UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

APLICACIONES DE LA TECNOLOGÍA MPLS EN LA RED DE UN PROVEEDOR DE INTERNET

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

ALEX MARTIN MENDOZA COTRINA

PROMOCIÓN
2003 - I

LIMA – PERÚ
2008

APLICACIONES DE LA TECNOLOGÍA MPLS EN LA RED DE UN PROVEEDOR DE INTERNET

Dedico este trabajo a:

Mi madre, por su dedicación, ejemplo y apoyo incondicional,
Mi padre, por sus valores, lealtad y capacidad para luchar en la vida,

Y a mis hermanos por su confianza y comprensión.

SUMARIO

El presente trabajo pretende describir las características de la tecnología MPLS, así como las nuevas posibilidades que brinda para la prestación de servicios, a través de las aplicaciones de Redes Privadas Virtuales con Calidad de Servicio sobre un backbone MPLS. La tecnología MPLS se considera fundamental en la construcción de las nuevas redes de backbones para los proveedores de servicio ya que puede funcionar sobre cualquier tecnología de transporte, simplificando por ejemplo la migración de las tradicionales redes ATM a MPLS y la integración con redes ópticas como DWDM.

El contenido del informe se ha enfocado principalmente al desarrollo de las configuraciones que se necesita realizar en los equipos enrutadores para la implementación de un backbone MPLS con aplicaciones de Redes Privadas Virtuales con Calidad de Servicio, ya que es la solución tecnológica ampliamente desarrollada en la mayoría de las redes de backbone de los operadores de telecomunicaciones del mundo, sin embargo no se ha descuidado la descripción de la arquitectura de la tecnología MPLS, sus funcionalidades, componentes y beneficios que ofrece mediante sus distintas aplicaciones como son las Redes Privadas Virtuales, Calidad de Servicio en base a la integración con DiffServ, Ingeniería de Tráfico, enrutamiento IP Multicast y GMPLS.

Se tiene por objetivo que el presente informe sirva de guía para aquellos que se encuentran en proceso de implementación de una red MPLS o en proceso de aprendizaje de esta nueva arquitectura, esperando que sea un valioso aporte para facilitar el entendimiento de la tecnología MPLS.

ÍNDICE

PRÓLOGO

El crecimiento acelerado de la Internet actual, el aumento del tipo de aplicaciones con requerimientos de mayor ancho de banda y calidad de servicio, la necesidad de una red convergente capaz de soportar la integración de tráfico de voz y datos, y la búsqueda por reducir los costos de infraestructura, ha significado grandes cambios tecnológicos en el mundo de las telecomunicaciones, como por ejemplo el desarrollo de nuevas tecnologías de transmisión de fibra óptica como DWDM que ofrecen en la actualidad la posibilidad de transportar información a grandes velocidades.

Así surge la tecnología *MultiProtocol Label Switching* (MPLS) que es el último paso en la evolución de las tecnologías de conmutación multinivel o también llamadas conmutación IP que es una de las propuestas desarrolladas por el *Internet Engeenering Task Force* (IETF). Es un estándar capaz de soportar cualquier tipo de tráfico e integrarse con cualquier tecnología de transporte, como por ejemplo ATM, Frame Relay, ADSL entre otras. Actualmente también con capacidad de integrarse directamente sobre redes ópticas como es el caso de GMPLS que está desplazando a las tradicionales redes formadas por 4 niveles: IP para el transporte de aplicaciones y servicios, ATM para la ingeniería de trafico, SDH para la transmisión y DWDM para aumentar la capacidad de transmisión.

MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las tecnologías actuales de enrutamiento IP (típicamente limitadas a enrutamiento por dirección de destino). Así mismo permite hacer ingeniería de tráfico IP, mantener clases de servicio y soportar con gran eficacia la creación de redes privadas virtuales.

El presente trabajo pretende explicar la tecnología MPLS, su funcionamiento, aplicaciones y beneficios, así como la simplicidad de la configuración que se necesita realizar para la implementación de un backbone MPLS con soporte para redes privadas virtuales con calidad de servicio.

El capitulo I, se centra en la descripción funcional del MPLS, de los principales componentes que intervienen en esta arquitectura y de la actuación conjunta de los mismos, así mismo se describe los beneficios de MPLS para el soporte de procedimientos de enrutamiento y envío de paquetes en backbones IP.

En el capitulo II se describe la posibilidad de proporcionar nuevas aplicaciones y servicios, en redes IP y en la Internet en general. En concreto, se presenta las distintas aplicaciones como son ingeniería de tráfico, de diferenciación de servicios en distintas clases y de establecimiento de redes privadas virtuales sobre una topología inteligente, muy superior en prestaciones a las soluciones tradicionales de túneles y circuitos virtuales, se describe también el soporte para enrutamiento IP Multicast y la integración con redes ópticas es decir GMPLS.

En el capitulo III se diseña una topología básica formada por cuatro enrutadores, dos LSR y dos LER, que se utiliza para ilustrar el procedimiento de configuración de un backbone MPLS en base a enrutadores Cisco, usando OSPF y LDP como protocolos de enrutamiento interno y distribución de etiquetas respectivamente, finalmente se muestra el procedimiento para la verificación de la red en caso se presentasen problemas.

En el capitulo IV se desarrolla la configuración de una red MPLS con soporte para redes privadas virtuales que utiliza el MP-BGP como protocolo para el enrutamiento de prefijos VPN sobre el backbone MPLS. También se define y muestra la configuración de clases de servicio y las políticas de servicio que se aplicaran a las clases definidas, esto con la integración de MPLS/DiffServ, así mismo se mencionan algunos comandos que nos permitirán resolver los eventuales problemas que pudieran presentarse en la red. Finalmente se muestran los resultados de pruebas realizadas con la finalidad de validar el correcto funcionamiento de las configuraciones realizadas en la red MPLS.

Las conclusiones nos resumen los puntos más resaltantes sobre la tecnología MPLS, las ventajas y desventajas de las diferentes aplicaciones de esta arquitectura.

CAPITULO I
DESCRIPCIÓN GENERAL DE MPLS

1.1 Introducción

Es evidente que el crecimiento de Internet es imparable. El número de usuarios que se conectan a la red no cesa de incrementar, pero no es éste el mayor reto al que tiene que enfrentarse la Internet actual. También está aumentando el tipo de aplicaciones que viajan por la red, como las que se realizan en entornos corporativos (VoIP y videoconferencia, entre otros) que requieren un tratamiento distinto.

El éxito de la Internet actual está muy vinculado al uso de los protocolos TCP/IP para soportar las aplicaciones y los servicios que existen sobre ella, pero hoy en día no es capaz de satisfacer las nuevas necesidades que están surgiendo. Una carencia fundamental de esta red es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de los usuarios.

La idea original de Internet es proveer acceso a las distintas ubicaciones y distribuir contenidos. En su inicio, no era tan importante el servicio de transporte de datos, conocido como Best Effort. Hoy en día no debe tratarse de la misma manera un paquete de voz que necesita muy poco ancho de banda, donde el retardo está muy acotado y es menos importante la pérdida de paquetes, que una transmisión FTP con unos requerimientos de ancho de banda mucho mayores, con una necesidad de pérdida de paquetes muy baja pero relativamente poco estricta en el retardo. Es necesario que permitan ofrecer distinto tratamiento a diferentes tipos de tráfico.

Una de las soluciones propuestas por el *Internet Engeenering Task Force* (IETF) con el objetivo de proporcionar Calidad de Servicio (*QoS*) a una red de datos es *MultiProtocol Label Switching* (MPLS). Se trata de un estándar de arquitectura multinivel, capaz de soportar cualquier tipo de tráfico (nosotros nos centraremos en el tráfico IP) e independiente del nivel de transporte de datos sobre el que se apoya, capaz de ofrecer una gran eficiencia a la hora de realizar la transmisión de paquetes de un extremo a otro de la red MPLS gracias a la combinación de la flexibilidad del nivel de red IP con los beneficios propios de un modelo de red orientado a conexión.

En una red IP tradicional, un router conmuta los paquetes de una interfaz de entrada a una interfaz de salida; además, actualiza la información de enrutamiento. Para enviar los

paquetes, debe examinar la cabecera del paquete IP para cada paquete. Estas dos funciones, envío y enrutamiento, tienen lugar en cada salto que realiza un paquete que atraviesa la red. Lo que se busca con MPLS a este respecto es llevar las funciones de enrutamiento únicamente a los equipos exteriores del dominio MPLS, de forma que en el interior de dicho dominio no sea necesario realizar labores de enrutamiento, sino sólo de conmutación mediante la consulta de unas etiquetas añadidas a cada paquete en el momento de entrada al dominio.

MPLS es una solución global de conmutación multinivel y, por tanto, se basa en:

- La separación entre las funciones de control (routing) y de envío (forwarding).
- El paradigma de intercambio de etiquetas para el envío de datos.

MPLS es un método mejorado de reenvío de paquetes a través de una red usando la información contenida en las etiquetas adjuntadas al paquete IP. Las etiquetas son insertadas entre la cabecera de la capa 3 y la cabecera de la capa 2 en caso se trate de una tecnología basada en Frames y estos son contenidos en un campo VPI (Virtual Path Identifier) y un VCI (Vvirtual Channel Identifier) en el caso se trate de una tecnología basada en celdas, tal como ATM.

MPLS combina la tecnología de conmutación usada en la capa 2 con la tecnología de enrutamiento usada en la capa 3. El principal objetivo de MPLS es crear una red flexible y escalable que proporcione una mayor estabilidad y desempeño que las actuales. Esto incluye Ingeniería de tráfico y capacidades VPN, que ofrecen calidad de servicio (QoS) con múltiples clases de servicio (CoS).

En una red MPLS, a los paquetes de entrada, se les asigna una etiqueta en el router de borde, LER (*Label Edge Router*). Así, los paquetes son enviados a lo largo de un camino llamado LSP (*Label Switched Path*) donde cada LSR (*Label Switched Router*) hace decisiones de enrutamiento basados solamente en el contenido de la etiqueta. En cada salto, el LSR quita la etiqueta y adjunta una nueva, lo cual indica como será reenviado el paquete al siguiente salto. Finalmente la etiqueta será retirada cuando el paquete egrese de la red MPLS, en el LER de salida, y el paquete será enviado a su destino. El termino *MultiProtocolo* indica que MPLS trabaja con cualquier protocolo de la capa de Red.

1.1.1 Evolución de MPLS

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente entre 1997 y 1998 a que varios fabricantes desarrollasen técnicas con la finalidad de lograr la integración de los niveles 2 y 3 de forma efectiva.

Esas técnicas se conocieron inicialmente como "conmutación IP" (*IP switching*) o "conmutación multinivel" (*multilayer switching*). Una serie de tecnologías privadas, entre las que merecen citarse: *IP Switching* de IPSILON Networks, *Tag Switching* de CISCO, *Aggregate Route-Base IP Switching (ARIS*) de IBM, *IP Navigator* de Lucent y *Cell Switching Router (CSR)* de Toshiba, soluciones que finalmente condujeron a la formación del grupo de trabajo para el desarrollo del actual estándar MPLS del IETF.

El problema que presentaban tales soluciones de conmutación IP era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3), a lo que se sumaba que la mayoría de esas soluciones necesitaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas (Frame Relay, PPP, SONET/SDH y LANs). Se quería obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace. De aquí que el Grupo de Trabajo de MPLS que se estableció en el IETF en 1977 se propuso como objetivo la adopción de un estándar unificado e interoperativo.

Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM.
- MPLS debía soportar el envío de paquetes tanto unicast como multicast.
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP.
- MPLS debía permitir el crecimiento constante de la Internet.
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

1.1.2 Beneficios de MPLS

El método de conmutación de etiquetas permite a los enrutadores y conmutadores ATM tomar decisiones de reenvío de paquetes basándose en el contenido de una simple etiqueta, no como en las complejas decisiones de enrutamiento basados en la dirección IP de destino. Esta técnica de conmutación de etiquetas trae muchos beneficios a las redes basadas en IP, como se indica a continuación:

- Redes Privadas Virtuales. Con el uso de la arquitectura MPLS, los proveedores de servicios de telecomunicaciones pueden crear Redes Privadas Virtuales de capa 3 a través del *backbone* de la red MPLS para múltiples clientes, usando la misma infraestructura de red, y sin la necesidad de utilizar otras técnicas de seguridad como encriptar las aplicaciones de los usuarios finales.

- Ingeniería de Tráfico. Proporciona la habilidad para configurar una ruta o múltiples rutas a través de la red para cursar el tráfico. Esta característica optimiza la utilización de recursos como son el ancho de banda y las rutas poco utilizadas.
- Calidad de Servicio. Con el uso de la calidad de servicio (QoS) en MPLS, los proveedores de servicio pueden proporcionar múltiples clases de servicio con una alta calidad de servicio garantizada a sus clientes.
- Integración de IP y ATM. La gran mayoría de proveedores de servicios tienen actualmente implementado su backbone con un modelo de diseño en el cual usan ATM para la capa2 e IP para la capa3. Este modelo no es escalable. Con el uso de MPLS, los proveedores de servicio pueden migrar muchas de las funciones del plano de control ATM a la capa 3, de tal modo se simplifica la tarea de aprovisionamiento, administración y complejidad de la red. Esta técnica ofrece una inmensa escalabilidad y elimina la cabecera inherente a las celdas ATM en el tráfico IP.

Los proveedores de servicio han aprovechado las mejoras de MPLS en comparación con redes IP sobre ATM convencionales. MPLS combina el desempeño y capacidad de conmutación de la capa 2 con la escalabilidad del enrutamiento de la capa 3. Esto permite a los ISP encontrar los desafíos del explosivo crecimiento en la utilización de la red mientras proporcionan la oportunidad de diferenciar servicios sin sacrificar la existente infraestructura de red. La arquitectura MPLS es flexible y puede ser empleada en combinación con diferentes tecnologías de la capa2.

1.2 Arquitectura de MPLS

La arquitectura definida en MPLS utiliza asignación de etiquetas en sentido *downstream* para tráfico IP Unicast. Además soporta asignación de etiquetas bajo demanda en sentido *downstream* y asignación no solicitada. Esto permite que las etiquetas sean globalmente únicas por nodo o por interfase.

Las etiquetas poseen una gran granularidad, lo cual puede traer problemas cuando se producen diferencias de granularidad entre LSRs (Label Switching Routers) adyacentes.

Para soportar una estructura jerárquica de asignación de etiquetas emplea el mecanismo LIFO (last-in-first-out). De esta manera, la decisión de reenvió (*forwarding*) se realiza sobre la primera de las etiquetas de la pila.

Las etiquetas se distribuyen utilizando un protocolo de señalización como LDP (*Label Distribution Protocol*) o RSVP (*ReSouerce reserVation Protocol*), o también, añadidas a protocolos de enrutamiento como BGP u OSPF.

Para la selección de camino MPLS propone dos mecanismos: enrutamiento salto a salto y enrutamiento Explicito. En el primer caso, el enrutamiento salto a salto es designado utilizando los resultados obtenidos de los protocolos de enrutamiento convencionales. En el segundo caso, una ruta explícita es especificada completamente por la fuente. Todos los LSRs son capaces de reenviar paquetes utilizando este mecanismo, pero no tienen la capacidad de originarlos.

Así mismo se definen dos formas para el requerimiento de los LSPs: Control-driven (antes de la transmisión de de datos) y Data-driven (una vez detectado un cierto flujo de datos). La arquitectura de MPLS no requiere la utilización del mecanismo Control-Driven para la asignación de etiquetas, aun cuando este método es el más utilizado en estas redes.

1.2.1 Elementos de la arquitectura MPLS

- LSP (*Label-Switched Path*): Un LSP es un camino específico por el cual pasa tráfico en una red MPLS. LSPs son aprovisionados usando un protocolo de distribución de etiquetas que puede ser LDP.
- FEC (*Forwarding Equivalence Class*): Agrupación de paquetes que comparten las mismas características para su transporte, así todos recibirán el mismo tratamiento en su camino hacia el destino. La asignación de un paquete a un determinado FEC se produce una vez que el paquete entra a la red MPLS. Todos los paquetes que forman parte del FEC, siguen un mismo LSP.
- LSR (*Label Switch Router*): Una red MPLS o Internet consiste en un grupo de nodos, los cuales son llamados LSR (router de conmutación de etiquetas), los LSRs son dispositivos internos a la red MPLS y sus funciones se pueden dividir de acuerdo al plano de control y reenvió. En el plano de control se encargan de mantener la información de enrutamiento confiable mediante algún protocolo de enrutamiento y asignar etiquetas e intercambiar esta información mediante un protocolo de distribución de etiquetas. En el plano de reenvió, el envió de paquetes etiquetados utilizando la información de distribución de etiquetas.
- LER (*Label Edge Router*): Router de conmutación de etiquetas de frontera, es el dispositivo ubicado en la frontera entre una red IP tradicional y una red MPLS, las funciones en el plano de control son iguales al LSR y en el plano de envió se encargan de: recibir paquetes etiquetados y reenviarlos con una nueva etiqueta, recibir paquetes IP tradicionales etiquetarlos y reenviarlos, recibir paquetes etiquetados y reenviarlos como paquetes IP tradicionales.

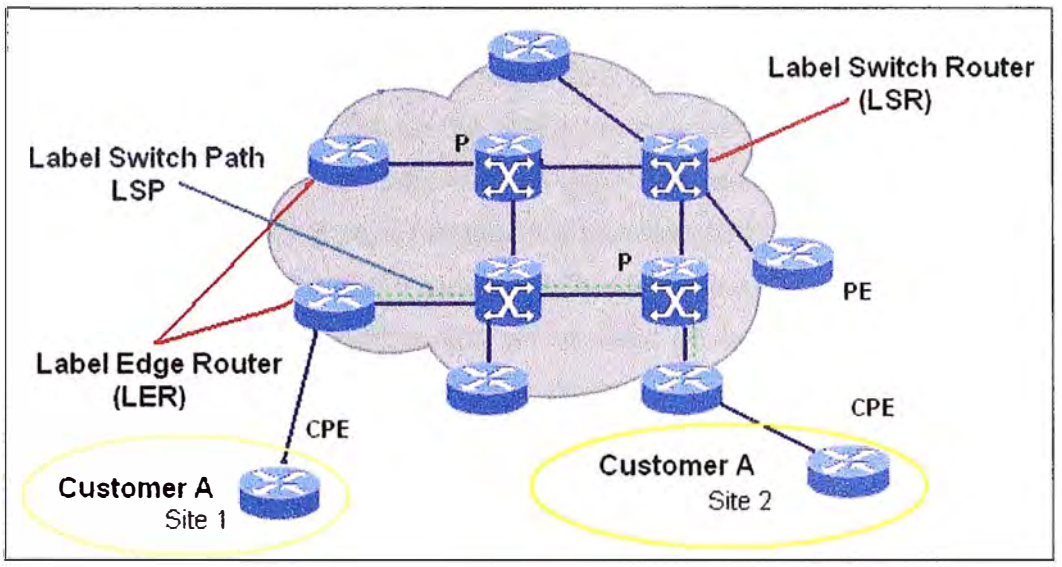

Figura 1.1 Elementos de la arquitectura MPLS

1.2.2 Funcionamiento de MPLS

La arquitectura MPLS divide claramente las funciones de enrutamiento (el control de la información sobre la topología y tráfico de la red), de las funciones de reenvió (el envió en sí de datos entre elementos de la red). Esta conformada por el plano de reenvió y el plano de control. Al separar el plano de control (enrutamiento) del plano de reenvió, cada uno de ellos se puede implementar y modificar independientemente. En la figura 1.2 se representa la separación funcional de los dos planos. El único requisito es que el plano de control mantenga la comunicación con el plano de reenvió mediante la tabla de reenvió de paquetes y actualice la información.

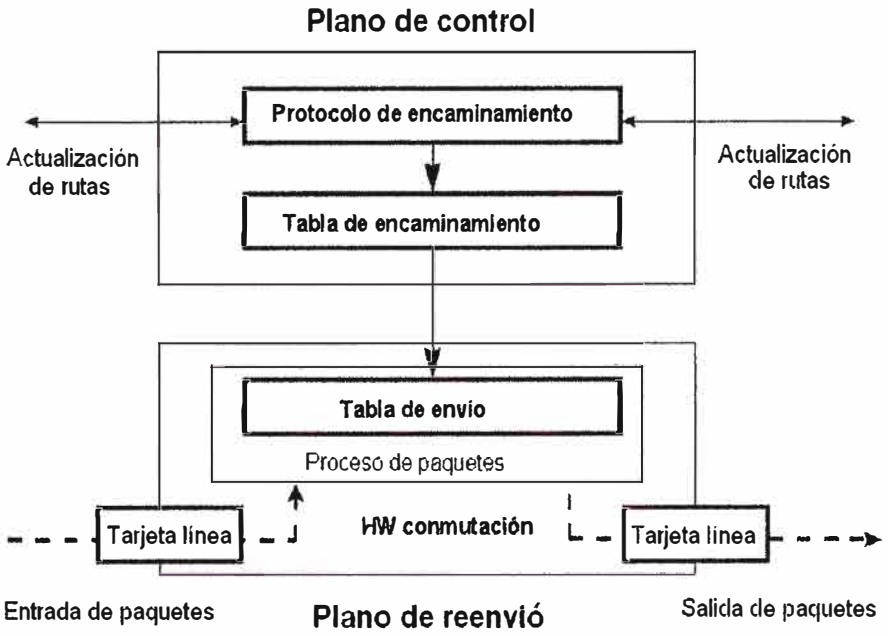

Figura 1.2 Plano de control y reenvió

a) Plano de reenvío

El plano de reenvío (también conocido como data plane) es responsable del reenvío de paquetes basados en los valores de las etiquetas adjuntadas. El plano de reenvío usa una etiqueta de información de reenvío LFIB (*label forwarding information base*) que es mantenida por el nodo MPLS para reenviar los paquetes etiquetados El algoritmo usado por el componente para conmutar y reenviar etiquetas usa la información contenida en el LFIB así como la información contenida en el valor de la etiqueta. Cada nodo MPLS mantiene dos tablas relevantes en el proceso de reenvío: la LIB (*label information base*) y el LFIB. La LIB contiene todas las etiquetas asignadas por el nodo MPLS local y la relación entre estas etiquetas con las etiquetas recibidas de los vecinos MPLS. La LFIB usa un grupo de etiquetas contenidas en la LIB para el reenvío de un paquete actual.

