Evaluación de los protocolos OSPF-TE y BGP en funciones de autodescubrimiento para L1VPN sobre GMPLS

Protocol evaluation (OSPF-TE and BGP) regarding autodiscovery mechanisms in L1VPN over GMPLS

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*

Cesar Hernández
Ingeniero Electrónico, magister 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: ca*hernandezs@udistrital.edu.co*

Fecha de recepción: 14 de noviembre de 2011 **Fecha de aceptación: 17 de abril de 2012**

Clasificación del artículo: Investigación

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

Key words: routing, GLASS, GMPLS, L1VPN, protocol, virtual private network.

RESUMEN

Las tecnologías GMPLS (Generalized Multiprotocol Label Switching Architecture) conforman un nuevo framework de protocolos, el cual es una versión extendida de MPLS que no solamente realiza las labores MPLS sino que, además, tiene protocolos especializados para descubrir vecinos, distribuir infor-mación de enlace, realizar administración de la topología, realizar administración de rutas, balanceo de cargas, implementar un control centralizado, manejar ancho de banda bajo demanda y así mismo manejar VPNs (Virtual private networks) a nivel físico-óptico mediante el uso de los dispositivos ópticos adecuados. En este artículo se evaluan los resultados de una simulación del mecanismo de autodescubrimiento en una VPN de capa uno, usando los protocolos OSPF-TE y BGP, utilizando como herramienta de simulacion el simulador GLASS(GMPLS Lightwave Agile Switching Simulator). Con esto se pretende dar una visión al lector de todo el potencial de GMPLS como nuevo framework a implementar y así mismo realizar un análisis mediante el cual se puedan ver las ventajas y desventajas de utilizar OSPF-TE o BGP como protocolo de autodescubrimiento en una VPN de capa uno para un escenario de red especifico.

ABSTRACT

GMPLS (Generalized Multiprotocol Label Switching Architecture) is a new Framework of protocols which is not only an extended version of MPLS. Instead of that It is a specialized group of protocols to discover neighbors, discover link state information, topology management, route management, load balancing, centralized control, bandwidth on demand management and man-agement of VPNs (Virtual private networks) in physical-optical level through the use of adequate optical devices. In this paper are evaluated the results of a simulation for autodiscovery mechanism for a layer one VPN using the OSPF-TE and BGP protocols and comparing them. This paper pre-tends to give a vision to the reader of the potential of GMPLS framework and analyze the advantages and disadvantages to use OSPF-TE instead BGP for autodiscovery purposes in a layer one virtual private network for an specific network scenario.

* * *

1. INTRODUCCIÓN

El objetivo principal de una VPN es extender una red privada dentro de una red pública no segura y no controlada, de manera que se obtenga privacidad y cierta calidad de servicio usando los recursos disponibles en dicha red. Las VPN son una buena opción para obtener comunicaciones seguras a través de una canal no seguro o no controlado, manteniendo costos de mantenimiento bajos y dando así la oportunidad a muchas empresas, gobiernos y entidades, inclusive personas naturales, de tener un canal de comunicación seguro. Sin embargo, en la implementación de estas redes privadas virtuales hay un grado de complejidad alto a la hora de garantizar ciertos servicios como calidad de servicio (QoS), seguridad y enrutamiento, debido a que la red se conforma mediante los recursos, protocolos y equipos que estén disponibles entre el punto A y el punto B, que se quieren comunicar.

Además, estas redes, topologías, protocolos y algoritmos de enrutamiento no están bajo control propio sino bajo el control de los propietarios de las redes que hacen parte de la red pública. El desarrollo de técnicas de conmutación y enrutamiento en los distintos niveles del modelo OSI, tales como MPLS (Multiprotocol Label Switching), GMPLS y las nuevas tecnologías, han

permitido implementar VPNs tanto a nivel de red, a nivel de enlace y así mismo a nivel físico; por lo cual se hace imprescindible poder tener una visión acerca del rendimiento ventajas y desventajas de utilizar distintos tipos de protocolos para el buen desempeño y funcionamiento de las redes privadas virtuales de capa uno. Por esto se propone realizar una simulación del mecanismo de autodescubrimiento de una red VPN capa uno, usando un simulador de redes (GLASS) que utiliza dispositivos capaces de soportar el framework GMPLS de tal manera que sea factible evaluar el desempeño de los protocolos de enrutamiento OSPF-TE y BGP para propósitos de autodescubrimiento en este tipo de redes.GMPLS (Generalized Multiprotocol Label Switching).

2. GMPLS

En la actualidad, para poder enviar datos mediante una red es necesario encapsular el tráfico en varias capas dependiendo del tipo de red al que se desea acceder. Por ejemplo, si se desea enviar información por una red de voz se deben encapsular [1], [2] varias capas como se muestra en la figura 1.

Este encapsulamiento se ha vuelto ineficiente y costoso con el gran volumen de información que se maneja en la redes actualmente, por lo cual nace un nuevo framework que propone una solución a este problema. GMPLS surge con una única interface y un control centralizado. La figura 2 ilustra como seria el nuevo modelo que propone GMPLS

Como se puede ver, sólo se tienen dos capas en las cuales el control y la administración son realizados por GMPLS [3] viéndose de forma clara cómo se puede mejorar la eficiencia y velocidad de transmisión en las redes.

