Introducción a IGRP

Contenido

Introducción

Este documento presenta el IGRP (Interior Gateway Routing Protocol). Tiene dos propósitos. Uno es presentar una introducción a la tecnología IGRP, para los que estén interesados en usarla, evaluarla y posiblemente implementarla. El otro es ofrecer una exposición más amplia de algunas ideas y conceptos interesantes que se incluyen en IGRP. Consulte Configuración de IGRP, Implementación del IGRP de Cisco y Comandos IGRP para obtener información sobre cómo configurar IGRP.

Objetivos del IGRP

El protocolo IGRP permite que varios gatewayes coordinen su encaminamiento. Las metas son las siguientes:

- Ruteo estable aún en redes muy grandes o complejas. Ningunos loopes de la encaminamiento deben ocurrir, incluso durante los transeúntes.
- Respuesta rápida a los cambios en la topología de la red

- Tara baja. Es decir, IGRP en sí no debe usar más banda ancha de la que necesita realmente para realizar su tarea.
- La división de tráfico entre varias rutas paralelas cuando son de conveniencia apenas similar.
- Tener en cuenta las tasas de errores y el nivel de tráfico en distintos trayectos.

La implementación actual de IGRP maneja el ruteo para TCP/IP. Sin embargo, el diseño básico se piensa para poder manejar una variedad de protocolos.

Nadie herramienta va a solucionar todos los problemas de ruteo. Convencionalmente el problema de ruteo se desglosa en varias partes. Los protocolos tales como IGRP se llaman los “protocolos internal gateway” (los IGP). Su propósito es utilizarse dentro de un único grupo de redes, tanto bajo una sola administración como en administraciones muy coordinadas. Estos conjuntos de redes se encuentran conectados mediante "protocolos de gateway externa" (EGP). Un IGP está diseñado para hacer un seguimiento detallado de la topología de una red. La prioridad en el diseño de un IGP se pone en producir las rutas óptimo y la respuesta rápidamente a los cambios. Se espera que un EGP proteja a un sistema de redes contra errores o contra una distorsión intencional por parte de otros sistemas, el BGP es uno de estos protocolos de gateway exterior. La prioridad en la designación de un EGP está en la estabilidad y en los controles administrativos. A menudo es suficiente para que un EGP produzca una ruta razonable, en lugar de una ruta óptima.

IGRP tiene algunos aspectos similares a otros protocolos más antiguos como el Protocolo de información de ruteo de Xerox, el RIP de Berkeley y el Hello de Dave Mills. Difiere de estos protocolos principalmente en que están diseñados para redes más extensas y más complejas. Consulte la sección Comparación con RIP, para obtener una comparación más detallada con RIP, que es el protocolo más utilizado de la generación más antigua de protocolos.

Como estos protocolos anteriores, IGRP es un protocolo del vector distancia. En tal protocolo, los gatewayes intercambian la información de ruteo solamente por los gatewayes adyacentes. Esta información de ruteo contiene un resumen de información sobre el resto de la red. Puede ser mostrado matemáticamente que todos los gatewayes tomados juntos están solucionando un problema de optimización por qué cantidades a un algoritmo distribuido. Cada gateway sólo debe resolver parte del problema y sólo debe recibir una porción del total de los datos.

La alternativa principal para IGRP es IGRP mejorada (EIGRP) y una clase de algoritmos referidos como SPF (trayecto más corto primero). El OSPF utiliza este concepto. Para aprender más sobre el OSPF refiera a la guía de diseño OSPF. El OSPF que son éstos se basa en una técnica de la inundación, donde cada gateway se mantiene actualizado sobre el estatus de cada interfaz en cada otro gateway. Cada gateway soluciona independientemente el problema de optimización desde su punto de vista mediante los datos para toda la red. Cada método tiene sus ventajas. En algunas circunstancias, el SPF podrá responder a los cambios con mayor rapidez. Para evitar los loops de ruteo, IGRP debe ignorar la información nueva por algunos minutos después de que se producen ciertos tipos de cambios. Debido a que SPF recibe información directamente de cada gateway, puede evitar estos loops de ruteo. Por lo tanto puede actuar sobre información nueva en forma inmediata. Sin embargo, el SPF debe procesar considerablemente más datos que el IGRP, tanto en estructuras internas de datos como en mensajes entre gateways.

El problema del ruteo

IGRP está destinado para usarse en gateways que conectan varias redes. Asumimos que las redes utilizan la tecnología del paquete basado. En efecto, los gateways actúan como switches de paquete. Cuando un sistema conectado a una red desea enviar un paquete a un sistema de una

red diferente, dirige el paquete a una gateway. Si el destino está en una de las redes conectadas a la gateway, ésta enviará el paquete al destino. Si el destino es más distante, el gateway remitirá el paquete a otro gateway que esté más cercano al destino. Tablas de ruteo del uso de los gatewayes para ayudarles a decidir qué hacer con los paquetes. Aquí está una tabla de ruteo del ejemplo simple. (Los direccionamientos usados en los ejemplos son IP Addresses tomados de la Universidad Rutgers. Tenga en cuenta que el problema básico de ruteo es similar para otros protocolos también, pero esta descripción supondrá que IGRP se usa para el ruteo de IP.)

Figura 1

```
network      gateway     interface
  -------      -------     ---------
  128.6.4      none        ethernet 0
  128.6.5      none        ethernet 1
  128.6.21     128.6.4.1   ethernet 0
  128.121      128.6.5.4   ethernet 1
  10           128.6.5.4   ethernet 1
```

(Las tablas de ruteo de IGRP reales tienen información adicional para cada gateway, pues veremos.) Este gateway está conectado con dos Ethernets, llamados 0 y 1. Se han dado a network number IP (realmente números de la subred) 128.6.4 y 128.6.5. Así los paquetes dirigidos para estas redes específicas se pueden enviar directamente al destino, simplemente usando la interfaz de Ethernet apropiada. Hay dos gateways cercanas, 128.6.4.1 y 128.6.5.4. Los paquetes para redes con excepción de 128.6.4 y de 128.6.5 serán remitidos a uno o al otro de esos gateways. La tabla de ruteo indica qué gateway debe ser utilizado para el cual red. Por ejemplo, los paquetes direccionados a un host en la red 10 deberían ser reenviados a la gateway 128.6.5.4. Uno espera que este gateway esté más cercano a la red 10, es decir que el mejor trayecto a la red 10 pasa a través de este gateway. El objetivo principal de IGRP es permitir que los gateways generen y mantengan tablas de ruteo como esta.

Resumen de IGRP

Como se mencionó anteriormente, el IGRP es un protocolo que permite que los gatewayes acumulen su tabla de ruteo intercambiando la información por otros gatewayes. Una gateway comienza con entradas para todas las redes directamente conectadas con ella. Obtiene información sobre otras redes mediante el intercambio de actualizaciones de ruteo con gateways adyacentes. En el caso más simple, el gateway encontrará una trayectoria que represente la mejor manera de conseguir a cada red. Un trayecto se caracteriza por el siguiente gateway al que se deben enviar los paquetes, la interfaz de red que debe usarse y la información métrica. La información de medidas es un conjunto de números que caracteriza cómo es bueno es la trayectoria. Esto le permite a la gateway comparar los trayectos que escuchó de varias gateways y decidir cuál utilizar. Hay a menudo los casos donde tiene sentido de partir el tráfico entre dos o más trayectorias. IGRP hará esto siempre que dos o más trayectos sean igualmente buenos. El usuario puede también configurarlo para partir el tráfico cuando las trayectorias son casi igualmente buenas. En este caso se enviará más tráfico a lo largo del trayecto con la mejor métrica. El motivo es que el tráfico puede dividirse entre una línea de 9600 BPS y una de 19200 BPS, y la línea de 19200 recibir aproximadamente el doble de tráfico que la línea de 9600 BPS.

Las métricas usadas por el IGRP incluyen el siguiente:

- Tiempo de retardo tipológico
- Ancho de banda del segmento de ancho de banda más angosto del trayecto
- Ocupación del canal de la trayectoria
- Confiabilidad del trayecto

El tiempo de retraso topológico es la cantidad de tiempo que tomaría para conseguir al destino a lo largo de esa trayectoria, si se asume que una red descargada. Por supuesto, existe un retardo adicional cuando la red está cargada. Sin embargo, la carga es explicada usando la figura de la ocupación del canal, no intentando medir los retardos reales. El ancho de banda del trayecto es simplemente el ancho de banda en bits por segundo del link más lento de la trayectoria. La ocupación del canal indica cuánto de ese ancho de banda es actualmente funcionando. Se mide, y cambiará con la carga. La confiabilidad indica el índice de errores actual. Es la fracción de los paquetes que llegan el destino indemne. Se mide.

Aunque no se utilicen como parte del métrico, dos informaciones de la adición se pasan con él: conteo de saltos y MTU. El conteo de saltos es simplemente la cantidad de gateways que un paquete tendrá que atravesar para llegar a destino. MTU es el tamaño máximo de paquete que se puede enviar en todo el trayecto sin fragmentación. (Es decir, es la cantidad mínima de las MTU de todas las redes involucradas en el trayecto).

