MPLS Y SU APLICACIÓN EN REDES PRIVADAS VIRTUALES (L2VPNs Y L3VPNs)

Javier Rafael Gómez Valdivia, Ms C.
ETECSA, Sancti Spíritus, Sancti Spíritus, Cuba, javier@ssp.tel.etecsa.cu

Carmen Moliner Peña, Dr C.
CUJAE, Ciudad de la Habana, Ciudad de la Habana, Cuba, carmen@tesla.cujae.edu.cu

Resumen

La necesidad de una arquitectura que reuniera los beneficios de las tecnologías anteriores hizo que en 1997 el IETF (*Internet Engineering Task Force*) a través del Grupo de Trabajo MPLS crearan una nueva arquitectura: MPLS (*Multiprotocol Label Switching*).

MPLS posibilita a los operadores de telecomunicaciones ofrecer un número de servicios imposibles de brindar con las técnicas tradicionales de enrutamiento IP, entre los que se encuentran Calidad de Servicio (QoS, *Quality of Service*) en redes IP, Ingeniería de Tráfico (TE, *Traffic Engineering*) y Redes Privadas Virtuales (MPLS/VPN). MPLS permite integrar el nivel IP con cualquiera de las técnicas existentes en el nivel de enlace, como FR (*Frame Relay*), ATM (*Asynchronous Transfer Mode*), Ethernet, etc.

En el presente trabajo se analiza el estado actual de las MPLS/VPN de Capa 3 (BGP MPLS/VPN) y de Capa 2 (EoMPLS, ATMoMPLS, FRoMPLS, PPPoMPLS, HDLCoMPLS), logrando arribar a conclusiones de utilidad para Proveedores de Servicios.

1. Introducción

Las necesidades crecientes de intercambio de datos, el proyecto de Informatización de la Sociedad Cubana y los programas especiales imponen nuevas metas. Lo anterior, unido al crecimiento previsto de aplicaciones (videoconferencias, telemedicina, teletrabajo, educación a distancia y otros servicios de banda ancha) incrementan a un ritmo elevado las solicitudes de recursos de la red, por lo que se debe planificar los cambios necesarios en las mismas, tanto más cuando sean SP (*Service Providers*), para proveer en tiempo dichos servicios.

Con las VPNs se soporta aplicaciones intra/extranet, integrando voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. El presente trabajo tiene como objetivo caracterizar las VPN sobre MPLS de Capa 3 y 2, ya que los SP necesitan transportar tanto tráfico de Capa 2 como de Capa 3. Una red privada virtual (VPN, *Virtual Private Network*) se construye a base de conexiones realizadas sobre una infraestructura compartida con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada real.

El estudio de las MPLS/VPN como técnica emergente posibilita recomendar y enfrentar futuras soluciones necesarias en las redes de datos. Con este trabajo se obtendrá elementos que podrán contribuir a futuras proyecciones de redes, así como elementos fundamentales para la comercialización de nuevos servicios.

2. BGP MPLS/VPN (RFC 2547)

Con la llegada del MPLS, que combina los beneficios de la conmutación de Capa 2 con los del enrutamiento de Capa 3, es posible construir una tecnología que permite combinar los beneficios de un modelo de VPN superpuesto (como seguridad y aislamiento entre clientes) con los beneficios que en cuanto a enrutamiento brinda un modelo de VPN par a par. La tecnología llamada BGP MPLS/VPN también hace posible un número de topologías muy difíciles de implementar en los modelos de VPN anteriores (superpuestas o par a par); MPLS también presenta los beneficios de ser orientado a conexión a través del establecimiento de trayectorias de conmutación de etiquetas (LSP, *Label Switch Path*) las que son creadas antes del flujo de tráfico, basados en información de la topología, por la ejecución del conjunto de protocolos de la familia MPLS.

2.1 Ejemplo: MPLS/VPN de Capa 3 en la Red del SP

Con el objetivo de explicar mejor los conceptos de BGP MPLS/VPN se utiliza un ejemplo hipotético. Imaginemos un SP, que ofrece servicios MPLS/VPN de Capa 3. El proveedor de servicio del ejemplo tiene dos puntos de presencia POP (*Point of Presence*), uno que llamaremos PE1 y uno que llamaremos PE2, estando los POP enlazados a través de dos enrutadores de núcleo nombrados P1 y P2.

En el ejemplo el SP tiene dos clientes: Empresa A que conformara la VPN-A, con el sitio-1 y el Sitio-2 conectado a PE1 y el sitio-3 conectado a PE2 y la Empresa B que conformara la VPN-B con el sitio-1 conectado a PE2 y el sitio-2 conectado a PE1. La red descrita anteriormente es mostrada en la Figura 2.1.

