Tecnura
ISSN: 0123-921X
tecnura@udistrital.edu.co
Universidad Distrital Francisco José de Caldas
Colombia

SALCEDO, OCTAVIO; PEDRAZA, LUIS F.; ESPINOSA, MÓNICA
Evaluación de redes MPLS/VPN/BGP con rutas reflejadas
Tecnura, vol. 16, núm. 32, abril-junio, 2012, pp. 107-116
Universidad Distrital Francisco José de Caldas
Bogotá, Colombia

Evaluación de redes MPLS/VPN/BGP con rutas reflejadas

Network assessment MPLS/VPN/BGP with mirror routes

Octavio Salcedo
Ingeniero en Sistemas, magíster en Teleinformatica, estudiante de Doctorado. Docente de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia. *ojsalcedop@udistrital.edu.co*

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

Mónica Espinosa
Ingeniera en Sistemas. Investigadora de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia. *mespinosa@udistrital.edu.co*

Clasificación del artículo: Revisión de Tema (Recreaciones)

Fecha de recepción: Agosto 22 de 2011 **Fecha de aceptación: Febrero 27 de 2012**

Palabras clave: BGP, desempeño, MPLS, ruta reflejada, VPN.

Key words: BGP, performance, MPLS, route reflection, VPN.

RESUMEN

En este artículo se realiza el estudio y evaluación de las redes MPLS/VPN/BGP a nivel de Backbone considerando el RFC 4364, sobre ambientes de intranet.

El algoritmo BGP se evalúa en escenarios Route-Reflection para la conexión de los enrutadores CE (CustomerEdge) y PE (ProviderEdge) de la Red MPLS desde el establecimiento de VRF (Virtual Routing and Forwarding)y su rendimiento en la conexión a través de la VPN.

ABSTRACT

In this paper, we study and evaluate the MPLS/VPN/BGP backbone level according to RFC 4364, focusing on connecting intranet systems.

The algorithm evaluates BGP Route Reflection scenarios for connecting routers CE (Customer Edge) and PE (Provider Edge) Network since the establishment of MPLS VRF (Virtual Routing and Forwarding) and its performance in connection through the VPN.

* * *

1. INTRODUCCIÓN

El objetivo de los carriers de comunicación es transportar y mejorar el rendimiento sobre el cliente, por ello los backbone basados en MPLS/VPN son ampliamente usados a nivel mundial, teniendo la ventaja de ser transparentes para los clientes y adicionalmente brindan un gran nivel de seguridad [1]. En estas redes se busca trabajar con grandes niveles de convergencia, por ello, se evalúan múltiples mecanismos en [2], implementando las rutas reflejadas.

Para tal fin se evaluarálas redes MPLS/BGP/VPN y la aplicación de rutas reflejas, utilizando el Opnet como herramienta de simulación para realizar el análisis.

2. MPLS/BGP/VPNs

Los elementos de la Red MPLS/VPN/BGP son el Customer Edge (CE), Provider Edge (PE) y Provider Core (P) como se muestra en la Fig. 1 [3]. El Backbone MPLS se compone por los enrutadores PE y P, a nivel del cliente se tiene el enrutador CE. El enrutador PE es el elemento que tiene contacto directo con la Red del cliente y el enrutador P es el enrutador interno de la Red MPLS el cual no tiene contacto con los clientes directamente. Los enrutadores PE y P trabajan en modo de conmutación de etiquetas en los que se construyen caminos (LSP) los cuales usan un protocolo de distribución de etiquetas (LDP), cuando un PE envía una dirección VPN a través de la Red MPLS para identificar el grupo de la VPN la Red le asigna un Label específico y asigna también

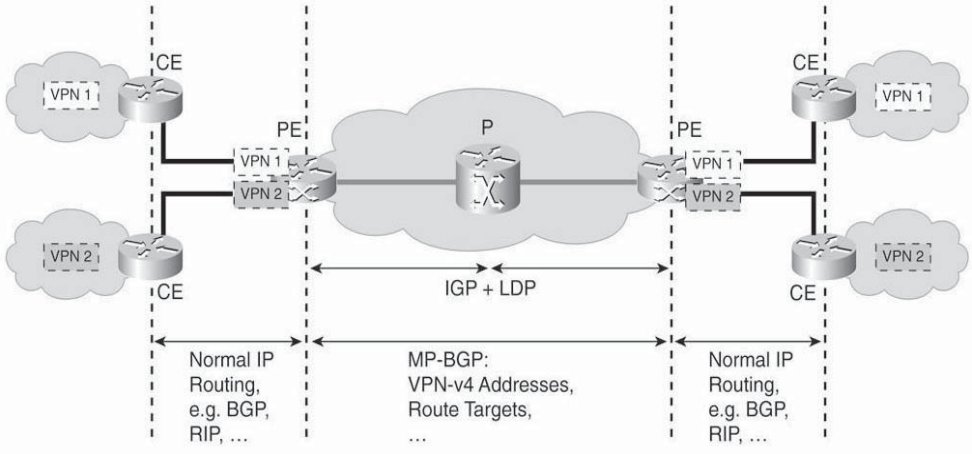

Fig. 1. Red MPLS.

