Algoritmos de Enrutamiento

Los protocolos de enrutamiento para la capa de red son usados para resolver peticiones de servicios de envío de paquetes de datos a través de diferentes redes de datos. El objetivo de esta sección es analizar algunos de los protocolos de enrutamiento vector-distancia y Estado de Enlace.

Introducción

La capa de Red, dentro de una arquitectura de redes de datos, es la que se encarga de llevar los paquetes de datos desde el origen (estación transmisora) hasta el destino (estación receptora). Llegar a destino, en tiempo y forma, puede requerir que el algoritmo de ruteo, que es el encargado de escoger las rutas y las estructuras de datos, cumpla con ciertas propiedades que aseguren la eficiencia de su trabajo.

Estas propiedades son: corrección, estabilidad, robustez, equitatividad, sencillez y optimalidad

La corrección y la sencillez casi no requieren comentarios; no así la necesidad de robustez, la cual se refiere a que el algoritmo debe ser diseñado para que funcione dentro de la red por años, sin fallas generales. El algoritmo deberá estar preparado para manejar cambios de topología y tráfico sin requerir el aborto de las actividades o el rearranque de la red.

La equitatividad y la optimalidad resultan con frecuencia contradictorias, ya que muchas veces se requiere una concesión entre la eficacia global (optimización) y la equitatividad; es decir, antes de intentar encontrar un justo medio entre estas dos, se debe decidir qué es lo que se busca optimizar.

Minimizar el retardo de los paquetes (disminuyendo escalas y ancho de banda) y maximizar el rendimiento total de la red sería la combinación más apropiada para un algoritmo de ruteo.

Propósitos de los protocolos de enrutamiento y de los sistemas autónomos

El objetivo de un protocolo de enrutamiento es crear y mantener una tabla de enrutamiento. Esta tabla contiene las redes conocidas y los puertos asociados a dichas redes. Los routers utilizan protocolos de enrutamiento para administrar la información recibida de otros routers, la información que se conoce a partir de la configuración de sus propias interfaces, y las rutas configuradas manualmente.

Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en las tablas de enrutamiento y descartan las rutas que ya no son válidas. El router utiliza la información en la tabla de enrutamiento para enviar los paquetes de datos.

El algoritmo de enrutamiento es fundamental para el enrutamiento dinámico. Al haber cambios en la topología de una red, por razones de crecimiento, reconfiguración o falla, la información conocida acerca de la red también debe cambiar. La información conocida debe reflejar una visión exacta y coherente de la nueva topología.

Cuando todos los routers de una red se encuentran operando con la misma información, se dice que la red ha hecho convergencia. Una rápida convergencia es deseable, ya que reduce el período de tiempo durante el cual los routers toman decisiones de enrutamiento erróneas.

Los sistemas autónomos (AS) permiten la división de la red global en subredes de menor tamaño, más manejables. Cada AS cuenta con su propio conjunto de reglas y políticas, y con un único número AS que lo distingue de los demás sistemas autónomos del mundo.

Algoritmos de Enrutamiento

El algoritmo de enrutamiento es la parte del software de la capa de red encargada de decidir la línea de salida por la que se transmitirá un paquete de entrada.

Si la subred usa datagramas entonces esta decisión debe hacerse cada vez que llega un paquete de datos de entrada, debido a que la mejor ruta podría haber cambiado desde la última vez.

Si la subred utiliza circuitos virtuales internamente, las decisiones de enrutamiento se tomarán sólo al establecerse el circuito y los paquetes seguirán la ruta previamente establecida.

Clasificación de Algoritmos de Enrutamiento

Los algoritmos de enrutamiento pueden agruparse en dos clases principales:

Algoritmos No adaptables: No basan sus decisiones de enrutamiento en mediciones o estimaciones del tráfico ni en la topología. La decisión de qué ruta tomar de I a J se calcula por adelantado, fuera de línea y se cargan en los routers al iniciar la red. Éste procedimiento se llama enrutamiento estáticos.

Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas.
Debido a que las rutas estáticas deben configurarse manualmente, cualquier cambio en la topología de la red requiere que el administrador agregue o elimine las rutas estáticas afectadas por dichos cambios. En una red de gran tamaño, el mantenimiento manual de las tablas de enrutamiento puede requerir de una enorme cantidad de tiempo de administración. En redes pequeñas, con pocos cambios, las rutas estáticas requieren muy poco mantenimiento. Debido a los requisitos de administración adicionales, el enrutamiento estático no tiene la escalabilidad o capacidad de adaptarse al crecimiento del

enrutamiento dinámico. Aun en redes de gran tamaño, a menudo se configuran rutas estáticas, cuyo objetivo es satisfacer requerimientos específicos, junto con un protocolo de enrutamiento dinámico.

Las operaciones con rutas estáticas pueden dividirse en tres partes, como sigue:

- El administrador de red configura la ruta.
- El router instala la ruta en la tabla de enrutamiento.
- Los paquetes se enrutan de acuerdo a la ruta estática.

Algoritmos Adaptables: En contraste con los algoritmos no adaptables, éstos cambian sus decisiones de enrutamiento para reflejar los cambios de topología y de tráfico. Difieren de los algoritmos estáticos en el lugar de obtención de su información (ej. localmente, en los routers adyacentes o de todos), el momento del cambio de sus rutas (ej. cada t seg., o cuando cambia la carga) y la métrica usada para la optimalidad (ej. distancia, no de escalas, tiempo estimado del tránsito). Este tipo de algoritmos no pueden ser demasiado complejos ya que son implementados en los routers y deben ejecutarse en tiempo real con recursos de CPU y la memoria con que el router dispone. En las siguientes secciones estudiaremos una variedad de algoritmos de enrutamiento dinámicos, que es el caso de estudio.

Principio de Optimización

Este postulado establece que, si el enrutador J está en la trayectoria óptima del enrutador I al enrutador K, entonces la trayectoria óptima de J a K también está en la misma ruta. Haciendo referencia a la Fig. 1.1, llamemos r1 a la parte de la ruta de I a J, y r2 al resto de la ruta. Si existiera una ruta mejor que r2 entre J y K, podría concatenarse con r1 para mejorar la ruta entre I y K, contradiciendo nuestra aseveración de que r 1 y r2 es óptima.

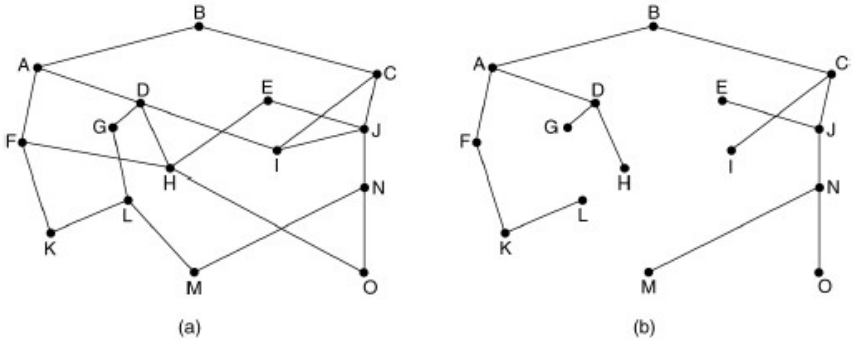

Fig. 1.1 (a) Subred. (b) Árbol de Descenso para el enrutador B.