Sobre la base de la información de la métrica, se calcula una sola "métrica compuesta" para el trayecto. La medición compuesta combina el efecto de los diversos componentes métricos en un solo número que representa la “calidad” de esa trayectoria. Es la medición compuesta que se utiliza realmente para decidir sobre el mejor trayecto.

En forma periódica, cada gateway transmite toda su tabla de ruteo (con ciertas restricciones debido a la regla de horizonte dividido) hacia todas las gateways adyacentes. Cuando un gateway consigue esto transmitida de otro gateway, compara la tabla con su tabla existente. Cualesquiera nuevos destinos y trayectoria se agregan a la tabla de ruteo del gateway. Las trayectorias en el broadcast se comparan con los trayectos existentes. Si una nueva trayectoria es mejor, puede substituir el existencia. La información en la difusión también se utiliza para actualizar la ocupación de canales y otra información sobre trayectos existentes. Este procedimiento general es similar al utilizado por todos los protocolos del vector de distancia. Se refiere en la bibliografía sobre matemática como el algoritmo Bellman-Ford. Refiera al RFC 1058 para un desarrollo detallado del procedimiento básico, que describe el RIP, un más viejo protocolo del vector distancia.

En IGRP, el algoritmo Bellman-Ford general se modifica en tres aspectos importantes. Primero, en vez de un métrico simple, un vector de métrica se utiliza para caracterizar las trayectorias. En segundo lugar, en vez de elegir un solo trayecto con la medición más pequeña, el tráfico se divide en varios trayectos, cuyas mediciones se ajustan a un rango específico. Tercero, varias características se introducen para proporcionar la estabilidad en las situaciones donde la topología está cambiando.

Se selecciona el mejor trayecto sobre la base de una métrica compuesta:

```
[(K1 / Be) + (K2 * Dc)] r
```

Donde K1, K2 = constantes, Be = ancho de banda del trayecto descargado x (1 - ocupación del canal), Dc =(retardo topológico) y r = fiabilidad.

La ruta que contenga la menor métrica compuesta será la mejor ruta. Donde hay trayectos múltiples al mismo destino, el gateway puede rutear los paquetes sobre más de una trayectoria. Esto se realiza de acuerdo con la métrica compuesta para cada trayecto de datos. Por ejemplo, si un trayecto tiene una métrica compuesta de 1 y otro trayecto tiene una métrica compuesta de 3, será enviado tanto como el triple de paquetes por el trayecto de datos que tiene la métrica compuesta de 1.

Hay dos ventajas a usar una información de vector de métrica. La primera es que brinda la

capacidad de admitir diversos tipos de servicio desde el mismo conjunto de datos. La segunda ventaja es una precisión mejorada. Cuando se utiliza una sola métrica, se lo suele tratar como si fuera una demora. Cada link en la trayectoria se agrega al total métrico. Si hay un link con un ancho de banda baja, es representado normalmente por un retardo grande. Sin embargo, las limitaciones de ancho de banda no acumulan realmente la manera que lo hacen los retardos. Tratando el ancho de banda como componente separado, puede ser dirigida correctamente. De manera similar, la carga puede ser administrada por un número de ocupación de canal separado.

El IGRP proporciona un sistema para interconectar las redes informáticas que pueden manejar estable una topología general de gráfico incluyendo los loopes. El sistema mantiene la información de medidas de la ruta completa, es decir, conoce los parámetros path a las cualesquier otras redes con las cuales cualquier gateway está conectado. El tráfico puede distribuirse sobre los trayectos paralelos y pueden computarse simultáneamente los parámetros de trayecto múltiple por toda la red.

Comparación con RIP

Esta sección compara el IGRP con el RIP. Esta comparación es útil ya que RIP se usa con frecuencia con propósitos similares a IGRP. Sin embargo, si se hace esto no es totalmente justo. El RIP no fue pensado para resolver todas las mismas metas que el IGRP. El RIP fue pensado para el uso en las pequeñas redes con razonablemente la tecnología uniforme. En dichas aplicaciones es generalmente adecuado.

La mayoría de la diferencia básica entre el IGRP y el RIP es la estructura de su métrica. Lamentablemente, este cambio no se puede retroadaptar al RIP. Requiere los nuevos algoritmos y estructuras de datos presentes en el IGRP.

RIP usa una métrica simple de "recuento de saltos" para describir la red. A diferencia del IGRP, donde cada trayectoria es descrita por un retardo, un ancho de banda, un etc., en el RIP es descrito por un número a partir de la 1 a 15. Este número se utiliza normalmente para representar cuántos gatewayes va la trayectoria a través antes de conseguir al destino. Esto significa que no se distingue entre una línea serial lenta y una Ethernet. En algunas implementaciones del RIP, es posible que el administrador de sistema especifique que un salto dado debe ser contado más de una vez. Las redes lentas pueden estar representadas por un gran conteo de saltos. Pero puesto que el máximo es 15, esto no se puede hacer mucho. E.g si un Ethernet es representado por 1 y una línea 56Kb por 3, puede haber a lo más 5 líneas 56Kb en una trayectoria, o el máximo de 15 se excede. Para representar el alcance total de las velocidades de la red disponibles, y tener en cuenta una Red grande, los estudios hechos por Cisco sugieren que un 24-bit métrico es necesario. Si la métrica máxima es demasiado pequeña, el administrador del sistema tendrá que tomar una decisión poco agradable: no puede distinguir entre rutas rápidas y lentas, o bien no puede aceptar su red completa dentro del límite. De hecho varias redes nacionales son bastante grandes ahora que el RIP no puede manejarlas incluso si cada salto se cuenta solamente una vez. El RIP (Protocolo de información de ruteo) simplemente no puede usarse para tales redes.

La respuesta obvia sería que se modifique el RIP para permitir una métrica más amplia. Lamentablemente, esto no funcionará. Como todos los protocolos del vector distancia, el RIP tiene el problema de la “cuenta al infinito”. Esto se describe más detalladamente en el RFC 1058 . Cuando los cambios de la topología, las rutas espúreo serán introducidos. Las métricas asociadas a estas rutas espúreo aumentan lentamente hasta que alcancen 15, momento en el cual que se quitan las rutas. 15 es bastante pequeño máximos que convergerá este proceso bastante rápidamente, si se asume que las actualizaciones activadas están utilizadas. Si el RIP fuera modificado para permitir un 24-bit métrico, los loopes persistirían bastante tiempo para que el

métrico sea contado hasta 2**24. Esto no es tolerable. IGRP tiene funciones diseñadas para evitar la introducción de rutas falsas. Éstos se discuten abajo en la sección 5.2. No es práctica manejar las redes complejas sin la introducción de tales características o el cambio a un protocolo tal como SPF.

IGRP hace algo más que simplemente incrementar el rango de métricas admitidas. Reestructura la métrica para describir el retardo, el ancho de banda, la confiabilidad y la carga. Tales consideraciones pueden representarse en una sola métrica como RIP. Sin embargo, el enfoque aplicado por IGRP es potencialmente más exacto. Por ejemplo, con un solo métrico, varios links rápidos sucesivos aparecerán ser equivalentes a un solo reducen uno. Ésta puede ser la caja para el tráfico interactivo, donde está el problema principal el retardo. Sin embargo, para transferencia masiva de datos, la principal preocupación es el ancho de banda y, en este caso, agregar métricas en forma conjunta no es el enfoque correcto. IGRP maneja la demora y el ancho de banda por separado, acumulando las demoras y tomando el mínimo de los anchos de banda. No es fácil ver cómo incorporar los efectos de confiabilidad y carga en una métrica de un solo componente.

En mi opinión, una de las ventajas grandes del IGRP es facilidad de la configuración. Puede representar directamente las cantidades que tienen significado físico. Esto significa que puede ser configurada automáticamente, sobre la base del tipo de interfaz, velocidad de línea, etc. Con un métrico de un solo componente, el métrico es más probable tener que “ser cocinado” para incorporar los efectos de varias diversas cosas.

Otras innovaciones están más vinculadas con algoritmos y estructuras de datos que con el protocolo de ruteo. Por ejemplo, IGRP especifica algoritmos y estructuras de datos que soportan la división del tráfico entre varias rutas. Es ciertamente posible diseñar una implementación del RIP que haga esto. Sin embargo, una vez que el ruteo está siendo reimplementado, no hay motivo para quedarse con RIP.

He descrito hasta ahora el “IGRP genérico”, una tecnología que podría soportar la encaminamiento para cualquier Network Protocol. No obstante, en esta sección cabe mencionar un poco más acerca de la implementación específica de TCP/IP. Ésa es la implementación que se comparará con RIP.

