UNIVERSIDAD CENTRAL DE VENEZUELA

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA ELÉCTRICA

ESTUDIO DE LA TECNOLOGÍA MPLS (CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLOS), SU APLICACIÓN EN REDES PRIVADAS VIRTUALES (VPN) CON PARÁMETROS DE CALIDAD DE SERVICIO (QoS)

Trabajo Especial de Grado
para optar al Título de
Especialista de Comunicaciones y
Redes de Comunicación de Datos

AUTOR: Ing. Ramos, Rosangel D.

Caracas, Noviembre 2004

UNIVERSIDAD CENTRAL DE VENEZUELA

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA ELÉCTRICA

ESTUDIO DE LA TECNOLOGÍA MPLS (CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLOS), SU APLICACIÓN EN REDES PRIVADAS VIRTUALES (VPN) CON PARÁMETROS DE CALIDAD DE SERVICIO (QoS)

Trabajo Especial de Grado
para optar al Título de
Especialista de Comunicaciones y
Redes de Comunicación de Datos

AUTOR: Ing. Ramos, Rosangel D.
TUTOR ACADEMICO: Prof. Franklin Planchart

Caracas, Noviembre 2004

Hecho el Depósito de Ley
Depósito Legal Nº lft487200400446

AGRADECIMIENTOS

A Dios Padre Todopoderoso, mi mayor guía y protector.

A mi esposo Teo, gracias por tu estímulo, paciencia y apoyo incondicional. Gracias por esa motivación que día a día me alentaba a la culminación de esta tesis.

A la señora Yipsy, secretaria del Departamento de Postgrado, por su colaboración y apoyo en este proceso.

Al profesor **Franklin Planchart**, por su colaboración como tutor.

Lograr una de mis metas me causa inmensa satisfacción; por esto mi agradecimiento extensivo a todas aquellas personas que de una u otra forma me impulsaron a lograrlo.

Mil Gracias...

DEDICATORIA

A mi mamá, por sembrar en mí la fortaleza y el espíritu de continuar hacia adelante sin importar las circunstancias que la vida nos presente.

A mi esposo, por su apoyo, comprensión y por tener siempre las palabras de aliento necesarias.

A la memoria de un gran hombre, **mi Papa Abuelo Domingo**, un ejemplo a seguir de lucha, dedicación, fortaleza y actitud perseverante.

Le doy gracias a Dios porque están y estarán siempre presente en mi vida...

Ramos, Rosangel D.

ESTUDIO DE LA TECNOLOGÍA MPLS (MULTIPROTOCOL LABEL SWITCHING), SU APLICACIÓN EN REDES VIRTUALES PRIVADAS (VPN) CON MANEJO DE PARÁMETROS DE CALIDAD DE SERVICIO (QoS)

Tutor Académico: Prof. Franklin Planchart. Tesis. Caracas, U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Año 2004.

Palabras claves: MPLS, VPN, IP

Resumen: El explosivo crecimiento de Internet ha presentado un serio reto a los proveedores de servicios y a los fabricantes de equipamiento en términos de un enorme aumento del tráfico y del número de clientes. La Conmutación de Celdas Multiprotocolos (MPLS) combina la inteligencia del enrutamiento con el desempeño de la conmutación y proporciona importantes ventajas a las redes con una arquitectura IP pura, así como aquellas con IP y ATM, o una mezcla de otras tecnologías de capa 2. La tecnología MPLS es clave para las redes privadas virtuales (VPN) ampliables y la calidad de servicio (QoS) de extremo a extremo, ya que permite una utilización eficiente de las redes existentes para satisfacer el crecimiento futuro.

CONTENIDO

CAPÍTULO 1

Pág.

1. INTRODUCCIÓN..... 1

1.1. ANÁLISIS DEL PROBLEMA..... 2

1.1.1. Expansión de las redes..... 2

1.1.2. Relación precio/rendimiento entre enrutadores y conmutadores..... 2

1.1.3. Integración de las redes IP y las redes ATM..... 3

1.2. CRITERIOS DIVERSOS PARA SOLVENTAR EL PROBLEMA..... 6

1.2.1. Conmutación de celdas desarrollado por Toshiba (CSR)..... 6

1.2.2. Conmutación IP desarrollado por Ipsilon (IP Switching: IpS)..... 6

1.2.3. Conmutación de etiquetas desarrollado por Cisco (TgS)..... 6

1.2.4. Conmutación IP basado en rutas agregadas por IBM (ARIS)..... 7

CAPÍTULO 2

2. CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLOS (MPLS)..... 8

2.1. ARQUITECTURA..... 10

2.1.1. Proceso de etiquetado del paquete en un LSR de borde..... 13

2.1.2. Reenvío del paquete MPLS..... 15

2.2. OPERACIÓN EN MODO TRAMA..... 16

2.2.1. Encabezado de la pila de etiquetas 17

2.2.2. Conmutación de las etiquetas 18

2.2.3. Propagación de las etiquetas 19

2.2.3.1. Establecimiento de la sesión TDP / LDP..... 20

2.2.3.2. Distribución de las etiquetas..... 20

2.2.4. Convergencia de la red MPLS 21

2.2.5. Proceso de un LSR para enrutar hacia una red IP (Penultimate Hop Popping PHH)..... 22

2.3. OPERACIÓN MPLS MODO CELDA..... 24

2.3.1. Conectividad del plano de control 25

2.3.2. Intercambio de un paquete etiquetado..... 26

2.3.3. Colocación y distribución de las etiquetas 28

2.3.4. Convergencia de la red a través de un dominio ATM..... 30

CAPÍTULO 3

3. REDES PRIVADAS VIRTUALES BASADAS EN MPLS 31

3.1. OPCIONES DE IMPLEMENTACIÓN..... 32

3.1.1. Modelo de revestimiento (oVPN)..... 32

3.1.2. Modelo par a par (PtP)..... 34

3.1.3. Modelo VPN MPLS..... 38

3.1.3.1. MPLS como mecanismo de intercambio..... 40

3.1.3.1.1. Tabla de enrutamiento y reenvío (VRF)..... 42

3.1.3.1.2. Marcador de rutas (Route targets)..... 43

3.1.3.1.3. Propagación de enrutamiento entre PEs..... 43

3.1.3.2. Enrutamiento..... 45

3.1.3.3. Escalabilidad..... 45

3.1.3.4. Seguridad..... 47

3.1.3.5. Calidad de Servicio..... 48

CAPITULO 4

4. PERSPECTIVA DE LA TECNOLOGÍA MPLS A NIVEL MUNDIAL..... 53

CAPITULO 5

5. EJEMPLO DE IMPLEMENTACIÓN 55

CONCLUSIONES..... 65

GLOSARIO DE TÉRMINOS..... 68

INDICE DE FIGURAS..... 71

BIBLIOGRAFÍA..... 72

1. INTRODUCCIÓN

Las redes IP tradicionales realizan el intercambio o envío del paquete analizando la dirección destino contenida en el encabezado del paquete para que éste pueda viajar desde un origen a un destino. El enrutador analiza la dirección destino independientemente de cada salto en la red y los protocolos de enrutamiento dinámicos o estáticos construyen las bases de datos necesarias para analizar la ruta.

Actualmente la propuesta de MPLS es el resultado de un proceso de integración y convergencia de las redes de los proveedores de servicios sobre una misma infraestructura IP, y que se propone como la tecnología que se impondrá en los próximos años para solventar ciertas restricciones de las redes tradicionales IP.

Con la introducción del concepto MPLS, es posible construir una nueva aplicación denominada *redes virtuales privadas* basadas en MPLS (VPN MPLS). En el desarrollo del documento y como uno de sus objetivos principales se analizará la implementación de MPLS para crear VPN y los beneficios de escalabilidad, seguridad y calidad de servicio que esta nueva aplicación puede ofrecer.

A continuación se presenta un análisis de la tecnología MPLS: concepto, arquitectura, funcionamiento y su implementación en las redes virtuales.

1.1 ANÁLISIS DEL PROBLEMA

1.1.1 Expansión de las Redes

El crecimiento tanto del número de usuarios como de los requerimientos de ancho de banda, ha incrementado la demanda de las redes en los *proveedores de servicios de Internet* (ISPs). Para ofrecer estos requerimientos los ISPs deben aumentar el rendimiento de los equipos de conmutación y enrutamiento.

Para aumentar el número de nodos se requiere mayor cantidad de rutas y por ende aumenta el flujo de tráfico. En consecuencia, los ISPs necesitan de una red con un alto nivel de e*scalabilidad* que permita su crecimiento sin disminuir la eficiencia y el rendimiento. La conmutación de etiquetas ha sido motivada por la necesidad de una red altamente escalable, además de involucrar las funcionalidades de enrutamiento de Internet y de todas las redes IP en general.

1.1.2 Relación precio/rendimiento entre enrutadores y conmutadores

Uno de los componentes principales en todas las redes IP, sean públicas o privadas es el *enrutador* (Router). La tarea fundamental de un enrutador es el intercambio de paquetes a través de una red. Además el enrutador ejecuta otras funciones como, filtrado de paquetes, etc. De hecho la característica más importante del enrutador para muchas aplicaciones no es cuán rápido se intercambia los paquetes sino el conjunto de funcionalidades que éste puede ofrecer.

Otro componente importante dentro de la red es el *conmutador* (Switch). Comparados con los enrutadores, los conmutadores no proveen la misma cantidad de funcionalidades y normalmente soportan un número limitado de protocolos y tipos de interfaz.

Caracterizar el nivel de *rendimiento* tanto en los enrutadores como en los conmutadores es un poco complejo, debido a que involucran muchos factores, como por ejemplo el patrón de tráfico. Si hablamos de la relación precio/rendimiento se puede decir que los conmutadores resaltan sobre los enrutadores, debido a que el precio de los enrutadores tiende a subir cuando aumentan los niveles de funcionalidad. En consecuencia, el mayor nivel de rendimiento es encontrado en los conmutadores más que en los enrutadores. Entonces, ¿cómo se puede construir un equipo que realice la tarea principal de un enrutador (Intercambio de paquetes) usando una arquitectura física de un conmutador?. Este es otro de los principales motivos para el desarrollo de la conmutación de etiquetas.

1.1.3 Integración de las redes IP y las redes ATM

Otro de los problemas que condujeron al desarrollo de la conmutación de etiquetas es la interacción de las redes IP y el m*odo de transferencia asíncrona* (ATM). Los conmutadores empezaron a existir en el mercado en el año 1980 y la promesa fue proporcionar un mayor rendimiento sobre las otras tecnologías de red. Sin embargo, debido a que el estándar de ATM involucra organismos como la Unión Internacional de Telecomunicaciones (ITU) y el Forum ATM, su arquitectura difiere significativamente con la arquitectura de las redes IP.

IP esta basado en un modelo *no orientado a conexión* (Connectionless) y ATM esta basado en un modelo *orientado a conexión* (Connection Oriented), además poseen direccionamientos diferentes, etc.

Los enrutadores y las estaciones podrán comunicarse si están dentro de la misma subred. Si están en subredes diferentes entonces uno o más enrutadores serán involucrados en el reenvío del paquete desde la subred fuente hasta la subred destino. El modelo clásico reconoce que los dispositivos IP podrían estar conectados a una red ATM común estando en subredes diferentes. De allí se introduce el concepto de *subred IP lógica* (LIS).

Una LIS consiste en un grupo de estaciones de trabajo y enrutadores IP que están conectados a una red ATM común, es decir, el RFC 1577 solo permite la comunicación entre LIS y asume que para enviar un paquete desde un LIS a otro, estos necesitan ir a través de un enrutador que conecte a ambos LIS (Ver figura 1).

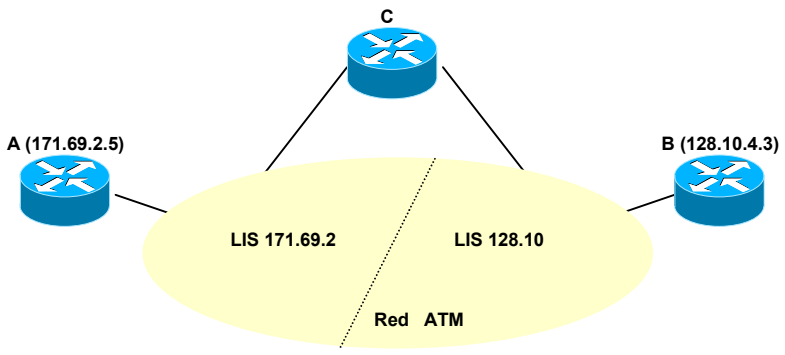

Figura 1: LIS (Subred IP lógica)

La idea de que en el modelo clásico no se pueda crear un circuito virtual entre LIS a través de la red ATM, sino que se deben comunicar a través de un enrutador no se vio como idea atractiva, debido a que condiciona severamente la eficiencia y las ventajas propias de ATM como son: la alta velocidad de transmisión, la reducción de los retardos y la calidad de servicio. En función a esto se establece un mecanismo para que dos dispositivos del mismo LIS puedan establecer comunicación: ATMARP.

El protocolo ARP es usado en el medio convencional Ethernet para permitir que los dispositivos IP aprendan la información de direccionamiento necesaria para su comunicación. De forma similar ATMARP permite que dos dispositivos puedan aprender sus direcciones ATM correspondiente.

Debido a que ARP funciona a través de *paquetes de inundación* (Broadcast) en la capa de enlace, lo cual no es soportado por ATM, ATMARP introduce el concepto de servidor ARP, un único nodo que provee la resolución de direcciones IP a ATM para cada LIS. Cada LIS puede entonces hacer la petición al servidor ARP para resolver la dirección IP en una dirección ATM. Luego de tener la dirección ATM se podrá configurar un *circuito virtual* (VC) usando señalización ATM y empezar el envío de paquetes.

1.2 CRITERIOS DIVERSOS PARA SOLVENTAR EL PROBLEMA

1.2.1 Conmutación de celdas desarrollado por Toshiba (CSR)

CSR introduce la idea de que una conmutación ATM podría ser controlada por protocolos IP más que por protocolos de señalización ATM. El CSR fue presentado por un grupo de la IETF y luego por BOF “Birds of a Feather” cerca del 1995.

1.2.2 Conmutación IP desarrollado por Ipsilon (IpS)

IpS fue definido por la compañía Ipsilon. Una de las premisas básicas de IpS es que la alternativa del modelo IP sobre ATM es compleja e ineficiente. IpS como otra de las tecnologías de conmutación de etiquetas, usa el componente IP más el protocolo de etiquetas para permitir el intercambio de paquetes IP en una arquitectura ATM. Este enfoque remueve completamente el plano de control ATM y la necesidad de adaptar los planos de control tanto de IP como ATM.

Tanto la propuesta de Ipsilon como la de Toshiba utilizan dispositivos híbridos con funciones de conmutación y enrutamiento y se basan en la identificación del flujo de tráfico, es decir, se crean circuitos virtuales dependiendo del tipo de tráfico.

1.2.3 Conmutación de celdas desarrollado por Cisco (TgS)

Cisco System anuncia otra mejora llamada *conmutación de celdas* (TgS), la cual posee una divergencia técnica considerable con respecto a CSR y IpS. A diferencia de Ipsilon, Cisco anuncia su intención de estandarizar TgS en la IETF.

TgS se enfoca en agregar funcionalidades como rutas explícitas y mejorar la escalabilidad a través del uso de enrutamiento jerárquico. TgS se puede implementar tanto en enrutadores como en conmutadores sin requerir modificación en la parte física del equipo. La red de TgS se basa en crear un enrutador de borde cuya función es entregar paquetes no etiquetados en paquetes etiquetados, y un conmutador cuya función es reenviar paquetes etiquetados.

1.2.4 IBM`s ARIS

Después del anuncio de Cisco, IBM describe otro anuncio de conmutación de etiquetas llamado conmutación IP basado en rutas agregadas (ARIS). ARIS tuvo más en común con TgS que con los otros, sin embargo, difieren en algunos temas significativos. Muchas de las ideas de ARIS fueron tomadas en cuenta en la estandarización de MPLS.

A diferencia de IpS y CSR, TgS y ARIS son propuestas denominadas manejo de control debido a que la conmutación de los datos se realiza independientemente de su naturaleza. Es decir, que un mismo circuito virtual puede tener distintos tipos de tráfico.

2. CONMUTACIÓN DE ETIQUETAS MULTIPROCOLOS (MPLS)

El nombre de MPLS fue adoptado principalmente porque los nombres Conmutación IP (IpS) y Conmutación de Etiquetas Cisco (TgS) estaban asociados a una compañía en particular y era necesario un término neutral.