una etiqueta exterior, identificando el PE de salida. La etiqueta en el interior de la Red es utilizada por el PE de Salida para determinar el puerto de la VPN al que el paquete debe ser direccionado [1]. El enrutador CE (Customer Edge) y el enrutador PE (Provider Edge) soporta múltiples niveles de encaminamiento y sus respectivas tablas son llamadas VRF (virtual route forwarding). Las VRFs son lógicamente independientes y pueden llegar a contener traslape de direcciones en otras VRFs.

Las VPNs se forman mediante la definición del cliente que accede a ser miembro de una VRF y este se encuentra en la tabla formada por los sitios que el enrutador PE ha creado. El enrutador PE hace uso de BGP (Border Gateway Protocol) para la propagación de la información acerca de las rutas de la VPNs, así como las etiquetas en el interior de MPLS.

3.MPLS-VRF

Los nodos que pertenecen a otras VPNs se pueden adjuntar a un mismo nodo PE. Dado que estas VPNs podrían compartir el mismo rango de direcciones IP teniendo direcciones privadas. La RFC 4364 [1] introduce el concepto de VRF con el fin de apoyar las direcciones de solapamiento así como la opción de separación de tráfico por opciones de seguridad. El uso de las VRFs sobre los enrutadores PE asegura que el tráfico sobre una VPN no sea direccionado a otra. Las principales características que las VRFs pueden soportar son:

- Las direcciones se superponen, lo que permite la reutilización de las direcciones IP en el enrutador PE para diferentes VPNs.
- Reutilización de los puertos TCP/UDP lo cual permite usar los mismo puertos en diferentes VRFs.
- El Backbone MPLS puede interactuar en dos planos diferentes de implementación: plano de encaminamiento y plano de control de datos.

3.1 Plano Encaminamiento

El plano de encaminamiento está a cargo de la ruta de aprendizaje y proceso de distribución. Cuando el enrutador PE aprende una nueva ruta del nodo CE, un nuevo label es asignado a esta ruta, este label es conocido como “Label de la ruta VPN”.

El enrutador PE sabe el conjunto de nodos que están involucrados en la VPN, así que hace uso de BGP para propagar la asociación de la ruta de entrada y “Label de la ruta VPN”. Cuando un nodo PE recibe tal asociación, se inserta la información de enrutamiento en el VRF correspondiente y designa la fuente del mensaje como “BGP Nexthop”.

El enrutador PE en primer lugar debe identificar a cual VRF le corresponde el paquete IP, ya que para este solo es permitida una VRF. Cuando el paquete IP llega de diferentes VPNs el enrutador PE asocia una determinada VRF. Si no hay una VRF asociada el enrutador PE asociará el enrutamiento por defecto.

Habría tres diferentes resultados de la búsqueda de VRF. Si el destino es otro CE ajuntado a un mismo PE, el PE transmitiría directamente el paquete IP. Si el paquete IP debe atravesar el backbone, deberá buscar el ‘BGP Nexthop’ y el tráfico ingresa directamente al PE, el enrutador PE agrega ‘VPN routelabel’ y envía el tráfico que ingresa a la red MPLS.

3.2 Planosdecontrol de datos

En primer lugar, el enrutador PE debe identificar que el paquete IP que ingresa al nodo pertenezca a la VRF, para el tráfico entrante y tráfico saliente del enrutador PE. Por tanto, el PE enrutador hace una búsqueda sobre la tabla de rutas IP asociadas a la VRF. Si no hay VRF vinculada a una interfaz, el enrutador PE utilizará la ruta predeterminada, ver Fig. 2.

