Evaluación del tiempo de recuperación de fallas para LSP L1VPN sobre redes GMPLS

Time failover evaluation on GMPLS LSP L1VPN networks

Octavio Salcedo
Ingeniero en Sistemas, magister en Teleinformática, candidato a Doctor en Informática. Docente de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia. Contacto: *ojsalcedop@udistrital.edu.co*

Danilo López
Ingeniero Electrónico, magíster en Teleinformática. Docente e investigador de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia.
Contacto: *dalopezs@udistrital.edu.co*

Luis F. Pedraza
Ingeniero Electrónico, magíster en Ciencias de la Información y las Comunicaciones, estudiante de doctorado en Ingeniería de Sistemas y Computación de la Universidad Nacional de Colombia. Docente e investigador de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia.
Contacto: *lfpedrazam@udistrital.edu.co*

Fecha de recepción: 14 de noviembre de 2011 **Clasificación del artículo: Investigación**

Fecha de aceptación: 28 de agosto de 2012 **Financiamiento: Universidad Distrital Francisco José de Caldas**

Palabras clave: enrutamiento, GLASS, GMPLS, L1VPN, protocolo, red privada virtual.

Key words: routing, GLASS, GMPLS, L1VP, protocol, virtual private network.

RESUMEN

Las fallas de red son un problema común en las redes actualmente y dependen, en mayor o menor grado, de diferentes factores como el número de dispositivos que conforman los enlaces, la calidad de los mismos, la ubicación geográfica, condiciones ambientales o socioeconómicas, entre otras. Son muchos los factores que influyen cuando se presentan fallas en una red, lo cual indica que las redes van a tener fallas en mayor o menor medida pero siempre van a estar pre-

sentes. Sin embargo, el tema central no es si se tienen fallas de red o no, el tema central es qué tan rápido se puede la red recuperar de estas y restablecer el servicio. Este artículo se enfoca en los tiempos de recuperación de fallas en una red L1VPN sobre GMPLS en la cual las fallas pueden ser resueltas automáticamente mediante protocolos de enrutamiento redireccionando los paquetes por rutas alternas.

ABSTRACT

Nowadays network failure is a common problem that is caused, to certain extent, by various factors such as the number of devices involved in a link, the quality of these devices, their geographical location, and environmental conditions among others. There is a great deal of factors influencing network failure occurrence, which indicates that, whether expected or not, failure will always be present. However, the issue is not about having or avoiding failure but about how quickly can a network recover and restore its services.

The present paper addresses the point of failure-recovery time of an L1VPN over GMPLS technology, where failure can be automatically overcome through routing protocols by redirecting packets to alternate routes.

* * *

1. INTRODUCCIÓN

La recuperación de la comunicación ante una falla de red se ha convertido en una métrica importante a la hora de determinar la confiabilidad de una red en términos de calidad de servicio y de cumplir con ciertos acuerdos de nivel de servicio (SLAs). Con GMPLS surgiendo con una nueva tecnología en redes ópticas, se hace necesario determinar los tiempos de recuperación ante una falla de un enlace o un nodo de la red teniendo en cuenta el tiempo que se tarda en detectar la falla y el tiempo de restablecimiento del servicio, con lo cual se puede determinar qué tan fiable son los procedimientos de detección y corrección de fallas en esta nueva tecnología.

2. GMPLS (GENERALIZED MULTIPROTOCOL LABEL SWITCHING)

Los investigadores en MPLS probaron que una etiqueta podría ser mapeada a un color en el espectro y que los paquetes pueden ser enlazados directamente hacia una red óptica [1], [2]. Este proceso inicial fue llamado MPIS o MPLambdaS. A medida que las investigaciones continuaron se hizo necesario crear un método que realizara un control total de la red óptica.

Con la implementación de este método de control total también surge la necesidad de modificar un conjunto de protocolos para hacerlos capaces de manejar los distintos tipos de dispositivos de la red y realizar un control sobre la misma. En la figura 1 se puede observar una red GMPLS que opera en modalidad end to end en protocolo IP, opera MPLS de enrutador de borde a enrutador de borde y GMPLS entre dispositivos ópticos.

2.1 Plano de control GMPLS

El plano de control de GMPLS es el encargado de controlar todos los aspectos de la red de datos y controla desde protocolos hasta dispositivos de red. Este plano de control provee cinco niveles de función [2].

