RIP (Routing information Protocol) Análisis y simulación

Alemany Eric David – Gigena, Cesar Esteban – Ing. Giovanardi Ezequiel
Facultad de Ingeniería
Instituto Universitario Aeronáutico
Av. Fuerza Aérea 6500, Córdoba, Argentina

Resumen - ***RIP [1] fue uno de los primeros protocolos de ruteo y uno de las más usados. El propósito de este trabajo es dar un análisis del protocolo en cuanto a funcionamiento,virtudes y también defectos.***

Aún hoy en día, RIP en su versión 2 [2][3][4][7] es muy usado en redes donde necesita aplicarse un mecanismo de ruteo dinámico y en donde, en muchos casos, no justifica el uso (y a veces pago) de un mecanismo más complejo.

El contenido del trabajo esta dividido en el análisis del protocolo y su funcionamiento, formato de mensajes y heurística. Por último se plantea un escenario de simulación a través del software OPNET IT GURU[8][9] versión académica. En el mismo se plantea un fallo en un enlace para observar como el protocolo debe re-acomodarse al cambio.

Palabras Claves – ***Redes, Paquetes, Protocolo, Router, RIP, Request, Response.***

I. INTRODUCCIÓN

El protocolo RIP surgió como un método para el cálculo de enrutamiento en redes.

En un principio, se preveía que las redes (sobre todo las de gran tamaño) estarían compuestas de un conjunto de Sistemas Autónomos interconectados. Cada uno de estos Sistemas Autónomos sería administrado por una entidad y, por ello, cada uno tendría su propio método de enrutamiento. A un protocolo de enrutamiento de un Sistema Autónomo se lo denomina "Interior Router Protocol" IGP y al método que une los diferentes Sistemas Autónomos se lo conoce como "Exterior Router Protocol" EGP. RIP fue diseñado para que sea implementado dentro de un Sistema Autónomo, es decir como un protocolo IGP.

RIP usa un mecanismo de cálculo de rutas llamado algoritmo Vector-Distancia o Bellman-Ford. Consiste en el armado de una tabla con rutas hacia diferentes destinos, donde cada uno presenta un valor numeral (métrica) indicando el "costo" de utilizar esa ruta.

RIP está limitado a redes de una complejidad moderada y de tamaño mediano. Tiene un mecanismo para situaciones donde sea inestable llamado "conteo al infinito". Dependiendo que tan rápido resuelva el estado a través del conteo al infinito, definirá que tan eficiente y seguro es el protocolo en la red.

La versión 1 fue definida en la RFC 1058 y la versión 2 en la RFC 1388 que luego fue actualizada en la RFC 1723 y, finalmente, en el RFC 2453. Ésta fue la última actualización realizada respecto de la versión 2 del protocolo RIP.

RIP versión 2 no es un nuevo protocolo sino que es una extensión del protocolo de ruteo original.

Las modificaciones hechas respecto a RIP versión 2 MIB [5] y Método de Autenticación MD5 [6] son detalladas en otros documentos (RFCs 1724 y 2082 respectivamente).

La justificación de realizar una mejora al existente protocolo RIP fue que, aún cuando existen otros protocolos de IGP más robustos como OSPF e IS-IS[11], todavía contaba con algunas ventajas muy importantes tales como el pequeño exceso de cabecera de sus mensajes (lo cual no impacta en el uso de ancho de banda), fácil configuración y manejabilidad.

II. OPERACIÓN, PROCESAMIENTO ENTRADA/SALIDA Y CONTEO AL INFINITO

A. Operación

RIP está diseñado para permitir a Hosts y Routers el intercambio de información para los cómputos de las rutas a través de una red basada en IP.

El propósito del ruteo es encontrar la manera de mandar un paquete a un destino por la mejor ruta. El algoritmo Vector-Distancia [1][7] se basa en una tabla que proporciona la mejor ruta para cada destino en el sistema. En orden de definir cual ruta es la mejor, se debe tener una manera de medir cual es la mejor. Esto es referido a las "métricas" donde la métrica de una red está integrada entre 1 y 15 inclusive.

Cada Router que implementa RIP debe tener una tabla de ruteo. Esta tabla tiene una entrada a cada destino que alcance. Cada entrada tiene:

1. La dirección IP del destino.
2. Una métrica, que representa el costo total de pasar un paquete desde el host hasta el destino.
3. La dirección de IP del siguiente Router a través del destino.
4. Una "Bandera de cambio de ruta" que indique la información si hubo algún cambio reciente en la ruta para llegar a destino.
5. Contadores asociados a la ruta.

