Tipos de Enrutamiento

Los routers para conmutar los paquetes IP consultan su tabla de enrutamiento.

Esta se carga inicialmente y en forma automática con las redes que el router tiene configuradas en sus interfaces.

Para poder conmutar a redes remotas estas deben ser cargadas en la tabla de enrutamiento, ya sea en forma manual mediante el ingreso de comandos o en forma automática a través de un protocolo de enrutamiento.

- **Enrutamiento Estático**. El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los routers toda la información que contienen, es que el router no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red. Sin embargo, este método de enrutamiento resulta ventajoso en las siguientes situaciones:
    - Un circuito poco fiable que deja de funcionar constantemente. Un protocolo de enrutamiento dinámico podría producir demasiada inestabilidad, mientras que las rutas estáticas no cambian.
    - Se puede acceder a una red a través de una conexión de acceso telefónico. Dicha red no puede proporcionar las actualizaciones constantes que requiere un protocolo de enrutamiento dinámico.
    - Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.
    - Un cliente no desea intercambiar información de enrutamiento dinámico.
- **Enrutamiento Dinámico**. Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero.

Tipos de Direccionamiento y otros conceptos

Para el diseño de arquitectura de cualquier red, es también muy importante conocer y utilizar los siguientes conceptos:

- **Direccionamiento Sin Clase**. Modifica el enrutamiento con clase publicando la red y la máscara configurada, permitió el mejor aprovechamiento de las direcciones IP con el subneteo con máscaras de subred de longitud variable VLSM y la reducción de las tablas de enrutamiento con la publicación de resumen de redes o CIDR.
- **Subnetting**. La técnica de subnetting, permite dividir una red en varias subredes más pequeñas que contienen un menor número de hosts. Esto nos permite adquirir, por ejemplo, una red de clase B, y crear subredes para aprovechar este espacio de direcciones entre los distintos sitios de nuestra

empresa. Esto se consigue alterando la máscara natural, de forma que al añadir unos en lugar de ceros, hemos ampliado el número de subredes y disminuido el número de hosts para cada subred.

- **Máscara de Subred de Longitud Variable (VLSM)**. Utilizar protocolos de enrutamiento y dispositivos que soporten VLSM, nos permite poder utilizar diferentes máscaras en los distintos dispositivos de nuestra red, lo cual no es más que una extensión de la técnica de subnetting. Mediante VLSM, podemos dividir una clase C para albergar dos subredes de 50 máquinas cada una, y otra subred con 100 máquinas. Es importante tener en cuenta que RIP1 e IGRP no suportan VLSM.
- **Supernetting o CIDR**. La técnica de supernetting o agregación, permite agrupar varias redes en una única superred. Para esto se altera la máscara de red, al igual que se hacía en subnetting, pero en este se sustituyen algunos unos por ceros. El principal beneficio es para las tablas de enrutamiento, disminuyendo drásticamente su tamaño. Un dominio al que se le ha asignado un rango de direcciones tiene la autoridad exclusiva de la agregación de sus direcciones, y debería agregar todo lo que sea posible siempre y cuando no introduzca ambigüedades, lo cual es posible en el caso de redes con interconexiones múltiples a distintos proveedores.
- **Traducción de Dirección de Red (NAT)**. La tecnología NAT permite a las redes con IP privadas conectarse a Internet. El router NAT se coloca en la frontera de un dominio, de forma que cuando un equipo de la red privada se desea comunicar con otro en Internet, el router NAT envía los paquetes a Internet con la dirección pública del router, y cuando le responden renvía los paquetes al host de origen. Para realizar esto, basta con relacionar los sockets abiertos desde el equipo NAT a los equipos de la red privada, con los sockets abiertos desde el equipo NAT a los equipos de Internet, así como modificar las cabeceras de los paquetes renviados.
- **Convergencia**. La convergencia se refiere al tiempo que tardan todos los routers de la red en actualizarse en relación con los cambios que se han sufrido en la topología de la red.