Al llegar los paquetes, el plano de reenvío, examina la información de la cabecera del paquete, busca en la tabla de reenvió la entrada correspondiente y dirige el paquete desde la interfaz de entrada a la de salida a través del correspondiente hardware de comunicación. A continuación se explica la LFIB y el algoritmo de reenvió de etiquetas:

- LFIB (Tabla de información de reenvío de etiquetas): La LFIB consiste en una secuencia de entradas. Cada entrada consiste en una etiqueta de entrada y una o más sub-entradas. La tabla LFIB es ordenada por el valor contenido en la etiqueta de entrada. Cada sub-entrada esta compuesta por una etiqueta de salida, interfaz de salida, y la dirección del siguiente salto. Las sub-entradas en una individual entrada pueden tener la misma o diferente etiqueta de salida. Los paquetes *multicast* requieren sub-entradas con diferentes etiquetas de salida, donde un paquete de entrada que arriba a una interfaz puede ser enviado a múltiples interfaces de salida. Además de la etiqueta de salida, la interfaz de salida y la dirección del siguiente salto, una entrada en la tabla de reenvío puede incluir información relacionada a los recursos que el paquete puede usar, tales como la cola de salida en la cual el paquete será ubicado antes de ser enviada. Un nodo MPLS puede mantener una sola tabla de reenvío, una tabla de reenvío por cada una de sus interfaces, o una combinación de ambos. En el caso de múltiples tablas de reenvío, el paquete reenviado es manipulado de acuerdo al valor de su etiqueta de entrada y la interfaz de entrada por la cual llega el paquete.
- Algoritmo de reenvío de etiqueta: Algoritmos convencionales de reenvío de paquetes usan múltiples algoritmos para el reenvío de paquetes unicast y multicast usando el campo ToS. Sin embargo, MPLS usa un solo algoritmo de reenvío de paquetes basado en el cambio de etiquetas. El nodo MPLS mantiene una sola LFIB y extrae el valor de la etiqueta, del campo *etiqueta* en el paquete de

entrada, y usa este valor como un índice en la tabla LFIB. Después de que se encuentra la relación entre el paquete de entrada y el LFIB, el nodo MPLS reemplaza la etiqueta del paquete con una nueva etiqueta de salida obtenida de la sub-entrada para luego ser enviada por una interfaz específica de salida al siguiente salto que también son especificados en la sub-entrada. Un nodo MPLS puede obtener toda la información que necesita para reenviar un paquete así como también para determinar reservación de recursos necesarios por un paquete usando un simple acceso de memoria. Esta habilidad de reenvío y búsqueda rápida hace de la conmutación de etiquetas una tecnología de conmutación de alto funcionamiento. MPLS también puede ser soportado por otros protocolos de la capa de red como IPv6, IPX, o Apple Talk además de IPv4. Esta propiedad hace de MPLS una atractiva tecnología para migrar de redes IPv4 a redes IPv6.

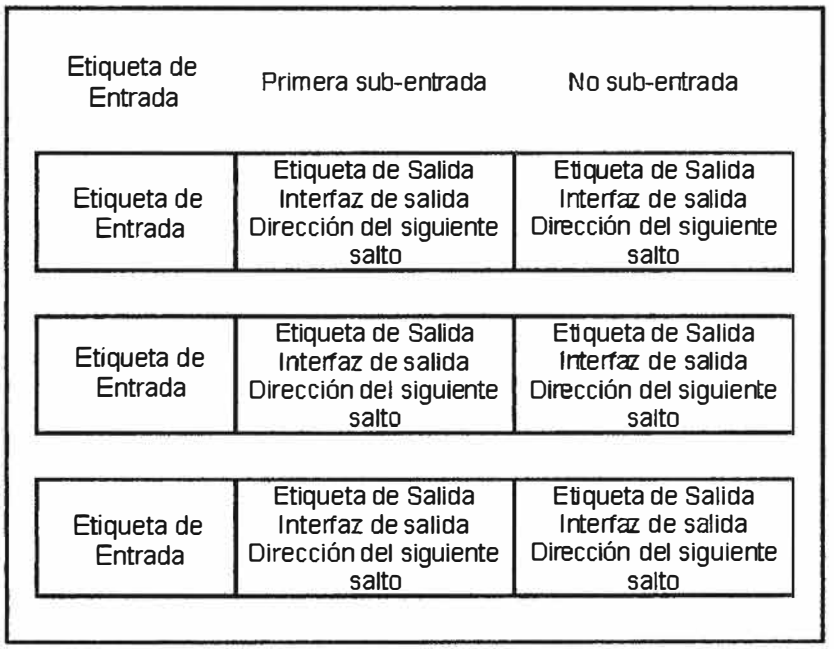

Figura 1.3 Estructura LFIB

b) Plano de control

El plano de control (control plane) es responsable del vínculo entre la etiqueta y la ruta en la red y la distribución de estos vínculos entre los nodos MPLS. Las etiquetas están unidas a las rutas en la tabla de enrutamiento, entonces el nodo MPLS necesitará tener una tabla de enrutamiento. Para obtener una tabla de enrutamiento, se necesita un protocolo de enrutamiento (o se pueden usar rutas estáticas lo cual no es recomendable). Ahora que se tiene una tabla de enrutamiento, es necesario intercambiar las etiquetas.

Este intercambio de etiquetas se puede lograr utilizando un protocolo de distribución de etiquetas como LDP (*Label Distribution Protocol*) desarrollado por IETF, que es una versión del protocolo TDP (*Tag Distribution Protocol*) desarrollado por CISCO.

Protocolos de estado de enlace como OSPF e IS-IS son los protocolos escogidos en MPLS debido a que proporcionan a cada nodo MPLS una visión completa de la red, también protocolos como PIM y BGP pueden ser usados para la distribución de la información de asociación de etiquetas. En enrutadores convencionales, la tabla de enrutamiento IP es usada para construir un espacio de memoria cache de rápida conmutación de paquetes y una tabla FIB (*Fordward Information Base*). Sin embargo, en MPLS, la tabla de enrutamiento IP proporciona información de redes externas y prefijos que usan la asociación de etiquetas.

El intercambio de etiquetas con nodos MPLS adyacentes es usado para construir la LFIB. MPLS usa el paradigma de reenvío basado en el intercambio de etiquetas que puede ser combinado con un rango de diferentes módulos de control. Cada modulo de control es responsable de asignar y distribuir un grupo de etiquetas, así como mantener otras informaciones de control relevantes. Los IGPs (*Interior Gateway Protocols*) son usados para definir si una red es alcanzable, vinculados y relacionados entre la FEC y el siguiente salto.

A continuación se describen los módulos de control que incluye MPLS:

- Módulo de enrutamiento *Unicast*: Construye la tabla FEC utilizando un convencional IGP tal como OSPF, IS-IS ú otro. La tabla de enrutamiento es usada para intercambiar la asociación entre etiquetas con los nodos MPLS adyacentes para las sub-redes que están contenidas en la tabla de enrutamiento IP. La distribución de la asociación entre etiquetas se hace usando el protocolo LDP o TDP para el caso de equipos CISCO.
- Módulo de enrutamiento *Multicast*: Construye la tabla FEC usando un protocolo de enrutamiento *multicast* tal como PIM (*Protocol-Independent Multicast*). La tabla de enrutamiento *multicast* es usada para intercambiar la asociación entre etiquetas con los nodos MPLS adyacentes para las sub-redes que están contenidas en la tabla de enrutamiento multicast. La distribución de la asociación entre etiquetas se hace usando el protocolo PIM v2 con extensión MPLS.
- Módulo Ingeniería de Tráfico: permite explícitamente especificar la ruta por la cual la etiqueta será conmutada a través de la red para propósitos de ingeniería de tráfico. Esto usa la definición de túnel MPLS y las extensiones de los protocolos de enrutamiento IS-IS ú OSPF para construir la tabla FEC. La distribución de la

asociación entre etiquetas se hace usando el protocolo RSVP (Resource Reservation Protocol) o CR-LDP (Constraint-based Routing LDP).

- Módulo VPN: usa tablas de enrutamiento por VPN para las tablas FEC, las cuales son construidas usando protocolos de enrutamiento entre el router CPE y el nodo MPLS del proveedor de servicio ubicado al borde de la red. La distribución de asociación entre etiquetas para una tabla específica de enrutamiento VPN es realizada usando el protocolo BGP.
- Módulo de Calidad de Servicio: construye la tabla FEC usando un protocolo IGP convencional como OSPF o IS-IS. La tabla de enrutamiento IP es usado para intercambiar la asociación entre etiquetas con los nodos MPLS adyacentes para sub-redes contenidas en la tabla de enrutamiento IP. La distribución de la asociación entre etiquetas es realizada usando el protocolo LDP o la versión propietaria de CISCO TDP.

1.2.3 Funciones de conmutación de etiquetas

La conmutación de etiquetas exige que en los LSR y LER realicen una serie de funciones para la asignación, reenvío y remoción de etiquetas a los paquetes IP, estas funciones son las siguientes:

- IMPOSE (Imposición de Etiqueta): la función de IMPOSE se realiza en los LER y consiste en insertar una etiqueta MPLS a un paquete IP que ingresa al enrutador, la etiqueta se asigna de acuerdo al FEC (Forwarding Equivalente Class) correspondiente, que en el caso de tráfico IP Unicast corresponde a un prefijo de red en la tabla de enrutamiento. La información para el etiquetado se encuentra en la Tabla de Envío IP en el Plano de Datos.
- SWAP (Conmutación de Paquetes Etiquetados): la función SWAP consiste en recibir un paquete etiquetado, verificar la etiqueta en la Tabla de Envío MPLS, cambiar la etiqueta al paquete y colocarlo en el puerto de salida, esta función la realizan tanto los LSR como los E-LSR.
- POP (Remoción de Etiqueta): La función de POP o Remoción de Etiqueta es efectuada en los E-LSR y consiste en eliminar la etiqueta a un paquete IP. Una vez eliminada la etiqueta el E-LSR realiza una nueva búsqueda en Tabla de Envío IP y reenvía el paquete de la manera tradicional.
- PHP (Remoción de Etiqueta en el Penúltimo Salto): El PHP (Penultimote Hop Pop) consiste en eliminar la etiqueta en el dispositivo anterior al E-LSR, de esta forma el paquete arriba al E-LSR como un paquete IP tradicional evitando la

búsqueda y eliminación de etiquetas. Esta función ahorra recursos de procesamiento en el ELSR.

1.3 Apilamiento de etiquetas

Una de las características más importantes que tiene MPLS es el apilamiento de etiquetas que maneja un paquete etiquetado puede contener varias etiquetas organizadas en modo Ultimo en Entrar Primero en Salir (LIFO). El procesado de etiquetas en MPLS siempre se basa en la etiqueta superior, por lo que en cualquier LSR se puede añadir (push) o remover (pop) una etiqueta. La ventaja principal del apilamiento de etiquetas es que permite añadir rutas parciales dentro de la red a un LSP existente creando así túneles.

Al principio de cada túnel los LSR asignan la misma etiqueta a los paquetes que van entrando mediante la operación push que mencionamos anteriormente. Al final de cada túnel pasa lo inverso, el LSR de salida remueve la etiqueta superior (añadida a la entrada del túnel) para mostrar la etiqueta original con el fin de que siga su trayectoria original. Esta operación se pude realizar indefinidamente formando así una red de túneles dentro de cada LSP original. Esta es una de las características que ATM maneja, sin embargo solo maneja apilamiento de un nivel.

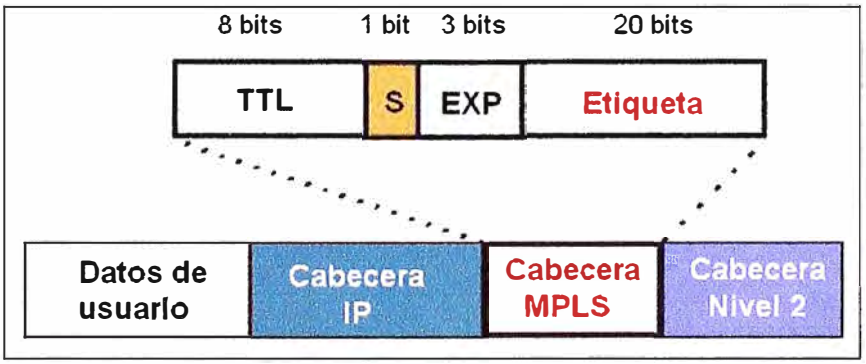

Figura 1.4 Formato de la etiqueta MPLS

1.3.1 Etiquetas MPLS

Una etiqueta tiene 32 bits y es usada para identificar un FEC determinado, usualmente de significado local. La etiqueta, la cual es adjunta a un paquete particular, representa la FEC a la cual el paquete será asignado. En la figura 1.4 se observa el formato de la etiqueta MPLS.

Esta etiqueta esta dividida en los siguientes campos:

- Etiqueta (*20 bits*). Contiene el valor de la etiqueta asignada.
- Experimental (*3bits*). Identifica la clase de servicio.

- S (*1 bit*). Permite apilar etiquetas de forma jerárquica: si el valor es 1, entonces indicará la posición inferior.
- TTL (*8 bits*). Tiempo de vida (time-to-live), últimos bits del paquete utilizados para codificar el valor del conteo de saltos (IPv6) o de tiempo de vida (IPv4).

Para el caso de ATM, la etiqueta es ubicada dentro del campo VCI o VPI de la cabecera ATM. Sin embargo, en el frame de Frame Relay, la etiqueta ocupa el campo DLCI de la cabecera Frame Relay.

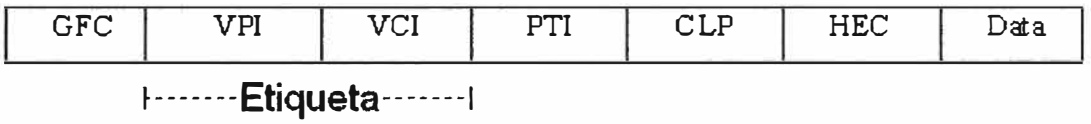

Figura 1.5 Cabecera ATM

Tecnologías de la capa 2 como Ethernet, Token Ring, FDDI y enlaces PPP no pueden utilizar el campo de dirección de la capa 2 para llevar la etiqueta. Esta tecnología lleva la etiqueta en un campo llamada *Shim Header*. La etiqueta en la cabecera *shim* es insertada entre las cabeceras de la capa de enlace y la capa de red. El uso de la cabecera *shim* permite a MPLS ser soportado sobre muchas de las tecnologías de la capa 2.

Figura 1.6 Cabecera Shim

La lectura de la cabecera *shim* debe de ser soportada por el router que envía y el que recibe el frame. Esto es facilitado de manera diferente por cada tecnología. Por ejemplo:

- *Ethernet* usa para el campo *ethertype* los valores de 0x8847 y 0x8848 para indicar la presencia de la cabecera *shim*. El valor de 0x8847 es usado para indicar que un frame esta llevando un paquete *unicast MPLS*, y el valor de 0x8848 es usado para indicar que un frame esta llevando un paquete *multicast MPLS*.
- *Token Ring y FDDI* también usan valores como parte de la cabecera SNAP.
- En el caso de *PPP*, se hace uso de un modificado NCP (*Network Control Program*) conocido como protocolo de control de MPLS (MPLSCP) y marca todos los paquetes contenidos en la cabecera *shim* con 0x8281 en el campo del protocolo PPP. *Frame Relay* usa el Identificador de protocolo de la de la capa de

red SNAP (NLPID: *Network Layer Protocol ID)* y la cabecera SNAP se marca con el valor *type* de 0x8847 y 0x8848.

Es posible que los paquetes etiquetados requieran de fragmentación, como en el caso de paquetes IP, ya que es posible que un paquete requiera la asignación de más de una etiqueta, por lo cual puede requerirse la fragmentación del mismo. Para estos casos, la fragmentación es realizada sobre el datagrama IP, y luego se especifica la misma utilizando el bit de *Stack* y la información de etiqueta.
Existen etiquetas reservadas para los casos de fragmentación, estas son:

1. 0: IPv4 Explicit Null.
2. 1: Router Alert.
3. 2: IPv6 Explicit Null.
4. 3: Implicit Null.
5. 4-15: Reservado para uso futuro

La etiqueta *Explicit Null* es utilizada en los casos donde se necesita encapsulación de etiqueta, pero no se necesita una etiqueta valida. Cuando se utiliza esta etiqueta, deberá ser la única en la pila de etiquetas. La mayoría de las encapsulaciones utilizadas en Capa 2, como PPP, Ethernet, etc., contienen un campo que especifica el protocolo de capa 3.
La etiqueta *Router Alert* es utilizada para informar al router que el paquete necesita ser tratado de forma más amplia que simplemente realizar un reenvió del mismo. Cuando un LSR recibe un paquete con esta etiqueta, toma la primera etiqueta de la pila de etiquetas y reenvía el mismo utilizando esta información de etiqueta en caso que el paquete deba ser reenviado.
La etiqueta *Implicit Null* no es un valor valido de etiqueta que puede aparecer en el *Header* de un paquete transmitido, esta reservada para ser utilizada por el protocolo de distribución de etiqueta.

1.3.2 Procesando el TTL

Un elemento clave en el encabezado de un paquete IP es el campo TTL (Time To Live) y el límite de saltos. En un ambiente común de Internet (basado en el protocolo IP), dicho campo TTL va disminuyendo uno a uno hasta que llega a cero y se elimina el paquete. Esta es una medida que se utiliza con la finalidad de evitar que los paquetes caigan en un bucle o estén demasiado tiempo circulando en Internet debido a un enrutamiento mediocre que pueda originar problemas como congestión de la red por tráfico innecesario.

En el enrutamiento MPLS no se lee el encabezado de los paquetes, es por eso que se añaden estos 8 bits que manejan el TTL para evitar que ocurra lo mencionado anteriormente.
A continuación algunas reglas que se utilizan para procesar el campo TTL:

a) Cuando un paquete IP llega al router de entrada de un dominio MPLS, solo se añade una etiqueta de entrada a la pila, el valor de TTL de este campo se obtiene del valor original del TTL en IP. En este paso se da por supuesto que el campo ya fue disminuido, como parte del proceso IP. Cuando un paquete MPLS llega a uno de los LSR internos, el valor del campo TTL de la etiqueta del primer elemento en la pila es disminuido. Entonces:

- Si el valor es 0, no se reenvía el paquete, dependiendo del valor que tenga la etiqueta del paquete puede ser desechado o es enviado al nivel de red para procesamiento de errores.
- Si el valor es positivo, se le añade a la nueva etiqueta de la pila en el campo TTL y es reenviado al siguiente salto. El valor del campo TTL del paquete reenviado esta dado en función del valor del campo de Tiempo de Vida del paquete original.

b) Cuando un paquete MPLS llega aun un LSR de salida, el valor del campo TTL en la etiqueta es diminuido (uno por uno) y posteriormente se quita la etiqueta de la pila, lo que deja una pila vacía. Entonces:

- Si el valor es 0, no se reenvía el paquete, dependiendo del valor que tenga la etiqueta del paquete puede ser desechado o es enviado al nivel de red para procesamiento de errores.
- Si el valor es positivo, se coloca en el campo TTL del encabezado IP y es enviado utilizando enrutamiento IP tradicional.

Es importante mencionar que cuando el valor del campo TTL llega a 0 y el paquete no ha llegado a su destino predefinido en el valor de la etiqueta, dicho paquete es desechado y se envía un mensaje del Protocolo de Control de Mensajes de Internet (ICMP) al remitente. Esto con el fin de evitar que un paquete no entregado se quede circulando en el Internet.
En teoría TTL esta medido en segundos, aunque cada equipo que pase el paquete debe reducir el Tiempo de Vida en al menos una unidad. El campo TTL es disminuido en una unidad en cada salto, es por eso que en IPv6 a este decremento de unidades en cada salto se la llama Conteo de Saltos.

1.3.3 Pila de etiquetas

La última sección del formato de las etiquetas es la sección S, en donde esta contenida la información del orden de la pila. Cuando S=1 indica que es la última etiqueta y que al salir quedará vacía la pila, esto generalmente ocurre en el router de salida, cuando es S=0 indica que por lo menos hay otra etiqueta antes, en la pila.

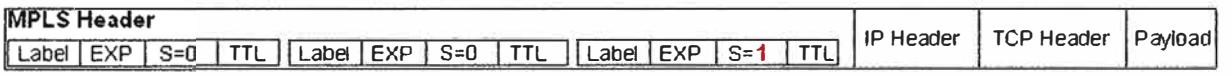

Figura 1.7 Pila de etiquetas MPLS

Lo anterior se puede ver claramente en la Figura 1.7. Es muy importante considerar que cuando un enrutador de etiquetas de frontera (LER) saca el último encabezado MPLS del paquete este debe de mandar la información (payload) fuera de la nube MPLS al destino contenido en el encabezado IP, previamente obtenido por el router de entrada. La importancia radica en que los enrutadores MPLS no cuentan con tablas de búsqueda de etiquetas.

