Modelo para la protección de conexiones en redes IPS

Model for the protection of IPS networking

DaniloLópez
Ingeniero Electrónico, Magíster en Teleinformática. Docente de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia. dalopezs@udistrital.edu.co

Nancy Yaneth Gelvez García
Ingeniera de Sistemas, Candidata a Magíster en Ciencias de la Información y las Comunicaciones. Docente de la Escuela Colombiana de Carreras Industriales (ECCI). Bogotá, Colombia. nayag24@hotmail.com

Luis F. Pedraza
Ingeniero Electrónico, Magíster en Ciencias de la Información y las Comunicaciones, Docente de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia. lfpedrazam@udistrital.edu.co

Clasificación del artículo: investigación (Recreaciones)

Fecha de recepción: mayo 26 de 2010 Fecha de aceptación: febrero 1 de 2011

Palabras clave: IP, LER, LSR, LSP, MPLS, Nodo, QoS.

Key words: IP, LER, LSR, LSP, MPLS, Node, QoS.

Resumen

Este artículo resume la primera aproximación generada a una propuesta que permita reducir la probabilidad de riesgo de desconexiones y pérdidas de datos en redes IP.

Abstract

The paper summarizes the first approximation generated to a proposal that permits to reduce the risk probability of disconnections and losing data in IP networks.

* * *

1. Introducción

Desde la década de 1990 los ISP han enfocado sus esfuerzos en consolidar una única red que permita la convergencia de cualquier tipo de servicio a usuarios finales y todo parece indicar que la red que tiene esta titánica labor es Internet; esto conlleva a una dependencia cada vez mayor del ser humano

con las networking. Desde este punto de vista, una de las mayores preocupaciones que se derivan de tal afirmación es ¿cómo solucionar un fallo físico en algún enlace de comunicaciones sin que se pierda la comunicación? La solución más utilizada ha sido la adición de enlaces de respaldo que entran en funcionamiento cuando la línea principal deja de funcionar. Este mecanismo tiene la desventaja de ser costoso, además de generar pérdidas importantes en los anchos de banda disponibles en los enlaces. Otra solución se enfoca en una estrategia más inteligente y menos costosa, relacionada con la modificación del concepto de red, de tal manera que ésta funcione a través de algoritmos de re-routeque que sean capaces de establecer estos caminos alternativos, los cuales entran en funcionamiento cuando se produce la caída del enlace o nodo.

Particularmente, desde el punto de vista de las telecomunicaciones, las redes están divididas en conmutación de circuitos que no brindan por sí mismas un elemento de recuperación de las transmisiones en marcha y conmutación de paquetes que ante congestiones o caída de enlaces, la red examina la topología en busca de rutas con el fin de garantizar que los nuevos datos puedan arribar a su destino por el nuevo segmento sin que se pierda la conexión, aunque sí parte de los paquetes.

Desde este punto de vista se podría conjeturar que las redes de conmutación de paquetes son la solución al problema relacionado con la pérdida en la comunicación ante fallos físicos, sin embargo, los tiempos que tarda la red en ubicar ese enlace sustituto es demasiado elevado (en algunos casos puede tardar minutos) con técnicas tradicionales como el enrutamiento mediante OSPF, IS-IS, RIP. En este sentido, es necesario buscar alternativas valederas que den una mejor solución a la problemática planteada. Una de las tecnologías que más está siendo utilizada por los ISP es la conmutación de etiquetas multiprotocolo, que permiten el establecimiento de enlaces virtuales que no necesariamente son el resultado de la ejecución de un protocolo de *routing* sino de la aplicación de ingeniería de tráfico, es más ésta es quizás una de las razones más valederas para que este protocolo sea tenido en cuenta cuando se requieran caminos opcionales y disyuntivos.

El presente trabajo pretende estudiar el comportamiento de MPLS cuando se le aplica una técnica FRR (Fast-Reroute) a un *backbone* dentro de un mismo sistema autónomo.

2. Sistemas de protección

Antes de continuar, es necesario diferenciar entre reencaminamiento y protección.