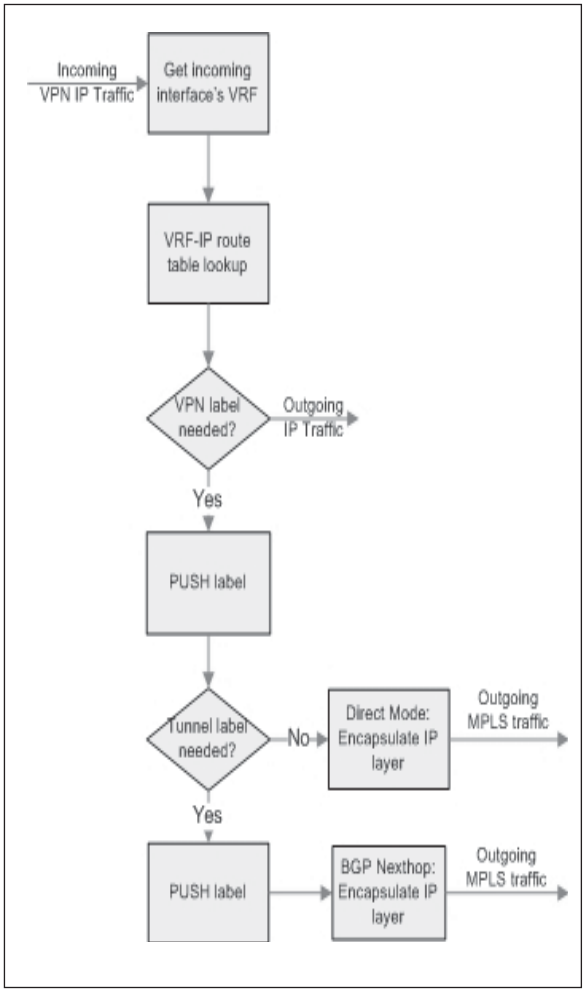

Fig. 2. Diagrama de flujo de tráfico de entrada en el enrutador PE

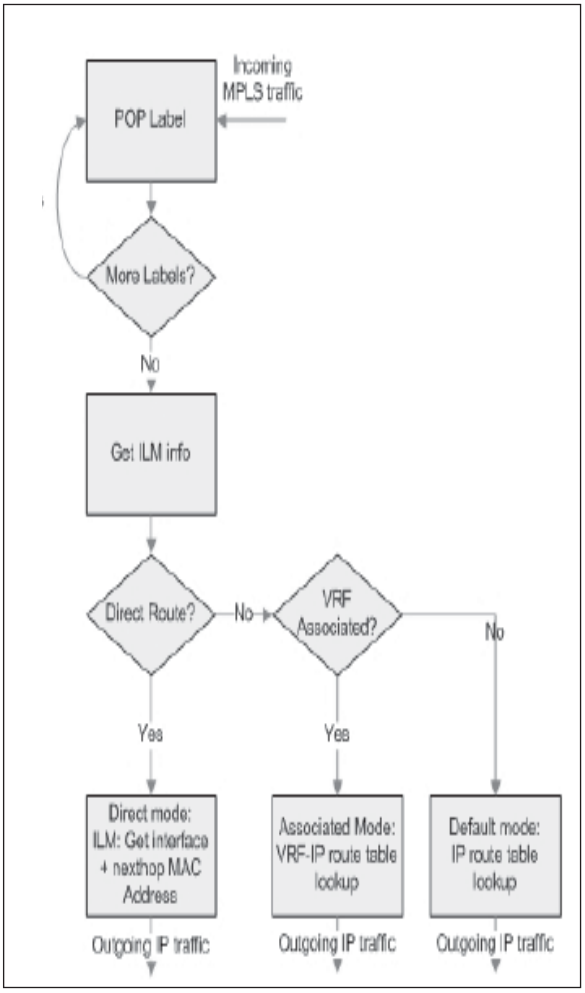

Fig. 3. Diagrama de flujo de tráfico de salida de enrutador PE

En la Fig. 2 y Fig. 3 se muestranlos correspondientes diagramas de bloques que resumen el comportamiento de PE enrutador cuando llega el tráfico MPLS, utilizando la función PUSH para colocar las etiquetas dentro del tráfico MPLS y la función POP para quitar las etiquetas.

La información se propaga del PE local a todos los demás enrutadores PE en la red utilizando BGP. Para garantizar la unicidad de prefijos de diferentes VPNs, un identificador único llama la ruta distinguisher (RD), creando una nueva familia de direcciones para VPN IPv4 [4].

El protocolo BGP permite manejar diferentes familias de direcciones, se utiliza para distribuir el resultado de la publicación de rutas para el PE remoto. Estos, a su vez, son el filtro en la recepción, de tal manera que solo podrán ingresar el subconjunto de rutas que provengan del enrutador CE [4].

Por ejemplo, en la Fig. 3, se mantiene el anuncio PE2 de PE1, porque 2 de VPN sitio gris se adjunta a la misma. Sin embargo, PE3 no, porque no tiene los sitios pertenecientes a la VPN gris [4].