En versión 2 se añade la máscara de subred del destino [7]. RIP cuenta con unos contadores para limitar cada

cuanto tiempo se deben anunciar las rutas conocidas o cuánto tiempo deben permanecer las entradas de ruteo en la tabla.

Cada 30 segundos, el proceso de salida es invocado para generar un mensaje Response con la tabla de ruteo completa hacia todos los vecinos del Router.

Respecto de las rutas existen tres contadores asociados como el "tiempo de vida" (lifetime-180 segundos), el "tiempo de recolección de basura" (garbage collector-120 segundos) y "tiempo de espera" (holddown-130 segundos). El tiempo de vida de una ruta se renueva cada vez que llega una actualización de esa ruta. Al final de este tiempo, la ruta se marca como inválida y empieza el tiempo de recolección de basura donde al final de este la ruta es eliminada por completo. El tiempo de espera dicta que si una ruta es anunciada como inválida y en el siguiente anuncio es válida, el router espera un tiempo en donde las actualizaciones que lleguen deben decir que efectivamente es válida antes de cambiar el estado.

La manera de marcar cuando una ruta no debe ser tenida en cuenta es a través de la métrica. Aprovechando que el límite máximo de una red que use RIP como protocolo de ruteo es de 15 saltos, una ruta que ya no es viable se pone a 16. Este valor simboliza que es inalcanzable y se dice que tiene métrica de "infinito".

B. Procesamiento Entrada / Salida

En el proceso de entrada, el primer chequeo que se hace a un mensaje RIP es al campo Versión para evaluar si debe ser descartado o no.

Los mensajes que contengan como valor de campo igual a 1 serán procesados, si todos los campos que están definidos como "Deben ser Cero" (MBZ), no contienen otro tipo de información que no sea cero.

Paquetes que contengan un valor mayor a 1 serán procesados. En este caso, el contenido de los campos "Deben ser Cero" serán ignorados.

El procesamiento dependerá del tipo de mensaje: Request o Response.

- ✓ Request

Este tipo de mensajes es usado para exigir un respuesta (Response) que contenga toda o parte de la tabla de ruteo de otro router. Los Requests son enviados como Broadcasts (o Multicast), desde el puerto UDP 520. En el caso de mandar un Request a un Router en particular (no se usa Broadcast) debe usarse otro número de puerto UDP como puerto origen. El puerto destino SIEMPRE tiene que ser UDP 520.

Un mensaje de Request es procesado entrada por entrada. Si solo contiene una entrada donde el campo "Identificador de Familia de Dirección" (Family Address Identifier) es igual a 0 y tiene una métrica de infinito, este es un mensaje para que se envié la tabla de ruteo entera. Si por el contrario contiene varias entradas, el proceso se hará uno por uno revisando el destino en la tabla de ruteo. Si la ruta no existe, se marca la misma con el valor de infinito. Por el contrario, si existe la ruta, se completa con la métrica que tiene en la tabla de ruteo local.

Una vez que se procesa todo el mensaje, se cambia el comando a Response y se envía de regreso al puerto de donde vino.

- ✓ Response

Un mensaje de Response puede ser recibido por diferentes razones tales como:

1. Responder por una búsqueda específica.
2. Actualizaciones regulares.
3. Actualizaciones Activadas generadas por un cambio de métrica.

El procesamiento es la misma sin importar cómo se hayan generado.

Existe una serie de chequeos[1] para validar el mensaje puesto que pueden cambiar la tabla de ruteo local. Por ello se debe chequear que el puerto origen solamente sea UDP 520, que la dirección de origen viene de un vecino válido o si no pertenece a una de las interfaces propias del router.

Luego de que se valida el mensaje, se procede a procesar el mensaje entrada por entrada. Aquellas entradas que contengan un valor más grande que infinito serán descartadas y se pasará a la siguiente. Luego se observa la dirección de destino y el Identificador de Familia de Direcciones el cual debe contener un valor válido (2 para IP), caso contrario se descarta la entrada y se pasa a la siguiente. Seguido de esto se chequea la dirección donde se ignorarán aquellas entradas que sean de clase D o E si están en la red 0 (a excepción de 0.0.0.0) o de red 127 (loopback).

