Apuntes

de

Redes de Ordenadores

Tema 11

IP Routing

Uploaded by

IngTeleco

http://ingteleco.iespana.es
ingtelecoweb@hotmail.com

La dirección URL puede sufrir modificaciones en el futuro. Si no funciona contacta por email

11.- PROTOCOLOS DE ROUTING DE INTERNET

11.1.- PROTOCOLOS DE ROUTING DE INTERNET

Internet está formada por multitud de redes interconectadas, pertenecientes a diversas empresas u organismos. Todas estas redes están conectadas de una u otra forma, y todas ellas comparten a nivel de red el protocolo IP. A pesar de esta interoperabilidad, existen dos aspectos fundamentales en los que las redes pueden diferir entre si:

- **La información de routing y el protocolo utilizado**: existen como veremos multitud de protocolos de routing diferentes, unos basados en el algoritmo del vector distancia y otros en el del estado del enlace; incluso utilizando el mismo algoritmo se pueden emplean protocolos diferentes. Aún utilizando el mismo protocolo de routing dos proveedores diferentes normalmente no querrán que sus routers intercambien con los routers de otro proveedor la misma información que intercambian internamente.

- La **política de intercambio de tráfico**: una red puede tener acuerdos bilaterales o multilaterales para intercambiar tráfico con otras, pero por ejemplo puede no estar dispuesta a ser vía de tránsito para el tráfico entre dos redes, aun cuando desde el punto de vista técnico pueda ser el camino mas corto entre ambas.

Sistema Autónomo

Para permitir a cada red intercambiar su información de routing y definir su política de intercambio de tráfico se ha creado el concepto de Sistema Autónomo. Entendemos por Sistema Autónomo (AS, Autonomous System) la subred que es administrada o gestionada por una autoridad común, que tiene un protocolo de routing homogéneo mediante el cual intercambia información en toda la subred, y que posee una política común para el intercambio de tráfico con otras redes o sistemas autónomos.

Normalmente cada ISP (Internet Service Provider) constituye su propio sistema autónomo; en España, como en otros países, la red académica RedIRIS tiene un sistema autónomo propio. Los sistemas autónomos reciben números de dos bytes que se registran de forma análoga a las direcciones IP; por ejemplo el sistema autónomo de RedIRIS tiene el número 766.

Así pues, como mínimo en la Internet se dan dos niveles jerárquicos de routing, el que se realiza dentro de un sistema autónomo (AS) y el que se efectúa *entre* sistemas autónomos. Al primero lo denominamos routing interno, o routing en el interior de la pasarela (pasarela es una antigua denominación de router). Al routing entre sistemas autónomos lo denominamos routing externo, o también routing exterior a la pasarela. Dado que los requerimientos en uno y otro caso son muy diferentes, se utilizan protocolos de routing distintos en uno y otro caso.

Con el fin de poder efectuar correctamente la función de routing, es preciso que los routers mantengan sus tablas de encaminamiento sincronizadas y con una visión coherente de la red. La función básica de un protocolo de routing es comunicar la accesibilidad a las redes, de modo que cada “router” de una red pueda determinar la mejor ruta desde una red hasta otra.

Un protocolo de routing debe estar diseñado para:

- Describir el coste de la mejor ruta haciendo uso de una métrica de encaminamiento.
- Contemplar la existencia de múltiples rutas activas entre dos redes.
- Propagar la información de encaminamiento con precisión evitando crear rutas incorrectas.
- Minimizar el tráfico de la red debido al propio protocolo de routing.
- Minimizar la carga de las máquinas que no desarrollan funciones de encaminamiento.
- Evitar repentinos picos de tráfico en la red después del cambio de una ruta.
- Escalar bien a redes grandes.
- Converger rápidamente en una topología aceptada por todos los “routers” después de un cambio de rutas.
- Evitar propagar fallos de encaminamiento a largas distancias.
- Tener aspectos de seguridad que prevengan falsas notificaciones.

Los protocolos de routing dentro de un sistema autónomo se denominan IGP (Interior Gateway Protocol), mientras que los utilizados entre sistemas autónomos diferentes se llaman EGP (Exterior Gateway Protocol).

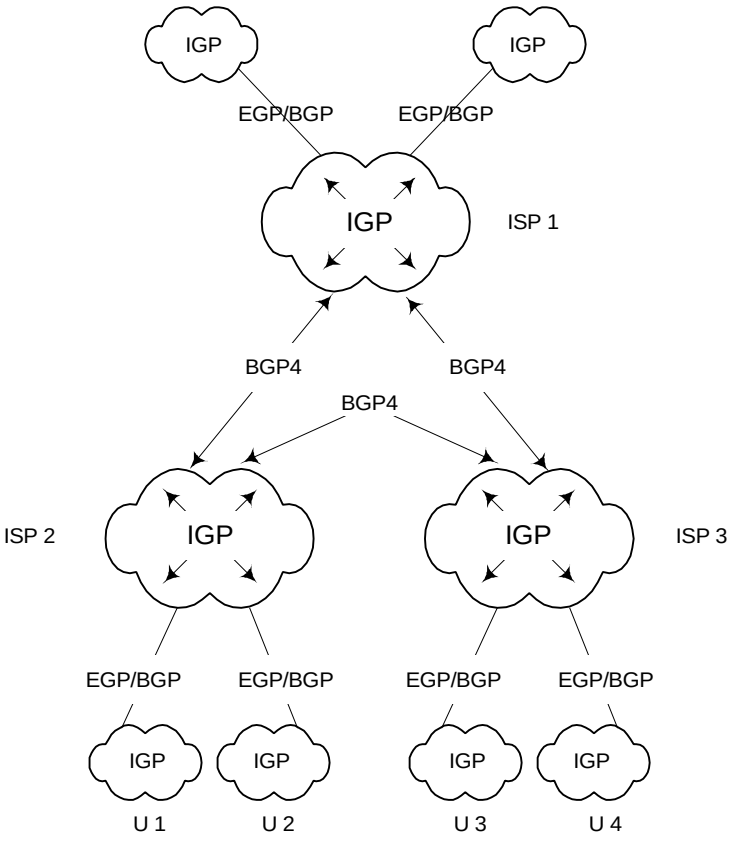

Figura 11.1

11.2.- PROTOCOLOS DE ROUTING INTERNO (IGP)

IGP describe una necesidad y no el nombre de un protocolo definido. La mayoría de las redes corporativas operan como sistemas autónomos, aunque no estén conectados a Internet, por lo que los IGPs son utilizados con profusión. Los protocolos IGP nunca aparecen en Internet, sino que permanecen restringidos al ámbito de un Sistema Autónomo.

En la Internet se usan actualmente diversos protocolos de routing IGP (Interior Gateway Protocol). Estos pueden agruparse en protocolos de vector distancia (RIP, RIPv2, IGRP y EIGRP) y protocolos del estado del enlace (IS-IS y OSPF). Describiremos a continuación las características y operación de algunos de ellos.

11.3.- RIP y RIPv2

RIP (Routing Information Protocol) es uno de los protocolos de routing más antiguos, derivado del protocolo de routing de XNS (Xerox Network Systems); RIP sufre los problemas típicos de los algoritmos basados en el vector distancia, tales como la cuenta a infinito, envío de excesiva información de routing, etc. Estos problemas aumentan a medida que aumenta el tamaño de los sistemas autónomos. A pesar de esto es aún muy utilizado en la Internet. Existen dos versiones de RIP: la versión 1, que se definió en el RFC 1058 y se publicó en 1983 (aunque se empezó a utilizar mucho antes) se ha declarado histórica, es decir su uso está desaconsejado. En vista de la popularidad de RIP y de los muchos problemas que presentaba en 1993 se publicó RIP versión 2 intentando resolver algunos de ellos (RFC 1388).

Para los requerimientos de las redes actuales RIP es bastante limitado:

- Sólo mide el rendimiento de una ruta mediante la cuenta de saltos.
- El número de “routers” entre un punto y el destino está limitado, por motivos de rendimiento, a 15.
- No tiene soporte explícito para direccionamiento de subred, por lo que no puede contempla máscaras de subred de longitud variable.
- No puede utilizar múltiples rutas activas entre dos redes; siempre se elige la ruta con menor número de saltos aún cuando haya otra ruta con más saltos que utilice circuitos más rápidos y tenga menor retraso.
- No responde rápidamente ante los fallos en la red.
- No es fácilmente escalable y puede consumir una capacidad considerable del circuito cuando se produce una actualización de las tablas.
- Utiliza difusión a nivel MAC (Ethernet) para las actualizaciones de tablas, que son recibidas por todos los nodos de la red, aún cuando no estén interesados en la actualización.
- En las versiones originales era posible la existencia de bucles de encaminamiento, si bien las versiones más recientes han asegurado que los bucles se resuelven más rápidamente, a expensas del volumen de tráfico RIP.