Los mensajes de actualización de RIP simplemente contienen instantáneas de la tabla de ruteo. Es decir, tienen una cantidad de destinos y valores de métrica y un poco más. La instrumentación de IP del IGRP tiene estructura adicional. Primero, el mensaje de actualización es identificado por un “número del sistema autónomo.” Esta terminología procede de la tradición de Arpanet y, en ese ámbito, tiene un significado específico. Sin embargo, para la mayoría de las redes, significa que es posible ejecutar distintos sistemas de ruteo en la misma red. Esto es útil para los lugares en donde convergen las redes de varias organizaciones. Cada organización puede mantener su propio ruteo. Dado que cada actualización es etiquetada, es posible configurar que las gateways presten atención sólo a la correcta. Ciertas puertas de enlace están configuradas para recibir actualizaciones desde varios sistemas independientes. Éstas pasan información entre los sistemas de manera controlada. Tenga en cuenta que ésta no es una solución completa para los problemas de seguridad de ruteo. Cualquier gateway se puede configurar para escuchar las actualizaciones de cualquier sistema autónomo. Sin embargo, todavía es una herramienta muy útil a la hora de implementar políticas de ruteo cuando hay un cierto grado de confianza entre los administradores de red.

La segunda función estructural acerca de los mensajes de actualización de IGRP afecta el modo en que IGRP maneja las rutas predeterminadas. La mayoría de los protocolos de ruteo poseen un concepto de ruta predeterminada. No es a menudo práctica para que las actualizaciones de ruteo

enumeren cada red en el mundo. Por lo general un conjunto de gateways necesitan información de ruteo detallada para las redes dentro de su organización. Todo el tráfico para los destinos fuera de su organización se puede enviar a uno de algunos gatewayes de frontera. Esas gateways delimitadoras quizás tengan información más completa. La ruta al mejor gateway de frontera es una “ruta predeterminado”. Es un valor por defecto en el sentido que se utiliza para conseguir a cualquier destino que no se enumere específicamente en las actualizaciones de ruteo internas. El RIP, y algunos otros Routing Protocol, distribuyen la información sobre la ruta predeterminado como si fuera una red real. IGRP aplica un enfoque diferente. En lugar de una sola entrada falsa para la ruta predeterminada, IGRP permite que las redes reales se marquen como candidatas para convertirse en una predeterminada. Esto se implementa colocando la información sobre esas redes en una sección exterior especial del mensaje de actualización. Sin embargo, puede ser que también sea pensado en como girar un bit asociado a esas redes. Periódicamente IGRP busca todas las rutas predeterminadas de los candidatos y elige la de métrica inferior como la ruta predeterminada real.

Potencialmente, esta metodología de las rutas predeterminadas es de algún modo más flexible que aquella adoptada por la mayoría de las implementaciones RIP. Más comúnmente se pueden configurar los gateways RIP de modo que generen una ruta predeterminada con una determinada métrica especificada. La intención es que debería hacerse en las gateways de límite.

Descripción detallada

Esta sección proporciona una descripción detallada del IGRP.

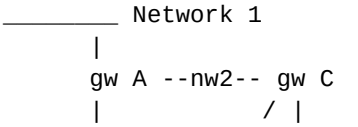
Descripción completa

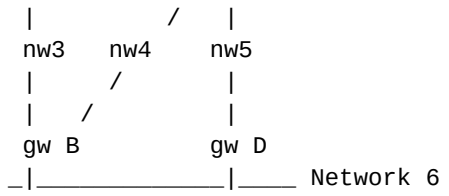
Al activar una gateway por primera vez, se inicializa su tabla de ruteo. Esto puede ser llevado a cabo por un operador desde una terminal de consola o mediante la lectura de la información en los archivos de configuración. Se provee una descripción de cada red conectada a la gateway, que incluye el retraso topológico a lo largo del link (por ejemplo, cuánto tiempo tarda un solo bit en atravesar el link) y el ancho de banda del link.

Figura 2

Por ejemplo, en el diagrama anterior, el gateway S estaría conectada a las redes 2 y 3 a través de las correspondientes interfaces. Así, inicialmente, el gateway 2 sabe solamente que puede alcanzar cualquier computadora destino en las redes 2 y 3. Todos los gatewayes se programan para transmitir periódicamente a sus gatewayes de vecindad la información que se han inicializado con, así como la información recopilada de otros gatewayes. Así, el gateway S recibiría las actualizaciones de los gatewayes R y T y aprendería que puede alcanzar los ordenadores en la red 1 a través del gateway R y los ordenadores en la red 4 a través del gateway T. Puesto que el gateway S envía su tabla de ruteo entera, en el gateway siguiente del ciclo T aprenderá que puede conseguir a la red 1 a través del gateway S. Es fácil ver que la información acerca de cada red del sistema llegará eventualmente a todas las gateways del sistema, siempre que la red se encuentre totalmente conectada.

Figura 3





Cada gateway computa una métrica compuesta para determinar la conveniencia de los trayectos de datos a las computadoras de destino. Por ejemplo, en el diagrama sobre, para un destino en la red 6, gateway A (el gw A) computaría las funciones de medición para dos trayectorias, vía los gatewayes B y el C. Observe que las trayectorias son definidas simplemente por el salto siguiente. Hay realmente tres rutas posibles de A a la red 6:

- Dirija a B
- Al C y entonces a B
- A C y luego a D

Sin embargo, el gateway A no necesita elegir entre las dos rutas que implican el C. La tabla de ruteo en A tiene una sola entrada que representa la trayectoria al C. Su métrico representa la mejor manera de conseguir del C al destino final. Si A envía un paquete a C, C es el que decide si usa B o D.

Ecuación 1

A continuación se muestra la función de métrica compuesta calculada para cada trayecto de datos.

```
[(K1 / Be) + (K2 * Dc)] r
```

Donde estén r = la confiabilidad fraccional (% de las transmisiones que se reciben con éxito en el salto siguiente), DC = retraso compuesto, = ancho de banda efectivo: ancho de banda sin cargar x (1 - ocupación del canal), y k1 y K2 = constantes.

Ecuación 2

En principio, el retraso compuesto, Dc, podría determinarse como se muestra a continuación:

```
Dc = Ds + Dcir + Dt
```

Donde Ds = retardo de conmutación , Dcir = retardo de circuito (retardo de propagación de 1 bit), y DT = retardo de transmisión (retardo sin carga para un mensaje de 1500 bits).

Sin embargo, una cifra de retardo estándar se utiliza en la práctica para cada tecnología del tipo de red. Por ejemplo, existirá una cifra de retardo estándar para Ethernet y para las líneas seriales a cualquier velocidad en bits determinada.

Aquí se brinda un ejemplo de cómo podría verse la tabla de ruteo del gateway A en el caso del diagrama de red 6 presentado anteriormente. (Observe que no se muestran los componentes individuales del vector métrico por razones de simplicidad.)

Ejemplo de la tabla de ruteo:

Red	Interfaz	Gateway siguiente	Métrico
1	NW 1	Ninguno	Conectado directamente
2	NW 2	Ninguno	Conectado

			directamente
3	NW 3	Ninguno	Conectado directamente
4	NW 2	C	1270
	NW 3	B	1180
5	NW 2	C	1270
	NW 3	B	2130
6	NW 2	C	2040
	NW 3	B	1180

El proceso básico de creación de una tabla de ruteo mediante el intercambio de información con los vecinos se describe por medio del algoritmo de Bellman-Ford. El algoritmo se ha utilizado en protocolos anteriores tales como RIP (RFC 1058). Para manejar redes más complejas, IGRP agrega tres funciones al algoritmo básico Bellman-Ford:

1. Para caracterizar trayectos, se usa un vector de métricas en vez de una métrica simple. Según la Ecuación 1, que se muestra más arriba, desde este vector se puede computar una métrica compuesta única. El uso de un vector permite que el gateway acomode diversos tipos de servicio, usando varios diversos coeficientes en la ecuación 1. Además, permite una representación más exacta de las características de la red que una sola métrica.
2. En vez de elegir un solo trayecto con la medición más pequeña, el tráfico se divide en varios trayectos, cuyas mediciones se ajustan a un rango específico. Esto permite que varias rutas sean utilizadas paralelamente, proporcionando a un mayor ancho de banda efectivo que cualquier solo ruta. El administrador de red especifica una V diferente. Todos los trayectos con la mínima métrica compuesta M se mantienen. Además, se conservan todos los trayectos cuya métrica es inferior a V x M. El tráfico se distribuye entre los trayectos múltiples en la proporción inversa a las mediciones compuestas.
3. Existen algunos problemas con este concepto de varianza. Es difícil subir con las estrategias que hacen uso de los valores de la variación mayores de 1, y también no lleva a los paquetes la colocación. En la Versión 8.2 de Cisco, no se implementa la característica de varianza. (No estoy seguro en qué versión fue quitada la característica.) El efecto de esto es fijar la variación permanentemente a 1.
4. Se han incorporado varias características a fin de proporcionar estabilidad en situaciones en las que la topología está cambiando. Estas características se piensan para evitar el rutear de los loopes y la “cuenta al infinito,” que han caracterizado las tentativas anteriores de utilizar los algoritmos del Ford-tipo para este tipo de aplicación. Las funciones de estabilidad primarias son "retenciones", "actualizaciones activadas", "horizontes divididos" y "envenenamiento". Éstos serán discutidos más detalladamente abajo.