Como consecuencia directa del principio de optimalidad, podemos ver que el grupo de trayectorias óptimas de todas las de orígenes a un destino dado forma un árbol con raíz en el destino. Ese árbol que se forma, se llama árbol de descenso, donde la métrica de distancia es el número de escalas. El árbol de descenso puede no ser único, pueden existir otros árboles con las mismas longitudes de trayectoria.

Dado que un árbol de descenso ciertamente es un árbol, no contiene ciclos, por lo que cada paquete será entregado con un número de escalas infinito y limitado.

En la práctica, no siempre sucede esto, los enlaces y los enrutadores pueden caerse y reactivarse durante la operación, por lo que diferentes enrutadores pueden tener ideas distintas sobre la topología actual de la subred.

Algoritmos Dinámicos

La mayoría de los algoritmos de enrutamiento pertenecen a una de estas dos categorías:

- Vector-distancia
- Estado del enlace

Enrutamiento Vector de Distancia

Los algoritmos de enrutamiento por vector de distancia operan haciendo que cada enrutador mantenga una tabla (por ejemplo, un vector) que da la mejor distancia conocida a cada destino y la línea a usar para llegar ahí. Estas tablas se actualizan intercambiando información con vecinos.

Este algoritmo recibe otros nombres como: algoritmo de enrutamiento Bellman-Ford distribuido y el algoritmo Ford-Fullkerson, en reconocimiento a los investigadores que lo desarrollaron.

En el enrutamiento por vector de distancia, cada enrutador mantiene una tabla de enrutamiento indizada por, y conteniendo un registro de, cada enrutador de la subred. Esta entrada comprende dos partes: la línea preferida de salida hacia ese destino y una estimación del tiempo o distancia a ese destino.

La métrica usada podría ser la cantidad de escalas, el retardo de tiempo en milisegundos, el número total de paquetes encolados por la trayectoria, o algo parecido.

Supóngase que se usa como métrica el retardo y que el enrutador conoce el retardo a cada uno de sus vecinos. Cada T mseg, cada enrutador envía a todos sus vecinos una lista de los retardos estimados a cada uno de los destinos. También recibe una lista parecida de cada vecino. Imagine que una de estas tablas acaba de llegar del vecino X, siendo Xi la estimación de X respecto al tiempo que le toma llegar al enrutador i a través de X en Xi + m mseg vía X . Efectuando este cálculo para cada vecino, un

enrutador puede encontrar la estimación que parezca ser la mejor y usar esa estimación y la línea correspondiente en su nueva tabla de enrutamiento.

Este proceso de actualización se ilustra en la Fig. 1.2. En la parte (a) se muestra una subred. En las primeras cuatro columnas de la parte (b) aparecen los vectores de retardo recibidos de los vecinos del enrutador J. A indica tener un retardo de 12 mseg a B, un retardo de 25 mseg a C, un retado de 40 mseg a D, etc. Suponiendo que J ha medido o estimado el retardo de sus miembros, A, I, H y K en 8, 10, 12 y 16 mseg, respectivamente.
Considere la manera en que J calcula su nueva ruta al enrutador G. Sabe que puede llegar a A en 8 mseg, y A indica ser capaz de llegar a G en 18 mseg, por lo que J sabe que puede contar con un retador de 26 mseg a G si enviaría a A los paquetes destinados a G. Del mismo modo, J calcula el retardo a G a través de I, H y K en 41 (31+10), 18 (6+12) y 37 (31+6) mseg, respectivamente. El mejor de estos valores es 18, por lo que escribe una entrada en su tabla de enrutamiento indicando que el retardo a G es de 18 mseg, y que la ruta a usar es vía H. Se lleva a cabo el mismo cálculo para los demás destinos, y la nueva tabla de enrutamiento se muestra en la última columna de la Fig. 1.2.

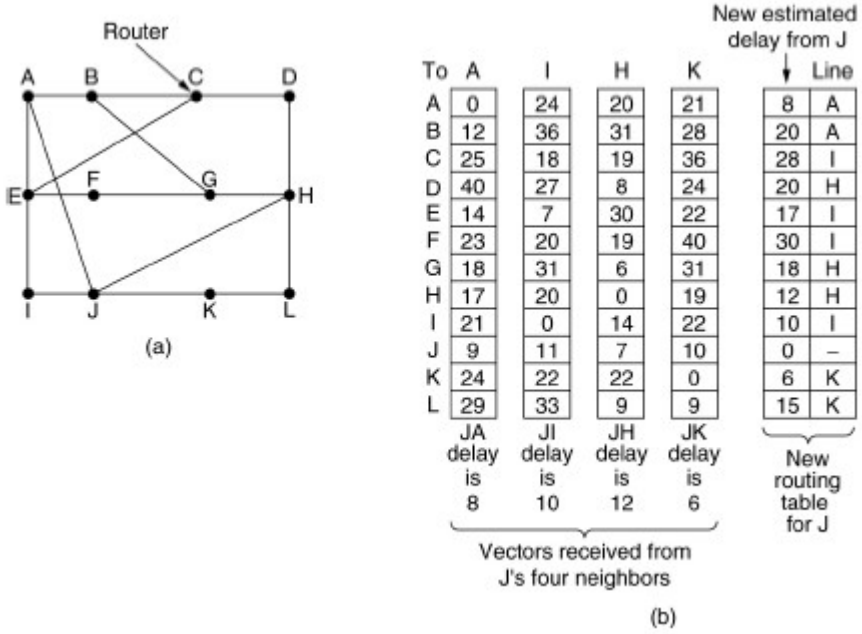

Fig. 1.2: (a) Subred. (b) Entrada de A, I, H, K, y la nueva Tabla de Enrutamiento de J.

Los algoritmos de vector-distancia no permiten que un router conozca la topología exacta de una red, ya que cada router solo ve a sus routers vecinos.
Cada router que utiliza el enrutamiento por vector-distancia comienza por identificar sus propios vecinos.

Las actualizaciones de las tablas de enrutamiento se producen al haber cambios en la topología. Al igual que en el proceso de descubrimiento de la red, las actualizaciones de cambios de topología avanzan paso a paso, de un router a otro.

Actualizaciones en el enrutamiento por vector - distancia

En el protocolo de vector-distancia, las actualizaciones de las tablas de enrutamiento se hacen periódicamente, o cuando cambia la topología de la red. Es importante que un protocolo de enrutamiento sea eficiente en su tarea de actualizar las tablas de enrutamiento. Al igual que en el proceso de descubrimiento de la red, las actualizaciones de cambio de topología se producen de forma sistemática de un enrutador a otro.

Los algoritmos de vector - distancia requieren que cada enrutador envíe toda la tabla de enrutamiento a cada uno de sus vecinos adyacentes. Las tablas de enrutamiento incluyen información acerca del costo total de la ruta (definido por su métrica) y la dirección lógica del primer enrutador en la ruta hacia cada una de las redes indicadas en la tabla.