Las actualizaciones que se han hecho de RIP han solucionado en parte algunas de las limitaciones anteriores, con lo que RIP puede operar de forma plenamente satisfactoria en redes de tráfico limitado. Es posible, sin embargo, que cuando se utilizan equipos de diferentes vendedores aparezcan versiones diferentes de RIP que no sean plenamente compatibles y que el comportamiento no sea exactamente el esperado.

11.3.1.- Funcionamiento de RIP

Cuando un “router” RIP arranca, conoce a partir de sus ficheros de configuración las redes a las que está conectado. Recoge esta información en una tabla de encaminamiento y difunde tramas para enviarlas por todas ellas como notificaciones de las redes que puede alcanzar. RIP utiliza el puerto 520 UDP. Otros “routers” en la red escuchan las notificaciones y añaden las direcciones de red encontradas en ellas a su tabla de encaminamiento. Cuando el “router” vuelva a difundir su tabla de encaminamiento, incluirá las nuevas direcciones encontradas en las notificaciones de otros “routers”.
La tabla de un “router” RIP tendrá los siguientes campos para cada dirección de red:

- Dirección. Dirección IP de una red.
- Pasarela. El “router” vecino con un camino hacia dicha red.
- Interfaz. El interfaz físico a emplear para acceder al “router”.
- Métrica. El número de saltos hasta dicha red.
- Tiempo. Tiempo pasado desde la última actualización de esta entrada.

En sus notificaciones, los “routers” deben indicar el número de saltos (costo) necesario para alcanzar la red, definido un salto como el paso a través de un “router”. Cuando la notificación de una red pasa de un interfaz a otro, el costo de alcanzarla aumenta en uno, de modo que un “router” que conozca varias rutas para llegar a una red pueda decidir cual es la mejor de ellas (la más corta).

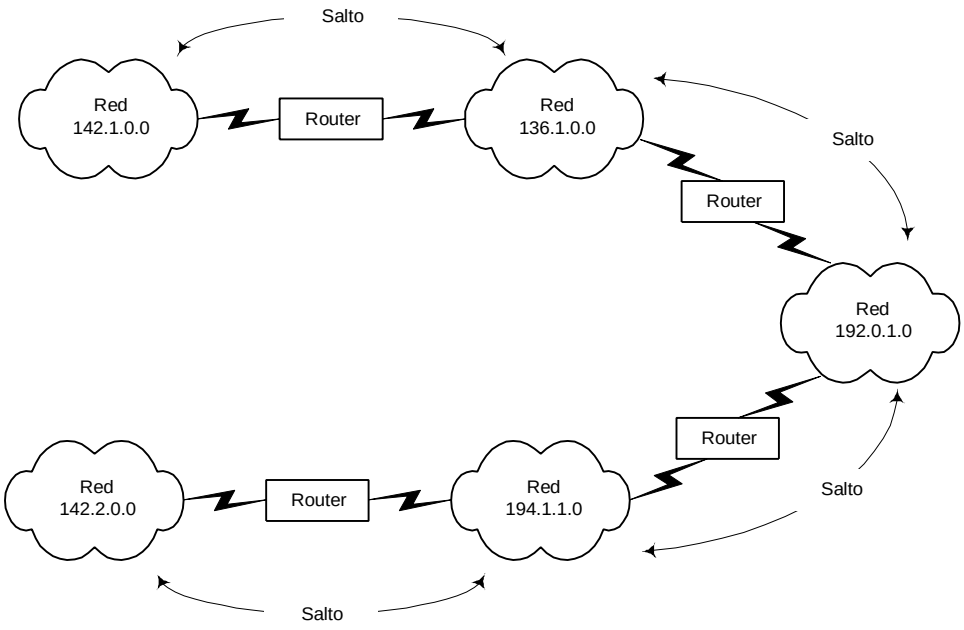

Figura 11.2

Consideremos una situación como la de la figura, con tres redes conectadas entre su mediante dos “routers” A y B. Después de un cierto tiempo, los “routers” habrán visto las notificaciones del otro y habrán alcanzado un estado estable en su visión de las redes del sistema.

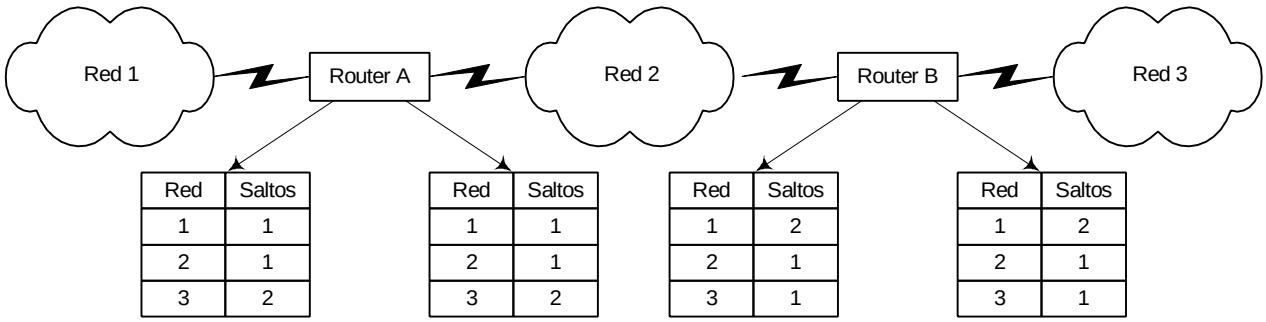

Figura 11.3

Consideremos lo que ocurriría si la red 3 fallara. El “router” B lo detectaría de inmediato, pero supongamos que la primera notificación a enviar correspondiera al “router” A, que enviaría su tabla como se ve en la figura indicando que conoce una ruta para alcanzar la red 3 en dos saltos.

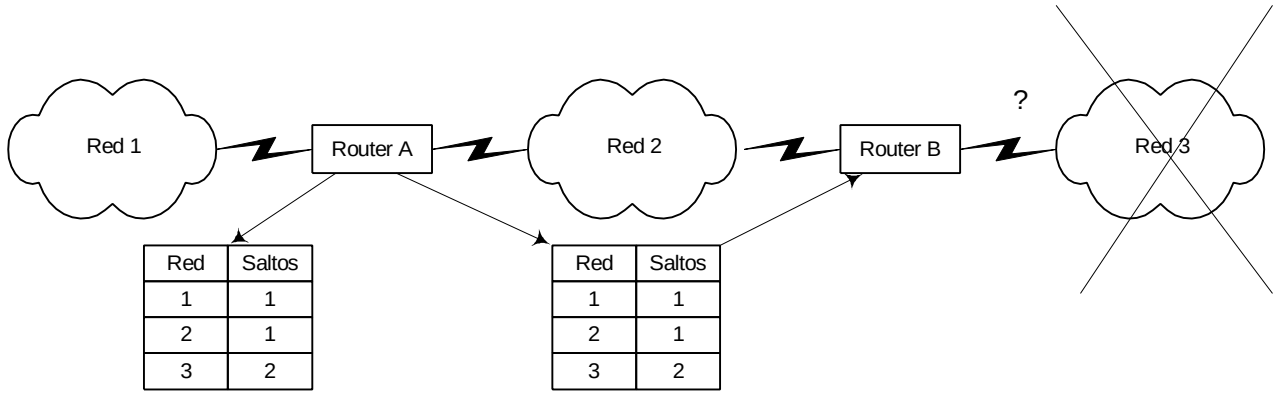

Figura 11.4

B aceptaría la notificación de A y establecería en su tabla de encaminamiento una nueva forma de alcanzar la red 3 a través del “router” A en tres saltos, lo que incluirá en su próxima notificación.