La división del tráfico (punto 2) plantea un riesgo bastante sutil. La variación V está diseñada para permitir que las gateways usen rutas paralelas con diferentes velocidades. Por ejemplo, puede haber una línea de 9600 BPS ejecutándose paralelamente con una línea de 19200 BPS para la redundancia. Si la variación V es 1, sólo el mejor trayecto será utilizado. La línea de 9600 BPS no será utilizada tan si la línea de 19200 BPS tiene una confiabilidad razonable. (Sin embargo, si varias trayectorias son lo mismo, la carga será compartida entre ellos.) Aumentando la variación, podemos permitir que el tráfico esté partido entre la mejor ruta y otras rutas que están casi como buenos. Con una variación suficientemente grande, el tráfico se dividirá entre dos líneas. El peligro es que en caso de una variación lo suficientemente grande, las rutas permitidas no sólo son más lentas sino que también tienen una "dirección equivocada". Por lo tanto, debe existir una

regla adicional para evitar que el tráfico se envíe “en sentido ascendente”: No se envía tráfico junto a aquellos trayectos cuya métrica compuesta remota (la métrica compuesta calculada en el siguiente salto) es mayor que la métrica compuesta calculada en el gateway. Por lo general, se recomienda a los administradores de sistemas que no fijen la variación sobre 1, excepto en situaciones específicas donde sea necesario usar trayectos paralelos. En este caso, la varianza es configurada cuidadosamente para proveer los resultados "correctos".

IGRP está diseñado para gestionar varios "tipos de servicios" y varios protocolos. El tipo de servicio es una especificación en un paquete de datos que modifique la manera que las trayectorias deben para ser evaluadas. Por ejemplo, el protocolo TCP/IP le permite al paquete especificar la importancia relativa del ancho de banda alto, del retraso bajo o de la confiabilidad alta. Generalmente, las aplicaciones inactivas especificarán un retraso bajo, mientras que las aplicaciones de transferencia masiva especificarán un ancho de banda alto. Estos requisitos determinan los valores relativos de K1 y K2 que son apropiados para usarlos en Eq. 1. Cada combinación de especificaciones en el paquete que ha de admitirse se denomina "tipo de servicio". Para cada tipo de servicio debe elegirse un conjunto de parámetros K1 y K2. Se guarda una tabla de ruteo para cada tipo de servicio. Esto es así porque los trayectos son seleccionados y ordenados de acuerdo con la métrica compuesta definida por Eq. 1. Esto es diferente para cada tipo de servicio. La información de todas estas tablas de ruteo se combina para producir los mensajes de actualización de ruteo que intercambian las gateways, como lo describe la figura 7.

Características de estabilidad

Esta sección describe las retenciones, las actualizaciones activadas, el horizonte dividido y el envenenamiento. Estas funciones se han diseñado para evitar que los gateways elijan rutas erróneas. Según lo descrito en el RFC 1058 , esto puede suceder cuando una ruta vence inutilizable, al error de un gateway o de una red. En principio, los gateways adyacentes detectan las fallas. Luego, envían actualizaciones de ruteo que indican que la antigua ruta no se puede utilizar. Sin embargo, es posible que las actualizaciones no alcanzar a algunas partes de la red en absoluto, o sean retrasadas en alcanzar ciertos gatewayes. Una gateway que aún cree que la ruta vieja es buena puede continuar repartiendo esa información y, de esta forma, reintroduciendo a la ruta fallida dentro del sistema. Esta información propagará a través de la red y vendrá eventual detrás al gateway que la reinyectó. El resultado es una ruta circular.

De hecho hay una cierta Redundancia entre las contramedidas. Básicamente, las retenciones y las actualizaciones activadas deberían ser suficientes para evitar rutas erróneas en primer lugar. No obstante, en la práctica, diferentes errores de comunicación pueden hacer que resulten insuficientes. El horizonte y el envenenamiento de ruta partidos se piensan para evitar el rutear de los loopes en todo caso.

Normalmente, las nuevas tablas de ruteo se envían a los gatewayes de vecindad en una base normal (cada 90 segundos por abandono, aunque esto se pueda ajustar por el administrador de sistema). Una actualización disparada es una nueva tabla de ruteo que se envía inmediatamente en respuesta a algún cambio. El cambio más importante es retiro de una ruta. Esto puede suceder porque ha expirado un descanso (probablemente un gateway de vecindad o una línea ha ido abajo), o porque un mensaje de actualización del gateway siguiente en la trayectoria muestra que la trayectoria es no más usable. Cuando una gateway G detecta que una ruta ya no se puede utilizar, genera inmediatamente una actualización. Esta actualización mostrará que la ruta es inutilizable. Considere lo que sucede cuando esta actualización llega a las gateways vecinas. Si la ruta del vecino apuntaba a G, el vecino debe quitar la ruta. Esto hace al vecino accionar una actualización, un etc. Así un error accionará una ola de mensajes de actualización. Esta onda propagará en esa porción de la red en la cual las rutas entraron a través del gateway o de la red

fallado.

Las actualizaciones disparadas serían suficientes si pudiéramos garantizar que la ola de actualizaciones ha alcanzado cada gateway apropiada de manera inmediata. Sin embargo, hay dos problemas. Primero, los paquetes que contienen el mensaje de actualización se pueden caer o corromper por un cierto link en la red. Segundo, las actualizaciones provocadas no suceden de manera instantánea. Es posible que una gateway cuya actualización no haya sido activada emita una actualización normal en el tiempo incorrecto, haciendo que se vuelva a insertar la ruta incorrecta en un vecino cuya actualización ya ha sido activada. Las retenciones están diseñadas para solucionar estos problemas. La regla de retención indica que cuando se remueve una ruta, por algún tiempo no se aceptará ninguna ruta nueva para el mismo destino. Esto le otorga el tiempo necesario a las actualizaciones activadas para llegar a todos los otros gateways, para asegurarse de que cada nueva ruta que obtengamos no sea simplemente algún gateway reinsertando la antigua. El periodo de tiempo de retención debe ser de largo bastante tener en cuenta la onda de las actualizaciones activadas ir en la red. Además, debería incluir un par de ciclos de difusión para administrar paquetes caídos. Considere qué sucede si una de las actualizaciones activadas se cae o se corrompe. el gateway que envió la actualización enviará otra actualización cuando corresponda. Esto reiniciará la onda de las actualizaciones activadas en los vecinos que perdieron la onda inicial.

La combinación de actualizaciones activadas y de asentamientos debe ser suficiente librarse de las rutas caducado y evitar que sean reinsertadas. Sin embargo, algunas precauciones adicionales valen el hacer de todos modos. Permiten mismo las redes que presentas pérdidas de información, y las redes que se han dividido. Las precauciones adicionales que requiere IGRP son horizonte dividido y envenenamiento de ruta. El horizonte dividido surge de la observación de que no tiene sentido hacer que una ruta vuelva en la dirección por la cual vino. Considere la siguiente situación:

```
network 1        network 2
  -------------X-----------------X
           gateway A           gateway B
```

El gateway A dirá a B que tiene una ruta a la red 1. Cuando B envía las actualizaciones a A, nunca hay cualquier razón de ella para mencionar la red 1. Puesto que A está más cercano a 1, no hay razón de ella para considerar ir vía el B. La regla de división del horizonte dice un mensaje de actualización separado se debe generar para cada vecino (realmente cada red vecina). La actualización de un cierto vecino debería omitir rutas que apuntan a ese vecino. Esta regla previene los loopes entre los gatewayes adyacentes. El ejemplo supone que A es una interfaz para fallas de la red 1. Sin la regla de división del horizonte, B sería diciendo a A que puede conseguir a 1. Puesto que tiene no más una ruta real, A pudo coger esa ruta. En este caso, A y B ambas tendrían rutas a 1. Pero A señalaría a B y a B señalaría a las actualizaciones activadas A. por supuesto y los asentamientos deben evitar que esto suceda. Sin embargo, debido a que no existe ninguna razón para enviar la información al lugar de dónde provino, de todos modos es recomendable dividir el horizonte. Además de su función en la prevención de loops, la división del horizonte mantiene el tamaño de los mensajes de actualización en un nivel bajo.

El horizonte dividido previene los loops entre gateways adyacentes. El envenenamiento de ruta se piensa para romper loopes más grandes. La regla es que cuando una actualización muestra que la medición de una ruta existente se ha incrementado lo suficiente, hay un loop. La ruta deberá quitarse y colocarse en retención. La regla es actualmente que una ruta está quitada si la medición compuesta aumenta más que un factor de 1.1. No es seguro que apenas ningún aumento en la medición compuesta accione el retiro de la ruta, puesto que los pequeños cambios métricos pueden ocurrir debido a los cambios en la ocupación del canal o la confiabilidad. Por lo tanto, el factor de 1.1 es sólo un heurístico. El valor exacto no es crítico. Esperamos que esta

regla sea necesitada solamente para romper los loopes muy grandes, puesto que los pequeños serán prevenidos por las actualizaciones activadas y los asentamientos.