Para entender esto podemos ver que cuando a un router MPLS le llega el valor S=1 en el encabezado MPLS se sabe que el siguiente encabezado es el encabezado de red y que debe usarlo para reenviar el paquete conforme al mecanismo de ese tipo de red. Como se menciona anteriormente MPLS soporta múltiples protocolos de red, en realidad todos, pero un encabezado IP no tiene la misma estructura Ethernet, por lo que aunque el router de salida sepa que lo siguiente en la pila es un encabezado de red, no sabe de que tipo es y no puede interpretarla.

Esto se soluciona leyendo los valores reservados del campo de valor de la etiqueta de 20 bits, esto indicará el tipo de encabezado de la red para que así pueda entender lo que este le dice.

1.4 LSP

Un LSP (*Label-Switched Path*) es un camino específico por el cual pasa tráfico en una red MPLS. Los LSPs son aprovisionados usando un protocolo de distribución de etiquetas que puede ser LDP (*Label Distribution Protocol*) o el protocolo TDP (*Tag Distribution Protocol*) propietario de CISCO, RSVP (*Resource Reservation Protocol*) con una extensión de ingeniería de tráfico (RSVP-TE), o una extensión de protocolos de enrutamiento tales como Multi-Protocolo BGP.

Un LSP puede ser considerado el camino creado sobre un grupo de LSRs en el cual los paquetes que viajan pertenecen a una cierta FEC para alcanzar su destino.

MPLS permite una jerarquía de etiquetas conocida como pila de etiquetas. Por consiguiente es posible tener diferentes LSPs con diferentes niveles de etiquetas en un paquete para alcanzar su destino. LSPs son unidireccionales, esto significa que un paquete podría tomar una ruta diferente en su camino de regreso.
Para construir un LSP, los LSRs hacen uso de protocolos de enrutamiento y las rutas aprendidas de estos protocolos. LSRs pueden usar otros protocolos tal como RSVP, pero ya no son requeridos.

1.4.1 Establecimiento de un LSP

Para el establecimiento del los LSP, MPLS utiliza dos mecanismos de control:

- Control Ordenado: la asignación de etiquetas se realiza de forma ordenada desde un extremo a otro del LSP. El establecimiento del mismo puede ser generado por el LER de ingreso (cabecera) o egreso (cola) del LSP. Un LSR puede distinguir si es LER de cola para un dado FEC, si el siguiente salto para este FEC no es un LSR entonces, asignará una etiqueta al FEC, y publicará la asignación a su LSR adyacente. Cualquier adyacencia que tenga al Edge LSR como siguiente salto para dicho FEC, le asignará una etiqueta a dicho FEC y lo publicará a su adyacencia, y así sucesivamente. Así, la asignación de etiquetas sigue un procedimiento ordenado de egreso a ingreso. Este mecanismo ayuda a la prevención de bucles. Es útil en redes que se encuentren migrando de un enrutamiento IP convencional a MPLS
- Control Independiente: la conmutación de etiquetas se realiza sobre la base de protocolos de enrutamiento; cada LSR deberá tomar una decisión independiente para asignar una etiqueta a un FEC predeterminado, y luego publicar esta asignación a su adyacencia. El establecimiento del LSP estará afectado por la convergencia del protocolo de enrutamiento utilizado.

Con el mecanismo Control Independiente, cada LSR realiza una elección propia acerca de cómo distribuir el conjunto de los posibles paquetes de datos dentro de los FECs. Si el LSR adyacente toma una decisión diferente a cerca de los FEC que utilizará, no será posible establecer un LSP para dichos FECs. En Control Ordenado, la elección de FECs puede ser realizada en el LSR que inicia el LSP. Así todos los LSR utilizarán el mismo FEC. El LSR deberá determinar el siguiente salto para un FEC predeterminado, de manera de poder determinar si conexión proviene del siguiente salto correcto. Una desventaja es el tiempo que se requiere para el establecimiento de un LSP. Requiere que las asignaciones sean propagadas a través de todos los LSR antes que el LSP sea

establecido. Durante este período algunos paquetes pueden ser descartados incrementando la carga del procesador en los LSR. Esto no sucede en Control Independiente, ya que un LSR puede establecer y publicar asignaciones de etiqueta en cualquier momento, sin tener que esperar la propagación de los mensajes.
Otra característica importante de Control Independiente se basa en el hecho que los LSRs tienen la capacidad de almacenar la asignación de etiqueta de los LSRs que eran adyacentes al momento de realizar la propagación de las mismas, lo cual le permite establecer LSPs en forma casi instantánea cuando se producen cambios en el enrutamiento. Esto redunda en una más rápida convergencia que la que se tiene con Control Ordenado.

1.4.2 Selección de ruta

Es el método empleado para seleccionar el camino (LSP) para un FEC en concreto. Existen 2 opciones para seleccionar una ruta:

- Enrutamiento salto a salto: cada enrutador LSR puede seleccionar independientemente el siguiente salto para un FEC determinado (similar a la metodología usada en redes IP). El enrutador LSR utiliza cualquier protocolo de enrutamiento disponible como OSPF, ATM PNNI (ATM Private Network-Node Interface), etc.
- Enrutamiento explicito: El LER de entrada determina la secuencia de saltos explicita desde la entrada hasta la salida (ER-LSP Explicit Routing LSP). Puede que la ruta no este completamente especificada, es decir, puede haber un conjunto de nodos (Nodo Abstracto) que es representado como un único salto en la ruta. También puede contener un identificador de Sistema Autónomo que permite que el LSP sea encaminado a través de un área de la red que esta fuera del control administrativo de quien inicio el LSP. Dentro de estos dos casos se hará un enrutamiento salto a salto. Puede clasificarse como estricto (strict), aquel camino que incluye todos los nodos, nodos abstractos y Sistemas Autónomos por los que pasa y el orden establecido; o como tolerante (loose), aquel que incluye todos los saltos y mantiene el orden, pero puede incluir saltos que sean necesarios para alcanzar algún salto especifico. El camino puede que no sea óptimo puesto que deben tenerse en cuenta los parámetros del servicio. Los recursos serán reservados a lo largo del camino para asegurar calidad de servicio (QoS). Esto facilita la ingeniería de tráfico y el poder tener servicios diferenciados usando políticas de tráfico o métodos de gestión de red.

1.5 Prevención y detección de bucles

Los paquetes MPLS poseen un campo TTL al igual que los paquetes IP, el cual es utilizado para descartar paquetes que hayan caído bajo un bucle transitorio. No obstante, con ciertas tecnologías de red este campo no esta disponible, como el caso de MPLS sobre ATM.

Una forma de mitigar el efecto de los bucles es mediante la utilización de *Buffers*. Esto es útil en el caso de utilizar MPLS sobre ATM, ya que ATM tiene la capacidad de limitar la capacidad de los *Buffers* para un dado VC, lo cual disminuye el efecto producido por los paquetes que entraron en un bucle transitorio. Esta técnica de utilización de *Buffers* también es valida para los casos de bucles no transitorios, los cuales pueden ocurrir por errores de configuración.

Otra forma de controlar la formación de bucles en tecnologías que no soporten TTL es mediante la cuenta de saltos, pero este mecanismo pude no ser suficiente para controlar el efecto adverso de los bucles transitorios.

Un mecanismo utilizado por MPLS para realizar la detección de bucles es el denominado *Path Vectors*. Un *Path Vector* es una lista de LSRs por los cuales han pasado mensajes de *Label Requets* o *Label Mapping*. Si un bucle de enrutamiento causa que un mensaje de *Label Request* o *Label Mapping* viaje en un bucle, eventualmente un LSR "verá" su dirección en el mensaje de *Label Request* o *Label Mapping*, y así detectará un estado de bucle.

El mecanismo denominado *Colored Threads*, es utilizado por la arquitectura MPLS para la prevención de bucles. Este requiere de la utilización del mecanismo Control Ordenado para el establecimiento de los LSPs a través de la red MPLS. El establecimiento del LSP se realiza mediante la extensión de un único flujo, o *Thread*, coloreado en sentido ingreso a egreso del LSP. Si el bucle del flujo vuelve sobre si mismo, un nodo detectará un color que él ya había "visto" antes, y así concluirá que se trata de un bucle. En este punto, se interrumpe el establecimiento del LSP hasta que desaparezca el bucle. Este mecanismo es tan robusto como el método de *Path Vector* para la prevención de bucles en el establecimiento de LSPs, pero requiere mucha menor transmisión y almacenamiento de información en cada salto.

1.6 Protocolos de señalización

La arquitectura MLPS permite varios protocolos de señalización para la distribución de etiquetas entre los enrutadores LSRs, el uso de cada uno de ellos dependerá del hardware de la red MPLS y de las políticas de administración de esta.

Protocolos de enrutamiento como BGP permiten llevar piggybacked información sobre las etiquetas entre los contenidos propios del protocolo, se utilizan para etiquetas externas en Redes Privadas Virtuales.
RSVP también ha sido extendido para soportar intercambio de etiquetas piggybacked.
Además, MPLS tiene su propio protocolo LDP para señalización y gestión del espacio de etiquetas, a este se le han añadido extensiones para soportar, también, requerimientos de calidad de servicio y clases de servicio, así tenemos CR-LDP (Constraint-based LDP)

1.6.1 LDP (Protocolo de Distribución de etiquetas)

El protocolo de distribución de etiquetas LDP es usado en conjunto con el protocolo de red estándar para distribuir la información de unión de etiquetas entre dispositivos LSR en una red de conmutación de etiquetas. El protocolo LDP permite a un enrutador LSR distribuir etiquetas a su *peer* LDP usando el puerto TCP 646, mientras que el protocolo TDP de Cisco usa el puerto TCP 711. El uso de TCP como el protocolo de la capa de transporte permite un confiable envío de información LDP con un robusto control de flujo y manejo de mecanismos de congestión.
El protocolo de distribución de etiquetas TDP de Cisco y el Standard LDP en MPLS tienen funciones cercanamente idénticas, pero usan formatos incompatibles de mensajes y algunos diferentes procedimientos.
Cuando un LSR asigna una etiqueta a una FEC, este LSR necesita dar a conocer a sus pares acerca de esta etiqueta y de su significado. LDP es usado para este propósito. Un grupo de etiquetas del LER de ingreso al LER de egreso en un dominio MPLS definen un LSP. Las etiquetas son usadas como mapas del enrutamiento de la capa de red a los caminos conmutados de la capa de enlace de datos. LDP ayuda a establecer un LSP usando un grupo de procedimientos para distribuir las etiquetas entre los pares LSRs.
LDP proporciona a un LSR mecanismos de descubrimiento para permitir a los pares LSR ubicar uno al otro y establecer comunicación.

LDP define cuatro clases de mensajes:

- Mensajes *Discovery.*
- Mensajes *Adyacency*. Permiten la inicialización, *keepalive*, y cierre de sesiones entre dispositivos LSR.
- Mensajes *Label Advertisement.* Permiten la publicación de *bindings* de etiquetas, pedidos, y liberaciones.
- Mensajes *Notification.* Permiten enviar información de aviso de problemas y señalizar errores.

a) LSR Neighbor Discovery

El protocolo LDP Neighbor Discovery se implementa sobre UDP. Un LSR envía periódicamente, en forma Multicast, mensajes de *Hello* utilizando un puerto UDP bien conocido, así todos los LSR escuchan sobre este puerto UDP por mensajes de *Hello*, aprendiendo de esta manera todos los LSR con los cuales tendrá conexiones.

Cuando un LSR aprende la dirección de otro LSR mediante este mecanismo, establece una conexión TCP con este, estableciéndose así una sesión LDP entre ambos. La sesión LDP es bidireccional.

Un mecanismo de *Discovery* adicional le permite a un LSR descubrir otro LSR aun cuando no estén directamente conectados por una sub-red. En este caso, un LSR envía periódicamente mensajes de *Hello Unicast*, sobre un puerto UDP bien conocido, a una dirección IP especifica, la cual debe aprender por algún otro medio, por ejemplo: por configuración. El LSR receptor de este mensaje puede responder con un mensaje de *Hello Unicast* al LSR que lo origino, estableciéndose luego una sesión TCP entre ambos y la sesión LDP. Este mecanismo es útil para el caso de utilizar *Traffic Engineering* sobre un LSP entre dos LSR.

b) Transporte confiable

La necesidad de contar con un transporte confiable surge de que si una asignación de etiqueta o el pedido de un asignación no son entregados en forma satisfactoria, el tráfico no podrá ser conmutado utilizando conmutación de etiquetas, por lo cual debería ser tratado utilizando el proceso de control o descartado. Además, en ciertos casos es necesario recibir los mensajes en orden. Ambas características son logradas utilizando TCP como protocolo de transporte.

TCP le provee a LDP una paquetización eficiente de mensajes de capaz superiores dentro de datagramas IP, el *piggybacking* de mensajes de *ACK* en paquetes de datos, y el control de flujo, lo cual es una característica importante para un protocolo de control como lo es LDP.

No obstante, TCP provee de un mecanismo de control de congestión que puede no ser necesario para un protocolo de control *neighbor-to-neighbor*, lo mismo con el control estricto de secuencia en la entrega paquetes.

c) Mensajes LDP

Existen las siguientes clases de mensajes LDP:

- *Mensajes de Inicialización.* Los mensajes de Inicialización son enviados al comienzo de una sesión LDP, para permitir que dos LSRs acuerden los parámetros y opciones de la sesión. Estos mensajes incluyen: Label Allocation Mode, Timers y información sobre el rango de etiquetas a ser utilizado entre dos LSRs. Ambos LSRs pueden enviar mensajes de Inicialización y responder con un *Keepalive* si los parámetros son aceptados. Si alguno de los parámetros no es aceptado, el LSR responde con un mensaje de *Error Notificación*, y la inicialización de la sesión es terminada.
- *Mensajes Keepalive.* Son enviados periódicamente por los LSRs en ausencia de algún otro mensaje de modo de asegurar que cada uno de los pares LDP sabe que el otro par se encuentra funcionando correctamente. En ausencia de mensajes *Keepalive*, o de algún otro mensaje LDP dentro de un intervalo de tiempo, un LSR concluye que el par LSR, o que la conexión entre ambos, no se encuentra activa, y termina la sesión LDP.
- *Mensajes Label Mapping.* Forman una parte fundamental dentro del mecanismo de distribución de etiquetas. Se utilizan para la publicación de información de asignación entre un FEC y una etiqueta.
- *Mensajes Label Withdrawal.* Son utilizados para remover información de asignación entre un FEC y una etiqueta que fuera previamente publicada.
- *Mensajes Label Release.* Son utilizados por un LSR que previamente recibió un mapeo de etiqueta y que ya no necesita de tal mapeo. Esto sucede cuando un LSR encuentra que el siguiente salto para dicha asignación no es el LSR publicado. Para esto el LSR se debe encontrar operando en el modo *Conservative Label Retention*.
- *Mensajes Label Request.* Son utilizados cuando un LSR solicita una asignación de etiqueta a su par LSR, en sentido downstream o upstream dependiendo del modo que se encuentre operando, ya sea en modo de asignación de etiqueta Unsolicited Downstream o Upstream-on-demand.
- *Mensajes Label Request Abort.* Si un mensaje Label Request necesita ser rechazado antes de ser satisfecho, por ejemplo, si el siguiente salto para el FEC en cuestión ha cambiado, el par LSR aborta el pedido enviando un mensaje *Label Request Abort*.

d) Modos de Distribución de etiquetas

Los modos de distribución de etiquetas son:

- Unsolicited Downstream.

- Unsolicited Upstream.
- Downstream-on-Demand Label Assignment.
- Upstream-on-Demand Label Assignment.
- Ordered LSP Control.
- Independent LSP Control.
- Liberal Label Retention.
- Conservative Label Retention.

Todos estos tipos de modos de distribución son negociados al inicio de una sesión LDP. Cuando un LSR opera en modo *Conservative Label Retention* sólo almacena las asignaciones entre FEC y etiquetas que necesitan en un cierto instante. Toda otra información de asignación es desechada.
Cuando un LSR opera en modo *Liberal Label Retention* almacena todas las asignaciones entre FEC y etiqueta que le hayan sido publicados. Este modo de operación permite tener un mejor tiempo de respuesta ante cambios de enrutamiento, lo cual es importante en dispositivos que almacenan en hardware información de asignación de etiquetas para luego realizar el reenvió de paquetes, como el caso de ATM-LS.

1.6.2 CR-LDP

(Constraint-Based LDP), a diferencia de RSVP-TE, no necesita de implementaciones adicionales ya que esta basado en LDP y utiliza su misma estructura para los mensajes.
Es un protocolo *hard state*, es decir, toda la información se intercambia al iniciar la conexión y no se produce más información adicional hasta que el LSP se elimine. CR-LDP utiliza conexiones TCP entre compañeros LSR lo que hace que estas sean más fiables y seguras, así mismo las conexiones TCP CR-LDP permiten detectar un fallo mediante notificaciones propias de TCP. Al igual que RSVP-TE soporta re-enrutamiento.
Creación de un ER-LSP (Explicit Routing LSP):

1. El E-LSR (Edge LSR) de entrada quiere establecer un nuevo LSP hacia el E-LSR de salida. Los parámetros de trafico determinan por donde debe pasar la ruta, así que el E-LSR de entrada reserva los recursos que necesita y envía un mensaje LABEL_REQUEST con la ruta explicita hacia el E-LSR de salida y con los parámetros de trafico que requiere la sesión.
2. Cada nodo de la ruta que recibe el mensaje reserva los recursos y determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje LABEL_REQUEST eliminándose de la ruta. Puede reducir la reserva si los parámetros de tráfico están marcados como negociables.

3. Una vez llega al E-LSR de salida, esté realiza cualquier negociación final sobre los recursos y hace la reserva. Asigna una nueva etiqueta al nuevo LSP y la distribuye en un mensaje LABEL_MAPPING que contiene los parámetros de tráfico finales reservados para el LSP.
4. Los LSRs intermedios emparejan los mensajes LABEL_REQUEST y LABEL_MAPPING que han recibido según el identificador de LSP, asignan una etiqueta para el LSP, rellenan la tabla de envió y envían la nueva etiqueta en otro mensaje LABEL_MAPPING.
5. En cuanto llegue al E-LSR de entrada se habrá establecido el LSP.

1.6.3 RSVP-TE

(Resource ReSerVation Protocol-Traffic Engineering) es una extensión del protocolo RSVP original que fue diseñado para ejecutar la distribución de etiquetas sobre MPLS. RSVP-TE es un protocolo de señalización *soft state* que utiliza UDP o datagramas IP para la comunicación entre compañeros LSR (pares LSR), lo cual significa que la información es intercambiada cuando se establece el LSP, pero se deben enviar mensajes periódicos para notificar que la conexión todavía se requiere. El hecho que RSVP-TE sea *soft state* introduce una sobrecarga adicional y esto hace que no sea escalable ya que esta sobrecarga crecerá proporcionalmente con el número de sesiones RVSP, para evitar esto se intenta resumir la información y aprovechar un único mensaje para enviar varios mensajes de refresco.

Una de las características adicionales más importantes de este protocolo es que permite el re-enrutamiento de los túneles LSP, con el fin de dar una solución ante caídas de red, congestión y cuellos de botella.

Originalmente el IETF propuso a RSVP-TE como el protocolo de señalización principal, ya que este era utilizado por la mayoría de las compañías de Internet en MPLS y porque la tendencia es utilizar un protocolo de señalización RSVP.

Creación de un ER-LSP (Explicit Routing LSP):

1. El E-LSR (Edge Label Swicth Router) de entrada quiere establecer un nuevo LSP hacia el E-LSR de salida. Los parámetros de tráfico determinan por donde debe pasar la ruta, así que el E-LSR de entrada envía un mensaje PATH con la ruta explicita hacia el E-LSR de salida y con los parámetros de tráfico que requiere la sesión.
2. Cada nodo de la ruta que recibe el mensaje determina si es la salida para ese LSP, si lo es, sigue enviando el mensaje PATH eliminándose de la ruta. En cualquier caso cada LSR creará una nueva sesión.

3. Una vez que llega al E-LSR de salida, este determina que recursos ha de reservar y devuelve un mensaje RESV que distribuirá la etiqueta que ha elegido para ese LSP y contendrá los detalles de la reserva. La etiqueta se envía y distribuye dentro del mensaje RESV en el objeto LABEL. El mensaje se envía por el puerto donde llego el mensaje PATH.
4. Los LSRs intermedios emparejan los mensajes PATH y RESV que han recibido según el identificador de LSP, reservan los recursos que indica RESV, asignan una etiqueta para LSP, rellenan la tabla de envió y envían la nueva etiqueta en otro mensaje RESV.
5. El E-LSR de entrada, cuando recibe el mensaje RESV, enviará un mensaje de confirmación RESVConf para indicar que se ha establecido el LSP.