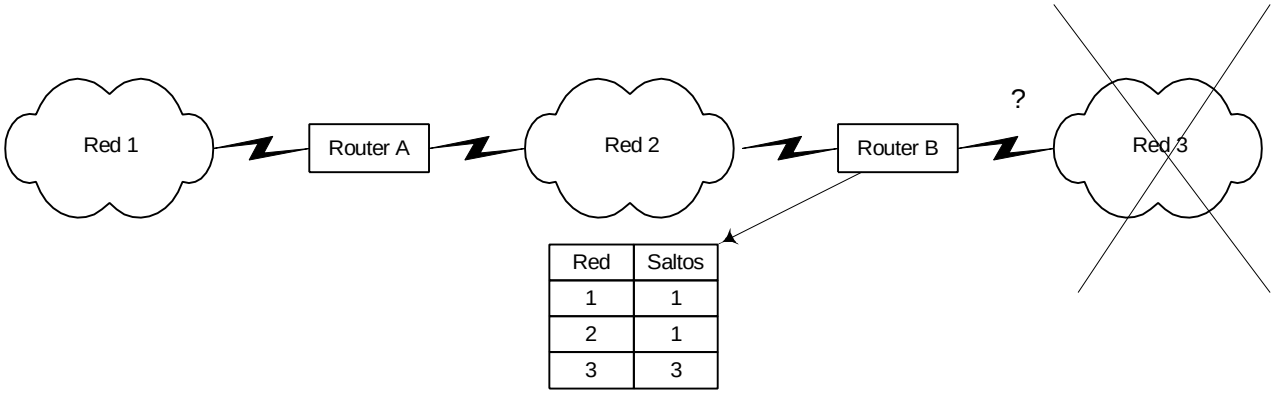

Figura 11.5

Cuando A reciba ésta actualizará su tabla de encaminamiento al apreciar que el costo de la ruta desde B a la red 3 ha empeorado y ahora vale 3, por lo que modificará su tabla indicando que el nuevo costo de la ruta es 4.

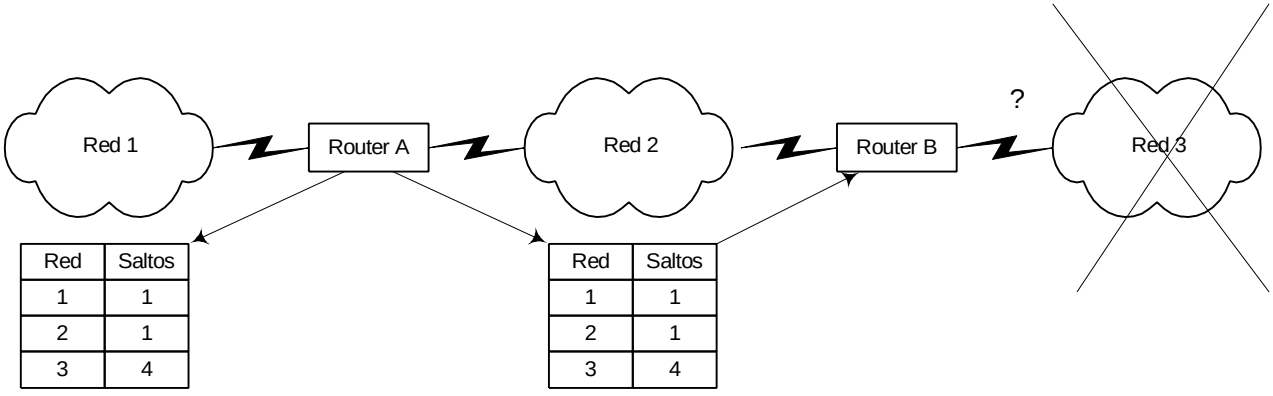

Figura 11.6

Esta sucesión de notificaciones terminará cuando el costo de la ruta alcance el valor 16, momento en que se entenderá que todas las rutas hacia la red 3 han fallado. Las notificaciones RIP se envían cada 30 segundos y por lo tanto el proceso anterior puede necesitar unos siete minutos, lo que es el tiempo de convergencia de RIP. De hecho, la limitación a 16 hace que el problema de la “cuenta hasta infinito” quede parcialmente solucionado, acelerando la convergencia.

En un intento por mejorar el tiempo de convergencia de RIP se han desarrollado una serie de mejoras a éste, que son los procedimientos denominados “**Split Horizon**”, “**Reverse Poison**” y “**Triggered Updates**”.

Split Horizon reduce el número de redes notificadas y por lo tanto el tráfico de encaminamiento así como el tiempo de convergencia impidiendo a los “routers” enviar notificaciones de una ruta por el mismo interfaz el que “aprendieron” dicha ruta. Como se ve en la figura, la red 3 sólo transporta notificaciones referentes a las redes 1 y 3; en caso de un fallo en la red 3, el “router” B nunca vería una notificación de A respecto de dicha red. Sin embargo, todavía es necesario un tiempo importante para que A aprecie que no recibe notificaciones respecto de la red 3 y considere que el camino hacia dicha red ha fallado. Este procedimiento, por lo tanto, reduce la posibilidad de bucles circulares, pero la convergencia es todavía lenta. Además, y como puede comprobarse, con este procedimiento pueden evitarse bucles en los que haya dos routers involucrados, pero falla cuando son más de dos.

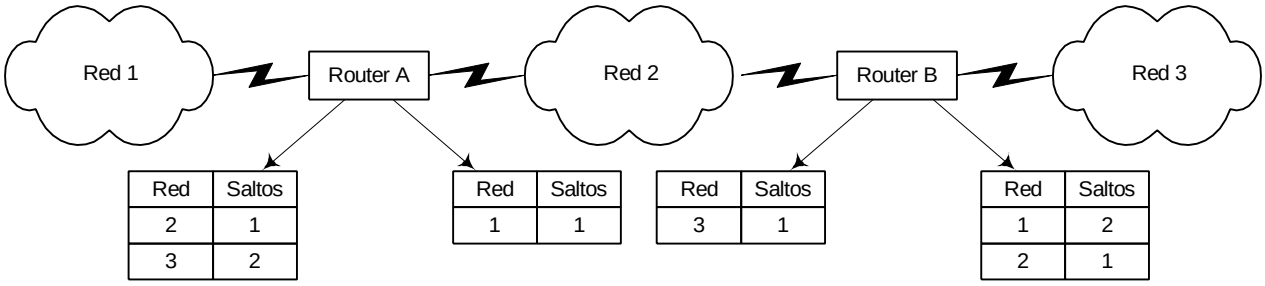

Figura 11.7

Reverse Poison es una técnica que se utiliza combinada con Split Horizon, para mejorar la convergencia. Con esta técnica, se notifican las rutas por el interfaz por el que se aprendieron, pero siempre con el valor de cuenta de saltos puesto a 16, indicando que el camino no es utilizable. En caso de que la red 3 fallara, el “router” B recibiría una notificación de A respecto de dicha red, pero con un costo 16 y por lo tanto la ignoraría. De nuevo este procedimiento reduce la posibilidad de bucles de encaminamiento, pero el problema de la lentitud de la convergencia persiste.

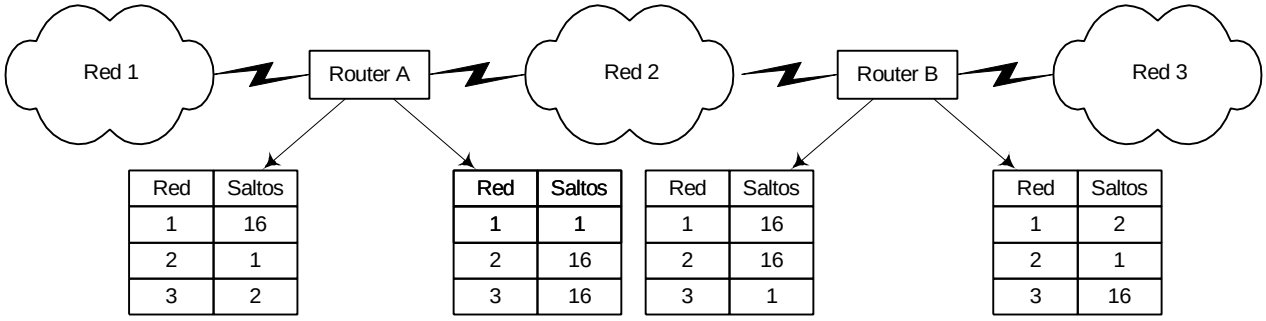

Figura 11.8

Triggered Updates constituye una mejora significativa de la velocidad de convergencia de RIP. Con esta técnica, los “routers” pueden enviar notificaciones indicando que el costo para alcanzar una red es 16 tan pronto como detecten el problema, en vez de tener que esperar el tiempo normal de notificación. Si todos los “routers” hacen esto, la convergencia se acelera, pero a expensas de un aumento del tráfico de difusión de la red cuando se detecta un fallo, lo cual puede suponer un problema grave en las redes grandes.

