CAPÍTULO 5

INTRODUCCIÓN A LOS PROTOCOLOS DE ENRUTAMIENTO POR ESTADO DE ENLACE

MÁSCARAS DE SUBRED DE LONGITUD VARIABLE

El crecimiento exponencial de las redes ha hecho que el direccionamiento IPv4 no permita un desarrollo y una escalabilidad acorde a lo deseado por los administradores de red. IPv4 pronto sea reemplazado por IP versión 6 (IPv6) como protocolo dominante de Internet. IPv6 posee un espacio de direccionamiento prácticamente ilimitado y algunos administradores ya han empezado a implementarlo en sus redes. Para dar soporte al direccionamiento IPv4 se ha creado **VLSM** (máscara de subred de longitud variable) que permite incluir más de una máscara de subred dentro de una misma dirección de red. VLSM es soportado únicamente por protocolos sin clase tales como OSPF, RIPv2 y EIGRP.

El uso de las máscaras de subred de longitud variable permita el uso más eficaz del direccionamiento IP. Al permitir niveles de jerarquía se pueden resumir diferentes direcciones en una sola, evitando gran cantidad de actualizaciones de ruta.

Hasta ahora las direcciones de host que pertenecían a la subred "cero" se perdían al no poder utilizarlos. Si se configura el comando **`ip subnet-zero`** todas las direcciones de host pertenecientes a esta subred se podrán admitir como válidos.

Observe el ejemplo:

La red **192.168.1.0/24** se divide en subredes utilizando una máscara de subred de 28 bits.

Hasta ahora la primer subred utilizable era la 192.168.1.16/28, configurando el router con el comando **`ip subnet-zero`** la dirección IP 192.168.1.0/28 será una dirección válida pudiendo sumar 14 host válidos más al direccionamiento total.

Siguiendo el esquema de direccionamiento anterior una de las subredes que surgen de la división se utilizará para un enlace serial entre dos routers. En este caso la máscara de 28 bits permite el uso válido de 14 host desperdiciándose 12 direcciones de host para este enlace. El uso de VLSM permite volver a dividir más subredes otra subred, en este caso la máscara ideal sería una /30.

Proceso de creación de VLSM

Siguiendo el ejemplo anterior, la red 192.168.1.0/24 será divida en 14 subredes validas:

Se obtienen las siguientes subredes

192.168.1.0/28
192.168.1.16/28
192.168.1.32/28
192.168.1.48/28
192.168.1.64/28
192.168.1.80/28
192.168.1.96/28
192.168.1.112/28
192.168.1.128/28
192.168.1.144/28
192.168.1.160/28
192.168.1.176/28
192.168.1.192/28
192.168.1.208/28
192.168.1.224/28
192.168.1.240/28

Observe que se tomará en cuenta la 192.168.1.0 al configurar el ip subnet-zero y Que se descartará la última quedando un total de 15 subredes válidas.

Para el enlace serial entre los router se utilizará una máscara /30 que nos permita el uso de dos host. Elija una de las subredes creadas en el paso anterior, esta subred elegida **NO** podrá utilizarse con la máscara /28 puesto que se seguirá dividiendo en subredes más pequeñas.

Paso 1

Piense en binario.

Paso 2

La red 192.168.1.0/24 se divide en subredes con una máscara /28, escriba en binario el ultimo octeto.

/24	/28	
0000	0000	=0
0001	0000	=16
0010	0000	=32
....	....	
1000	0000	=128
....	....	

Paso 3

Elija una de las subredes para dividirla con una máscara /30, en este caso la 128. Trace una línea que separe los bits con la máscara /28 y otra que separe a los bits con máscara /30. Las subredes se obtienen haciendo las combinaciones correspondientes entre el bit 128 y los contenidos entre las dos paralelas.

/24	/28	/30	
1000	00	00	=128
1000	01	00	=132
1000	10	00	=136
1000	11	00	=140

Paso 4

Las direcciones de host se obtienen haciendo la combinación con los dos bits libres en cada una de las subredes obtenidas.