Después de haberse establecido el LSP se enviarán mensajes periódicos para mantener el camino y las reservas. En el tráfico multicast en RSVP-TE y CR-LDP se le llama caminos multicast de conmutación de etiquetas (mLSP) al conjunto de LSPs configurados. Una de las ventajas que tiene RSVP-TE sobre CR-LDP es que la operación de actualización de los mensajes PATH y RESV muestra los enlaces activos para identificar fácilmente cuando un LSP no puede ser establecido. Cuando esto pasa se generan los mensajes PATHERR y RESVERR. Otra forma de descartar errores, mas sencilla y robusta, es mediante HELLO, para descartar fallas nodo a nodo.
Los nuevos objetos en RSVP-TE:

- LABEL_REQUEST (PATH): Para requerir una etiqueta
- LABEL (RESV): Contiene una etiqueta
- EXPLICIT_ROUTE (PATH): Contiene una lista de router que definen el túnel
- RECORD_ROUTE (PATH/RESV): Contiene los routers que definen el túnel
- SESSION_ATTRIBUTE (PATH)

A lo largo del capitulo se ha descrito como funciona MPLS, los principales componentes que intervienen en esta arquitectura y como actúan de forma conjunta. Conceptos que son necesarios de conocer con la finalidad de comprender mejor el desarrollo del siguiente capitulo que trata de las aplicaciones en MPLS.

II
APLICACIONES EN MPLS

En el momento actual, todos los proveedores de servicio tienen ante sí el enorme reto de gestionar redes cada vez más complejas y extensas, con una mayor gama de servicios y con creciente demanda de ancho de banda, calidad y garantías. Para los backbones, las posibilidades que ofrecen la extensión de infraestructuras de fibra óptica y las nuevas tecnologías de transmisión DWDM son enormes. En este contexto, la evolución natural de redes IP y aplicaciones TCP/IP han llevado a desarrollar la arquitectura MPLS como una de las opciones más prometedoras para proporcionar los nuevos servicios del siglo XXI.

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel, es una arquitectura multiprocolo capaz de funcionar sobre cualquier tecnología de transporte lo que facilita de modo significativo la migración para la próxima generación de la Internet óptica, en la que se acorta la distancia entre el nivel de red IP y la fibra.

MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las tecnologías tradicionales de encaminamiento IP, permite hacer Ingeniería de Tráfico IP, mantener clases de servicio, soporta con gran eficacia la creación de VPNs, el enrutamiento Multicast, así como la extensión sobre redes ópticas con el denominado GMPLS. Por todo ello, MPLS es actualmente la arquitectura que promete poder mantener el ritmo actual de crecimiento de la Internet.

2.1 Red Privada Virtual

En la actualidad es muy frecuente escuchar el término VPN, debido a la gran demanda de redes privadas por parte de empresas y organismos, y dada su fuerte inserción en el mercado de los proveedores de servicio.

Si bien han aparecido nuevos protocolos y tecnologías que proponen mejorar las prestaciones, reducir los costos, incrementar los niveles de seguridad o extender los métodos de acceso, el concepto de VPN lleva más de una década en el mercado sin modificarse.

Una VPN es una red (corporativa, educativa, etc.) en la que los distintos sitios que la conforman son conectados utilizando una infraestructura compartida, pero quedando independiente y asilada de otras redes.
La infraestructura compartida normalmente es provista por el proveedor de servicios (quien administra los recursos y mantiene las políticas de acceso y seguridad dentro de la red) o hasta incluso también podría serlo la misma Internet.
Existen dos modelos principales para la implementación de Redes Privadas Virtuales:

- Overlay VPN.
- Per-to-Per VPN.

El modelo Overlay VPN es ampliamente utilizado y es el más sencillo de entender. En este modelo establece claramente la separación entre las responsabilidades del cliente y el proveedor de servicios:

- El proveedor de servicios proporciona al cliente los circuitos virtuales necesarios para establecer conectividad entre sus sitios sin preocuparse por el plan de direccionamiento del cliente.
- El cliente por su parte establece comunicación enrutador a enrutador desde sus sitios, utilizando los circuitos virtuales establecidos por el proveedor y administra su plan de direccionamiento.

Este tipo de VPN se implementa principalmente con tecnologías de nivel 2 como Frame Relay y ATM y normalmente los circuitos virtuales son conocidos como PVCs (Permanent Virtual Circuit). También pueden construirse sobre una red IP de nivel 3 utilizando túneles de nivel 2 utilizando protocolos como L2TP.
La principal desventaja de este tipo de VPN es que la administración de los PVC y de los túneles se realiza de manera manual por el operador de la red y en caso de alguna falla no reacciona automáticamente, además de que la agregación o remoción de sitios del cliente es lenta y administrativamente costosa.

En el modelo Per-to-Per VPN la conexión entre el cliente y el proveedor de servicios es entre un par de enrutadores: uno en la frontera de la red del proveedor (conocido como PE) y el otro en el sitio del cliente (conocido como CPE).
Este par de enrutadores intercambian directamente información de enrutamiento con lo que el proveedor de servicios se involucra directamente en el plan de direccionamiento del cliente. El proveedor de servicios ofrece este modelo sobre una red IP. El modelo Per-to-Per presenta una serie de ventajas con respecto al modelo anterior (Overlay VPN):

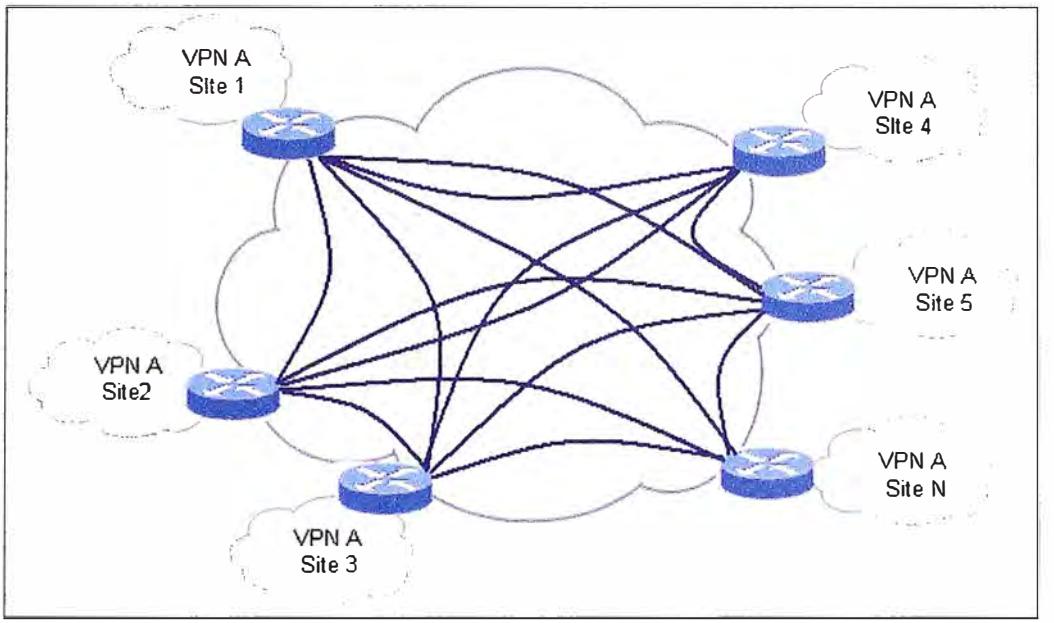

Figura 2.1 Modelo Overlay VPN

- El CPE solo tiene que intercambiar información de enrutamiento con el PE, no con todos los enrutadores en los sitios conectados.
- Las trayectorias entre los sitios del cliente son las mejores, ya que el enrutamiento está a cargo del protocolo de enrutamiento habilitado en la red del proveedor,
- El aprovisionamiento de ancho de banda solo tiene que contemplar la conexión entre el CPE y el PE, no en todos los PVC.
- La adición de nuevos sitios es sencilla ya que solo hay que conectar el CPE del nuevo sitio y automáticamente se tiene información de enrutamiento para alcanzar las direcciones de red incorporadas.

Un par de desventajas pueden apreciarse en esta solución:

- Para mantener aisladas cada una de las VPN se necesita un PE por cada PCE.
- Se debe ser cuidadoso con el plan de direccionamiento del cliente para que no se traslape con alguna otra VPN.

Existen soluciones para ocultar estas desventajas pero son costosas tanto en recursos de procesamiento como en su administración.

La topología de una VPN también puede ser diversa, como por ejemplo:

- Hub and Spoke: En donde los distintos sitios de una compañía están conectados al Headquarter, que puede proveer o no comunicación entre sucursales. Similar a una topología en estrella.

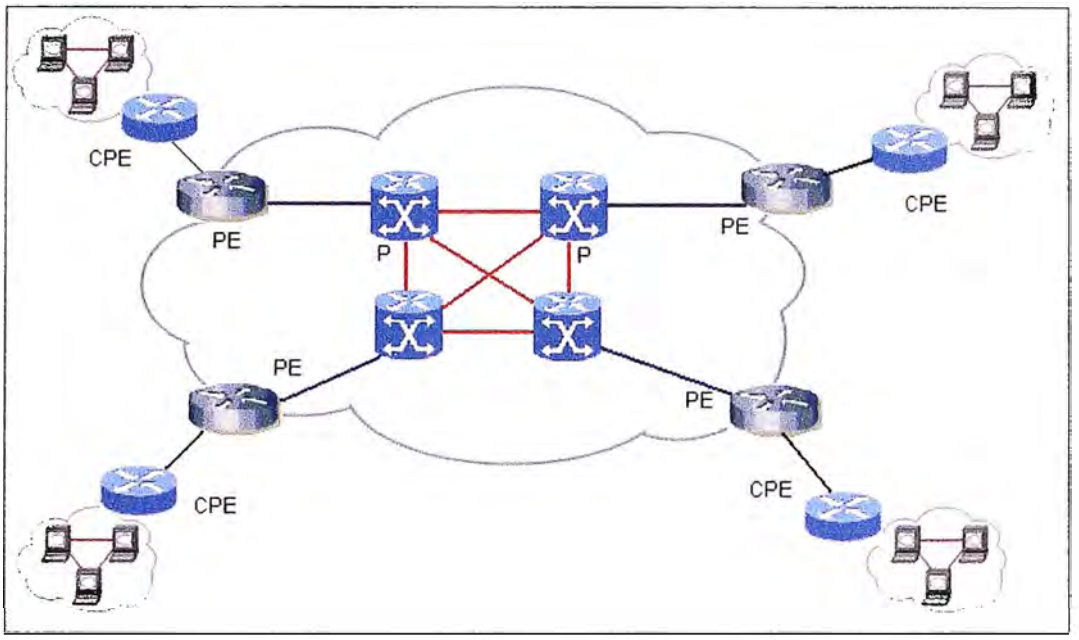

Figura 2.2 Nodelo Per-to-Per VPN

- Full Mesh: En donde todos los sitios de la Red Privada Virtual están conectados entre sí. Las redes con topología Full Mesh pueden implicar altos costos de mantenimiento y administración.
- Partial Mesh: Se establecen relaciones de algunos con al algunos dentro de la Red Privada Virtual. Esta topología se presenta como una solución cuando no se tienen los recursos necesarios o bien cuando no hace falta tener una relación todos contra todos.

2.1.1 Arquitectura MPLS-VPN

La solución MPLS-VPN combina los beneficios de las Overlay VPN, como son la seguridad y el aislamiento y la capacidad de reacción ante las fallas de las Per-to-Per VPN. MPLS-VPN proporciona un enrutamiento simple con el sitio del cliente y un aprovisionamiento sencillo en la red del proveedor, además de permitir la creación de topologías difíciles de implementar en las soluciones anteriores.

En la arquitectura MPLS-VPN se tienen 3 tipos de dispositivos:

- PE (*Provider Edge Router*): enrutador que se encuentra en la frontera de la red MPLS del proveedor con conexión a los enrutadores CPE.
- P (*Provider Core Router*): enrutador que se ubica en la red interna del proveedor, sin conexión a los enrutadores CPE.
- CPE (*Customer Premise Equipment*): enrutador frontera ubicado en el sitio del cliente, conectado a algún enrutador PE de la red del proveedor de servicios de telecomunicaciones.

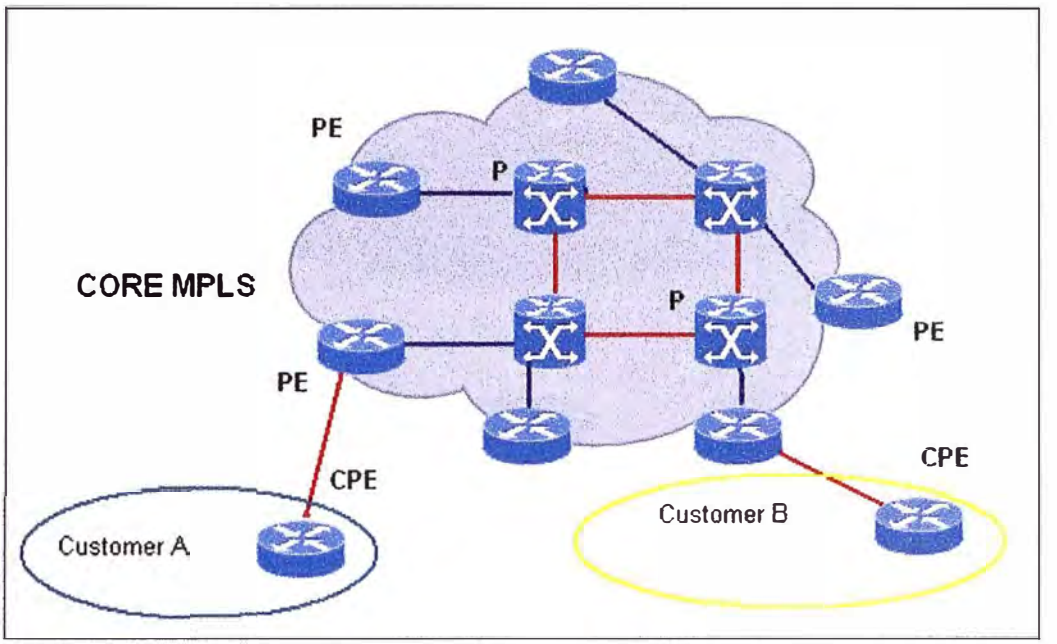

Figura 2.3 Arquitectura MPLS-VPN

El aprovisionamiento de los recursos de red para cada una de las VPN se realiza con base a etiquetas MPLS y un concepto conocido como enrutador virtual.

a) Enrutador Virtual

Cada enrutador PE es capaz de administrar en forma aislada la información de enrutamiento de varias Redes Privadas Virtuales mediante la función de Enrutador Virtual. Bajo este concepto para cada Red Privada Virtual se creada una tabla de enrutamiento totalmente independiente conocida como VRF (*VPN Routing and Forwarding*), en cada VRF solo aparece la información de los prefijos de red correspondientes a la Red Privada Virtual del cliente. Esta función permite asignar a los clientes un plan de direccionamiento privado e incluso utilizar el mismo direccionamiento en varias Redes Privadas Virtuales para diferentes clientes. En la figura 2.4 se muestra un esquema que permite entender la idea de enrutador virtual.

b) Asignación de interfaces

Cuando se conecta un enrutador CPE a un enrutador PE, la interfaz utilizada en el enrutador PE para recibir el enlace desde el enrutador CPE debe ser asignada en forma fija a la VRF correspondiente a la Red Privada Virtual del cliente en la red MPLS. Para el enrutador CPE en el sitio del cliente es transparente esta asignación. Sobre el enlace entre el enrutador CPE y el enrutador PE se realiza el intercambio de la información de enrutamiento, la cual solo se vera reflejada en la VRF que corresponda a la Red Privada Virtual del cliente conectado.

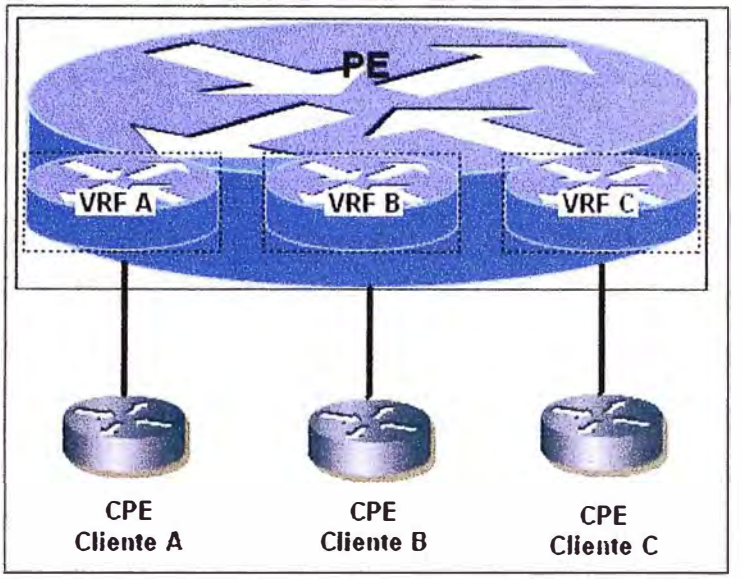

Figura 2.4 Enrutador Virtual

2.1.2 Enrutamiento en MPLS-VPN

El proveedor de servicios mantiene información del enrutamiento, es decir un conocimiento total de todos los sitios de la Red Privada Virtual, de manera ágil y dinámica, se le informa a los enrutadores CPEs mediante distintas alternativas como BGP, RIP, OSPF, etc. De esta manera la carga administrativa y compleja que implica el control de enrutamiento en el lado del cliente se transforma en algo sencillo, preciso y eficiente. Podemos dividir el enrutamiento correspondiente a la MPLS/VPN en enrutamiento PE – PE y enrutamiento PE – CPE.

a) Enrutamiento PE - CPE

El intercambio de información de enrutamiento entre los enrutadores CPE y PE puede realizarse utilizando distintos protocolos de enrutamiento, los cuales sirven para poblar la tabla de enrutamiento en el enrutador CPE y la VRF en el PE con la información de los prefijos de red de todos los sitios del cliente, estos protocolos pueden ser:

- RIP v2
- OSPF
- EIGRP
- BGP
- Rutas estáticas

b) Enrutamiento PE - PE

Normalmente una MPLS-VPN interconecta múltiples sitios conectados a diferentes PE en la red del proveedor, esta condición obliga a que los PE tengan que intercambiar entre sí

información de enrutamiento relacionada a cada una de las VPN. El intercambio de esta información se logra mediante la integración de varios protocolos de enrutamiento en la red del proveedor. Estos protocolos son:

- Un IGP como OSPF para anunciar las rutas internas.
- MPLS-IP Unicast para la creación de la malla LSP interna.
- BGP para el establecimiento de sesiones IBGP entre todos los PE de la red.
- MP-BGP para el intercambio de la información de enrutamiento de cada una de las Redes Privadas Virtuales.

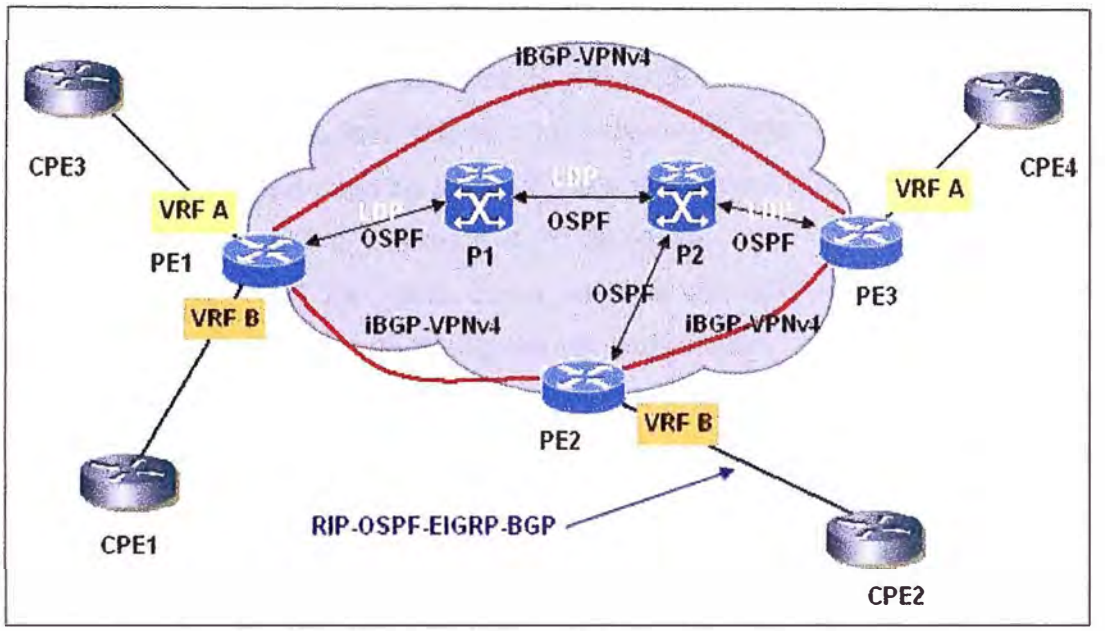

Figura 2.5 Enrutamiento en MPLS-VPN

Además se agregan un par de elementos a la información de enrutamiento que permiten un transporte confiable y aislado de las rutas del cliente, estos elementos son:

- RD (*Route Distinguisher*). La facilidad de manejar el mismo plan de numeración en varias VPN y el utilizar un solo protocolo para el intercambio de la información de enrutamiento (MP-BGP) implicaría una confusión en los procesos de enrutamiento. Para solucionar este problema es utilizado el distintivo de ruta (Route Distinguisher) el cual es añadido a cada uno de los prefijos de red aumentando la longitud del prefijo de 32 a 96 bytes, obviamente el RD debe ser diferente para cada VRF. MP-BGP tiene las condiciones para transportar información de rutas de esta longitud.
- RT (*Route Target*). Es un indicador que se anexa a las rutas correspondientes a una VPN. Este indicador se transporta junto con la información de ruta utilizando MP-BGP y es idéntico para todas las rutas anunciadas desde una VRF. La

información de rutas acompañada por el RT es transportada a través de las sesiones MP-BGP y llega a todos los PE, y entonces aquellos PE que incluyan sitios de la VPN del cliente importarán la información basados en el RT y la incluirán en la VRF correspondiente.