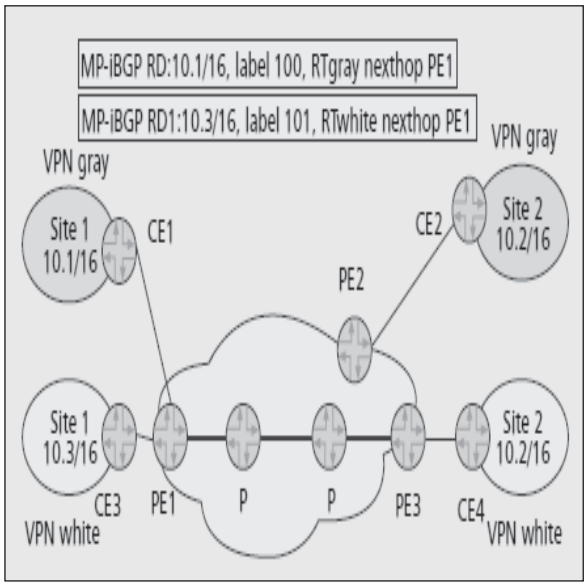

Fig. 4. Encaminamiento VPNs

La filtración se realiza mediante el etiquetado de rutas con una o más comunidades ampliadas, llamadas ruta de objetivos (RT) y la configuración de la exportación de políticas para los enrutadores de la red. Por ejemplo, en la Fig. 4 la ruta subred 1 perteneciente a la de VPN que se encuentra en el sitio caracterizado con gris en el que se origina la ruta de exportación por PE1 y etiquetados con objetivo "gris", PE2 está configurado con una importación ruta de destino "gris" y, por tanto, mantiene la ruta, permitiendo la escalabilidad y buen desempeño. En el caso de una plena conectividad entre todos los sitios en una VPN, una sola ruta de destino puede utilizar por VPN tanto para la importación y la exportación. Sin embargo, las complejas políticas de control de acceso y el acceso muy granular de control se puede lograr mediante el uso de múltiples rutas distintos objetivos y políticas de importación y exportación.

La información de encaminamiento de VPN (tras el paso de la ruta distinguida) almacena en el PE las distintas rutas virtuales de enrutamiento y transmisión (VRF) por la VPN. El Tráfico perteneciente a una VPN es transferido de acuerdo con la transmisión de la tabla VRF. Esto asegura la distinción de tráfico entre las diferentes VPNs, ya que la búsqueda se realiza solo en la tabla que contiene prefijos pertenecientes a la VPN. La Fig. 5 muestra la transmisión por separado en los cuadros creados por PE1 VPN de blanco y gris para la otra VPN.

La cuestión es cómo se transmite el tráfico sobre la base de la información por la VPN. El tráfico que llega al PE sobre la interfaz PE-CE se identifica como perteneciente a una particular VPN, basado en la interfaz de entrada. El mapeo entre las interfaces y las VPNses configurado en el enrutador PE. Por ejemplo, en la Fig. 5 el tráfico PE1 que llega de la interfaz CE1 es transmitido sobre la VPN gris.

El tráfico que llega a una máquina (local) PE de otro (control remoto) PE debe ser etiquetado en la transmisión, de una forma que determina a los CE, los cuales son los receptores del tráfico.

Esto se logra utilizando un label de MPLS, llamado label VPN. El tráfico en la misma VPN puede ser etiquetado con diferentes etiquetas, ya que estas etiquetas no se identifican realmente con la VPN, pero sí con la transmisión del próximo salto, de esta forma simple se permite la comunicación de las diferentes LANs. El PE local recoge la etiqueta de la VPN y lo envía junto con la ruta publicada al PE. También se instala la transmisión del Estado que transmita el tráfico etiquetado con la etiqueta de VPN para el correcto CE.

Las etiquetas del PE remoto direccionan el tráfico destinado a la VPN con esta etiqueta. Por ejemplo, en la Fig. 5, el enrutador PE1 publicó la ruta para la subred 10.1/16 perteneciente al sitio 1 en la VPN del sitio que también obtiene la VPN gris y la etiqueta 100. La publicación de la ruta en la subred 10.3/16 perteneciente a la VPN de sitio 1 blanco contiene la etiqueta de VPN 101. PE1 espera el tráfico entrante a ser etiquetado con pre-