Ejemplo con una red clase B

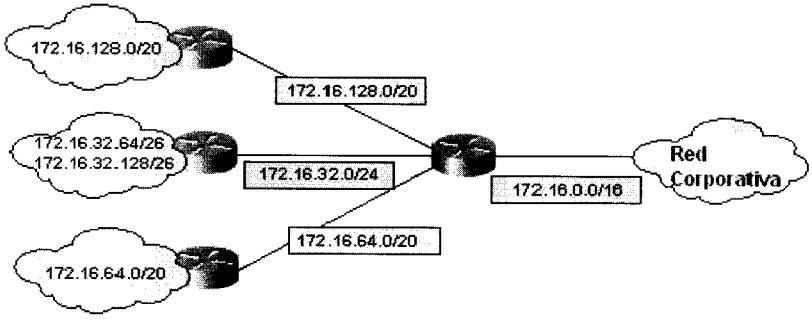
172.16.0.0/16
se divide en subredes con una máscara /21, para seguir el proceso elijo la
172.16.8.0/21
se divide en subredes con una máscara /24, para seguir el proceso elijo la
172.16.10.0/24
se divide en subredes con una máscara /26, para seguir el proceso elijo la
172.16.10.128/26
se divide en subredes con una máscara /30
172.16.10.132/30

En binarios

		/16	/21	/24	/26	/30
172.16.0.0/16	10101100	00010000	00000	000	00	0000
172.16.8.0/21	10101100	00010000	00001	000	00	0000
172.16.10.0/24	10101100	00010000	00001	010	00	0000
172.16.10.128/26	10101100	00010000	00001	010	10	0000
172.16.10.132/30	10101100	00010000	00001	010	10	0001

Resumen de ruta con VLSM

El resumen de ruta **CIDR** (agregación de ruta o supernetting) reduce la cantidad de rutas que un router debe mantener en sus tablas anunciando y manteniendo una sola dirección que contengas a las demás.



El router de resumen tiene múltiples entradas de redes consecutivas, siendo este el principal factor en el resumen de ruta, pero solo anunciará al router remoto la red que contiene a todas las demás.

Explicación de funcionamiento de CIDR

Imagine que un router posee un rango de redes directamente conectadas, de la 172.16.168.0/24 a la 172.16.175.0/24. El router buscará el bit común más alto para determinar cuál será el resumen de ruta.

En binarios

DIRECCIÓN DE SUBRED	PRIMER OCTETO	SEGUNDO OCTETO	TERCER OCTETO		CUARTO OCTETO
172.16.168.0/24	10101100	00010000	10101	000	00000000
172.16.169.0/24	10101100	00010000	10101	001	00000000
172.16.170.0/24	10101100	00010000	10101	010	00000000
172.16.171.0/24	10101100	00010000	10101	011	00000000
172.16.172.0/24	10101100	00010000	10101	100	00000000
172.16.173.0/24	10101100	00010000	10101	101	00000000
172.16.174.0/24	10101100	00010000	10101	110	00000000
172.16.175.0/24	10101100	00010000	10101	111	00000000
	Bits comunes = 21 Resumen 172.16.168.0/21			**Bits no comunes o de host**	

Por lo tanto para el rango especificado el router utilizará la dirección **172.16.168.0/21** para el resumen de ruta solicitado.

WILDCARD

Las listas de acceso y algunos protocolos de enrutamiento hacen uso del concepto conocido como máscara wildcard. Aunque parece similar a la máscara de red, la máscara wildcard parece la inversa de la máscara de red. Las posiciones de bit establecidas a **1** en la máscara wildcard que coinciden con el bit correspondiente de la máscara de red serán **ignorados**, mientras que los que posean el valor 0 serán tomados en cuenta por el router. Una máscara wildcard de 0.0.0.255 coincide con cualquier número en el rango 0 a 255 que aparezca en el cuarto octeto de una dirección IP. Una máscara wildcard de 0.0.3.255 coincide con cualquier dirección IP que tenga un 0, 1, 2 ó 3 en el tercer octeto y cualquier número en el cuarto octeto. Las máscaras wildcard permiten que el administrador de red especifique, por ejemplo, rangos de direcciones.

