             0           32768  i
RouterC#

```

11.7.6. Route refresh

Tras cualquier configuración de BGP, es necesario resetear la sesión TCP para que los cambios tengan efecto.

Es posible realizar un rebote suave (soft reboot), el cual destruirá y reconstruirá el peering, pero sin rebotar el proceso de BGP.

Para rebotar todas las sesiones es:

```
Router#clear ip bgp *
```

El comando para decirle al emisor que vuelva a reenviar una actualización BGP en particular es:

```
Router#clear ip bgp dirección-del-vecino in
```

El comando para decirle al proceso que reenvíe una actualización de BGP es:


```
Router#clear ip bgp dirección-del-vecino out
```

También es posible configurar el proceso BGP para almacenar los prefijos antes de aplicar la política, esto permite que las nuevas configuraciones sean implementadas sin tirar abajo las sesiones de los peers.

La configuración se aplica basada en el vecino y necesita ser aplicada en las actualizaciones entrantes:

```
Router(config-router)#neighbor dirección-del-vecino  
soft-configuration inbound
```

Por supuesto después del cambio de configuración es necesario resetar:

```
Router#clear ip bgp dirección-del-vecino soft [in |  
out]
```

11.7.7. Peer groups

Sin los Peer Groups, cada peer iBGP recibe la misma actualización. Esto significa que cada router iBGP realiza los mismos cálculos, gasto de CPU y restringe la escalabilidad de iBGP.

Una vez definidos los Peer Groups, cada router del Peer Group tiene la misma política de tráfico de salida, pero permite diferentes políticas de entrada en cada sistema. Es decir, se genera una única actualización para todo el Peer Group.

Los beneficios son:

La sobrecarga administrativa se reduce, ya que la configuración es simple reduciendo la probabilidad de errores.

Es necesaria menor cantidad de CPU, acelerando el trabajo en la red, y por tanto la convergencia es más rápida y la red por tanto más estable.

Para definir un Peer Group:

```
Router(config-router)#neighbor nombre-del-peer-group
peer-group
Router(config-router)#neighbor nombre-del-peer-group
remote-as sistema-autónomo
Router(config-router)#neighbor IP-peer-BGP peer-group
nombre-del-peer-group
```

11.8. Verificación de iBGP

11.8.0.1. Verificar la operación de iBGP

El siguiente ejemplo muestra el comando que muestra la configuración del router y sus vecinos.

```
RouterB#show ip bgp neighbors 192.168.1.2
BGP neighbor is 192.168.1.2, remote AS 100, internal link
  BGP version 4, remote router ID 192.168.1.2
  BGP state = Established, up for 03:33:14
  Last read 00:00:13, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Received 271 messages, 0 notifications, 0 in queue
  Sent 265 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Default minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  1 accepted prefixes consume 36 bytes
  Prefix advertised 6, suppressed 0, withdrawn 0
  Number of NLRI in the update sent: max 1, min 0
  Connections established 6; dropped 5
  Last reset 03:33:42, due to User reset
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 192.168.1.1, Local port: 11010
Foreign host: 192.168.1.2, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)
Event Timers (current time is 0xED5B3C):
Timer           Starts      Wakeups      Next
```