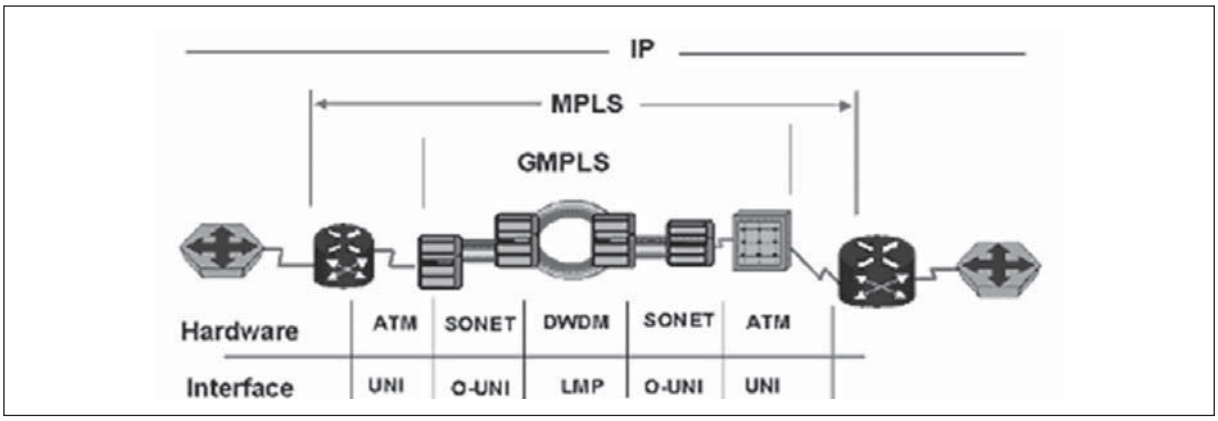

Figura 1. Tipos de redes punto a punto.
Fuente: tomado de [1]

2.1.1 Descubrimiento de vecinos

Para manipular los dispositivos de una red todos estos deben ser conocidos por el plano de control, para esto se utiliza un protocolo llamado LMP por sus siglas en inglés (LINK Managenment Protocol).

2.1.2 Diseminación de estado de enlace

Realiza una diseminación de información con el fin de determinar los estados de los enlaces. Para estos casos se utilizan los estados de los enlaces los cuales pueden ser determinados por el protocolo de enrutamiento OSPF-TE.

2.1.3 Administración de estado de enlace

Para la topología de red, además de los dispositivos que tiene la red, también es necesario saber el estado en el cual están dichos enlaces. Protocolos como OSPF (figura 5) pueden ser usados para verificar estos enlaces permanentemente.

2.1.4 Path Management

Para el manejo de caminos, GMPLS utiliza el protocolo RSVP-TE [3], el cual está siendo reevaluado por el comité de la IETF, y va modificado junto con el protocolo LDP para suplir las necesidades completas en cuanto a enrutamiento se refiere para GMPLS.

2.1.5 Administración del estado del enlace

En MPLS se usa el LSP (Label Switch Path) para establecer, bajar y subir enlaces. En GMPLS se encarga de estas funciones el protocolo LMP (Link Management Protocol) el cual hereda las funciones de MPLS para aplicarlas a un plano óptico.

GMPLS surge entonces como un avance evolutivo de MPLS, en el cual no se conmutan únicamente paquetes sino que se hace conmutación de tiempo, longitudes de onda y de fibras ópticas.

GMPLS abarca, además de los enrutadores IP y los switches ATM, dispositivos de conmutación tales como: conmutadores digitales de señales multiplexadas en el tiempo o DXC (Digital Cross Connect), conmutadores de longitudes de onda con conversión electroóptica o OXC (Optical Cross Connect) y conmutadores de longitudes de onda totalmente ópticos o PXC (Photonic Cross Connect) [1]. Para ello, GMPLS extiende

ciertas funciones base del tradicional MPLS y, en algunos casos, añade nueva funcionalidad. Estas adaptaciones han supuesto la extensión de los mecanismos de etiqueta y de LSP, para crear etiquetas generalizadas y G-LSP **(**Generalized LSP**)**; afectando también a los protocolos de encaminamiento y señalización para actividades como: la distribución de etiquetas, la ingeniería del tráfico, y la protección y restauración de enlaces.

2.2 Redes privadas virtuales de capa uno (L1VPN) sobre GMPLS

El "framework" de las redes privadas virtuales de capa 1(L1VPN) emerge de la necesidad de extender el intercambio de paquetes (Switching) hacia el dominio del intercambio de circuitos. En resumen, los grandes clientes desean tener sus propias redes de transporte/intercambio, pero no desean desplegar sus propias infraestructuras; adicionalmente, muchos proveedores desean realizar una partición de sus redes, en redes virtuales de capa 1 separadas que sirvan diferentes unidades de negocio [4]. Las redes privadas virtuales de capa 1 atienden estas necesidades asignando a los clientes un conjunto de recursos de la red física (nodos, puertos y capacidades de enlaces) y dando a cada cliente la responsabilidad de administrar dichos recursos independientemente. Para los clientes, esto permite un aprovisionamiento rápido y eficiente de servicios multicapa sin la necesidad de desplegar una red propia, así mismo, para los proveedores esto implica costos operacionales muchos menores.