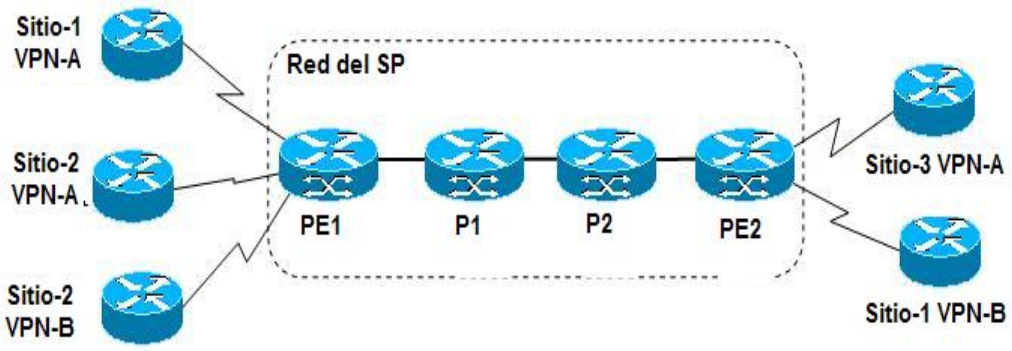

Figura 2.1 Red y sus Clientes.

Acorde a las siguientes terminologías los enrutadores en la Figura 2.1 tienen las siguientes funciones:

- ✓ Los enrutadores PE1 y PE2 que enlazan la red con sus clientes son enrutadores de la frontera del proveedor de servicio (PE, *Provider Edge*).
- ✓ Los enrutadores P1 y P2 que no tiene conexiones directas con los clientes son enrutadores del núcleo de la red del proveedor (P, *Provider*).
- ✓ Los enrutadores de los clientes conectados al PE1 en el sitio-1 y sitio-2 de la Empresa A y en el sitio-2 de la Empresa B al igual que los conectados al PE2 en los sitio-1 y sitio-3 de la Empresa B y la Empresa A respectivamente son enrutadores de la frontera del cliente (CE, *Customer Edge*).

Asumiendo que ambas Empresas la A y B, siguen la misma convención para el direccionamiento de sus VPN, los sitios-1 usan direcciones IP públicas, mientras que los sitios-2 y el sitio-3 de ambas Empresas, usan espacios de direcciones IP privadas (red 10.0.0.0).

El direccionamiento IP usado por estas dos empresas está resumido en la Tabla 2.1.

Compañía	Sitio	Subred
Empresa A	Sitio-1	192.168.2.0/24
	Sitio-2	10.5.1.0/24
	Sitio-3	10.5.2.0/24
Empresa B	Sitio-1	192.168.8.0/24
	Sitio-2	10.5.1.0/24

Tabla 2.1 Espacio de direcciones de Empresa A y Empresa B.

El proveedor de servicio pretende ofertar un servicio basado en el modelo par a par (no un número de túneles IP sobre IP), pero hay que tener en cuente un número de detalles porque el espacio de direcciones IP de los sitios-2 conectados al mismo enrutador PE1 se solapan.

El solapamiento de direcciones usualmente resultado del uso de direcciones IP privadas en las redes de los clientes es uno de los mayores obstáculos para el desarrollo de implementaciones VPN par a par. La tecnología MPLS/VPN de Capa 3 brinda una solución eficiente a este dilema. Cada VPN tiene su propia tabla de envío y enrutamiento en el enrutador, así cualquier cliente o sitio que pertenezca a una VPN le está sólo permitido el acceso a un grupo de rutas contenidas dentro de la tabla. Cualquier enrutador PE en una red MPLS/VPN contiene un número de tablas de enrutamiento por VPN y una tabla de enrutamiento global que es usada para alcanzar los otros enrutadores en la red del proveedor, así como destinos alcanzables externos, como por ejemplo, el resto de Internet. Efectivamente un número de enrutadores virtuales son creados en un único enrutador físico, como se muestra en la Figura 2.2 para el caso del enrutador PE1 de la red.

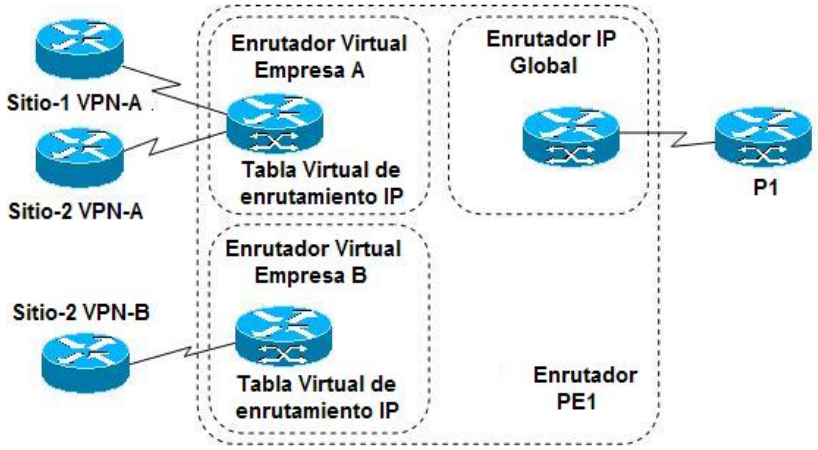

Figura 2.2 Enrutadores Virtuales creados en un enrutador PE1.