Deshabilitar retenciones

A partir de la versión 8.2, el código de Cisco tienen una opción para inhabilitar la retención. La desventaja de las retenciones es que retrasan la adopción de una nueva ruta cuando falla una ruta antigua. Con los parámetros predeterminados, puede tardar varios minutos hasta que el router adopte una nueva ruta luego de una carga. Sin embargo, por los motivos explicados anteriormente, no es seguro simplemente quitar las retenciones. El resultado sería cuenta a infinito, según lo descrito en el RFC 1058. Conjeturamos, pero no podemos probar, que con una versión más fuerte del envenenamiento de ruta, los asentamientos están necesitados no más para parar la cuenta a infinito. De esta forma, la inhabilitación de las retenciones da lugar a esta forma más fuerte de envenenamiento de ruta. Observe que las actualizaciones activadas y de división del horizonte siguen vigentes.

La manera más severa de envenenamiento de ruta está basada en un conteo de saltos. Si la cuenta de saltos para un trayecto aumenta, se elimina la ruta. Esto quitará obviamente las rutas que son todavía válidas. Si algo más de la red cambia de manera que el trayecto ahora atraviesa una o más puertas de enlace, se incrementará el recuento de saltos. En este ejemplo, la ruta continúa siendo válida. Sin embargo, no existe manera alguna que sea completamente segura de distinguir este caso de los loops de ruteo (cuenta a infinito) Por lo tanto, el enfoque más seguro es eliminar la ruta cada vez que aumenta el conteo de saltos. Si la ruta aún es legítima, será reinstalada por la actualización siguiente, y eso causará una actualización activada que reinstalará la ruta en otro lugar dentro del sistema.

El vector de distancia algorithms1 adopta generalmente las nuevas rutas fácilmente. El problema es borrar completamente los anteriores del sistema. De esta manera, una norma que es sumamente agresiva acerca de las rutas sospechosas que se eliminan, debería ser segura.

Detalles del proceso de actualización

El conjunto de procesos descripto en las Figuras 4 a 8 están diseñados para manejar un protocolo de red simple, por ejemplo, TCP/IP, DECnet o el protocolo ISO/OSI. Sin embargo, los detalles del protocolo se darán sólo para TCP/IP. Un único gateway puede procesar datos que obedecen a más de un protocolo. Porque cada protocolo tiene las diversos estructuras de direccionamiento y formatos de paquetes, el código de la computadora usado para implementar los cuadros 4 a 8 será generalmente diferente para cada protocolo. El proceso descrito en el cuadro 4 variará la mayoría, según lo descrito en las notas detalladas para el cuadro 4. Los procesos descritos en el cuadro 5 a 8 tendrán la misma estructura general. La diferencia principal entre un protocolo y otro será el formato del paquete de actualización de ruteo, el cual debe ser diseñado para que sea compatible con un protocolo específico.

Observe que la definición de un destino puede variar de protocolo a protocolo. El método descrito puede utilizarse para el ruteo a hosts individuales, a redes o para esquemas de direcciones jerárquicas más complejos. El tipo de ruteo usado dependerá de la estructura de direccionamiento del protocolo. La implementación de TCP/IP actual sólo admite el ruteo a redes IP. Así el “destino” significa realmente la red del IP o el subnet number. La información de subred sólo se mantiene para las redes conectadas.

Las figuras de la 4 a la 7 muestran el seudocódigo para varias partes del proceso de ruteo utilizado por las gateways. Al inicio del programa, se ingresan parámetros y protocolos aceptables

que describen cada interfaz.

El gateway manejará solamente ciertos protocolos que sean mencionados. Toda comunicación desde un sistema mediante un protocolo que no se encuentre en la lista será ignorada. Las entradas de datos son las siguientes:

- Las redes a las cuales se conecta el gateway.
- Ancho de banda descargado de cada red.
- Retardo topológico de cada red.
- Confiabilidad de cada red.
- Ocupación de canal de cada red.
- MTU de cada red.

La función de medición para cada trayecto de datos entonces se computa según la ecuación 1. Observe que los primeros tres elementos son razonablemente permanentes. Son una función de la tecnología de red subyacente y no dependen de que la carga. Se las puede configurar desde un archivo de configuración o por entrada directa del operador. Tenga en cuenta que IGRP no utiliza el retraso medido. Tanto la teoría como la experiencia sugieren que es muy difícil para los protocolos que usan retraso medido mantener un ruteo estable. Existen dos parámetros medidos: confiabilidad y ocupación del canal. La confiabilidad se basa en las tasas de errores sobre los que informan por el hardware o firmware de las interfaces de red.

Además de estas entradas, el algoritmo de ruteo requiere un valor para varios parámetros de ruteo. Esto incluye los valores del temporizador, variación, y si los asentamientos están habilitados. Normalmente esto se especificaría mediante un archivo de configuración o un operador de entrada. (A partir de la versión Cisco 8.2, la varianza está configurada en 1 de manera permanente).

Una vez que se ingresa la información inicial, las operaciones en el gateway son accionadas por los eventos — la llegada de un paquete de datos a la una de las interfaces de la red, o la expiración de un temporizador. Los procesos descritos en las figuras 4 a 7 se accionan de la siguiente manera:

- Cuando llega un paquete, se procesa según el cuadro 4. Como resultado, el paquete se envía a otra interfaz, se descarta o se acepta para seguir procesándolo.
- Cuando un paquete es validado por el gateway para el procesamiento adicional, se analiza en una moda del protocol específico no descrita en esta especificación. Si el paquete es una actualización del ruteo, se procesa de acuerdo con la Figura 5.
- El cuadro 6 muestra los eventos accionados por un temporizador. El temporizador se establece para generar una interrupción una vez por segundo. Cuando ocurre una interrupción, se ejecuta el proceso mostrado en la Figura 6.
- El cuadro 7 muestra una subrutina de la actualización de ruteo. Las llamadas a esta subrutina se muestran en las Figuras 5 y 6.
- Además, la Figura 8 muestra detalles de cálculos de métricas a los que hacen referencia las Figuras 5 y 7.

Hay cuatro constantes de tiempo críticos que propagación y expiración de la ruta del control. Estos constantes de tiempo se pueden fijar por el administrador de sistema. Sin embargo, hay valores predeterminados. Dichas constantes de tiempo son:

- Tiempo de broadcast — Las actualizaciones son transmitidas por todos los gatewayes en todas las interfaces conectadas esto a menudo. Lo predeterminado es una vez cada 90

segundos.

- Tiempo no válido — Si no se ha recibido ninguna actualización para una determinada trayectoria dentro de esta cantidad de tiempo, se considera haber medido el tiempo hacia fuera. Debe ser varias veces el tiempo de broadcast, para tener en cuenta la posibilidad que los paquetes que contenían una actualización se podrían caer por la red. El valor predeterminado es el triple del tiempo de difusión.
- Tiempo en espera — Cuando un destino se ha convertido en inalcanzable (o el métrico ha aumentado bastantes para causar el envenenamiento), el destino entra el “asentamiento”. Durante este estado, no se validará ninguna nueva trayectoria para el mismo destino para esta cantidad de tiempo. El período de inactividad indica cuánto debe durar este estado. Debería ser varias veces el tiempo de transmisión. El valor predeterminado es el triple del tiempo de difusión más 10 segundos. (Tal como se describe en la sección Deshabilitar retenciones, es posible deshabilitar las retenciones.)
- Flush time — Si no se ha recibido ninguna actualización para un destino determinado dentro de esta cantidad de tiempo, la entrada para ella se quita de la tabla de ruteo. Observe la diferencia entre el tiempo no válido y el tiempo de purga: Un trayecto se elimina y remueve luego del tiempo inválido. Si ya no quedan trayectos hacia un destino, el destino está ahora fuera de alcance. Sin embargo, la entrada de base de datos para el destina permanece. Debe permanecer para imponer el tiempo de retención. Luego del momento de purgar, la entrada de la base de datos se elimina de la tabla. Debe ser más largo que el tiempo no válido más el tiempo de retención. El tiempo predeterminado es de 7 veces el tiempo de transmisión.

Estas figuras presuponen las estructuras de datos principales siguientes. Un conjunto aparte de estas estructuras de datos se mantienen para cada protocolo suportado por la gateway. Dentro de cada protocolo, se mantiene un conjunto distinto de estructuras de datos para cada tipo de servicio que se debe admitir.

Para cada destino conocido en el sistema, existe una lista (posiblemente nula) de trayectos hacia el destino, un vencimiento de retención y un último plazo de actualización. La fecha de la última actualización es la última vez en que se incluyó un trayecto para este destino en una actualización desde otra gateway. Tenga en cuenta que también existen tiempos de actualización para cada trayecto. Cuando se elimina el último trayecto hacia un destino, se desactiva ese destino, a menos que esté inhabilitada la opción de desactivar (consulte la sección Inhabilitar la función desactivar para obtener más información). El tiempo de vencimiento de retención indica el tiempo en el cual expira la retención. El hecho de que sea no-cero indica que el destino está en el asentamiento. A fin de ahorrar tiempo de cálculo, también es una buena idea mantener una "mejor métrica" para cada destino. Esto es simplemente el mínimo de la métrica compuesta para todos los trayectos dirigidos al destino.