Lo más significativo es que estas redes virtuales pueden dominar una gran cantidad de protocolos de capas más altas [5]. La figura 2 ilustra el concepto de una red privada virtual de capa 1 la cual es capaz proporcionar diferentes servicios y protocolos de niveles superiores a distintos clientes en la L1VPN.

Entre las ventajas que ofrece una red virtual de capa 1 es que los clientes pueden utilizar una red de transporte, virtualmente dedicada a ellos, sin tener que construir una red ellos mismos; de igual

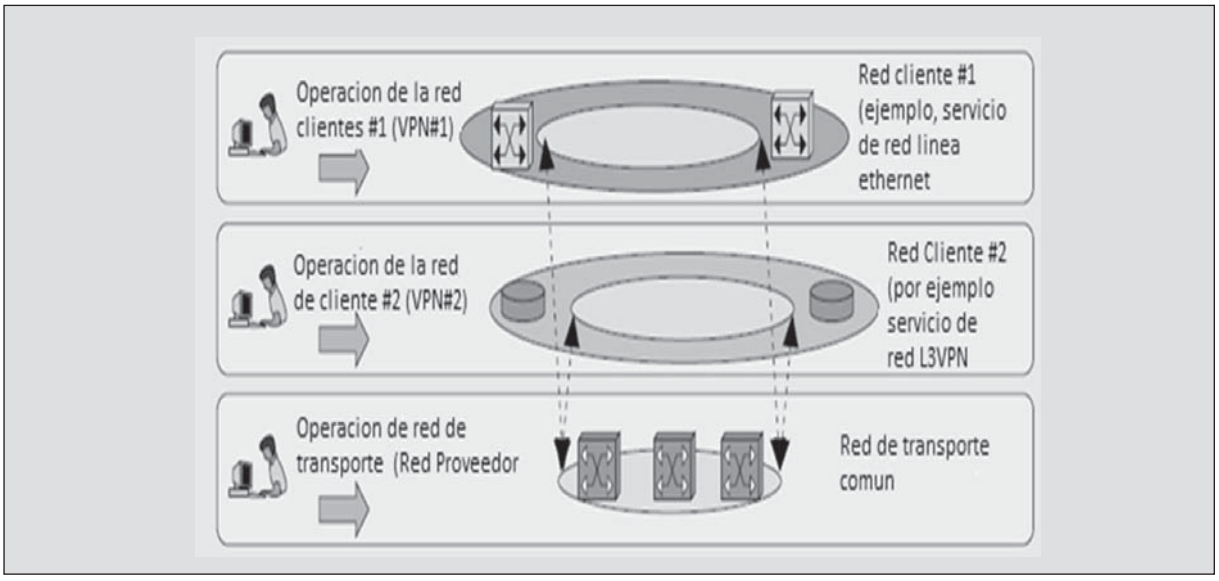

Figura 2. Concepto de una red L1VPN.
Fuente: tomado de [6]

manera, la operación y administración de dicha red puede ser entregada al proveedor, con lo que varios clientes que manejen redes virtuales, dentro de la misma red de transporte, pueden compartir los costos de administración. Así mismo, el proveedor puede ofrecer servicio dinámico bajo demanda [6], [7].

Para la implementación de funciones VPN hay diversos modelos de servicio usando protocolos GMPLS. Entre estos modelos, se encuentra el modelo basado en administración en el cual el cliente accede a los recursos de la L1VPN del proveedor mediante una interface de administración (por ejemplo una interfaz web) y de esta manera controla y administra su propia porción de la red. A este modelo se le llama modelo de servicio basado en administración y no requiere necesariamente un manejo de GMPLS en la red del cliente [6]. El siguiente modelo es el modelo basado en señalización, en el cual se implementan funciones de señalización de GMPLS en los nodos borde del cliente. Los clientes pueden solicitar configuración de la conexión, borrado o modificación mediante señalización. En GMPLS la conexión se le conoce con el nombre de camino de intercambio de etiquetas (LSP – Label Switched Path). La utilización de GMPLS entre el cliente de borde y el proveedor de borde asegura la interoperabilidad. Así mismo, GMPLS provee mecanismos de notificación rápida de falla en el LSP. El tercer modelo es una interoperabilidad total entre el cliente y proveedor, para lo cual es necesario la implementación de GMPLS tanto a nivel de proveedor como de cliente, permitiendo el intercambio de información de enrutamiento y señalización directamente entre cliente y proveedor.