En los protocolos de enrutamiento como OSPF se debe especificar la red o subred que se quiere publicar con exactitud haciendo uso de las máscaras wildcard, haciendo coincidir los bits en 0 con la parte correspondiente a la porción de red/subred para que sean tomados en cuenta y los bits en 1 para la parte de host para que el router los ignore.

La red 192.168.1.0/24 posee una máscara que identifica a los primeros 24 bits como pertenecientes a la red y los últimos 8 al rango de host, por lo tanto estos deberán ser ignorados por el router poniendo los bits en 1 en la máscara wildcard:

DIRECCIÓN IP	192	168	1	0
EN BINARIOS	11000000	10101000	00000001	00000000
MÁSCARA DE RED	11111111	11111111	11111111	**00000000**
WILDCARD	00000000	00000000	00000000	**11111111**
RESULTADO	SE TOMAN EN CUENTA 8 BITS	SE TOMAN EN CUENTA 8 BITS	SE TOMAN EN CUENTA 8 BITS	IGNORADOS

Wildcard: 0.0.0.255

El mismo caso con la subred 172.16.32.0/19:

DIRECCIÓN IP	172	16	32	0
EN BINARIOS	10101100	00010000	00100000	00000000
MÁSCARA DE RED	11111111	11111111	111**00000**	**00000000**
WILDCARD	00000000	00000000	000**11111**	**11111111**
RESULTADO	SE TOMAN EN CUENTA 8 BITS	SE TOMAN EN CUENTA 8 BITS	SE TOMAN EN CUENTA 3 BITS SE IGNORAN 5	IGNORADOS

Wildcard: 0.0.31.255

CONFIGURACIÓN DE EIGRP

El protocolo de enrutamiento de gateway interior mejorado (Enchaced Interior Gateway Routing Protocol, **EIGRP**) es una versión mejorada del protocolo IGRP original desarrollado por Cisco Systems.

EIGRP combina las ventajas de los protocolos de estado de enlace con las de los protocolos de vector de distancia.

EIGRP mantiene el mismo algoritmo de vector de distancia y la información de métrica original de IGRP; no obstante, se han mejorado apreciablemente el tiempo de convergencia y los aspectos relativos a la capacidad de ampliación. EIGRP e IGRP usan cálculos de métrica diferentes. EIGRP multiplica la métrica de IGRP por un factor de 256. Esto ocurre porque EIGRP usa una métrica que tiene 32 bits de largo, e IGRP usa una métrica de 24 bits. La información EIGRP puede multiplicarse o dividirse por 256 para un intercambio fácil con IGRP. IGRP tiene un número de saltos máximo de 255. El límite máximo para el número de saltos en EIGRP es 224. Esto es más que suficiente para admitir grandes redes.

EIGRP ofrece características que no se encontraban en su antecesor, IGRP como el soporte para **VLSM** y los resúmenes de ruta. Además, EIGRP ofrece características que se encuentran en protocolos como OSPF, como las actualizaciones increméntales parciales y un tiempo de convergencia reducido. Como en el caso del protocolo IGRP, EIGRP publica la información de la tabla de enrutamiento sólo a los routers vecinos.

EIGRP mantiene las siguientes tres tablas:

- Tabla de vecinos
- Tabla de topología
- Tabla de enrutamiento

Los routers vecinos se descubren por medio de un protocolo **Hello** sencillo intercambiado por los routers que pertenecen a la misma red física estableciendo adyacencias. Hello utiliza para intercambiar paquetes de saludo una dirección multicast **224.0.0.10**. Una vez descubiertos los routers vecinos, EIGRP utiliza un protocolo de transporte fiable para garantizar la entrega correcta y ordenada de la información y las actualizaciones de la tabla de enrutamiento.