2.1.3 Transporte en MPLS-VPN

El transporte de paquetes en la red MPLS/VPN esta basado en etiquetas y prefijos vpnv4.

a) Etiquetado de paquetes IP

Una vez que la información de enrutamiento se distribuyó apropiadamente en las correspondientes VRF de todos los PEs, la red está casi lista para el transporte de los paquetes IP del cliente, solo falta aclarar un par de conceptos:

- Cómo etiquetar un paquete en el PE de entrada para que este sea transportado a través de la red MPLS y alcance el PE de salida.
- Una vez en el PE de salida cómo saber a que VRF el paquete tiene que ser reenviado para entregarlo al sitio del cliente correcto.

b) Pila de etiquetas

Para poder transportar un paquete IP a través de la VPN es necesario etiquetarlo con un par de etiquetas. La etiqueta exterior sirve para trasladar el paquete a través del dominio MPLS y llevarlo desde el PE de ingreso hasta el PE de salida y la etiqueta interior marcada con el bit S (*bottom-of-stack*) es utilizada para indicar a que VPN pertenece el paquete.

- Etiqueta exterior. La etiqueta exterior se genera de acuerdo a los procedimientos vistos en el capítulo anterior, cada enrutador PE posee una dirección que lo identifica en las sesiones IBGP, para estas direcciones la red MPLS genera una malla LSP que permite alcanzarlas mediante conmutación de etiquetas. Solo es necesario establecer trayectorias hacia las direcciones de los PE, no hacia las rutas o prefijos de los clientes VPN, esto debido a que para cualquier ruta anunciada mediante BGP la dirección de próximo salto corresponde a la dirección del PE que anunció está ruta y ya que los paquetes finalmente se dirigen del PE de ingreso al PE de egreso, con esta etiqueta es suficiente para alcanzarlos. Los enrutadores interiores P no necesitan tener información de las rutas de los clientes VPN, solo de las rutas internas, para la generación de las LSP. Los paquetes de los clientes VPN se conmutan a través de los enrutadores P mediante la etiqueta exterior.

- Etiqueta interior: Cada PE asigna una etiqueta a cada una de las rutas en la VRF asociada a la Red Privada Virtual del cliente. Estas etiquetas son propagadas junto con las correspondientes rutas a través de las sesiones MP-BGP hacia el resto de los PE. Cuando un enrutador PE recibe las actualizaciones de enrutamiento MP-BGP, toma la información de las rutas VPN y su etiqueta y las instala en la VRF asignada (de acuerdo al RT).

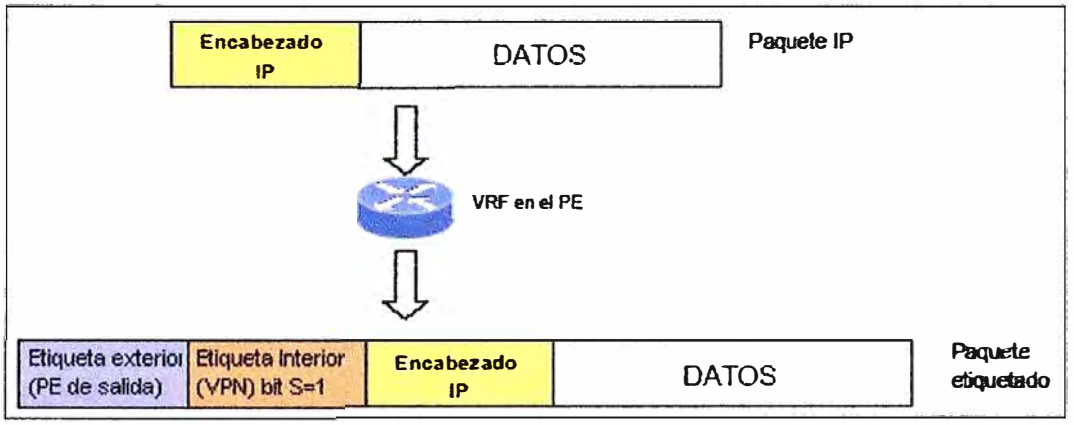

Figura 2.6 Pila de etiquetas

c) Transporte de paquete IP por VPN

El transporte de un paquete IP a través de la Red Privada Virtual del cliente se realiza de acuerdo a los siguientes puntos:

- El paquete es enviado desde el enrutador CPE en el sitio del cliente con los encabezados IP tradicionales.
- Al ingresar al enrutador PE el paquete es analizado en la VRF asociada, en donde se determina la dirección de próximo salto asociada al prefijo de la red de destino. La dirección de próximo salto corresponde a la dirección del enrutador PE que originalmente anunció este prefijo de red.
- Al paquete se le adhiere la pila de etiquetas para su traslado a través de la red
- El paquete etiquetado se envía al siguiente enrutador P en donde se realiza la función SWAP con la etiqueta exterior enviando el paquete al siguiente enrutador P especificado en la trayectoria LSP.
- En el último enrutador P de la trayectoria LSP, la etiqueta exterior P es eliminada (PHP) y el paquete es enviado al enrutador PE de salida solo con la etiqueta que identifica a la Red Privada Virtual.
- En el enrutador PE la etiqueta que acompaña al paquete es analizada y removida, entonces el paquete es entregado a la VRF que esta asociada a la Red Privada Virtual del cliente.

- En la VRF el paquete IP se analiza y es enviado con los encabezados IP originales, por la interfaz que enlaza al PE con el CPE en el sitio del cliente.

Para el cliente, la red MPLS-VPN es totalmente transparente, el enrutador CPE envía paquetes IP y recibe paquetes IP. Además esto se realiza en forma segura y aislada de los demás clientes.

2.2 Calidad de Servicio en MPLS

En la actualidad, el protocolo IP es el dominante en la mayoría de las redes. Desde su creación, su filosofía sin conexión y con envío de tráfico de naturaleza *best effort* ha dado muy buenos resultados y, por lo tanto, contribuido a su expansión. Sin embargo, las nuevas aplicaciones que han ido surgiendo en los últimos años requieren más de lo que la actual tecnología IP puede proporcionar: altos requerimientos de ancho de banda, necesidad de transmisión con bajo retardo o sin pérdidas, etc. Para responder a estos requerimientos se han desarrollado varias formas de dotar a las redes IP de QoS (*Quality of Service*). El IETF ha propuesto diversas tecnologías:

- *Arquitectura IntServ.* Internet de Servicios Integrados, basado en la utilización de algún protocolo de reserva (RSVP) que permite la reserva de recursos a lo largo de los enrutadores implicados en la comunicación, sin embargo el principal problema de este modelo es la necesidad de mantener información sobre cada flujo en todos los enrutadores de la red, lo cual lleva a problemas de escalabilidad.
- *Arquitectura DiffServ.* Internet de Servicios Diferenciados, es una de las propuestas más importantes, se basa en la división del tráfico en diferentes clases, y en la asignación de prioridades a estos agregados, mediante el campo de 8 bits DSCP-DiffServ Code Point (campo ToS-Type of Service en IPv4 y Clase de Tráfico en IPv6). En función de este campo, cada nodo intermedio tratará el paquete de la forma adecuada. A este comportamiento se le denomina PHB (*Per Hop Behaviour*), implementado mediante diferentes algoritmos de colas como PQ (*Priority Queuing*), WPQ (*Weighted Priority Queuing*) o WRR (*Weighted Round Robin*) entre otros.

La arquitectura MPLS no aporta específicamente, mecanismos para soportar calidad de servicio de forma explicita, por lo que se apoya en las arquitecturas antes mencionadas IntServ y DiffServ para brindar calidad de Servicio.

La integración de DiffServ sobre MPLS es en la actualidad la solución mas apropiada para mejorar la calidad en las redes IP, definida en el RFC 3270. Mediante la integración

de los modelos *MPLS/DiffServ* obtenemos una nueva arquitectura en la que MPLS se sitúa en el nivel de red-enlace, proporcionando un método de envío rápido por su conmutación de etiquetas y sus caminos LSP (*Label Switched Path*), así mismo sirve para evitar la congestión de la red, aportando sus características de ingeniería de tráfico. Mientras, DiffServ asegura unos ciertos parámetros de calidad de servicio realizando la diferenciación y priorización del tráfico necesario para dotar a IP de QoS. Por último, la incorporación a esta arquitectura de un elemento gestor del dominio aportará ventajas como ingeniería de tráfico, optimización de recursos y control del uso de los recursos.
La aplicación de mecanismos de ingeniería de tráfico y de diferenciación de servicios no resulta suficiente para la provisión de garantías QoS si no se evita que la red llegue a una situación de sobre utilización de sus recursos, inevitablemente provocando congestión.

2.2.1 Arquitectura de Servicios Diferenciados

La arquitectura DifServ se basa en dividir el tráfico en clases, controlar la cantidad de tráfico que cada cliente envía a la red de cada clase de tráfico y asegurar requerimientos de QoS utilizando en cada enlace políticas de scheduling y dropping.
En este modelo se establecen acuerdos con el cliente SLA (*Service Level Agreements*), en el cual entre otras cosas se le garantizan para ciertas clases de tráfico ciertas garantías de QoS siempre que el cliente envié el tráfico dentro de un cierto perfil (normalmente definido por valores de media, pico y tamaño máximo de burst).
Como mencionamos el tráfico es separado en clases en el ingreso a la red y marcado para registrar la clase a la que pertenece. Esa marca llamada DSCP (*Differentiated Service Code Point*) usa 6 bits para distinguir una clase de otra. Estos seis bits se registran en el campo TOS (*Type of Service*) en la cabecera de IPv4 o en el campo Clase de Tráfico de IPv6. A cada DSCP le correspondería luego un tratamiento especifico en cada nodo de la red. Este tratamiento específico que se le brinda a cada clase de tráfico se llama en DiffServ PHB (*Per Hop Behavior*). El DSCP es seteado en la frontera de la red y en los enrutadores internos es examinado para asociarlo con el PHB correspondiente. En este sentido la mayor complejidad residiría en los nodos de la frontera, aunque en los nodos interiores habría que configurar políticas de scheduling y dropping que pueden ser complejas.
Existen dos componentes principales en esta arquitectura:

1. El clasificador, que selecciona paquetes de acuerdo a ciertos criterios y los redirecciona en base a esta selección.
2. El acondicionador de tráfico, que de acuerdo al SLA y en particular al perfil de tráfico acordado, acondiciona el tráfico que ingresa de cada clase.

En la figura 2.7 podemos observar los componentes de la arquitectura de Servicios Diferenciados. La clasificación puede ser de dos tipos: MF (MultiField), es decir que analizando diferentes campos del paquete se define la clase a la que pertenece el paquete o simplemente basado en el campo DSCP si el paquete ya venia marcado. El paquete en este modelo puede venir marcado desde el cliente (sea este un usuario final u otro proveedor de servicios).

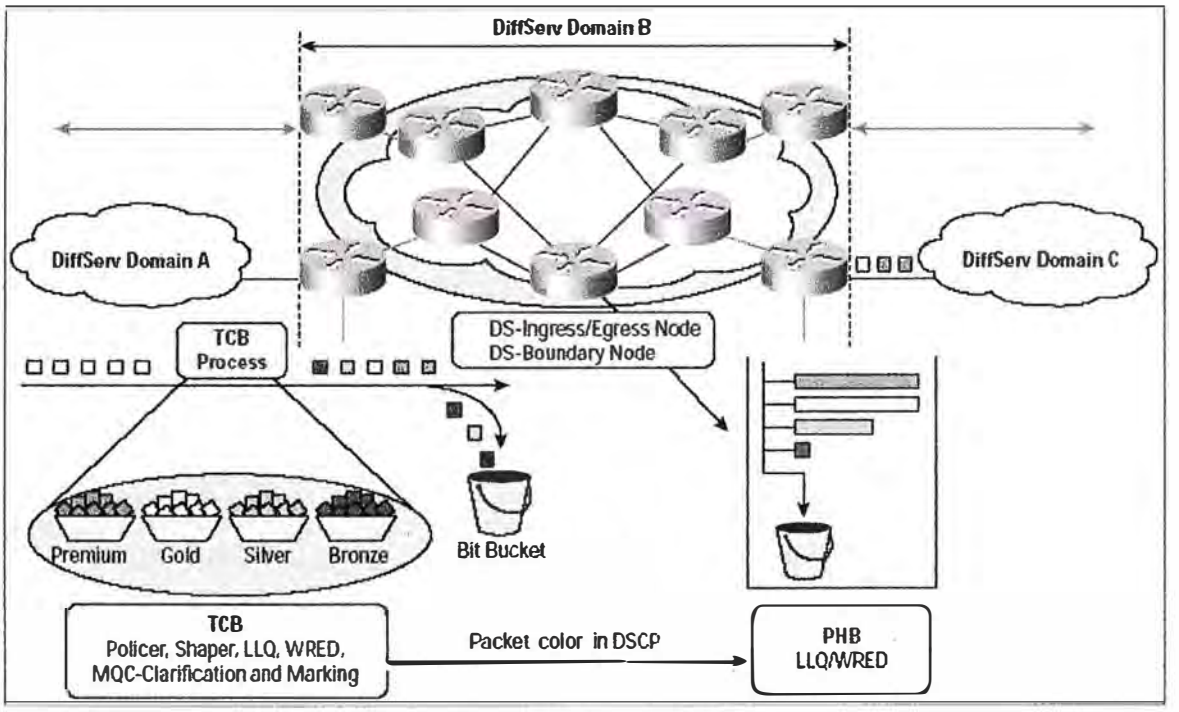

Figura 2.7 Arquitectura DiffServ

La función de acondicionamiento del tráfico clasifica los paquetes en In-profile o Out-profile. In-profile puede ser mandado sin ningún otro procesamiento. Los Out-profile podrían ser re-acondicionados, re-marcados (en alguna clase más baja por ejemplo) o descartados. Esto dependería del acuerdo establecido con el cliente.

Los componentes básicos del acondicionador son:

- Meter: realiza mediciones temporales del conjunto de paquetes seleccionados por el clasificador contra el TCA (Traffic conditioning agreement).
- Marker: Setea el campo DS de la cabecera IP con un código particular y lo asocia así a una clase particular.
- Shaper: retarda algunos o todos los paquetes para que cumplan con el traffic profile.
- Dropper: descarta algunos o todos los paquetes para que cumplan con el traffic profile.

En un nodo interior se examina el DSCP y se define el PHB que debe darse al paquete. El PHB esta definido como una descripción del comportamiento de reenvió observado exteriormente. Esto quiere decir que en un PHB se especifica como debe observarse como caja negra el tratamiento que reciben los paquetes de esa clase. La implementación de un PHB puede ser hecha por diferentes mecanismos. En general los mecanismos usados actualmente para implementar un PHB son mediante políticas de scheduling para reservar ancho de banda y dropping como RED (Random Early Detection) o RIO (Red In-profile out-profile).

Los PHBs pueden ser definidos individualmente o como grupo. Un grupo PHB contendría en general una restricción común como por ejemplo un algoritmo de scheduling común. Un nodo DiffServ puede soportar múltiples y simultáneos grupos de PHBs. Los recursos serían compartidos entre los grupos de acuerdo a la política de servicios ofrecidos.

Se han definido varios PHB entre ellos:

- Best Effort. Con un tratamiento similar al de Internet actualmente.
- Expedited Forwarding (EF), RFC 2598. El rate mínimo de salida asegurado en todo router al agregado de paquetes EF, debería ser mayor que el rate máximo de entrada. Para su implementación: se requieren colas con prioridades o WFQ (Weight Fair Queueing), etc. El objetivo es que el flujo agregado vea siempre (o casi) la cola vacía.
- Assured Forwarding (AF), RFC 2597. Se definen 4 clases independientes con 3 niveles de descarte dentro de cada clase, valores que se observan en la tabla 2.1. A cada clase se le debe asignar una cantidad mínima de recursos y puede obtener más si hay exceso. Dentro de una clase: La probabilidad de un paquete de ser enviado no puede menor si tiene un nivel de descarte menor. Debe responder a condiciones de congestión a largo plazo. Los mecanismos comúnmente usados para su implementación son un Scheduler para reservar recursos y mecanismos de gestión de buffer para manejar niveles de precedencia de descarte.

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low	(AF11) 001010	(AF21) 010010	(AF31) 011010	(AF41) 100010
Médium	(AF12) 001100	(AF22) 010100	(AF32) 011100	(AF42) 100100
High	(AF13) 001110	(AF23) 010110	(AF33) 011110	(AF43) 100110

Tabla 2.1 Assured Forwarding

El PHB especifica cual seria el comportamiento que recibiría una clase al atravesar un nodo de la red, pero no dice nada sobre cual seria el comportamiento observado de punta a punta de la red. Para esto se define el concepto de PDB (Per Domain Behavior). El concepto de PDB se define en el RFC 3086. La idea es usar PHBs, clasificadores y acondicionadores para componer agregados de trafico que experimenten un tratamiento especificado cuando transiten por un dominio DiffServ. Especifica métricas para cuantificar el tratamiento que un agregado con un DSCP recibiría al atravesar el dominio.

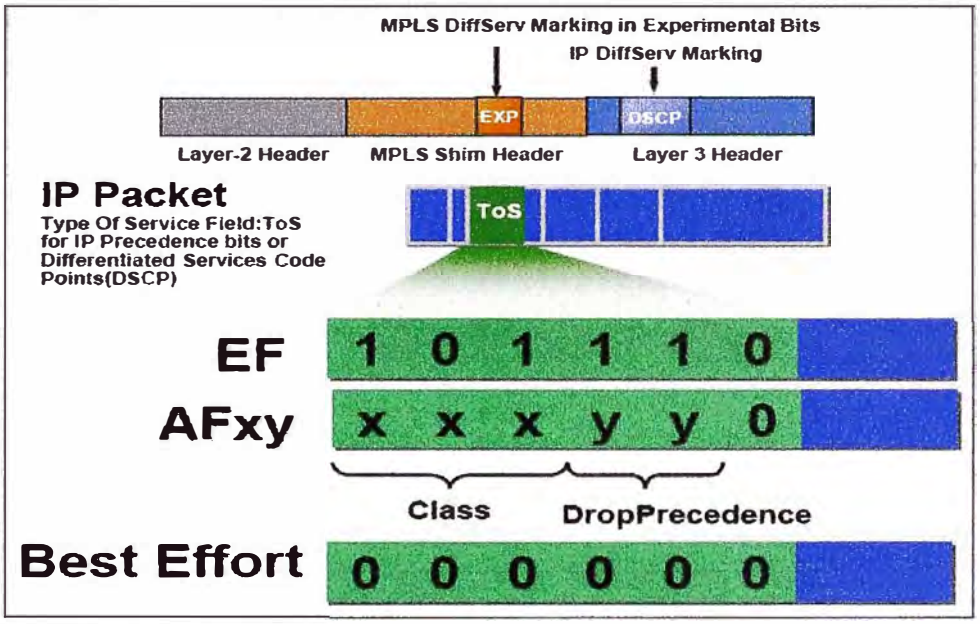

Figura 2.8 Clasificación de tráfico

2.2.2 Implementación de MPLS/DiffServ

En la red MPLS cada LSP puede estar asociado a varios FEC (*Forward Equivalence Class*), y pueden asignarse tantos flujos de información a cada FEC como sea necesario. Esto conlleva que, a efectos prácticos, pueda elegirse qué tráfico va a ser encaminado por qué LSP concreto, pudiendo implicar éste solo hecho la alteración de la calidad de servicio ofertada.

La RFC 3270 describe los mecanismo para el soporte MPLS/DiffServ. El primer desafió para el soporte de DiffServ en una red MPLS es que los LSRs toman la decisión de reenvió basados en la cabecera Shim de MPLS, no eximan la cabecera IP donde se transporta el DSCP. Para resolver este problema el IETF asigna los 3 bits del campo experimental (EXP) de la cabecera MPLS para transportar la información de DiffServ en MPLS. Esta solución resuelve el problema inicial de transportar el PHB en la cabecera MPLS, pero introduce un nuevo problema: como mapear los valores de 6 bits del campo

DSCP que puede tener hasta 64 valores, dentro del campo EXP de 3 bits que puede portar hasta 8 distintas clases de servicio. Se tienen dos soluciones para este problema:

- La primera solución aplica a redes que soportan hasta menos de 8 PHBs. Aquí, el mapeo es sencillo: un DSCP particular es equivalente a un EXP y mapea hacia un particular PHB (scheduling and drop priority). Durante el reenvió, la etiqueta determina donde reenviar el paquete, y los bits del EXP determinan el PHB. Los bits del EXP pueden ser seteados de acuerdo a los bits DSCP de los paquetes IP transportados en el LSP, o ellos pueden ser seteados por el administrador de la red. Este método es llamado EXP-Inferred-PSC LSP (E-LSP). E-LSPs pueden llevar paquetes con hasta ocho distintos PHB en un simple LSP. Figura 2.9.