Protección frente al reencaminamiento. La recuperación basada en reencaminamiento calcula y establece el camino o segmento de respaldo bajo demanda después de ocurrido el fallo (aunque en ocasiones el cálculo puede ser anterior al fallo, no así laseñalización que implica el establecimiento [1]). En cambio, en una recuperación basadaen protección, el camino o segmento de respaldo ha sido calculado y establecidopreviamente al fallo. Sólo en caso de algún problema, el tráfico se conmuta al camino preestablecido [2].

Existen varias técnicas de protección o recuperación de fallos, entre las que se encuentran:

1+1: en este caso un camino de respaldo sólo protege un camino principal, es decir que la información es enviada simultáneamente por la ruta de respaldo. El PML (PathMergeLSR) es el que se encarga de seleccionarde cuál de los caminosobtener el tráfico.

*1:1:*el flujo se transmite por el enlace respaldo solamente si el primario deja de funcionar.

*1:N:*un camino de respaldo protege N caminos principales.

M:N: M caminos de respaldo son utilizados para proteger N caminos primarios y se conmutan entre sí siempre y cuando falle el principal.

3. Técnicas FRR (Fast-Reroute)

Tal y como se había dicho inicialmente, en una topología cualquiera los enlaces virtuales, físicos y nodos están supeditados a posibles problemas de conectividad. La tarea fundamental de las técnicas FRR (Fast-Reroute) consiste en reducir la probabilidad de riesgo de desconexión. El mecanismo FFR sigue un ciclo que abarca desde la localización de la falla hasta el reestablecimiento del medio de transmisión o nodo. Dicho ciclo comprende cinco componentes fundamentales que son:

- Un método de *re-routing* que selecciona el o los posibles enlaces de respaldo.
- Un algoritmo que gestiona la reserva de ancho de banda y de distribución de etiquetas en la ruta primaria y secundaria.
- Un algoritmo de detección-notificación de problemas que da la posición exacta del nodo que debe generar la acción de respuesta al fallo generado.
- Una aplicación que tenga la capacidad de hacer el reenvío desde el enlace que generó la desconexión al secundario.
- Opcionalmente, se puede contar con un algoritmo que detecte la restauración de la ruta primaria y que permita el desvió del flujo de nuevo a su estado original.

Makam planteó un posible algoritmo para protección de redes, el cual aplica protección y *re-route*. Este consiste en que el nodo que detecta la desconexión despacha una alerta al *router,* ingreso del sistema autónomo del tráfico protegido para que éste lo conmute hacia el enlace redundante. El principal inconveniente de este modelo es que el nodo que detecta el fallo debe enviar un aviso al *head-end* [3]. Durante el tiempo que tarda esta notificación es posible que se pierdan muchos paquetes ya que quien toma la decisión de la recuperación es el *router* de entrada al dominio.

Hasking propuso un algoritmo que mejora las prestaciones de su predecesor en el sentido de que es el propio nodo que detecta el fallo el que se encarga de la protección [4], minimizándose así la pérdida de paquetes.

Con la globalización de las redes MPLS es importante aprovechar las virtudes que éstas tienen en el momento de emplear ingeniería de tráfico a la protección, donde ésta puede aplicar a un único segmento o a toda una ruta de origen a destino. A continuación se muestran los avances que se han generado hasta el momento en relación a la generación de un algoritmo que puede mejorar las prestaciones en cuanto a protección y *re-route* en entornos IP/MPLS.

4. Aplicación de re-route en redes IP mediante Mpls

Se parte de que la topología a utilizar para la evaluación del modelo hace parte de un mismo dominio.

Dentro de las características de la red (Figura 1), se observa que está constituida por 9 LSRs (LSR_A, LSR_B, LSR_C, LSR_D, LSR_E, LSR_F, LSR_G, LSR_H, LSR_I,) que forman lo que es el *backbone* MPLS y dos nodos netamente IP (que representan el origen y el destino de los datos).

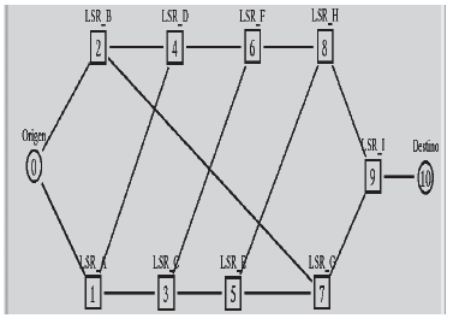

Figura 1. Topología de la red.