Un router hace el seguimiento de sus propias rutas conectadas y, además, de todas las rutas publicas de los routers vecinos. Basándose en esta información, EIGRP puede seleccionar eficaz y rápidamente la ruta de menor coste hasta un destino y garantizar que la ruta no forma parte de un bucle de enrutamiento esta ruta elegida como principal será la llamada **Sucesor**.

Al almacenar la información de enrutamiento de los routers vecinos, el algoritmo puede determinar con mayor rapidez una ruta de sustitución o un **Sucesor**

factible en caso de que haya un fallo de enlace o cualquier otro evento de modificación de la topología.

El saludo y la información de enrutamiento EIGRP son transportados mediante el protocolo de transporte EIGRP. El transporte EIGRP define un protocolo fiable de publicación, acuse de recibo y petición para garantizar que el saludo y la información de enrutamiento de distribuyen adecuadamente a todos los routers vecinos.

Cuando existen cambios de topologías EIGRP recurre a **DUAL** (algoritmo de actualización difusa) para conseguir una rápida convergencia entre los routers, estos almacenan sus propias tabas de enrutamiento con rutas alternativas (Sucesor factible), si no existiera alguna ruta alternativa, EIGRP recurre a sus routers vecinos para conseguir información acerca de ese camino alternativo.

Sintaxis de la configuración de EIGRP

```
router(config)#router eigrp 240
router(config-router)#network network-number
router(config-if)#bandwidth kilobits
router(config-router)#eigrp log-neighbor-changes
```

router eigrp 240 especifica como protocolo de enrutamiento a EIGRP para el sistema autónomo **240**, este valor varia de 1 a 65535

network especifica las redes directamente conectadas al router que serán anunciadas por EIGRP.

bandwidth el proceso de enrutamiento utiliza el comando bandwidth para calcular la métrica y es conveniente configurar el comando para que coincida con la velocidad de línea de la interfaz.

log-neighbor-changes habilita el registro de los cambios de adyacencia de vecinos para monitorear la estabilidad del sistema de enrutamiento y para ayudar a detectar problemas.

En versiones actuales de IOS EIGRP agrega al comando **network** la correspondiente **wildcard** esto permite al protocolo la identificación de subredes,

```
router(config)#router eigrp 240
router(config-router)#network 192.168.16.0 0.0.0.255
```

Algunos comandos para la verificación y control EIGRP son:

show ip route
Muestra la tabla de enrutamiento.

show ip protocols
Muestra los parámetros del protocolo.

show ip eigrp neighbors
Muestra la información de los vecinos EIGRP.

show ip eigrp topology
Muestra la tabla de topología EIGRP.

debug ip eigrp
Muestra la información de los paquetes.

CONFIGURACIÓN DE OSPF

El protocolo **OSPF**, Primero la ruta libre más corta, (Open Shortest Path First) fue creado a finales de los 80. Se diseño para cubrir las necesidades de las grandes redes IP que otros protocolos como RIP no podían soportar, incluyendo **VLSM**, autenticación de origen de ruta, convergencia rápida, etiquetado de rutas conocidas mediante protocolos de enrutamiento externo y publicaciones de ruta de multidifusión. El protocolo OSPF versión 2 es la implementación más actualizada, aparece especificado en la RFC 2328.

OSPF funciona dividiendo una Intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza a un área backbone mediante un router fronterizo. Todos los paquetes enviados desde una dirección de una estación de trabajo de un área a otra de un área diferente atraviesan el área backbone, independientemente de la existencia de una conexión directa entre las dos áreas. Aunque es posible el funcionamiento de una red OSPF únicamente con el área backbone, OSPF escala bien cuando la red se subdivide en un número de áreas más pequeñas.