2.1 Enrutamiento optimo Ingeniería de tráfico

Para enmarcar el enrutamiento optimo es necesario tener en cuenta la ingeniería de tráfico TE, ya que esta es la que hace posible que se puedan usar los recursos, aplicación y características de una red para entregar los paquetes, haciendo uso optimo de los recursos de la red. El término ingeniería de tráfico es definido por [4] como una tecnología enfocada en optimizar el rendimiento de redes operacionales y, en general, es un conjunto de mecanismos herramientas y principios científicos que permiten la medida, modelado, caracterización y control de los paquetes de datos que viajan por la red con el fin de alcanzar ciertos objetivos de rendimiento.

Los autores Farrel Adran, Bryskin Igor [4] definen dos objetivos de la ingeniería de tráfico los

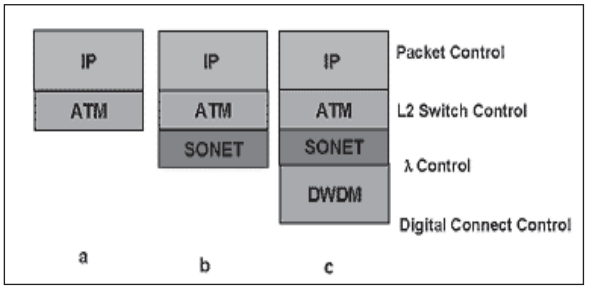

Figura 1. Encapsulamiento de datos, ATM, SONET, DWDM [2].
Fuente: elaboración propia

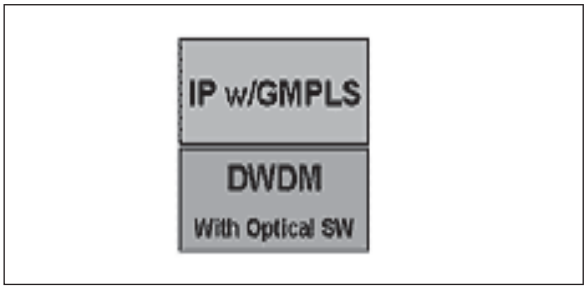

Figura 2. Encapsulamiento GMPLS [2].
Fuente: elaboración propia

cuales están representados por ingeniería de tráfico orientada a tráfico, en la cual el principio es mejorar la calidad de servicio, las tramas de tráfico, minimizar perdida de datos, minimizar los retrasos, garantizar un alto nivel de entrega de datos. El segundo objetivo está dirigido a los recursos de red, el cual es más importante para los proveedores de servicio puesto que implica menor costo de infraestructura y un mejor uso de los recursos. La ingeniería de tráfico está orientada a redes ampliamente utilizadas y con recursos suficientes para proveer rutas alternas de envió de paquetes. Es decir que, para redes en las cuales hay sobreprovisionamiento y que no cuentan con la infraestructura física adecuada, no es viable implementar una solución de ingeniería de tráfico. Como indica el RFC 2702 la ingeniería de tráfico es útil cuando un camino es calculado de manera dinámica y hay más de un camino disponible para enviar el tráfico.

2.2 Mecanismo de autodescubrimiento

Con los recientes desarrollos en las arquitecturas de VPNs basadas en el proveedor, como MPLS capa dos y capa tres, nuevas técnicas han reducido la complejidad operacional de manejar y configurar servicios VPN. Un componente clave de estas técnicas está siendo estandarizado actualmente por la IETF, y es llamado mecanismo de autodescubrimiento VPN [5]. El objetivo principal de este mecanismo es permitir a los miembros de la VPN descubrir dinámicamente la información apropiada para realizar la conectividad entre los diferentes sitios. Todos los dispositivos en una red tienen puertos que son miembros de la VPN y necesitan ser configurados con una lista de miembros VPN, mediante la cual se forma una matriz para poder encontrar la información de direccionamiento cliente-proveedor. El mecanismo de autodescubrimiento VPN permite que la configuración de cambios y adiciones a un nuevo sitio sea limitada únicamente a dispositivos adicionados a ese sitio. Este mecanismo de autodescubrimiento distribuye la información (por ejemplo adición de un nuevo sitio) a todos los PEs que necesitan estar alerta por el nuevo miembro. Esta distribución no requiere intervención de ningún operador.

Para propósitos de usar el mecanismo de autodescubrimiento en el contexto de las L1VPNs los PE que tienen una VPN configurada, se darán localmente:

- La membresía VPN de cada puerto adjunto a un CE.
- Los identificadores de direccionamiento del puerto expresados entre ambos; el espacio de direccionamiento dentro de la VPN y el espacio de direccionamiento del proveedor.
- Opcionalmente, la topología de conectividad como atributo de cada puerto.

El mecanismo de autodescubrimiento VPN para L1VPN puede ser implementado utilizando un servidor centralizado y un plano de control distribuido. El servidor centralizado requiere que dicho servidor sea configurado con una lista de los miembros VPN y su correspondiente lista de direcciones cliente-proveedor (asociaciones CPI-PPI); cada CE y PE tendrán que tener acceso a este servidor para poder solicitar nuevas conexiones. La técnica de plano de control distribuido lleva la información de descubrimiento VPN sobre el plano de control cliente/proveedor. Por ejemplo, la técnica de plano de control usa (MP-BGP) como mecanismo de autodescubrimiento, el cual fue utilizado inicialmente en VPNS basadas en L3MPLS.