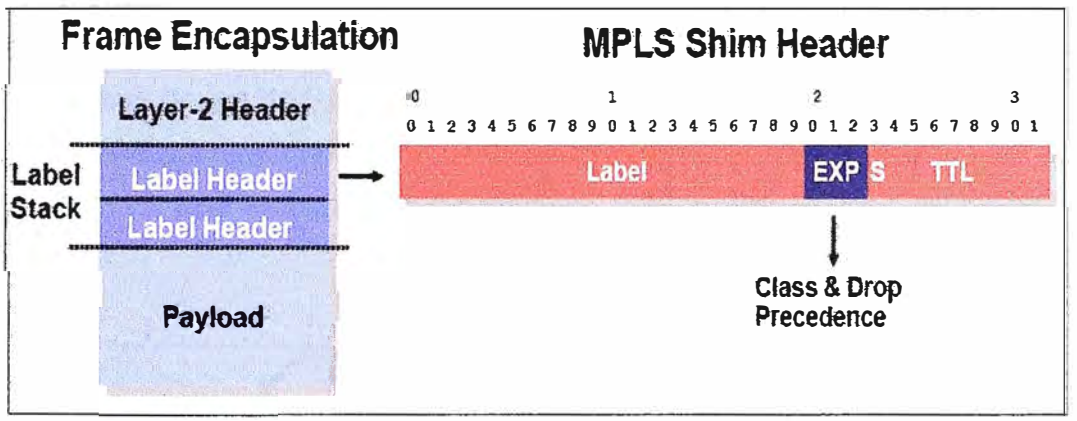

Figura 2.9 EXP-Inferred-PSC LSP (E-LSP)

- La segunda aplica a redes que soportan más de 8 PHBs. Aquí los bits EXP no puede llevar toda la información necesaria para distinguir entre PHBs. El único otro campo en la cabecera MPLS que puede ser usado para este propósito es la misma etiqueta. Durante el reenvió, la etiqueta determina donde reenviar el paquete y que comportamiento se aplicará a este, los bits del campo EXP transporta información con respecto a la prioridad de descarte asignada al paquete. Así, el PHB es determinado por ambos valores, la etiqueta y los bits EXP. La etiqueta esta implícitamente amarrada con el PHB, esta información necesita ser transportada cuando se señaliza el LSP. Los LSP que usan la etiqueta para transportar el PHB deseado son llamados L-LSPs (Label-Only-Inferred-PSC LSP). Los L-LSPs pueden llevar paquetes desde un simple PHB, o desde varios PHBs que tienen el mismo régimen de comportamiento pero diferente prioridades de descarte (Como AFxy donde x es constante y y es no constante). El modelo explicado se observa en la figura 2.10.

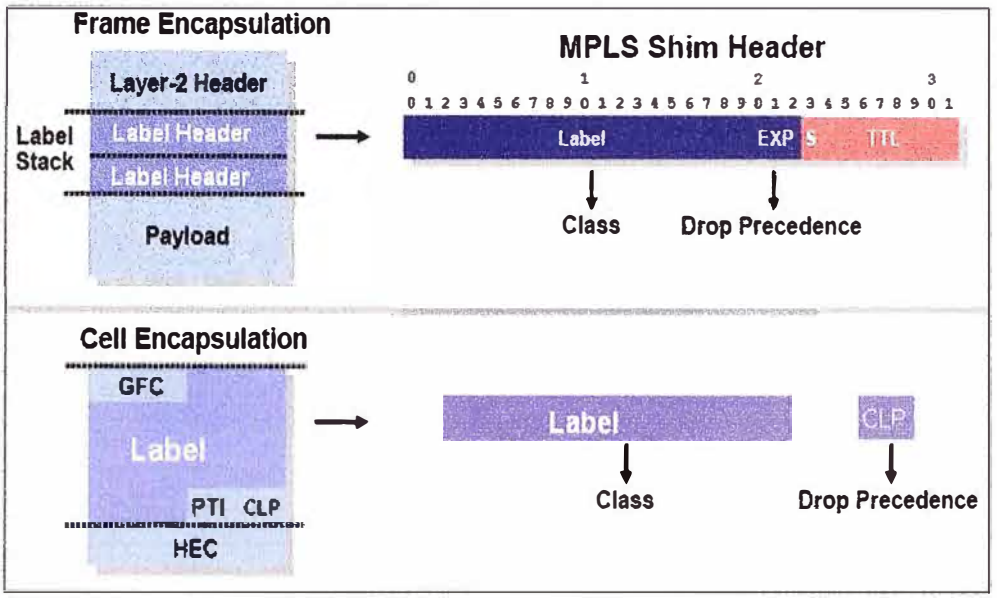

Figura 2.10 Label-Only-Inferred-PSC LSP (L-LSP)

2.2.3 Estructura de los nodos

La estructura básica de un nodo en la nueva arquitectura MPLS/DiffServ que se muestra be la figura 2.11, esta formada por los módulos DiffServ Pre-Routing, MPLS y DiffServ Post-Routing.

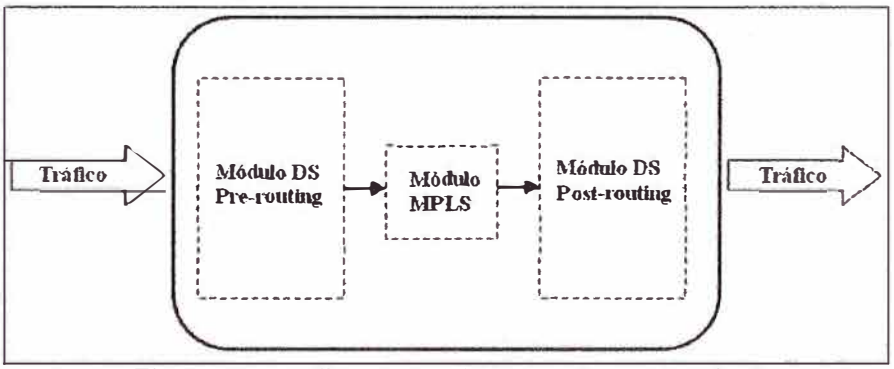

Figura 2.11 Esquema de un nodo a alto nivel

a) Módulo DiffServ Pre-routing

El módulo pre-routing clasifica los paquetes, los marca y realiza las correspondientes funciones de acondicionado del tráfico si se trata de un LER (*Label Edge Router*). Este módulo sólo se encuentra en los enrutadores LERs. La figura 2.12 muestra el módulo de *pre-routing*, donde pueden distinguirse los distintos componentes funcionales de este módulo, así como las tablas de información y estado (perfiles y PHB) que usa. El cuadro punteado corresponde al módulo siguiente, el módulo MPLS a donde son reenviados todos los paquetes para la siguiente fase del proceso.

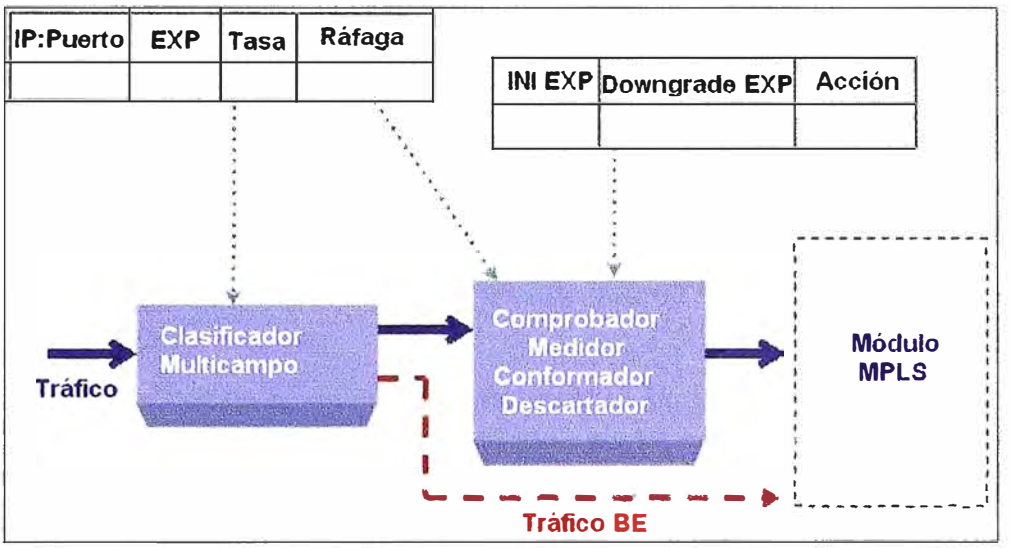

Figura 2.12 Módulo de pre-rounting en detalle

b) Módulo MPLS

El módulo MPLS realiza las funciones de enrutamiento propias de MPLS, etiquetando previamente el paquete si se trata de un enrutador LER. En este bloque se traduce directamente el campo DSCP (*DiffServ CodePoint*) de la cabecera IP al campo EXP de la cabecera MPLS. Además se realizan las tareas propias de enrutamiento de MPLS que harán que un paquete se inserte en un determinado módulo DiffServ *post-routing* u otro dependiendo de su interfaz de salida.

c) Módulo DiffServ *Post-routing*

El módulo MPLS dirige los paquetes a su interfaz de salida correspondiente. En cada interfaz se encuentra este módulo DS (figura 2.13), que primero realiza una clasificación por agregados de comportamiento (clasificador EXP) e inserta el paquete en la sub-cola adecuada, que se gestionan mediante un planificador DWRR (*Deficit Weighted Round Robin*).

Con respecto a la elección del algoritmo de planificación de colas, el principal requerimiento a la hora de elegirlo para la arquitectura de servicios diferenciados es que sea capaz de discriminar distintos tipos de tráfico. La política propuesta es DWRR, debido a que considera los flujos de paquetes de longitud variable, su complejidad algorítmica es baja, protege a los flujos dentro de una clase de otros flujos con mal comportamiento que puedan existir en el resto de las clases y actualmente se encuentra implementado en multitud de enrutadores reales.

En cuanto al tipo de colas que se van a usar, todas serán de tipo FIFO, aunque se utilizarán las siguientes políticas de descarte para cada cola:

- Para la cola EF se utilizará una política simple de *Tail Drop*. Creemos que sería suficiente ya que dado que es el servicio que a priori, será el más minoritario y su prioridad es la mayor, no se esperan situaciones de congestión.
- Las colas AF serán reguladas mediante el algoritmo WRED (*Weighted Random Early Detection*) para proporcionar un mecanismo de descarte RED (*Random Early Detection*) en base a los diferentes sub-servicios AF con sus diferentes precedencias de descarte.
- Por último, el tráfico BE se regulará mediante el Algoritmo de red.

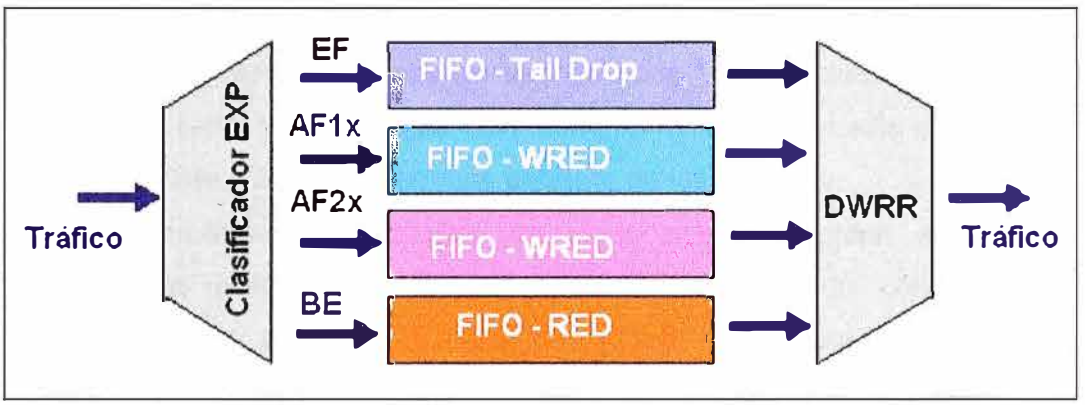

Figura 2.13 Módulo de post-routing en detalle

2.3 Ingeniería de tráfico en MPLS

La ingeniería de tráfico es el proceso que mejora la utilización de la red mediante la distribución del tráfico en ella de acuerdo con la disponibilidad de los recursos, el tráfico actual y el esperado. Como resultado, tenemos que se evita la congestión en cualquier camino. El hecho de hablar de mejora de la utilización de la red no implica necesariamente que se obtenga el mejor camino, pero sí el mejor camino para un determinado tipo de tráfico.

MPLS facilita la asignación de recursos en las redes para balancear la carga dependiendo de la demanda y proporciona diferentes niveles de soporte dependiendo de las demandas de tráfico de los usuarios. El protocolo IP provee una forma primitiva de Ingeniería de tráfico al igual que el protocolo del OSPF que permite a los enrutadores cambiar la ruta de los paquetes cuando sea necesario para balancear la carga. Sin embargo esto no es suficiente ya que este tipo de enrutamiento dinámico puede llevar a congestionar la red.

Todo tráfico entre dos puntos finales sigue la misma ruta y puede ser cambiada si ocurriera congestión, sin embargo este cambio solo ocurre cuando hay congestión que es

algo que siempre se trata de evitar. En MPLS a diferencia de OSPF no se ve paquete por paquete si no flujos de paquetes con su respectivo QoS y demanda tráfico predecible. Con este protocolo es posible predecir rutas en base a flujos individuales, pudiendo haber diferentes enrutadores.

Si llegase a presentarse un problema de congestión en la red MPLS, las rutas MPLS pueden ser re-enrutadas inteligentemente de esta manera se pueden cambiar las rutas de flujo de paquetes dinámicamente conforme a las demandas de tráfico de cada flujo.

Entre los principales beneficios de MPLS-TE tenemos:

- El administrador de la red puede establecer rutas específicas por LSRs concretos.
- Permite obtener estadísticas de uso de cada LSP en detalle, es decir, cuánto tráfico se cursa y de qué tipo. Con esta información, se puede re-planificar la red de forma que ofrezca un uso más eficiente de los recursos.
- Hacer enrutamiento restringido de modo que se pueden seleccionar rutas específicas para transportar el tráfico de un tipo en concreto con unos requerimientos específicos. Esta posibilidad está directamente ligada a los Acuerdos de Nivel de Servicio que un proveedor acuerde con el cliente, al que puede facturar así de un modo mucho más flexible y adaptable a sus necesidades.
- Se puede aplicar directamente sobre una red IP, independientemente de la infraestructura que le de soporte (ATM, Frame-Relay, PPP, etc) con un mayor nivel de detalle, de forma más sencilla y eficiente.

El RFC 2702, MPLS Traffic Engineering (TE) establece que la ingeniería de trafico concierne a la optimización del desempeño de una red MPLS e involucra diversas áreas, mediciones de tráfico, modelado de tráfico y redes, control de tráfico en Internet y evaluación de desempeño.

Se establece que los principales objetivos de MPLS-TE son:

- Mover el tráfico del camino establecido por el IGP (Interior Gateway Protocol) a un camino menos congestionado.
- Utilizar el exceso de ancho de banda sobre los enlaces sud-utilizados.
- Maximizar la utilización de los enlaces y nodos de la red.
- Aumentar la confiabilidad del servicio.
- Alcanzar requerimientos impuestos.

Así mismo se mencionan los siguientes requerimientos:

- Orientados al tráfico: pérdidas de paquetes, retardos, etc.
- Orientados a los recursos: fundamentalmente utilización de la capacidad de la red

La implementación de acciones de control en MPLS-TE puede involucrar:

- Modificación de los parámetros de Gestión de Tráfico,
- Modificación de los parámetros asociados al enrutamiento, y
- Modificación de los parámetros y atributos asociados con los recursos.

El RFC 2702 establece que MPLS-TE tiene que resolver 3 problemas fundamentales:

- Cómo mapear paquetes en FECs.
- Cómo mapear FECs en troncales de tráfico.
- Cómo mapear troncales de tráfico en la topología de red física a través de LSPs.

2.3.1. Enrutamiento Explicito

La principal característica de MPLS que permite realizar Ingeniería de tráfico es el enrutamiento explicito. Una ruta explicita es una secuencia de nodos lógicos entre un nodo de ingreso y uno de egreso que se definen y establecen desde un nodo de la frontera. Una ruta explicita puede ser una lista de direcciones IP. También pueden especificarse los primeros N saltos solamente y luego la ruta definida por el protocolo de enrutamiento IP. Puede usarse también en una ruta explicita el concepto de Nodo Abstracto: Colección de nodos presentados como un solo paso en una ruta explicita. Un ejemplo de nodo abstracto puede ser un Sistema Autónomo.

Si el nodo ingreso quiere establecer una ruta que no sigue el camino que sigue por defecto el protocolo de enrutamiento IP, debe utilizar un protocolo de distribución de etiquetas que soporte la definición de rutas explicitas. Existen dos definidos por el IETF: CR-LDP y RSVP.

La ruta LSP puede ser restringida por la capacidad de recursos y la capacidad de los nodos de cumplir con los requerimientos de QoS. Esto lleva al concepto de ruta con restricciones. Una ruta con restricciones es una ruta que se obtiene imponiendo un conjunto de restricciones que se deben cumplir. Por ejemplo: información de QoS del enlace (ancho de banda disponible, retardo, etc.), clases, prioridades, etc.

EL LER de ingreso calcula una ruta que satisfaga un conjunto de restricciones en el estado actual de la red.

Para encontrar una ruta con restricciones se debe correr un algoritmo de enrutamiento basado en restricciones (Constrain-Based Routing).
En el RFC 2702 se establece que para realizar TE una red MPLS y particularmente CBR debe ser posible definir:
a) Atributos asociados a las troncales de tráfico que en conjunto especifican su comportamiento. Dentro de estos atributos se encuentran:

- Parámetros del tráfico de la troncal. Características del tráfico que utilizara esa troncal.
- Atributos para el establecimiento y mantenimiento de caminos establecidos administrativamente.
- Reglas para establecer preferencias de ciertos caminos que pueden ser mandatarios o no. Se considera adecuado tener atributos que establezcan una jerarquía o preferencia para mapear una troncal dentro de un conjunto de posibles caminos.
- Clase de afinidad con recursos. Se recomienda contar con atributos que permitan establecer clases de afinidad entre los recursos y las troncales de forma de establecer caminos para las troncales usando aquellos recursos que le son afines.
- Adaptabilidad a cambios. Debe poder especificarse si ante cambios en el estado de la red se re-calculan o no los caminos establecidos para la troncal.
- Prioridad de las troncales a la hora de establecer y de mantener un LSP.
- Atributos asociados al re-enrutamiento. Se debe poder decidir ante cambios en la red, si una troncal se re-enrutará solo si hay caminos con recursos suficientes o si se re-enrutará siempre.
- Atributos de Policing para definir que acciones se toman si la troncal no cumple con los parámetros de tráfico que se especificaron.

b) Atributos asociados a los recursos. En este punto se establecen básicamente dos atributos que son:

- Maximun Allocation Multiplier Máximo ancho de banda que se permite reservar para los caminos que atraviesan dicho enlace.
- Clases de recursos. Afinidad que restringe el mapeo de las troncales sobre los recursos.

c) Enrutamiento basado en restricciones para realizar el mapeo. Este algoritmo tendrá en cuenta: Atributos asociados con las troncales de tráfico, atributos asociados con los recursos e información del estado de la red.

2.3.2 Enrutamiento basado en restricciones

El enrutamiento restringido o CBR (Constraint-based Routing) permite seleccionar rutas específicas para transportar el tráfico de un tipo concreto con unos requerimientos específicos, como por ejemplo, garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

El mecanismo basado en restricciones selecciona la mejor ruta que obedece a las restricciones establecidas de manera a reducir el coste y balancear la carga en la red. Esas restricciones son impuestas, por un lado, por políticas de enrutamiento, que administran, gestionan y controlan el acceso a los recursos de red, y por otro lado, por requisitos de calidad de servicio, dado por el uso del ancho de banda, retrasos, jitter y las pérdidas de paquetes.

Sin embargo, el CBR necesita habilitar un modelo capaz de identificar los caminos menos congestionados, las mejores rutas y el balanceo de carga en la red.

En el enrutamiento basado en restricciones no se reservan recursos apenas se calcula la ruta. Para ello es necesario conocer la disponibilidad de recursos de red para establecer las restricciones en el uso de los mismos. Normalmente se consideran algoritmos IGP con la extensión TE para enrutar la demanda sobre la red.

2.3.3 Balanceo de carga

Una herramienta potente de MPLS-TE es que permite realizar el balanceo de carga entre diferentes LSPs. Esta herramienta brinda la posibilidad de enrutar troncales cuyo tráfico es superior a las posibilidades de un único camino en la red, y permite también mejorar el uso de recursos de la red.

Para realizar el balanceo de carga se deben tener en cuenta dos aspectos. El primero es el algoritmo con el cual se decide los coeficientes de balanceo de carga entre los LSPs. El segundo es el mecanismo (una vez fijados los coeficientes) que se utiliza para asignar los paquetes a uno u otro LSP.

La distribución de la carga entre LSPs se puede realizar por paquete o por flujo.

2.3.4 Métricas IGP con extensión TE.

Una de las ventajas de ingeniería de tráfico MPLS es que se evita inundaciones innecesarias para informar el estado de la red a los enrutadores practicado por la métrica IGP tradicional. En MPLS TE informa a los enrutadores del estado de la red cuando el ancho de banda de los enlaces sufre alguna mudanza debido al tráfico cursado. El proceso de inundación que informa del estado de la red a los enrutadores actúa

considerando tres estados distintos de la red: cuando hay un cambio significativo de estado, en la actualización de forma periódica y si antes de una actualización del estado de la red ocurre un error grave.