Enrutamiento

Sistemas Autónomos

Un Sistema Autónomo (SA) es un conjunto de redes, o de routers, que tienen una única política de enrutamiento y que se ejecuta bajo una administración común, utilizando habitualmente un único IGP. Para el mundo exterior, el SA es visto como una única entidad. Cada SA tiene un número identificador de 16 bits, que se le asigna mediante un Registro de Internet (como RIPE, ARIN, o APNIC), o un proveedor de servicios en el caso de los SA privados. Así, conseguimos dividir el mundo en distintas administraciones, con la capacidad de tener una gran red dividida en redes más pequeñas y manipulables. En un POP dónde se junten varios SA, cada uno de estos utilizará un router de gama alta que llamaremos **router fronterizo**, cuya función principal es intercambiar tráfico e información de rutas con los distintos routers fronterizos del POP. Así, un concepto importante de comprender es el **tráfico de tránsito**, que no es más que todo tráfico que entra en un SA con un origen y destino distinto al SA local.

En Internet, la IANA es la organización que gestiona las direcciones IP y números de AS, teniendo en cuenta que cada Sistema Autónomo se identifica por un número inequívoco que no puede ser superior a 65535, teniendo en cuenta que la colección 65412-65535 son SA privados para ser utilizados entre los proveedores y los clientes. Así, podemos ponernos en contacto con RIPE, ARIN o APNIC para solicitar rangos de direcciones IP o números de AS.

- **SA de conexión única, sin tránsito**. Se considera que un SA es de conexión única cuando alcanza las redes exteriores a través de un único punto de salida. En este caso disponemos de varios métodos por los cuales el ISP puede aprender y publicar las rutas del cliente.
    - Una posibilidad para el proveedor es enumerar las subredes del cliente como entradas estáticas en su router, y publicarlas a Internet a través de BGP.
    - Alternativamente, se puede emplear un IGP entre el cliente y el proveedor, para que el cliente publique sus rutas.
    - El tercer método es utilizar BGP entre el cliente y el proveedor. En este caso, el cliente podrá registrar su propio número SA, o bien utilizar un número de SA privado si el proveedor tiene soporte para ello.
- **SA de múltiples conexiones, sin tránsito**. Un SA puede tener múltiples conexiones hacia un proveedor o hacia varios proveedores, sin permitir el pasó de tráfico de tránsito a través de él. Para ello, el SA sólo publicará sus propias rutas y no propagará las rutas que haya aprendido de otros SA. Los SA sin tránsito y con múltiples conexiones no necesitan realmente ejecutar BGP con sus proveedores, aunque es recomendable y la mayor parte de las veces es requerido por el proveedor.
- **SA de múltiples conexiones, con tránsito**. Esto es un SA con más de una conexión con el exterior, y que puede ser utilizado para el tráfico de tránsito por otros SA. Para ello, un SA de tránsito publicará las rutas que haya aprendido de otros SA, como medio para abrirse al tráfico que no le pertenezca. Es muy aconsejable (y en la mayoría de los casos requerido) que los SA de tránsito de múltiples conexiones utilicen BGP-4 para sus conexiones a otros SA, mientras que los routers internos pueden ejecutar enrutamiento predeterminado hacia los routers BGP.

Algoritmos de enrutamiento por vector de distancia

El término vector de distancia se deriva del hecho de que el protocolo incluye un vector (lista) de distancias (número de saltos u otras métricas) asociado con cada destino, requiriendo que cada nodo calcule por separado la mejor ruta para cada destino. Los envían mensajes actualizados a intervalos establecidos de tiempo, pasando toda su tabla de enrutamiento al router vecino más próximo (routers a los que está directamente conectado), los cuales repetirán este proceso hasta que todos los routers de la red están actualizados. Si un enlace o una ruta se vuelven inaccesibles justo después de una actualización, la propagación del fallo en la ruta se iniciará en la próxima propagación, ralentizándose la convergencia. Los protocolos de vector de distancia más nuevos, como EIGRP y RIP-2, introducen el concepto de **actualizaciones desencadenadas**. Éstas propagan los fallos tan pronto ocurran, acelerando la convergencia considerablemente. Los protocolos por

vector de distancia tradicionales trabajan sobre la base de actualizaciones periódicas y contadores de espera: si no se recibe una ruta en un cierto periodo de tiempo, la ruta entra en un estado de espera, envejece y desaparece, volviéndose inalcanzable.