MPLS, se ha convertido en el foco de atención para solventar los problemas relacionados con:

- Involucrar la arquitectura de enrutamiento de redes IP.
- Mejorar el rendimiento o la relación precio/rendimiento en los enrutadores.
- Disminuir la complejidad de integrar las direcciones IP en direcciones ATM.
- Escalabilidad
- La necesidad de agregar nuevas funciones de enrutamiento.

MPLS es una tecnología que surge con el propósito de dirimir muchos de los temas asociados con la tecnología IP existente. El objetivo principal del grupo de trabajo de MPLS es estandarizar la base para que integre el paradigma de la conmutación de etiquetas con la capa de red. MPLS asigna etiquetas a los paquetes para ser transportados. El mecanismo de enrutamiento de paquetes a través de la red se realiza utilizando un intercambio de etiquetas, en la cuál una unidad de datos porta una etiqueta de tamaño fijo que le informa a los nodos cómo procesar y reenviar la data.

Una diferencia significativa entre MPLS y las tecnologías WAN tradicionales es la forma cómo las etiquetas son asignadas y la capacidad de portar una pila de etiquetas adjunto al paquete. Este concepto involucra nuevas aplicaciones, como Ingeniería de Trafico, Redes Privadas Virtuales (VPN), etc.

En las redes IP convencionales, cualquier cambio en la información que controle el enrutamiento del paquete es comunicado a todos los dispositivos dentro de un dominio de enrutamiento. Estos cambios involucran un período de convergencia considerable dentro del algoritmo o protocolo utilizado. El mecanismo utilizado por las redes IP convencionales tienen implicaciones de escalabilidad en términos de propagación de las rutas, uso de memoria y procesamiento en los enrutadores centrales.

MPLS provee un mecanismo que permite cambios en la información de enrutamiento sin afectar a otros dispositivos en la red. Para implementar este mecanismo no se requiere la información destino localizada en el encabezado del paquete, debido a que el intercambio del paquete se realiza en base a la etiqueta añadida el cual indica el destino deseado del mismo. Esto quiere decir que cualquier cambio dentro del proceso de decisión puede ser comunicado a otros dispositivos a través de la distribución de las etiquetas.

MPLS es un mecanismo que permite a los dispositivos de enrutamiento interno conmutar un paquete a través de una red desde una interfaz de entrada hasta una interfaz de salida sin analizar la dirección de capa de red destino.

2.1 ARQUITECTURA

Para entender todos los tópicos que afectan la escalabilidad y la flexibilidad de las redes tradicionales, se debe empezar por revisar ciertos factores como:

- Cada vez que un nuevo enrutador es conectado a una red WAN, se debe establecer un circuito virtual entre uno y otro si se requiere un enrutamiento óptimo.
- Con la configuración de ciertos protocolos de enrutamiento, cada enrutador conectado a una red WAN capa 2 (construido con conmutadores ATM o Frame Relay) necesitan un circuito virtual dedicado hacia cada enrutador conectado a la misma red. Para lograr la redundancia necesaria se debe establecer protocolos de enrutamiento adyacentes con cada enrutador conectado. Pero de esto resulta una gran cantidad de tráfico de enrutamiento sumado a la propagación de rutas del protocolo de enrutamiento en uso.
- Complejidad en el manejo y provisión de los circuitos virtuales debido a que es muy difícil predecir la cantidad de tráfico exacto entre los enrutadores.

Con lo antes expuesto se evidencia la necesidad de usar un mecanismo diferente para permitir el intercambio de información de capa de red entre enrutadores y conmutadores WAN, que permita participar en la decisión de intercambio de paquetes y que las conexiones directas entre enrutadores de borde ya no sean requeridas.

La arquitectura de MPLS se divide en dos componentes: Componente de intercambio llamado *plano de data* (*data plane)* y el componente de control (*control plane*). El plano de data utiliza una base de datos para ejecutar el intercambio de paquetes basado en la etiqueta adjunta (Label-Forwarding Database). El componente de control es el responsable de crear y mantener la información de intercambio de etiquetas entre el grupo de conmutadores interconectados. La figura 2 muestra la arquitectura básica de un nodo MPLS ejecutando enrutamiento IP.

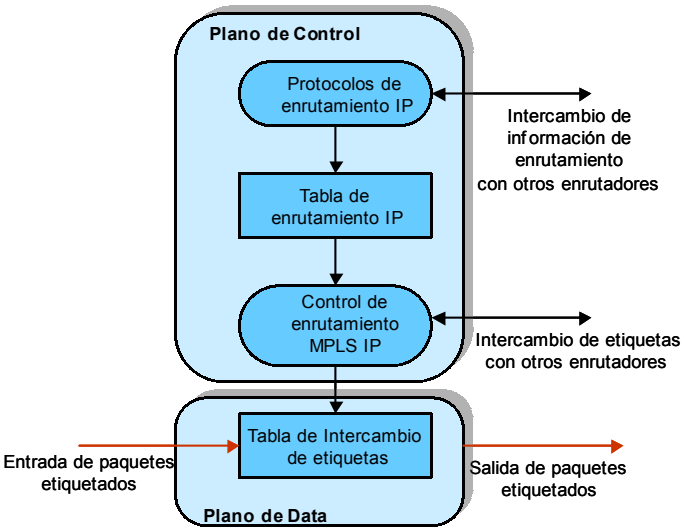

Figura 2: Arquitectura básica de un nodo MPLS

Cada nodo MPLS debe ejecutar uno o más protocolos para el intercambio de información de enrutamiento IP. En un nodo MPLS la tabla de enrutamiento es usada para determinar la etiqueta que está contenida en ella. Este intercambio de etiquetas por paquetes a un solo destino basado en la dirección IP es ejecutado usando un *protocolo de distribución de etiquetas* (Label Distribution Protocol LDP).

El primer equipo disponible para una red MPLS es el enrutador de etiquetas (Label Switch Router LSR). Cualquier enrutador o conmutador que implemente procedimientos de distribución de etiquetas está bajo esta categoría. La función básica del procedimiento es permitir a los LSRs distribuir sus etiquetas a otros LSRs dentro de una red MPLS.

Un LSR de borde (Edge-LSR) es un enrutador que ejecuta la *imposición de etiqueta* (push action) y la *disposición de etiquetas* (*pop* action) en una red MPLS.

La imposición es el acto de agregar una etiqueta o una pila de etiquetas a un paquete en un dominio MPLS y la disposición es el acto de remover la última etiqueta al paquete antes de que sea entregado al vecino fuera del dominio MPLS.

Un LSR de borde expande la arquitectura de la Figura 2 con un componente adicional en el plano de data. La tabla IP estándar es construida desde la tabla de enrutamiento y es expandida con la información de etiquetado.

Los paquetes entrantes pueden ser entregados como paquetes puros IP a nodos no-MPLS o pueden ser etiquetados y ser enviados a nodos MPLS. Para paquetes etiquetados destinados a nodos no-MPLS, la etiqueta es removida y se ejecuta una búsqueda capa 3 (Layer 3 lookup) para encontrar un destino no-MPLS.

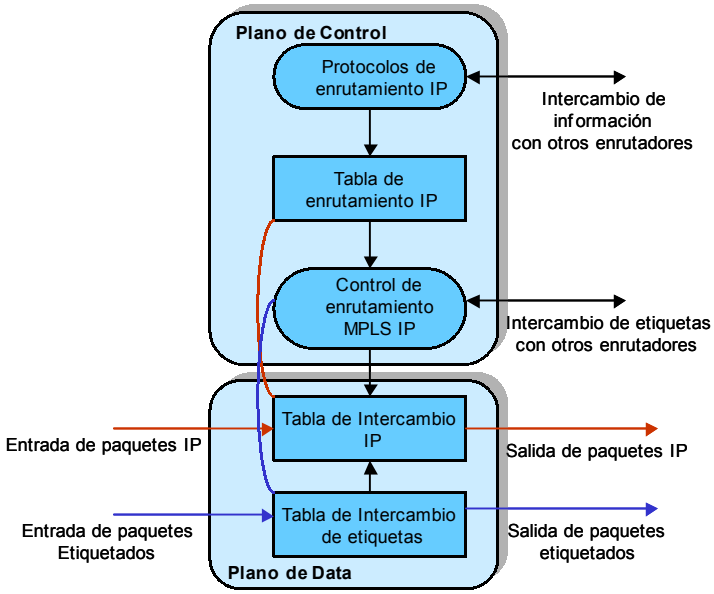

Figura 3. Arquitectura de un LSR de borde

2.1.1 Proceso de etiquetado en un LSR de borde

Tal como se mencionó anteriormente la imposición es el acto de añadir una etiqueta a un paquete para entrar en un dominio MPLS (Ver Figura 4). Esto es una función de un LSR de borde, lo que significa que el paquete debe ser etiquetado antes de ser entregado a un dominio MPLS. Para ejecutar esta función un LSR-borde necesita entender el encabezado del paquete y cuál etiqueta o grupo de etiquetas se debe asignar.

En un proceso capa 3 convencional, cada salto se ejecuta de acuerdo a la información del destino contenida en el encabezado del paquete. Para escoger el próximo salto de un paquete IP se ejecutan dos funciones: La primera función es separar los posibles paquetes en un conjunto de prefijos IP.

La segunda función es relacionar cada prefijo IP a una dirección del próximo salto. Esto significa que cada destino en la red es alcanzable por una ruta con respecto al flujo de tráfico desde un dispositivo entrante hasta un dispositivo de salida.

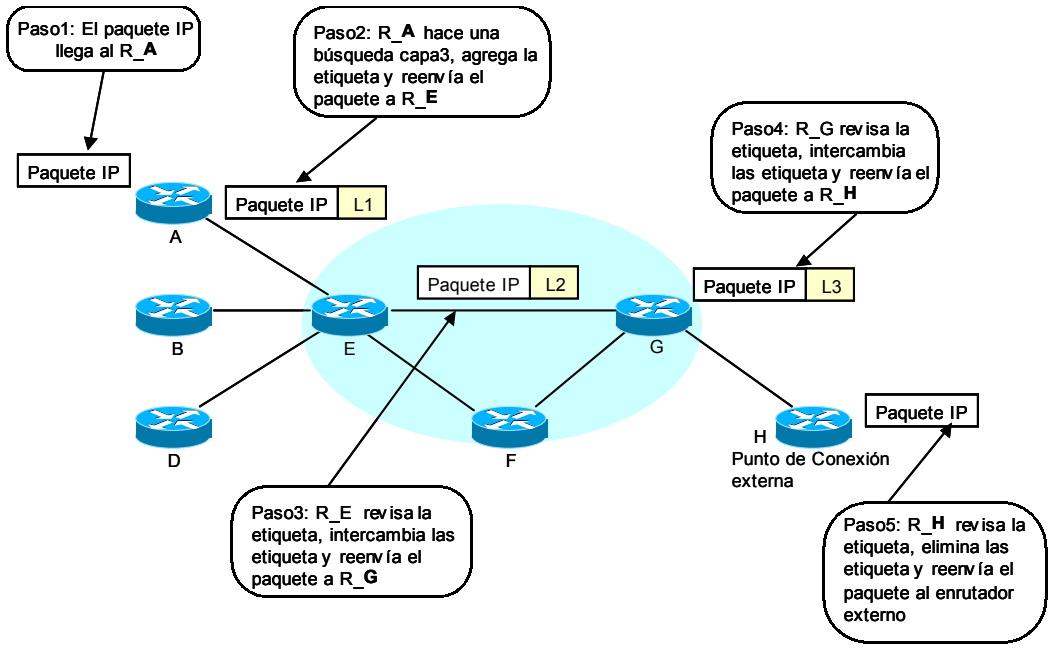

Figura 4: Colocación y reenvío de una etiqueta MPLS

Con la arquitectura de MPLS, el resultado de la primera función es conocido como *equivalencia de clases para el reenvío* (Forwarding Equivalence Classes FECs). Una FEC corresponde a una subred IP destino, pero también a cualquier flujo de tráfico que el LSR de borde considere significativo.

Con el método convencional IP, el procesamiento del paquete es ejecutado en cada salto de la red. Sin embargo, cuando se introduce MPLS, a un paquete particular se le asigna un FEC. Este FEC es codificado como un identificador de tamaño fijo conocido como etiqueta.

Cuando un paquete es entregado al próximo salto, la etiqueta es añadida para que el próximo dispositivo en la ruta pueda entregarlo tomando en cuenta la etiqueta codificada en lugar de la información capa 3 contenida en el encabezado.

2.1.2 Reenvío del paquete MPLS y rutas conmutadas a través de etiquetas

Cada paquete entra a una red MPLS por un LSR de entrada y sale por un LSR de salida, este mecanismo crea una *ruta conmutada a través de etiqueta* (Label Switched Path LSP), la cual describe un conjunto de LSRs por donde atraviesan los paquetes etiquetados para llegar al LSR destino de un FEC particular. Esta LSP es unidireccional, lo que significa que se utiliza un LSP diferente para retornar el tráfico. La creación de un LSP es orientada a conexión debido a que la ruta es configurada antes del flujo de tráfico.

Cada LSR mantiene dos tablas: la primera llamada *base de información de las etiquetas*, (Tag Information Base TIB para Cisco y Label Information Base LSB para MPLS estándar), la segunda llamada *base de información para el intercambio de etiquetas* (Tag Forwarding Information Base TFIB para Cisco y Label Forwarding Information Base LFIB para MPLS estándar).

2.2 OPERACIÓN DE MPLS EN MODO TRAMA

El LSR de borde recibe un paquete IP, clasifica el paquete en FEC, y le coloca la etiqueta correspondiente a ese FEC. El LSR recibe el paquete etiquetado y usa la tabla de intercambio (TFIB/LFIB) para intercambiar la etiqueta de entrada con su etiqueta de salida correspondiente al mismo FEC.

Cuando el LSR de borde destino para ese FEC particular recibe el paquete etiquetado, remueve la etiqueta y ejecuta el proceso tradicional capa 3.

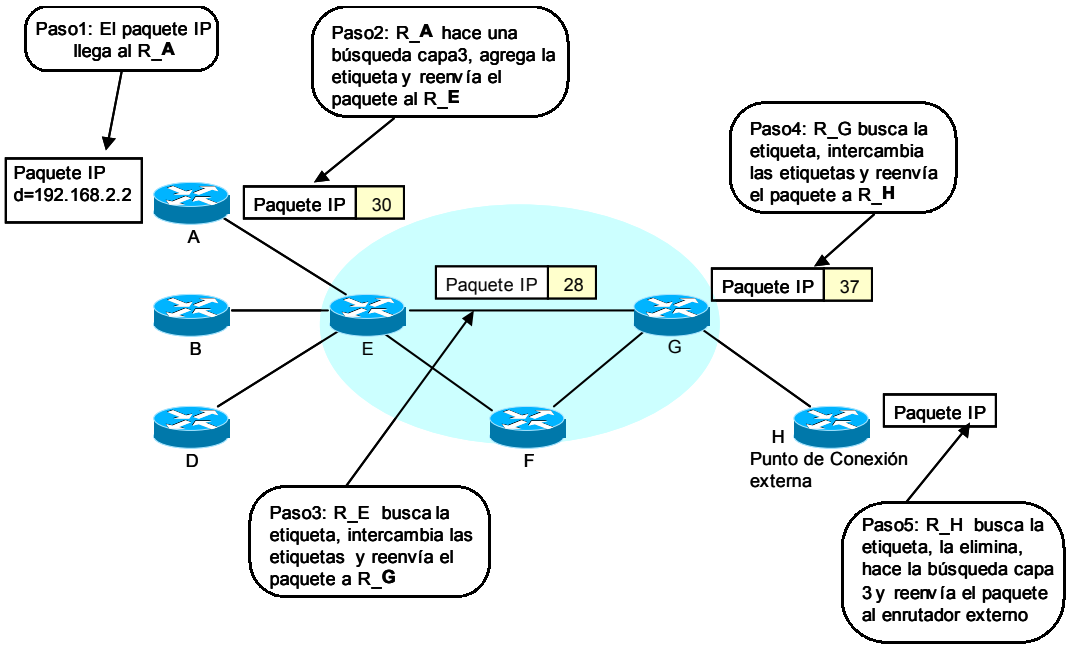

Figura 5: Proceso de reenvío de un paquete IP

2.2.1 Encabezado de la pila de etiquetas MPLS

Por razones de rendimiento la etiqueta MPLS debe estar insertada antes de los datos, la etiqueta debe ser insertada entre el encabezado capa 2 y el encabezado capa 3, tal como se muestra en la figura 6.