11.3.2.- Formato de RIP

El formato de los datagramas RIP es el indicado en la figura

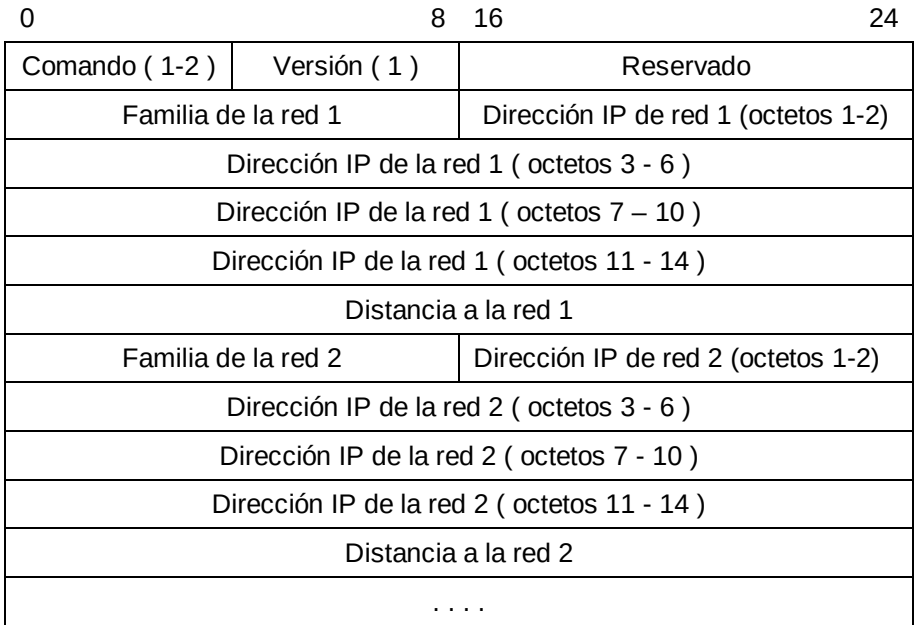

Figura 11.9

Comando puede tomar los valores 1 indicando una petición de información de encaminamiento y 2 indicando una respuesta. Los “routers” difunden información de encaminamiento no solicitadas cada 30 segundos.

V**ersión** puede ser 1 o 2 según la versión de RIP que se utilice.

El campo Familia **de direcciones** indica el tipo de protocolo de red utilizado, ya que RIP no está limitado a operar con IP. Para el protocolo IP toma el valor 2.

Dirección de red**.** Es un campo pensado para contener direcciones de red de diversos tipos y por lo tanto ocupa 112 bits, mucho más de lo que sería necesario para las direcciones IP, rellenándose el resto con ceros. En los sistemas TCP, los primeros 16 bits se dejan a cero de modo que la dirección IP se inserte dentro de los límites de 32 bits.

Distancia a la red es el número de saltos para alcanzar la red indicada.

Existe una limitación en el tamaño de los datagramas RIP fijada en 512 octetos. Si la notificación no cupiera en este tamaño, el “router” enviaría más notificaciones con el resto de la tabla de encaminamiento.

11.3.3.- RIP versión 2

La nueva versión de RIP fue diseñada pensando en la simplicidad, facilidad de manejo y baja sobrecarga de procesamiento, a la vez que en subsanar las principales deficiencias que aquejaban a RIP.

Los aspectos nuevos incluidos en RIPv2 son el soporte de máscaras de subred, “route tag”, dirección del siguiente salto, autenticación y multicasting. El formato de los mensajes es el indicado en la figura:

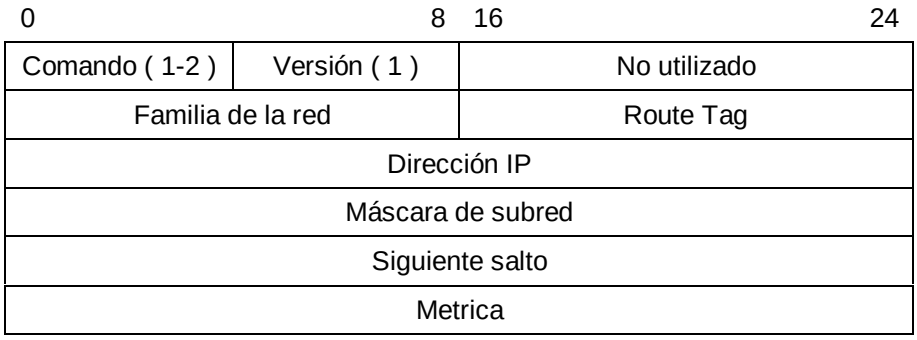

Figura 11.10

Los campos **Comando**, **Versión**, Familia de la red, **dirección IP** y **Métrica** mantienen la misma funcionalidad que en la versión anterior.

La inclusión de **máscara de subred** es la principal razón para actualizar el protocolo, al ser una necesidad para trabajar con múltiples subredes y CIDR.

Route Tag permite propagar información tal como números de sistemas autónomos, conseguidos desde protocolos EGP.

La dirección del **Siguiente salto** se utiliza en redes con varios protocolos IGP. permite a un “router” que opera con múltiples IGPs notificar la mejor ruta en lugar del router que debería hacerlo pero que no opera con RIP, para ello habrá tenido que aprender la ruta haciendo uso de otro protocolo de routing.

En RIPv2 la métrica está también limitada a 15 saltos para asegurar la compatibilidad con los “routers” que aún utilizan RIPv1.

La autenticación ha sido añadida para proteger frente a notificaciones de ruta no autorizadas. La especificación inicial sólo permite una clave de texto, pero en el futuro podrían emplearse otros mecanismos más sofisticados. Como no hay espacio suficiente en la cabecera, se utiliza una entrada de dirección completa para incluir la clave, indicándolo mediante una AFI de valor FFFF.

Otro de los problemas clave de RIPv1 es el número de broadcast que genera. RIPv2 puede emplear multicast para la actualización de las tablas, lo que libera a los nodos no involucrados en el encaminamiento. Esto también permite a los “routers” RIPv2 intercambiar información sin que la reciban los “routers” RIPv1, si bien cuando éstos están presentes las notificaciones se enviarán normalmente mediante difusiones.

11.4.- OSPF

La respuesta del IETF a los problemas de RIP fue OSPF (Open Shortest Path First), protocolo de routing basado en el estado del enlace. OSPF fue desarrollado entre 1988 y 1990, y en 1991 ya se había producido OSPF versión 2. OSPF esta basado en IS-IS y muchos de los conceptos que maneja estan basados en el. Es el protocolo actualmente recomendado por el IAB para sustituir a RIP. Su complejidad es notablemente superior, mientras que la descripción de RIP ocupa menos de 20 páginas la especificación de OSPF emplea más de 100.

Entre las características más notables de OSPF podemos destacar las siguientes:

- Es un algoritmo dinámico autoadaptativo, que reacciona a los cambios automática y rápidamente.
- Soporta una diversidad de parámetros para el cálculo de la métrica (distancia), tales como distancia física, retardo, etc.
- Soporta el parámetro *tipo de servicio* de la cabecera de datagrama IP; hasta la aparición de OSPF ningún protocolo de routing utilizaba este campo.
- Realiza balance de carga si existe más de una ruta con la misma distancia hacia un destino dado.
- Establece mecanismos de validación de los mensajes de routing, para evitar que un usuario malintencionado envíe mensajes engañosos a un router.
- Soporta rutas de red, de subred y de host.
- Se contempla la circunstancia en la que dos routers no tengan una línea directa entre ellos, por ejemplo cuando están conectados a través de un túnel.

OSPF permite un nivel adicional de jerarquía en el protocolo de routing, ya que prevé la división del sistema autónomo en áreas, de forma que un router sólo necesita conocer la topología e información de routing correspondiente a su área. En redes complejas esta es una característica muy valiosa.

Los algoritmos de routing se aplican dentro de cada área. En todo AS hay al menos un área, el área 0 denominada backbone. Un router puede pertenecer simultáneamente a dos o mas áreas, en cuyo caso debe disponer de la información de routing y ejecutar los cálculos correspondientes a todas ellas. Al menos un router de cada área debe estar además en el backbone, para conectar dicha área con el resto del AS. Dos áreas sólo pueden hablar entre sí a través del backbone.