Bucles de Enrutamiento en Algoritmos por Vector de Distancia

Los bucles de enrutamiento producen entradas de enrutamiento incoherentes, debido generalmente a un cambio en la topología. Si un enlace de un router A se vuelve inaccesible, los routers vecinos no se dan cuenta inmediatamente, por lo que se corre el riego de que el router A crea que puede llegar a la red perdida a través de sus vecinos que mantienen entradas antiguas. Así, añade una nueva entrada a su tabla de enrutamiento con un coste superior. A su vez, este proceso se repetiría una y otra vez, incrementándose el coste de las rutas, hasta que de alguna forma se parase dicho proceso. Los métodos utilizados para evitar este caso son los que siguen:

- **Horizonte Dividido**. La regla del horizonte dividido es que nunca resulta útil volver a enviar información acerca de una ruta a la dirección de dónde ha venido la actualización original.
- **Actualización Inversa**. Cuando una red de un router falla, este envenena su enlace creando una entrada para dicho enlace con coste infinito. Así deja de ser vulnerable a actualizaciones incorrectas proveniente de routers vecinos, donde esté involucrada dicha red. Cuando los routers vecinos ven que la red ha pasado a un coste infinito, envían una actualización inversa indicando que la ruta no está accesible.
- **Definición de Máximo**. Con este sistema, el protocolo de enrutamiento permite la repetición del bucle hasta que la métrica exceda el valor máximo permitido. Una vez que la red alcanza ese máximo, se considera inalcanzable.
- **Actualización desencadenada**. Normalmente, las nuevas tablas de enrutamiento se envían a los routers vecinos a intervalos regulares. Una actualización desencadenada es una nueva tabla de enrutamiento que se envía de forma inmediata, en respuesta a un cambio. El router que detecta el cambio envía inmediatamente un mensaje de actualización a los routers adyacentes que, a su vez, generan actualizaciones desencadenadas para notificar el cambio a todos sus vecinos. Sin embargo surgen dos problemas:
    - Los paquetes que contienen el mensaje de actualización podrían ser descartados o dañados por algún enlace de la red.
    - Las actualizaciones desencadenadas no suceden de forma instantánea. Es posible que un router que no haya recibido aún la actualización desencadenada genere una actualización regular que cause que la ruta defectuosa sea insertada en un vecino que hubiese recibido ya la actualización.

Combinando las actualizaciones desencadenadas con los temporizadores se obtiene un esquema que permite evitar estos problemas

Algoritmos de enrutamiento de estado de enlace

Utilizan un modelo de base de datos distribuida y replicada. Los routers intercambian paquetes de hello con sus vecinos para establecer que el enlace esta activo y publican actualizaciones de estado de enlace que informan a todos los routers de la red cuando el estado de sus interfaces (o enlaces) se modifica.

Esto significa que sólo se envía información acerca de las conexiones directas de un determinado router, (y no toda la tabla de enrutamiento) cuando hay una modificación en la topología (y no en forma periódica) como ocurre en el enrutamiento por vector de distancia.

Aplicando el algoritmo SPF (primero la ruta más corta), más conocido como algoritmo Dijkstra, cada router calcula un árbol de las ruta más cortas hacia cada destino, situándose a sí mismo en la raíz. Los protocolos de estado de enlace no pueden proporcionar una solución de conectividad global, como la que se requiere en grandes redes como Internet, pero si son utilizados por muchos proveedores como protocolo de enrutamiento en el interior de un SA. Los protocolos más conocidos son OSPF e IS-IS. Algunos de los beneficios de estos protocolos son:

- No hay límite en el número de saltos de una ruta. Los protocolos del estado de enlace trabajan sobre la base de las métricas de enlace en lugar de hacerlo en función del número de saltos.
- El ancho de banda del enlace y los retrasos puede ser factorizados cuando se calcule la ruta más corta hacia un destino determinado.
- Los cambios de enlace y nodo son inmediatamente introducidos en el dominio mediante actualizaciones del estado de enlace, lo que asegura una convergencia rápida
- Soporte para VLSM y CIDR, ya que intercambian información de máscara en las actualizaciones.
- NO se producen bucles de enrutamiento.