Bucles en el enrutamiento por vector-distancia

Los bucles de enrutamiento pueden ser el resultado de tablas de enrutamiento incongruentes, las cuales no se han actualizado debido a la lenta convergencia de una red sujeta a cambios. En la siguiente Fig.1.3, se ilustra el resultado de un bucle de enrutamiento.

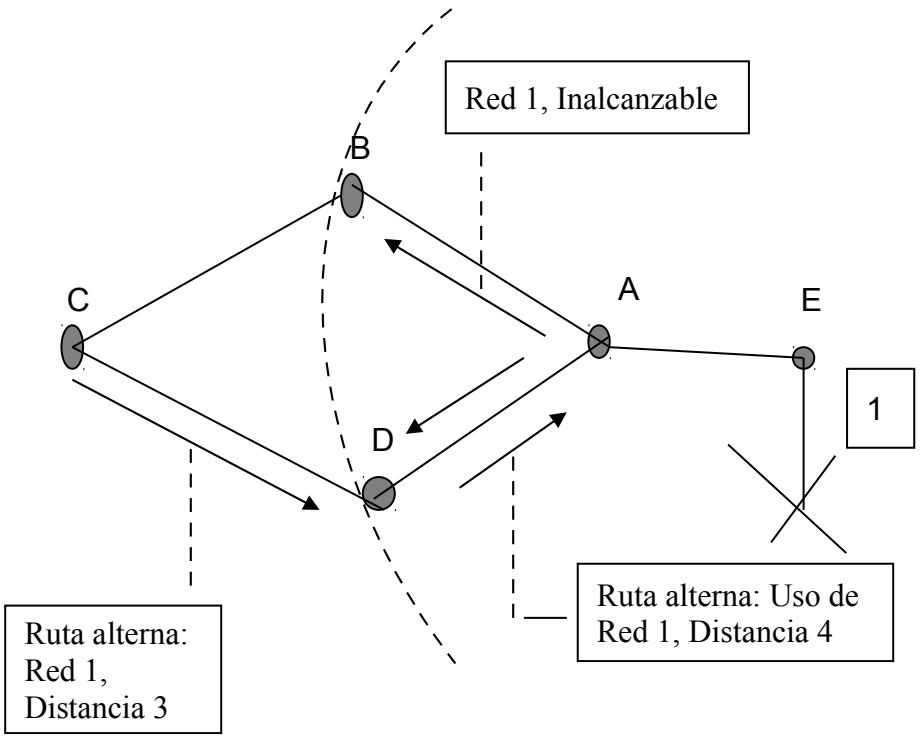

Fig. 1.3: Bucles de Enrutamiento

1. Antes de la falla de la red 1, todos los enrutadores poseen información coherente y tablas de enrutamiento correctas. Se dice que la red ha logrado la convergencia. Supongamos, para el resto de este ejemplo, que la ruta preferida del enrutador C hacia la red 1 es a través del enrutador B y que la distancia del enrutador C a la Red 1 es 3.

2. En el momento en que la red 1 falla, el enrutador E envía una actualización al enrutador A. El enrutador A deja de enrutar paquetes hacia la red 1, pero los enrutadores B, C y D siguen haciéndolo porque todavía no se les ha informado acerca de la falla. Cuando el enrutador A envía su actualización, los enrutadores B y D detienen el enrutamiento hacia la red 1; sin embargo, el enrutador C no ha recibido la actualización. Para el enrutador C, la red 1 todavía se puede alcanzar a través del enrutador B.

3. El enrutador C envía ahora una actualización periódica al enrutador D, que señala una ruta hacia la red 1 a través del enrutador B. El renrutador D cambia su tabla de enrutamiento para introducir esta información buena pero errónea, y transmite la información al enrutador A. El enrutador A transmite la información a los enrutadores B y E, etc. Cualquier paquete destinado a la red 1 ahora realizará un bucle desde el enrutador C al B, de allí al A y luego al D, y volverá nuevamente al C.

1.6.3.4 Definición de cuenta máxima

Las actualizaciones erróneas de la red 1 continuarán generando bucles hasta que algún otro proceso lo detenga. Esta condición, denominada cuenta al infinito, hace que los paquetes recorran la red en un ciclo continuo, a pesar del hecho fundamental de que la red de destino, la red 1, está fuera de servicio. Mientras los enrutadores cuentan al infinito, la información errónea hace que se produzca un bucle de enrutamiento.

Si no se toman medidas para detener la cuenta al infinito, la métrica del vector-distancia del número de saltos aumenta cada vez que el paquete atraviesa otro enrutador. Estos paquetes hacen un recorrido cíclico por la red debido a la información errónea en las tablas de enrutamiento.

Los algoritmos de enrutamiento por vector-distancia se corrigen automáticamente, pero un bucle de enrutamiento puede requerir primero una cuenta al infinito. Para evitar este problema, los protocolos de vector-distancia definen el infinito como un número máximo específico. Este número se refiere a una métrica de enrutamiento, la cual puede ser el número de saltos.

Con este enfoque, el protocolo de enrutamiento permite que el bucle de enrutamiento continúe hasta que la métrica supere el máximo valor permitido. En cualquier caso, cuando el valor de la métrica supera el valor máximo, se considera que no se puede alcanzar la red 1.

1.6.3.4 Eliminación de los bucles de enrutamiento mediante el horizonte dividido

Otra fuente posible de bucles de enrutamiento se presenta cuando se envía información incorrecta a un enrutador, la cual contradice información correcta que este envió originalmente. Así es como se produce el problema, Fig. 1.3:

1. El enrutador A transfiere una actualización al enrutador B y al enrutador D, la cual indica que la red 1 está fuera de servicio. El enrutador C, sin embargo, transmite una actualización

periódica al enrutador B, que señala que la red 1 está disponible a una distancia de 4, a través del enrutador D. Esto no rompe las reglas del horizonte dividido.

2. El enrutador B determina erróneamente que el enrutador C todavía tiene una ruta válida hacia la red 1, aunque con una métrica mucho menos favorable. El enrutador B envía una actualización periódica al enrutador A la cual indica al enrutador A la nueva ruta hacia la red 1.

3. El enrutador A ahora determina que puede enviar paquetes a la red 1 a través del enrutador B, el enrutador B determina que puede enviar paquetes a la red 1 a través del enrutador C, y el enrutador C determina que puede enviar paquetes a la red 1 a través del enrutador D. Cualquier paquete introducido en este entorno quedará atrapado en un bucle entre los enrutadores.

4. El horizonte dividido busca evitar esta situación. Si la actualización de enrutamiento relativa a la red 1 es enviada desde el router A, el router B o D no pueden enviar información sobre la red 1 de vuelta hacia el router A. El horizonte dividido reduce así los errores de enrutamiento, y también disminuye el procesamiento de información de enrutamiento.

1.6.3.5 Envenenamiento de rutas

El envenenamiento de rutas es utilizado por varios protocolos de vector-distancia para resolver grandes bucles de enrutamiento. A menudo, provee información explícita cuando no es posible el acceso a una subred o red. Esto se lleva a cabo normalmente mediante la configuración del número de saltos en la cantidad máxima más uno.