Una vez chequeado esto, se actualiza la métrica añadiendo el costo de la red por donde el mensaje ha llegado. Si la cuenta da 16 o más, se ignora la entrada y se sigue con otra. Con este valor en mano, se fija en la tabla de ruteo local para ver si existe una ruta hacia el destino. Si no existe, la entrada se añade a la tabla de ruteo local. Si existiese la entrada se compara la dirección del router por donde vino. Si es el mismo, pero la métrica calculada es menor, entonces se actualiza la ruta con la nueva métrica y se reinicia el tiempo de vida. Si por el contrario es igual a la métrica existente, no se cambia el valor pero si se resetea el contador puesto que la ruta todavía es válida. Si no es el mismo router por donde se aprendió previamente y la métrica es mejor, se actualiza la entrada. Si no, no se descarta puesto que ya existe una ruta igualmente valida.

El proceso de salida es activado:

- ✓ Por proceso de entrada, cuando un Request es recibido (este Response es unicast al que mando el Request)
- ✓ Por actualizaciones regulares de ruteo (broadcast/multicast cada 30 segundos)
- ✓ Por actualizaciones activadas (broadcast/multicast cuando una ruta cambia).

Un Response es preparado para cada red directamente conectada, y enviado a la dirección apropiada. Para los mensajes RESPONSE generados, existe un límite máximo de 25 Entradas de Rutas en el mensaje. Si hay más, iniciar otro RESPONSE.

C. *Conteo al Infinito: Horizonte dividido y Actualizaciones Activadas*

RIP aplica dos métodos para resolver el conteo al infinito: "Horizonte Dividido" (Split Horizon) u "Horizonte Dividido con Camino de Regreso Envenenado" (Split Horizon with Poison Reverse) y "Actualizaciones Activadas" (Triggered Updates).

Horizonte Dividido [1][7] no anuncia a los Routers las rutas que aprendió por ellos mismos. Tiene la ventaja que los mensajes no contienen toda la tabla de ruteo por lo que son más livianos. Esto es relevante en redes de gran tamaño cercano al límite del protocolo. Como desventaja, las rutas siguen en el sistema hasta ser eliminadas por un contador de tiempo de vida.

Horizonte Dividido con Camino de Regreso Envenenado [1][7] es más seguro que solo Horizonte Dividido. Consiste en anunciar las rutas a los routers por donde se aprendieron pero devolviéndolas con una métrica de infinito (16). De esta manera, el Router recibe la ruta y automáticamente la descarta. Este método es capaz de terminar con un loop de manera casi inmediata. Como contrapartida, se envía toda la tabla de ruteo en los anuncios (incluyendo las rutas no válidas) por lo que los mensajes son más grandes y necesitan realizar un procesamiento mayor que con Horizonte Dividido solamente.

El método de Horizonte Divido con Camino de Regreso Envenenado fue implementado para resolver situaciones donde dos routers creaban un loop. Si fuesen tres los routers envueltos en un loop, entonces este método no serviría y la única manera de alcanzar la estabilidad es esperar que las rutas involucradas sean declaradas inalcanzables.

Para ello se adopto un método llamado Actualizaciones Activadas [1][7]. Este método ayuda a alcanzar la estabilidad de la red más rápido a través de mensajes diciendo si un destino no es alcanzable al instante en que se detecta que no lo es (en vez de esperar a los anuncios regulares).

Estos mensajes son activados cuando se detecta un cambio de métrica y se envía aún si todavía no es tiempo de mandar un anuncio regular.

Estos mensajes pueden generar una carga excesiva en redes de capacidad limitada o con muchos routers. Por lo que se debe limitar la frecuencia con el que se mandan estos mensajes. Por ello, se activa un contador con un intervalo aleatorio de entre 1 y 5 segundos dentro del cual no puede enviarse otro mensaje de actualizaciones activadas.

III. FORMATO DE LOS MENSAJES

El protocolo RIP es un protocolo basado en UDP. Cada host que usa RIP tiene un proceso de ruteo que manda y recibe paquetes por el puerto UDP 520. Todas las comunicaciones direccionadas a otros procesos de RIP son enviados también a través del puerto 520. Las actualizaciones no solicitadas de mensajes de ruteo tienen la misma fuente y destino, para ambos casos utiliza el puerto 520. Los mensajes que son enviados en respuesta a pedidos específicos son enviados al puerto del cual vino el pedido.

El tamaño máximo del paquete es de 512 octetos e incluye solo la porción del cuerpo del mensaje. No se cuenta las cabeceras de IP o de UDP.

A. *Capturas en Red de Mensajes RIP v2*

A continuación se muestran dos capturas hechas en una red real de dos mensajes RIPv2 Request y Response [11].

Request

Este mensaje presenta en la figura 1, tiene la particularidad de tener una sola entrada de red nula con métrica infinita. Este mensaje es enviado cuando un servidor RIP necesita que le envíen la tabla de ruteo completa del vecino que este escuchando.