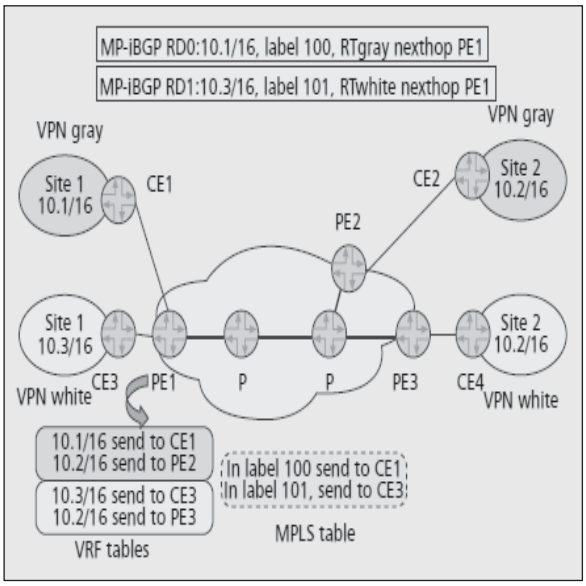

Fig. 5. Tablas de Encaminamiento VPNs

fijos 100 para10.1/16 en la gama de grises para la VPN. Se espera prefijos 101 para la etiqueta en la gama de 10.3/16 VPN blanco. El enrutador PE1 ha enviado el estado de la transmisión MPLS por tráfico directo con la etiqueta 100 al sitio1 de la VPN gris, ver Fig. 5.

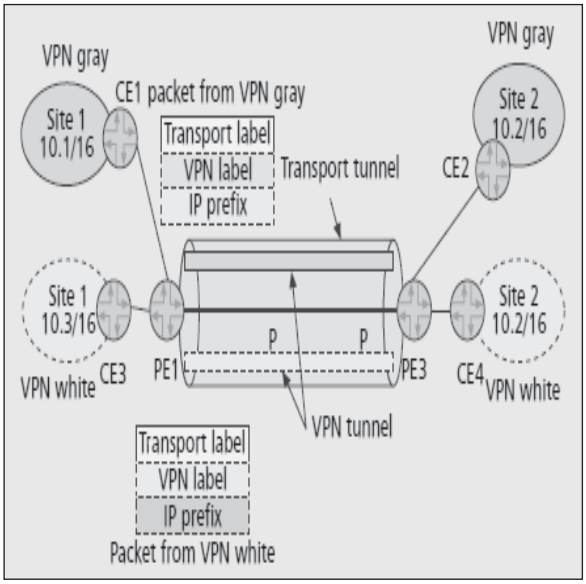

Fig. 6. Túneles de transporte MPLS

Normalmente, este reenvió se puede implementar de diferentes formas, pero una de las más utilizadas es mediante la construcción de túneles PE-PE (también se refiere a túneles de transporte), utilizando RSVP-TE (Protocolo de Reserva de Recursos de Tránsito) o LDP (Label Distribution Protocolo), lo que permite utilizar atributos (métricas) que garantizan la utilización de la ingeniería de tráfico.

De esta manera, el tráfico perteneciente a múltiples VPNs se remite a lo largo de la misma en el túnel del núcleo MPLS, y varios túneles VPN se llevan en el mismo túnel de transporte, como se muestra en la Fig. 6.

3.3 Eficiencia de las VPNs

La eficiencia para la investigación está enfocada en el tiempo de ejecución del encaminamiento en el plano de control. El enrutador PE anuncia todas las rutas de todos los sitios conectados a él mediante BGP. BGP es un protocolo diseñado específicamente para manejar un gran número de rutas [5]. Dispone de buenas propiedades de escala, ya que ha incorporado en los mecanismos control de flujo para el envío y recepción de mensajes, que permiten el control de error y de flujo, y no requiere de anuncios periódicos de información de enrutamiento, basándose solo en actualizaciones incrementales. Además, BGP lleva un único período de sesiones de las rutas de todas las distintas redes VPN, por lo que el número de sesiones de BGP no depende del número de VPN, en lugar de ello, es proporcional el número de compañeros a los que la información de enrutamiento se distribuye, que en el peor de los casos, es el número de otros enrutador PE en la red.

3.4 Reflector de rutas

Los Reflectores de Ruta (RR) reducen el número de sesiones BGP que debe mantener un PE. En

lugar de igualitarios con todos las demás proveedores de servicios en la red, los proveedores de servicios entre pares con el RR se convierten en lo que se llama ruta del reflector clientes.