OSPF es un protocolo de enrutamiento por estado de enlace que a diferencia de RIP e IGRP que publican sus rutas sólo a routers vecinos, los routers OSPF envían publicaciones del estado de enlace **LSA** (Link-State Advertisment) a todos los routers pertenecientes a la misma área jerárquica mediante una multidifusión de IP. La LSA contiene información sobre las interfaces conectadas, la métrica utilizada y otros datos adicionales necesarios para calcular las bases de datos de la ruta y la topología de red. Los routers OSPF acumulan información sobre el estado de enlace y ejecutan el algoritmo **SPF** (que también se conoce con el nombre de su creador, Dijkstra) para calcular la ruta más corta a cada nodo.

Para determinar qué interfaces reciben las publicaciones de estado de enlace, los routers ejecutan el protocolo OSPF **Hello**. Los routers vecinos intercambian mensajes hello para determinar qué otros routers existen en una determinada interfaz y sirven como mensajes de actividad que indican la accesibilidad de dichos routers.

Cuando se detecta un router vecino, se intercambia información de topología OSPF. Cuando los routers están sincronizados, se dice que han formado una adyacencia.

Las LSA se envían y reciben sólo en adyacencias. La información de la LSA se transporta en paquetes mediante la capa de transporte OSPF que define un proceso fiable de publicación, acuse de recibo y petición para garantizar que la información de la LSA se distribuye adecuadamente a todos los routers de un área. Existen cuatro tipos de LSA. Los tipos más comunes son los que publican información sobre los enlaces de red conectados de un router y los que publican las redes disponibles fuera de las áreas OSPF.

La métrica de enrutamiento de OSPF es el **coste** que se calcula en base al ancho de banda de la interfaz y es configurable por parte del usuario.

La fórmula para calcular el coste es

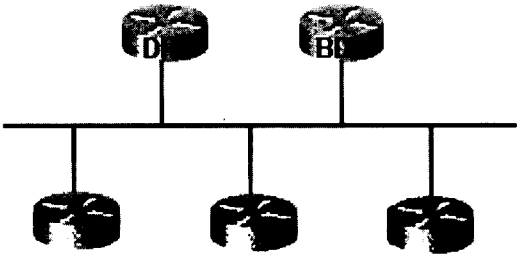
$$\frac{10^8}{\text{Ancho de banda}}$$

Funcionamiento de OSPF en una topología multiacceso con difusión

Dado que el enrutamiento OSPF depende del estado de enlace entre dos routers, los vecinos deben reconocerse entre si para compartir información. Este proceso se hace por medio del protocolo **Hello.**

Un router se ve a sí mismo listado en un paquete Hello que recibe de un vecino*

Los paquetes se envían cada 10 segundos (forma predeterminada) utilizando la dirección de multidifusión 224.0.0.5. Para declarar a un vecino caído el router espera cuatro veces el tiempo del intervalo **Hello** (intervalo **Dead**).



En redes con difusión se lleva a acabo la elección de DR y BDR

Los routers de un entorno multiacceso, como un entorno ethernet, deben elegir un Router Designado (**DR**) y un Router Designado de Reserva (**BDR**) para que representen a la red.

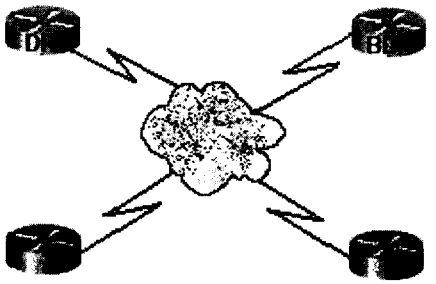
Un **DR** lleva a cabo tareas de envió y sincronización. El **BDR** solo actuará si el **DR** falla. Cada router debe establecer una adyacencia con el DR y el BDR.

Elección de un DR y un BDR en una topología Multiacceso con difusión

- El router con el valor de prioridad más alto es el Router Designado **DR**.
- El router con el segundo valor es el router designado de reserva **BDR**.
- El valor predeterminado de la prioridad OSPF de la interfaz es 1. Un router con prioridad 0 no es elegible. En caso de empate se usa el ID de router.
- ID DE ROUTER. Este número de 32 bits identifica únicamente al router dentro de un sistema autónomo. La dirección IP más alta de una interfaz activa se elige por defecto.