Para el caso específico de este trabajo se maneja el segundo escenario, en el cual el cliente no maneja una red GMPLS pero implementa funciones de señalización en los nodos borde del cliente. Se selecciona este escenario debido a las siguientes razones:

- El manejo de GMPLS se realiza en la red del proveedor únicamente, mientras que la red del cliente maneja MPLS restringiendo la detección y solución de fallas únicamente en el LSP GMPLS
- El soporte de la herramienta de simulación maneja únicamente GMPLS bajo la red proveedora, permitiendo manejo de MPLS para el cliente únicamente.
- Este escenario permite el manejo del modo básico de L1VPN.

Las redes VPN en modo básico [8], [9] son VPNs basadas en puerto cuya unidad básica de comunicación son las etiquetas (LSP) entre los puertos de inicio y de destino.

Para que la comunicación a nivel L1VPN sea viable, la red proveedora de este servicio debe ser una red que soporte GMPLS a nivel proveedor (como los dispositivos LAMBDA Switch capable – LSC, conexiones ópticas cruzadas, SONET/SDH). Estos elementos se dividen en dos categorías: dispositivos P (provider) y dispositivos PE (Provider Edge). Se diferencian en que los dispositivos P están conectados únicamente a otros dispositivos dentro de la misma red del proveedor y los dispositivos PE están conectados a tanto a dispositivos P o PE dentro de la red del proveedor así como a otros dispositivos por fuera de dicha red. Los otros dispositivos se van a identificar como CE (Customer Edge) dispositivos de borde de cliente, los cuales están conectados a dispositivos PE y a dispositivos de cliente.

Se presenta en la figura 3 un modelo de cómo sería una VPN capa uno [4], [10], con su respectiva red interna de proveedor.

2.3 Recuperación de fallos GMPLS

Los mecanismos de recuperación de fallas para los protocolos GMPLS, o para cualquier otro pro-

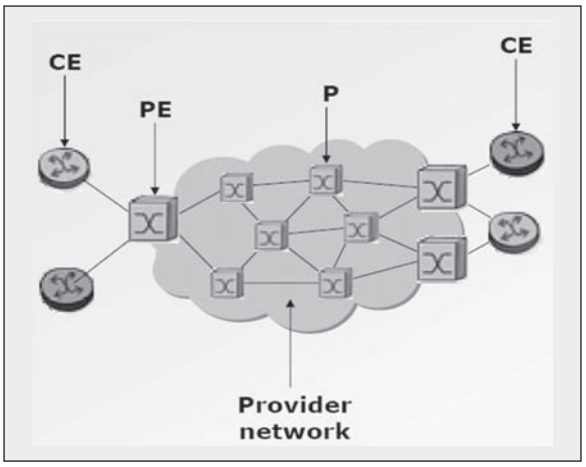

Figura 3. Modelo generalizado de una L1VPN.
Fuente: tomado de [11]

tocolo, deben cumplir con las siguientes fases en orden de realizar una recuperación exitosa: detección de la falla, localización de la falla, notificación de la falla, recuperación y reversión, siendo conocidas las primeras tres como administración de fallas (failure management)

3. METODOLOGÍA

Como herramienta de simulación del mecanismo de autodescubrimiento de la red privada virtual de capa uno, se utilizó GLASS (GMPLS LIGTHWAVE AGILE SWITCHING SIMULATOR) [12] - [14] el cual es un simulador capaz de soportar el Framework de GMPLS. La selección de la herramienta de simulación se realiza basados en la evaluación de diferentes herramientas de acuerdo a características necesarias para la implementación del mecanismo de autodescubrimiento. Dentro de las herramientas evaluadas se encuentran: OPNET, NS2, OMNET++, GLASS/SSF, QualNet, JSim, TOTEM y se selecciona GLASS como la herramienta más adecuada debido a que dicho simulador tiene soporte completo de redes ópticas, GMPLS, facilidad de adaptación de nuevos protocolos, algoritmos, manejo de protocolos de reserva de recursos RSVP-TE, ingeniería de tráfico (TE) y recuperación ante fallos a nivel GMPLS.