Así, cada PE mantiene un número constante de peerings independientemente del número de proveedores de servicios en la red. La adición de un nuevo PE en la red no requiere la configuración de BGP. El RR soluciona el problema añadiendo un nuevo PE a la red sin la necesidad de reconfigurar BGP a todos los demás proveedores de servicios. Sin embargo, el RR puede convertirse en un potencial cuello de botella en la expansión de las siguientes maneras:

- Como un elemento de la red que mantiene todas las rutas de VPN (limitación de memoria).
- Como el único elemento responsable del tiempo de propagación de todos VPN ruta cambios (de limitación de la CPU) [6]. Una forma de evitar el mantenimiento de todas las rutas de VPN en una ubicación centralizada es la partición entre varios reflectores. La Fig. 7 muestra una red de rutas que pertenecen a tres VPNs: VPNa, VPNb, y VPNc.

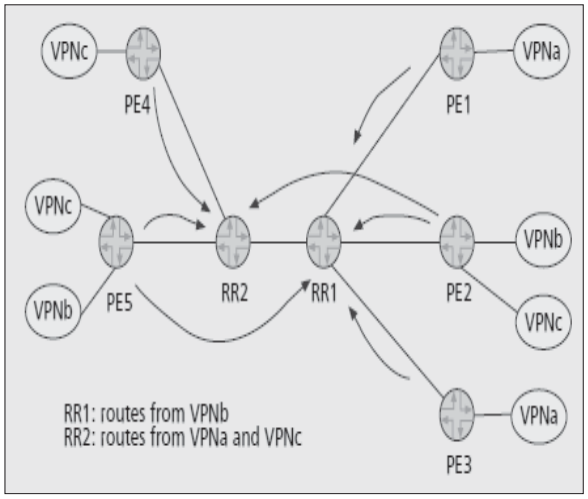

Fig. 7. Aplicación de rutas reflejadas.

En el escenario de una verdadera red, la carga de la CPU en el RR no crece proporcionalmente con el número de sus compañeros, por el contrario, tiende a aumentar mucho más rápido. BGP actualiza a menudo el cálculo de la actualización y lo repite a todos los clientes. La eficacia de esta estrategia depende de cómo los clientes son similares en términos de control de flujo.

Los grupos de RR pueden crecer en número de clientes, y estos clientes hacen que las redes se vuelvan más heterogéneas (como es el caso en la vida real donde se utiliza el despliegue equipos de diferentes fabricantes y versiones), la eficacia de las actualizaciones, disminuye y aumenta la carga de la CPU. Por tanto, la única solución para resolver realmente las limitaciones de la CPU en el RR, es reducir el número de VPNs.

3.5 Reducción del número de vía VPN anuncios

Para reducir el número de cambios que se originaron en el RR, el PE debe ser capaz de informar a la RR las rutas en las que está interesado. Así, la ruta la publicidad puede ser filtrada por el RR y no en el PE, ahorrando recursos de CPU en el RR y en el PE. El protocolo de mejora para la aplicación de esta funcionalidad se denomina ruta limitada [7]. La idea es volver a utilizar el mismo mecanismo BGP utilizado para la distribución de la accesibilidad a la información de filtrado de publicidad.

3.6 Simulador OPNET

OPNET es un simulador que es muy robusto y potente desde el punto de vista del usuario, el cual permite evaluar el rendimiento de ambientes de redes, entre otras especificaciones de

simulación, para diferentes redes de comunicaciones. En OPNET los eventos son simulados de forma discreta permitiendo observar el comportamiento de la red [8].

3.7 Modelo Jerárquico en OPNET

OPNET tiene cuatro herramientas de desarrollo para representación de modelos, estas herramientas son: editores de redes, editores de nodos y procesos, los cuales son organizados en modelos jerárquicos que son soportados para los modelos por niveles como se observa en la Fig. 8.

El análisis de la Simulación en OPNET para VPN MPLS permite la configuración de los parámetros MPLS como se muestra en la Fig. 9, los parámetros configurados son la información de la interface, túnel virtual, parámetros CSPF y etiquetas [8].

En la Fig.10 [8] se observa la red MPLS a simular, en donde inicialmente se tiene un modelo de red en el cual se interconectan 3 empresas por medio de conexiones PPP_SONET_OC3

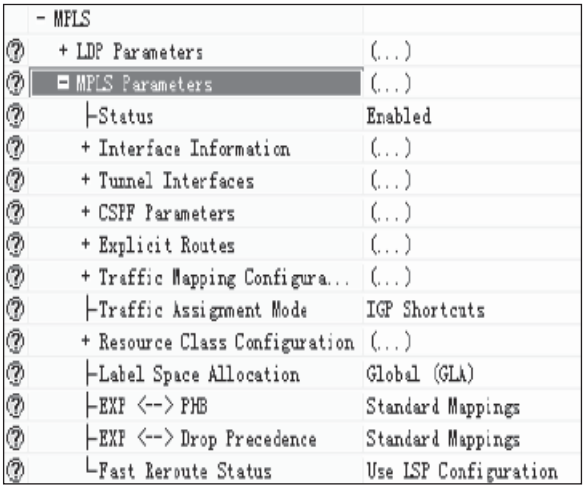

Fig. 9. Configuración de parámetros para MPLS.