El concepto de enrutadores virtuales les permite a los clientes usar cualquier espacio de direcciones globales o privadas en cada VPN. Para cada cliente o sitio perteneciente a una VPN existe un solo requerimiento, que el espacio de direcciones sea único dentro de la VPN. La exclusividad de direcciones no es requerida entre VPNs, excepto cuando dos VPN, que comparten el mismo espacio de direcciones privadas quieran comunicarse.

A cada enrutador virtual no solamente está asociada la tabla de enrutamiento virtual, hay más estructuras comprendidas en el enrutador virtual:

- ✓ Una tabla de envío que se obtiene de la tabla de enrutamiento.

- ✓ Un grupo de interfaces a usar por la tabla de envío.
- ✓ Reglas que controlan la importación y exportación de rutas desde y hacia la tabla de enrutamiento de la VPN.
- ✓ Un grupo de protocolos de enrutamiento, los cuales adicionan información en la tabla de enrutamiento de la VPN, incluyendo rutas estáticas.
- ✓ Enrutadores asociados con los protocolos de enrutamiento que son usados para llenar la tabla de enrutamiento de la VPN.

La combinación de las tablas de enrutamiento IP VPN y la asociada tabla de envío IP VPN es llamada Instancia de Enrutamiento y Envío VPN (***VRF***, *VPN Routing and Forwarding*).

2.1.1 Interconexión de Redes Privadas Virtuales

El ejemplo del SP utilizado hace creer que una VPN está asociada solamente con un VFR en un enrutador PE, aunque esto puede ser verdad en el caso de que los clientes de las VPN no necesiten conectividad con otras VPN, la situación pude hacerse más compleja y requerir más de un VFR por cliente VPN conectado a un enrutador PE.

Imaginemos que se desea ampliar los servicios ofertados con un servicio de voz sobre IP (***VoIP***, *Voice over IP*) con pasarelas (*gateways*) a la Red Pública de Voz localizadas en PE1 y PE2, como se muestra en la Figura 2.3.

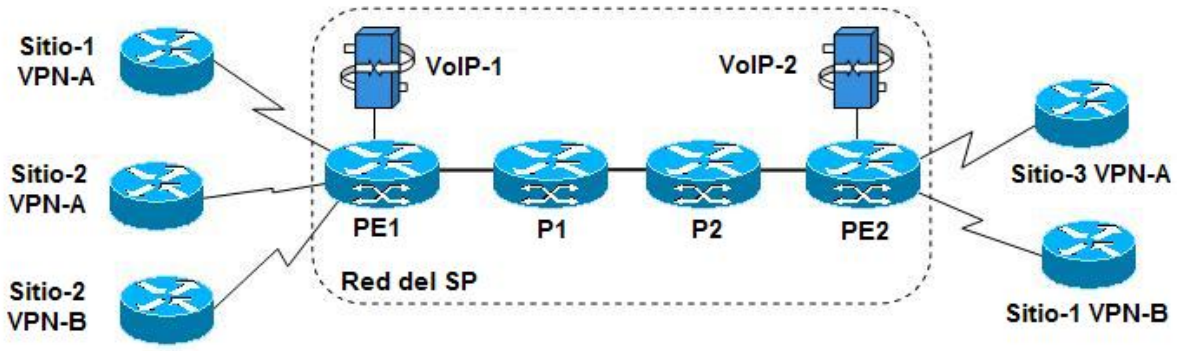

Figura 2.3 Pasarelas VoIP en red.

Una de las alternativas posibles es situar las pasarelas de VoIP en una VPN separada que llamaremos VPN-VoIP para incrementar la seguridad del nuevo servicio creado.

El direccionamiento IP de las pasarelas es como se muestra en la Tabla 2.2.