En OSPF se contemplan cuatro clases de routers:

- Routers *backbone*; los que se encuentran en el área backbone.
- Routers *internos*; los que pertenecen únicamente a un área.
- Routers *periféricos de área*; son los que están en mas de un área, y por tanto las interconectan (una de las áreas siempre es necesariamente el backbone).
- Routers *periféricos de AS*; los que intercambian tráfico con routers de otros ASes. Estos routers pueden estar en el backbone o en cualquier otra área.

Existen tres tipos de rutas: intra-área, inter-área e inter-AS. Las rutas intra-área son determinadas directamente por cualquier router, pues dispone de toda la información; las rutas inter-área se resuelven en tres fases: primero ruta hacia el backbone, después ruta hacia el área de destino dentro del backbone, y por último ruta hacia el router deseado en el área de destino.

En OSPF, las notificaciones de rutas se denominan Notificaciones de Estado de Enlace (LSA). Contienen información sobre las direcciones de red conocidas y las máscaras de subred que se emplean con cada una. OSPF trabaja con subredes y máscaras de subredes de longitud variable.

OSPF está diseñado para trabajar tanto en redes punto a punto como múltiple acceso, bien de difusión (Ethernet o Token Ring) o de no-difusión (X.25).

11.4.1.- Formato de la tramas

La cabecera de las tramas OSPF es común a todos sus mensajes y tiene el siguiente formato:

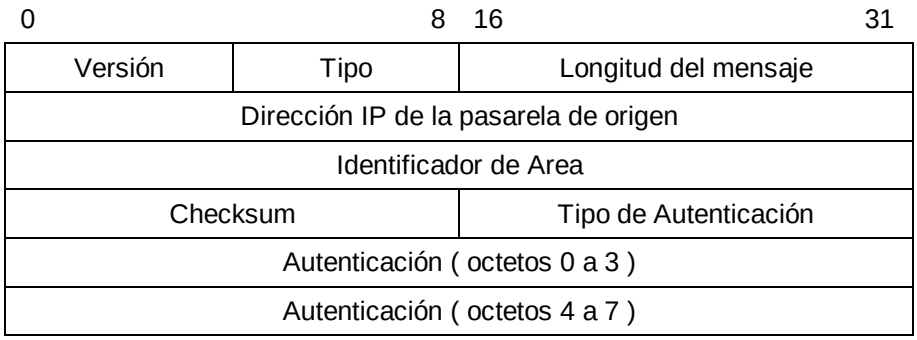

Figura 11.11

El campo tipo puede tomar los siguientes valores identificando el tipo de mensaje:

TIPO	SIGNIFICADO
1	HELLO
2	Descripción de la base de datos (topología)
3	Petición de estado de enlace
4	Actualización de estado de enlace
5	Reconocimiento de estado de enlace

Tabla 11.1

11.4.2.- Operación de OSPF

Cuando se inicializa un “router” OSPF envía en primer lugar un mensaje Hello por todos sus interfaces activos para establecer una conexión con sus vecinos.

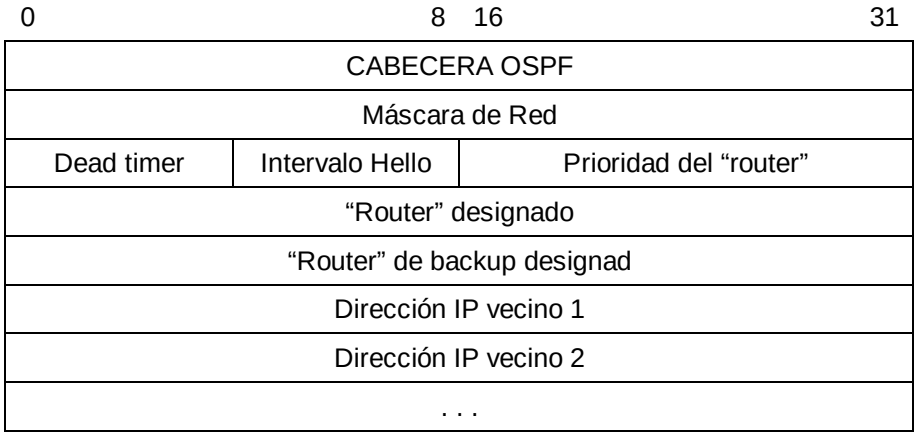

Figura 11.12

En redes de difusión, los “routers” utilizan la dirección multicast 224.0.0.5 reservada experimentalmente para este uso, mientras que en el resto de las redes es preciso configurar las direcciones de los vecinos en el “router”.

Estos mensajes sirven para elegir un “router” designado (RD), que será responsable de la notificación de rutas en representación de los demás “routers” de esa red. La existencia de un RD reduce el tráfico necesario para intercambiar la información entre “routers”. En una red local con *n* routers se producirían en principio $(n^2-n)/2$ intercambios de información diferentes, mientras que con el router designado se producirán solo *n-1* intercambios. También se elige un “router” designado alternativo para el caso de que falle el primero. Existe otra dirección multicast 224.0.0.6 reservada para los RDs y los de backup.

Una vez decidido el RD, se definen las adyacencias, es decir, se decide qué “routers” se comunicarán directamente entre sí. El camino entre dos “routers”, sea lógico o físico, es denominado una adyacencia. Esto es más claro en redes punto a punto y enlaces virtuales, pero en redes de difusión donde todos los “routers” pueden escucharse entre sí resulta más confuso. En esta situación, el DR es también el nodo que establece las adyacencias, en otras palabras, la línea de comunicaciones está limitada a los dos DRs y los otros “routers” y dos “routers” que no son DR nunca se comunican entre sí; esto permite pasar la información de encaminamiento mediante datagramas unicast en redes de no-difusión y mediante datagramas multicast en redes de difusión, reduciendo el tráfico de encaminamiento y su impacto sobre los nodos de la red.

La figura siguiente muestra dos redes multiacceso, una LAN y una X.25 donde es que todos los “routers” se comuniquen entre sí, pero para reducir el tráfico y simplificar el control del sistema el “router” 5 se convierte en DR y el “router” 6 en DR de backup en ambos casos.

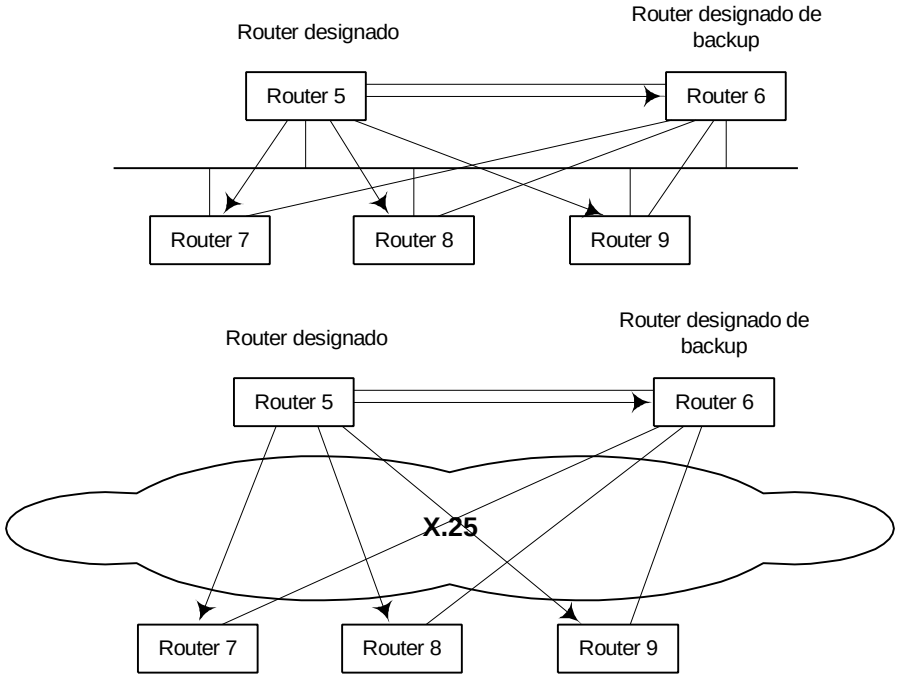

Figura 11.13

Las adyacencias se utilizan a continuación para pasar la información de la base de datos de encaminamiento a todos los “routers”. En OSPF, estas LSA, generadas por cada “router” indican el estado y el costo de sus interfaces y las adyacencias. Las LSA siempre circulan desde y hacia los DR, nunca directamente entre otros “routers”. Cada “router” en un área construirá su base de datos de encaminamiento a partir de la información proporcionada por los DR. Todos los “routers” en un área reciben las LSA y a partir de estas construyen una base de datos topológica de las interconexiones a través de su área. A partir de esta base de datos, y con ellos mismos como raíz, cada “router” construye un árbol indicando la conectividad con otras redes. A partir de los costos de

interfaz contenidos en las LSA, calcula el costo de viajar a cada rama del árbol. Cuando dos ramas proporcionan una conexión a la misma red, el camino de mayor costo no será utilizado, a menso que la ruta primaria falle. Se utilizará en primer lugar el camino más corto, y de ahí el nombre del protocolo.