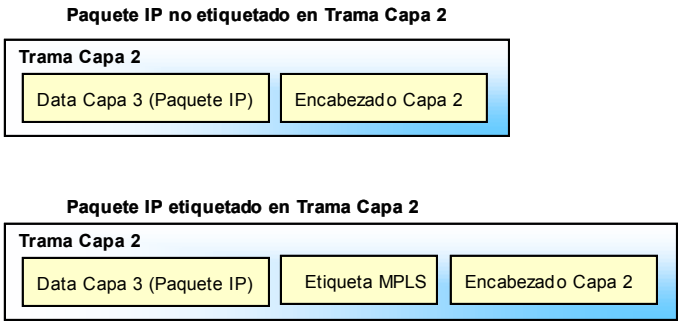

Figura 6: Posición de la etiqueta MPLS en una trama capa 2.

El encabezado de MPLS (mostrado en la figura 7) contiene 20 dígitos binarios (bits) para la etiqueta, 3 dígitos binarios para la información de clase de servicio también llamado dígito experimental, 8 dígitos para el tiempo de vida (Time-to-Live TTL) y 1 dígito para el final de la pila (*Bottom-of-Stack).*

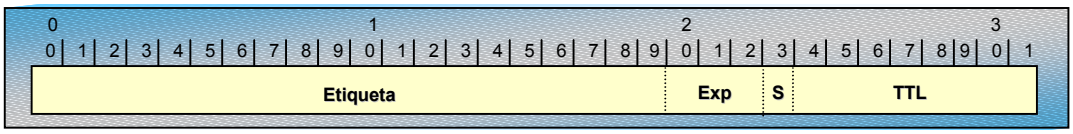

Figura 7: Encabezado de la pila de etiquetas MPLS

Con el encabezado de la pila de etiquetas que se inserta entre el encabezado capa 2 y la data capa 3, el enrutador que envía debe indicarle al enrutador que recibe

que el paquete que se está transmitiendo no es un paquete puro IP sino que es un paquete MPLS, es decir, que es un paquete etiquetado.

2.2.2 Conmutación de etiquetas MPLS

La conmutación de etiquetas se ejecuta en la misma vía independientemente de que el paquete contenga una o varias etiquetas. En ambos casos, el LSR utiliza solo la etiqueta superior de la pila ignorando las otras. Esta función permite una variedad de aplicaciones donde los enrutadores de borde (LSR de borde) pueden clasificar paquetes y asociar etiquetas sin reconocer los enrutadores del centro (LSR).

Por ejemplo, de acuerdo a la figura 8, se asume una VPN MPLS entre en enrutador A y el enrutador E, y ambos coinciden con la red 10.1.0.0/16 la cual es alcanzable a través del enrutador E, y se le asigna la etiqueta con valor de 73.

Para enviar un paquete a la red destino 10.1.0.0/16, el enrutador A construye una pila de etiquetas. La etiqueta inferior define la VPN MPLS hasta el enrutador E y la etiqueta superior es la etiqueta asignada a la dirección IP del enrutador B. Cuando la red propaga el paquete, la etiqueta superior es conmutada exactamente como se propaga un paquete IP a través de la red y la segunda etiqueta en la pila alcanza el enrutador E intacta.

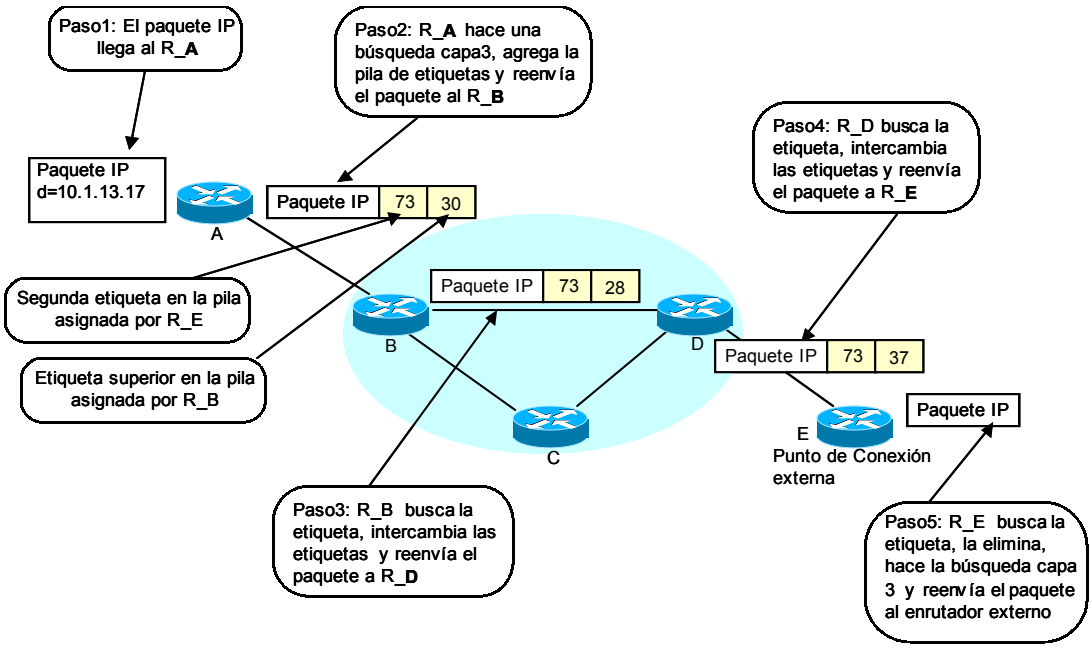

Figura 8: Conmutación de etiquetas a través de la pila

2.2.3 Propagación de las etiquetas en MPLS

El software Cisco IOS implementa dos protocolos que pueden ser usados para asociar las redes IP con las etiquetas MPLS con el propósito de enrutar paquetes únicos (Unicast) basados en destinos:

- ❖ Protocolo de Distribución de Etiquetas Cisco (Tag Distribution Protocol TDP):
- ❖ Protocolo de Distribución de Etiquetas Estándar IETF (Label Distribution Protocol LDP).

TDP y LDP funcionan de forma equivalente y ambos pueden ser usados dentro de una red, pero en cada interfaz dentro de un mismo LSR.

2.2.3.1 Establecimiento de la Sesión TDP/LDP

El proceso TDP/LDP empieza cuando se crea la estructura LIB (Label Information Base). El enrutador trata de descubrir otros LSRs en las interfaces que tengan MPLS, a través de paquetes *identificadores TDP* (Hello).

Los paquetes identificadores son enviados como paquetes de inundación (Broadcast) haciendo el descubrimiento automático de los vecinos. Luego que el proceso de los paquetes identificadores descubra los vecinos, se establece la sesión.

Las sesiones TDP usan el puerto TCP 711 y las sesiones LDP usan el puerto TCP 646. TCP (Protocolo de Control de Transporte) es usado como protocolo de transporte para asegurar la entrega de la información de manera confiable. Una vez establecida la sesión, se observa constantemente con paquetes de revisión (keepalive) para asegurar que está todavía operacional.

2.2.3.2 Distribución de las etiquetas

Tan pronto como sea creada la LIB en el enrutador, se le asigna una etiqueta a cada FEC conocido. El FEC es equivalente a un prefijo IGP (Protocolo Interior de Puerta de Salida - Interior Gateway Protocol) en el enrutamiento basado en destino a través de paquetes únicos (Unicast), es decir, se le asigna una etiqueta a cada prefijo en la tabla de enrutamiento IP y el mapeo entre los dos son almacenados en la LIB.

Debido a que los LSR asignan una etiqueta a cada prefijo IP en la tabla de enrutamiento, tan pronto como el prefijo aparezca en la tabla, significa que puede ser

usada por otros LSRs para enviar paquetes etiquetados hacia el LSR asignado, este método de la asignación y distribución de la etiqueta es denominado *Control Independiente* con distribución *en sentido descendiente no solicitado (Unsolicited Downstream):*

- La asignación de la etiqueta en los enrutadores se hace sin importar que se haya recibido o no una etiqueta del mismo prefijo desde el próximo enrutador.
- El método de distribución es *no solicitado* porque los LSR asignan las etiquetas y las anuncian al vecino ascendente sin importar que otros LSRs la necesiten.
- El método de distribución es descendente cuando un LSR asigna una etiqueta a un LSRs ascendente y pueden ser usadas para reenviar los paquetes etiquetados y anunciarlas a los vecinos.
- Todas las etiquetas colocadas son anunciadas inmediatamente a todos los enrutadores a través de sesiones TDP.

2.2.4 Convergencia de la Red MPLS en modo trama

Un aspecto importante en el diseño de una red MPLS es el tiempo de convergencia. La convergencia puede ser definida como el tiempo que toman los enrutadores dentro de un dominio para aprender los cambios topológicos y sincronizar sus tablas con otros enrutadores dentro del mismo dominio.

En algunas aplicaciones de MPLS como por ejemplo VPN MPLS es necesario un *protocolo* IGP para que la convergencia en el centro de la red no sea afectada por la propagación de las etiquetas. Los protocolos IGP, por definición, convergen mucho más

rápido que los protocolos de enrutamiento exterior (EGP). Por el contrario, los protocolos de enrutamiento exterior como por ejemplo el BGPv4 proveen una topología libre de lazos entre sistemas autónomos diferentes. Su objetivo principal, no es la convergencia rápida, sino provee una excelente capacidad de escalabilidad y flexibilidad para grandes números de rutas.

En una red modo trama para minimizar el retardo de la convergencia se utiliza el *modo de retención liberal* en combinación con el c*ontrol independiente* de las etiquetas y la distribución *descendente no solicitada.* Cada enrutador usando modo de retención liberal tiene etiquetas asignadas para un prefijo dado, eso quiere decir que ellos pueden encontrar una etiqueta de salida correcta sin preguntarle a su vecino por la etiqueta asignada. Cuando el enrutador recibe etiquetas para el mismo FEC desde diferentes vecinos, todas las etiquetas colocadas son retenidas. Sólo una de esas etiquetas será usada.

2.2.5 Proceso de un LSR de Salida para enrutar hacia una red IP (Penultimate Hop Hopping PHH)

Un LSR de salida en una red MPLS debe realizar dos búsquedas en el paquete recibido de un vecino MPLS y destinado a una red externa fuera del dominio MPLS. El LSR de salida debe inspeccionar la etiqueta en el encabezado de la pila y debe ejecutar una búsqueda para que la etiqueta sea removida.

La búsqueda capa 3 adicional debe ser realizada en el paquete antes de que éste sea reenviado a su destino final.

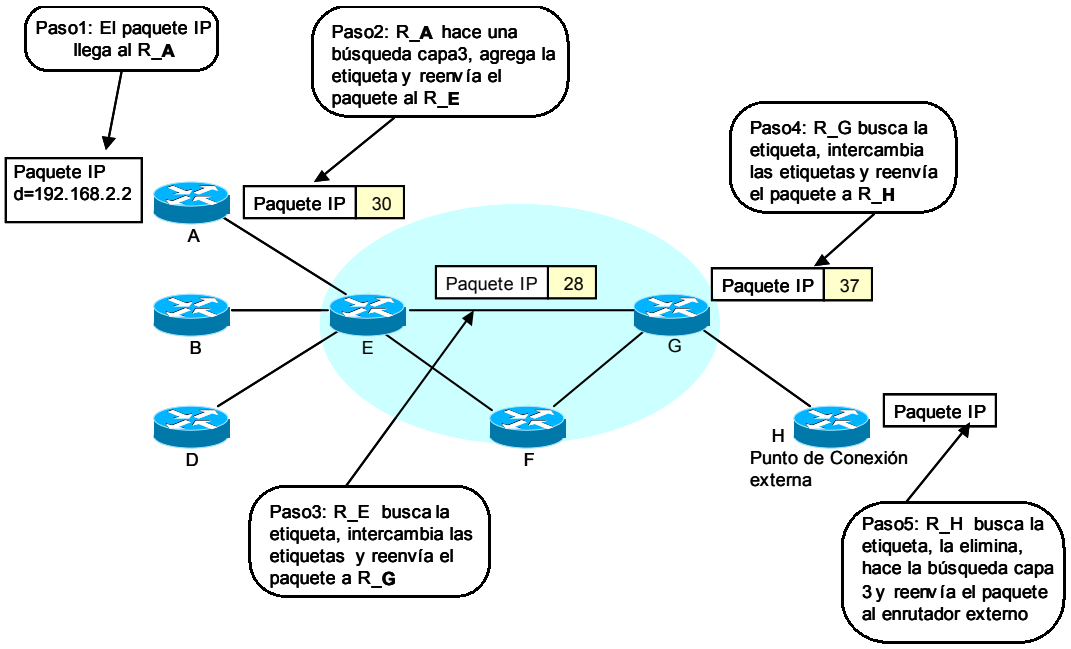

Figura 9: Proceso de doble búsqueda en el enrutador H.

La doble búsqueda en el enrutador H (Ver figura 9) puede reducir el rendimiento del nodo. Además, en ambientes donde MPLS y la conmutación IP se realizan en la parte física del equipo, el factor de la doble búsqueda necesita ser ejecutada y puede incrementar la complejidad de la implementación considerablemente.

PHH se usa sólo para conectar subredes directamente. En caso de una interfaz conectada directamente, es necesario hacer la búsqueda capa 3 para obtener la información correcta del próximo salto del paquete. Con el PHH, el enrutador de salida puede solicitar al enrutador ascendente vecino la remoción de la etiqueta. En la Figura 10 el enrutador G remueve la etiqueta y envía un paquete puro IP al enrutador H. Entonces el enrutador H tiene solo la función de hacer la búsqueda capa 3 y reenviar el paquete a su destino final.

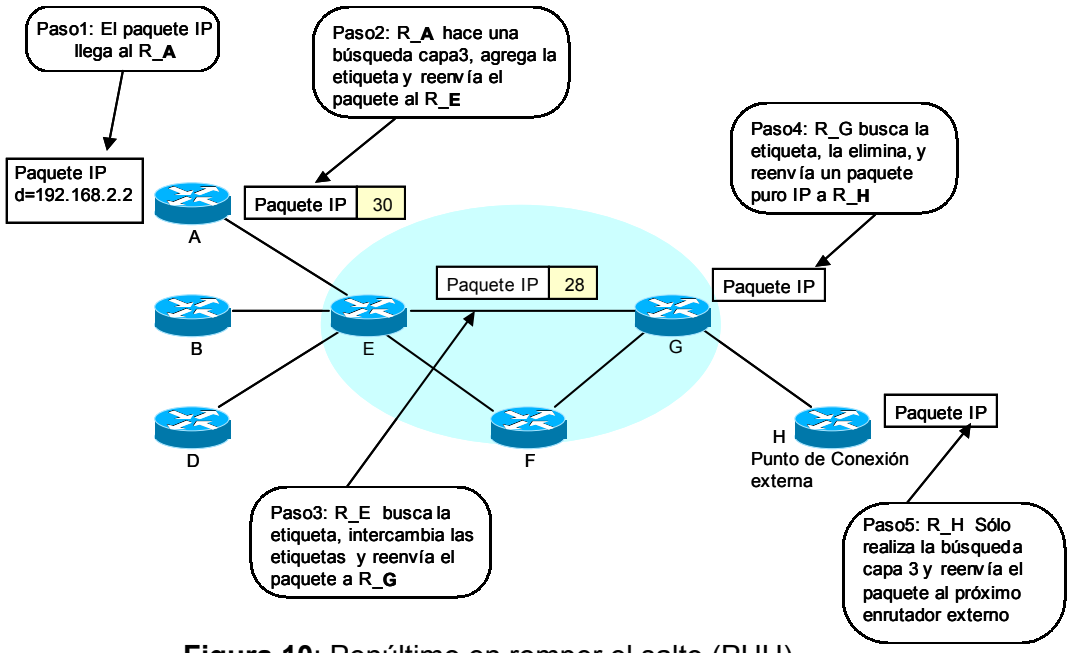

Figura 10: Penúltimo en romper el salto (PHH)

2.3 OPERACIÓN EN MODO CELDA

En el modo trama se puede observar el intercambio de paquetes puro IP y paquetes etiquetados MPLS sobre el mismo enlace. Cuando se trata de unir la arquitectura MPLS con ATM podemos conseguir los siguientes obstáculos:

- No existe un mecanismo directo para el intercambio de paquetes IP entre nodos adyacentes MPLS sobre una interfaz ATM. Todos los datos deben estar contenidos en un circuito virtual ATM (VC ATM).
- Los conmutadores ATM no ejecutan búsquedas de etiquetas ni tampoco búsquedas capa 3. La única capacidad de un conmutador ATM es mapear el VC de entrada en una celda hacia un VC de salida.