Para cada trayecto a un destino están la dirección del próximo salto en el trayecto, la interfaz a ser utilizada, un vector de mediciones con las características del trayecto, el cual inlcuye el retraso topológico, el ancho de banda, la confiabilidad y la ocupación del canal. La otra información también se asocia a cada trayectoria, incluyendo el conteo saltos, el MTU, la fuente de información, la medición compuesta remota, y una medición compuesta calculada de estos números según la ecuación 1. Hay también la hora de actualización más pasada. La fuente de información indica de dónde vino la actualización más reciente para ese trayecto. Éste es en la práctica lo mismo que el direccionamiento del salto siguiente. El último plazo de actualización es simplemente el tiempo en el cual la actualización más reciente llegó para este trayecto. Se utiliza para dar por finalizados trayectos con el tiempo de espera agotado.

Observe que un mensaje de actualización IGRP consta de tres partes. interior, sistema (que

significa "este sistema autónomo" pero no interior) y exterior. La sección interna es para rutas a subrutas. No toda la información de subred es incluida. Solamente las subredes de una red son incluidas. Es la red asociada con la dirección a la cual se envía la actualización. Normalmente, las actualizaciones se difunden en cada interfaz, por lo tanto, se trata simplemente de la red por medio de la cual se envía la difusión. (Otros casos se presentan para las respuestas a una petición de IGRP y a un IGRP de punto a punto.) Las redes principales (por ejemplo, NON-subredes) se ponen en la porción del sistema del mensaje de actualización a menos que se señalen por medio de una bandera específicamente como exterior.

Una red será señalada por medio de una bandera como exterior si era docta de otro gateway y la información llegó en la porción exterior del mensaje de actualización. La implementación de Cisco también permite que el administrador del sistema declare redes específicas como exteriores. Las rutas exteriores se denominan también "candidatas predeterminadas". Son las rutas a las cuales pase o a través de los gatewayes que se consideran ser apropiados como valores por defecto, que se utilizarán cuando no hay ruta explícita a un destino. Por ejemplo, en Rutgers configuramos la gateway que conecta Rutgers a nuestra red regional para que marque la ruta a la estructura básica NSFnet como externa. La implementación de Cisco elige una ruta predeterminada al seleccionar la ruta exterior con la métrica menor.

Las secciones siguientes se piensan para aclarar los cierta porcio'n de los cuadros 4 a 8.

Ruteo de Paquetes

La Figura 4 describe el procesamiento integral de los paquetes de entrada. Esto se utiliza simplemente para clarificar la terminología. Obviamente, ésta no es una descripción completa de lo que hace una gateway IP.

Este proceso usa la lista de protocolos soportados y la información acerca de las interfaces ingresada cuando la gateway se inicializa. Los detalles del procesamiento de paquetes dependen del protocolo que utilice el paquete. Está determinado en el Paso A. El Paso A es sólo una porción de la Figura 4 que está compartida con todo los protocolos. Una vez que conocen al Tipo de protocolo, la implementación del cuadro 4 apropiado al Tipo de protocolo se utiliza. El detalle del contenido de los paquetes se describe mediante las especificaciones del protocolo. Las especificaciones de un protocolo incluyen un procedimiento para determinar el destino de un paquete, un procedimiento para comparar el destino con las direcciones de la misma gateway para determinar si la gateway misma es el destino, un procedimiento para determinar si el paquete es una transmisión y un procedimiento para determinar si el destino es parte de una red especificada. Estos procedimientos se utilizan en los pasos B y el C del cuadro 4. La prueba en el paso D requiere una búsqueda de los destinos enumerados en la tabla de ruteo. Se satisface la prueba si hay una entrada en la tabla de ruteo para el destino, y ese destino ha asociado a él por lo menos un trayecto utilizable. Observe que el destino y los datos de trayecto usados en esto y el siguiente paso están mantenidos por separado para cada tipo de servicio soportado. Así, lo primero que hace este paso es determinar el tipo de servicio especificado por el paquete y seleccionar el conjunto de estructuras de datos correspondiente para usar en este y el siguiente paso.

Una trayectoria es usable con el propósito de los pasos D y E si su medición compuesta remota es menos que su medición compuesta. Un trayecto cuya métrica remota compuesta es mayor que la métrica compuesta en un trayecto en que el próximo salto está más lejos del destino, según la medición. Esto se refiere como “trayecto ascendente.” Normalmente, se esperaría que el uso de mediciones prevenga el cierre de las rutas ascendentes. Es fácil entender que un trayecto ascendente nunca puede ser el mejor. Sin embargo, si se permite una variación grande, las

trayectorias con excepción la mejor pueden ser utilizadas. Algunos de ésos podían estar por aguas arriba.

El paso E computa la ruta a utilizar. No se consideran los trayectos cuya métrica compuesta remota no es menor que sus métricas compuestas. Si más de una trayectoria es aceptable, tales trayectorias se utilizan en una forma cargada de alternancia circular. La frecuencia con la cual un trayecto se usa es inversamente proporcional a su métrica compleja.

Recepción de actualizaciones de ruteo

El cuadro 5 describe el proceso de una actualización de ruteo recibida de un gateway de vecindad. Tales actualizaciones consisten en una lista de entradas, que da la información para un destino único. En una actualización de ruteo único, puede ocurrir que exista más de una entrada para el mismo destino con el fin de acomodar los tipos de servicios múltiples. Cada uno de estas entradas se procesa individualmente, según lo descrito en el cuadro 5. Si una entrada se encuentra en la sección exterior de la actualización, el indicador exterior se configurará para el destino si se lo agrega como resultado de este proceso.

El proceso completo descrito en la Figura 5 debe repetirse una vez para cada tipo de servicio admitido por el gateway, mediante la información del conjunto destino / trayecto asociado con ese tipo de servicio. Esto se muestra en el Loop ultraperiférico en el cuadro 5. La actualización de ruteo entera se debe procesar una vez para cada tipo de servicio. (Observe que la implementación actual de IGRP no es compatible con varios tipos de servicio de manera que el loop ultraperiférico en realidad no está implementado).

En el paso A se realizan pruebas de aceptabilidad básica en el trayecto. Esto debería incluir pruebas de razonabilidad para el destino. Los números de red imposibles ("Marcianos") deben rechazarse. (Refiera al RFC 1009 y al RFC 1122 para más información.) Las actualizaciones también se rechazan si el destino que se refieren está en el asentamiento, es decir el tiempo de vencimiento de retención es no-cero y posterior que la hora actual.

En el paso B, se explora la tabla B para comprobar si esta entrada describe una ruta ya conocida. Una trayectoria en la tabla de ruteo es definida por el destino con el cual es asociada, el salto siguiente enumerado como parte de la trayectoria, la interfaz de salida que se utilizarán para la trayectoria, y la fuente de información (vino el direccionamiento de la cual la actualización — en la práctica normalmente lo mismo que el salto siguiente). La entrada desde el paquete de actualización se describe como una ruta cuyo destino se enumera en la entrada, cuya interfaz de salida es la interfaz a la que llegó la actualización, y cuyo próximo salto y fuente de información será la dirección de la gateway que envió la actualización (la "fuente" S).

En los pasos H y T, está programado el proceso de actualización descrito en la Figura 7. Este proceso se ejecutará, en realidad, después de finalizar todo el proceso descrito en la figura 5. Es decir, el proceso actualización descrito en el cuadro 7 sucederá solamente una vez, incluso si se acciona varias veces durante el proceso descrito en el cuadro 5. Además, se deben tomar precauciones para evitar que las actualizaciones se ejecuten con demasiada frecuencia, si la red está cambiando rápidamente.

Se hace el paso K si el destino descrito por la entrada actual en el paquete de actualización existe ya en la tabla de ruteo. K compara la nueva métrica compuesta computada desde la información en el paquete de actualización con la mejor métrica compuesta para el destino. Observe que la mejor métrica compuesta no se vuelve a calcular en este momento, entonces, si el trayecto que se considera ya está en la tabla de ruteo, esta prueba puede comparar métricas nuevas y

antiguas para el mismo trayecto.

El paso L se realiza para las trayectorias que son peores que la mejor medición compuesta existente. Esto incluye ambas nuevas trayectorias que sean peores que las existencias y los trayectos existentes cuya medición compuesta ha aumentado. El paso L comprueba si el nuevo trayecto es aceptable. Observe que esto introduce de forma experimental ambos la prueba para si una nueva trayectoria es bastante buena guardar, y envenenamiento de ruta. Para que sea aceptable, el valor de retardo no debe ser el valor especial que indica un destino inalcanzable (para la implementación de la IP actual, todos ellos en un campo de bit 24) y la métrica compuesta (calculada como se especifica en la figura 8) debe ser admisible. Para determinar si la medición compuesta es aceptable, compárela con las mediciones compuestas del resto de las trayectorias al destino. Deje M ser el mínimo de éstos. El nuevo trayecto es aceptable si es < V X M, DONDE V ES LA VARIANCIÓN CONFIGURADA CUANDO SE INICIÓ LA GATEWAY. SI V = 1 (LO QUE SIEMPRE ES VERDADERO EN LA VERSIÓN 8.2 DE CISCO), ENTONCES UNA MÉTRICA PEOR QUE LA EXISTENTE NO ES ACEPTABLE. HAY UNA SOLA EXCEPCIÓN A ESTO: SI EL TRAYECTO TODAVÍA YA Existe Y ES EL ÚNICO HACIA EL DESTINO, SERÁ RETENIDO SI LA MEDICIÓN NO HA AUMENTADO MÁS DEL 10% (O EN AQUELLOS CASOS EN QUE LAS RETENCIONES SE HAN INHABILITADO, SI EL CONTEO DE SALTOS NO HA INCREMENTADO).