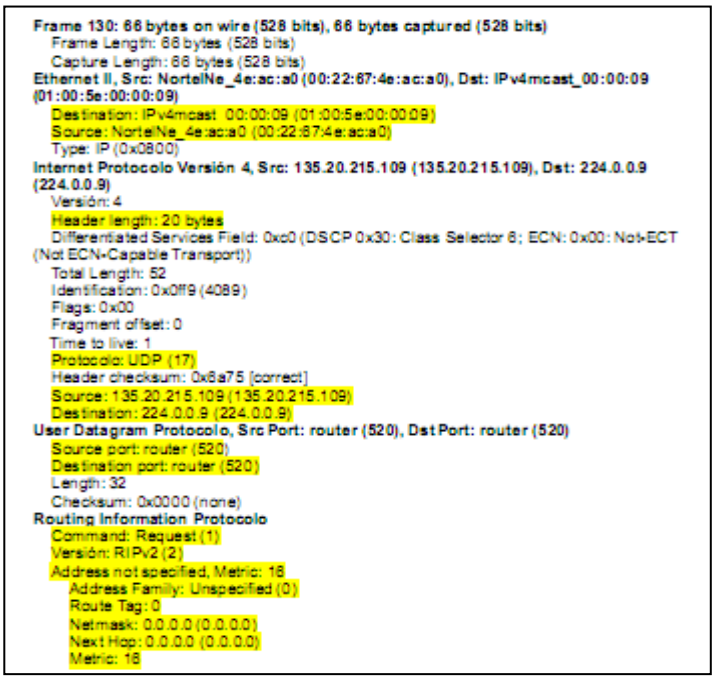

Figura 1

Response

Este mensaje que se presenta en la Figura 2, es un mensaje de anuncio clásico donde contiene las entradas de rutas locales. Tiene la particularidad de que utilice el mecanismo de Autenticación por Contraseña. Como se puede ver, la clave viaja en texto claro.

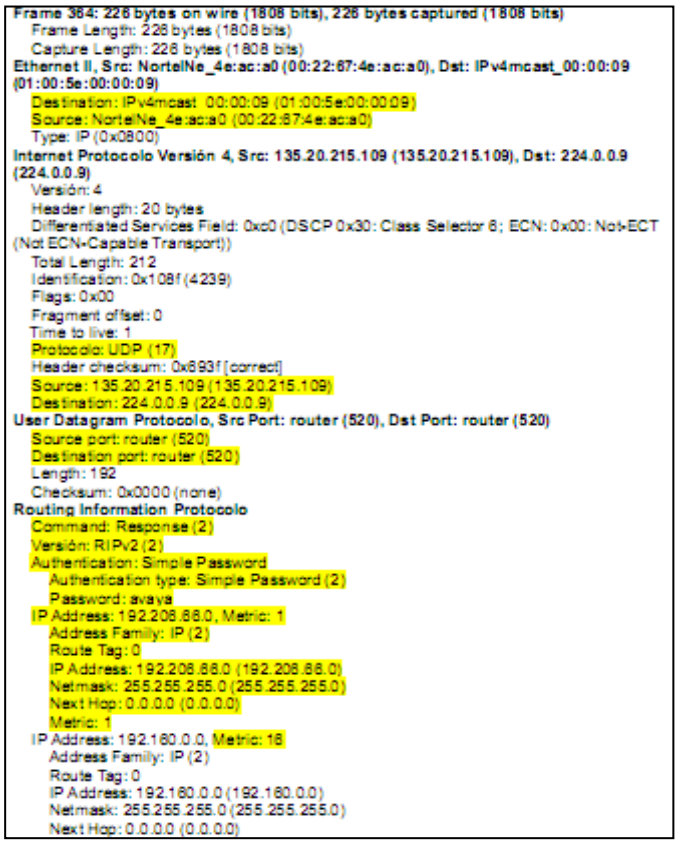

Figura 2

B. Formato RIP v1

En la figura 3 vemos el campo de "Identificador de Dirección de Familia" hasta el campo "Métrica" puede aparecer hasta 25 veces. Esto significa que puede haber como máximo 25 entradas de rutas en un solo mensaje RIP[1].

0 1 2 3 4 5 6 7	8 9 0 0 1 2 3 4 5	6 7 8 9 0 0 1 2 3 4 5 6 7 8 9 0 1
Comando (1)	Versión (1)	Debe ser cero (0)
Identificador de dirección de familia (2)		Debe ser cero (0)
Dirección IP		
Debe ser cero (4)		
Debe ser cero (4)		
Métrica (4)		
.		
.		
.		