El diseño y la arquitectura de ATM presentan algunos cambios en la implementación de MPLS:

- ❖ Los paquetes IP en panel de control no pueden ser intercambiados directamente sobre una interfaz ATM, se requiere establecer un VC entre los nodos MPLS.
- ❖ Los conmutadores ATM no pueden ejecutar una búsqueda de etiquetas. La etiqueta superior en una pila debe ser trasladada en el identificador de la ruta virtual (VPI) y en el identificador del circuito virtual (VCI).
- ❖ Los conmutadores ATM no pueden ejecutar búsqueda capa 3.

2.3.1 Conectividad del plano de control

La arquitectura MPLS requiere de una conectividad IP con el plano de control de los LSRs adyacentes para el intercambio de etiquetas. En el modo trama este requerimiento es sencillo debido a que los enrutadores pueden enviar y recibir paquetes IP y paquetes etiquetados por cualquier interfaz, LAN o WAN.

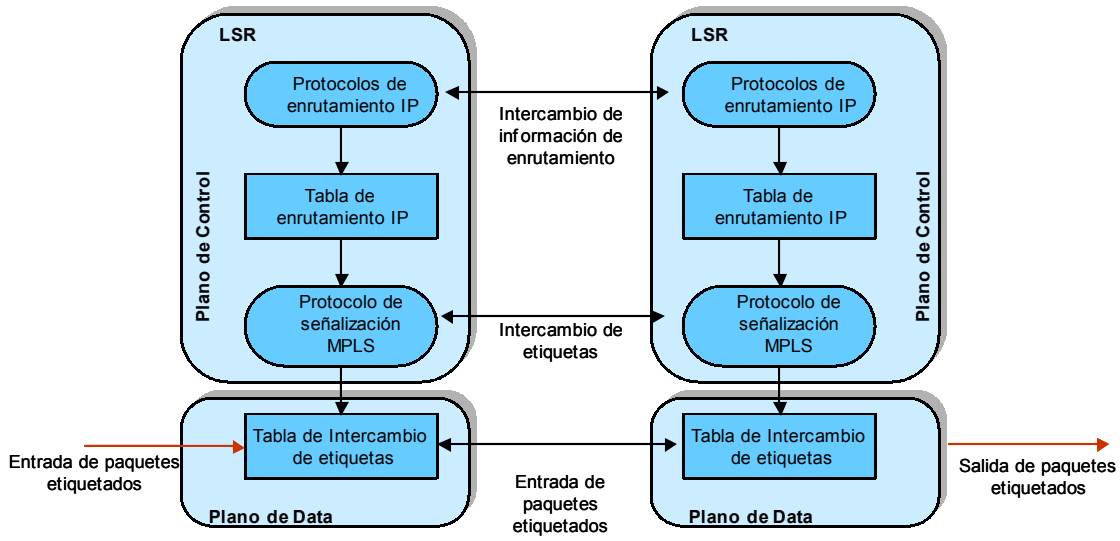

Figura 11: Intercambio de información entre LSRs

En ATM sin embargo, se deben realizar dos procedimientos para garantizar esta conectividad entre los ATM-LSR:

- A través de una conexión fuera de banda (Out-of-Band) como una conexión Ethernet entre dos conmutadores.
- A través de la administración de un circuito virtual VC en banda. El detalle de esta conexión se muestra en la Figura 12.

El VC MPLS es configurado por defecto en el VC 0/32 y debe usar encapsulado de paquetes IP LLC/SNAP.

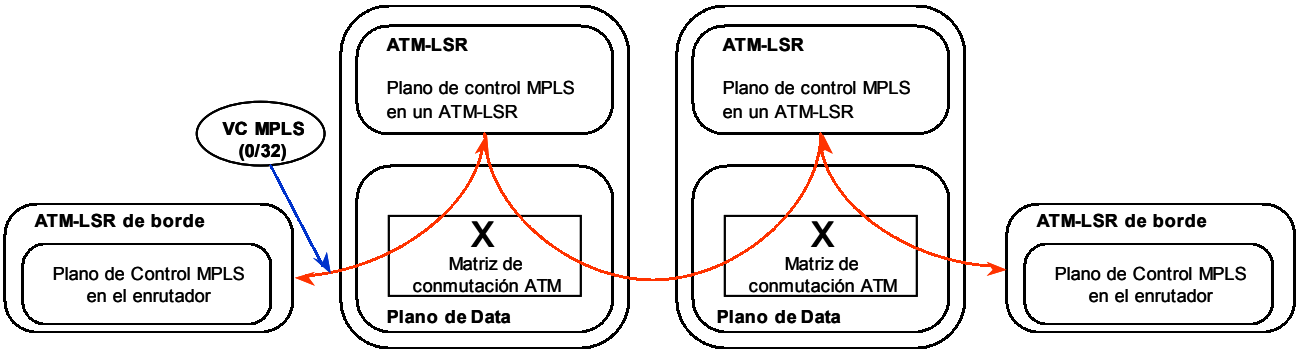

Figura 12: Arquitectura de un circuito virtual MPLS

2.3.2 Intercambio de un paquete etiquetado

El intercambio de un paquete etiquetado a través de un dominio ATM-LSR se ejecuta en tres pasos:

- El ATM-LSR entrante de borde recibe un paquete etiquetado o no, ejecuta una FIB o LFIB y encuentra el valor de salida VPI/VCI, la cual es usada por la

etiqueta de salida. El paquete etiquetado es segmentado en una celda ATM y se envía a través del próximo ATM-LSR. El valor VPI/VCI es encontrado durante la fase de búsqueda de la etiqueta y se coloca en el encabezado de la celda ATM.

- El mecanismo de conmutación es el mismo utilizado en la conmutación ATM tradicional, la colocación y distribución de etiquetas son responsables de mantener el correcto mapeo de los VPI/VCI entrante y saliente.
- El ATM-LSR saliente de borde reensambla las celdas en un paquete etiquetado, ejecuta la búsqueda, y envía el paquete hacia el próximo LSR. La búsqueda de etiqueta es basada en los valores VPI/VCI de las celdas entrantes, no en la etiqueta superior de la pila.

Existen tres diferencias significativas entre el modo trama y el modo celda, estas son:

- La búsqueda de etiquetas en modo trama se realiza en base a la etiqueta superior de la pila del encabezado MPLS. En el modo celda la búsqueda se realiza en función de los valores VPI/VCI en el encabezado de la celda ATM.
- El mecanismo de conmutación en el modo celda es similar al utilizado en la conmutación ATM tradicional basado en los valores VPI/VCI, la pila de etiquetas en MPLS es ignorada completamente por los ATM-LSRs.
- La etiqueta superior de la pila MPLS es configurada en 0 en el ATM-LSR saliente de borde.

2.3.3 Colocación y Distribución de las etiquetas

El proceso de colocación y distribución de etiquetas a través de un ATM-LSR se realiza bajo las siguientes características:

- La colocación de la etiqueta en equipos con capacidad capa 3 (Enrutadores) se hace sin importar si el enrutador ya ha recibido una etiqueta del mismo prefijo desde el próximo enrutador. Este proceso es llamado *Control Independiente.*
- La colocación de etiquetas en equipos capa 2 (Conmutadores ATM) se ejecuta solo si ya existe una etiqueta colocada en el paquete. Este proceso también es llamado *Control Ordenado*.
- El método de distribución de etiquetas sobre una interfaz ATM es por demanda descendiente (*downstream on demand*) debido a que los LSR asignan una etiqueta solo cuando haya sido solicitada por un LSR ascendente.

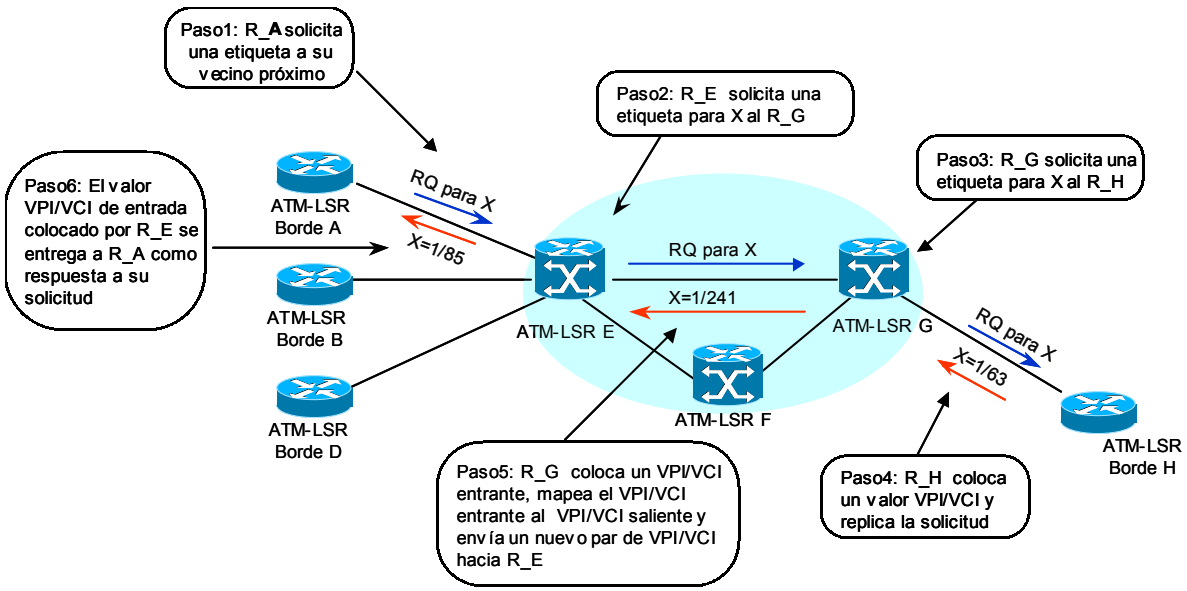

Figura 13: Proceso de etiquetado en un dominio ATM.

En la figura 13 se muestra el proceso para la colocación y distribución de etiquetas a un paquete con destino X, desde un ATM-LSR de borde A hacia una ATM-LSR de borde H.

- El R_A necesita una etiqueta para un destino X. Su tabla de enrutamiento indica que la mejor forma de llegar a X es a través de una interfaz ATM, entonces realiza la solicitud de una etiqueta a su ATM-LSR descendiente.
- El R_E es una conmutador clásico ATM (ATM-LSR) operando en modo *Control Ordenado*, entonces hace la solicitud de la etiqueta al R_G.
- Similarmente el R_G solicita una etiqueta al R_H.
- El R_H opera en modo *Control Independiente* y puede colocar inmediatamente una etiqueta para el destino solicitado. Si el R_H ya tiene una etiqueta para el destino X, éste mapea esa etiqueta con el valor colocado del VPI/VCI en su tabla LFIB. El valor VPI/VCI es enviado de regreso al R_G en un paquete TDP/LDP.
- Después de recibir la etiqueta, el R_G coloca otra etiqueta para su LSR ascendente y realiza el mapeo en su matriz de conmutación entre el nuevo par VPI/VCI y el que recibió del descendiente R_H. El nuevo par VPI/VCI es enviado al R_E en un paquete de respuesta TDP/LDP.
- El R_E realiza una operación similar, coloca otro par VPI/VCI y envía el nuevo par al R_A para el destino X.
- Después de recibir una respuesta a la solicitud de etiqueta, el R_A puede colocar el par VPI/VCI recibido por R_E en su FIB y en su LFIB.

2.3.4 Convergencia de la red a través de un dominio ATM

La convergencia de las redes ATM tradicionales consiste en:

- Un enrutador de borde detecta una falla en el enlace a través de señalización ATM, celdas de operación y mantenimiento (OAM) o a través de los tiempos de espera de los protocolos de enrutamiento.
- Cuando el enrutador de borde detecta la falla del enrutador vecino o adyacente, propaga el cambio de la topología de la red a todos los otros enrutadores.
- En los protocolos de estado de enlace, todos los enrutadores recalculan una nueva topología luego de un leve retraso.

Cuando se incluye MPLS a una red ATM, el tiempo de convergencia consiste en:

- Un LSR debe detectar la falla de un LSR vecino. Este proceso es usualmente muy rápido debido a que los enlaces punto a punto y la capa física entre LSRs adyacentes detectan las fallas muy rápido.
- Los LSR deben propagar los cambios en la topología de la red a otros LSRs. Este proceso toma mayor tiempo en la red MPLS debido al incremento del número de enrutadores entre el borde de la red ATM. Todos los conmutadores que son transparente al enrutamiento IP en la red ATM ahora actúan como enrutadores IP.
- Todos los LSR incluyendo los conmutadores ATM deben recalcular la nueva topología y cambiar su tabla de enrutamiento.
- Si el próximo salto para un destino X ha cambiado, el ATM-LSR de borde debe solicitar nueva etiqueta para ese destino. Los otros ATM-LSRs deben propagar esa solicitud de etiqueta hacia el dominio ATM.

3. REDES VIRTUALES PRIVADAS BASADAS EN MPLS

Las VPN´s son definidas como una red en la cual la conectividad de los clientes entre múltiples localidades es desarrollada en una infraestructura compartida con el mismo acceso y políticas de seguridad definidas como una red privada.

Existen tres grandes problemas en una organización típica que se ha tratado de solventar con las VPN´s:

- La comunicación Intra-Organizacional (Intranets)
- La comunicación entre oficinas (Extranet)
- Acceso a usuario móviles, oficinas remotas; a través de un medio económico como el dial-up (Virtual Private Dial-Up Network)

Estos tres tipos de soluciones usualmente abarcan muchas de las tecnologías ofrecidas por los proveedores de servicios, pero difieren grandemente en el nivel de seguridad requerida para su implementación.

Basándose en el intercambio de etiquetas, un único mecanismo de envío proporciona oportunidades a los nuevos paradigmas y aplicaciones. El envío de etiquetas MPLS se realiza con una búsqueda de una etiqueta entrante que, seguidamente, se intercambia con la etiqueta saliente y, finalmente, se envía al

siguiente nodo. Las etiquetas se colocan sólo una vez en los paquetes en el borde de la red MPLS y se quitan en el otro extremo.

La asignación de estas etiquetas a los paquetes se basa en las agrupaciones o en las clases de equivalencia de envío (FEC). Todos los paquetes que pertenecen a la misma FEC reciben un trato similar. La etiqueta se añade entre la cabecera de la capa 2 y la de la capa 3 (en un entorno de paquetes) o en el campo del identificador de ruta virtual / identificador de canal virtual (VPI/VCI) en redes ATM. La red principal simplemente lee las etiquetas, aplica los servicios apropiados y envía los paquetes basándose en ellas.

Este esquema de consulta y envío MPLS, ofrece la posibilidad de controlar explícitamente el enrutamiento basándose en las direcciones de destino y de origen, permitiendo así la introducción más sencilla de nuevos servicios IP.

3.1 OPCIONES DE IMPLEMENTACIÓN

3.1.1 Modelo de revestimiento (oVPN)

En este modelo los proveedores de servicios (ISP) entregan enlaces virtuales entre las distintas localidades del cliente (CPE). Dentro de las responsabilidades del ISP se encuentra proveer al cliente con líneas arrendadas llamadas circuitos virtuales (VCs). Dentro de su clasificación existen los circuitos virtuales permanentes (PVCs) y los circuitos virtuales conmutados (SVC).

El modelo oVPN es el más comúnmente usado en los proveedores de servicios. En este modelo se determina que el diseño y distribución de los circuitos virtuales deben ser de prioridad sobre el flujo de tráfico. Esto significa que se requiere de una estructura orientada a conexión para abastecer el servicio.

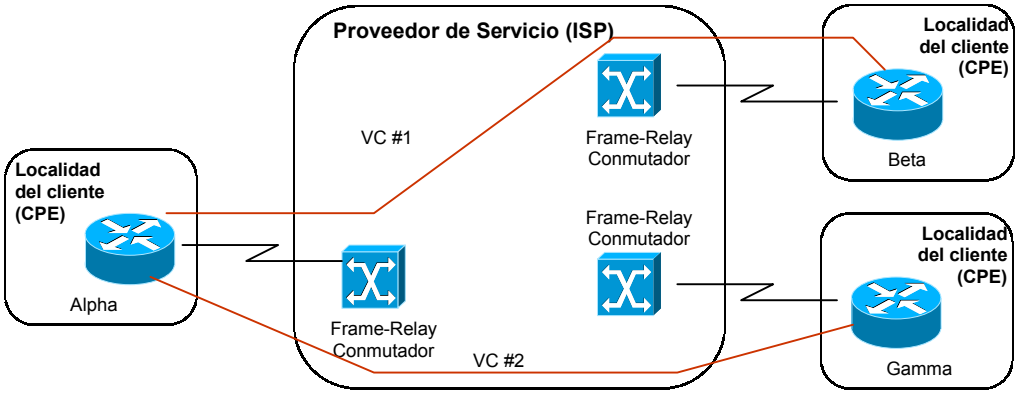

Figura 14: Modelo de una red oVPN

En este diseño el cliente establece una comunicación enrutador-a-enrutador entre el equipo CPE de las distintas localidades sobre los circuitos virtuales entregado por el ISP. La información de enrutamiento se intercambia entre los dispositivos del cliente y el ISP no tiene conocimiento de la estructura interna de la red del cliente.