Autodescubrimiento BGP: el mecanismo de autodescubrimiento BGP [6] procede donde cada PE advierte la siguiente información a los otros PEs en la VPN: su propia dirección IP y la lista de direcciones privadas y direcciones de proveedor tuplas locales a ese mismo PE y utiliza la infor-

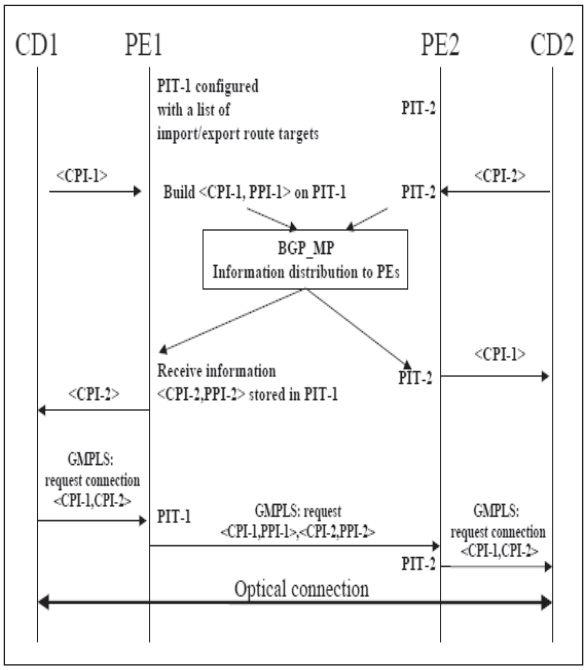

Figura 3. Mecanismo de autodescubrimiento L1VPN para BGP [6].

Fuente: elaboración propia

mación transportada dentro del mecanismo de autodescubrimiento para realizar la resolución de direcciones durante la fase señalización.

La figura 3 ilustra el mecanismo de autodescubrimiento para redes VPN de capa uno y para propósitos de este mecanismo BGP únicamente se ejecuta en la red del proveedor. Cada PE mantiene unas tablas de información de punto VPN llamadas tabla de información de puertos o PITs (por sus siglas en inglés) relacionando la <dirección privada y dirección de proveedor.

En el contexto de una VPN de capa uno, un CE está conectado a un PE por medio de un puerto, donde dicho puerto consiste en varios canales o subcanales cada puerto que conecta un CE con un PE tiene un identificador que es único dentro de la VPN pero no necesariamente debe ser único en varias VPNs, a este identificador se le conoce con el nombre de identificador de puerto de cliente (CPI). Cada puerto en el PE también tiene un identificador único dentro de la red del proveedor y este identificador es conocido como el identificador de puerto del proveedor o PPI (por su sigla en inglés, Provider Port Identifier). Por cada L1VPN que tiene al menos un puerto configurado en el PE, el PE mantiene la tabla de información de puertos (PIT). La PIT contiene una lista de tuplas <CPI, PPI> para todos los puertos dentro de la VPN. Una tabla de información de puertos es llenada con dos tipos de datos:

1. Información relacionada con los puertos CEs adjuntos a los puertos PEs la cual puede ser local al PE o ser recibida del CE.

2. Información recibida de otros PEs mediante mecanismos de autodescubrimiento.

La propagación de información local hacia otros PEs es completada usando las extensiones multiprotocolo de BGP [7].

Autodescubrimiento OSPF-TE: El mecanismo de autodescubrimiento para OSPF-TE se diferencia del de BGP en que, en lugar de usar BGP como protocolo de enrutamiento se usa el protocolo OSPF-TE y la forma en que se transmite la información de autodescubrimiento es distinta.

La figura 4 muestra el servicio L1VPN en modo básico, siendo soportada por OSPF como mecanismos de autodescubrimiento, la figura muestra dos enrutadores interconectados sobre un backbone GMPLS. En esta red, OSPF es utilizado para proveer membrecía, mapeo de puertos e información requerida para el soporte del modo básico de operación.

Para proveer un mecanismo de autodescubrimiento basado en OSPF se debe usar un nuevo tipo de LSA [9] que se refiere como un LSA para L1VPN. Éste lleva información en estructuras TLV (Tipo, Longitud, Valor). El TLV para una

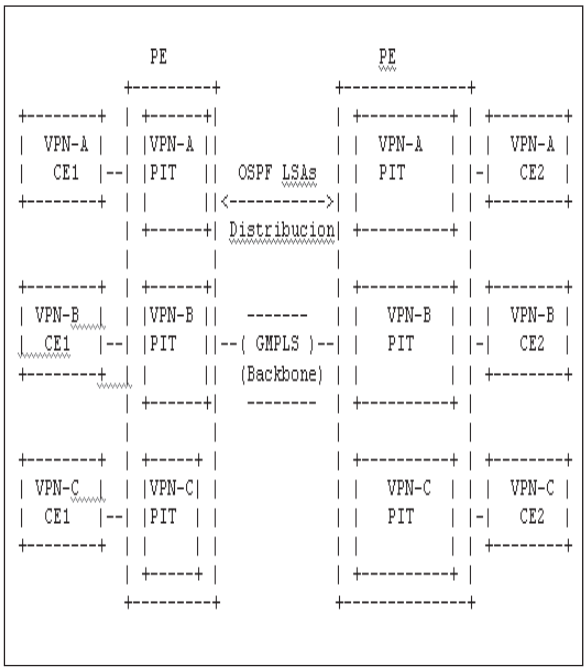

Figura 4. Mecanismo de autodescubrimiento L1VPN para OSPF-TE [8]

red VPN de capa uno es especificado para propagar la membresía VPN y la información de puertos. También puede llevar información de ingeniería de tráfico [10] específica como tipo de link, Id de link, interface local, interface remota, métrica ingeniería de tráfico, máximo ancho de banda, mínimo ancho de banda reservable, ancho de banda no reservado y grupo administrativo [11], [12].

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) [13] - [15] el cual es un simulador capaz de soportar el Framework de GMPLS. La selección de la herramienta de simulación se realiza basada 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; 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), MPLS, y parámetros de QoS.