3.1 Escenario

La figura 4 ilustra el escenario de red mediante el cual se realiza la simulación de la red. En el cual, el área azul determina la red del proveedor (P), los enrutadores encerrados en rojo indican que son dispositivos de borde de Proveedor (PE), los LSRs encerrados en negro indican los dispositi-

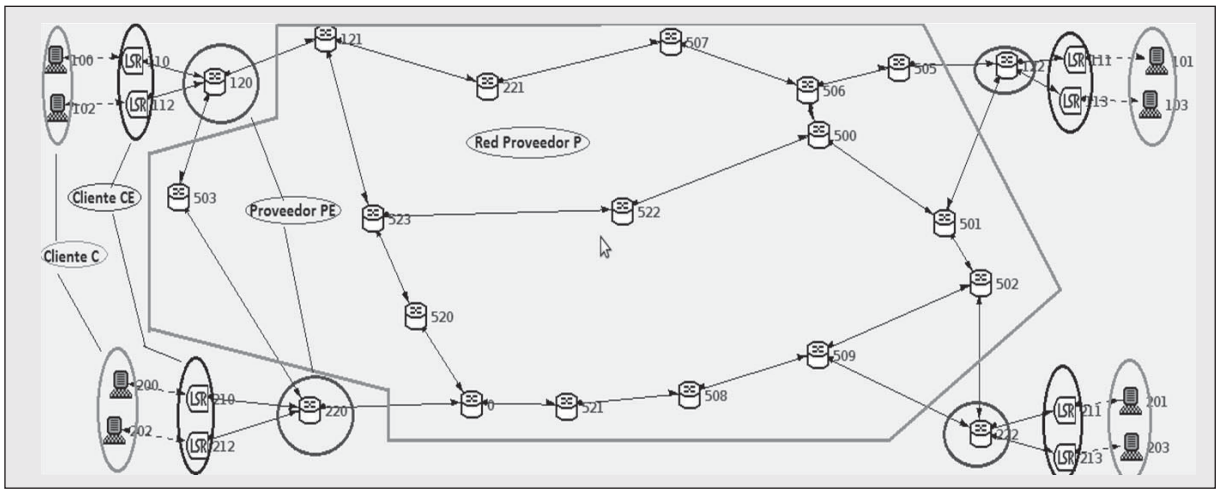

Figura 4. Escenario de la L1VPN.
Fuente: elaboración propia

vos de borde de cliente (CE) y las estaciones de trabajo en verde son los dispositivos cliente (C) de la VPN.

El modelo de la simulación de la L1VPN fue implementado con fallas programadas a los 120 segundos de tiempo de simulación.

3.2 Parámetros

Para efectos de este trabajo se realizó la simulación utilizando únicamente un establecimiento de VPN entre el los OXC ópticos, tomando como dispositivos de borde PE los OXC en rojo, de acuerdo a la figura 4.

3.2.1 Parámetros generales de la red

Frecuencia de RED: 20000000 la cual representa el valor físico de tiempo simulado, representando el número de tics de reloj por segundo simulado.

Generador: Mersennetwister es un parámetro de administración usado para la generación aleatoria de tramas en la simulación.

Trama: Seedstarter1 se usa para generar cadenas de datos de diferentes maneras de una forma totalmente aleatoria.

Nivel de reproductibilidad: Timeline determina qué tan separadas estarán las instancias de la generación aleatoria de números. Es un proceso que garantiza que la simulación que se ejecuta va a ser la misma para uno o para muchos procesadores.

Patrones de tráfico: clientes izquierda a servidores derecha y viceversa.

Cada uno de los host que hacen de servidores utiliza como protocolo de transporte el protocolo UDP saliendo por el puerto 10 a una tasa de 50000 paquetes por segundo y una distribución exponencial con un tamaño de 1000, una distribución del tamaño del paquete normal y una desviación de 0.3. Los host que hacen como clientes ejecutan los mismos protocolos, pero definen un tamaño de archivo de transmisión sobre el mismo UDP.

Para propósitos de este trabajo el establecimiento de la red VPN capa 1 se establecerá desde el LSR del primer host hasta el LSR del host destino de VPN. Puesto que el análisis de este trabajo se limita a la red exclusiva del proveedor donde se utiliza GMPLS. Protocolos utilizados por los LSR y los OXC:

RSVP-TE: Protocolo de señalización.

OSPF-TE: Protocolo OSPF para ingeniería de tráfico.

IP: Protocolo de Internet.

OSPF: Protocolo de camino más corto.

OXC: Protocolo de comunicación entre dispositivos ópticos.

Para la simulación del establecimiento con BGP se usa BGP en lugar de OSPF-TE.