Ubicación de la Pasarela VoIP	Dirección IP de la Pasarela VoIP
VoIP-1	200.55.33.32
VoIP-2	200.55.37.15

Tabla 2.2 Direcciones IP de las Pasarelas VoIP en la red

Ambos clientes Empresa A y Empresa B deciden usar el servicio de VoIP, pero sólo para sus sitios-1, los demás sitios en el ejemplo no necesitan hacer llamadas de larga distancia. Estos requerimientos nos llevan a un problema interesante, los sitios-1 de ambas compañías necesitan estar en dos VPNs, la VPN de sus empresas para alcanzar sus sitios remotos y la VPN-VoIP para alcanzar las pasarelas de VoIP. La conectividad necesaria se ilustra en la Figura 2.4

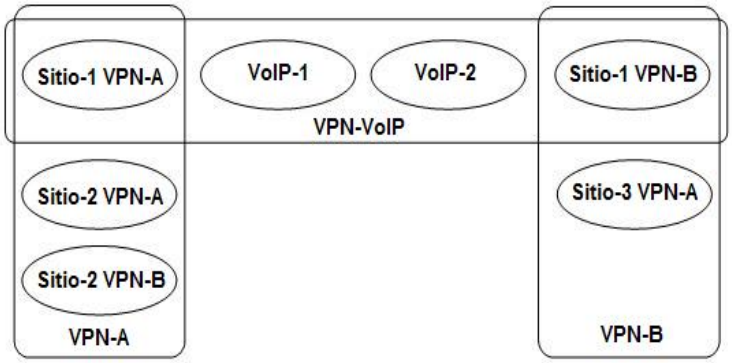

Figura 2.4 Conectividad necesaria en VPNs del ejemplo.

Para soportar requerimientos de conectividad similares a los de la Figura 2.4, la arquitectura MPLS/VPN de Capa 3 se apoya en el concepto de sitios (***sites***), donde una VPN es un arreglo de uno o múltiples sitios. Una VPN es esencialmente una colección de sitios compartiendo información de enrutamiento común, lo cual significa que un sitio puede pertenecer a más de una VPN si este sostiene rutas desde VPN separadas. Esto nos permite construir intranets y extranets, así como cualquier otra topología de las descritas anteriormente. Una VPN en la arquitectura MPLS/VPN de Capa 3 puede consecuentemente ser dibujada como una comunidad de intereses o un grupo cerrado de usuarios, lo cual es dictado por la visibilidad de enrutamiento que los sitios puedan tener.

El concepto de VRF introducido anteriormente puede ser modificado para soportar el concepto de sitios que pueden residir en más de una VPN, por ejemplo, el sitio-1 de la Empresa A no pueden usar el mismo VRF que el sitio-2 de la Empresa A conectado al mismo enrutador PE1. El sitio-1 Empresa B necesita acceso a las pasarelas de VoIP, por lo que las rutas hacia esta pasarela deben estar en el VRF para este sitio. Por lo que VFR es una colección de rutas que pueden estar disponibles para un sitio en particular o para un grupo de sitios conectados a un enrutador PE. Estas rutas pueden pertenecer a más de una VPN.

La relación entre las VPNs, sitios y VRFs pueden ser resumidas en la siguiente regla, la que puede ser usada como base para cualquier definición de VRF en una red MPLS/VPN de Capa 3.

Regla: todos los sitios que comparten la misma información de enrutamiento (usualmente esto significa que pertenecen al mismo grupo de VPNs) están autorizados a comunicarse directamente con los demás y están conectados al mismo enrutador PE pueden ser ubicados en una VRF común. (Guichard y Pepelnjak, 2000)

Usando esta regla, el mínimo grupo de VRFs en la red es la segunda columna (VRF), en la Tabla 2.3.

Enrutador PE	VRF	Sitios en la VRF	VPNs que pertenecen al VRF
PE1	Sitio-1 Empresa A	Sitio-1 Empresa A	VPN-A, VPN-VoIP
	Sitio-2 Empresa A	Sitio-2 Empresa A	VPN-A
	Sitio-2 Empresa B	Sitio-2 Empresa B	VPN-B
	VoIP-1	Pasarela VoIP-1	VPN-VoIP
PE 2	Sitio-3 Empresa A	Sitio-3 Empresa A	VPN-A
	Sitio-1 Empresa B	Sitio-1 Empresa B	VPN-B, VPN-VoIP
	VoIP-2	Pasarela VoIP-2	VPN-VoIP

Tabla 2.3 VRF en los enrutadores PE de la red.

Con lo estudiado anteriormente se arriba a que no existe un mapeo directo entre una VPN y un VRF, por lo que el enrutador necesita conocer cuales rutas debe insertar en cada VRF. Esto es resuelto con la introducción de otro concepto en la arquitectura MPLS/VPN de Capa 3 las **RT** (***route target)***, atributo que le permite a un enrutador conocer cuáles rutas insertar en cada VRF. Cuando una ruta VPN es exportada desde un VRF para ser ofertada a otros VRF, esta es etiquetada con una o más RT. También podemos asociar un grupo de RT con un VRF, y todas las rutas etiquetadas con al menos una de estas RT deben ser insertadas en el VRF. Las RT están conformadas por 64 bits, por motivos de simplificación, se asumen nombres para las RT en esta parte del trabajo.