Algunos enlaces poseen una estructura con un ancho de banda de 10 Gb y otros de 15 Gb, asociados a un retardo por enlace de 10 ms y a un tipo de cola CBQ (Encolamiento Basado en Clases). Ver Figuras 2 y 3.

```
# ESTABLECIMIENTO DE LOS NODOS
set node0  [$ns node]
set LSR1   [$ns mpls-node]
set LSR2   [$ns mpls-node]
set LSR3   [$ns mpls-node]
set LSR4   [$ns mpls-node]
set LSR5   [$ns mpls-node]
set LSR6   [$ns mpls-node]
set LSR7   [$ns mpls-node]
set LSR8   [$ns mpls-node]
set LSR9   [$ns mpls-node]
set node10 [$ns node]
```

Figura 2. Características de los nodos.

```
# INTERCONEXIÓN DE LOS NODOS Y CARACTERISTICAS
#DE LOS ENLACES
$ns duplex-link $node0 $LSR1  10Gb  10ms cbq
$ns duplex-link $node0 $LSR2  15Gb  10ms cbq
$ns duplex-link $LSR1  $LSR4  10Gb  10ms cbq
$ns duplex-link $LSR3  $LSR5  10Gb  10ms cbq
$ns duplex-link $LSR5  $LSR7  10Gb  10ms cbq
$ns duplex-link $LSR7  $LSR9  15Gb  10ms cbq
$ns duplex-link $LSR3  $LSR6  10Gb  10ms cbq
$ns duplex-link $LSR2  $LSR4  10Gb  10ms cbq
$ns duplex-link $LSR4  $LSR6  10Gb  10ms cbq
$ns duplex-link $LSR6  $LSR8  10Gb  10ms cbq
$ns duplex-link $LSR8  $LSR9  10Gb  10ms cbq
$ns duplex-link $LSR1  $LSR3  10Gb  10ms cbq
$ns duplex-link $LSR5  $LSR8  10Gb  10ms cbq
$ns duplex-link $LSR2  $LSR7  15Gb  10ms cbq
$ns duplex-link $LSR9  $node10  15Gb  10ms cbq
```

Figura 3. Características de los enlaces.

Inicialmente, el protocolo de enrutamiento OSPF genera actualizaciones con el fin de generar la tabla topológica y poder establecer la ruta más óptima de acuerdo a la demanda con los parámetros solicitados para posteriormente empezar la transferencia de la información que para la topología especificada es a través de los nodos 0-2-7-9-10, como se evidencia en la Figura 4.

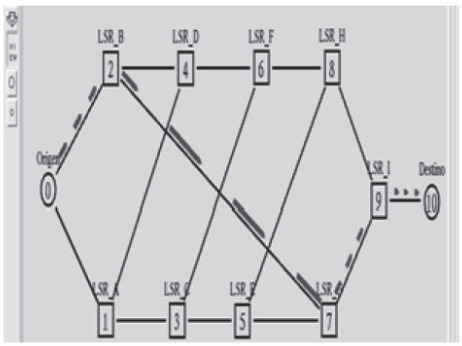

Figura 4. Envió de información de nodo IP origen a nodo IP destino.