teniendo para este ejemplo enrutamiento estático entre PE y CE, cada PE configura LSP y el protocolo entre los PE es BGP la siguiente capa de simulación a trabajar es el modelo de nodos Fig.11 [8], este modelo fue extendido para el enrutador PE, se puede observar el compartimiento en protocolo que es seminal para las redes de comunicaciones. En la Fig.12 [8] se observa el modelo de procesos de la simulación con la configuración de parámetros inicial para la implementación.

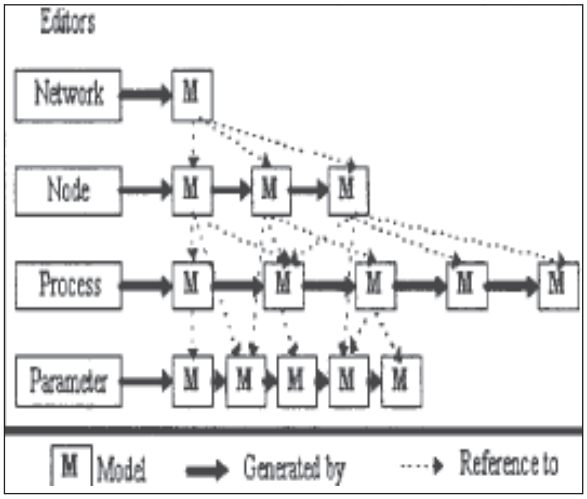

Fig. 8. Modelos OPNET.

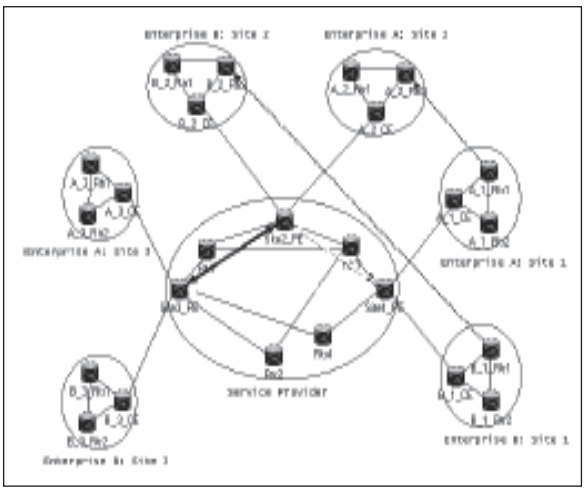

Fig. 10. Modelo de simulación de Red.