La *calidad de servicio* (QoS) garantizada en una red oVPN usualmente es expresada en términos de ancho de banda de los circuitos virtuales, a través de los valores como: *Tasa de información comprometida* CIR (Committed Information Rate), *Tasa de información pico* PIR (Peak Information Rate) y *Tasa de información mínimo* MIR (Minimum Information Rate).

A pesar de su fácil entendimiento y aplicación, este tipo de redes presenta algunas desventajas:

- Su diseño es aplicable fácilmente en estructuras que no ameriten conexiones redundantes como por ejemplo una localidad central y varias localidades remotas, pero se convierte sumamente difícil de administrar en configuraciones mezcladas. Esto implica una limitación para servicios VPN a gran escala.
- El abastecimiento de los VCs exige un conocimiento detallado de los perfiles de tráfico de localidad a localidad y un nivel de experticia considerable en enrutamiento IP y QoS lo que no es disponible con facilidad.
- Otros de los inconvenientes de una red oVPN son los cambios en las configuraciones cuando se va a agregar una nueva localidad. Para un cliente que requiera una estructura completamente mezclada agregar una nueva localidad implica cambio de configuración para todas las localidades existentes lo que dificulta la escalabilidad de la red del ISP.

3.1.2 Modelo de par a par (PtP VPN)

En este modelo el proveedor de servicio y los clientes intercambian información de enrutamiento capa 3 y el proveedor transmite los datos entre las localidades de los clientes sobre una ruta óptima.

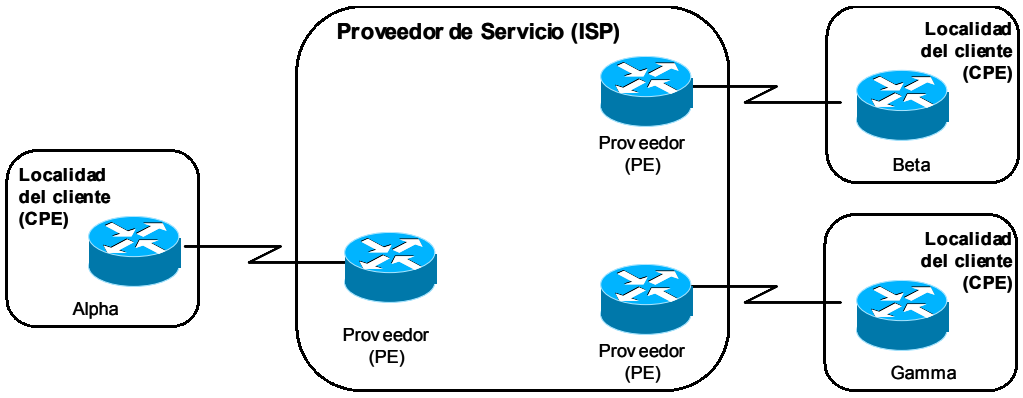

Figura 15: Modelo de Red PtP

Este diseño fue introducido para mejorar las desventajas del modelo oVPN. En el modelo PtP VPN el dispositivo del ISP (PE-enrutador) es un enrutador la cual intercambia información de enrutamiento directamente con el CPE.

Este modelo provee algunas ventajas con respecto al oVPN:

- El enrutamiento se hace más sencillo debido a que el cliente intercambia información de enrutamiento solo con un enrutador del proveedor (PE).
- El enrutamiento entre las localidades del cliente es óptima debido a que los enrutadores del proveedor conocen la topología del cliente y pueden establecer un enrutamiento entre localidades.
- El suministro del ancho de banda es más sencillo debido a que se especifica sólo el ancho de banda de entrada (inbound) y un ancho de banda de salida (outbound) para cada localidad, y no depende del perfil del tráfico entre las localidades.
- Es sencillo agregar una nueva localidad debido a que el proveedor de servicio sólo suministra una localidad adicional y lo agrega en la configuración de PE-

enrutador. En cambio en el modelo oVPN, el proveedor de servicio debe suministrar un VC para cada una de las localidades existentes.

El modelo par a par se divide en dos posibles opciones:

- Enrutador compartido, donde varias localidades comparten el mismo PE-enrutador. Cada cliente es conectado al mismo PE-enrutador, lo que significa que las listas de acceso (Access List) tienen que ser configuradas en cada interfaz PE-CPE para asegurar la separación entre los clientes y prevenir que la red de un cliente pueda interferir con otra.

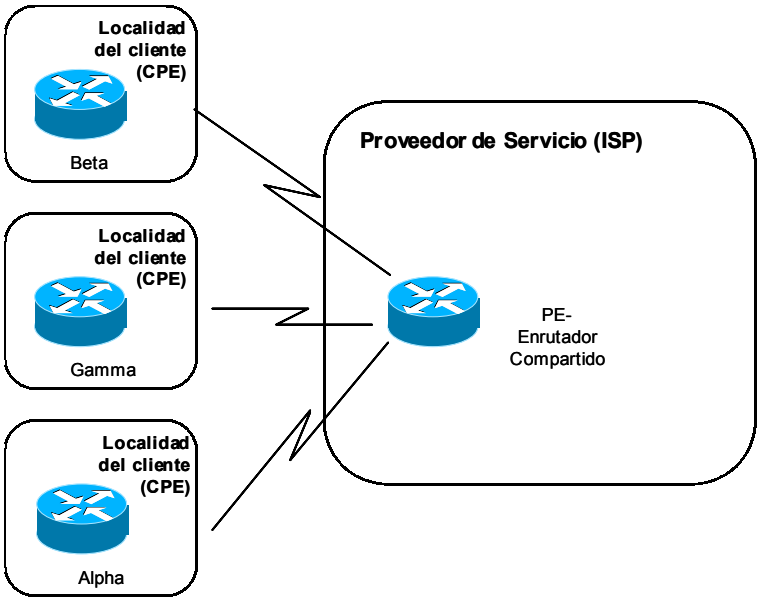

Figura 16: Modelo par a par con enrutador compartido

- Enrutador dedicado, donde cada localidad tiene su propio PE-Enrutador. En este modelo se usa protocolos para crear tablas de enrutamiento por cada VPN en los PE-enrutadores. Las tablas de enrutamiento de los PE-enrutadores contienen

solo las rutas anunciadas por el cliente conectado a ella resultando una mejor separación entre las redes de los clientes.

Desde el punto de vista de los proveedores de servicios el escalamiento de las redes de revestimiento (oVPN) es más compleja cuando se tiene que administrar y provisionar gran cantidad de circuitos entre los equipos del cliente. El protocolo diseñado para esto IGRP (Interior Gateway Protocol) es también difícil de administrar.

En otras palabras el modelo PtP (Par a Par) no tiene la necesidad de separar las redes entre los clientes y de coordinar el espacio de direcciones entre ellos.

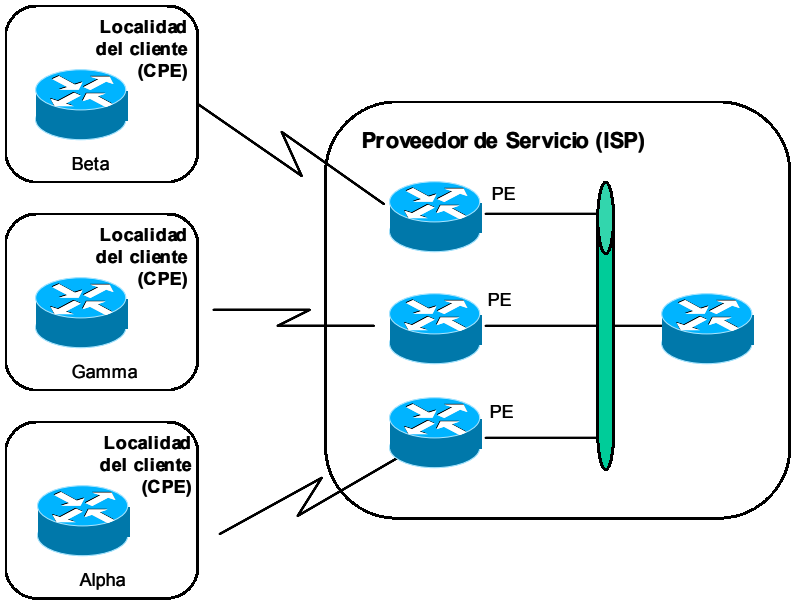

Figura 17: Modelo par a par con enrutador dedicado

3.1.3 Modelo VPN MPLS

La arquitectura de las redes VPN MPLS provee la capacidad de designar a una infraestructura IP para entregar servicios de redes *privadas* sobre una infraestructura *pública*. Las VPNs MPLS son implementadas sobre una estructura basada en MPLS en la red central del proveedor de servicio, tal como se muestra en la figura 18.

Los componentes principales de red VPN MPLS son:

- Enrutador del cliente (CE Customer Edge)
- Enrutador de borde del proveedor (PE Provider Edge)
- Enrutador central del proveedor (P Provider core router)

De acuerdo a la figura 18 se tiene, la VPN A y la VPN B ambas con tres localidades. Estas localidades están conectadas al proveedor de servicio a través de un enrutador cliente (CE). Una localidad puede tener uno o más clientes. Cada cliente CE esta conectado a un enrutador de borde del proveedor (PE), el cual puede conectar varias VPNs, además, estas localidades pueden tener la misma dirección IP. Esto es factible debido a que las direcciones IP son únicas dentro de la VPN pero no necesariamente únicas dentro de múltiples VPNs. El tercer enrutador utilizado en la arquitectura VPN MPLS es el enrutador central del proveedor (P), la cual no esta conectado a ningún CE directamente. Los enrutadores P se distinguen de los PEs debido a que sus funcionalidades son más restringidas.

La razón principal por la cual el modelo VPN MPLS entra dentro de la clasificación de los modelos par a par, es debido a que desde el punto de vista de enrutamiento, la red del proveedor de servicio actúa como un vecino de la red del cliente (CE), a diferencia del modelo de revestimiento donde el cliente se comunica sólo con otros clientes y no con el proveedor directamente.

Las VPN MPLS simplifican considerablemente la instalación de los servicios en comparación con las VPN IP tradicionales. A medida que aumenta el número de rutas y de clientes, las VPN MPLS se pueden ampliar con suma facilidad sin perder el mismo nivel de privacidad de las tecnologías de capa 2.

El modelo VPN MPLS funciona igual al modelo par a par pero:

- Los enrutadores PE reciben y mantienen la información de enrutamiento sólo de las VPN conectadas directamente.
- Se reduce la cantidad de información de enrutamiento que será almacenada en los PEs.
- La información de enrutamiento es proporcional al número de VPNs del enrutador conectado.
- MPLS es usado dentro del backbone para la conmutación de paquetes (No se requiere enrutamiento completo).

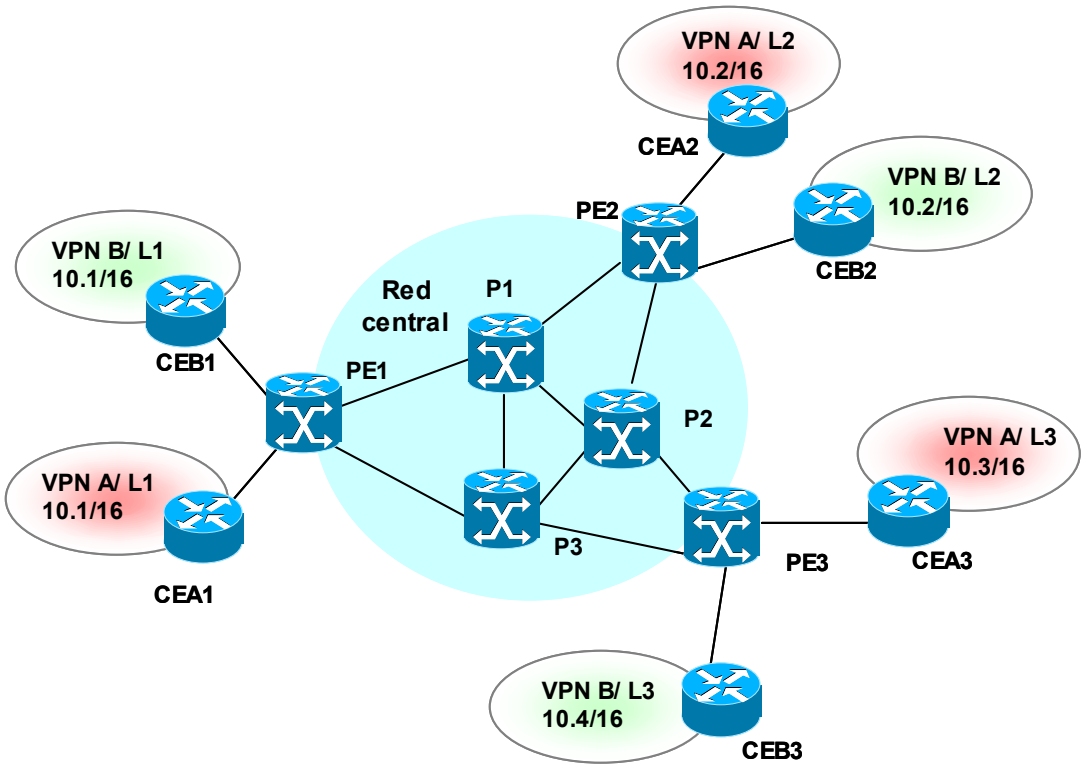

Figura 18: Modelo VPN MPLS

3.1.3.1 MPLS como mecanismo de Intercambio

Para permitir el reenvío de paquetes IP a través de rutas expresadas en términos de direcciones de VPN-IP, se utiliza MPLS. La razón por la cual MPLS permite que esto pueda ser posible es debido a que se hace un acople entre la información usada por el paquete reenviado, es decir, la etiqueta, desde la información cargada en el encabezado IP. Sin embargo, se puede enlazar rutas LSPs a VPN-IP y reenviar los paquetes IP a través de estas rutas usando MPLS como mecanismo de reenvío.

Para mostrar como se realiza este mecanismo se usará la Figura 19. Desde el punto de vista MPLS el enrutador PE es un LSR de borde, es decir, convierte un paquete no etiquetado en un paquete etiquetado.

Cuando el CE envía un paquete IP a un enrutador PE conectado directamente, el PE usa el puerto entrante (la interfaz por la cual el PE recibe el paquete) para identificar la VPN a la cual el CE esta conectado, mas precisamente, para identificar la *tabla de intercambio* (FIB: Forwarding Information Base) asociada a esa VPN.

Una vez que la FIB sea identificada, el PE ejecuta una búsqueda capa 3 en la FIB, usando la dirección destino localizada en el encabezado del paquete IP. Como resultado de la búsqueda el PE agrega la información apropiada de la etiqueta y reenvía el paquete. Para mejorar las propiedades de escalabilidad de este mecanismo se emplea una jerarquía de conocimiento de enrutamiento donde se utilizan dos niveles de etiquetas.

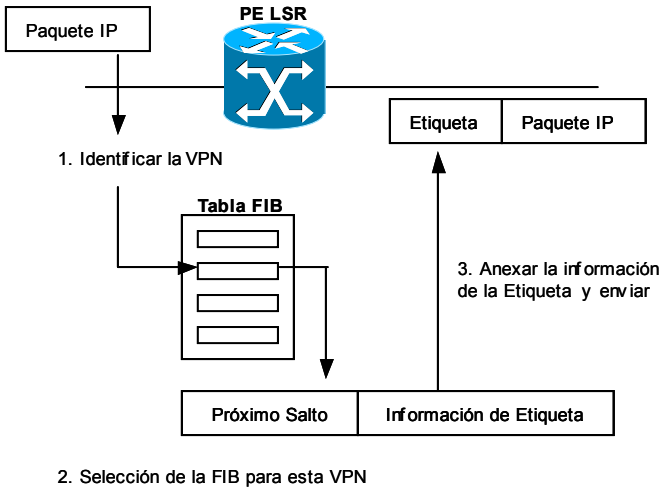

Figura 19: Colocación de la etiqueta por un PE LSR

La primera etiqueta es asociada con la ruta hacia un PE de salida y la segunda etiqueta controla el reenvío del PE de salida. La primera etiqueta puede ser distribuida vía LDP, la segunda etiqueta puede ser distribuida usando BGP.