La red contiene tres VPNs por lo que requiere tres RT, la asociación entre VRFs y RT en la red se observa en la Tabla 2.4.

Enrutador PE	**VRF**	**Sitios en el VRF**	***Route target* adjuntadas para exportar rutas**	***Route target* importadas**
PE1	Sitio-1 Empresa A	Sitio-1 Empresa A	Empresa A, VoIP	Empresa A, VoIP
	Sitio-2 Empresa A	Sitio-2 Empresa A	Empresa A	Empresa A
	Sitio-2 Empresa B	Sitio-2 Empresa B	Empresa B	Empresa B
	VoIP-1	Pasarela VoIP-1	VoIP	VoIP
PE2	Empresa A	Sitio-3 Empresa A	Empresa A	Empresa A
	Empresa B	Sitio-1 Empresa B	Empresa B, VoIP	Empresa B, VoIP
	VoIP-2	Pasarela VoIP-2	VoIP	VoIP

Tabla 2.4 Correspondencia entre VRFs y *Route targets* en red.

2.1.2 Propagación de información de enrutamiento en la red del proveedor.
Dos vías diferentes existen para el intercambio de información de enrutamiento VPN entre los enrutadores de frontera (PE) del proveedor de servicio.

- ✓ Corriendo algoritmos de enrutamiento diferentes en los enrutadores PE para cada VPN, por ejemplo copias de OSPF podrían estar corriendo para cada VPN, solución esta con serios problemas de escalabilidad en SP con gran número de VPN en sus redes.
- ✓ Correr un único protocolo de enrutamiento en el enrutador PE para el intercambio de todas las rutas de las VPNs. Con este método para poder soportar el solapamiento de los espacios de direcciones de las VPN, las direcciones IP usadas por los clientes deben ser aumentadas con información adicional que las haga únicas.

Para desarrollar la tecnología MPLS/VPN ha sido seleccionada la segunda de estas estrategias, las subredes IP propagadas por los enrutadores frontera del cliente (CE) serán aumentadas con un prefijo de 64 bits llamado un **RD** (***route distinguisher)***, atributo que se le adiciona a las direcciones IP para hacerlas únicas en un dominio MPLS. El direccionamiento en las VPN-IPv4 (VPNv4) es la combinación de una dirección IPv4 y el *route distinguisher* (Rosen y Rekhteri, 1999). El direccionamiento resultado compuesto por 96 bits será intercambiado entre los PE utilizando un direccionamiento especial de la familia de Multiprotocolos BGP (MP-BGP). Existen una serie de razones para escoger BGP (*Border Gateway Protocol*) como el protocolo para transportar las rutas VPNs, entre estas características mencionaremos, la posibilidad de BGP de soportar grandes listas de rutas y de transportar información adjuntada a las rutas como un atributo opcional de BGP, esta última posibilidad de BGP hace posible además la propagación de los RT entre los enrutadores PE.

Con lo anteriormente expuesto se resuelve el problema de que varias VPN puedan utilizar el mismo rango de direcciones IP en sus redes, pero recordemos que dentro de una misma VPN no pueden haber sitios

que utilicen el mismo rango de direcciones IP, tampoco podemos entrelazar VPNs que utilicen los mismos rangos de direcciones en sus redes. Este problema de solapamiento de direcciones IP ocurre también en los escenarios de redes IP estándar donde si es necesario una interconexión total entre sitios los rangos de direcciones han de ser únicos o desarrollar NAT.

Con la intención de ilustrar el intercambio de los protocolos de enrutamiento por VPNs con el MP-BGP usado en el núcleo de la red del SP, se considera el caso de la Empresa A en la red, se asume que el sitio-1 en el PE1 utiliza OSPF para interactuar con el *backbone*, el sitio-2 no utiliza protocolos de enrutamiento, es configurado con rutas estáticas y que el sitio-3 utiliza RIP (*Routing Information Protocol*). Lo mencionado anteriormente se muestra en la Figura 2.5.

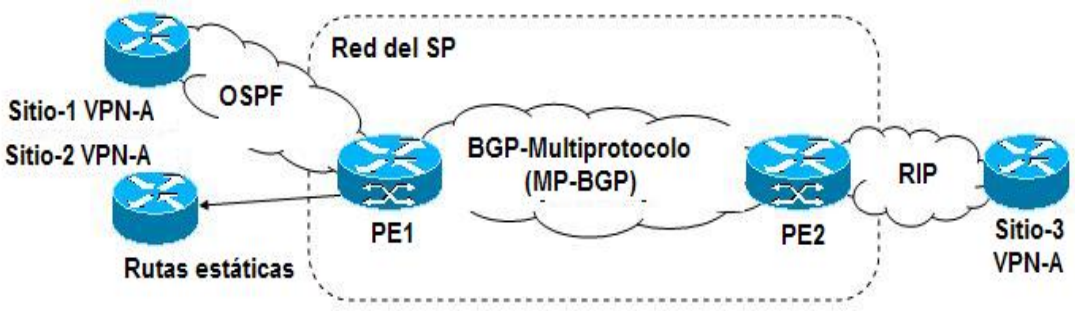

Figura 2.5 Protocolos de Enrutamiento usados en la VPN-A.