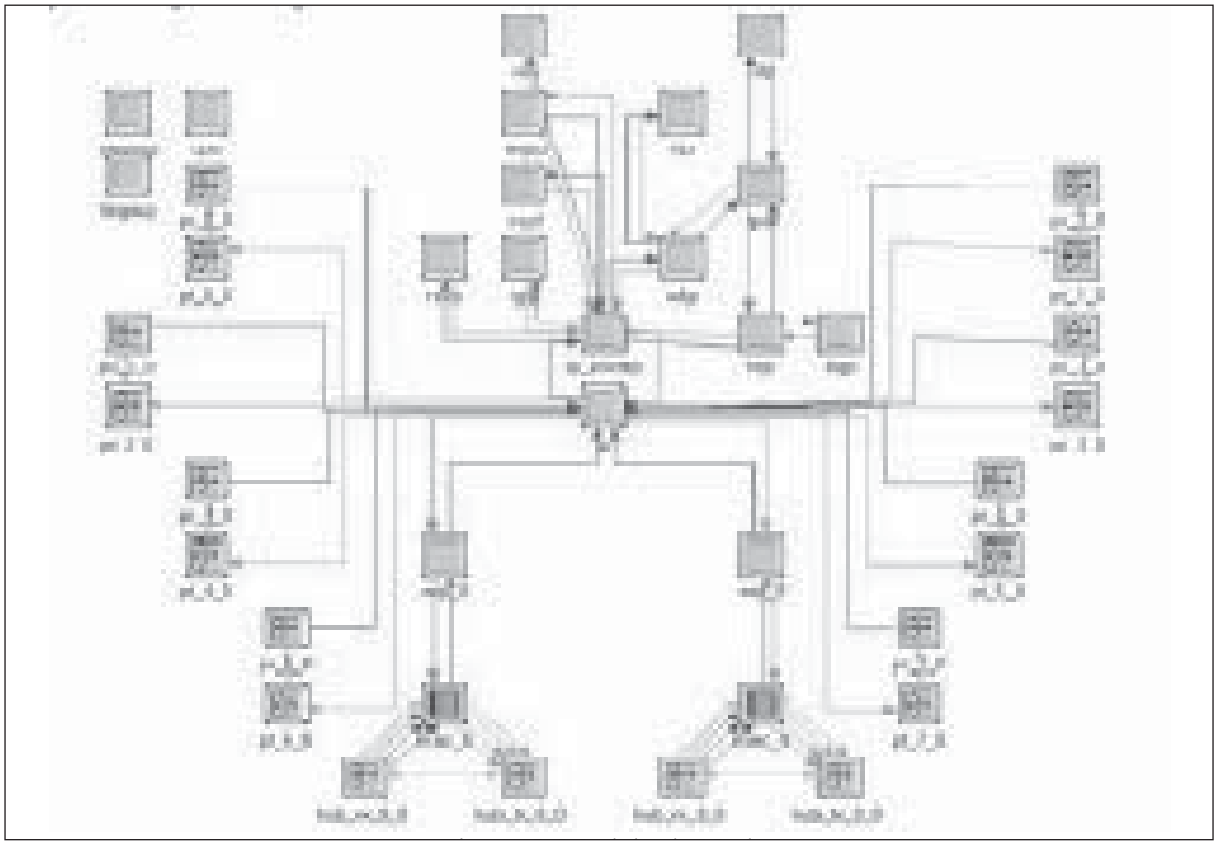

Fig. 11. Modelo de nodos

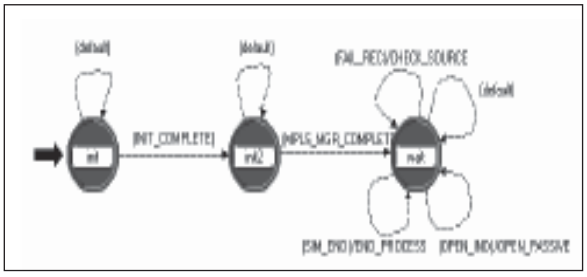

Fig. 12. Modelo de procesos

4. CONCLUSIONES

La solución BGP / MPLS IP VPN permite un creciente tamaño del despliegue de una VPN (en términos de VPN, sitios y rutas), añadiendo más enrutadores y teniendo más capacidad de la red. Esto es posible debido a que los enrutadores CE intercambian rutas con el enrutador PE que está conectado al proveedor, en lugar de hacerlo con cada uno de los otros enrutadores CE en la VPN.

BGP es usado para la distribución de información de VPN entre proveedores de servicios.

Además, el uso de la ruta de control de acceso se puede aprovechar para reducir el número de rutas de anuncios enviados a un BGP con conexión peer con el objetivo de filtrado de ruta de la VPN. El rendimiento es mejorado por el despliegue utilizando rutas de los reflectores, ya que reduce la tramitación de carga en la ruta del reflector.

REFERENCIAS

[1] E. Rosen and Y. Rekhter, *BGP/MPLS IP Virtual Private Networks (VPNs),* RFC 4364, Feb., 2006.

[2] A. Ala, M. Essaaidi, "Fast Convergence Mechanisms and Features Deployment Within Operator Backbone Infrastructures", *Microwave Symposium (MMS), 2009 Mediterrannean*. 2010.

[3] M. Behringer and M. Morrow,*MPLS VPN Security,* Indianapolis: Cisco Press, 2005.

[4] I. Minei and P. R Marques, "Scalability Considerations in BGP/MPLS IP VPNs", *Communications Magazine, IEEE*, vol. 45, Issue 4, 2007.

[5] J. Pico, J. Fajardo, A. Munoz and A. Ferro, "MPLS-VRF Integration: Forwarding Capabilities of BGP/MPLS IP VPN in GNU/Linux", *Optical Network Design and Modeling, 2008. ONDM 2008. International Conference on*,12-14 March, 2008.

[6] P. Márques andR. Bonica, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs),* RFC 4684.

[7] P. Márques, *BGP Route Reflection in Layer 3 VPN Networks*, [En línea]. Available: http://www.juniper.net/solutions/literature/white_papers/200160.pdf

[8] X. Chang, "Network Technology Research Center, School of EEE, Nanyang Technological University, Singapore 639798", *WSC '99 Proceedings of the 31st conference on Winter simulation: Simulation a bridge to the future,* vol. 1, 1999.