El costo de cruzar cada interfaz debe ser decidido y fijado en los “routers” por el gestor del sistema. Esto proporciona al gestor control sobre las decisiones de encaminamiento dentro de la red y por lo tanto permite gestionar el flujo de tráfico en la red.

Consideremos con detalle la situación de la siguiente figura.

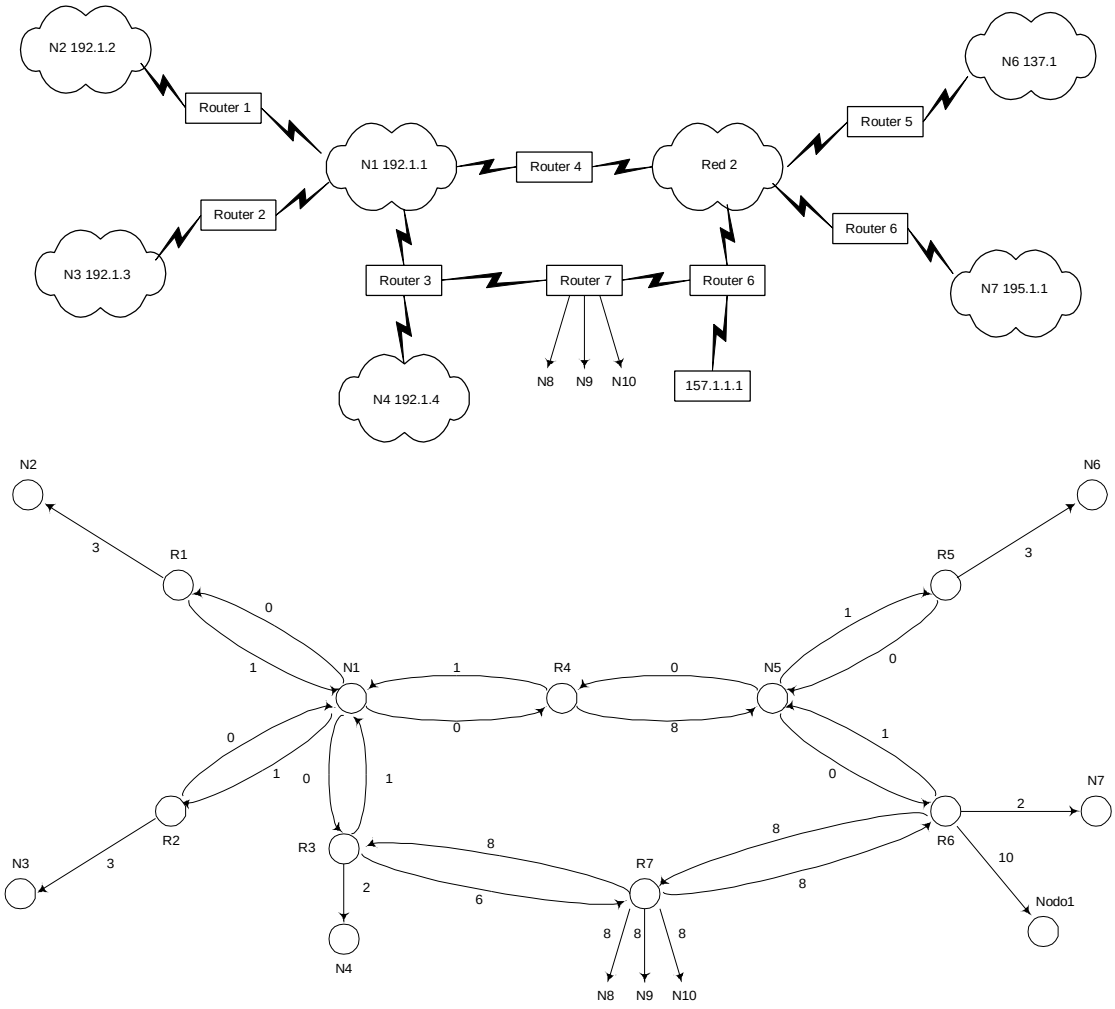

Figura 11.14

Las diez redes de este sistma (N1 a N10) utiizan varios sistemas de cableados con diferentes topologías y hay siete “routers” (R1-R7). Un nodo está conectado directamente al “router” R6 utilizando el protocolo SLIP. La ruta a este nodo directamente conectado es notificada en OSPF como una ruta específica a un nodo utiizando la dirección completa del mismo con una máscara de subred FFFFFFFF. En OSPF puede notificarse una ruta por defecto con una máscara de subred toda a cero.

Consideremos ahora el costo de los caminos que conectan los distintos “routers” y redes. Esto se conoce generalmente como grafo dirigido, y muestra los caminso entre cada entidad y el coste de atravesar dicho camino (el coste de ir desde una red al “router” es siempre 0).

A continuación dividimos la red en dos áreas con algunas redes externas al sistema autónomo conectadas a través del “router” R7. Como se muestra en la figura, R4 se convierte en un “router” inter-área y R7 en un “router” “backbone”, parte de la red “backbone”.