Tabla 1

C. Formato RIP v2

RIPv2 utiliza el mismo formato de paquete que RIP con la diferencia de los campos del cuerpo del mensaje (20 octetos). La cabecera sigue siendo la misma[7], como muestra la figura 4.

0 1 2 3 4 5 6 7	8 9 0 0 1 2 3 4 5	6 7 8 9 0 0 1 2 3 4 5 6 7 8 9 0 1
Comando (1)	Versión (1)	Debe ser cero (0)
Identificador de dirección de familia (2)		Etiquetado de Ruta (2)
Dirección IP		
Mascara de Subred (4)		
Próximo Salto (4)		
Métrica (4)		
.		
.		
.		

Tabla 2

D. Mensaje Autenticación por contraseña (RIPv2)

RIPv2 utiliza el espacio de una Entrada de Ruta. Para esto debe marcar el campo "Identificador de Campo de Familia" con un valor de *0xFFFF* de solamente la primera entrada como muestra la figura 5. Esto indica que el resto de esa entrada (16 octetos) se usarán para autenticación. Esto deja como máximo 24 Entradas de Rutas en el resto del mensaje.[7]

0 1 2 3 4 5 6 7	8 9 0 0 1 2 3 4 5	6 7 8 9 0 0 1 2 3 4 5 6 7 8 9 0 1
Comando (1)	Versión (1)	Debe ser cero (0)
0xFFFF		Tipo de autenticación (2)
Autenticación (16)		

Tabla 3

E. Mensaje Autenticación por MD5 (RIPv2)

Cuando MD5 es usado, la cabecera es conservada como estaba antes y el contenido también a excepción de los 16 octetos que componen el campo Authentication

Durante el cálculo de MD5, luego del campo "Datos de Autenticación" (Authentication Data), es seguida de un campo "Pad" y un campo "Length" como se define en RFC 1321 – Message Digest 5[6]. Se puede ver en la figura 6

0 1 2 3 4 5 6 7	8 9 0 0 1 2 3 4 5	6 7 8 9 0 0 1 2 3 4 5 6 7 8 9 0 1
Comando (1)	Versión (1)	Debe ser cero (0)
0xFFFF		Tipo de autenticación (2)
RIP 2 Tamaño del paquete		Key ID Long del dato de Autenticación
Numero de secuencia		
Debe ser cero (4)		
Debe ser cero (4)		

Tabla 4

IV. ESQUEMA DE ENVÍO DE MENSAJES RIP

En la figura 7 se muestran los mensajes que un servidor RIP encuentra a lo largo de su funcionamiento.

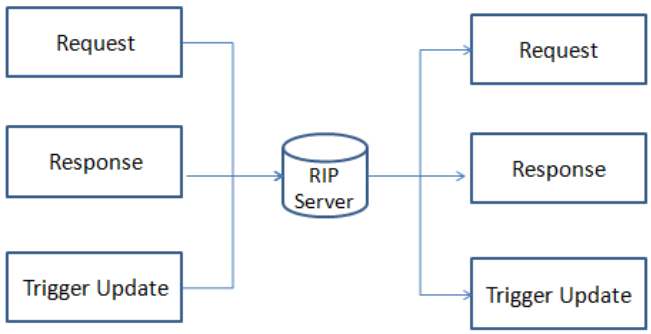

Figura 3

A continuación se explica cómo es el proceso de Request / Response / Trigger Update que sufre un servidor RIP.

El servidor RIP envía y recibe 3 tipos de mensajes, los cuales son procesados dependiendo del contenido.

Cuando un servidor RIP inicia manda dos tipos de mensajes, un Request y un Response:

- ✓ El Request contiene una sola entrada con el campo de identificador de familia de direcciones en 0 (cero) y en la métrica 16 (infinito), esto significa que solicita una tabla entera de ruteo al servidor RIP adyacente, este mensaje es enviado una sola vez cuando el servidor RIP inicia.
- ✓ El Response contiene la tabla entera de ruteo propia que normalmente solo contendrá las direcciones de

redes directamente conectadas, este mensaje es enviado cada 30 segundos.

El mensaje Trigger Update es enviado solamente cuando sucede un cambio de métrica y/o topología de la red y contiene solamente una parte parcial de la tabla de las rutas nuevas o que cambia dichas métricas, este mensaje es mandado como un Response cuando la red sufre un cambio anteriormente comentado. Entre cada mensaje de trigger Update existe un temporizador de espera de 1 a 5 segundos aleatorio.