3.1 Simulación

Al inicio de la simulación se ejecutan los algoritmos de ruta OSPF-TE y BGP para formar las primeras tuplas de las PIT de cada cliente como se muestra en la figura e iniciar el proceso de autodescubrimiento VPN.

Se realizan tres simulaciones para cada uno de los protocolos en una red que no tiene ninguna falla y se verifican los resultados para la salida de los dos protocolos.

3.1.1 Simulación sin fallas de red

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 simulaciones ejecutadas para cada uno de los protocolos OSPF-TE y BGP con sus respectivos algoritmos de enrutamiento, Dijkstra y Path Vector respectivamente, para un escenario en el cual no se presenta ninguna falla en la red y el mecanismo de autodescubrimiento opera de forma normal. Estas simulaciones se realizan con el fin de determinar el comportamiento y realizar un análisis de este proceso bajo las condiciones normales de la red que son las que más se presentan y las que pueden dar una visión más acertada para realizar una comparación.

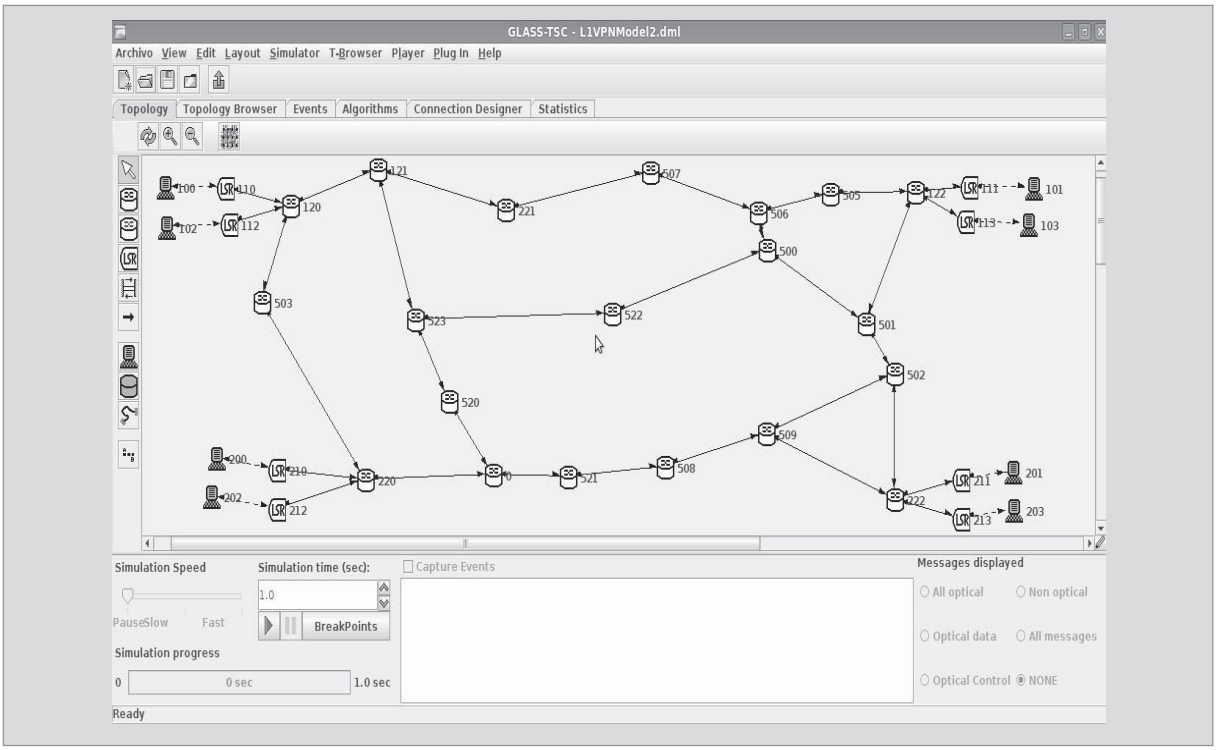

Figura 5. Topología de la red.
Fuente: elaboración propia

Red sin falla								
Simulación 1								
Algoritmo	Rutas calculadas	Saltos promedio	Retraso promedio	Distancia	Throuhgput	Bloqueo	BW(Gbps)	Utilización
ShortestPathDistanceSRLG (OSPF-TE)	2	8	0,002095925	58,6	1	0	-1	-1
Path Vector BGP	2	8	7,895411545	58,6	1	0	-1	-1
BESTFIT	-1	-1	-1	-1	-1	0	4	0,006369
Simulación 2								
Algoritmo	Rutas calculadas	Saltos promedio	Retraso promedio	Distancia	Throuhgput	Bloqueo	BW(Gbps)	Utilización
ShortestPathDistanceSRLG (OSPF-TE)	2	8	0,00255456	58,6	1	0	-1	-1
Path Vector BGP	2	8	7,45687244	58,6	1	0	-1	-1
BESTFIT	-1	-1	-1	-1	-1	0	4	0,0056547
Simulación 3								
Algoritmo	Rutas calculadas	Saltos promedio	Retraso promedio	Distancia	Throuhgput	Bloqueo	BW(Gbps)	Utilización
ShortestPathDistanceSRLG (OSPF-TE)	2	8	0,00354547	58,6	1	0	-1	-1
Path Vector BGP	2	8	7,25884782	58,6	1	0	-1	-1
BESTFIT	-1	-1	-1	-1	-1	0	4	0,0078564

Figura 6. Resultado de 3 simulaciones sin falla de red.
Fuente: elaboración propia

3.1.2 Simulación con fallas de red

Aunque las condiciones normales de una red implican que esta no presenta fallas, es indispensable conocer cómo es el comportamiento de los mecanismos de autodescubrimiento al momento de una o más fallas debido a que esto podría dar una visión más amplia acerca de la eficiencia del algoritmo en cuanto a recuperación en caso de falla de un nodo o enlace. Se presenta la topología de red ilustrando los puntos de falla de enlace en la figura 7.