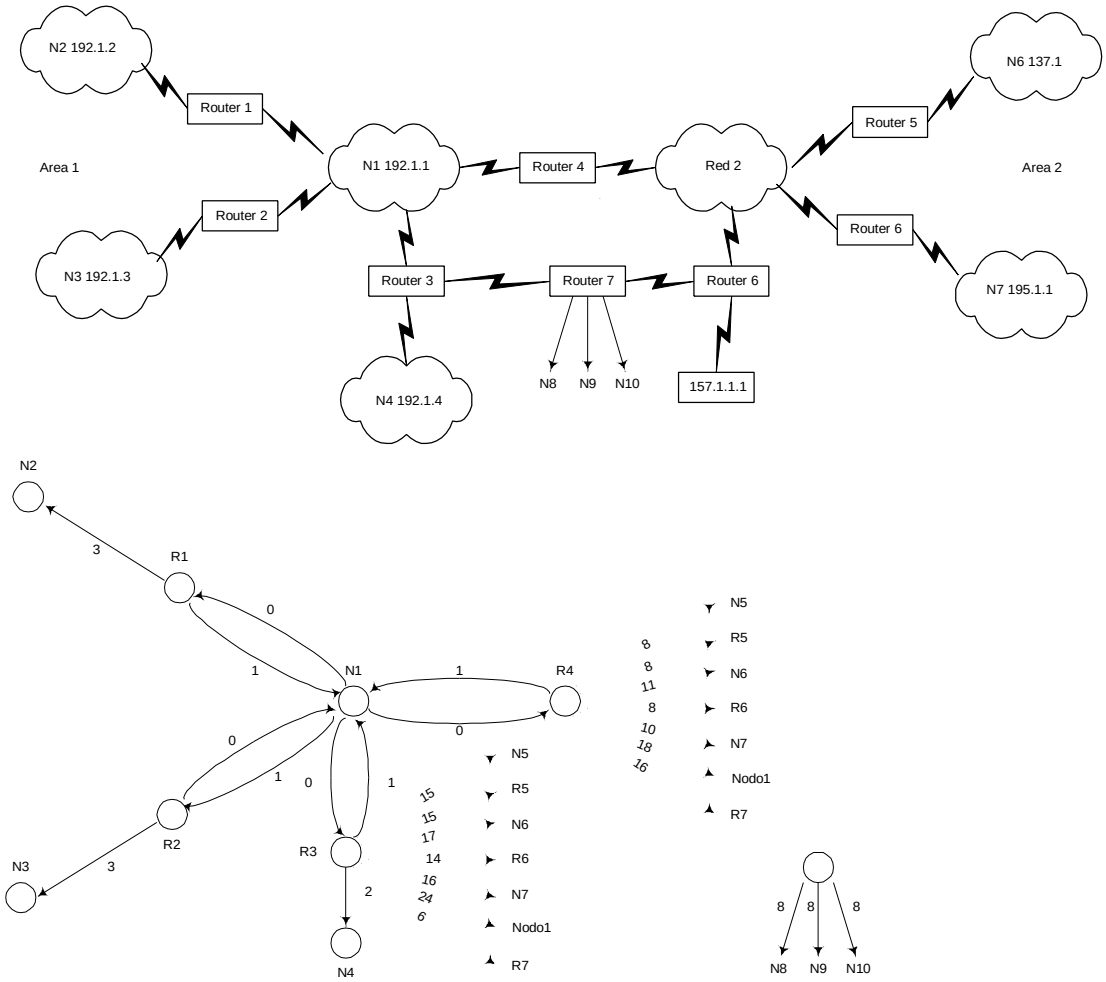

Figura 11.15

Si observamos la base de datos del área 1, podemos ver que el costo de alcanzar cada red. En este caso, vemos caminos duplicados a ciertos objetos, pero tienen costos diferentes. Si hubiera varios caminos del mismo costo, OSPF compartiría los datagramas entre ellos (un gran avance frente a otro protocolos de encaminamiento). Como se puede apreciar, R7 se muestra como parte separada de la base de datos, dado que no es parte del área 1. R4 tiene dos bases de datos, una para el área 1 y otra para el área 2.

11.4.3. Utilización de OSPF

La definición de OSPF describe los parámetros que necesitan ser configurados cuando se instala el sistema, además de la dirección IP y la máscara de subred:

- **Costo de cada interfaz.** Define el costo de enviar un datagrama por un interfaz, y es definido para cada puerto. Se eligen de forma arbitraria por el administrador del sistema con un rango entre 1 y 65535. El software del “router” elegirá costos por defecto inversamente proporcionales a la velocidad del interfaz. Puede haber costos distintos para cada TOS considerado por el “router”, determinando la ruta según el rendimiento, retraso, fiabilidad y costo económico, si bien la mayoría de los “routers” no lo soportan en la actualidad.

- **Intervalo de notificación**. Definido en segundos, es la frecuencia a la que se transmiten LSA por la red. Su valor debería ser mayor que el tiempo de retorno del interfaz al que se refiere; un valor típico para las redes locales es de 5 segundos.

- **Retraso de transferencia.** Es una estimación del tiempo (en segundos) que se necesita para enviar un mensaje de actualización de estado de enlace a través del interfaz; su valor habitual en una red local es de 1 segundo

- **Prioridad del "router".** Se utiliza para fijar qué "router" se convertirá en DR en redes de acceso múltiple; cuanto mayor sea el valor mayor será la probabilidad de convertirse en DR.

- **Intervalo de Hello.** Es la longitud en segundos entre datagramas Hello, y debería ser el mismo para todos los "routers" conectados a la misma red. Cuanto más pequeño sea este valor, más rápidamente se detectarán los fallos en la red, si bien a costa de aumentar el tráfico. En redes locales el valor recomendable es 10 segundos y 30 segundos en redes X.25.

- **Intervalo de "router dead".** Es el tiempo que debe pasar desde la última vez que se recibió un Hello de un "router" antes de considerar que ha fallado. Este valor debe ser también el mismo para todos los "routers" y del orden de cuatro veces el intervalo de Hello.

- Clave de autenticación. Es el valor utilizado para validar las actualizaciones de estado de enlace. En las implementaciones actuales es simplemente un texto.

Los "routers" OSPF necesitan una identificación única, que suele ser la menor de las direcciones IP de sus interfaces. También necesitan una identificación de área distinta de 0, valor este reservado para el "backbone". Cada "router" necesita igualmente una lista de todas las redes del área y de sus máscaras de red.

OSPF proporciona al gestor de red un control de las funciones de encaminamiento IP sin precedentes, habiendo eliminado todos los problemas que presentaba RIP:

- Soporta direccionamiento de subredes, y máscaras de subred de longitud variable.

- Permite asignar distintos métricas a caa enlace, de modo que puede tomar decisiones de encaminamiento en función del TOS SOLICITADO.

- No es preciso identificar los enlaces punto a punto entre "routers" con un número de red propio, conservando de este modo elespacio de direcciones IP.

- Divide las redes grandes en distintas áreas de gestión.

- No se pasan los detalles de encaminamiento de un área fuera de ella, lo que limita el tamaño y número de menajes de actualización.

- Utiliza multicasting en vez de broadcast para reducir la carga de los sistemas que no participan en el protocolo.

- Los intercambios entre "routers" se autentifican mediante una clave.

- Proporciona balanceo de carga, al poder distribuir el tráfico entre rutas alternativas del mismo costo hacia un mismo destino.

11.4.4.- Formato de los mensajes OSPF

A continuación se representa el formato de los mensajes utilizados en OSPF

MENSAJE DE DESCRIPCIÓN DE LA BASE DE DATOS

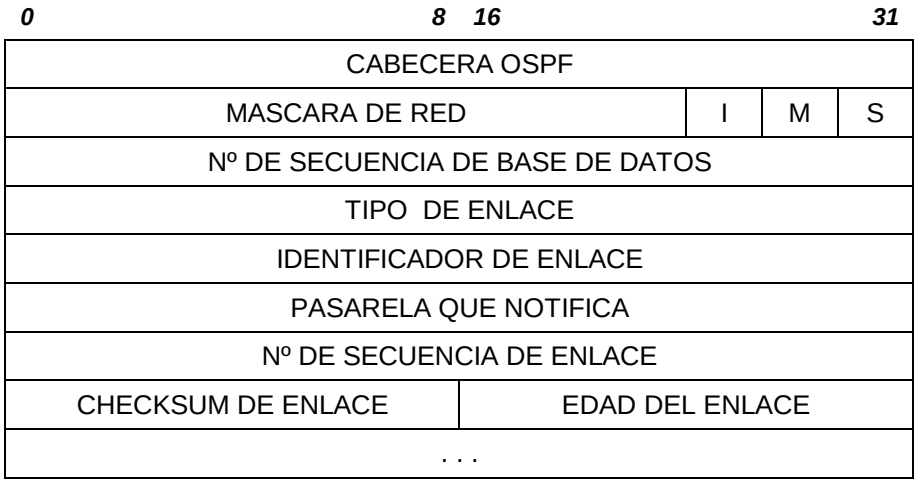

Figura 11.16

MENSAJE DE PETICIÓN DE ESTADO DE ENLACE

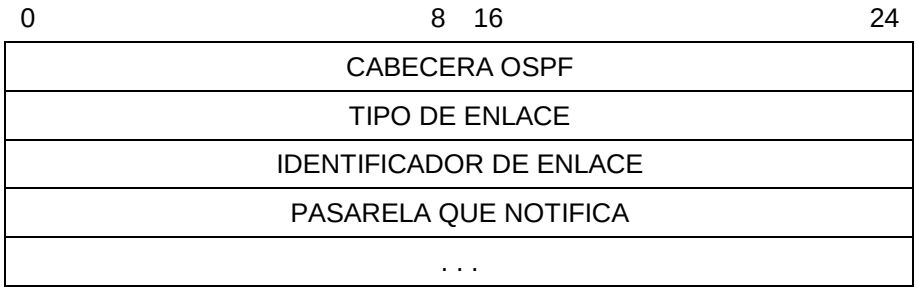

Figura 11.17

MENSAJE DE ACTUALIZACIÓN DE ESTADO DE ENLACE (LSA)