```

Retrans          218          0          0x0
TimeWait         0           0          0x0
AckHold          216         113         0x0
SendWnd          0           0          0x0
KeepAlive        0           0          0x0
GiveUp           0           0          0x0
PmtuAger         0           0          0x0
DeadWait         0           0          0x0
iss: 326559462  snduna: 326563662  sndnxt: 326563662      sndwnd: 15111
irs: 4213153520 rcvnxt: 4213157725 rcvwnd:      15111 delrcvwnd: 1273
SRTT: 300 ms, RTT0: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1460 bytes):
Rcvd: 323 (out of order: 0), with data: 216, total data bytes: 4204
Sent: 334 (retransmit: 0, fastretransmit: 0), with data: 217, total data bytes:9

```

11.9. Controlar el tráfico de BGP

Las actualizaciones de BGP pueden ser controladas, lo cual es ventajoso ya que se puede controlar el tráfico de BGP en la red, lo cual simplifica el mantenimiento y gestión de la red.

Existen tres formas de aplicar PBR en BGP:

- Tomando decisiones basadas en el path del AS, la comunidad o el prefijo.
- Aceptando o rechazando rutas.
- Modificando los atributos para influir en la selección del path.

Existen varias técnicas para filtrar el tráfico en un router Cisco.

- **Autonomous System Path Access Lists:** ACL utilizado en BGP para filtrar actualizaciones enviadas desde un peer basándonos en el path del AS.
- **Prefix List:** Utilizado para filtrar prefijos, particularmente en redistribución. Los prefix lists se basan en la dirección de prefijo. Esta opción es parte de IOS desde la versión 12.0.

- **Distribute List:** Utilizados para filtrar actualizaciones de routing. Aunque se utilicen en redistribución, no fueron creados para la redistribución, ya que se pueden aplicar en las actualizaciones entrantes y salientes.

Tanto los Distribute Lists como los Prefix Lists están basados en números de red, no en paths de ASs.

- **Route Maps:** Utilizados para definir políticas de routing. Un route map es un access lists sofisticado que define criterios ante los cuales el router tiene que actuar cuando haya una coincidencia en el criterio. Se utiliza en BGP para configurar los atributos que determinan las bases de selección del mejor camino a un destino.

11.9.1. Cómo funcionan los prefix lists

Los Prefix Lists son introducidos en BGP porque son una forma eficiente de filtrado muy rápido porque buscan el prefijo de las direcciones dadas por el administrador y la búsqueda es muy rápida.

Los Prefix Lists se pueden editar. La modificación de ACLs es bastante compleja.

Los Prefix Lists son fáciles de configurar y usar, pero antes de aplicarlos es necesario definir el criterio del Prefix List.

Cada línea de Prefix List está asociado a un número de secuencia que por defecto van aumentando de 5 en 5.

Si se especifica el número de secuencia se pueden intercalar sentencias y por tanto se puede modificar el Prefix List.

Si un Prefix List permite o deniega se hace mediante las siguientes premisas:

- Si la ruta se permite, la ruta se usa.
- Si la ruta se deniega, la ruta no se usa.
- Al final de cada Prefix List existe un deny any implícito.

- Si existen múltiples entradas de un prefix list se comprobarán por el prefijo, la entrada con el número de secuencia menor se utilizará.
- El router empieza la búsqueda al inicio del prefix list, en cuanto se encuentre una coincidencia (match), la búsqueda se detendrá.
- Los números de secuencia se generan automáticamente por defecto. Se pueden configurar utilizando el argumento seq número-de-secuencia en el comando ip prefix-list.
- El número de secuencia no tiene que ser especificado al borrar una entrada de la configuración.

11.9.2. Configuración de un prefix list de BGP

El siguiente comando crea una entrada en un prefix list y asigna un número de secuencia a la misma:

```
Router(config-router)#ip prefix-list nombre-prefix-list  
    [seq número-de-secuencia] {deny | permit}  
    red/longitud-del-prefijo [ge valor-mayor-que]  
    [le valor-menor-que]
```

Para configurar un router para que utilice un prefix list hay que utilizar el siguiente comando:

```
Router(config-router)#neighbor {dirección-ip |  
    peer-group} prefix-list nombre-del-prefix-list  
    {in | out}
```

- nombre-del-prefix-list: Nombre del prefix-list.

- `seq número-de-secuencia`: Número de secuencia asignado al criterio.
- `{deny | permit}`: Indica si la acción es permitida o denegada.
- `red/longitud-del-prefijo`: Indica la red y la máscara en formato número de bits.
- `[ge valor-mayor-que] [le valor-menor-que]`: Especifican el rango de coincidencia del prefijo.

A veces es necesario crear un rango de criterios, esto se hace con los parámetros `ge` y `le`.

- `ge`: mayor o igual.
- `le`: menor o igual.

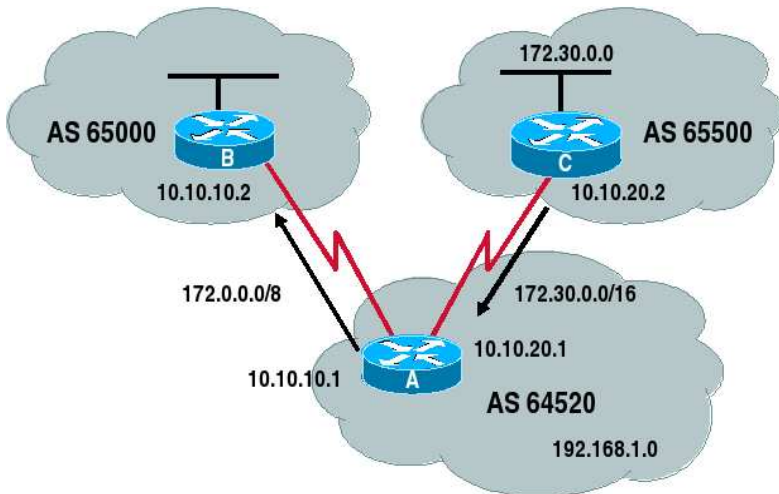
Estos parámetros opcionales son lo opuesto a `red/longitud-del-prefijo` que proporciona un valor absoluto.

Ejemplo:

```
Router(config)#ip prefix list lista-prefijo permit  
0.0.0.0/0 ge 0 le 24
```

El rango asumido para `ge` y `le` si no se especifica nada es 32.

11.9.2.1. Ejemplo de prefix list



```

A(config)#router bgp 64520
A(config-router)#network 192.168.1.0
A(config-router)#neighbor 10.10.10.2 remote-as 65000
A(config-router)#neighbor 10.10.20.2 remote-as 65500
A(config-router)#aggregate-address 172.0.0.0 255.0.0.0
A(config-router)#neighbor 10.10.10.2 prefix-list superred out
A(config-router)#exit
A(config)#ip prefix-list superred permit 172.0.0.0/8
A(config)#ip prefix-list superred description solo permite ruta agregada

```

11.9.3. Verificar la configuración de los prefix lists

Para mostrar información sobre los prefix list se utiliza el comando:

```
Router#show ip prefix-list [detail | summary] nombre  
[red/longitud-del-prefijo]  
[seq número-de-secuencia] [longer] [first-match]  
show ip prefix-list [detail | summary]
```

Muestra información sobre todos los prefix lists:

```
show ip prefix-list [detail | summary] nombre
```

Muestra una tabla mostrando las entradas en la prefix list identificadas con el nombre:

```
show ip prefix-list nombre [red/longitud-del-prefijo]
```

Muestra la asociación de filtrado con el nodo basada en el prefijo absoluto:

```
show ip prefix-list nombre [seq número-de-secuencia]
```

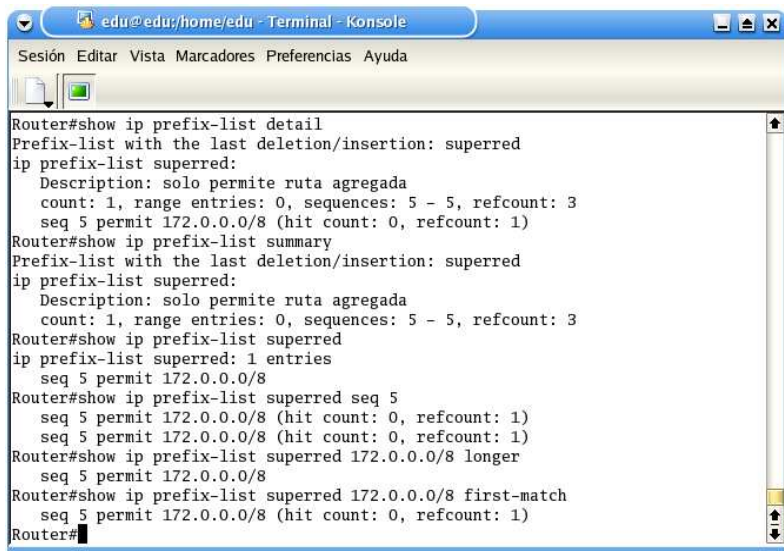
Muestra la asociación de filtrado con el nodo basada en el número de secuencia:

```
show ip prefix-list nombre [red/longitud-del-prefijo]  
longer
```

Muestra todas las entradas más específicas que la dada:


```
show ip prefix-list nombre [red/longitud-del-prefijo]
first-match
```

Muestra las entradas que coincidan con la dada:



```
Router#show ip prefix-list detail
Prefix-list with the last deletion/insertion: superred
ip prefix-list superred:
  Description: solo permite ruta agregada
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 3
  seq 5 permit 172.0.0.0/8 (hit count: 0, refcount: 1)
Router#show ip prefix-list summary
Prefix-list with the last deletion/insertion: superred
ip prefix-list superred:
  Description: solo permite ruta agregada
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 3
Router#show ip prefix-list superred
ip prefix-list superred: 1 entries
  seq 5 permit 172.0.0.0/8
Router#show ip prefix-list superred seq 5
  seq 5 permit 172.0.0.0/8 (hit count: 0, refcount: 1)
  seq 5 permit 172.0.0.0/8 (hit count: 0, refcount: 1)
Router#show ip prefix-list superred 172.0.0.0/8 longer
  seq 5 permit 172.0.0.0/8
Router#show ip prefix-list superred 172.0.0.0/8 first-match
  seq 5 permit 172.0.0.0/8 (hit count: 0, refcount: 1)
Router#
```

11.10. Conectar a Internet con BGP

11.10.1. Multihoming

Tener más de una conexión a Internet es estar multihomed.

La razón para duplicar la conexión a Internet es obtener redundancia y posibilidad de balanceo de carga que aumentará el rendimiento.

El multihoming puede ser:

- Varias conexiones con el mismo ISP.

- Disponer de una segunda conexión con otro ISP si es así:
 - Cada proveedor puede que no anuncie las mismas rutas, si no se anuncia una de las que necesitamos tendremos un problema.
 - Si nos conectamos con varios ISPs, nuestro AS puede convertirse en un AS de transito si un ISP ve un path al otro ISP a través nuestro y nuestro AS es la mejor ruta a ese destino.

La configuración a nivel del ISP es la solución a estos problemas.

11.10.2. Recibiendo información de routing de Internet

Cuando nos conectamos a algo tan vasto como Internet es necesario decidir que actualizaciones se van a enviar al resto del Mundo y como los routers del AS serán conocidos por el resto de Internet.