Una forma de evitar actualizaciones incongruentes es el envenenamiento de rutas. En la Fig. 1.4, cuando la red 5 sale fuera de servicio, el enrutador E inicia el envenenamiento de la ruta, mediante una entrada de valor 16 para la red 5, es decir, fuera de alcance.

Debido al envenenamiento de la ruta hacia la red 5, el enrutador C no es susceptible de efectuar actualizaciones incorrectas de la ruta hacia dicha red. Cuando el enrutador C recibe el envenenamiento de ruta desde el enrutador E, envía una actualización llamada actualización de envenenamiento inversa de vuelta al enrutador E. Esto asegura que todas las rutas del segmento hayan recibido la información del envenenamiento de la ruta.

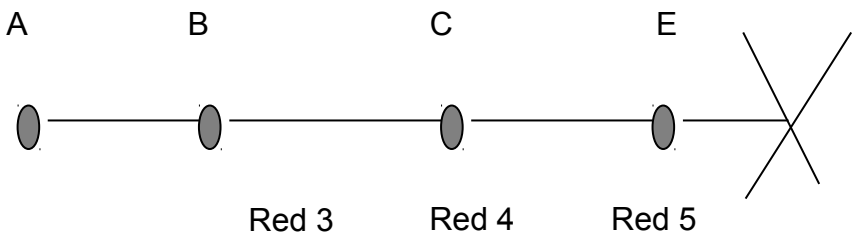

Fig. 1.4: Envenenamiento de Rutas

Cuando se combina el envenenamiento de rutas con las actualizaciones generadas por eventos, se agiliza el tiempo de convergencia ya que los routers vecinos no tienen que esperar 30 segundos antes de publicar la ruta envenenada.

El envenenamiento de rutas hace que el protocolo de enrutamiento publique rutas de métrica infinita para la ruta que está fuera de servicio. El envenenamiento de rutas no rompe las reglas del horizonte dividido. El horizonte dividido con envenenamiento de rutas es en esencia un envenenamiento de rutas, pero, colocada en los enlaces en los el horizonte dividido no permitiría el paso de información de enrutamiento. En cualquiera de los casos, el resultado es que las rutas que están fuera de servicio se publican con métricas infinitas.

1.6.3.6 Prevención de bucles de enrutamiento mediante temporizadores de espera

El problema de la cuenta al infinito puede evitarse mediante los temporizadores de espera (holddown timers):

- Si un enrutador recibe una actualización de un enrutador vecino, la cual indique que una red previamente accesible está ahora inaccesible, el enrutador marca la ruta como inaccesible y arranca un temporizador de espera. Si en algún momento, antes de que expire el temporizador de espera, se recibe una actualización por parte del mismo enrutador, la cual indique que la red se encuentra nuevamente accesible, el enrutador marca la red como accesible y desactiva el temporizador de espera.

- Si llega una actualización desde un enrutador distinto, la cual establece una métrica más conveniente que la originalmente registrada para la red, el enrutador marca la red como accesible y desactiva el temporizador de espera.

- Si en algún momento antes de que expire el temporizador de espera se recibe una actualización de un router distinto, la cual establece una métrica menos conveniente que la originalmente registrada para la red, la actualización no será tomada en cuenta. El descartar las actualizaciones con métricas menos convenientes mientras el temporizador de espera se encuentra activado, da más tiempo para que la información relativa a un cambio perjudicial sea transmitido a toda la red.

1.6.4 Protocolo RIP

1.6.4.1 Caracteristica del protocolo RIP

La Internet es una colección de varios sistemas autónomos (AS). Cada AS posee una tecnología de enrutamiento que puede diferir de otros sistemas autónomos. El protocolo de enrutamiento utilizado

dentro de un AS se conoce como Protocolo de enrutamiento interior (IGP). Un protocolo distinto utilizado para transferir información de enrutamiento entre los distintos sistemas autónomos se conoce como Protocolo de enrutamiento exterior (EGP). RIP está diseñado para trabajar como IGP en un AS de tamaño moderado. No ha sido concebido para utilizarse en entornos más complejos. RIP v1 se considera un IGP con clase.

RIP v1 es un protocolo de vector-distancia que envía la tabla de enrutamiento completa en broadcast a cada router vecino a determinados intervalos. El intervalo por defecto es de 30 segundos. RIP utiliza el número de saltos como métrica, siendo 15 el número máximo de saltos.

Si el router recibe información sobre una red y la interfaz receptora pertenece a la misma red pero se encuentra en una subred diferente, el router aplica la máscara de subred que está configurada en la interfaz receptora:

- Para las direcciones de Clase A, la máscara con clase por defecto es 255.0.0.0.
- Para las direcciones de Clase B, la máscara con clase por defecto es 255.255.0.0.
- Para las direcciones de Clase C, la máscara con clase por defecto es 255.255.255.0.

RIP v1 es un protocolo de enrutamiento común dado que prácticamente todos los routers IP lo admiten. La popularidad de RIP v1 se basa en la simplicidad y su demostrada compatibilidad universal. RIP es capaz de equilibrar las cargas hasta en seis rutas de igual costo, siendo cuatro rutas la cantidad por defecto.

RIP v1 posee las siguientes limitaciones:

- No envía información de máscara de subred en sus actualizaciones.
- Envía las actualizaciones en broadcasts a 255.255.255.255.
- No admite la autenticación
- No puede admitir enrutamiento entre dominios de VLSM o sin clase (CIDR).

RIP v1 es de muy fácil configuración.

RIP ha evolucionado a lo largo de los años desde el Protocolo de enrutamiento con definición de clases, RIP Versión 1 (RIP v1), hasta el Protocolo de enrutamiento sin clase, RIP Versión 2 (RIP v2). Las mejoras en RIP v2 incluyen:

- Capacidad para transportar mayor información relativa al enrutamiento de paquetes.

- Mecanismo de autenticación para la seguridad de origen al hacer actualizaciones de las tablas.

- Soporta enmascaramiento de subredes de longitud variable (VLSM).

- RIP evita que los bucles de enrutamiento se prolonguen en forma indefinida, mediante la fijación de un límite en el número de saltos permitido en una ruta, desde su origen hasta su destino. El número máximo de saltos permitido en una ruta es de 15. Cuando un router recibe una actualización de

enrutamiento que contiene una entrada nueva o cambiada, el valor de la métrica aumenta en 1, para incluir el salto correspondiente a sí mismo. Si este aumento hace que la métrica supere la cifra de 15, se considera que es infinita y la red de destino se considera fuera de alcance. RIP incluye diversas características las cuales están presentes en otros protocolos de enrutamiento. Por ejemplo, RIP implementa los mecanismos de espera y horizonte dividido para prevenir la propagación de información de enrutamiento errónea.

1.6.4.2 Configuración del protocolo RIP

El comando `router rip` habilita el protocolo de enrutamiento RIP. Luego se ejecuta el comando `network` para informar al router acerca de las interfaces donde RIP estará activo. A continuación, el proceso de enrutamiento asocia las interfaces específicas con las direcciones de red y comienza a enviar y a recibir actualizaciones RIP en estas interfaces.