El paso V se realiza cuando la nueva información para un trayecto indica que la métrica compuesta disminuirá. Las mediciones compuestas de todas las trayectorias al destino D se comparan. En esta comparación, se utiliza la nueva métrica compuesta P en lugar de la que aparece en la tabla de ruteo. Se calcula la métrica compuesta mínima M. Luego todos los trayectos D se vuelven a examinar. Si la métrica compuesta para cualquier trayecto > M x V, se elimina ese trayecto. V es la variación, ingresada cuando la gateway fue inicializada. (A partir de la versión Cisco 8.2, la varianza está configurada en 1 de manera permanente).

Procesamiento periódico

El proceso descrito en el cuadro 6 se acciona una vez al segundo. Examina varios temporizadores en la tabla de ruteo, para comprobar si alguno ha caducado. Estos temporizadores se describen más arriba.

En el Paso U, se activa el proceso descrito en la Figura 7.

Los pasos R y S son necesarios dado que la métrica compuesta almacenada en la tabla de ruteo depende de la ocupación del canal, que cambia en el tiempo, en función de las mediciones. La ocupación del canal se recalcula en forma periódica por medio de un promedio fluctuante de tráfico medido a través de la interfaz. Si el nuevo valor calculado difiere del existente, todas las métricas combinadas que conciernen a esa interfaz deben ser ajustadas. Se examinan todos los trayectos que se presentan en la tabla de ruteo. La métrica compuesta de cualquier ruta cuyo próximo salto use la interfaz "I" es recalculada. Esto se realiza de acuerdo con la Ecuación 1, usando como ocupación del canal el máximo del valor almacenado en la tabla de ruteo como parte de la métrica del trayecto y también, la ocupación del canal recientemente calculada de la interfaz.

Genere mensajes de actualización

La Figura 7 describe cómo el puerto de enlace genera mensajes de actualización para enviar a los otros puertos de enlace. Un mensaje separado se genera para cada interfaz de la red asociada al gateway. Ese mensaje es entonces enviado a otras gateways a las que se puede

acceder a través de la interfaz (Paso J). Esto se realiza por lo general, enviando el mensaje como una transmisión. Sin embargo, si la tecnología o el protocolo de red no permiten la transmisión, puede que sea necesario enviar el mensaje a cada gateway individualmente.

El mensaje es aumentado generalmente agregando una entrada para cada destino en la tabla de ruteo, en el paso G. Observe que el destino/los datos de trayecto asociados a cada tipo de servicio debe ser utilizado. En el peor de los casos, se agrega una nueva entrada a la actualización para cada destino para cada tipo de servicio. Sin embargo, antes de agregar una entrada en el mensaje de actualización en el paso G, se escanean las entradas que ya se agregaron. Si la nueva entrada está ya presente en el mensaje de actualización, no se agrega otra vez. Una nueva entrada duplica existente cuando los destinos y los gatewayes del salto siguiente son lo mismo.

Por la simplicidad, el pseudocode omite una cosa — los mensajes de la actualización de IGRP tienen tres porciones: el interior, el sistema, y el exterior, así que significa que hay realmente tres loopes sobre los destinos. El primer incluye solamente las subredes de la red a la cual se está enviando la actualización. El segundo incluye todas las redes principales (por ejemplo, las NON-subredes) que no se señalen por medio de una bandera como exterior. El tercero incluye todas las redes principales que se señalen por medio de una bandera como exterior.

El paso E implementa la prueba de división del horizonte. En el caso normal, esta prueba falla con las rutas cuyo mejor trayecto sale de la misma interfaz por la que se está enviando la actualización. Sin embargo, si se envía la actualización a un destino específico (por ejemplo, en respuesta a un pedido de IGRP desde otra gateway o como parte de un "IGPR punto a punto"), la división del horizonte falla sólo si el mejor trayecto provenía originalmente de ese destino (su "fuente de información" es la misma que el destino) y su interfaz de salida es la misma que aquella de donde vino el pedido.

Información de cálculo de métrica

La Figura 8 describe cómo se procesa la información métrica a partir de los mensajes de actualización recibidos por la gateway, y cómo se genera para los mensajes de actualización enviados por la gateway. Observe que la entrada se basa en una ruta específica al destino. Si hay más de una trayectoria al destino, se elige una trayectoria cuya medición compuesta es mínima. Si más de un trayecto posee la métrica compuesta mínima, se utiliza una regla para desempatar arbitraria. (Para la mayoría de los protocolos, esto se basa en la dirección del próximo hop gateway.)

Cuadro 4 — Proceso de los paquetes entrantes

```
Data packet arrives using interface I

A   Determine protocol used by packet

    If protocol is not supported
      then discard packet

B   If destination address matches any of gateway's addresses
    or the broadcast address
      then process packet in protocol-specific way

C   If destination is on a directly-connected network
      then send packet direct to the destination, using
      the encapsulation appropriate to the protocol and link type
```

```
D   If there are no paths to the destination in the routing
    table, or all paths are upstream
      then send protocol-specific error message and discard the packet

E   Choose the next path to use. If there are more than
    one, alternate round-robin with frequency proportional
    to inverse of composite metric.

    Get next hop from path chosen in previous step.

    Send packet to next hop, using encapsulation appropriate
    to protocol and data link type.
```

Cuadro 5 — Proceso de las actualizaciones de ruteo entrantes

```
Routing update arrives from source S

    For each type of service supported by gateway
      Use routing data associated with this type of service

      For each destination D shown in update

A       If D is unacceptable or in holddown
          then ignore this entry and continue loop with next destination D

B       Compute metrics for path P to D via S (see Fig 8)

        If destination D is not already in the routing table
        then Begin

          Add path P to the routing table, setting last
          update times for P and D to current time.

H         Trigger an update

          Set composite metric for D and P to new composite
          metric computed in step B.

          End

        Else begin (dest. D is already in routing table)

K         Compare the new composite metric for P with best
          existing metric for D.

           New > old:

L            If D is shown as unreachable in the update,
             or holddowns are enabled and
              the new composite metric >
                (the existing metric for D) * V
                [use 1.1 instead of V if V = 1,
                as it is as of Cisco release 8.2]
O            or holddowns are disabled and
             P has a new hop count > old hop count
             then Begin

              Remove P from routing table if present

              If P was the last route to D
                then Unless holddowns are disabled
                    Set holddown time for D to
                     current time + holddown time
T                  and Trigger an update
```

```
              End

             else Begin

              Compute new best composite metric for D

              Put the new metric information into the
              entry for P in the routing table

              Add path P to the routing table if it
              was not present.

              Set last update times for P and D to
              current time.

              End

           New <= OLD:

V            Set composite metric for D and P to new
             composite metric computed in step B.

             If any other paths to D are now outside the
             variance, remove them.

             Put the new metric information into the
             entry for P in the routing table

             Set last update times for P and D to
             current time.

          End

        End of for

      End of for
```

Cuadro 6 — Procesamiento periódico

```
Process is activated by regular clock, e.g. once per second

    For each path P in the routing table (except directly
    connected interfaces)

      If current time < P'S LAST UPDATE TIME + INVALID TIME
        THEN CONTINUE WITH THE NEXT PATH P

      Remove P from routing table

      If P was the last route to D
        then Set metric for D to inaccessible
          Unless holddowns are disabled,
            Start holddown timer for D and
          Trigger an update

        else Recompute the best metric for D

      End of for

    For each destination D in the routing table

      If D's metric is inaccessible
        then Begin
```

```
        Clear all paths to D

        If current time >= D's last update time + flush time
          then Remove entry for D

        End

      End of for

    For each network interface I attached to the gateway

R     Recompute channel occupancy and error rate

S     If channel occupancy or error rate has changed,
        then recompute metrics

      End of for

    At intervals of broadcast time

U     Trigger update
```

Cuadro 7 — Genere la actualización

```
Process is caused by "trigger update"

    For each network interface I attached to the gateway

      Create empty update message

      For each type of service S supported

        Use path/destination data for S

        For each destination D

E         If any paths to D have a next hop reached through I
            then continue with the next destination

          If any paths to D with minimal composite metric are
          already in the update message
            then continue with the next destination

G         Create an entry for D in the update message, using
          metric information from a path with minimal
          composite metric (see Fig. 8)

          End of for

        End of for

J     If there are any entries in the update message
       then send it out interface I

      End of for
```

Cuadro 8 — Detalles de los cálculos métricos

Esta sección describe el procedimiento para los cálculos de métrica y los conteos saltos de una actualización de ruteo de llegada. La entrada a esta función es la entrada para un destino específico en un paquete de actualización de ruteo. La salida es un vector de métrica que se puede utilizar para computar la medición compuesta, y un conteo saltos. Si se agrega este trayecto a la tabla de ruteo, se ingresa todo el vector de métrica en la tabla. Los parámetros de

interfaz utilizados en las siguientes definiciones son los que se configuraron al inicializar la gateway, para la interfaz a la cual llegó la actualización de ruteo, excepto que la ocupación del canal y la confiabilidad están basadas en un promedio fluctuante de tráfico medido a través de la interfaz.