3.1.3.1.1 Tabla de enrutamiento y reenvío (VRF VPN routing and Forwarding Table)

El solapamiento de las direcciones IP que resulta del uso de direcciones privadas en las localidades de los clientes es uno de los mayores obstáculos en la implementación del modelo par a par descrito anteriormente. La tecnología VPN MPLS provee una solución a este dilema: cada VPN tiene su propia tabla de enrutamiento y reenvío (VRF), entonces cualquier localidad de un cliente que pertenezca a una VPN tendrá acceso sólo al conjunto de rutas contenidas en esa tabla.

La VRF es el elemento principal dentro de la tecnología VPN MPLS. Las VRFs existen solo en los PEs y más de una VRF puede existir en un PE. Una VPN puede contener más de una VRF en un PE y contienen rutas que sólo están disponibles para un conjunto particular de localidades

Cualquier enrutador PE en una red VPN MPLS, contiene un número de tablas de enrutamiento por VPN y una tabla de enrutamiento global que es usada para alcanzar otros enrutadores en la red del proveedor de servicio, además de los destinos alcanzables globalmente (Internet). Efectivamente, los enrutadores virtuales son creados en una única interfaz física de enrutador.

El concepto de enrutador virtual permite que una localidad pueda usar un espacio de direcciones públicas o privadas para su VPN. Para cada localidad que pertenezca a una VPN el espacio de direcciones es único para esa VPN.

3.1.3.1.2 Marcador de rutas (Route Targets)

El marcador de rutas es un concepto que se introduce en la arquitectura de VPN MPLS para solventar el problema de cómo el enrutador conoce cuáles rutas deben ser insertadas y en cuál VRF. El marcador de rutas es similar a un identificador de VPN dentro de la arquitectura VPN MPLS. Cada VPN es marcada con una o más marcadores de rutas cuando son exportadas desde una VRF, es decir, ofrecidas a otros VRFs.

3.1.3.1.3 Propagación de la información de enrutamiento entre enrutadores PE

Existen dos formas para intercambiar rutas VPN entre los PE-Enrutador:

- Los PE-Enrutadores ejecuten un algoritmo de enrutamiento diferente para cada VPN, por ejemplo OSPF o EIGRP. Esta solución presenta problemas de escalabilidad con un gran número de VPNs.
- Los PE-Enrutadores ejecuten el mismo algoritmo de enrutamiento para intercambiar las rutas VPN. Para soportar solapamiento de direcciones en las VPNs de los clientes, la dirección IP utilizada debe ser ampliada con una información adicional para hacer la dirección única.

La segunda opción es la escogida para el intercambio de rutas entre PE en una arquitectura VPN MPLS. Las subredes anunciadas por los enrutadores CE a los enrutadores PE son ampliadas con un prefijo de 64 bits llamado *diferenciador de ruta* (Route Distinguisher) para hacerlas únicas dentro de la red. El resultado es una dirección de 96 dígitos binarios (bits) que son intercambiadas entre los enrutadores PE usando un multiprotocolo BGP (MP-BGP).

Este intercambio se hace a través del protocolo BGP por las siguientes razones:

- El número de rutas VPN en una red puede llegar a ser muy grande. BGP es el único protocolo de enrutamiento que puede soportar un número muy grande de rutas.
- BGP, EIGRP e IS-IS, son los únicos protocolos por diseño (MP-BGP). IS-IS y EIGRP sin embargo, no son recomendables para un gran número de rutas como lo es BGP. Además, BGP esta diseñado para intercambiar rutas que no estén conectadas directamente. Esta característica de BGP mantiene la información de enrutamiento fuera de los enrutadores centrales del proveedor de servicio (Enrutadores P).
- BGP puede cargar información de una ruta como un atributo opcional de BGP. Esta propiedad hace posible de manera muy sencilla la propagación de los marcadores de rutas entre enrutadores PE.

Intercambio de paquetes VPN.

Cada enrutador PE coloca una única etiqueta para cada ruta en la tabla VRF. Estas etiquetas son propagadas junto con la ruta correspondiente a través de un MP-BGP a todos los otros enrutadores PE. Los enrutadores PE reciben la actualización de MP-BGP e instalan las rutas y las etiquetas asignadas en su VRF. En este momento la red MPLS está preparada para el envío de un paquete VPN.

Cuando el paquete es recibido por el enrutador PE de entrada, se examina la tabla VRF correspondiente a esa VPN, y se asocia la etiqueta con la dirección destino

hacia el enrutador PE de salida. Además se agrega otra etiqueta que apunta hacia el enrutador de salida y que es obtenida desde la tabla de reenvío global. Ambas etiquetas son combinadas en la pila de etiquetas MPLS, son colocadas en el paquete VPN y enviadas hacia el PE de salida.

Todos los enrutadores P conmutan o reenvían el paquete basado sólo en la etiqueta superior de la pila, la cuál indica el camino hacia el PE de salida.

3.1.3.2 Enrutamiento

En una red VPN MPLS existen tres dominios de enrutamiento:

- Entre CE y PE: Se puede utilizar como protocolo de enrutamiento: rutas estáticas, RIPv2, EIGRP, OSPF y eBGP.
- Entre PE y PE: Las actualizaciones de rutas se pueden realizar a través de MP-BGP.
- Entre PE y P: Ninguna de las rutas VPN son intercambiada o almacenada por los enrutadores P. Los enrutadores P solo realizan la conmutación MPLS a través de la red del proveedor de servicio basado en el intercambio del primer nivel de etiquetas hacia el próximo salto.

3.1.3.3 Escalabilidad

En un diseño de VPN la cantidad de vecinos que el enrutador CE debe mantener es constante y por lo tanto independiente del total de números de localidades dentro de una VPN, así como también de los cambios de configuración necesarios cuando se agrega o elimina una localidad.

Ahora bien, primero, empleando la jerarquía de enrutamiento de MPLS se mantienen todos los enrutadores centrales del proveedor (P) libres de cualquier información de enrutamiento de VPN, es decir, la información de enrutamiento de las VPN es mantenida solo por los enrutadores PE.

Segundo, los PEs mantienen la información de enrutamiento de las VPNs solo las localidades que estén conectadas directamente. Si el volumen de información de enrutamiento es muy alto para ese PE, se puede agregar otro PE y mover algunas de las VPNs para ese nuevo PE.

Finalmente, cómo manejar los enrutadores reflectores con protocolos de enrutamientos interdominios (BGP). Los enrutadores reflectores son los que propagan las rutas iBGP entre otros vecinos iBGP. Con la introducción de enrutadors reflectores, la escalabilidad de MP-iBGP es más sencilla debido a que se elimina el requerimiento de una arquitectura completamente mezclada.

Para evitar la situación de que un solo reflector maneja todas las VPN, se divide el grupo en varios reflectores, es decir, las primeras 100 VPN en el primer reflector, las segundas 100 en el segundo reflector y así sucesivamente. Con lo anterior, se puede concluir que no existe un componente dentro de la red del proveedor de servicio que requiera mantener toda la información de todas las VPNs soportadas. Es decir, la capacidad de enrutamiento de las VPN de la red de un proveedor de servicio no depende de la capacidad de un componente individual, lo que resulta una característica no limitativa para la escalabilidad de las VPN MPLS.

3.1.3.4 Seguridad

La seguridad es uno de los componentes más importantes en soluciones de VPN confiables. El objetivo principal es cerciorarse de que, en ausencia de la interconexión deliberada o de la pérdida de configuración, los paquetes desde una VPN no podrían alcanzar o llegar a otra VPN.

Para estudiar como se puede alcanzar esto con MPLS, primero se debe observar que el intercambio de paquetes en un proveedor de servicio de VPN está basado en la conmutación de etiquetas y no en el intercambio tradicional de enrutamiento IP. Por lo tanto, el envío o intercambio de paquetes dentro del proveedor no esta determinado por la dirección IP que se encuentra en el encabezado del paquete sino en las LSPs asociadas a cada VPN IP, las cuales se originan y terminan solo en los enrutadores PE. Esto es, las LSPs son asociadas a una tabla de reenvío particular, y esa tabla a su vez está asociada con la interfaz del PE conectada directamente, la cual determina una VPN en particular.

Por lo tanto, cuando un PE envía un paquete a un CE que pertenece a una VPN particular, este paquete llega o a otro PE o a otro CE conectado directamente. Esto es posible siempre y cuando ambos CE pertenezcan a la misma VPN y compartan la misma tabla de reenvío. En último caso, el paquete tiene que ser reenviado por un PE a través de una LSP asociada con una tabla de reenvío particular, donde la tabla a su vez esa está asociada con la VPN a través de configuración.

Como resultado, en ausencia de una configuración consistente, inyectar un paquete en una VPN se podría hacer solamente a través de una interfaz asociada con esa VPN. Por lo tanto, los paquetes no se pueden inyectar maliciosamente o accidentalmente en una VPN al cual el remitente no pertenezca.

3.1.3.5 Calidad de Servicio (QoS)

En el área de Qos, el desafío es desarrollar un sistema de mecanismos que soporte QoS de una forma flexible y escalable para un gran número de clientes VPN. Por ejemplo, un proveedor de servicio podría ofrecer múltiples *clases de servicio* (CoS Class of Services), esto es, no todas las VPN tienen que usar todas las clases de servicios que el proveedor pueda ofrecer.

La Clase de Servicio (CoS) se refiere a los métodos que proveen *servicios diferenciados* (Diff-Serv), en la cuál la red entrega un servicio particular dependiendo de la clase de servicio especificado por cada paquete. La clase de servicio provee tres categorías específicas: Oro (Gold), Plata (Silver) y Mejor-Esfuerzo (Best-Effort).

MPLS utiliza diff-serv para asegurar que los paquetes marcados con el *código de servicio diferenciado* (DSCP) reciban el tratamiento adecuado en cada LSR de la red. Esto es, en MPLS se utiliza los 3 bits del encabezado de la etiqueta (bit experimental) para marcar la QoS en las redes de paquetes. Para el caso de las redes de celdas, el tratamiento es diferente puesto que se utiliza el valor de la etiqueta incluida en el VCI/VPI y no existe el bit experimental. En este caso se necesita reforzar los

mecanismos de distribución de etiquetas para transportar la información de clase de servicio dentro de la etiqueta.

A continuación se explican dos modelos que son usados por VPN MPLS para describir QoS en el contexto de las VPN, una forma de comercializar las VPN por parte de los proveedores de servicio: Modelo Tubo (Pipe) y Modelo Manga (Hose).

En el modelo tubo el proveedor de servicios suple a los clientes VPN con cierta garantía de QoS para el tráfico de un CE a otro. Un ejemplo de este modelo podría ser el mínimo ancho de banda garantizado por el proveedor entre dos localidades.

El modelo tubo es similar (pero no idéntico) al modelo de QoS utilizado por las soluciones basadas en ATM y Frame Relay. La diferencia principal radica en que el modelo tubo ofrece una garantía de QoS unidireccional. La razón por la cual el modelo tubo es unidireccional permite una solución asimétrica con respecto al patrón de tráfico, por lo que la cantidad de tráfico puede ser diferente a la dirección inversa.

En el ejemplo mostrado en la figura 20, se puede observar que el proveedor de servicio provee una VPN **A** con una tubo que garantiza un ancho de banda de 7 Mb por segundo para el tráfico desde la CE_{A3} a CE_{A1} y otro tubo que garantiza un ancho de banda de 10Mb por segundo desde CE_{A3} a CE_{A2}. Esto demuestra que un CE puede originar mas de una tubo, como es el caso del CE_{A3} en la figura 20. Asimismo, una CE también puede terminar más de un tubo.

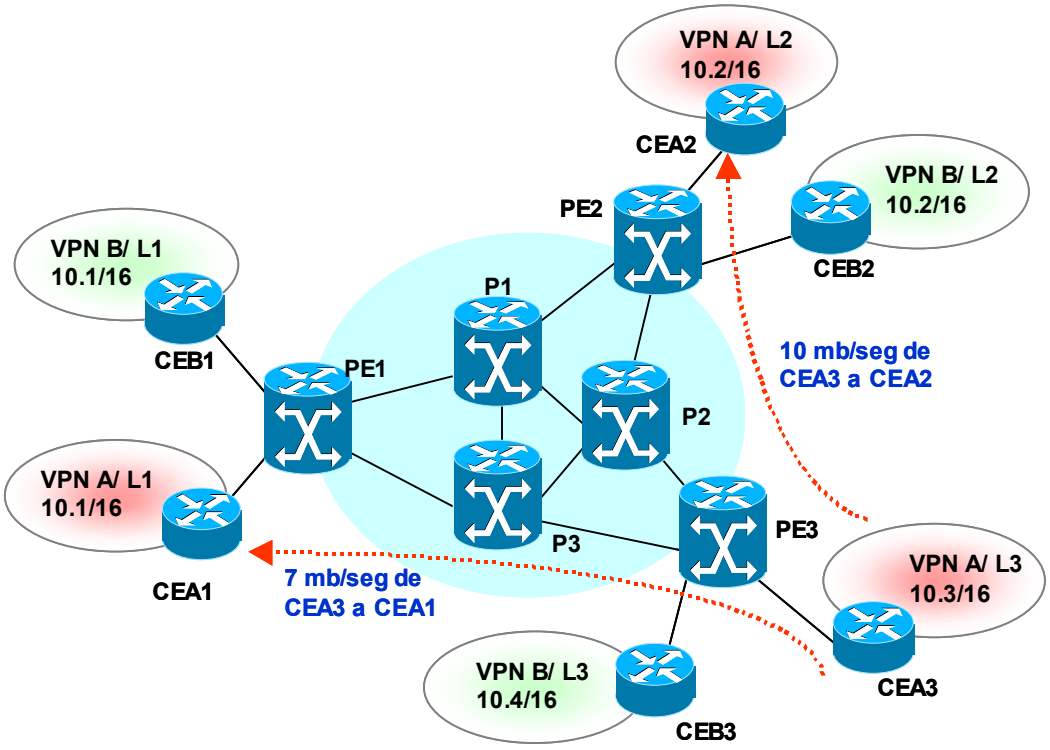

Figura 20: Modelo Tubo QoS

Una de las ventajas de este modelo tubo es que tiene mucha similitud con el modelo de QoS aplicado por ATM y Frame Relay, por lo tanto será fácil de entender y de aplicar. Pero también tiene algunas desventajas, como por ejemplo este modelo asume que los clientes (CE) conocen completamente la matriz de tráfico de cada localidad a la que pertenece. Esta información de tráfico no está disponible fácilmente y en caso de estarlo por lo general se encuentra obsoleta.

En el modelo manga mostrado en la figura 21, se usan dos parámetros: Tasa Confiable de Entrada (Ingress Committed Rate ICR) y la Tasa Confiable de Salida (Egress Committed Rate). El ICR es la cantidad de tráfico que un CE puede enviar a otro CE, mientras que el ECR es la cantidad de tráfico que un CE puede recibir de otro CE.