Las fallas se presentan en diferentes tiempos durante la simulación, obligando a recalcular rutas a los algoritmos y reenviar los paquetes por la ruta alternativa calculada. Se ilustra el resultado de la simulación en la figura 8.

4. RESULTADOS

Durante la fase de establecimiento de la L1VPN se crean las tablas de información de puertos en cada uno de los PEs para que estos conozcan los miembros de la VPN. La distribución de la información de dichas tablas se realiza mediante el mecanismo de autodescubrimiento, el cual es una manera de llevar la información de los miembros VPN por la red del proveedor. Esta distribución de información se realiza de manera automática mediante los protocolos OSPF-TE o BGP, que son los protocolos de enrutamiento que tiene el framework GMPLS. La evaluación de estos protocolos con su ingeniería de tráfico bajo métricas seleccionadas determinará cuál es el más adecuado para el autodescubrimiento. Cada protocolo es evaluado en este análisis de

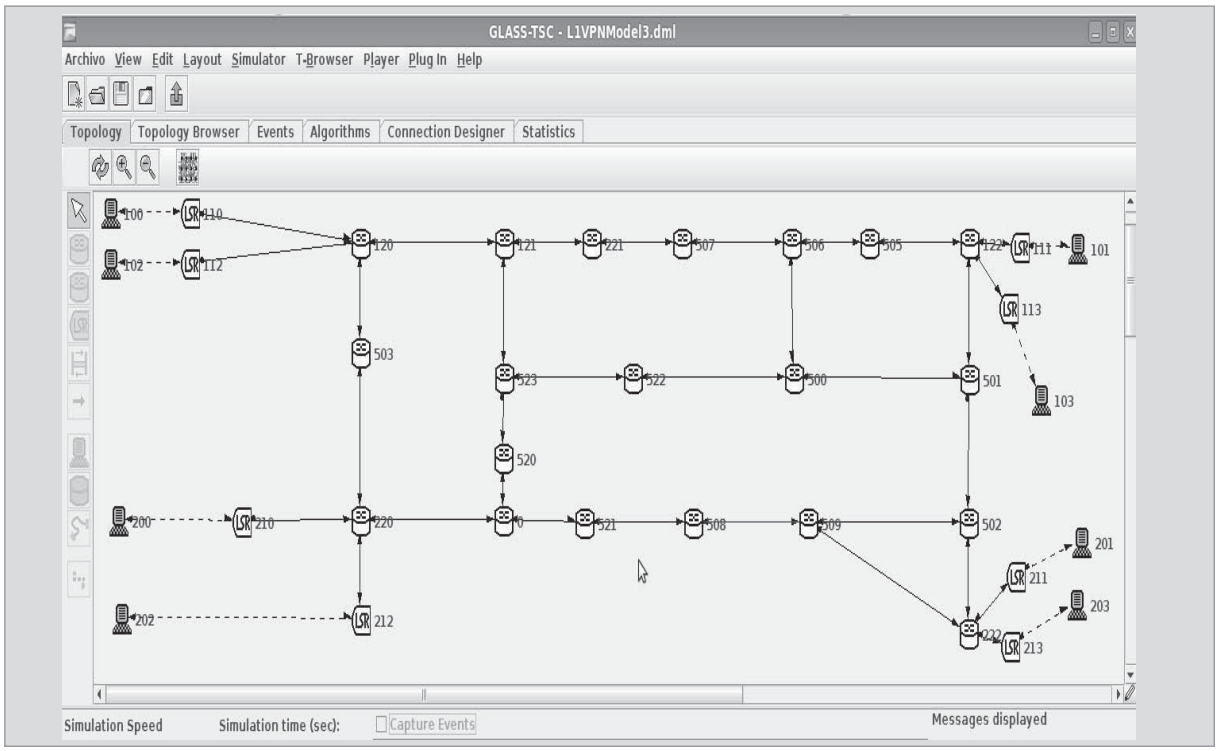

Figura 7. Topología de la red ilustrando fallas en rojo.
Fuente: elaboración propia

Falla enlace 508 - 509								
Simulación 1								
Algoritmo	Rutas calculadas	Saltos promedio	Retraso promedio	Distancia	Throuhgput	Bloqueo	BW(Gbps)	Utilización
ShortestPathDistanceSRLG (OSPF-TE)	2	10	0,00268450	85,65	1	0	-1	-1
Path Vector BGP	2	10	17,23526372	85,65	1	0	-1	-1
BESTFIT	-1	-1	-1	-1	-1	0	4	0,006369
Simulación 2								
Algoritmo	Rutas calculadas	Saltos promedio	Retraso promedio	Distancia	Throuhgput	Bloqueo	BW(Gbps)	Utilización
ShortestPathDistanceSRLG (OSPF-TE)	2	10	0,00234123	85,65	1	0	-1	-1
Path Vector BGP	2	10	18,75685465	85,65	1	0	-1	-1
BESTFIT	-1	-1	-1	-1	-1	0	4	0,006369
Simulación 2								
Algoritmo	Rutas calculadas	Saltos promedio	Retraso promedio	Distancia	Throuhgput	Bloqueo	BW(Gbps)	Utilización
ShortestPathDistanceSRLG (OSPF-TE)	2	10	0,00314567	85,65	1	0	-1	-1
Path Vector BGP	2	10	13,12352567	85,65	1	0	-1	-1
BESTFIT	-1	-1	-1	-1	-1	0	4	0,006369

Figura 8. Resultado de tres simulaciones con falla de red.
Fuente: elaboración propia

resultados bajo un conjunto de métricas que se describe a continuación.