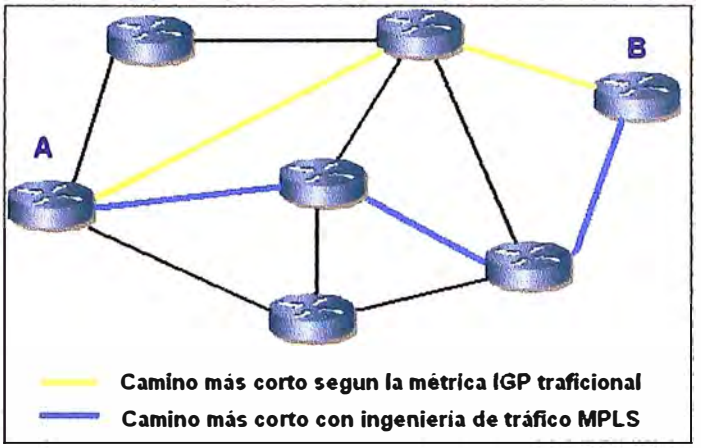

Figura 2.14 Comparación entre camino más corto IGP con ingeniaría de tráfico

La extensión de los protocolos IGP proporciona al encaminamiento la capacidad de transporte de recursos e información de la política practicada por la red. Los datos que son constantemente recolectados son utilizados para mantener la base de datos con la información del estado de los enlaces y la utilización de recursos.

a) OSPF TE

La extensión del protocolo OSPF fue propuesta por el IETF para describir la topología de la ingeniería de tráfico, considerando el ancho de banda, la administración de restricciones y la distribución de la información dentro de un área OSPF. Según la RFC 3630 la información por esa extensión puede ser utilizada para crear una base de datos con información de estado de los enlaces con atributos adicionales de ingeniería de tráfico. El uso de esta base de datos incluye:

- Control de los atributos adicionales (extendido),
- Enrutamiento de demandas basado en restricciones locales,
- Ingeniería de tráfico global.

Sin embargo, el OSPF TE posee algunas limitaciones, como por ejemplo, los procedimientos y extensiones propuestas no consideran métodos para distribución entre redes de diferentes áreas, con lo cual la información de ingeniería de tráfico se limita a un entorno intra-red. Otro aspecto que no está siendo abordado es el estado multiacceso, es

decir, enlaces duplicados, un procedimiento normalmente utilizado en la planificación y dimensionamiento de redes de paquetes. Por fin, dicho protocolo no soporta enlaces no enumerados o que no posee direcciones IP, la señalización actualmente usada en MPLS TE no provee soporte a este tipo de enlace porque no existe un identificador en caso de establecimiento de rutas explicitas.

b) IS-IS TE

La extensión del protocolo IS-IS fue propuesta por el IETF con el objetivo principal de añadir más información sobre las características del enlace a un LSP del tipo IS-IS. El segundo objetivo de esta extensión incluye el incremento del alcance dinámico de la métrica IS-IS y la creación de una codificación de prefijos IP. La idea es utilizar un código para los enrutadores (router id) de manera que le mismo pueda ser utilizado como una referencia única para la ingeniería de tráfico.

Para lograr sus objetivos dos nuevos tipos de TLV (Table, Length and Value) fueron definidos. Ambos TLVs tienen una parte de su longitud fija, el otro puede ser utilizado como un sub-TLV opcional, que permite añadir nuevas propiedades a los enlaces y prefijos, una de ellas es la ingeniería de tráfico.

Teniendo en cuente que los protocolos de enrutamiento de estado de enlace calculan los recursos libres de las rutas de una red, en IS-IS eso puede ser asegurado porque todos los enrutadores calculan sus tablas a partir de la misma información (LSP). Sin embargo, eso sólo funciona cuando los enrutadores tienen la misma versión de TLVs, caso contrario el cálculo del camino mínimo será diferente para las dos versiones porque solamente una de ellas ha considerado las restricciones de ingeniería de tráfico.

2.4 Enrutamiento IP Multicast

Las nuevas aplicaciones que están surgiendo en Internet han producido un aumento de la necesidad de transmitir información desde un origen a múltiples destinos (como por ejemplo video stream o videoconferencia) y que esta transmisión se haga garantizando ciertos parámetros de Calidad de Servicio (QoS), por ejemplo, el retardo máximo y el número de paquetes que pueden ser descartados sin afectar a la calidad de la transmisión de la información. Esta QoS no puede ser asegurada por los protocolos TCP/IP, por lo que se han desarrollado diferentes tecnologías para superar este inconveniente, entre ellas RSVP y MPLS.

La utilización de MPLS para el transporte de tráfico tipo IP Multicast tiene beneficios sobre la performance, y facilita el transporte sobre redes ATM.

Los paquetes IP Multicast utilizan la misma codificación que los paquetes IP Unicast, con la excepción que al utilizar Label Stack Encoding el protocolo de capa 1, como por ejemplo, Ethernet o PPP, utiliza un identificador de protocolo de capa 3, como por ejemplo, ethertype o PPP protocol ID, para indicar que el paquete MPLS etiquetado es transportado dentro del frame de capa 2. Sin embargo, se utilizan identificadores diferentes para paquetes IP Unicast e IP Multicast, lo cual tiene ciertas ventajas. Primero, esto hace que los paquetes IP Multicast sean fácilmente reconocidos sin tener que examinar la etiqueta utilizada. Segundo, permite que los paquetes IP Unicast e IP Multicast utilicen espacios de etiquetas diferentes, esto a su vez permite definir una LFIB (Label Forwarding Information Base) por interfase.

Los bucles presentan un caso particular cuando se trata con tráfico IP Multicast, ya que los paquetes IP Multicast que entran en un bucle pueden ser replicados debido al reenvió Multicast, lo cual conduce a incrementar el tráfico no deseado en la red hasta que desaparezca la condición que provoco el bucle. Esto puede ser mitigado con la utilización del campo TTL definido en los paquetes MPLS.

El soporte de transmitir tráfico IP Multicast en redes IP MPLS se complica debido al hecho de la variedad de protocolos de enrutamiento utilizados en IP Multicast. Diferentes protocolos de enrutamiento IP Multicast pueden generar diferentes estados de reenvió que necesitan ser tratados diferentemente al momento de establecer los LSPs.

Algunos protocolos de enrutamiento IP Multicast, como PIM-SM, generan dos estados para el reenvió de paquetes, estos son Shared Tree y Source-Specific Tree. Un Shared Tree permite el transporte de paquetes IP Multicast desde cualquier fuente hacia los receptores, mientras que un Source-Specific Tree transporta paquetes IP Multicast desde una fuente hacia un grupo de recept res. Los receptores deben estar lógicamente conectados al Shared Tree para poder recibir el tráfico generado por las fuentes IP Multicast, o pueden unirse a un Source-Specific Tree de modo de optimizar el trayecto entre la fuente y los receptores. Esto puede crear dificultades en un ambiente MPLS cuando un LSP Multicast es establecido para ambos casos, Shared Tree y Source-Specific Tree. De esta forma, una fuente debe enviar paquetes IP Multicast en ambos árboles de distribución, por lo cual un receptor lógicamente conectado en ambos árboles de distribución recibirá paquetes IP Multicast duplicados. Una solución podría ser utilizar MPLS sólo para el árbol de distribución Source-Specific y reenvió IP convencional para Shared Trees.

Otra dificultad que se plantea al utilizar IP Multicast sobre MPLS es la utilización del método de pyggybacking sobre los mensajes del protocolo de control, o utilizar un protocolo separado, como LDP, para realizar la distribución de etiquetas. Algunos

protocolos como PIM soportan la utilización del método de pyggybacking, pero otros como DVMRP no lo soportan.

2.5 GMPLS

En el escenario de desarrollo de las redes IP y de transporte óptico, la calidad de servicio ofrecida por la tecnología MPLS, unida a la extraordinaria capacidad soportada por las redes ópticas basadas en DWDM (Dense Wavelength Dvision Multiplexing), aparece como la combinación ideal para afrontar el reto de las futuras redes de telecomunicación. Esta combinación se refleja en lo que se ha dado en llamar MPλS (Multi-Protocol Lambda Switching), o más comúnmente GMPLS (Generalized Multi-Protocol Label Switching)

En síntesis, GMPLS es una evolución del plano de control multipropósito de MPLS, que tiene el objetivo de ser utilizado no sólo por dispositivos de conmutación de paquetes, sino también por dispositivos que lleven a cabo la conmutación en los dominios del tiempo, longitud de onda y espacio.

GMPLS puede verse, por tanto, como un integrador de las arquitecturas ópticas y de datos, y como tal, su desarrollo necesita de mejoras de la señalización y de los protocolos de encaminamiento IP actualmente existentes para extenderlos al entorno óptico. Los trabajos más recientes en este sentido intentan adaptar el plano de control MPLS, y especialmente sus protocolos de señalización y encaminamiento (CR-LDP y RSVP-TE), de manera que no solo sea utilizado por los enrutadores y conmutadores ATM, sino también por los cros-conectores ópticos (OXCs). Así mismo, GMPLS ha marcado el desarrollo de nuevos protocolos como el LMP (Link Management Protocol).

Pero más allá de la solución tecnológica, GMPLS también resuelve el factor económico al posibilitar una arquitectura de red más optimizada para transportar grandes volúmenes de tráfico que las actuales.

Hoy, típicamente, las redes de datos tienen cuatro niveles: IP para el transporte de aplicaciones y servicios, ATM para realizar ingeniería de tráfico, SONET/SDH para proveer transmisión y DWDM para aumentar la capacidad de transporte. Esta arquitectura en cuatro niveles tiene el inconveniente de la lentitud en su escalado para volúmenes de tráfico muy grandes, y al mismo tiempo resultan caras. Las arquitecturas de múltiples capas normalmente sufren de extrapolar las deficiencias de la capa menos efectiva. Si una de las capas puede limitar la capacidad de crecimiento de la red, esta se verá afectada en su conjunto, lo que al final se traduce en un aumento del coste de la red en su totalidad. Por lo tanto, podemos decir que a parte de las mejoras técnicas, GMPLS conlleva una optimización del transporte, que reducirá significativamente los costes de los operadores tanto en inversión, como en operación y mantenimiento.

Un transporte efectivo debería optimizar el coste del multiplexado y de la conmutación para un volumen de tráfico elevado. DWDM es una técnica de multiplexado efectiva que ofrece avances técnicos significativos. Básicamente crea múltiples fibras virtuales sobre una única fibra, soportando cada fibra virtual varios gigabits por segundo de capacidad. De la misma manera, los OXCs emergerán como la opción preferida para conmutar estos caudales de múltiples gigabits e incluso de terabits, dado que se elimina la conmutación electrónica.

De todas formas, se espera que el tráfico predominante en todas las redes sea IP, lo que sugiere que el desarrollo de los enrutadores es esencial para la agregación de caudales de capacidades moderadas a caudales que se ajusten a los OXCs. De la misma manera, el multiplexado estadístico basado en IP parece que será el predominante para flujos de paquetes menores que los que se adaptan a las velocidades de DWDM. Con estas consideraciones, el modelo final propuesto se basa en enrutadores IP interconectados vía OXCs con transmisión DWDM, complementándose, pero sin poder fusionarse en una sola. En la figura 2.15 se muestra un ejemplo de una red GMPLS.

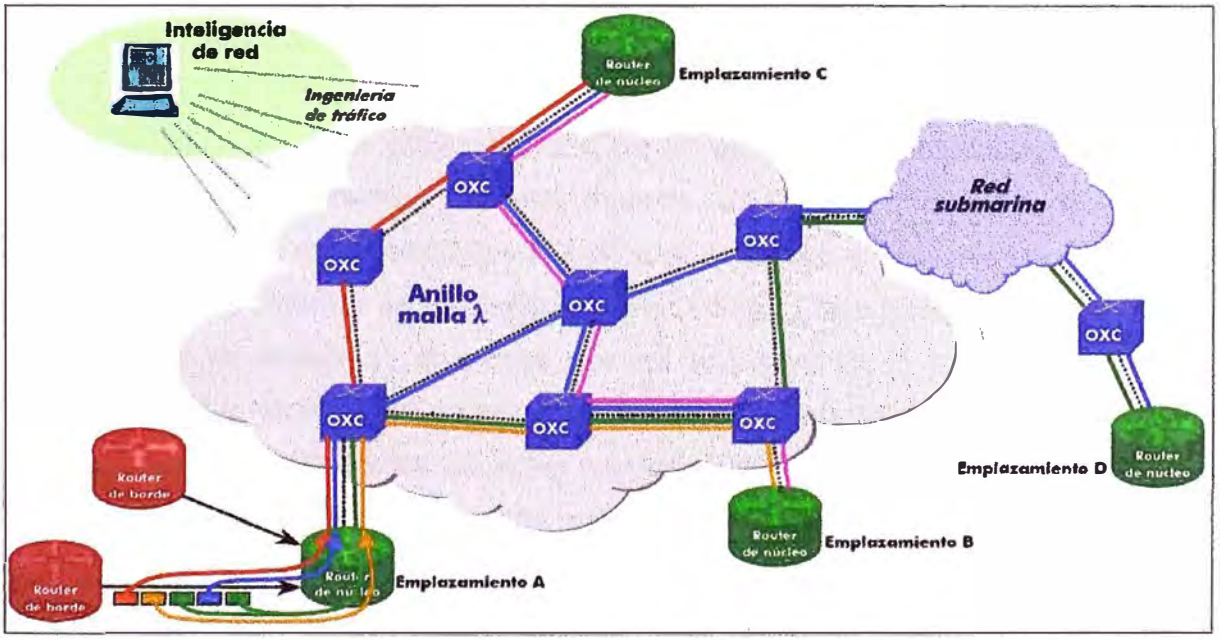

Figura 2.15 Modelo de Red GMPLS

En el presente capitulo se ha desarrollado las diferentes aplicaciones sobre MPLS, poniendo especial interés en la característica de MPLS para el soporte para Redes Privadas Virtuales y Calidad de Servicio, que juntamente con el desarrollo del capitulo I nos brindan los conocimientos necesarios para iniciar los capítulos III y IV donde se muestra el procedimiento de configuración para la implementación de la red MPLS con soporte de RPV con calidad de servicio.

III
ANÁLISIS Y CONFIGURACIÓN DEL BACKBONE MPLS

Esta parte del informe se centra en la configuración de los equipos del backbone MPLS, equipos denominados P (Provider) y PE (Provider Edge) también conocidos en MPLS como LSR y LER. Se ha definido una topología de red formada por 2 equipos P (P1 y P2) y 2 equipos PE (PE1 y PE2), sobre los cuales se realizará la configuración del protocolo de distribución de etiquetas LDP y de enrutamiento de estado de enlace OSPF, la configuración de VPNs y calidad de servicio se aborda en el siguiente capítulo, adicionalmente se incluyen algunos comandos que nos permiten verificar el correcto funcionamiento de la red.

Las configuraciones que se muestran en el desarrollo del presente y el siguiente capítulo se han ejecutado sobre 3 modelos de enrutadores del fabricante Cisco Systems (12406 XR, 7206 VXR y 2081), modelos que han sido elegidos en base a las funciones que deben desempeñar en la implementación de la red MPLS (enrutadores tipo P, PE o CPE). Así mismo comentar que son equipos sobres los cuales he tenido cierta experiencia que me ha permitido llevar a cabo el desarrollo el presente trabajo. Para la gran variedad de modelos de enrutadores del proveedor Cisco Systems, los comandos y configuración se realiza de la misma manera que para los 3 modelos que se han seleccionado. La forma de los comandos y como se aplican estos para configurar MPLS en equipos de otros fabricantes como por ejemplo Alcatel, Nortel, Huawei, Juniper, etc. se realizan de manera diferente para cada proveedor, no significando esto problema alguno cuando se interconectan equipos de diferentes fabricantes, ya que los parámetros definidos en la RFC para la arquitectura MPLS son únicos, solo que representados de distinta manera por cada fabricante.

3.1 Arquitectura de red

Para el desarrollo del presente y el siguiente capítulo que consisten en el análisis y configuración de un backbone MPLS con soporte para Redes Privadas Virtuales con Clases de Servicio se ha definido una topología de backbone MPLS básica que nos permita simular la red de un proveedor de servicios de telecomunicaciones y entender el funcionamiento de los diferentes componentes de MPLS.

3.1.1 Topología del Backbone IP/MPLS.

Los enrutadores tipo P se encuentran en el Core de la Red, es decir solo tiene conexión con otros enrutadores de tipo P y PE, mientras que los enrutadores tipo PE se encuentra en el borde de la red y tiene conexión con los equipos CPE (Customer Premise Equitment) ubicados en el local del cliente. Para el esquema desarrollado se ha definido una red MPLS formada por 2 enrutadores tipo P (P1 y P2) y 2 enrutadores tipo PE (PE1 y PE2). En la tabla 3.1 podemos observar los equipos utilizados, fabricante, modelo y el software IOS respectivo para cada modelo con soporte MPLS.

Tipo de enrutador	Proveedor	Modelo	Versión IOS
P (Provider)	Cisco	12406 XR	12.0(28)S3
PE (Provider Edge)	Cisco	7206 VXR	12.4(4)XD2
CPE (Customer Premise Equitment)	Cisco	2801	12.4(8d)

Tabla 3.1 Equipos utilizados en la topología de la red

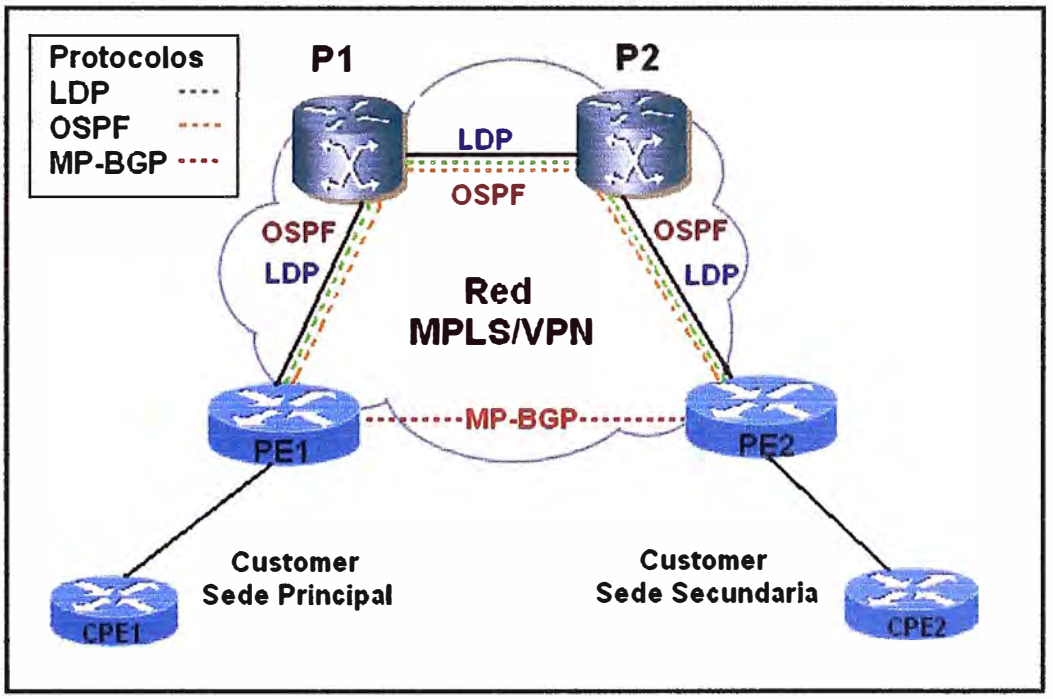

Figura 3.1 Topología del backbone MPLS

3.1.2 Protocolos usados

Se ha seleccionado el protocolo de enrutamiento de estado de enlace OSPF, y el protocolo LDP para la distribución de etiquetas:

- Protocolo de distribución de etiquetas: En los routers Cisco pueden utilizarse dos protocolos para la distribución de etiquetas: LDP (Label Distribution Protocol)

estándar del IETF y TDP (Tagging Distribution Protocol) desarrollado por Cisco. Se ha elegido el protocolo LDP ya que es el estándar del IETF utilizado por los proveedores de servicios en la actualidad que nos permite interconectar equipos de cualquier fabricante lo que no sucede con TDP que es propietario de Cisco.

- Protocolos de enrutamiento: Para la implementación de la Red IP/MPLS el protocolo de enrutamiento IGP a utilizar es OSFP, que nos va a permitir establecer conectividad entre todos los equipos P y PE que hemos definido en la topología de red. El protocolo de enrutamiento OSPF se va a configurar en los enlaces de enrutadores P a P y P a PE, tiene la finalidad del intercambio de información para la construcción y el mantenimiento de las tablas de enrutamiento que son utilizadas por el protocolo LDP para el establecimiento de los LSPs y asignación de etiquetas. El desarrollo del protocolo Interno MP BGP (MP-iBGP) se va ha a implementar y configurar en el siguiente capitulo que es donde se desarrolla la red MPLS/VPN.

Descripción	Red IP	Máscara IP
RED Administración	172.16.1.0	255.255.255.0
RED WAN	172.16.2.0	255.255.255.0
RED WAN CPE	172.16.3.0	255.255.255.0

Tabla 3.2 Direccionamiento IP

3.2 Plan de direccionamiento IP

Parte de la implementación del backbone IP/MPLS consiste en diseñar un esquema de direccionamiento IP para la asignación y configuración de los equipos P, PE y CPE. Para ello se ha considerado la utilización de las subredes indicadas en la tabla 3.2. La subred 172.16.1.0/24 se ha asignado para el direccionamiento IP de las interfaces Loopback de los equipos P y PE, serán utilizadas en la gestión de los equipos correspondientes.