La información de enrutamiento colectada por varios protocolos de enrutamiento, así como las rutas estáticas configuradas en el enrutador PE1 son redistribuidas dentro de MP-BGP, las direcciones son aumentadas con el RD en el momento de la redistribución y las rutas exportan las RT especificadas en los VRF origen, también adjuntadas. La información de enrutamiento resultante de 96 bits es propagada por MP-BGP hasta el enrutador PE2. El enrutador PE2 después de recibir las rutas a través de MP-BGP inserta las rutas recibidas en varias tablas VRF, basándose en el RT adjuntado a cada ruta individual. El RD es eliminado de los 96 bits cuando la ruta es insertada dentro del VRF, terminando nuevamente como un enrutamiento IP tradicional, por último la información de enrutamiento recibida a través de BGP es redistribuida dentro de procesos RIP y transmitida al sitio-3 al RIP realizar actualizaciones.

2.1.3 Envío de paquetes en una VPN

En el envío de paquetes utilizando MPLS, cada paquete es etiquetado a la entrada del dominio MPLS con una etiqueta que identifica el punto de salida del dominio MPLS, con esta etiqueta es enviado a través de la red; todos los enrutadores del núcleo de la red conmutan las etiquetas sin necesidad de conocer la cabecera IP. Ahora cuando un enrutador PE (salida de un dominio MPLS) recibe un paquete de una VPN, este paquete no tiene información de su VPN destino. Para lograr que la comunicación entre sitios de una VPN sea única un segundo nivel de etiquetas debe ser incorporado.

Cada enrutador PE asigna una etiqueta única para cada ruta en cada instancia de Enrutamiento y Envío VPN (VRF). Estas etiquetas son propagadas conjuntamente con las correspondientes rutas a través del MP-BGP hasta todos los enrutadores PE. Los enrutadores PE reciben las actualizaciones MP-BGP e instalan las rutas recibidas en sus tablas VRF, también instalan las etiquetas VPN asignadas por los enrutadores PE en sus tablas VRF, con lo anterior expuesto la red MPLS/VPN está lista para el envió de paquetes VPN. Cuando un paquete VPN es recibido por un enrutador PE (entrada al dominio MPLS), es examinado el VRF que le corresponde y la etiqueta asociada con la dirección destino por el enrutador PE (salida del dominio MPLS) es buscada. Otra etiqueta orientada hacia el enrutador PE (salida) es obtenida desde la tabla de envío global. Ambas etiquetas son combinadas en la pila de etiquetas, y adjuntadas en la delantera del paquete VPN, luego son enviadas hacia el enrutador PE (salida).

Todos los enrutadores P en la red conmutan los paquetes VPN basados solamente en la primera etiqueta de la pila, las que apuntan al enrutador PE (salida). En las reglas normales del envío en MPLS los enrutadores P nunca analizan más allá de la primera etiqueta y son así completamente ajenos a la segunda etiqueta y los paquetes transportados por la red. Los enrutadores PE (salida) reciben los paquetes etiquetados con la segunda etiqueta las cuales únicamente identifican la VRF destino y en algunas ocasiones la interface de salida en el enrutador PE. Un análisis es ejecutado en el VRF y el paquete es enviado hacia el adecuado enrutador frontera del cliente (CE).

2.1.4 Provisión de un servicio VPN con la utilización de MPLS/VPN

A continuación se enumeran los pasos razonables en la configuración de una Red Privada Virtual (VPN) de Capa 3 sobre un *backbone* MPLS:

1. Definir y configurar las VRFs.
2. Definir y configurar las *Route Distinguishers.*
3. Definir y configurar las políticas de importar y exportar rutas (*Route Target*).
4. Configurar los enlaces entre los PE – CE.
5. Asociar las interfaces de los CE a las VRFs definidas previamente.
6. Configurar el Multiprotoclo BGP.