Con el tiempo estable, el servidor RIP recibe 3 tipos distintos de mensajes, Request, Response y Trigger Update:

- ✓ El mensaje de Request recibido es debido a que un servidor RIP adyacente inicializa, le manda este mensaje para que responda con su tabla completa de ruteo con sus métricas.
- ✓ El mensaje Response es un anuncio periódico de las tablas de ruteo.
- ✓ El mensaje de Trigger Update es recibido solamente cuando sucede un cambio de métrica y/o topología de la red y contiene solamente una parte parcial de la tabla de las rutas nuevas o que cambia dichas métricas, con esta nueva métrica, el servidor RIP analiza en su tabla actual y cambia en el caso que sea una nueva ruta o si su métrica sea menor a la existente, en este caso el servidor RIP manda un mensaje de Trigger Update a sus Servidores adyacentes. Si la métrica es mayor o si ya tiene la ruta por un camino distinto y si la métrica es mayor ignora este Trigger Update.

La figura 8 simboliza la heurística que sigue RIP cuando recibe un mensaje Response (ya sea Triggered Update o un anuncio regular). Lo importante de destacar es que cualquier cambio en la entrada de ruta en la tabla local, el servidor RIP debe anunciar este cambio a los Routers vecinos.

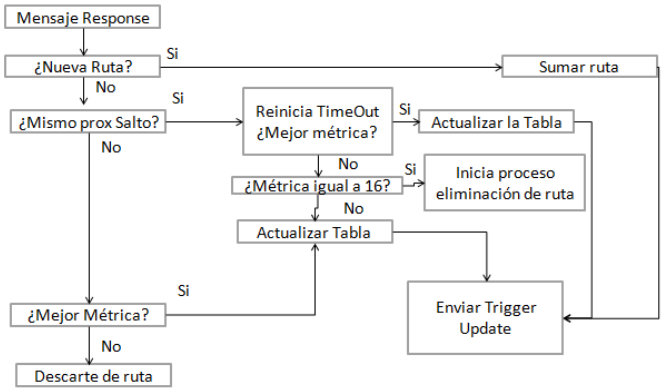

Figura 4

V. SIMULACIÓN DEL ESCENARIO BGP

A. Planteo del escenario

Las simulaciones [8][9] fueron hechas en un escenario donde se encuentran 4 routers interconectados donde cada uno de ellos está directamente conectado a un par de redes, como muestra la figura 9.

Para poder lograr ver de qué manera reacciona RIP ante un cambio, se dará de baja a un enlace entre dos routers a los 200 segundos de correrse la simulación. De esta manera deberíamos ver como los routers deben acomodarse para poder lograr la convergencia nuevamente.

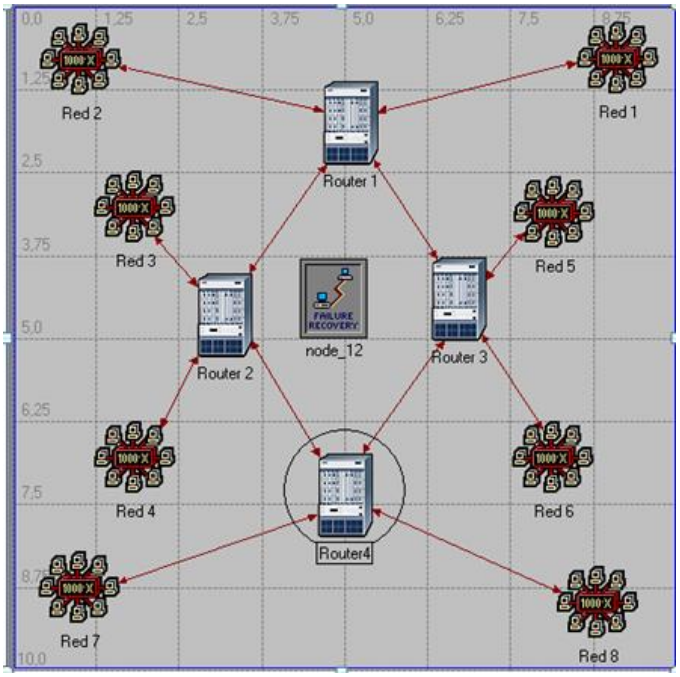

Figura 5

Vamos a establecer las diferencias en un sistema en donde el protocolo que corra será RIP v2 con Auto Summary habilitado, Broadcast/Multicast y que aplica Horizonte Dividido con Camino de Regreso Envenenado. El costo usado en cada enlace es de valor 1. La duración total de la simulación es de 10 minutos.