Rutas calculadas:

Este tipo de métrica comprende el número de rutas calculadas por el protocolo evaluado OSPF-TE y BGP. Este parámetro depende de las restricciones con las cuales se ejecuta el algoritmo. Para el caso en particular de esta simulación se seleccionaron las restricciones de ancho de banda, solicitando un ancho de banda de 22.5 Gbps y que los caminos calculados tuvieran un diferente SRLG (SHARED RISK LINK GROUP), es decir, que las rutas calculadas no compartan recursos compartidos que puedan llegar a fallar. Como se puede observar en la gráfica de la figura 9, el número de rutas calculadas es exactamente el mismo ya que los dos algoritmos tienen un panorama entero de la red pero su forma de generarlo es la que varía. Este comportamiento es el mismo para las tres simulaciones en las cuales la red no presenta fallas. Para la red que presenta falla el número de rutas disminuye a una sola ruta (la ruta de backup SRLG) calculada.

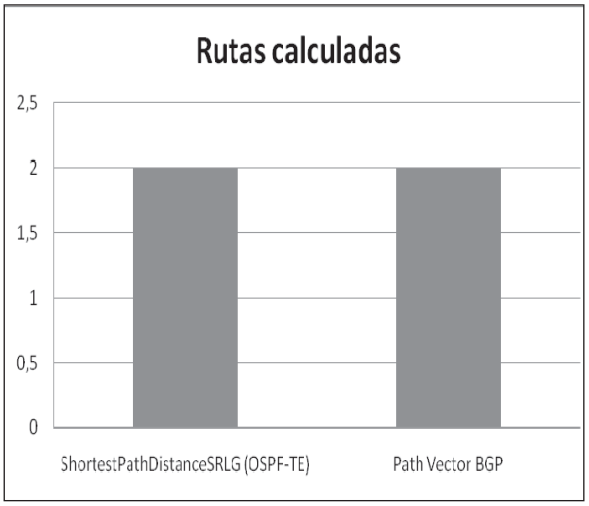

Figura 9. Gráfica rutas calculadas para OSPF y BGP.
Fuente: elaboración propia

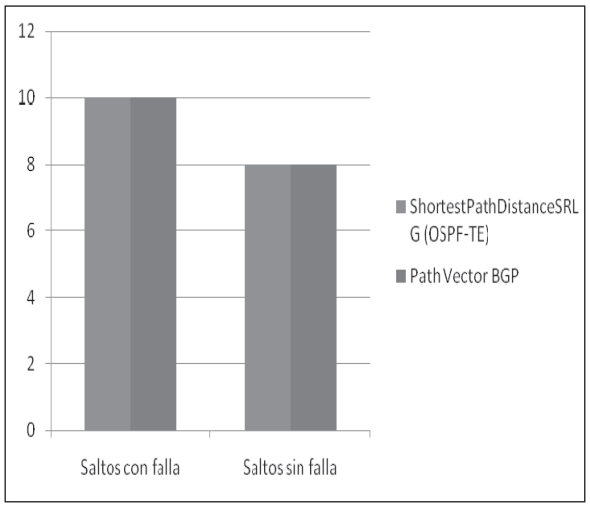

Figura 10. Promedio de saltos para OSPF y BGP.
Fuente: elaboración propia

4.1 Número promedio de saltos

Otra de las métricas utilizadas es la distancia entre un punto y otro. La selección de esta métrica se realiza debido a que, a mayor distancia entre nodo y nodo la probabilidad de pérdida aumenta así como el retraso entre fuente y destino. Este factor se tiene en cuenta como una métrica por el algoritmo de enrutamiento al calcular la ruta más corta hasta el destino. Hay que tener en cuenta que la ruta calculada puede no ser la más corta, puesto que el cálculo también depende de otras métricas como el ancho de banda y el retardo. Como la figura 10 lo ilustra, el número promedio de saltos para la simulación en la red donde no se presentan fallas es de ocho saltos (OXC (122) – OXC (501) - OXC (502) - OXC (509) - OXC (508) - OXC (521) - OXC (0) - OXC (220). El número de saltos se incrementa en dos saltos al realizar la simulación en la red que falla ya que se elige el siguiente camino de ruta más corta.

4.2 Retraso promedio en segundos

El análisis más importante con respecto al autodescubrimiento y a los protocolos es el tiempo de convergencia de los algoritmos, ya que de este depende el cálculo de las rutas y la distribución de las PIT para el establecimiento de la VPN. Este tiempo de retraso afecta la inclusión de nuevos clientes en la VPN, la distribución inicial de rutas y la recuperación en caso de fallas, ya que el proceso de autodescubrimiento se realiza mediante la información adicional que lleva cada protocolo por lo cual está muy ligado al desempeño del mismo, así como a sus ventajas y desventajas. Se realiza un análisis de la convergencia de cada uno de los protocolos al hallar la PIT en cada lado de la VPN. y se verifica cuál de los dos protocolos es más eficiente y tiene un menor tiempo de convergencia. Sin embargo, esto no significa que se afirme que un protocolo deba ser utilizado en vez de otro debido a que las características de los mismos son diferentes y están orientados a prestar servicios en diferentes áreas de la red. Lo que se pretende es que se tenga un conocimiento de los resultados que se puedan esperar y que la decisión de usar uno u otro se tenga en cuenta este análisis. Así mismo, el retardo también depende de las restricciones de TE, tanto de ancho de banda, retardo, numero de saltos y SRLG que se utilizaron para calcular las rutas que cumplan con dichas restricciones.