3.3 Ejecución

La simulación tiene una duración total de 240 segundos de simulación durante los cuales se presentan fallas en el tiempo a los 120 segundos y se toman mediciones del tiempo de recuperación de los LSPs para estas fallas. En total se ejecutan 10 simulaciones, que tienen como fin tomar los tiempos de recuperación de cada una de las fallas de los enlaces, de forma que se tengan datos más

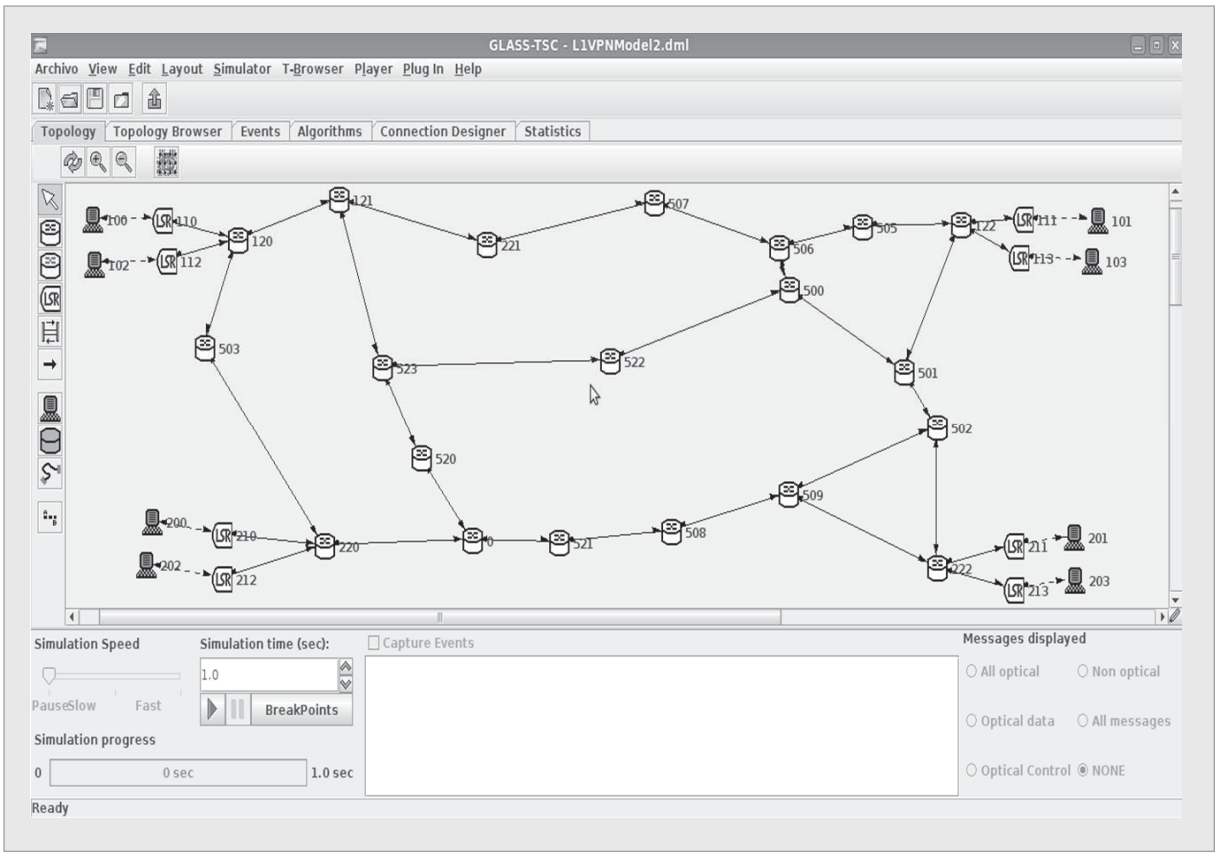

Figura 5. Topología de la red.
Fuente: elaboración propia

exactos del tiempo de recuperación ante una falla en cada una de sus fases.

4. RESULTADOS

Durante el proceso en que se presenta la falla y la normalización de la operación de la red se presentan cuatro fases: detección, notificación, recuperación y normalización; cada una tiene sus propios tiempos de duración, la sumatoria de estos tiempos da como resultado el tiempo total de recuperación ante una falla de un enlace. En la figura 5 se puede apreciar la topología de red usada para todas las simulaciones y en la figura 6 se puede ver el resultado de las 10 simulaciones ejecutadas. Estas simulaciones se realizan con el fin de determinar los tiempos de recuperación ante