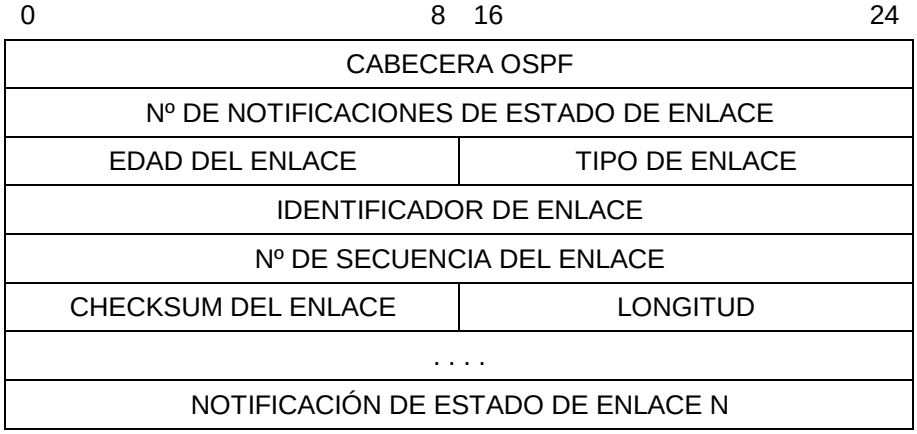

Figura 11.18

11.5.- OTROS PROTOCOLOS IGP

IGRP y EIGRP

A pesar de sus inconvenientes, el routing por vector distancia tiene algunos serios partidarios. Quizá el más importante sea la empresa Cisco, principal fabricante de routers del mundo. En 1988, cuando el único protocolo de routing ampliamente utilizado era RIP, Cisco optó por crear un protocolo de routing propio denominado IGRP (Internet Gateway Routing Protocol), basado también en el vector distancia, intentando resolver alguno de los problemas de RIP. Cisco ha seguido apostando por los protocolos de routing basados en el vector distancia y en 1993 produjo una nueva versión denominada EIGRP (Enhanced IGRP) que introducía mejoras importantes. Conviene destacar que tanto IGRP como EIGRP son protocolos propietarios, y no hay implementaciones para equipos de otros fabricantes, por lo que el uso de estos protocolos requiere que todos los routers del sistema autónomo correspondiente sean de Cisco. Los routers Cisco también pueden funcionar con protocolos estándar, tales como RIP y OSPF.

IS-IS

En este contexto, un IS es un “router” y IS-IS es un protocolo de routing entre sistemas intermedios estandarizado por los comités OSI como IS10589 para su utilización entre “routers” con el Protocolo OSI de Red no orientado a la conexión (OSI CLNP).

Fue desarrollado paralelamente a OSPF y comparte muchas de las cualidades de aquel. El marco de encaminamiento en que se fundamente se divide en una jerarquía de cuatro niveles de los cuales IS-IS forma el nivel más bajo, equivalente a un IGP. DEC incorporó OSI CLNP, junto con IP como los protocolos principales de DECNET phase V y ha tenido una participación significativa en el desarrollo y promoción de los protocolos IS-IS que finalmente fueron recogidos en el RFC 1195 como Integrated IS-IS, una modificación del OSI IS-IS original que permite a los “routers” interpretar y encaminar bien datagramas OSI CLNP o IP o ambos simultáneamente. Al tratar conjuntamente ambos protocolos consigue un significativo ahorro en memoria, procesamiento y capacidad de red para el almacenamiento y actualización de las tablas de encaminamiento.

Soporta direcciones de subred IP, máscaras de longitud variable, encaminamiento por TOS, autenticación de actualizaciones. Al igual que OSPF permite dividir la red en dos niveles cuyos detalles de encaminamiento se ocultan entre ellos. El segundo corresponde al “backbone” que puede tener varias áreas de nivel 1.

Aunque similar en prestaciones a OSPF, el apoyo que la IAB ha concedido a este último y el desarrollo de IPv6 en vez de adoptar CLNP hacen que en el futuro IS-IS no sea un protocolo de routing habitual en los entornos TCP/IP.

11.6.- PROTOCOLO DE ROUTING EXTERNO (EGP)

El encaminamiento entre sistemas autónomos (ASes), más que resolver el problema de encontrar la ruta óptima en cada caso, debe atender criterios externos que obedezcan a razones de tipo político, económico, administrativo, etc. Recordemos que se trata de decidir el routing entre redes que pertenecen a organizaciones diferentes (empresas, operadores o países). Por este motivo entre ASes se utilizan otro tipo de protocolos de routing.

BGP

Hasta 1990 se utilizaba como protocolo de routing externo en la Internet EGP (Exterior Gateway Protocol), diseñado entre 1982 y 1984. Como es normal, un protocolo diseñado en esa época no fue capaz de soportar la enorme evolución que sufrió la red durante esos años, y como ya era habitual el IETF abordó la tarea de desarrollar un nuevo protocolo de routing externo, denominado BGP (Border Gateway Protocol). La primera especificación de BGP apareció en 1989; desde entonces el IETF ha producido cuatro versiones de BGP; las especificaciones de BGP-4 se encuentran en el RFC-1654.

Los routers que utilizan el protocolo BGP (pertenecientes a diferentes ASes) forman entre ellos una red e intercambian información de routing para calcular las rutas óptimas; se utiliza el vector distancia, pero para evitar el problema de la cuenta a infinito la información intercambiada incluye, además de los routers accesibles y el costo, la ruta exacta utilizada en cada caso; así el router que recibe la información descarta inmediatamente las rutas que pasan por él mismo.

BGP permite introducir manualmente restricciones o reglas de tipo 'político'; éstas se traducen en que cualquier ruta que viola la regla recibe automáticamente una distancia de infinito.

Para simplificar la gestión de los ASes se crean Confederaciones de ASes; que se ve como un único AS desde el exterior, con lo que en la práctica esto equivale a incluir un nivel adicional de routing.

11.7.- PUNTOS NEUTROS

Cuando dos ISPs están conectados a la Internet siempre es posible el intercambio de información entre ellos. Sin embargo esto no siempre ocurre por el camino óptimo. Por ejemplo, si en España dos ISPs contratan conectividad Internet, uno a Telefónica y el otro a British Telecom (BT), su intercambio de tráfico puede llevarse a cabo en Washington, lo cual no es óptimo. La solución a este problema sería la realización de un acuerdo bilateral entre los dos proveedores (Telefónica y BT), de forma que se establezca un enlace directo entre los sistemas autónomos de ambos a través del cual puedan intercambiar tráfico los dos ISPs. Sin embargo, si el número de proveedores aumenta la cantidad de acuerdos bilaterales que hay que realizar crece rápidamente, concretamente para *n* proveedores sería $(n^2-n)/2$. Para simplificar este problema se suelen crear los denominados puntos neutros de interconexión. Un punto neutro consiste simplemente en un nodo normalmente gestionado por una entidad independiente para garantizar su 'neutralidad', al cual se conectan los routers de cada uno de los proveedores que desean participar.

En España el punto neutro de interconexión, denominado ESPANIX, entró en funcionamiento en febrero de 1997 en el Centro de Proceso de Datos de Banesto, en Madrid. Por su cometido solo los proveedores con conectividad internacional propia pueden conectarse al punto neutro. Actualmente (agosto de 2000) se conectan al punto neutro español los siguientes proveedores:

Airtel (en proceso)
BT Telecomunicaciones, S.A.
Cable & Wireless
Colt
Comunitel
EUnet-GOYA
Fujitsu-ICL Medusa
GLOBAL ONE
IBM Global Services
IPFnet
Jazztel (en proceso)
Retevision
Sarenet
Telefónica Transmisión de Datos
Unisource
Wisper

La implementación del punto neutro español es muy sencilla. Se trata simplemente de un conmutador LAN en el que a cada operador se le asigna una LAN en la cual puede conectar sus routers. Cada operador conecta su red con el punto neutro de la manera que considera mas adecuada, y sufraga el costo correspondiente. Los routers de diferentes operadores intercambian información de routing mediante BGP.

Existen puntos neutros de interconexión en muchos países. Antes de existir el punto neutro español los operadores mencionados intercambiaban tráfico a través de puntos neutros de otros países. Los operadores que no tienen enlaces internacionales con Internet utilizan necesariamente los servicios de alguno de los operadores antes mencionados, por lo que no necesitan conectarse al punto neutro ya que su proveedor de servicio ya se ocupa de intercambiar su tráfico con los demás operadores.

11.- PROTOCOLOS DE ROUTING DE INTERNET 1
11.1.- PROTOCOLOS DE ROUTING DE INTERNET 1
11.2.- PROTOCOLOS DE ROUTING INTERNO (IGP) 3
11.3.- RIP y RIPv2 3
11.3.1.- Funcionamiento de RIP 3
11.3.2.- Formato de RIP 7
11.3.3.- RIP versión 2 7
11.4.- OSPF 9
11.4.1.- Formato de la tramas 10
11.4.2.- Operación de OSPF 10
11.4.3. Utilización de OSPF 13
11.4.4.- Formato de los mensajes OSPF 15
11.5.- OTROS PROTOCOLOS IGP 16
11.6.- PROTOCOLO DE ROUTING EXTERNO (EGP) 16
BGP 16
11.7.- PUNTOS NEUTROS 17