3. MPLS/VPN de Capa 2.

En los últimos años otra aplicación basada en la tecnología MPLS ha emergido, teniendo una gran acogida por los clientes y los SP, las MPLS/VPN de Capa 2, estas redes tienen la naturaleza de ser multiprotocolos, es decir, pueden transportar tanto tráfico IP como tráfico no IP, gran parte de las especificaciones del IETF sobre como transportar el tráfico de Capa 2 (Ethernet, Frame Relay, ATM, HDLC, PPP) a través de una red MPLS, están ya descritas. Esto da la oportunidad a los SP de con la misma infraestructura MPLS, transportar los tráficos asociados a servicios tradicionales, en especial el Frame Relay en nuestro país. A pesar de que las especificaciones mencionadas todavía no están estandarizadas (RFC=?), varios fabricantes de equipos ya han anunciado que soportan el borrador Martini del IETF (IETF Martini drafts). Los borradores Martini definen los mecanismos de encapsular y distribuir etiquetas para transportar Frame Relay, ATM, Ethernet, HDLC, PPP, sobre una red MPLS.

Relacionado con las VPLS (Virtual Private LAN Services) [1], hay dos borradores que marchan en la avanzada en los Grupos de Trabajo del IETF, “draft Kompella” y “draft Lasserre-VKompella” según análisis realizado por el fabricante líder en el mercado Juniper Network de estos borradores, concluye que para dar el servicio de interconexión de LAN multipunto a multipunto por su características en cuanto a “Auto-Discovery” y “Signaling” el borrador con mayor nivel de automatización y una operación eficiente es el descrito por Kireeti Kompella “draft Kompella”. (Capuno, 2003)(Kompella, 2004)(Martini, 2004)

3.1 La solución de Cisco

Cisco como líder en el mercado de los fabricantes de infraestructura de redes, para transportar tramas de Capa 2 sobre un *backbone* IP/MPLS propone una solución que denomina AToM (Any Transport over MPLS). Esta solución de Cisco habilita a los SP, a proveer conectividad de Capa 2 entre los sitios de los clientes utilizando una misma infraestructura de red basada en paquetes IP/MPLS. Los SP pueden realizar las conexiones tradicionales Frame Relay, ATM y las conexiones Ethernet sobre un *backbone* IP/MPLS. AToM soporta los siguientes tipos de transporte: ATM AAL5 sobre MPLS, ATM Cell Relay sobre MPLS, Ethernet sobre MPLS, Frame Relay sobre MPLS, PPP sobre MPLS y HDLC sobre MPLS.

[1] ***VPLS***, *Virtual Private LAN Segments en la RFC 2764*

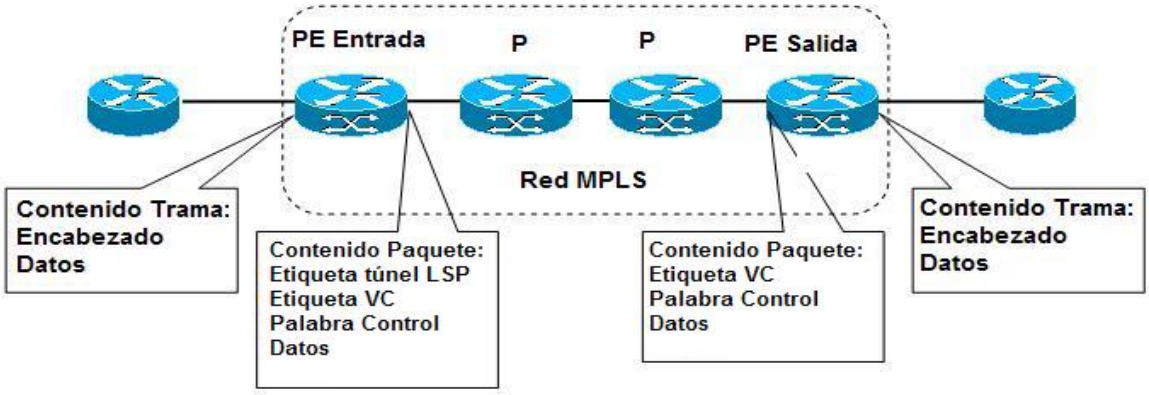

Figura 3.1 Tramas Ethernet o Frame Relay al ser trasportadas en un backbone MPLS.

La Figura 3.1 muestra los estados de una trama Ethernet o Frame Relay al ser transportada por un *backbone* IP/MPLS. (Cisco, 2002)

4. Conclusiones

Gran número de empresas líderes en el sector de las telecomunicaciones están invirtiendo en la investigación y desarrollo de la arquitectura MPLS. La estandarización de esta tecnología ha jugado un papel importante en el desarrollo de aplicaciones sobre esta arquitectura, entre las que se destacan las Redes Privadas Virtuales (VPN) de Capa 2 y 3.