Protocolos de Gateway Interior (IGP)

Se encargan del enrutamiento de paquetes dentro de un dominio de enrutamiento o sistema autónomo. Los IGP, como **RIP, EIGRP u OSPF**, se configuran en cada uno de los routers incluidos en el dominio.

- **Routing Information Protocol (RIP):** RIP es un protocolo universal de enrutamiento por vector de distancia que utiliza el número de saltos como único sistema métrico. Un salto es el paso de los paquetes de una red a otra. Si existen dos rutas posibles para alcanzar el mismo destino, RIP elegirá la ruta que presente un menor número de saltos. RIP no tiene en cuenta la velocidad ni la fiabilidad de las líneas a la hora de seleccionar la mejor ruta. RIP envía su tabla de enrutamiento a sus vecinos cada 30 segundos (tiempo predeterminado en routers Cisco), utilizando el protocolo UDP para el envío de los avisos y está limitado a un número máximo de 15 saltos.

RIP V1, no soporta VLSM y CIDR, y no soporta actualizaciones desencadenadas. RIP-1 puede realizar equilibrado de la carga en un máximo de seis rutas de igual coste.

RIP V2 es un protocolo sin clase que admite CIDR, VLSM, resumen de rutas y seguridad y autenticación MD5.

Open Short Path First (OSPF). OSPF es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP. Básicamente, OSPF utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes. **OSPF soporta VLSM**, ofrece **convergencia rápida**, **autenticación** de origen de ruta, y publicación de ruta mediante multidifusión. **OSPF publica sus rutas a todos los routers de la misma área**. En la RFC 2328 se describe el concepto y operatividad del estado de enlace en OSPF, mientras que la implementación de OSPF versión 2 se muestra en la RFC 1583. OSPF toma las decisiones en función del corte de la ruta, disponiendo de una **métrica máxima de 65535**.

OSPF funciona dividiendo una intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza con un área backbone mediante un router fronterizo. Así, todos los paquetes direccionados desde un área a otra diferente, atraviesan el área backbone. OSPF envía Publicaciones del Estado de Enlace (Link-State Advertisement – LSA) a todos los routers pertenecientes a la misma área jerárquica mediante **multidifusión IP**. 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. La información de la LSA se transporta en paquetes mediante la capa de transporte OSPF (con acuse de recibo) para garantizar que la información se distribuye adecuadamente. Para la configuración de OSPF se requiere un número de proceso, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. Los administradores acostumbran usar un número de SA como número de proceso

- **Interior Gateway Protocol (IGRP)**. IGRP fue diseñado por Cisco a mediados de los ochenta, para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grandes con enlaces de diferentes anchos de banda, siendo un protocolo **propietario de Cisco**. IGRP es un protocolo de enrutamiento por vector de distancia capaz de utilizar hasta **5 métricas distintas** (ancho de banda K1, retraso K3, carga, fiabilidad, MTU), utilizándose por defecto únicamente el ancho de banda y el retraso. Estas métrica pueden referirse al ancho de banda, a la carga (cantidad de tráfico que ya gestiona un determinado router) y al coste de la comunicación (los paquetes se envían por la ruta más barata). Para la configuración de OSPF se **requiere un número de proceso**, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. Los administradores acostumbran usar un número de SA como número de proceso. IGRP envía mensajes de actualización del enrutamiento a

intervalos de tiempo mayores que RIP, utiliza un formato más eficiente, y **soporta actualizaciones desencadenadas**. IGRP posee un número máximo predeterminado de 100 saltos, que puede ser configurado hasta 255 saltos, por lo que puede implementarse en grandes interconexiones donde RIP resultaría del todo ineficiente. IGRP puede mantener hasta un máximo de **seis rutas paralelas de coste diferente**; Por ejemplo, si una ruta es tres veces mejor que otra, se utilizará con una frecuencia tres veces mayor. **IGRP no soporta VLSM**. **IGRP publica sus rutas sólo a los routers vecinos**.

- **Enhaced IGRP - EIGRP**. Basado en IGRP y como mejora de este, es un protocolo híbrido que pretende ofrecer las ventajas de los protocolos por vector de distancia y las ventajas de los protocolos de estado de enlace. **EIGRP soporta VLSM** y soporta una **convergencia muy rápida**. **EIGRP publica sus rutas sólo a los routers vecinos**.