RIP envía mensajes de actualización de enrutamiento a intervalos regulares. Cuando un router recibe una actualización de enrutamiento que incluya cambios a una entrada de su tabla de enrutamiento, actualiza la dicha tabla para reflejar la nueva ruta. El valor recibido de la métrica de la ruta aumenta en 1 y la interfaz de origen de la actualización se señala como el salto siguiente en la tabla de enrutamiento. Los routers RIP conservan sólo la mejor ruta hacia un destino pero pueden conservar más de una ruta al mismo destino si el costo de todas es igual.

La mayoría de los protocolos de enrutamiento usan una combinación de actualizaciones causadas por eventos (event-driven) o por tiempo (time-driven). RIP es time-driven, pero la implementación Cisco de RIP envía actualizaciones tan pronto se detectan cambios. Cambios en la topología también originan actualizaciones inmediatas en routers IGRP, independientes del valor del temporizador de actualización. Sin actualizaciones event-driven RIP e IGRP no funcionarían adecuadamente. Una vez que se haya actualizado la tabla de enrutamiento por cambios en la configuración, el router comienza inmediatamente a transmitir las actualizaciones de enrutamiento, a fin de informar de estos cambios a los otros routers. Estas actualizaciones, denominadas actualizaciones generadas por eventos, se envían independientemente de las actualizaciones periódicas que envían los routers RIP a intervalos regulares.

1.6.5 Protocolo IGRP

1.6.5.1 Características del protocolo IGRP

IGRP es un protocolo de enrutamiento de vector-distancia desarrollado por Cisco. IGRP envía actualizaciones de enrutamiento a intervalos de 90 segundos, las cuales publican las redes de un sistema autónomo en particular. Las características claves de IGRP son las siguientes:

- La versatilidad para manejar automáticamente topologías indefinidas y complejas.
- La flexibilidad necesaria para segmentarse con distintas características de ancho de banda y de

retardo.

- La escalabilidad para operar en redes de gran tamaño

Por defecto, el protocolo IGRP de enrutamiento usa el ancho de banda y el retardo como métrica.

Además, IGRP puede configurarse para utilizar una combinación de variables para calcular una métrica compuesta. Estas variables incluyen:

- Ancho de banda
- Retardo
- Carga
- Confiabilidad

1.6.5.2 Métricas de IGRP

La métrica de IGRP es compuesta y más precisa que la métrica del número de saltos que usa RIP para elegir una ruta hacia un destino. La ruta de menor valor métrico es la mejor.

Las métricas que utiliza el protocolo IGRP son:

- Ancho de banda: el menor valor de ancho de banda en la ruta.
- Retardo: el retardo acumulado de la interfaz a lo largo de la ruta.
- Confiabilidad: la confiabilidad del enlace hacia el destino, según sea determinada por el intercambio de mensajes de actividad (keepalives).
- Carga: la carga sobre un enlace hacia el destino, medida en bits por segundos.

Esta métrica se calcula como función del ancho de banda, el retardo, la carga y la confiabilidad. Por defecto, sólo se considera el ancho de banda y el retardo. Los parámetros restantes sólo se consideran si se habilitan a través de la configuración. El retardo y el ancho de banda no son valores medidos, sino que se fijan a través de los comandos de interfaces relativos al ancho de banda y al retardo. Un enlace de mayor ancho de banda tendrá una métrica de menor valor y una ruta con menor retardo acumulado tendrá una métrica de menor valor.

1.6.5.3 Rutas IGRP

IGRP publica tres tipos de rutas:

- Interiores
- Del sistema
- Exteriores

Interiores

Las rutas interiores son rutas entre subredes de la red conectada a una interfaz de un router. Si la red que está conectada a un router no está dividida en subredes, IGRP no publica rutas interiores.

Sistema
Las rutas del sistema son rutas hacia redes ubicadas dentro de un sistema autónomo. El IOS de Cisco deriva rutas de sistema de las interfaces de red conectadas directamente y de la información de rutas de sistema suministrada por otros routers que ejecutan IGRP o por servidores de acceso. Las rutas de sistema no incluyen información acerca de las subredes.

Exteriores
Las rutas exteriores son rutas hacia redes fuera del sistema autónomo, las cuales se tienen en cuenta al identificar un gateway de último recurso. El IOS de Cisco elige un gateway de último recurso de la lista de rutas exteriores que suministra IGRP. El software usa el gateway (router) de último recurso si no se encuentra una ruta mejor y si el destino no es una red conectada. Si el sistema autónomo tiene más de una conexión hacia una red externa, cada router puede seleccionar un router exterior diferente como gateway de último recurso.

1.6.5.4 Características de estabilidad del protocolo IGRP

IGRP ofrece una serie de funciones diseñadas para mejorar su estabilidad, por ejemplo:

- Lapsos de espera.
- Horizontes divididos.
- Actualizaciones inversas envenenadas.

Lapsos de espera.
Los lapsos de espera se utilizan para evitar que los mensajes periódicos de actualización puedan reinstalar erróneamente una ruta que podría estar fuera de servicio. Cuando un router sale de servicio, los routers vecinos detectan ese evento por la falta de mensajes de actualización periódicos.

Horizontes divididos.
Los horizontes divididos se originan en la premisa que dice que no es útil enviar información acerca de una ruta de vuelta a la dirección desde donde se originó. La técnica del horizonte dividido ayuda a prevenir los bucles de enrutamiento entre router adyacentes.

Actualizaciones inversas envenenadas.
Las actualizaciones inversas envenenadas son necesarias para romper los bucles de enrutamiento de mayor envergadura. En general, los aumentos en las métricas de enrutamiento señalan la presencia de bucles. Entonces, se envían actualizaciones inversas envenenadas para eliminar la ruta y colocarla en espera. En IGRP, las actualizaciones inversas envenenadas se envían sólo si la métrica de la ruta ha aumentado en un factor de 1,1 o más.

IGRP también mantiene un cierto número de temporizadores y de variables que contienen los intervalos de tiempo. Estos incluyen un temporizador de actualizaciones, un temporizador de caída del

servicio, un temporizador de espera y un temporizador de purga.

El temporizador de actualizaciones especifica a qué frecuencia se deben enviar los mensajes de actualización de enrutamiento. Por defecto, en IGRP el valor de esta variable es de 90 segundos.

El temporizador de caída del servicio especifica cuánto tiempo debe esperar un router ante la ausencia de mensajes de actualización de enrutamiento en relación a una ruta específica antes de declarar que está fuera de servicio. Por defecto, en IGRP esta variable es tres veces el lapso de las actualizaciones.

El temporizador de espera especifica la cantidad de tiempo durante el cual no se toma en cuenta la información sobre rutas menos convenientes. Por defecto, en IGRP esta variable es tres veces el lapso de las actualizaciones, más 10 segundos.

Por último, el temporizador de purga indica cuánto tiempo debe transcurrir antes de que se purgue una ruta de la tabla de enrutamiento. Por defecto, es siete veces el lapso de las actualizaciones del temporizador de enrutamiento.