- Retardo = retardo del retraso topológico del paquete + de la interfaz
- Ancho de banda = máx (ancho de banda de paquete, ancho de banda de interfaz)
- Confiabilidad = mín (confiabilidad desde el paquete, confiabilidad de la interfaz)
- Ocupación de canales = máx (ocupación de canales del paquete, ocupación de canales de la interfaz)(Máximo se utiliza para el ancho de banda porque el ancho de banda métrico se salva en la forma inversa. Conceptual, queremos el ancho de banda mínima.) Observe que la ocupación del canal original del paquete debe ser guardada, puesto que será necesaria recalcular la ocupación del canal eficaz siempre que la ocupación de canal de interfaz cambie.

Los valores siguientes no forman parte del vector métrico, pero también se mantienen en la tabla de ruteo como características del trayecto:

- Conteo saltos = conteo saltos del paquete.
- MTU = mín (MTU de paquete, MTU de interfaz)
- Medición compuesta remota = calculado de la ecuación 1 usando los valores métricos del paquete. Es decir, los componentes de la métrica son los del paquete y no están actualizados como se muestra arriba. Esto debe ser calculada obviamente antes de que los ajustes mostrados arriba se hagan.
- Métrica compuesta = calculada desde la ecuación 1 utilizando los valores métricos calculados según se describe en esta sección.

Esta parte restante de esta sección describe el procedimiento para calcular métricas y conteo de saltos para el envío de actualizaciones de ruteo.

Esta función determina la información de medición y el recuento de saltos que se introducirán en un paquete de actualización saliente. Se basa en una trayectoria específica a un destino, si hay algunos trayectos utilizables. Si no existen trayectos, o los trayectos son todos ascendentes, el destino se denomina inaccesible.

```
If destination is inaccessible, this is indicated by using a specific
        value in the delay field. This value is chosen to be larger
        than the largest valid delay. For the IP implementation this is
        all ones in a 24-bit field.

   If destination is directly reachable through one of the interfaces, use
        the delay, bandwidth, reliability, and channel occupancy of the
        interface. Set hop count to 0.

   Otherwise, use the vector of metrics associated with the path in the
        routing table. Add one to the hop count from the path in the
        routing table.
```

Detalles de la implementación de IP

Esta sección describe brevemente los formatos de paquete que utiliza Cisco IGRP. El IGRP se envía usando los datagramas IP con protocolo IP 9 (IGP). El paquete comienza con un encabezado. Comienza inmediatamente después del encabezado IP.

```
unsigned version: 4;  /* protocol version number */
```

```
    unsigned opcode: 4;   /* opcode */
    uchar edition;        /* edition number */
    ushort asystem;       /* autonomous system number */
    ushort ninterior;     /* number of subnets in local net */
    ushort nsystem;       /* number of networks in AS */
    ushort nexterior;     /* number of networks outside AS */
    ushort checksum;      /* checksum of IGRP header and data */
```

Para los mensajes de actualización, la información de ruteo va inmediatamente después del encabezado.

El número de la versión es los paquetes 1. que tienen otros números de la versión se ignora actualmente.

El opcode puede ser 1 = update o 2 = request

Esto indica el tipo de mensaje. El formato de los dos tipos de mensajes se brindará a continuación.

La edición es un número de serie que se incrementa toda vez que se produce un cambio en la tabla de ruteo. (Esto se hace en esas condiciones en las cuales el pseudocode antedicho diga para accionar una actualización de ruteo.) El número de edición permite que los gatewayes eviten procesar las actualizaciones que contienen la información que han considerado ya. (Esto no se implementa actualmente. Es decir, el número de edición se genera correctamente, pero se ignora en la entrada. Dado que es posible que se pierdan paquetes, no queda claro si el número de edición es suficiente para evitar duplicar el proceso. Deberá verificar que todos los paquetes asociados con la edición hayan sido procesados.

Asystem es el número de sistema autónomo. En la implementación de Cisco, un gateway puede participar en más de un sistema autónomo. Cada uno de esos sistemas ejecuta su propio protocolo IGRP. Conceptualmente, hay tablas de ruteo completamente separadas para cada sistema autónomo. Las rutas que llegan vía IGRP desde un sistema autónomo se envían solamente en actualizaciones para ese AS. Este campo permite que el gateway seleccione el conjunto de tablas de ruteo que utilizará para el procesamiento de este mensaje. Si la gateway recibe un mensaje IGRP de un AS para el cual no está configurado, se ignora. De hecho, la implementación de Cisco permite que la información se "fugue" de un AS a otro. Sin embargo, considero que eso es una herramienta administrativa y no una parte del protocolo.

Ninterior, nsystem y nexterior indican el número de entradas en cada una de las tres secciones de mensajes de actualización. Estas secciones se describieron anteriormente. No hay otra demarcación entre las secciones. Se toma a las primeras n entradas interiores como interiores, las próximas n entradas del sistema como del sistema y la n exterior final como exterior.

La suma de comprobación es una suma de comprobación de IP, computada usando el mismo algoritmo de suma de comprobación como un suma de comprobación de UDP. La suma de comprobación se calcula en el encabezado IGRP y en toda información de ruteo que le sigue. El campo de checksum se fija a cero al computar la suma de comprobación. La suma de comprobación no incluye el encabezado IP, ni hay cualquier encabezado virtual como en el UDP y el TCP.

Solicitudes

Una petición de IGRP pide que el beneficiario envíe su tabla de ruteo. El mensaje request tiene solamente una encabezado. Solamente se utilizan la versión, el opcode, y los campos del

asystem. El resto de los campos son cero. Se espera que el receptor envíe un mensaje de actualización normal IGRP al solicitante.

Actualizaciones

Un mensaje de la actualización de IGRP contiene una encabezado, seguida inmediatamente por las entradas de ruteo. Se incluirá la cantidad de entradas de ruteo que quepa en un datagrama de 1500 bytes (incluido el encabezado IP). Con las declaraciones de la estructura actual, esto permite hasta 104 entradas. Si se necesitan más entradas, se envían diversos mensajes de actualización. Debido a que los mensajes de actualización son simplemente procesados entrada por entrada, no tiene ninguna ventaja utilizar un mensaje único fragmentado a varios independientes.

Aquí está la estructura de una entrada de ruteo:

```
uchar number[3];       /* 3 significant octets of IP address */
    uchar delay[3];        /* delay, in tens of microseconds */
    uchar bandwidth[3];    /* bandwidth, in units of 1 Kbit/sec */
    uchar mtu[2];          /* MTU, in octets */
    uchar reliability;     /* percent packets successfully tx/rx */
    uchar load;            /* percent of channel occupied */
    uchar hopcount;        /* hop count */
```

Los campos definidos como uchar[2] y uchar[3] son meramente números enteros binarios de 16 y 24 bits, en un orden de red IP normal.

Number define el destino que se describe. Es una dirección IP. Para ahorrar espacio, se proporcionan únicamente los 3 primeros bytes de la dirección IP, salvo en la sección interior. En la sección interior, se dan los 3 últimos bytes. Para las rutas de sistema y externas, no son posibles las subredes, por lo que el byte de orden bajo es siempre cero. Las rutas interiores son siempre subredes de una red conocida, por lo que se suministra el primer byte de ese número de red.

El retraso es en unidades de 10 microsegundos. Esto le proporciona un rango de 10 microsegundos a 168 segundos, que parece ser suficiente. Un retardo de todos unos indica que la red es inalcanzable.

El ancho de banda es ancho de banda inverso en bits por segundo ampliado por un factor de 1.0e10. El rango comprende desde una línea de 1200 BPS a 10 Gbps. (Esto es, si el ancho de banda es N Kbps, el número utilizado es 10000000 / N).

La MTU es en bytes.

La confiabilidad se da como una parte de 255. Es decir, 255 es el 100%.

La carga está dada como una fracción de 255.

El conteo saltos es una cuenta simple.

Debido a las unidades extrañas utilizadas para el ancho de banda y retardo, algunos ejemplos parecen correctos. Éstos son los valores predeterminados usados para varios medios comunes.

	Delay	Bandwidth
Satellite	200,000 (2 sec)	20 (500 Mbit)

```
Ethernet            100 (1 ms)           1,000
1.544 Mbit         2000 (20 ms)          6,476
64 Kbit            2000                156,250
56 Kbit            2000                178,571
10 Kbit            2000              1,000,000
1 Kbit             2000             10,000,000
```

Cómputos métricos

Aquí tiene una descripción de cómo se computa la métrica compuesta en la versión 8.0(3) de Cisco.

```
metric = [K1*bandwidth + (K2*bandwidth)/(256 - load) + K3*delay] *
                         [K5/(reliability + K4)]

    If K5 == 0, the reliability term is not included.

    The default version of IGRP has K1 == K3 == 1, K2 == K4 == K5 == 0
```

Información Relacionada

- Página de Soporte de IP Routing
- Página de soporte de IGRP
- Soporte Técnico - Cisco Systems