Protocolos de Gateway Exterior

Los protocolos de enrutamiento exterior fueron creados para controlar la expansión de las tablas de enrutamiento y para proporcionar una vista más estructurada de Internet mediante la división de dominios de enrutamiento en administraciones separadas, llamadas **Sistemas Autónomos (SA)**, los cuales tienen cada uno sus propias políticas de enrutamiento. Durante los primeros días de Internet, se utilizaba el protocolo **EGP** (no confundirlo con los protocolos de enrutamiento exterior en general). NSFNET utilizaba EGP para intercambiar información de accesibilidad entre el backbone y las redes regionales. Actualmente, **BGP IPv6** es el estándar a partir del 6 de junio del 2012 para el enrutamiento entre dominios en Internet.

- **Border Gateway Protocol (BGP)**. Es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, estándar en Internet. BGP gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados Sistemas Autónomos.

  Los routers BGP se configuran con la información del vecino a fin de que puedan formar una conexión TCP fiable sobre la que transportar información de la ruta de acceso del sistema autónomo y la ruta de la red. Tras establecer una sesión BGP entre vecinos, ésta sigue abierta a menos que se cierre específicamente o que haya un fallo en el enlace. Si dos routers vecinos intercambian información de ruta y sesiones BGP, se dice que son **iguales BGP**. En principio, los iguales BGP intercambian todo el contenido de las tablas de enrutamiento BGP. Posteriormente, sólo se envían actualizaciones incrementales entre los iguales para avisarles de las rutas nuevas o eliminadas.

  Todas las rutas BGP guardan el último número de versión de la tabla que se ha publicado a sus iguales, así como su propia versión interna de la tabla. Cuando se recibe un cambio en un igual, la versión interna se incrementa y

se compara con las versiones de los iguales, para asegurar que todos los iguales se mantienen sincronizados. BGP también guarda una tabla de rutas BGP independiente que contiene todas las rutas de acceso posibles a las redes publicadas.

Los iguales BGP se dividen en dos categorías: Los iguales BGP de distintos sistemas autónomos que intercambian información de enrutamiento son **iguales BGP externos (EBGP)**. Los iguales BGP del mismo sistema autónomo que intercambian información de enrutamiento son **iguales BGP internos (IBGP)**.

La selección de ruta óptima BGP se basa en la longitud de la ruta de acceso del sistema autónomo para una ruta de red. La longitud se define como el número de sistemas autónomos distintos necesarios para acceder a la red. Cuanto menor sea la distancia, más apetecible será la ruta de acceso. A través del uso de controles administrativos, BGP es uno de los protocolos de enrutamiento más flexibles y totalmente configurables disponibles.

Un uso típico de BGP, para una red conectada a Internet a través de varios ISP, es el uso de EBGP con los ISP, así como el uso de IBGP en la red interna, para así ofrecer una óptima selección de rutas. Las redes conocidas de otros sistemas autónomos a través de EBGP se intercambiarán entre los iguales IBGP. Si sólo hubiera un ISP, valdría con utilizar una ruta resumen o predeterminada para la salida a internet.

Tenga en cuenta que los routers BGP publican las rutas conocidas de un igual BGP a todos sus otros iguales BGP. Por ejemplo, las rutas conocidas a través de EBGP con un ISP se volverán a publicar a los iguales IBGP, que a su vez volverán a publicarlos a otros ISP a través de EBGP. Mediante la publicación reiterada de rutas, la red puede pasar a ser una red de tránsito entre los proveedores con los que se conecte. BGP puede parametrizarse tanto para que la red interna actúe como una red de tránsito, como para que no.