Se analizará el resultado sobre el Router 3, que se muestra en la figura anterior. Desafortunadamente, el simulador muestra solo la cantidad de actualizaciones y la tabla de ruteo al final de la simulación no así el proceso para el cual se llego a esa tabla de ruteo ni los mensajes de anuncios y su contenido.

B. Resultados obtenidos

La tabla 1 muestra la cantidad de actualizaciones hechas a la tabla de ruteo. Estas actualizaciones son cambios de información (métricas, próximo salto) en rutas existentes, rutas que se añaden o rutas que se eliminan. La frecuencia con que se mandan los mensajes es de 30 segundos.

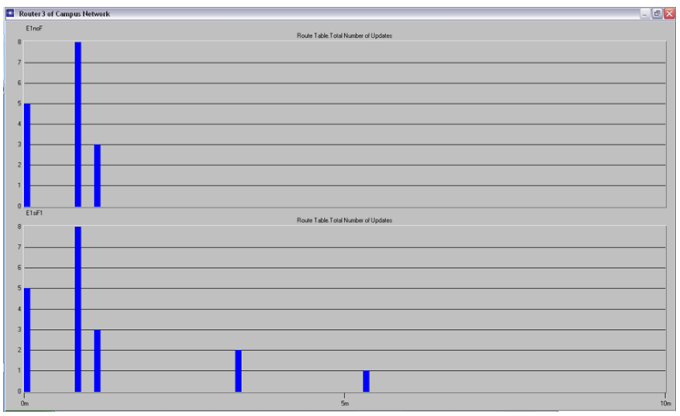

Figura 6

La tabla 2 muestra la tabla de ruteo una vez que finaliza la simulación en el escenario donde el enlace del Router 2 <-> Router 1 está activo.

Cuando el escenario no sufre cambios, RIP solo realiza unas pocas actualizaciones a la tabla de ruteo local. Luego se mantiene estable utilizando el mecanismo de anuncios regulares. Ninguna ruta es eliminada en el transcurso del mismo.

Dir Destino	Mascara Subred	Sig Salto	Nombre Inteface	Metrica	Protocolo	Tempo insertion
192.0.9.0	255.255.255.0	192.0.9.2	IF 0	0	Direct	0.000
192.0.10.0	255.255.255.0	192.0.10.2	IF 1	0	Direct	0.000
192.0.3.0	255.255.255.0	192.0.3.2	IF 10	0	Direct	0.000
192.0.11.0	255.255.255.0	192.0.11.1	IF 11	0	Direct	0.000
192.0.12.0	255.255.255.0	192.0.12.1	Loopback	0	Direct	0.000
192.0.7.0	255.255.255.0	192.0.11.2	IF 11	1	RIP	50.000
192.0.13.0	255.255.255.0	192.0.11.2	IF 11	1	RIP	50.000
192.0.14.0	255.255.255.0	192.0.11.2	IF 11	1	RIP	50.000
192.0.15.0	255.255.255.0	192.0.11.2	IF 11	1	RIP	50.000
192.0.0.0	255.255.255.0	192.0.3.1	IF 10	1	RIP	50.000
192.0.1.0	255.255.255.0	192.0.3.1	IF 10	1	RIP	50.000
192.0.2.0	255.255.255.0	192.0.3.1	IF 10	1	RIP	50.000
192.0.4.0	255.255.255.0	192.0.3.1	IF 10	1	RIP	50.000
192.0.5.0	255.255.255.0	192.0.11.2	IF 11	2	RIP	70.839
192.0.6.0	255.255.255.0	192.0.11.2	IF 11	2	RIP	70.839
192.0.8.0	255.255.255.0	192.0.11.2	IF 11	2	RIP	70.839

Tabla 5

La tabla 3 muestra la tabla de ruteo una vez que finaliza la simulación en el escenario donde el enlace del Router 2 <-> Router 1 cae.