Las MPLS/VPN de Capa 3 están ya desarrolladas e implementadas basadas en estándares como la RFC 2745, sin embargo, las MPLS/VPN de Capa 2 a pesar de la existencia de gran cantidad de especificaciones sobre su implementación en varios borradores del IETF (“drafts Martini”, “draft Kompella”, “draft Lasserre-Kompella” y otros), aún no están estandarizadas en RFC por el IETF, algo a tener muy en cuenta por los SP en el momento de invertir en equipamiento.

Los proyectos como el de Telemedicina, Educación a Distancia y otros, unido al aumento de la necesidad de crear fuertes Intranets en la gran mayoría de las empresas, demandan cada ves más recursos de las redes de datos, lo que lleva a utilizar tecnologías que exploten las redes de la forma más eficiente posible, como lo es en estos momentos la arquitectura MPLS.

Es de vital importancia para empresas que prestan servicios de telecomunicaciones y cuentan con infraestructuras para el transporte de datos el estudio de estas nuevas arquitecturas que están revolucionando el mundo de las redes de datos, tanto o más de lo que fue capaz de revolucionarlo en su momento el surgimiento de X.25, FR o ATM.

Referencias Bibliográficas

Capuano Mike. “VPLS: Scalable Transparent LAN Services”, Juniper; Marzo 2003, http://www.juniper.net

Cisco. “Software and Multiprotocol Label Switching”; 2002, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/prodlit/iosmp_ai.pdf

Guichard Jim, Pepelnjak Ivan. “MPLS and VPN Architectures”, Cisco Press, ISBN: 1-58705-002-1; 2000

Kompella Kireeti. “draft Kompella”, IETF; Enero 2004, http://www.ietf.org/internet-drafts/draft-kompella-l2vpn-l2vpn-01.txt

Martini Luca. “draft Martini”, IETF; Enero 2004, http://www.ietf.org/internet-drafts/draft-martini-ethernet-encap-mpls-02.txt

Rosen E, Y. Rekhter. “RFC 2547 BGP/MPLS VPNs”, IETF; Marzo 1999, http://www.ietf.org/rfc/rfc2547.txt

Información Biográfica

Ms C. Javier R. GÓMEZ VALDIVIA. Ms C. Gómez Valdivia es Subgerente de la Filial CubaDATA de la Empresa de Telecomunicaciones de Cuba en Sancti Spíritus. CubaDATA es la Unidad de Negocios de ETECSA que brinda servicios de Transporte de Datos. El es graduado de Ing. en Telecomunicaciones y Electrónica en 1995 y Ms C. Telemáticas en el 2004, es instructor adjunto del Centro de Capacitación de ETECSA.

Dr C. Carmen MOLINER PEÑA. Dr C. Moliner Peña es Profesora Titular del Departamento de Telemática de la Facultad de Ingeniería Eléctrica del Instituto Superior Politécnico José Antonio Echeverría, (CUJAE). Responsable de la Maestría en Temática, Miembro del Consejo Científico de la Facultad de Ingeniería Eléctrica y de la Comisión de Postgrado de la CUJAE. Miembro de la Comisión Nacional de la Carrera de Telecomunicaciones.

Siglario de Términos

	Ingles	**Español**
BGP	*Border Gateway Protocol*	Protocolo de Pasarela de Borde
CE	*Customer Edge*	Frontera del Cliente
CPE	*Customer Premises Equipment*	Equipos en Instalación del Cliente
EoMPLS	*Ethernet over MPLS*	Ethernet sobre MPLS
FR	*Frame Relay*	Conmutación de Tramas
HDLCoMPLS	*HDLC over MPLS*	HDLC sobre MPLS
IETF	*Internet Engineering Task Force*	Grupo Especial sobre Ingeniería de Internet
MP-BGP	*MultiProtocol- BGP*	BGP Multiprotocolo
MPLS	*Multiprotocol Label Switching*	Conmutación de Etiqueta de Multiprotocolo
NAT	*Network Address Translation*	Traslación de Direcciones de Red
OSPF	*Open Shortest Path First*	Primer Trayecto Abierto más Corto
P	*Provider*	Proveedor
PE	*Provider Edge*	Frontera del Proveedor
POP	*Points of Presence*	Punto de Presencia
PPP	*Point to Point Protocol*	Protocolo Punto a Punto
QoS	*Quality of Service*	Calidad de Servicio
RD	*Route Distinguishers*	Complemento a direcciones IP en dominio MPLS
RIP	*Routing Information Protocol*	Protocolo de Información de Enrutamiento.
RT	*Route Target*	Identificador de Ruta.
SP	*Service Provider*	Proveedor de Servicio.
TE	*Traffic Engineering*	Ingeniería de Tráfico.
VPLS	*Virtual Private LAN Segments*	Segmentos LAN Privados Virtuales.
VPN	*Virtual Private Network*	Red Privada Virtual.
VRF	*VPN Routing and Forwarding.*	Instancia de Enrutamiento y Envío VPN.