Criterios de Selección de Protocolos de Enrutamiento

- **Topología de Red**. Los protocolos del tipo OSPF e IS-IS requieren un modelo jerárquico formado un backbone y una o varias áreas lógicas, lo que nos puede llegar a exigir que rediseñemos la red.
- **Resumen de Ruta y Dirección**. Mediante VLSM podemos reducir considerablemente el número de entradas en la tabla de enrutamiento, y en consecuencia la carga de los routers, por lo que son recomendados protocolos como OSPF y EIGRP.
- **Velocidad de Convergencia**. Uno de los criterios más importantes es la velocidad con la que un protocolo de enrutamiento identifica una ruta no disponible, selecciona una nueva y propaga la información sobre ésta. Protocolos como RIP-1 e IGRP suelen ser más lentos en converger que protocolos como EIGRP y OSPF.
- **Criterios de Selección de Ruta**. Cuando las diferentes rutas de la Intranet se compongan de varios tipos de medios LAN y WAN, puede ser

desaconsejable un protocolo que dependa estrictamente del número de satos, como es el caso de RIP. RIP considera que el salto de un router en un segmento Fast Ethernet tiene el mismo coste que un salto por un enlace WAN a 56 Kbps.

- **Capacidad de ampliación**. Los protocolos de vector de distancia consumen menos ciclos de CPU que los protocolos de estado de enlace con sus complejos algoritmos SPF. Sin embargo, los protocolos de estado de enlace consumen menos ancho de banda que los protocolos de vector de distancia.
- **Sencillez de implementación**. RIP, IGRP, y EIGRP no requieren mucha planificación ni organización en la topología para que se puedan ejecutar de manera eficaz. OSPF e IS-IS requieren que se haya pensado muy cuidadosamente la topología de la red y los modelos de direccionamiento antes de su implementación.
- **Seguridad**. Algunos protocolos como OSPF y EIGRP admiten poderosos métodos de autenticación, como las autenticaciones de claves MD5.
- **Compatibilidad**. Teniendo en cuenta el carácter propietario de Cisco de protocolos como IGRP y EIGRP, dichos protocolos no los podremos utilizar con protocolos de distintos fabricantes.

La regla de enrutamiento de correspondencia más larga

Un router que tenga que decidir entre dos prefijos de longitudes diferentes de la misma red siempre seguirá la máscara más larga (es decir, la ruta de red más específica). Suponga, por ejemplo, que un router tiene las dos entradas siguientes en su tabla de enrutamiento.

- 192.32.1.0/24 por la ruta 1.
- 192.32.0.0/16 por la ruta 2.

Cuando intenta enviar tráfico al host 192.32.1.1, el router lo intentará pasar por la ruta 1. Si la ruta 1 no estuviese disponible por alguna razón, entonces lo pasaría por la ruta 2.

Bucles de Enrutamiento y Agujeros Negros

Un **bucle de enrutamiento** se produce cuando el tráfico circula hacia atrás y hacia delante entre elementos de la red, no alcanzando nunca su destino final. Suponga que la conexión entre el ISP1 y su cliente Foonet (dónde existe la red 192.32.1.0/24) se vuelve inaccesible. Suponga también que el ISP1 tiene una ruta predeterminada 0.0.0.0/0 que apunta a ISP2 para las direcciones no conocidas. El tráfico hacia 192.32.1.1 no encontrará su destino en ISP1, por lo que seguirá la ruta predeterminada hacia ISP2, volviendo a ISP1 y a ISP2, y así una y otra vez.

Un **agujero negro** ocurre cuando el tráfico llega y se para en un destino que no es el destino propuesto y desde el que no puede ser renviado.

Estas dos situaciones tienden a ocurrir cuando se dispone de tablas de enrutamiento gestionadas en una parte por protocolos de enrutamiento, y en otra

por rutas estáticas, así como por una incorrecta agregación de rutas de otros proveedores.

Resumen de Protocolos de Enrutamiento

	RIP-2	EIGRP	OSPF	BGP
¿Soporta VLSM?	SI	SI	SI	SI
Velocidad Convergencia	Media	Rápida	Rápida	Rápida
Tecnología	Vector	Vector	Enlace	Vector
Número máx. Saltos	15	224	65535	
Seguridad	MD5	MD5	MD5	
Selección de Ruta	Saltos	Varias Métricas	Ancho Banda	
Compatibilidad	Universal	Cisco	Universal	Universal
Tipo	IGP	IGP	IGP	EGP
¿Proceso / ASN?	NO	PROCESO	PROCESO	ASN
¿Despende de Topología?	NO	NO	SI	NO