La técnica implementada a través del código desarrollado en el software NS-2.34 bajo ambiente linux implica el resguardo para toda la ruta que está transmitiendo los datos (origen a destino). Esto se logró conseguir configurando el FRR en los LSR_B, LSR_G , LSR_I que corresponden a los extremos del dominio MPLS, detectando así cualquier fallo independientemente de donde se genere éste dentro de la ruta seleccionada. Esto se traduce en que se garantiza la propagación de la señal de fallo FIS (FaultIndicationSignal) hasta el LER que detectó la desconexión, reduciendo en gran medida el tiempo de restauración a un valor menor delos 50 ms y la pérdida de paquetes. El algoritmo implementado se muestra en la Figura 5.

```
proc set-danilo-FRR {option} {
    global ns LSR2 LSR7 LSR9
    set LSRmpls2 [$LSR2 get-module "MPLS"]
    set LSRmpls7 [$LSR7 get-module "MPLS"]
    set LSRmpls9 [$LSR9 get-module "MPLS"]
    switch $option {
        drop            {
                          # se activa el re-route cuando el enlace o nodo falla
                          $ns enable-reroute drop
                          $LSRmpls2 enable-data-driven
                        }
        action-driven   { # Acción a tomar cuando el link falle
                          $ns enable-reroute L3
                          $LSRmpls1 set-protection-flow 0.1 0.01 10 -1

                          # Eventos propios del protocolo LDP
                          $ns enable-on-demand
                          $ns enable-ordered-control
                          $ns enable-data-driven
                        }
    }
}
```

```
#.....................................................................
proc set-reroute-event-dals {option} {
    global ns LSR2 LSR7 LSR9
    set LSRmpls2 [$LSR2 get-module "MPLS"]
    set LSRmpls7 [$LSR7 get-module "MPLS"]
    set LSRmpls9 [$LSR9 get-module "MPLS"]
    switch $option {
        danilo          {
                          # LSP: Ruta principal
                          $ns at 0.0  "$LSRmpls2  setup-erlsp  9   2_7_9     1300"

                          #LSP: Ruta alternativa
                          $ns at 0.1  "$LSRmpls1  setup-erlsp  9   2_4_6_8_9     2000"
                          $ns at 0.3  "$LSRmpls1 bind-flow-erlsp   3   90   1000"

                          $ns at 0.3  "$LSRmpls1 reroute-lsp-binding     1000    2001"
                          $ns at 0.3  "$LSRmpls4 reroute-lsp-binding     1000    2003"
                          $ns at 0.3  "$LSRmpls6 reroute-lsp-binding     1000    2003"
                          $ns at 0.3  "$LSRmpls8 reroute-lsp-binding     1000    2003"
                          $ns at 0.3  "$LSRmpls9 reroute-lsp-binding     1000    2003"
                        }
    }
}
```

Figura 5. Código de protección diseñado.

Tal y como se detalla en el programa desarrollado, para garantizar la protección del camino el LSR_2 se configuró para que tuviera funcionalidad PSL (Protection Source LSR), el otro nodo extremo (el LSR_9) se activó como PLM (Protection Source LSR) para que cumpla la función de permitir la interacción entre los flujos que vienen desde el camino principal y secundario, siempre y cuando pertenezcan al mismo LSP.

A continuación, a manera de prueba, se muestra una serie de eventos que permiten visualizar y comprobar el comportamiento de la *networking* ante la caída de un enlace principal, secundario y la restauración del primario.

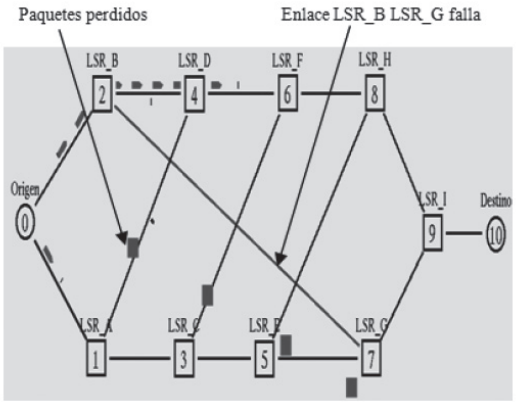

Figura 6. Evento que simula la caída del enlace entre los nodos LSR_B y LSR_C.

Se puede apreciar que una vez es detectado el problema en el enlace que conecta al LSR_B con LSR_G se generan actualizaciones y se pone en funcionamiento el camino de respaldo LSR_A - LSR_D - LSR_F - LSR_H - LSR_I. Los paquetes que están en cola y aquellos que se encuentran entre la ruta origen y LSR_B no se pierden sino que son re-encaminados a través del LSR_D y tenderán a retomar la ruta secundaria, como se aprecia en la Figura 7.