En la actualidad se hace evidente la antigüedad de IGRP, ya que carece de capacidades para manejar máscaras de subred de longitud variable (VLSM). Antes que desarrollar un IGRP versión 2 para corregir este problema, Cisco se ha apoyado en el legado de éxito de IGRP para desarrollar el Enhanced IGRP (IGRP mejorado).

1.6.5.5 Configuración del protocolo IGRP

Para configurar un proceso de enrutamiento IGRP, se usa el comando de configuración `router igrp`.

```
RouterA(config)#router igrp as-number
```

El número de Sistema Autónomo (AS) identifica el proceso IGRP. También se utiliza para marcar la información de enrutamiento.
Para especificar una lista de redes para los procesos de enrutamiento IGRP, se usa el comando `network` de configuración del router.

1.6.6 Protocolo de enrutamiento de estado del enlace

El segundo algoritmo básico que se utiliza para enrutamiento es el algoritmo de estado del enlace. Los algoritmos de estado del enlace también se conocen como algoritmos Dijkstra o SPF ("primero la ruta más corta"). Los protocolos de enrutamiento de estado del enlace mantienen una base de datos compleja, con la información de la topología de la red.

El enrutamiento de estado del enlace utiliza:

- Publicaciones de estado del enlace (LSA): una publicación del estado del enlace (LSA) es un paquete pequeño de información sobre el enrutamiento, el cual es enviado de router a router.
- Base de datos topológica: una base de datos topológica es un cúmulo de información que se ha reunido mediante las LSA.
- Algoritmo SPF: el algoritmo "primero la ruta más corta" (SPF) realiza cálculos en la base de datos, y el resultado es el árbol SPF.
- Tablas de enrutamiento: una lista de las rutas e interfaces conocidas.

Proceso de descubrimiento de la red para el enrutamiento de estado del enlace: el intercambio de LSAs se inicia en las redes conectadas directamente al router, de las cuales tiene información directa. Cada router, en paralelo con los demás, genera una base de datos topológica que contiene toda la información recibida por intercambio de LSAs.

El algoritmo SPF determina la conectividad de la red. El router construye esta topología lógica en forma de árbol, con él mismo como raíz, y cuyas ramas son todas las rutas posibles hacia cada subred de la red. Luego ordena dichas rutas, y coloca las ruta más cortas primero (SPF). El router elabora una lista de las mejores rutas a las redes de destino, y de las interfaces que permiten llegar a ellas. Esta información se incluye en la tabla de enrutamiento. También mantiene otras bases de datos, de los elementos de la topología y de los detalles del estado de la red.

El router que primero conoce de un cambio en la topología envía la información al resto de los routers, para que puedan usarla para hacer sus actualizaciones y publicaciones.

Esto implica el envío de información de enrutamiento, la cual es común a todos los routers de la red. Para lograr la convergencia, cada router monitorea sus routers vecinos, sus nombres, el estado de la interconexión y el costo del enlace con cada uno de ellos. El router genera una LSA, la cual incluye toda esa información, junto con información relativa a nuevos vecinos, los cambios en el costo de los enlaces y los enlaces que ya no son válidos. La LSA es enviada entonces, a fin de que los demás routers la reciban.

Cuando un router recibe una LSA, actualiza su base de datos con la información más reciente y elabora un mapa de la red con base en los datos acumulados, y calcula la ruta más corta hacia otras redes mediante el algoritmo SPF. Cada vez que una LSA genera cambios en la base de datos, el algoritmo de estado del enlace (SPF) vuelve a calcular las mejores rutas, y actualiza la tabla de enrutamiento.

Los routers que usan protocolos de estado del enlace requieren de más memoria y exigen mas esfuerzo al procesador, que los que usan protocolos de enrutamiento por vector-distancia. Los routers deben tener la memoria suficiente para almacenar toda la información de las diversas bases de datos, el árbol de topología y la tabla de enrutamiento.

La avalancha de LSAs que ocurre al activar un router consume una porción del ancho de banda. Durante el proceso de descubrimiento inicial, todos los routers que utilizan protocolos de enrutamiento de estado del enlace envían LSAs a todos los demás routers. Esta acción genera un gran volumen de tráfico y reduce temporalmente el ancho de banda disponible para el tráfico enrutado de los usuarios.

Después de esta disminución inicial de la eficiencia de la red, los protocolos de enrutamiento del estado del enlace generalmente consumen un ancho de banda mínimo, sólo para enviar las ocasionales LSAs que informan de algún cambio en la topología.

1.6.7 Característica del Protocolo OSPF

OSPF es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. Se describe en diversos estándares de la Fuerza de Tareas de Ingeniería de Internet (IETF). El término "libre" en "Primero la ruta libre más corta" significa que está abierto al público y no es propiedad de ninguna empresa.

En comparación con RIP v1 y v2, OSPF es el IGP preferido porque es escalable. RIP se limita a 15 saltos, converge lentamente y a veces elige rutas lentas porque pasa por alto ciertos factores críticos como por ejemplo el ancho de banda a la hora de determinar la ruta. Una desventaja de usar OSPF es que solo soporta el conjunto de protocolos TCP/IP.

OSPF se ha convertido en un protocolo de enrutamiento sólido y escalable adecuado para las redes modernas. OSPF se puede usar y configurar en una sola área en las redes pequeñas y en redes grandes utilizando un diseño jerárquico.

Este protocolo utiliza el algoritmo de la mejor ruta es la de menor costo. El algoritmo fue desarrollado por Dijkstra, un especialista holandés en informática en 1959. El algoritmo considera la red como un conjunto de nodos conectados con enlaces punto a punto. Cada enlace tiene un costo. Cada nodo tiene un nombre. Cada nodo cuenta con una base de datos completa de todos los enlaces y por lo tanto se conoce la información sobre la topología física en su totalidad. Todas las bases de datos del estado de enlace, dentro de un área determinada, son idénticas.

El algoritmo de la ruta más corta calcula una topología sin bucles con el nodo como punto de partida y examinando a su vez la información que posee sobre nodos adyacentes.

1.6.7.1 Método de OSPF

Los routers de estado de enlace identifican a los routers vecinos y luego se comunican con los vecinos identificados. El protocolo OSPF tiene su propia terminología.

OSPF reúne la información de los routers vecinos acerca del estado de enlace de cada router OSPF.

Con esta información se inunda a todos los vecinos. Un router OSPF publica sus propios estados de enlace y traslada los estados de enlace recibidos. Los routers procesan la información acerca de los estados de enlace y crean una base de datos del estado de enlace.

Cada router del área OSPF tendrá la misma base de datos del estado de enlace. Por lo tanto, cada router tiene la misma información sobre el estado del enlace y los vecinos de cada uno de los demás routers.

Cada router luego aplica el algoritmo SPF a su propia copia de la base de datos. Este cálculo determina la mejor ruta hacia un destino. El algoritmo SPF va sumando el costo, un valor que corresponde generalmente al ancho de banda. La ruta de menor costo se agrega a la tabla de enrutamiento, que se conoce también como la base de datos de envío.

Cada router mantiene una lista de vecinos adyacentes, que se conoce como base de datos de adyacencia. La base de datos de adyacencia es una lista de todos los routers vecinos con los que un router ha establecido comunicación bidireccional. Esto es exclusivo de cada router.