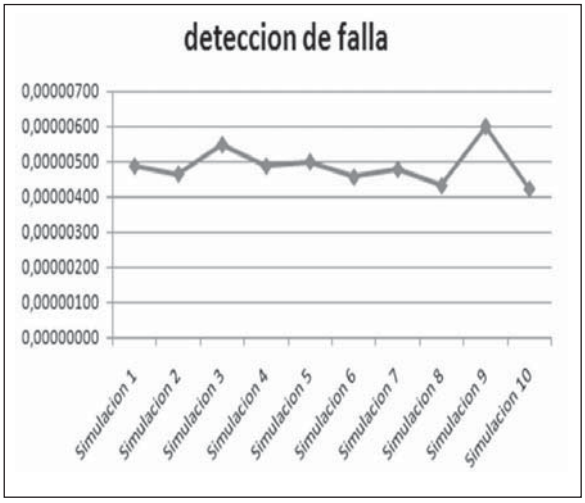

Figura 6. Resultados de las simulaciones detección de la falla.
Fuente: elaboración propia

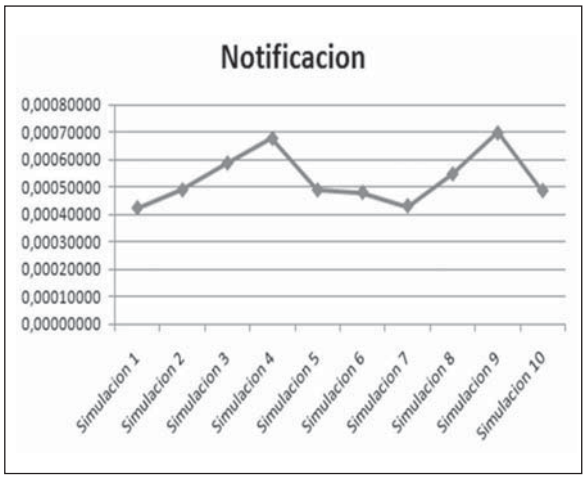

Figura 7. Tiempos de notificación de falla.
Fuente: elaboración propia

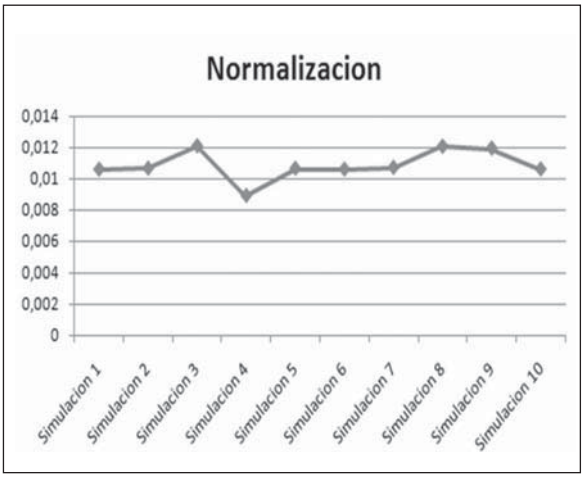

Figura 9. Tiempos de normalización.
Fuente: elaboración propia

fallas en cada una de las fases de detección de la falla y recuperación ante la misma.

En la figura 7 se puede apreciar la notificación de la falla, es decir, el tiempo en el cual los nodos que están al inicio y al final del LSP son advertidos de que ha ocurrido una falla y son notificados en donde ha sucedido esta falla.

En la figura 8 se puede apreciar el resultado de la recuperación, seleccionando un LSP adicional que evite falla y que tenga las mismas características de TE que el LSP que presentó la falla.

La figura 9 identifica el tiempo de normalización de la operación de la red después de recuperarse de la falla.

La figura 10 representa el tiempo total desde que se presenta la falla a los 120 segundos hasta la normalización del proceso de red.