Al realizar las simulaciones y observar las figuras 11 y 12 se puede observar que los tiempos de convergencia de los algoritmos OSPF-TE son menores al del algoritmo BGP, por lo cual la generación de las PIT para el método de autodescubrimiento basado en OSPF-TE es menor que el método de autodescubrimiento basado en BGP. El tiempo de convergencia es mayor para BGP cuando se presentan fallas de red, lo anterior sucede a causa de la misma naturaleza del algoritmo de vector de ruta, que es una versión modificada de un algoritmo de vector de distancia y que por ende hereda muchas de sus ventajas como de sus desventa-

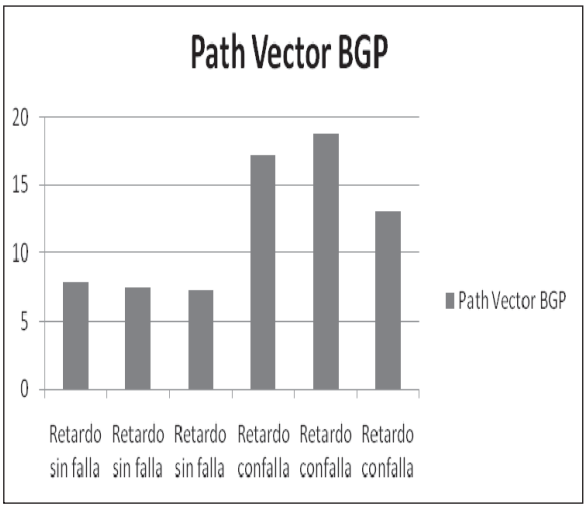

Figura 11. Resultado de las simulaciones para BPG.
Fuente: elaboración propia

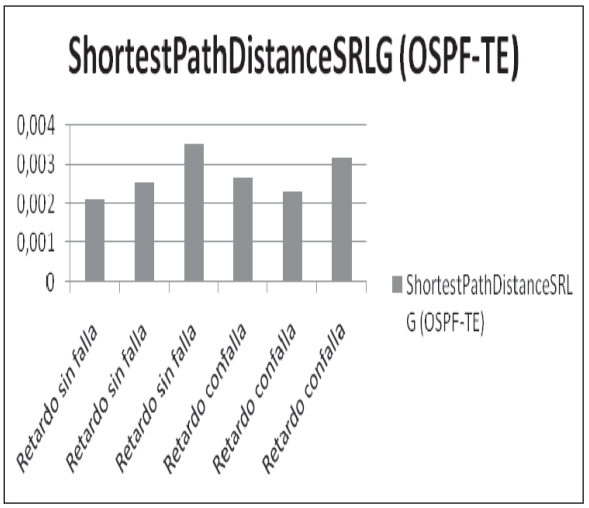

Figura 12. Resultado de las simulaciones para OSPF-TE.
Fuente: elaboración propia

jas. Entre estas desventajas se puede ver que el tiempo de convergencia frente a malas noticias (caída de un enlace, caída de un nodo) es muy alto.

Como se puede ver en las figuras 11 y 12, en las cuales se simulan los protocolos de red, los tiempos de convergencia entre un protocolo y el otro son muy grandes. Es posible concluir que la utilización de OSPF-TE es mejor que el uso de BGP en cuanto a funciones de autodescubrimiento, sin embargo, se debe tener presente que BGP mantiene un conjunto de parámetros que hacen que su tiempo de convergencia sea mayor, como por ejemplo el temporizador de sesión BGP Hold Down Timer (este indica qué tanto esperará un enrutador para escuchar mensajes de sus vecinos, este tiempo por lo general está en 180 segundos, sin embargo, para efectos de la simulación se disminuyó a 6 segundos). Este temporizador incrementa en 180 segundos, en el mejor de los casos, los tiempos de convergencia de BGP puesto que la falla es advertida 180 segundos después de que sucede.

Otro de los aspectos a tener en cuenta es que OSPF-TE es un protocolo que consume más recursos de procesamiento en los enrutadores ya que las tablas de enrutamiento se distribuyen por toda la red y el cálculo de las rutas más cortas es más complejo. De la simulación como tal, en cuanto a tiempo de convergencia, se puede concluir que OSPF-TE tiene muchas más ventajas que desventajas con respecto a BGP ya que es capaz de distribuir en un menor tiempo las tablas de información de puerto en una red de capa uno sobre un Framework GMPLS.

También se debe tener en cuenta que OSPF-TE no es un protocolo diseñado para ser utilizado en pasarelas exteriores, por lo cual esta comparación únicamente se puede realizar a nivel interior. La decisión de aplicar un protocolo u otro depende de los requerimientos que se tengan, ya sea el tipo de red, el tamaño de la misma, las políticas de enrutamiento o la calidad de servicio requerida. La comparación de ambos protocolos obedece a una comparación dentro de un mismo sistema autónomo y no tiene alcance para varios sistemas autónomos debido a que, en estos casos, se necesita

un protocolo de pasarela exterior y OSPF-TE no cumpliría.