Para reducir la cantidad de intercambios de la información de enrutamiento entre los distintos vecinos de una misma red, los routers de OSPF seleccionan un router designado (DR) y un router designado de respaldo (BDR) que sirven como puntos de enfoque para el intercambio de información de enrutamiento.

El router DR se hace adyacente a todos los demás routers del segmento de broadcast. Todos los demás routers del segmento envían su información del estado de enlace al DR. El DR a su vez actúa como portavoz del segmento. El DR envía información del estado de enlace a todos los demás routers del segmento a través de la dirección de multicast 224.0.0.5 para todos los routers OSPF.

A pesar de la ganancia en eficiencia que permite la elección de DR, existe una desventaja. El DR representa un punto único de falla. Se elige un segundo router como router designado de respaldo (BDR) para que se haga cargo de las responsabilidades del DR en caso de que éste fallara.

1.6.7.2 Protocolo Hello de OSPF

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete hello y sigue enviando hellos a intervalos regulares. Las reglas que gobiernan el intercambio de paquetes hello de OSPF se denominan protocolo Hello.
En la capa 3 del modelo OSI, los paquetes hello se direccionan hacia la dirección multicast 224.0.0.5. Esta dirección equivale a "todos los routers OSPF". Los routers OSPF utilizan los paquetes hello para iniciar nuevas adyacencias y asegurarse de que los routers vecinos sigan funcionando. Los Hellos se envían cada 10 segundos por defecto en las redes multiacceso de broadcast y punto a punto. En las interfaces que se conectan a las redes NBMA, como por ejemplo Frame Relay, el tiempo por defecto es de 30 segundos.
En las redes multiacceso el protocolo Hello elige un router designado (DR) y un router designado de respaldo (BDR).
Aunque el paquete hello es pequeño, consiste en un encabezado de paquete OSPF.

El paquete hello transmite información para la cual todos los vecinos deben estar de acuerdo antes de que se forme una adyacencia y que se pueda intercambiar información del estado de enlace.

1.6.7.3 Pasos en la operación de OSPF

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete Hello y sigue enviando Hellos a intervalos regulares. El conjunto de reglas que rigen el intercambio de paquetes Hello de OSPF se denomina protocolo Hello.

En las redes multiacceso el protocolo Hello elige un router designado (DR) y un router designado de respaldo (BDR). Hello transmite información que todos los vecinos deberán aceptar para que se pueda formar una adyacencia y para que se pueda intercambiar información del estado de enlace. En las redes multiaceso, el DR y el BDR mantienen adyacencias con todos los demás routers OSPF en la red.

Los routers adyacentes pasan por una secuencia de estados. Los routers adyacentes deben estar en su estado completo antes de crear tablas de enrutamiento y enrutar el tráfico. Cada router envía publicaciones del estado de enlace (LSA) en paquetes de actualización del estado de enlace (LSU). Estas LSA describen todos los enlaces de los routers. Cada router que recibe una LSA de su vecino registra la LSA en la base de datos del estado de enlace. Este proceso se repite para todos los routers de la red OSPF.

Una vez completas las bases de datos, cada router utiliza el algoritmo SPF para calcular una topología lógica sin bucles hacia cada red conocida. Se utiliza la ruta más corta con el menor costo para crear esta topología, por lo tanto, se selecciona la mejor ruta.

La información de enrutamiento ahora se mantiene. Cuando existe un cambio en el estado de un enlace, los routers utilizan un proceso de inundación para notificar a los demás routers en la red acerca del cambio. El intervalo muerto del protocolo Hello ofrece un mecanismo sencillo para determinar que un vecino adyacente está desactivado.

1.6.7.4 Configuración del proceso de enrutamiento OSPF

El enrutamiento OSPF utiliza el concepto de áreas. Cada router contiene una base de datos completa de los estados de enlace de un área específica. A un área de la red OSPF se le puede asignar cualquier número de 0 a 65.535. Sin embargo a una sola área se le asigna el número 0 y se la conoce como área 0. En las redes OSPF con varias áreas, se requiere que todas las áreas se conecten al área 0. El área 0 también se denomina el área backbone.
La configuración de OSPF requiere que el proceso de enrutamiento OSPF esté activo en el router con las direcciones de red y la información de área especificadas.

Las direcciones de red se configuran con una máscara wildcard y no con una máscara de subred. La máscara wildcard representa las direcciones de enlaces o de host que pueden estar presentes en este segmento.

Para habilitar el enrutamiento OSPF, se utiliza la sintaxis:

```
Router(config)#router ospf process-id
```

El ID de proceso es un número que se utiliza para identificar un proceso de enrutamiento OSPF en el

router. Se pueden iniciar varios procesos OSPF en el mismo router. El número puede tener cualquier valor entre 1 y 65.535. La mayoría de los administradores de red mantienen el mismo ID de proceso en todo un sistema autónomo, pero esto no es un requisito. Rara vez es necesario ejecutar más de un proceso OSPF en un router. Las redes IP se publican de la siguiente manera en OSPF:

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

Cada red se debe identificar con un área a la cual pertenece. La dirección de red puede ser una red completa, una subred o la dirección de la interfaz. La máscara wildcard representa el conjunto de direcciones de host que admite el segmento. Esto es distinto de lo que ocurre con una máscara de subred que se utiliza al configurar las direcciones IP en las interfaces.

En las redes multiacceso de broadcast es posible que haya más de dos routers. OSPF elige un router designado (DR) para que sea el punto de enfoque de todas las actualizaciones del estado de enlace y de las publicaciones del estado de enlace. Debido a que la función del DR es crítica, se elige un router designado de respaldo (BDR) para que reemplace a DR en caso de que éste falle.

Si el tipo de red de una interfaz es broadcast, la prioridad OSPF por defecto es 1. Cuando las prioridades OSPF son iguales, la elección de OSPF para DR se decide a base del ID del router. Se selecciona el router de ID más elevado.

El resultado de la elección puede determinarse asegurándose de que las votaciones, los paquetes hello, contengan una prioridad para dicha interfaz de router. La interfaz que registra la mayor prioridad para un router permitirá asegurar de que se convertirá en DR.

Las prioridades se pueden establecer en cualquier valor de 0 a 255. Un valor de 0 evita que el router sea elegido. Se seleccionará como DR al router con la prioridad OSPF más alta. El router con la segunda prioridad más alta será BDR.

Después del proceso de elección, el DR y el BDR conservan sus funciones aun cuando se agreguen a la red routers con valores de prioridad OSPF más altos.

1.6.7.5 Modificación de la métrica de costos de OSPF

OSPF utiliza el costo como métrica para determinar la mejor ruta. Un costo se asocia con el lado de salida de cada interfaz de router. Los costos también se asocian con datos de enrutamiento derivados en forma externa. Por lo general, el costo de ruta se calcula mediante la fórmula 10^8/ancho de banda, donde el ancho de banda se expresa en bps. El administrador de sistema también puede usar otros métodos para configurar el costo. Cuanto más bajo sea el costo, más probabilidad hay de que la interfaz sea utilizada para enviar tráfico de datos.