Dir Destino	Mascara Subred	Sig Salto	Nombre Interfaz	Métrica	Protocolo	Tiempo Inserción
192.0.9.0	255.255.255.0	192.0.9.2	IF 0	0	Directo	0.000
192.0.10.0	255.255.255.0	192.0.10.2	IF 1	0	Directo	0.000
192.0.3.0	255.255.255.0	192.0.3.2	IF 10	0	Directo	0.000
192.0.11.0	255.255.255.0	192.0.11.1	IF 11	0	Directo	0.000
192.0.12.0	255.255.255.0	192.0.12.1	Loopback	0	Directo	0.000
192.0.7.0	255.255.255.0	192.0.11.2	IF 11	1	RIP	50.000
192.0.13.0	255.255.255.0	192.0.11.2	IF 11	1	RIP	50.000
192.0.14.0	255.255.255.0	192.0.11.2	IF 11	1	RIP	50.000
192.0.15.0	255.255.255.0	192.0.11.2	IF 11	1	RIP	50.000
192.0.0.0	255.255.255.0	192.0.3.1	IF 10	1	RIP	50.000
192.0.1.0	255.255.255.0	192.0.3.1	IF 10	1	RIP	50.000
192.0.4.0	255.255.255.0	192.0.3.1	IF 10	1	RIP	50.000
192.0.5.0	255.255.255.0	192.0.11.2	IF 11	2	RIP	70.839
192.0.6.0	255.255.255.0	192.0.11.2	IF 11	2	RIP	70.839
192.0.8.0	255.255.255.0	192.0.11.2	IF 11	2	RIP	70.839

Tabla 6

Cuando el escenario sufre la caída del enlace entre los Routers 1 y 2, el sistema (que ha había llegado a una convergencia) debe reordenarse al evento y actualizar sus tablas mediantes las actualizaciones activadas y las regulares. Usando el mecanismo de Horizonte Dividido con Camino de Regreso Envenenado, acelera la convergencia ya que solo se anunciaría la ruta fallida minimizando el peligro de crear un loop a través del "envenenamiento" de la ruta cuando es anunciada en la interfaz por donde se aprendió.

En particular, el cambio específico es que una ruta que atravesaba el enlace entre los Routers debió ser reconfigurado para utilizar otra interfaz, así tuvo que cambiar la métrica (de 1 a 3, lo que indica que el camino es ahora más lejano) y la dirección de próximo salto hacia una nueva interfaz (de IF10 a IF11). A su vez, la red que indicaba el enlace ya no se encuentra en la tabla de ruteo puesto que al ser declarada inalcanzable, los contadores se pusieron en marcha y al final del tiempo de recolección de basura, la ruta fue finalmente eliminada del sistema.

VI. CONCLUSIÓN

RIP es un protocolo IGP para ser usado en redes de diámetro menor a 15 saltos y con una complejidad media-baja. Cuenta con métodos para solucionar situaciones donde el sistema sufre una lenta convergencia. Su versión mejorada introduce el uso de mascaras de subred, autenticación a traces de MD5 y la inclusión de objetos de control en MIB.

Es fácilmente configurable. Los contadores pueden personalizarse para cumplir con las exigencias que las diferentes redes puedan tener, si bien siempre se recomienda usar los tiempos por defecto [10].

Es de fácil implementación y por ello fácil de buscar y corregir posibles errores.

A través de la simulación, se observa el funcionamiento del protocolo en cuanto a actualizaciones de entradas de rutas y las variaciones debido a los posibles cambios que pueden suceder. Se puede observar que en un escenario estable, el protocolo solo realiza unas pocas actualizaciones y llega a un estado de convergencia rápidamente. En el caso de sufrir un cambio (como un enlace caído), el sistema vuelve a adaptarse a través de mensajes de cambios de métricas y reorganizando las tablas de ruteo. Aún así, es igualmente rápido y confiable.

Si bien cuesta creer que dicho protocolo haya sido muy popular y aun hoy en día siga siendo muy utilizado, se puede llegar a la conclusión que la razón de que a pesar de sus limitaciones, el protocolo simplemente funciona y ese hecho no se toma a la ligera. Más aún, funciona extremadamente bien en la mayoría de los entornos actuales donde la estabilidad de un sistema es observado, cuidado y manejado con recelo, lo hace que aun este viejo protocolo sea muy efectivo.

VII. BIBLIOGRAFÍA

[1] RFC 1058,C. Hedrick,June 1988.
[2] RFC 1721,G. Malkin,November 1994.
[3] RFC 1722,G. Malkin,November 1994.
[4] RFC 1723,G. Malkin,November 1994.
[5] RFC 1724,F. Baker,November 1994.
[6] RFC 2082,F. Baker,R. Atkinson, January 1997.
[7] RFC 2453,G. Malkin, November 1998.
[8]OPNET: Manual de usuario,Departament d'Enginyeria Telemática,Universitat Politécnica de Catalunya, Septiembre 2004.
[9]OPNET Laboratory 6:RIP Routing Information Protocolo. ITG_Academic_Edition_v1999
[10]Contivity Secure IP Services Gateway - RIP Routing Configuration, Nortel Networks, July 2003.
[11]RIPtcpip,http://personales.upv.es/rmartin/TcpIp/cap03s02.html