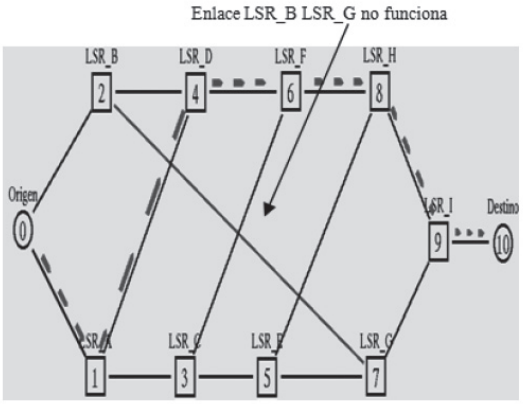

Figura 7. Camino de respaldo generado por la aplicación.

El siguiente evento (Figura 8) permite establecer el comportamiento del modelo cuando el enlace LSR_H-LSR_I de la ruta de respaldo establecida se cae.

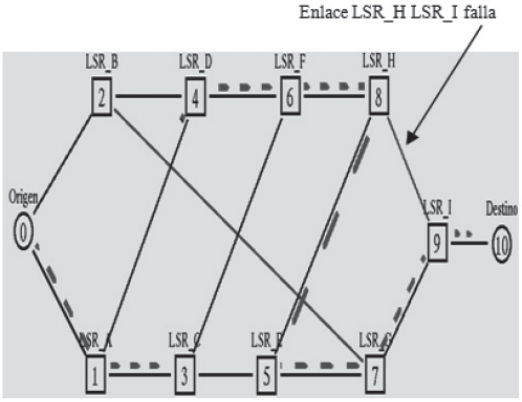

Figura 8. Comportamiento de la red MPLS cuando la ruta entre LSR_H-LSR_I deja de funcionar.

Finalmente se presenta la dinámica suscitada cuando se restablece la ruta principal al destino (Figura 9). Aquí se puede ver que MPLS, asociado con FRR, tiende a determinar en qué instante se restaura el enlace entre el LSR_B y el LSR_G para poder reutilizar el LSP que inicialmente había sido generado por MPLS y que garantizaba, de forma óptima, los requerimientos exigidos.

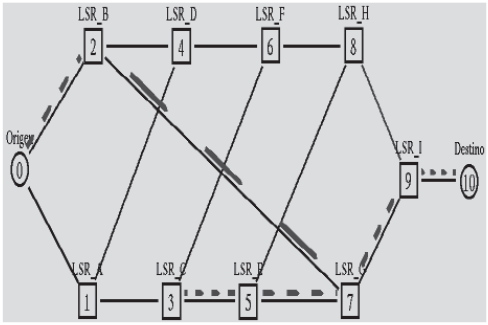

Figura 9. Reutilización del LSP inicial.

5. Conclusiones

En el presente artículo se ha realizado una primera aproximación enfocada a garantizar la protección de conexiones lógicas y físicas preestablecidas en redes IP.

Una de las desventajas encontradas en este algoritmo es que el consumo de ancho de banda incrementa debido a las actualizaciones producto de la evaluación del estado de cada segmento. Hecho que se revisará con el fin de mejorar la prestaciones del mismo.

Dentro de las ventajas del modelo propuesto está la búsqueda de rutas redundantes, siempre y cuando éstas existan, independientemente de que sean caminos primarios o secundarios, aunque habrá que evaluar el tiempo promedio que tarda en generarlas y si éstas son capaces de crearse garantizando las prestaciones exigidas por el usuario.

Referencias bibliográficas

[1] J-P. Vasseur, M. Pickavet, P. Demeester, "Network Recovery: Protection and Restoration of Optical", *SONET-SDH, IP, MPLS.Morgan Kaufmann Publishers Inc*, San Francisco, CA, USA, 2004.

[2] V. Sharma, F. Hellstrand, "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery", *RFC 3469 (Informational)*, feb 2003.

[3] S. Makam, V. Sharma, K. Owens, C.Huang,"Protection/Restoration ofMPLS Networks",*draft-makam-mpls-protection-00.txt*, oct 1999.

[4] D. Haskin, R. Krishnan,"A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute",*draft-haskin-mpls-fast-reroute-05.txt*, nov 2000.