Es posible cambiar el costo para afectar el resultado de los cálculos de costo OSPF. Una situación común que requiere un cambio de costo es un entorno de enrutamiento de diversos fabricantes. Un cambio de costo puede asegurar que el valor de costo de un fabricante coincida con el valor de costo de otro fabricante. Otra situación se produce al utilizar Gigabit Ethernet. Con la configuración por defecto,

se asigna el valor de costo más bajo (1) a un enlace de 100 Mbps. En una situación con con enlaces Gigabit Ethernet y 100-Mbps, los valores de costo por defecto podrían hacer que el enrutamiento tome una ruta menos deseable a menos que estos se ajusten. El número de costo se puede establecer entre 1 y 65.535.

1.6.7.6 Configuración de la autenticación de OSPF

Cada interfaz OSPF puede presentar una clave de autenticación para que la usen los routers que envían información de OSPF hacia otros routers del segmento. La clave de autenticación, conocida como contraseña, es un secreto compartido entre los routers. Esta clave se utiliza para generar los datos de autenticación en el encabezado del paquete de OSPF.

Con la autenticación sencilla, se envía la contraseña como texto sin cifrar. Esto significa que se puede decodificar fácilmente si un husmeador de paquetes captura un paquete de OSPF. Para enviar la información de autenticación cifrada y asegurar mayor seguridad, OSPF utiliza la autenticación MD5.

1.6.8 Característica del Protocolo EIGRP

Cisco lanzó EIGRP en 1994 como una versión escalable y mejorada de su protocolo propietario de enrutamiento por vector-distancia, IGRP.

EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP. Esto permite que una red tenga una arquitectura mejorada y pueda mantener las inversiones actuales en IGRP.

Además, EIGRP puede reemplazar al Protocolo de Mantenimiento de Tablas de Enrutamiento (RTMP) AppleTalk y Novell RIP. EIGRP funciona en las redes IPX y AppleTalk con potente eficiencia.

Con frecuencia, se describe EIGRP como un protocolo de enrutamiento híbrido que ofrece lo mejor de los algoritmos de vector-distancia y del estado de enlace. EIGRP es una opción ideal para las grandes redes multiprotocolo construidas principalmente con routers Cisco.

EIGRP es un protocolo de enrutamiento avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Sin embargo, EIGRP es más fácil de configurar que OSPF.

1.6.8.1 Conceptos y terminología de EIGRP

Los routers EIGRP mantienen información de ruta y topología a disposición en la RAM, para que puedan reaccionar rápidamente ante los cambios. Al igual que OSPF, EIGRP guarda esta información en varias tablas y bases de datos.

EIGRP guarda las rutas que se aprenden de maneras específicas. Las rutas reciben un estado específico y se pueden rotular para proporcionar información adicional de utilidad.

EIGRP mantiene las siguientes tres tablas:

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

La tabla de vecinos es la más importante de EIGRP. Cada router EIGRP mantiene una tabla de vecinos que enumera a los routers adyacentes. Esta tabla puede compararse con la base de datos de adyacencia utilizada por OSPF. Existe una tabla de vecinos por cada protocolo que admite EIGRP.

Al conocer nuevos vecinos, se registran la dirección y la interfaz del vecino. Esta información se guarda en la estructura de datos del vecino. Cuando un vecino envía un paquete hello, publica un tiempo de espera. El tiempo de espera es la cantidad de tiempo durante el cual un router considera que un vecino se puede alcanzar y que funciona. Si un paquete de salutación (hello) no se recibe dentro del tiempo de espera, entonces vence el tiempo de espera. Cuando vence el tiempo de espera, se informa al Algoritmo de Actualización Difusa (DUAL), que es el algoritmo de vector-distancia de EIGRP, acerca del cambio en la topología para que recalcule la nueva topología.

La tabla de topología se compone de todas las tablas de enrutamiento EIGRP en el sistema autónomo. DUAL toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo hacia cada destino.

EIGRP rastrea esta información para que los routers EIGRP puedan identificar y conmutar a rutas alternativas rápidamente. La información que el router recibe de DUAL se utiliza para determinar la ruta del sucesor, que es el término utilizado para identificar la ruta principal o la mejor. Esta información también se introduce a la tabla de topología. Los routers EIGRP mantienen una tabla de topología por cada protocolo configurado de red. La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

La tabla de enrutamiento EIGRP contiene las mejores rutas hacia un destino. Esta información se recupera de la tabla de topología. Los routers EIGRP mantienen una tabla de enrutamiento por cada protocolo de red.

Un sucesor es una ruta seleccionada como ruta principal para alcanzar un destino.
DUAL identifica esta ruta en base a la información que contienen las tablas de vecinos y de topología y la coloca en la tabla de enrutamiento. Puede haber hasta cuatro rutas de sucesor para cada destino en particular. Éstas pueden ser de costo igual o desigual y se identifican como las mejores rutas sin bucles hacia un destino determinado.

Un sucesor factible (FS) es una ruta de respaldo.
Estas rutas se identifican al mismo tiempo que los sucesores, pero sólo se mantienen en la tabla de topología. Los múltiples sucesores factibles para un destino se pueden mantener en la tabla de topología, aunque no es obligatorio.

Los routers EIGRP no envían las tablas en su totalidad, sino que envían actualizaciones parciales e incrementales. Esto es parecido a la operación de OSPF, salvo que los routers EIGRP envían estas actualizaciones parciales sólo a los routers que necesitan la información, no a todos los routers del área. Por este motivo, se denominan actualizaciones limitadas. En vez de enviar actualizaciones de enrutamiento temporizadas, los routers EIGRP usan pequeños paquetes hello para mantener la comunicación entre sí. Aunque se intercambian con regularidad, los paquetes hello no usan una cantidad significativa de ancho de banda.

1.6.8.2 Configuración de EIGRP

A pesar de la complejidad de DUAL, la configuración de EIGRP puede ser relativamente sencilla. Los comandos de configuración de EIGRP varían según el protocolo que debe enrutarse. Algunos ejemplos de estos protocolos son IP, IPX y AppleTalk.

El comando `router eigrp` habilita el protocolo de enrutamiento EIGRP, se debe definir el sistema autónomo. El número de sistema autónomo se usa para identificar todos los routers que pertenecen a la internetwork. Este valor debe coincidir para todos los routers dentro de la internetwork.

```
router(config)#router eigrp autonomous-system-number
```

Se debe indicar cuáles son las redes que pertenecen al sistema autónomo EIGRP en el router local mediante el comando `network.`

```
router(config-router)#network network-number
```

Al configurar los enlaces seriales mediante EIGRP, es importante configurar el valor del ancho de banda en la interfaz. Si el ancho de banda de estas interfaces no se modifica, EIGRP supone el ancho de banda por defecto en el enlace en lugar del verdadero ancho de banda. Si el enlace es más lento, es posible que el router no pueda convergir, que se pierdan las actualizaciones de enrutamiento o se produzca una selección de rutas por debajo de la óptima. Para establecer el ancho de banda para la interfaz.

```
router(config-if)#bandwidth kbps
```