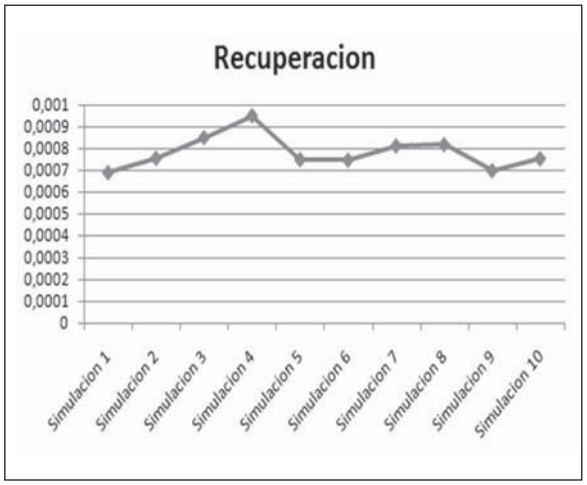

Figura 8. Tiempos de recuperación de la falla.
Fuente: elaboración propia

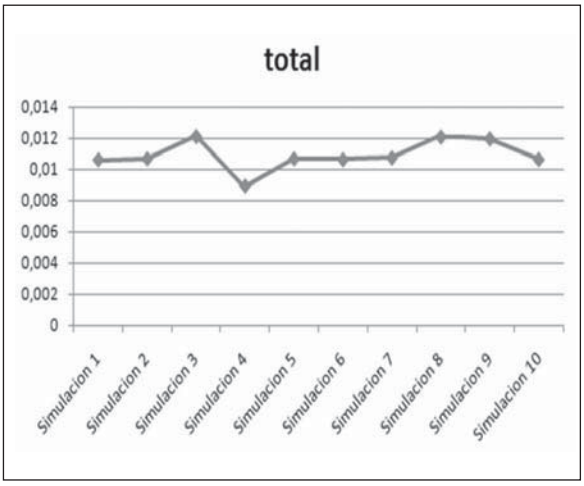

Figura 10. Tiempo total de recuperación.
Fuente: elaboración propia

5. CONCLUSIONES

Del escenario planteado en este análisis se puede verificar que, en las cuatro fases presentadas, los tiempos de recuperación ante fallas son mucho mayores en la fase de normalización de la red, puesto que es la fase de inicialización de la operación normal con el nuevo LSP, el cual, de acuerdo a la tabla, cubre una distancia más grande y contiene un mayor número de nodos.

Los tiempos detección de la falla son bastante cortos en comparación con los tiempos de las demás fases del proceso de recuperación. Esto sucede debido a que las notificaciones de la falla deben pasar mediante RSVP-TE por todos los nodos del LSP hasta llegar a los nodos en cada extremo del LSP, indicando en dónde fue la falla.

El análisis de los tiempos de recuperación de falla en GLASS es bastante dispendioso puesto que la herramienta no cuenta con los reportes adecuados de tiempo y es necesario recurrir a los Logs de la simulación en orden de determinar tiempos, y protocolos.

REFERENCIAS

[1] E. Mannie, *Generalized Multi-Protocol Label Switching (GMPLS) Architecture*.

[2] R. Coltun, FORE Systems, "The OSPF Opaque LSA Option", *RFC 2370*, July 1998.

[3] D.Katz, K. Kompela, and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", *RFC 3630*, September, 2003.

[4] J. Scharf and M. Köhn, *Traffic Demand Modeling for Dynamic Layer 1 VPN Services*, University of Stuttgart, Institute of Communication Networks and Computer Engineering (IKR), April, 2006.

[5] N. Ghani, D. Benhaddou, W. Alanqar, V. M. Muthalaly, and M. Hari, *Performance of dynamic Shared Layer 1 VPN Services in next generation SONET SDH networks*, Tennesee Tech University, University of Houston, Sprint Nextel.

[6] T. Takeda, NTT, D. Brungard, AT&T LABS, D. Papadimitriou, ALCATEL, H. Brahim, NORTEL, "Layer 1 Virtual Private Networks: Driven Forces and Realization by GMPLS", *IEEE communications magazine*, Vol 43, No.7, July, 2005.

[7] T. Takeda, et al, "Layer 1 Virtual Private Networks: Service Concepts, Architecture Requirements, and Related Advances in Standardization", *IEEE Comm. Magazine*, Vol. 42, No. 6, pp. 132-138, June, 2004.

[8] D. Fedyk, Ed. Request for Comments: 5251 Nortel Category: Standards Track Y. Rekhter, Ed. Juniper Networks, D. Papadimitriou, Alcatel-Lucent, R. Rabbat Google, L. Berger, *RFC 5251. Layer 1 VPN Basic Mode*

[9] N. Yamanaka, KOEI Shiomoto, EIJI Oki, *GMPLS TECHNOLOGIES Broadband Backbone Networks and Systems*

[10] L. Andersson and T.Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", *RFC 4026 (Informational)*, March 2005

[11] D. Papadimitriou, "Routing in L1VPN networks", *MPLS* Japan 2006, Tokio October, 2006

[12] National institute of standards and technology, *Links in the GMPLS Lightwave Agile Switching simulator (GLASS)*, [Online], Available: http://www.x.antd.nist.gov/glass/doc/pdf/optical/links_in_Glass_Draft_1.0.pdf

[13] National institute of standards and technology, *The GMPLS Lightwave Agile Switching simulator (GLASS) – An Overview*, [Online], Available: http://wwwx.antd.nist.gov/glass/doc/pdf/optical/GLASS_Overview.pdf

[14] K. Youngtak, et al, *GLASS (GMPLS Lightwave Agile Switching Simulator) - A Scalable Discrete Event Network Simulator for GMPLS-based Optical Internet Advanced Network Technologies Division (ANTD)*, National Institute of Standards and Technology (NIST).