Funcionamiento de OSPF en una topología NBMA

Las redes **NBMA** son aquellas que soportan más de dos routers pero que no tienen capacidad de difusión. Frame-Relay, ATM, X.25 son algunos ejemplos de redes NBMA. La selección del DR se convierte en un tema importante ya que el DR y el BDR deben tener conectividad física total con todos los routers de la red.



OSPF en redes NBMA:
debe existir conectividad entre todos los routers

Funcionamiento de OSPF en una topología punto a punto

En redes punto a punto el router detecta dinámicamente a sus vecinos enviando paquetes **Hello** con la dirección de multidifusión 224.0.0.5. **No se lleva a cabo elección y no existe concepto de DR o BDR.**

Los intervalos **Hello** y **Dead** son de 10 y 40 segundos respectivamente.

OSPF en redes Punto a Punto:
no hay elección de DR ni BDR

Cómo mantener información sobre enrutamiento OSPF

Paso 1-Un router advierte un cambio de estado de un enlace y hace una multidifusión de un paquete LSU (actualización de estado de enlace) con la IP 224.0.0.6.

Paso 2-El DR acusa recepción e inunda la red con la LSU utilizando la dirección de multidifusión 224.0.0.5.

Paso 3-Si se conecta un router con otra red, reenviará la LSU al DR de dicha red.

Paso 4-Cuando un router recibe la LSU que incluye la LSA (publicación de estado de enlace) diferente, cambiará su base de datos.

Proceso de configuración de OSPF en un solo área

Habilitar OSPF por medio del comando:

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

Donde:

process-id es el número que se usa internamente para identificar si existen múltiples procesos OSPF en ejecución dentro del router.

network identifica las redes directamente conectadas, identificadas por medio de su correspondiente máscara de wildcard.

area para cada red, deberá identificar además a que área pertenece. El área principal o de Backbone es el área 0.

La modificación del ID de router OSPF en una dirección loopback implica definirla de la siguiente manera:

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

La modificación de la prioridad de router implica cambiar la prioridad OSPF de una interfaz por medio del siguiente comando:

```
Router(config-if)#ip ospf priority number
Router#show ip ospf interface type number
```

Cálculo del coste del enlace

El coste se calcula usando la formula 10^8/bandwidth donde el ancho de banda se expresa en bps. El cisco IOS determina automáticamente el coste basándose en el ancho de banda de la interfaz.

Para modificar el ancho de banda sobre la interfaz utilice el siguiente comando:

```
Router(config)#interface serial 0/0
Router(config-if)#bandwidth 64
```

Use el siguiente comando de configuración de interfaz para cambiar el coste del enlace:

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

Comandos de autenticación OSPF

```
Router(config-if)#ip ospf authentication-key password
Router(config-router)#area area-number authentication
Router(config-if)#ip ospf message-digest-key key-id md5 encryption-
type key
Router(config-router)#area area-id authentication message-digest
```

Para configurar los intervalos de Hello y de Dead en una interfaz utilizar los siguientes comandos:

```
Router(config-if)#ip ospf hello-interval seconds
Router(config-if)#ip ospf dead-interval seconds
```

Algunos comandos para el verificación y control OSPF son:

show ip route
Muestra la tabla de enrutamiento.

show ip protocols
Muestra los parámetros del protocolo.

show ip ospf neighbors
Muestra la información de los vecinos OSPF.

debug ip ospf events
Muestra adyacencias, DR, inundaciones etc.

debug ip ospf packet
Muestra la información de los paquetes.

debug ip ospf hello
Muestra las actualizaciones hello.

RECUERDE:

En principio el router intentará utilizar un ID buscando interfaces virtuales o loopback, si no encuentra configuración de las mismas lo hará con la interfaz física con la dirección IP más alta.

Los valores de los intervalos de Hello y de Dead deben coincidir en los router adyacentes para que OSPF funcione correctamente.

Ante la posibilidad de Flapping los routers esperan unos instantes antes de recalcular su tabla de enrutamiento.