Para tomar esta decisión existen tres aproximaciones:

- Aceptar únicamente rutas por defecto de todos los proveedores.
- Aceptar rutas parciales además de las rutas por defecto de todos los proveedores.
- Aceptar todas las actualizaciones de routing (full routing) de todos los proveedores.

11.10.3. Aceptar únicamente rutas por defecto de todos los ISPs

Recursos de memoria bajos.

Recursos de CPU bajos.

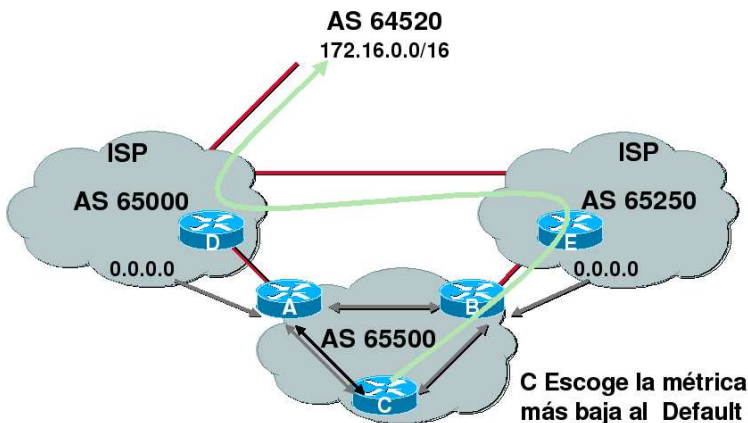
IGP escoge la mejor métrica como ruta por defecto.

BGP selecciona el mejor camino a una red externa yendo al gateway más cercano que anuncia el path.

No se pueden modificar los atributos de BGP.

El AS envía todas sus rutas al ISP.

El ISP escoge en path de entrada al AS.



11.10.4. Aceptar rutas parciales de todos los ISPs

Recursos de memoria medios.

Recursos de CPU medios.

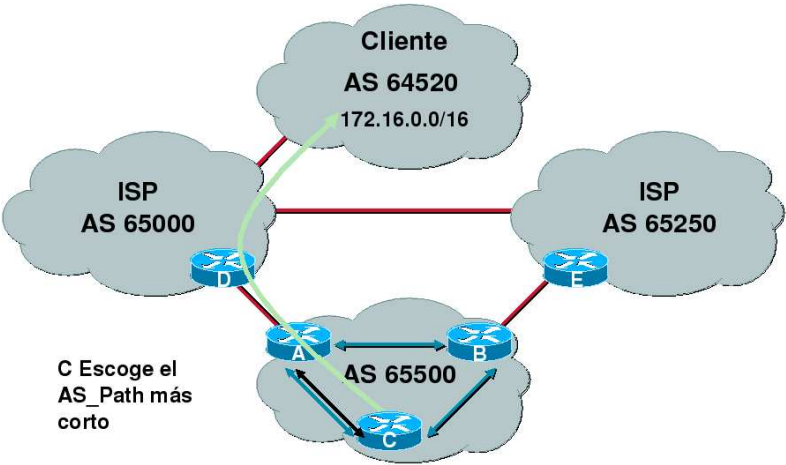
IGP escoge la mejor métrica como ruta por defecto.

BGP selecciona el mejor camino a una red externa mediante el AS_Path (normalmente).

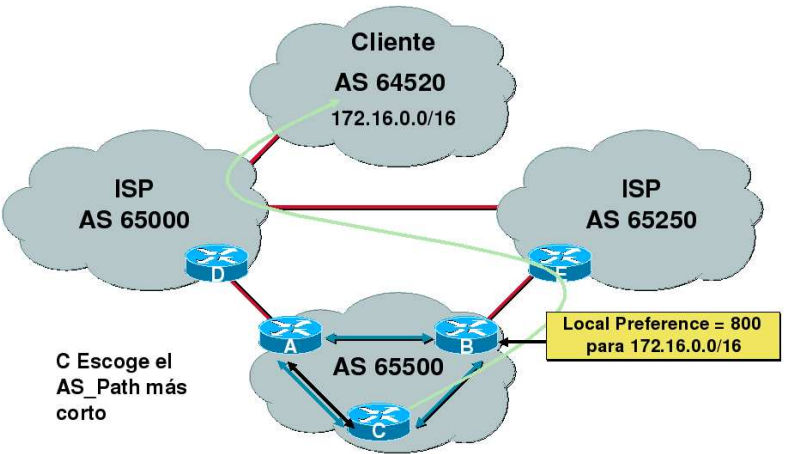
Se pueden modificar los atributos de BGP.

El AS envía todas sus rutas al ISP.

El ISP escoge en path de entrada al AS.



En el siguiente caso hemos modificado la Local Preference que por defecto es 100 a 800 y hemos modificado la elección de la salida.



11.10.5. Aceptar full routing de todos los ISPs

Recursos de memoria altos.

Recursos de CPU altos.

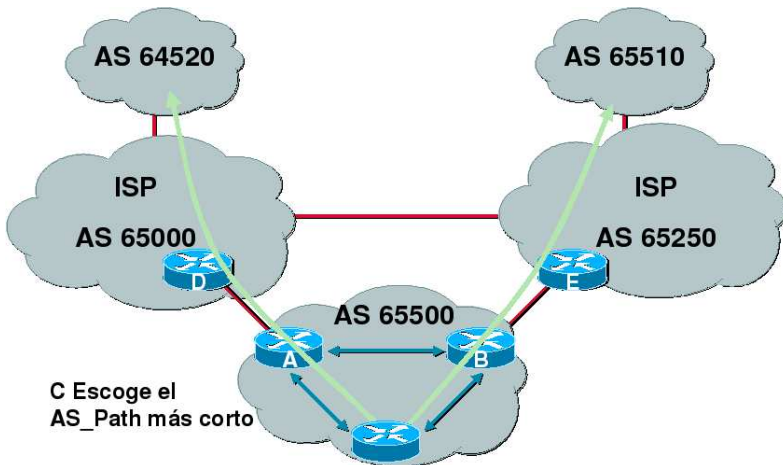
IGP escoge la mejor métrica como ruta por defecto.

BGP selecciona el mejor camino a una red externa mediante el AS_Path (normalmente).

Se pueden modificar los atributos de BGP.

El AS envía todas sus rutas al ISP.

El ISP escoge en path de entrada al AS.



11.11. Determinar el path de BGP modificando atributos

11.11.1. Modificar el atributo weight

El atributo Weight selecciona el path de salida del router cuando hay múltiples paths al mismo destino.

Cuanto mayor sea el valor mejor path.

Este es un atributo local y por tanto no será propagado.

Es propietario de Cisco Systems.

Para configurar el atributo weight:

```
Router(config-router)#neighbor {dirección-ip |  
    nombre-del-peer-group} weight peso
```

neighbor: Indica que el resto del comando está dirigido a un peer de BGP.

dirección-ip: Dirección IP del router vecino.

nombre-del-peer-group: Identifica el peer group.

weight peso: Propietario de Cisco y se utiliza en la selección de rutas. Es local del router, y no se propaga a otros routers. El valor por defecto es 32.762 y el rango va desde 0 hasta 65.535.

11.11.2. Modificar el atributo Local Preference

Este atributo se utiliza para decirle a los otros routers dentro del AS como salir del AS en caso que tengamos varias posibilidades.

Su configuración es:

- Si lo aplicamos a un route map.

```
Router(config-route-map)#set local-preference  
    local-preference
```

- Si lo aplicamos por defecto.

```
Router(config-router)#bgp default local-preference  
    valor
```

11.11.3. Verificar la configuración de los atributos

El comando `show ip bgp` muestra los valores de todos los atributos y sus estados.

```
7206#sh ip bgp
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
*> 1.1.1.1/32      0.0.0.0                0      32768 i
*> 2.2.2.2/32      70.0.0.2                0     100      0 (100) i
* 3.3.3.3/32      121.1.1.102            0     100      0 (100 23456) i
```

11.12. Redistribución entre IGP y BGP

11.12.1. Anunciar Rutas desde IGP a BGP

Existen tres formas de propagar la tabla de BGP en las tablas de IGP.

- Utilizando el comando **network**: Se utiliza para anunciar rutas que están en la tabla de routing IP.
- Redistribuyendo rutas estáticas³: Cualquier ruta estática puede ser redistribuida en BGP. Haciendo una ruta estática a null 0 hacemos que el router no tenga punto de salida para esta ruta porque no existe pero será redistribuida en BGP. El problema empieza si la ruta desaparece de la tabla de routing IP, entonces el tráfico circulará por el AS hasta que muera. Cisco recomienda utilizar el comando **aggregate-address**.

³Además de hacer el:

```
Router(config)#ip route x.y.z.t x.y.z.t null 0
```

hay que hacer:

```
Router(config-router)#redistribute static
```

- Redistribuyendo dinámicamente rutas de IGP: Esta configuración no es aconsejada porque causa gran dependencia en la tabla de IGP.
- La redistribución de rutas de Internet en redes pequeñas es muy imprudente.
- Los ISPs utilizan eBGP e iBGP intensivamente, pero en las rutas internas utilizan un protocolo IGP sin redistribuir debido a:
 - Los recursos están disponibles para otros procesos.
 - La tabla de routing IGP es manejable.
 - La función de sincronización no es necesaria en este tipo de redes ya que o es totalmente mallada o se ha diseñado para funcionar con route reflector.
- Si BGP es multihomed entonces la redistribución es necesaria ya que el IGP será el encargado de transportar las rutas de un eBGP a otro.
- En este último caso será necesario configurar filtering.