Dentro de los parámetros que restan por analizar están: el bloqueo, el ancho de banda y la utilización del canal, en los cuales la simulación no arroja resultados diferentes para los protocolos OSPF-TE o BGP como tales sino para el algoritmo de BESTFIT (algoritmo de asignación de longitud de onda), algoritmo encargado de procesar las posibles rutas encontradas por los algoritmos de selección de ruta (OSPF-TE o BGP), realizar el proceso de asignación de recursos y de validar que el camino seleccionado es alcanzable y existe. Por este motivo es que el algoritmo BESTFIT es el que consume los recursos de ancho de banda, de bloqueo y de utilización. Los resultados en todas las simulaciones para el ancho de banda, el bloqueo y la utilización son prácticamente los mismos en las seis simulaciones llevadas a cabo, por lo que se puede concluir que para una red del tamaño de la representada acá este parámetro no afectaría en nada el análisis de cada algoritmo.

5. CONCLUSIONES

Por las mismas definiciones y utilización de los protocolos BGP y OSPF- TE es complejo determinar el comportamiento de cada algoritmo como tal para evaluar si el mecanismo de autodescubrimiento L1VPN es más óptimo para alguno de los protocolos en particular. Sin embargo, teniendo en cuenta los resultados de la simulación que se llevó a cabo para el modelo de servicio seleccionado, la topología ilustrada, los protocolos usados, los algoritmos seleccionados y la configuración de la red simulada, se puede afirmar que la utilización de OSPF-TE, como método de autodescubrimiento para redes virtuales de capa 1 L1VPN, es más eficiente en este escenario debido a los tiempos de convergencia que muestra BGP. Lo anterior aplicaría manejando la VPN dentro de una red intradominio en la cual se maneja iBGP y OSPF-TE. Esta comparación es viable realizarla ya que a nivel de redes virtuales de capa 1 se puede implementar cualquiera de estos dos protocolos para propósitos de autodescubrimiento. El tema de definición de cuál protocolo es el más apto para esta labor aún es discutido por expertos, puesto que la implementación de uno u otro protocolo depende de factores como el costo, el uso, la eficiencia entre algoritmos Path Vector y Dijkstra y las políticas.

El uso de BGP u OSPF-TE como mecanismo de autodescubrimiento depende no solo del rendimiento de los algoritmos sino de otros factores que influyen también para decidir entre uno u otro. En la comunidad de expertos hay discusiones [22] acerca de las ventajas y desventajas de ambos protocolos para este mecanismo, aunque la mayoría de expertos están de acuerdo en usar BGP y únicamente BGP como mecanismo de autodescubrimiento, tanto en este documento como en la misma discusión se evalúan escenarios que deben ser tenidos en cuenta al seleccionar el protocolo. Entre estos factores de selección se encuentran:

El tiempo que se tenga para implementar una solución u otra, debido a que la implementación de BGP es más compleja pues es necesaria la implementación de la TE para este protocolo, mientras que OSPF ya cuenta con esta adición, lo que hace que OSPF sea más fácil de implementar a nivel de tiempo. Así mismo, el framework de GMPLS está mucho más enfocado hacia OSPF con su TE que hacia BGP.

Costo, este factor depende de la necesidad ya sea de tener un protocolo sencillo para redes virtuales de capa 1 2 ó 3 o si la necesidad es tener únicamente un protocolo para la TE de redes de capa 1 solamente, esta selección puede afectar en poca o gran medida los costos de implementación dependiendo del protocolo seleccionado.

Rendimiento, este factor concierne directamente al comportamiento de cada uno de los algoritmos path vector vs Link State Protocol, en cuanto a rendimiento, lo cual fue analizado en este trabajo.

En relación al rendimiento de los protocolos, se estaría hablando de path vector vs link state protocol teniendo en cuenta que la relación de impacto y propiedades de ambos son diferentes por la naturaleza de cada uno de ellos. Se deben tener en cuenta también otros factores que afectan el resultado del tiempo de convergencia entre los protocolos, como son el caso de los tiempos de espera que tiene BGP, los cuales son bastante amplios haciendo que la convergencia en BGP sea mucho más lenta que para OSPF-TE.

REFERENCIAS

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

[2] R. Gallager, "MPLS training guide – building multiprotocol label switching networks", Cap. 6*, Introduction to Multi-Protocol Lambda Switching (MPλS) and Generalized Multi-Protocol Label Switching* (GMPLS).

[3] X. Hesselbach, M. Huerta, O. Calderon, "Departamento de ingeniería telemática. Universidad politécnica de Catalunya", *Introduccion a las tecnologias MPLS, MPλS, y GMPLS*, Barcelona: España.

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

[5] L. Andersson and T.Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", *RFC4026 (Informational)*, March, 2005.

[6] 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.

[7] T. Takeda, NTT; D. Brungard, AT&T Labs; D. Papadimitriou, AlcateL; H. Brahim Ould, Nortel, "Layer 1 Virtual Private Networks: Driven Forces and Realization by GMPLS", *IEEE Communications Magazine*. July, Vol 43, No. 7, 2005.

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

[9] D. F. Hamid Ould-Brahim; P. Ashwood-Smith; Nortel Networks; Y. Rekhter; Juniper Networks, E. C. Rosen; Cisco Systems, *BGP based Auto-Discovery echanism for Optical VPNs IETF*, Minneapolis, March, 2001.

[10] T. Bates, R. Chandra, D. Katz, and Y. Rekhter, "Multiprotocol Extensions for BGP-4", *RFC 4760,* January, 2007.

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

[12] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, M. and J. McManus, "Re-

quirements for Traffic Engineering Over MPLS", *RFC 2702,* September 1999.

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

[14] K. Kompela and Y. Rekhter, "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", *RFC4203,* October, 2005.

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