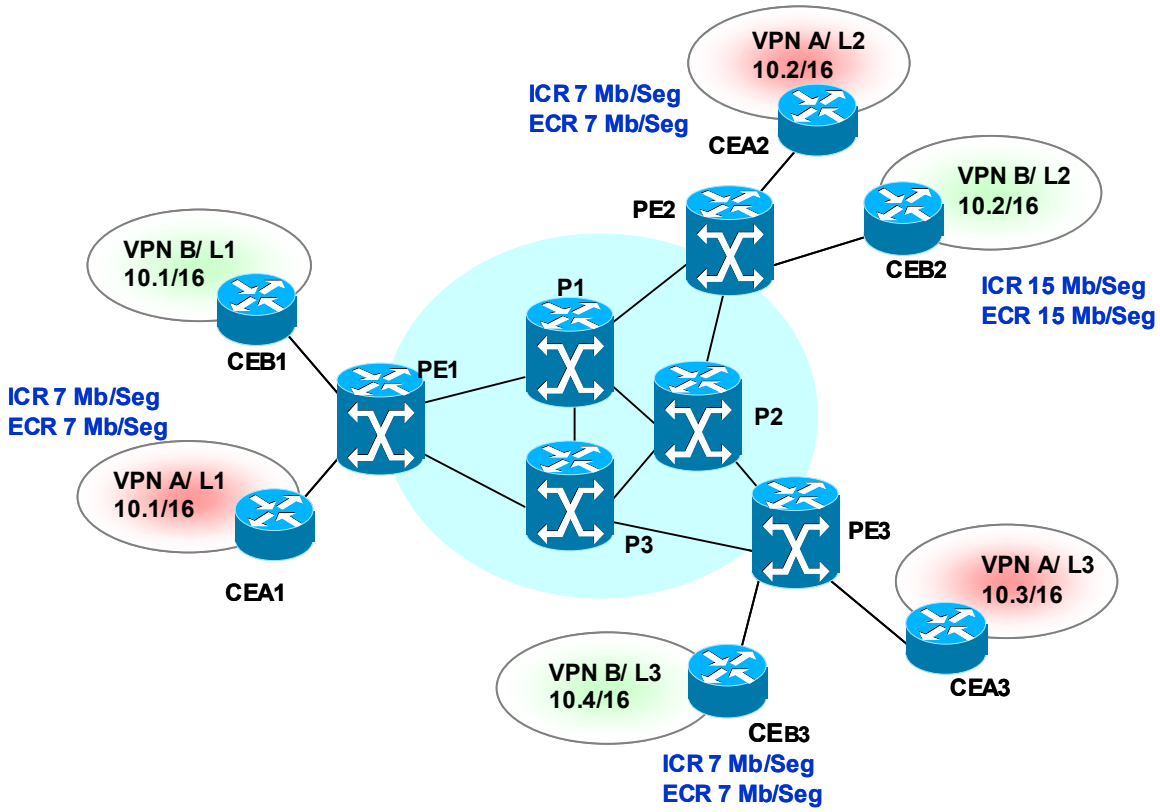

Figura 21: Modelo Manga QoS

De acuerdo a lo mostrado en la figura 21 el proveedor de servicio entrega una VPN **B** garantizando hasta 15 Mb por segundo para el tráfico desde la localidad 2 (CE_{B2}) a otras localidades, sin importar que este tráfico vaya a la localidad 1 (CE_{B1}) o a la localidad 3 (CE_{B3}) o si es distribuida entre CE_{B1} y CE_{B3}.

Para soportar el modelo tubo, se utiliza las LSPs con ancho de banda garantizado. Las LSPs se originan y terminan en los enrutadores PE y son usadas para proporcionar ancho de banda garantizado para todos los tubos desde un PE a otro. Por ejemplo, en la figura 20 puede hacer un tubo para VPN **A** desde CE_{A3} hasta CE_{A1} y otro tubo para VPN **B** desde CE_{B3} hasta CE_{B1}. Para soportar estos dos tubos se establece

una única LSP con ancho de banda garantizado desde PE_3 hasta PE_1 y se reserva en esa LSP la cantidad de ancho de banda igual a la suma de los anchos de banda de los dos tubos. Cuando PE_3 recibe un paquete desde CEA_3 que está destinado a la localidad 1 de la VPN **A**, entonces el PE_3 envía el paquete a través de la LSP con ancho de banda garantizado que ya estaba establecida desde PE_3 a PE_1.

Usando esta técnica de la LSP con ancho de banda garantizado para cargar múltiples tubos entre un par de PE, mejora las propiedades de escalabilidad de la solución debido a que el número de LSPs con ancho de banda garantizado que el proveedor de servicio puede establecer y mantener, está limitado por el número de pares de PEs más que por el número de clientes (CE) que el proveedor pueda tener.

4. PERSPECTIVA DE LA TECNOLOGÍA MPLS

Actualmente la propuesta de MPLS es el resultado de un proceso de integración y convergencia de las redes de los proveedores de servicios sobre una misma infraestructura IP, y que se propone como la tecnología que se impondrá en los próximos años.

En Venezuela hoy día la perspectiva de la tecnología MPLS se percibe como muy exitosa para los proveedores de servicios, TELCEL y NETUNO son los primeros ISP que migraron a MPLS; y de acuerdo al mercado, la demanda se inclina a servicios Capa 2, sobre una red central pura MPLS. Cisco es uno de los fabricantes que ha incorporado esta solución en su portafolio.

Los servicios de Capa 2 con ancho de banda asegurado, combinan cualquier transmisión de datos por MPLS, ingeniería de tráfico y calidad de servicio (QoS). Los proveedores de servicios ahora pueden conectar cualquier transporte Capa 2 en una infraestructura convergente de IP/MPLS única, lo que representa un ahorro significativo en los costos operativos, y en la capacidad de ofrecer servicios de valor agregado como intranets, redes privadas de voz por IP, etc.

Tecnologías como Ethernet sobre MPLS (EoMPLS), ATM sobre MPLS (ATMoMPLS), Frame Relay sobre MPLS (FRoMPLS); refuerzan la definición de MPLS como una tecnología convergente.

La solución multicast MPLS (M-MPLS) está siendo fuertemente discutida por las compañías de telecomunicaciones. Esta tecnología ha sido diseñada como mecanismo de transporte para las redes de acceso, el cual permite la distribución simultánea de grandes volúmenes de datos como: video, multimedia Interactiva en tiempo real, etc.

Otra de las soluciones innovadoras es MPLS VPLS (MPLS Virtual Private LAN Services). VPLS es una tecnología de servicios capa 2 multipunto que permite la conexión de varias localidades sobre un dominio Ethernet a través de un proveedor de servicio basado en IP/MPLS, es decir, VPLS entrega servicios capa 2 sobre una infraestructura capa 3. Es una extensión de EoMPLS para la entrega de servicios capa 2 punto a punto.

Haciendo una análisis de todas las tecnologías y soluciones que se derivan de MPLS, personalmente opino que existen muchos intereses por parte de los fabricantes como para llegar a una integración completa entre IP y ATM; me inclino más bien hacia la convergencia de las tecnologías de transporte que hacia la integración en la red central de los proveedores de servicio. De hecho, la mayoría de las tecnologías y soluciones antes mencionadas se basan en servicios capa 2 pero sobre una red central IP/MPLS.

5. EJEMPLO DE IMPLEMENTACIÓN

Introducción

De acuerdo a lo expuesto anteriormente en la perspectiva de la tecnología MPLS y resumiendo los beneficios de las redes virtuales privadas a través de MPLS a continuación se presenta un ejemplo de implementación orientado a aquellos proveedores de servicios (ISP) que desean ofrecer servicios de valor agregado para usuarios residenciales utilizando una estructura de red central pura IP/MPLS. Con esta tecnología, los proveedores de servicio pueden ofrecer servicios avanzados y escalables entre diferentes localidades para la creación de VPN, ofreciendo valores agregados y soluciones diferenciales basadas en IP.

El objetivo principal es permitir Acceso Remoto a Internet para usuarios residenciales a través de una red central VPN MPLS de un proveedor de servicio, bajo los siguientes requerimientos:

- Interoperabilidad e integración: El diseño propuesto es una plataforma flexible capaz de integrarse con los servicios IP propios de un ISP.
- Escalabilidad: Se propone un diseño altamente escalable tomando en consideración los beneficios de la VPN MPLS.
- Seguridad: Cada usuario residencial gozará de los niveles de seguridad propios de una VPN a través de la red de un ISP.

- Rentabilidad: Se propone un diseño rentable tanto para el usuario final como para el ISP. La solución de última milla está basada en acceso inalámbrico bajo la banda de frecuencia no licenciada 2.4GHZ. Este servicio cuenta con un equipamiento económico.

Premisas de diseño

1. Se propone un diseño para ISPs que tenga una estructura con capacidad de ofrecer servicios de Internet y que desean integrar nuevas tecnologías de acuerdo a la demanda del mercado actual.
2. Se requiere de una solución de completa interoperabilidad e integración con los servicios IP propios de un proveedor de servicio.
3. Se requiere una red central IP capaz de escalar y de soportar la inserción de redes virtuales privadas basadas en IP (IP VPNs) garantizando su calidad de servicio (IP QoS).
4. La red de transmisión entre Celdas se basa en capacidades de E1(2.048Mbps), o múltiples de estas capacidades (nxE1).
5. Se requiere una plataforma lo suficientemente flexible para la creación de servicios adicionales de voz, datos o video que permita ahorrar costos de inversión futuros.
6. La red central estará formada por cuatro ciudades principales: Caracas, Valencia, Maracaibo y Puerto La Cruz; concentrando la mayor cantidad de tráfico en Caracas.
7. Cantidad de clientes propuesto para el primer semestre:

Ciudad	Celdas	Sectores	Cliente x Sector	Total Clientes
Caracas	2	12	60	720
Valencia	1	6	60	360
Maracaibo	1	6	60	360
Puerto La Cruz	1	6	60	360
Totales	**5**	**30**		**1800**

8. Se ofrecerá tres niveles de servicios principales para el acceso a Internet:
    a. MPLS VPN Oro: 1024Kbps
    b. MPLS VPN Plata: 512Kbps
    c. MPLS VPN Bronce. 256Kbps

Topología de la Red

La funcionalidad del servicio está basada en el Acceso Remoto a Internet a través de MPLS VPN, donde el acceso inalámbrico del cliente esta basado en VPN de diferentes servicios. Los enrutadores PE terminan todas las sesiones PPPoE y mapea el usuario remoto a la VRF correspondiente. EL siguiente evento ocurre cuando el usuario remoto crea una sesión PPPoE para accesar al proveedor de servicio o a su red corporativa.

1. El usuario remoto inicia una sesión PPPoE. Si el usuario final es residencial, la sesión PPPoE es conmutada a través del cliente PPPoE instalado en la máquina del suscriptor. Si la sesión es creada por una red, el cliente PPPoE es ofrecido por el enrutador del cliente. La unidad inalámbrica del suscriptor actúa como

conmutador en los enlaces de datos Ethernet permitiendo todo tipo de tráfico sin modificar la trama.

La sesión PPPoE provee la habilidad de conectar una red o PC a través de un dispositivo de acceso (SU) hacia un equipo o concentrador de acceso remoto (PE). El control de acceso, facturación, y tipo de servicio es realizado por usuario más que por localidad, en vista de que la solución es ofrecida para usuarios residenciales. Cuando el cliente inicia una sesión PPPoE, éste debe primero identificar a cuál servidor le realizará la petición y obtener los datos necesarios para el acceso a la red del proveedor de servicio.

2. El enrutador instalado en la celda es el PE, éste recibe y termina todas las sesiones PPPoE. Envía las consultas al RADIUS (consisten en mensajes de solicitud de acceso al servidor de Registro de Acceso) para asociar al usuario remoto con la MPLS VPN específica de ese usuario. La tabla VRF debe estar previamente configurada.

3. El enrutador PE completa la autenticación del usuario remoto a través del servidor RADIUS. La autenticación se basa en el nombre de usuario y la contraseña.
4. Durante la negociación el enrutador PE envía los parámetros de red al usuario remoto para realizar la conexión: dirección IP, máscara de subred, enrutador de salida y servidores DNS.
5. El usuario remoto es ahora parte de una MPLS VPN para el acceso a Internet. Los paquetes pueden fluir desde o hacia el usuario remoto.

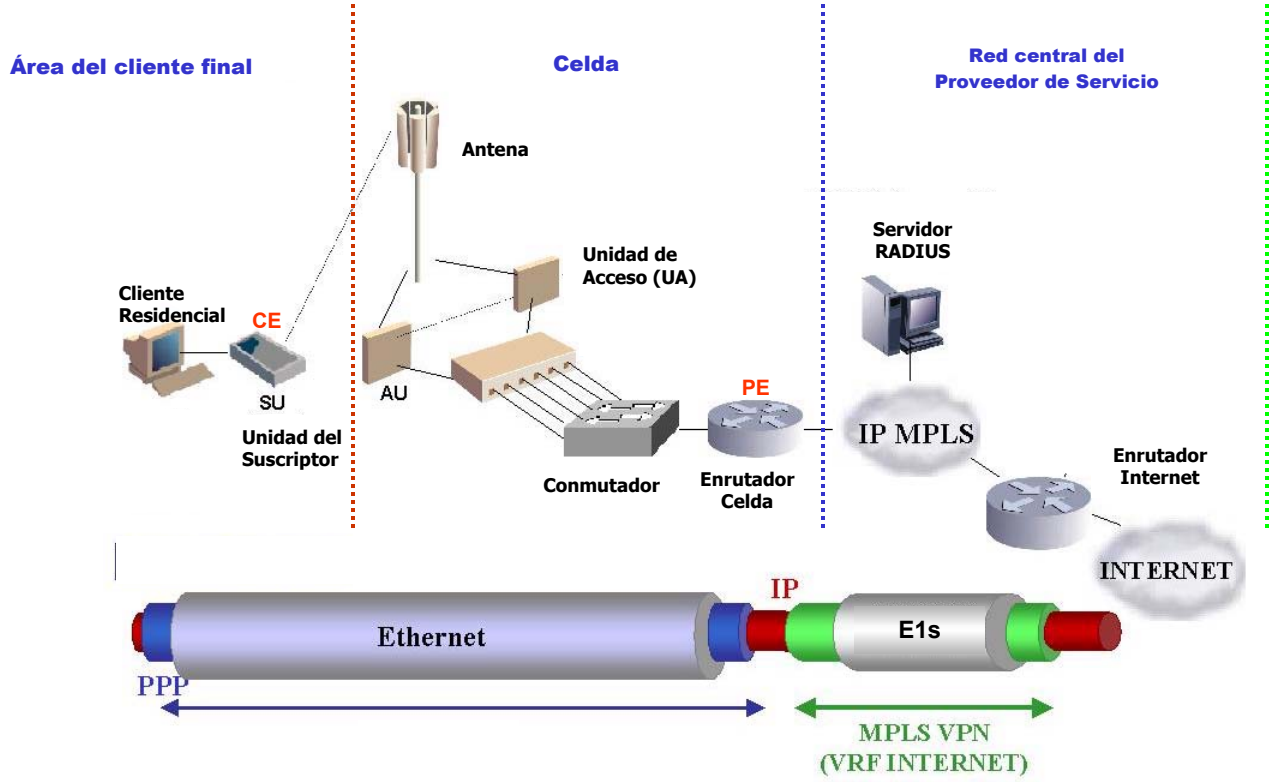

Figura 22: Ejemplo de Implementación, Acceso Remoto Residencial a Internet

Descripción de los equipos

Celda

Tomando en consideración que el ejemplo de implementación presentado es para soluciones residenciales, llamamos CELDA a la solución inalámbrica que funcionará como enlace entre el cliente final y la red central del proveedor de servicio. Cada celda esta conformada por seis Unidades de Acceso (UA) inalámbrico. Una Unidad de Acceso consiste en un sector, teniendo en consecuencia seis sectores por cada celda. Cada sector forma un enlace punto-punto o punto-multipunto con una

ancho de banda entre 2Mbps y 10Mbps los cuales dependerá de las características del fabricante de la UA.

Para la conexión a la red central IP/MPLS de las celdas, se propone un enrutador multiservicio de última generación, con una alta capacidad de conmutación de paquetes por segundo para garantizar que será capaz de soportar los servicios de voz y datos a ser prestados por cada celda. Este equipo debe soportar tarjetas con cuatro (4) puertos E1 para una capacidad total de enlace entre la celda y la red central IP/MPLS de 8Mbps.

Además se provee de un conmutador de red de área local (LAN), con capacidad de 24 puertos 10/100BaseT para la conexión del enrutador y de los puertos 10BaseT provenientes de los radios de cada sector de la celda.

El equipo disponible para el cliente final se denominará Unidad del Suscritor (SU). Este consiste en un equipo que formará un enlace inalámbrico punto-punto o punto-multipunto con la Unidad de Acceso (UA) y una conexión Ethernet 10/100Mbps para la conexión del equipo final del cliente. Esta conexión inalámbrica se realizará en la banda de frecuencia no licenciada de 2.4Ghz del espectro de frecuencia.

Red Central

Basados en la premisas anteriores se propone una red central IP basada en conmutadores de celdas/paquetes con capacidades de implementar MPLS. Los volúmenes de tráfico actuales y futuros que se necesitan manejar en la red requieren de

soluciones de la red central IP capaces de conmutar millones de paquetes IP por segundo (Mpps), conservando la calidad de servicios (QoS) necesaria para transporte de la voz y los otros tipos de servicios IP a ser provistos por esta red.

Los conmutadores de celdas-paquetes basados en MPLS son dispositivos de la red central capaces de asumir esta carga de tráfico IP. Como se puede observar en el diagrama siguiente se propone para la red central IP de cada ciudad, una solución basada en conmutadores celdas/paquetes IP como dispositivo de conmutación IP/MPLS de alta capacidad.

Listado de Equipos propuestos para esta solución:

1. Área del cliente
    a. Unidad del Suscriptor (US): Puente de acceso inalámbrico en la banda no licenciada 2.4Ghz. Se requiere mínimo 1 puerto Ethernet 10/100Mbps y
    b. PCs con sistema operativo que soporte protocolo PPPoE

2. Celda
    a. Unidad de Acceso (UA): Puente de acceso inalámbrico en la banda no licencia 2.4Ghz.
    b. Estación Base (EB): Equipo concentrador para estaciones inalámbricas.
    c. Conmutador de 12 o 24 puertos 10/100Mbps
    d. Enrutador de celda con capacidad de enlaces de alta velocidad (E1).

3. Red Central

   a. Red Central MPLS compuesta de conmutadores-enrutadores de alta capacidad

   b. Servidor RADIUS: Este servidor permite la autenticación, autorización y facturación permitiendo una mejor y mayor administración del acceso a la red, almacenando y centralizando todos los niveles de seguridad en una base de datos común:

      i. Autenticación: determinar la identidad del usuario y permite el acceso a la red.

      ii. Autorización: determina el nivel de servicio del usuario después de autenticado.

      iii. Facturación: mantiene un registro de la actividad de cada usuario para proceder a la facturación.

   c. Enrutador de alta capacidad para el acceso a Internet

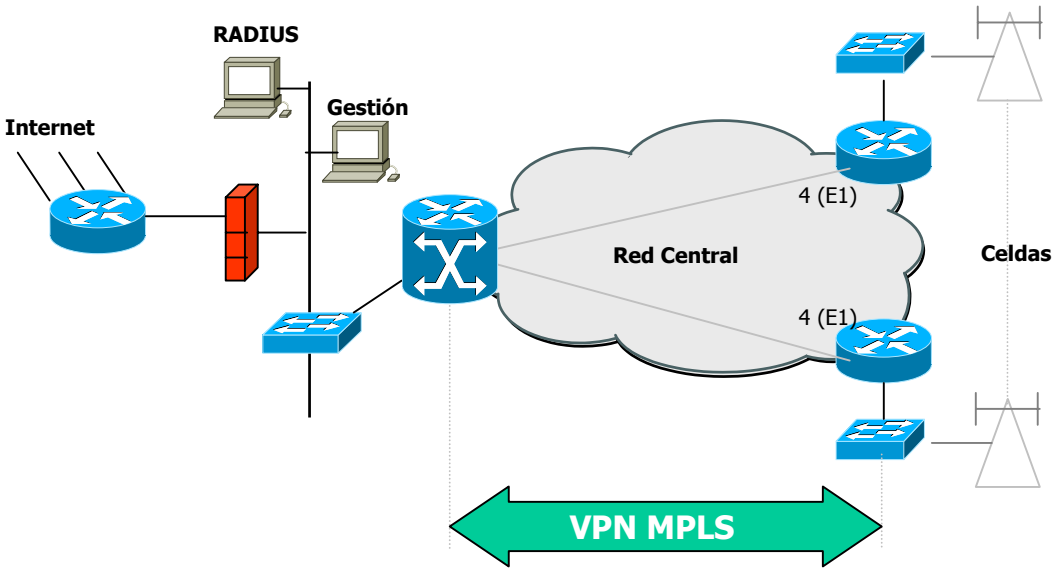

Figura 23: Conexión de Red Central

Operación de MPLS

Paso 1: La red automáticamente construye las tablas de enrutamiento a través de protocolos como OSPF entre los LSR que participan internamente. El protocolo LDP utiliza la topología de esas tablas de enrutamiento para establecer los valores de las etiquetas entre los equipos adyacentes.

Paso 2: El paquete llega al ELSR de entrada donde es procesado para determinar el servicio capa 3 requerido, como por ejemplo QoS o administración de ancho de banda. Basado en el requerimiento del paquete el ELSR selecciona y aplica una etiqueta al encabezado del paquete para entregarlo al LSR siguiente.

Paso 3: El LSR lee la etiqueta en cada paquete, la reemplaza con una nueva etiqueta listada en la tabla y entrega el paquete. Esta acción se repite de acuerdo a la cantidad de saltos (LSR) de la red central.

Paso 4: El ELSR de salida elimina la etiqueta, lee el encabezado del paquete y lo entrega a su destino final.

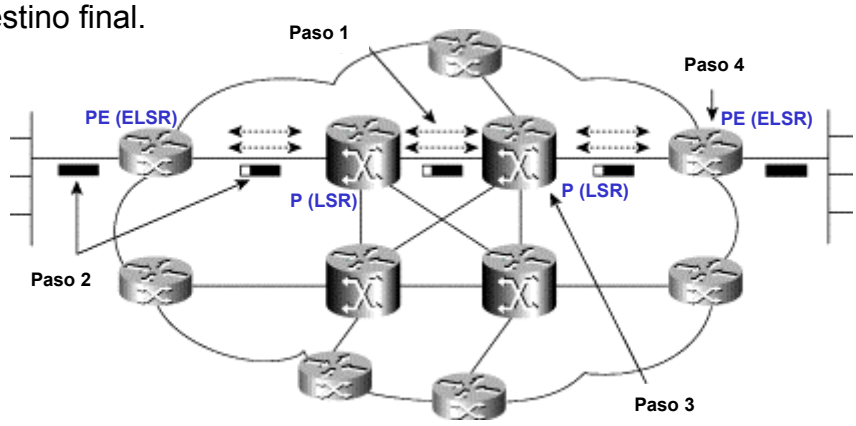

Figura 24: Operación de la red IP MPLS

Modelo de conectividad y enrutamiento VPN MPLS

Para el intercambio de información de enrutamiento se utilizará:

- Protocolo LDP entre P-P
- Protocolo OSPF entre P-PE
- Protocolo MP-iBGP entre PEs

El protocolo OSPF garantizará el mantenimiento de las tablas globales entre P-P y P-PE y el MP-iBGP garantizará el mantenimiento de las tablas VRF entre enrutadores PEs.

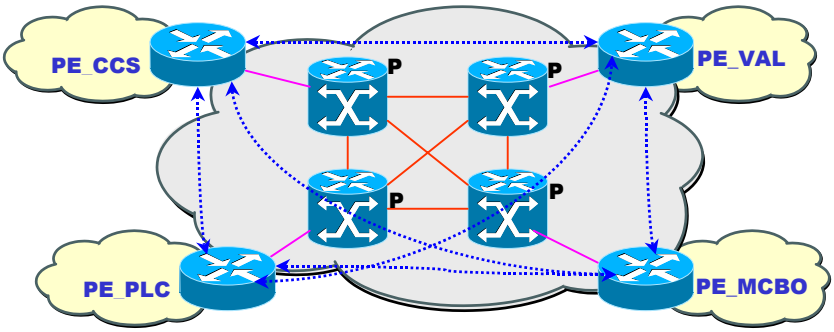

Figura 24: Modelo de conectividad

CONCLUSIONES

En la economía global, las empresas se enfrentan al desafío de gestionar la complejidad de ambientes en constantes cambios. Para muchas de estas empresas, hay un área fundamental que debe estar siempre actualizada: la red corporativa. Algunos ejemplos son: la conexión de nuevas sucursales, el establecimiento de VPNs y la implementación de aplicaciones críticas de negocios en varias localidades. Sin embargo las empresas actualmente demandan mucho más de sus redes y solicitan la ayuda de proveedores de soluciones para resolver estos nuevos desafíos. Es necesario entonces disponer de nuevas tecnologías que maneje grandes volúmenes de datos que conlleva a su vez a mejorar la calidad de servicio.

MPLS es el resultado de un largo proceso de convergencia e interacción entre IP y ATM, y se propone como una de las tecnologías que se impondrá en los últimos años. La característica técnica más importante de la tecnología MPLS es el uso de una etiqueta para la toma de decisión de entrega o reenvío, más que la información IP contenida en el encabezado del paquete. El uso de esta etiqueta trae consigo una enorme flexibilidad en el desarrollo de nuevas funcionalidades de enrutamiento. Como por ejemplo el cambio de paradigma del enrutamiento IP tradicional salto por salto, al enrutamiento basado en destino.

El acto de añadir una etiqueta al paquete hace posible crear redes privadas virtuales escalables con una característica importante, como lo es el uso tanto de

direcciones privadas como direcciones públicas para las redes del cliente. En efecto las VPN MPLS pueden usar el direccionamiento IP que más le convenga debido al identificador de 64 bits para hacerlas globalmente únicas. Una VPN MPLS consiste en un conjunto de localidades interconectadas a través de un proveedor de servicio basado en MPLS.

La seguridad es uno de los temas más importante cuando se habla de redes virtuales privadas, en las VPN MPLS el envío o intercambio de paquetes dentro del proveedor no está determinado por la dirección IP que se encuentra en el encabezado del paquete sino en las LSPs asociadas a cada VPN IP, las cuales se originan y terminan solo en los enrutadores PE. La separación del tráfico en el interior de la red se hace a través de atribuciones únicas VRF (Tabla de enrutamiento virtual - Virtual Routing Forwarding) para cada VPN del cliente. Esto ofrece el mismo nivel de privacidad que una red basada en ATM o Frame Relay, ya que los usuarios de una VPN específica no tienen acceso al tráfico fuera de su VPN.

También es de vital importancia contar con soporte para los diferentes niveles de QoS si sólo se dispone de una red para todos los formatos de información, incluyendo aplicaciones de voz, vídeo, correo electrónico, transferencia de archivos, etc. MPLS facilita este soporte para QoS mediante unas etiquetas que permiten a los enrutadores o conmutadores de la red identificar los requisitos de cada paquete de IP y darles la prioridad adecuada. La calidad de servicio está enfocada en términos de clases de servicios, los proveedores de servicios VPN pueden ofrecer a sus clientes una gran

flexibilidad en cuanto a las políticas que controlan qué clases de servicios aplicar a qué tipo de cliente.

En el área de escalabilidad se pueden crear grandes números de localidades por cada VPN, esto es posible debido a que se emplea mecanismo como: jerarquía de enrutamiento, donde los enrutadores centrales del proveedor se mantienen libre de cualquier información de enrutamiento; los enrutadores de borde mantienen sólo la información de las localidades que están conectadas directamente; además se utiliza el protocolo BGP como protocolo de enrutamiento entre dominios, el cuál permite una mayor escalabilidad por ser un protocolo que maneja grandes volúmenes de rutas y su flexibilidad para cargar parámetros opcionales sin afecta las funcionalidades del protocolo.

Estas características hacen de las VPN MPLS una plataforma de rápido y fácil desarrollo con servicios de valores agregados como: intranets, extranets, voz, multimedia, etc.

GLOSARIO DE TÉRMINOS

- **ARIS (Aggregate route-based IP switching).** Nombre asignado por IBM para la tecnología de conmutación de etiquetas.
-
- **ATMARP (Asynchronous transfer mode address resolution protocol).** Servidor que provee la resolución de direcciones IP a ATM para cada subred lógica.
-
- **BGP (Border gateway protocol)**. Protocolo de enrutamiento interdominio usado para redes IP.

- **Diferenciador de rutas (Route distinguisher)**. Identificador de 64 bits utilizado por VPN MPLS para asegurar que las direcciones sean únicas cuando se usan múltiples VPNs con la misma dirección.

- **EBGP (External BGP).** Sesión BGP entre enrutadores en diferentes sistemas autónomos.

- **Etiqueta (Label).** Identificador de tamaño fijo usado para determinar el intercambio de un paquete usando un algoritmo exacto y que es usualmente reescrito durante el reenvío.

- **FEC (Forwarding equivalence class).** Un sistema de paquetes que se pueden manejar de forma equivalente y que es conveniente ligar a una misma etiqueta.

- **FIB (Forwarding information base).** Tabla de reenvío de un enrutador.

- **Etiqueta (Label).** Identificador de tamaño fijo usado para determinar el intercambio de un paquete usando un algoritmo exacto y que es usualmente reescrito durante el reenvío.

- **Intercambio (Forwarding).** Se refiere a la acción que ejecuta un conmutador o un enrutador para recibir un paquete por una interfaz de entrada, determinar su salida por medio de algunos archivos dentro del paquete y enviarlo a la salida más apropiada.

- **IBGP (Internal BGP).** Sesión BGP entre enrutadores dentro del mismo sistema autónomo.

- **IETF (Internet Engineering Task Force).** Cuerpo de mayor jerarquía para la estandarización de protocolos de Internet y de IP.

- **IGP (Interior gateway protocol).** Protocolo de enrutamiento usado dentro de un dominio simple, como OSPF, IS-IS.

- **LSR de borde (Edge LSR).** Es el primer enrutador que aplica la etiqueta a un paquete.

- **LSR (Label switching router).** Término general que se le aplica a los equipos que manejan conmutación de etiquetas.

- **LDP (Label distribution protocol).** Protocolo para distribuir las etiquetas en una red MPLS definido por la IETF.

- **LIS (Logical IP subnet)**. Conjunto de nodos IP conectados a una red ATM y que comparten la misma dirección de subred.

- **LSP (Label switch path).** Una ruta que es seguida por el paquete etiquetado, empieza en el LSR de entrada y terminan en el LSR de salida.

- **MPLS (Multiprotocol label switching).** Estándar definido por la IETF para la conmutación de etiquetas.

- **Marcador de ruta (Route target).** Identifica un grupo de enrutadores y en cada enrutador un conjunto de rutas que son anunciadas con BGP.

- **PPPoE (Point-to-Point Protocol over Ethernet).** Protocolo punto a punto sobre Ethernet.

- **TDP (Tag distribution protocol).** Protocolo para la distribución de etiquetas desarrollado por Cisco System.

- **TFIB (Tag forwarding information base).** Estructura de datos que relaciona las etiquetas de entrada con las etiquetas de salida.

- **VCI (Virtual circuit identifier)**. Es usado en el encabezado ATM para identificar un circuito virtual.

- **VPI (Virtual path identifier).** Es usado en el encabezado ATM para identificar la ruta.

INDICE DE FIGURAS

Pág.

- **Figura 1.** Modelo de subred IP lógica..... 4
- **Figura 2.** Arquitectura básica de un nodo MPLS (LSR)..... 11
- **Figura 3.** Arquitectura de un LSR de borde..... 13
- **Figura 4.** Colocación y reenvío de una etiqueta MPLS..... 14
- **Figura 5.** Proceso de reenvío de un paquete IP..... 16
- **Figura 6.** Posición de la etiqueta MPLS en una trama capa 2..... 17
- **Figura 7.** Encabezado de la pila de etiquetas MPLS..... 17
- **Figura 8.** Conmutación de etiquetas a través de la pila..... 19
- **Figura 9.** Proceso de doble búsqueda en un enrutador..... 23
- **Figura 10.** PHH Penúltimo en romper el salto..... 24
- **Figura 11.** Intercambio de información entre LSR..... 25
- **Figura 12.** Arquitectura de un circuito virtual MPLS..... 26
- **Figura 13.** Proceso de etiquetado en un dominio ATM..... 28
- **Figura 14.** Modelo de una red oVPN..... 33
- **Figura 15.** Modelo de una red par a par..... 35
- **Figura 16.** Modelo par a par con enrutador compartido..... 36
- **Figura 17.** Modelo par a par con enrutador dedicado..... 37
- **Figura 18.** Modelo de una red VPN MPLS..... 40
- **Figura 19.** Colocación de etiquetas por un LSR de borde..... 41
- **Figura 20.** Modelo de red tubo para QoS..... 50
- **Figura 21.** Modelo de red manga para QoS..... 51
- **Figura 22.** Ejemplo de Implementación..... 58
- **Figura 23.** Conexión de Red Central..... 61
- **Figura 24.** Operación de la red MPLS..... 62
- **Figura 25.** Modelo de conectividad..... 63

BIBLIOGRAFIA

- Ivan Pepelnjak, Jim Guichard, “MPLS and VPN Arquitectures,” Cisco Press. 201 West 103rd Street Indianapolis, IN 46290 USA
- Bruce Davie, Yakov Rekhter, “MPLS Technologies and Applications”, Morgan Kaufmann Publishers.
- http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/rampls2/ovprov/
- http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/_sp_xlsw_ds.htm
- http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/ios_dsl/rel122/config/04conf06.htm
- http://www.cisco.com/warp/public/732/Tech/mpls/
- http://www.mplsforum.org/tech/MPLSQOSWPMay2003.pdf
- http://www.cisco.com/univercd/cc/td/doc/product/wanbu/bpx8600/mpls/9_3_1/mpls01.htm#xtocid204050
- http://www.cisco.com/en/US/tech/tk436/tk832/technologies_q_and_a_item09186a00801a0c91.shtml
- http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800a85c5.shtml
- http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800b010f.shtml