Enlace	Equipo	Interfase	IP WAN	Máscara
P1 - P2	P1	GE 1/0	172.16.2.1	255.255.255.252
	P2	GE 1/0	172.16.2.2	255.255.255.252
P1 - PE1	P1	GE 1/1	172.16.2.5	255.255.255.252
	PE1	GE 1/0	172.16.2.6	255.255.255.252
P2 - PE2	P2	GE 1/1	172.16.2.9	255.255.255.252
	PE2	GE 1/0	172.16.2.10	255.255.255.252

Tabla 3.3 Asignación de direcciones IP WAN

La subred 172.16.2.0/24 se ha considerado para ser configurada en las interfaces WAN que conectan a los equipos P y PE. Finalmente la red 172.16.3.0 se ha definido para configurarse en las interfaces WAN entre PEs y CPEs. En la tabla 3.3 se muestra la asignación de direcciones IP WAN a los enrutadores P1, P2, PE1 y PE2; y en la tabla 3.4 la asignación de IP Loopbacks a usarse para los procesos OSPF, LDP y MP-BGP.

Equipo	IP Loopback	Máscara
P1	172.16.1.1	255.255.255.255
P2	172.16.1.2	255.255.255.255
PE1	172.16.1.3	255.255.255.255
PE2	172.16.1.4	255.255.255.255

Tabla 3.4 Asignación de direcciones IP loopback

3.3 Configuración de parámetros globales

En esta sección vamos a realizar la configuración de parámetros básicos de los enrutadores P y PE que forman parte de la topología del backbone IP/MPLS. Una de las primeras tareas de configuración básica por ejemplo es asignar el nombre correspondiente a los equipos, que nos ayudará a una mejor administración de la red al identificar unívocamente a cada uno de los enrutadores. Así mismo se va a configurar las direcciones IP WAN y Loopback asignadas en base al plan de direccionamiento descrito en la sección anterior. En la figura 3.2 podemos observar el plan de direccionamiento mencionado.

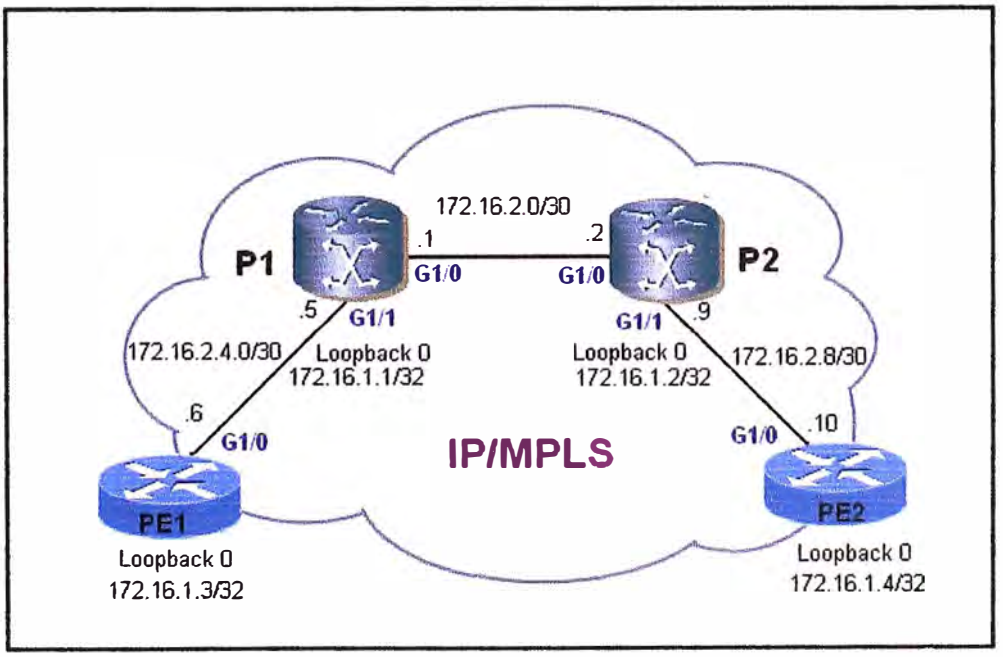

Figura 3.2 Esquema de direccionamiento IP

En la figura 3.3 se muestra el procedimiento a seguir para configurar los parámetros básicos en el router P1, para ello se utilizan los siguientes comandos:

- *hostname*: asigna un nombre al router que me permite diferenciar a cada equipo P y PE en la red MPLS.
- *ip subset-zero*. Permite la utilización de la subred cero en todas la interfaces.
- *interface.* Nos permite entrar al modo de configuración de la interfaz seleccionada.
- *description*. Se utilizan para identificar la información importante que nos ayuda a entender mejor el enlace.
- *ip address.* Nos permite asignar una dirección IP y su respectiva mascara de subred, a la interfaz sobre la cual se configura.
- *no shutdwon.* Este comando nos permite activar una interfaz, ya que por defecto las interfaces están desactivadas.
- *ip classless*. No es necesario activarlo viene habilitado por defecto en los enrutadores Cisco.

```
Router (config) # configure terminal
Router (config) # hostname P1
P1 (config) # ip subnet-zero
P1 (config) # interface Loopback 0
P1 (config-if) # description Proceso BGP – OSPF - MPLS
P1 (config-if) # ip address 172.16.1.1 255.255.255.255
P1 (config-if) # exit
P1 (config) # interface GigabitEthernet1/0
P1 (config-if) # description Enlace MPLS P1 >> P2 GE 1/0
P1 (config-if) # ip address 172.16.2.1 255.255.255.252
P1 (config-if) # no shutdown
P1 (config-if) # exit
P1 (config) # interface GigabitEthernet1/1
P1 (config-if) # description Enlace MPLS P1 >> PE1 GE 1/1
P1 (config-if) # ip address 172.16.2.5 255.255.255.252
P1 (config-if) # no shutdown
```

Figura 3.3 Configuración básica de P1

La misma secuencia de configuración debe realizarse en los enrutadores P1, P2, PE1 y PE2, luego de lo cual obtenemos las configuraciones parciales que se muestran en las figuras 3.4, 3.5, 3.6 y 3.7. En las figuras indicadas 3.4, 3.5, 3.6 y 3.7 podemos observar que se han configurado los parámetros básicos para establecer la comunicación entre los equipos directamente conectados, como es el caso de las direcciones IP de las interfaces, nombre de los enrutadores, descripción de las interfaces, entre otros. Para el

ejemplo del enrutador P1 como se observa en la figura 3.4 hemos utilizado el comando *description,* que nos permite colocar una descripción para indicar el enlace al que corresponde, por ejemplo en la interfase G1/0 del enrutador P1 se tiene como descripción "Enlace MPLS P1 >> P2 GE1/0" que indica que esta interfase esta conectada a la interfase GE1/0 del enrutador P2

Configuración de las interfaces de P1

```
hostname P1
!
ip subnet-zero
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.1 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS P1 >> P2 GE 1/0
 ip address 172.16.2.1 255.255.255.252
!
interface GigabitEthernet1/1
 description Enlace MPLS P1 >> PE1 GE 1/1
 ip address 172.16.2.5 255.255.255.252
!
ip classless
```

Figura 3.4 Configuración de las interfaces de P1

Configuración de las interfaces de P2

```
hostname P2
!
ip subnet-zero
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.2 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS P2 >> P1 GE 1/0
 ip address 172.16.2.2 255.255.255.252
!
interface GigabitEthernet1/1
 description Enlace MPLS P2 >> PE2 GE 1/1
 ip address 172.16.2.9 255.255.255.252
!
ip classless
```

Figura 3.5 Configuración de las interfaces P2

Configuración de las interfaces de PE1

```
hostname PE1
!
ip subnet-zero
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.3 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS PE1 >> P1 GE 1/1
 ip address 172.16.2.6 255.255.255.252
!
ip classless
```

Figura 3.6 Configuración de las interfaces de PE1

Configuración de las interfaces de PE2

```
hostname PE2
!
ip subnet-zero
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.4 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS PE2 >> P2 GE 1/1
 ip address 172.16.2.10 255.255.255.252
!
ip classless
```

Figura 3.7 Configuración de interfaces de PE2

3.4 Configuración del enrutamiento con OSPF

Siguiendo el esquema de diseño mencionado anteriormente el IGP elegido para el enrutamiento en el interior de la red es el protocolo OSPF, que tendrá por función la publicación de las direcciones IP de las interfaces loopbacks y redes asignadas a las interfaces de conexión entre los enrutadores P y PE del backbone IP/MPLS. De esta manera conseguimos la conectividad total entre todos los equipos de la red.

Así mismo se ha definido el área 0 como el área del backbone OSPF donde se van a configurar las interfaces loopback 0 de los P y PE, así como los enlaces entre P y PE.

El software IOS de Cisco inicializa un proceso del protocolo de enrutamiento OSPF cuando el administrador del router introduce la orden de configuración global:

Router (config) **# router ospf** *id-proceso*

El comando *router ospf*, seguido de un número de *id-proceso,* lanza un proceso de encaminamiento de OSPF con el identificador de proceso asignado. A diferencia de otros protocolos como IGRP y EIGRP, este valor es específico del router y no se utiliza para identificar sistemas autónomos de OSPF diferentes. Se pueden ejecutar múltiples procesos de OSPF en cualquier router dado utilizando ID de procedo únicos para cada uno de ellos. El campo de *id-proceso* es de 16 bits y esta comprendido entre 1 y 65535.
El proceso de OSPF definido debe estar asociado a una interfaz IP activa en el router para que OSPF comience a crear adyacencias de vecino y tablas de enrutamiento.

Router (config - router) **# network** *dirección mascara-wildcard* **area** *id-área*

La orden *network area* permite al proceso que se enteré que interfaces están utilizando OSPF. El parámetro *dirección* puede ser la dirección IP de la interfaz, la subred o la dirección de red de la interfaz a la que se debe aplicar enrutamiento de OSPF.
Unido al parámetro *dirección* tenemos el parámetro *máscara-wildcard*, cuyo valor identifica que bit del valor del parámetro *dirección* se utiliza para interpretar el valor del parámetro *dirección.* El valor del parámetro *id-área* identifica a que área de OSPF esta asociada la red especificada. El *id-área* puede ser un número decimal en el rango de 0 a 4294967295 conformado por 32 bits, o se puede escribir en el formato decimal con puntos de una dirección IP.

Router (config-router) **# router-id** *dirección_ip*

El comando *router-id* nos permite seleccionar que dirección IP será utilizada como identificador de router, ya que OSPF precisa de un identificador de router (ID de router) para que la operación tenga éxito. Cada router selecciona como ID de router la dirección IP más elevada en cualquier interfaz activa. En caso de que está falle, el proceso OSPF no puede continuar. Para garantizar que OSPF sea estable, se configura una dirección loopback para utilizarse como identificador de router.

Router (config-router) **# auto-cost reference-bandwidth** *mbps*
Router (config-router) **# log-adjacency-changes**

El comando *auto-cost reference-bandwidth* nos permite cambiar el valor de referencia por defecto de 100Mbps que se utiliza para el cálculo del costo del enlace.

El comando *log-adjacency-changes* nos muestra los eventos que se presenta con el proceso ospf, en versiones de IOS superiores a las 12.2 este comando se configura automáticamente al habilitar el proceso OSPF, por lo que el comando mencionado solo es utilizado con versiones de IOS menores o iguales a la 12.1.

Router (config-router) **# area** *id-área* **authentication message-digest**

El comando indicado permite introducir la autenticación MD5 en el proceso OSPF, esta configuración es realizada como medio de proporcionar seguridad a las actualizaciones de la tabla de enrutamiento. Cuando se utiliza la autenticación los enrutadores de Cisco se protegen no anunciando rutas a enrutadores promiscuos no autorizados ni recibiendo información de enrutamiento de ellos.
La autenticación se define en el nivel de interfaz y, por tanto, proporciona una selección discreta de las interfaces que deben utilizar autenticación. La autenticación queda determinada por la configuración de una cadena de clave especificada de la interfaz.
Es necesario habilitar la autenticación en la interfase que va a participar en el proceso de enrutamiento OSPF:

Router (config-if) **# ip ospf message-digest-key** *key-id* **md5** *encryption-type key*

Donde "*key-id*" es un identificador en el rango desde el 1 a 255. Y key es una clave alfanumérica de 16 bytes. El "*encryption-type*" puede ser de 0 a 7; 0 es por defecto; 7 es propietario de Cisco.

A continuación en la figura 3.8 se muestra el proceso de configuración en el router P1 tomando las direcciones IP asignadas en el plan de direccionamiento y los comandos mencionados para la configuración del protocolo de enrutamiento OSPF. Como se observa se define el proceso ospf 1 (*router ospf1*), se ha configurado como identificador del router la dirección IP de la interfaz virtual Loopbackp (*router-id 172.16.1.1*), que será utilizada para el intercambio de información de enrutamiento OSPF con los otros enrutadores, se publica luego por intermedio del comando *network* las redes que formarán parte del proceso ospf como por ejemplo (*network 172.16.2.0 0.0.0.3 area 0*), que es la red WAN conecta a los enrutadores P1 y P2. Finalmente dentro del modo de configuración de cada interfase que participa en el proceso de enrutamiento OSPF se ha definido el proceso de autenticación para el intercambio de información de enrutamiento de manera segura.

```
P1 # configure terminal
P1 (config) # router ospf 1
P1 (config-router) # router-id 172.16.1.1
P1 (config-router) # auto-cost reference-bandwidth 10000
P1 (config-router) # area 0 authentication message-digest
P1 (config-router) # network 172.16.1.1 0.0.0.0 area 0
P1 (config-router) # network 172.16.2.0 0.0.0.3 area 0
P1 (config-router) # network 172.16.2.4 0.0.0.3 area 0
P1 (config-router) # exit
P1 (config) # interface GigabitEthernet1/0
P1 (config-if) # ip ospf message-digest-key 1 md5 7 cisco
P1 (config-router) # exit
P1 (config) # interface GigabitEthernet1/1
P1 (config-if) # ip ospf message-digest-key 1 md5 7 cisco
```

Figura 3.8 Configuración OSPF del enrutador P1

Finalmente luego de realizar el mismo procedimiento de configuración en los enrutadores P2, PE1 y PE2 para el protocolo de enrutamiento dinámico OSPF que el ejecutado en el enrutador P1, se debe tener las configuraciones parciales que se muestran en las figuras 3.9, 3.10, 3.11 y 3.12.

Configuración OSPF de P1

```
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.1 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS P1 >> P2 GE 1/0
 ip address 172.16.2.1 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427191B2E3E69797578
!
interface GigabitEthernet1/1
 description Enlace MPLS P1 >> PE1 GE 1/1
 ip address 172.16.2.5 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427191B2E3E45857438
!
router ospf 1
 router-id 172.16.1.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.1 0.0.0.0 area 0
 network 172.16.2.0 0.0.0.3 area 0
 network 172.16.2.4 0.0.0.3 area 0
```

Figura 3.9 Configuración del proceso OSPF del enrutador P1

Configuración OSPF de P2

```
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.2 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS P2 >> P1 GE 1/0
 ip address 172.16.2.2 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427345B2E3E69796134
!
interface GigabitEthernet1/1
 description Enlace MPLS P2 >> PE2 GE 1/1
 ip address 172.16.2.9 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427345B2E3E61122135
!
router ospf 1
 router-id 172.16.1.2
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.2 0.0.0.0 area 0
 network 172.16.2.0 0.0.0.3 area 0
 network 172.16.2.8 0.0.0.3 area 0
```

Figura 3.10 Configuración del proceso OSPF del enrutador P2

Configuración OSPF de PE1

```
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.3 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS PE1 >> P1 GE 1/1
 ip address 172.16.2.6 255.255.255.252
 ip ospf message-digest-key 1 md5 7 152417345B2E3E68196154
!
router ospf 1
 router-id 172.16.1.3
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.3 0.0.0.0 area 0
 network 172.16.2.4 0.0.0.3 area 0
```

Figura 3.11 Configuración del proceso OSPF del enrutador PE1

Podemos apreciar en la figura 3.11 que el enrutador PE1 utiliza la dirección IP 172.16.1.3 como su identificador para el intercambio de información de enrutamiento con el resto de enrutadores del backbone MPLS que están corriendo OSPF como son P1, P2 y PE2.

Configuración OSPF de PE2

```
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.4 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS PE2 >> P2 GE 1/1
 ip address 172.16.2.10 255.255.255.252
 ip ospf message-digest-key 1 md5 7 143427345B2E3E69796128
!
router ospf 1
 router-id 172.16.1.4
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.4 0.0.0.0 area 0
 network 172.16.2.8 0.0.0.3 area 0
```

Figura 3.12 Configuración del proceso OSPF del enrutador PE2

3.5 Configuración de MPLS LDP

Una vez establecido el protocolo de enrutamiento OSPF se han de configurar las funcionalidades MPLS en los nodos P y PE. Para ello hay que arrancar el protocolo de distribución de etiquetas en las distintas interfaces por las que queremos hablar MPLS. Para nuestro diseño vamos a implementar el protocolo de distribución de etiquetas LDP entre los enlaces P – P y P – PE como se observa en la figura 3.13.

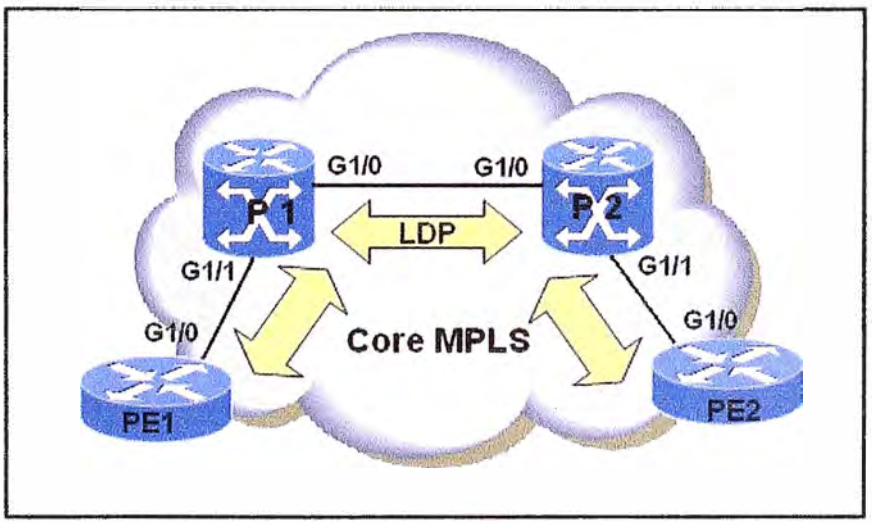

Figura 3.13 Implementación de LDP

Para la implementación de MPLS es necesario configurar el CEF (*Cisco Express Forwarding*) en todos los enrutadores con funcionalidad PE y P. CEF es el conjunto de

funcionalidades que reúnen los equipos Cisco para poder trabajar en un entorno MPLS, entre otras funciones proporciona un mejor aprovechamiento del procesamiento del CPU. CEF construye 2 estructuras de datos: FIB (*Forwarding Information Base*), la cual contiene los mejores caminos hacia el destino, y una tabla de adyacencias, en la cual se define la información del siguiente salto.
La configuración de MPLS requiere primero habilitar CEF (*Cisco Express Forwarding*) en todos los enrutadores con funcionalidad PE y P. El comando para configurar CEF en un router es *ip cef* el cual se ingresa en el modo de configuración global, así mismo se recomienda utilizar la interfase Loopback 0 como ID de router para el protocolo de distribución de etiquetas (LDP)

Router # configure terminal
Router (config) # **ip cef**
Router (config) # **mpls ldp router-id** *Loopback 0*

Habilitar MPLS en las interfaces de los enrutadores P y PE que van a correr MPLS, para ello se debe ingresar al modo de configuración de la interfaz y definir el comando *mpls ip* que habilita el reenvió MPLS salto a salto para una determinada interfase. Tener en cuenta que al definir este comando en el modo de configuración global no habilita MPLS en las interfaces.

Router # configure terminal
Router (config) # **interface** *interface*
Router (config-if) # **mpls ip**

A partir de la versión del Cisco IOS 12.3 (4) el protocolo de distribución de etiquetas por defecto en MPLS es LDP, por lo que al habilitar el comando *mpls ip* en la interfase correspondiente se esta habilitando automáticamente LDP, no es necesario aplicar el comando *mpls label protocolo ldp* como se realizaba con versiones anteriores, cuando se tenía como protocolo por defecto a TDP.

Para la implementación de nuestro modelo MPLS vamos a definir el protocolo LDP como el protocolo por defecto para toda la plataforma en los router P y PE, es decir el protocolo por defecto para cualquier interfase que opere MPLS (como se indicó anteriormente a partir de la versión 12.3 (4) del Cisco IOS en adelante, MPLS habilita el protocolo LDP por defecto, por lo que no sería necesario definirlo globalmente sin embargo es recomendable definirlo de forma manual). Para tal fin se define el comando *mpls label protocol ldp* en el modo de configuración global:

Router # configure terminal
Router (config) **# mpls ip**
Router (config) **# mpls label protocol ldp**

Si en la implementación de la red tenemos algunos equipos enrutadores P o PE utilizando el protocolo TDP, podemos seleccionar que la interfase que se conecta con dichos equipos utilice el protocolo TDP definiendo el comando *mpls label protocol tdp* en el modo de configuración de la interfaz correspondiente, también se puede configurar una interfaz para que opere con ambos protocolos en simultaneo, es decir TDP y LDP.

Router (config) # no mpls ip propagate-ttl

El comando *mpls ip propagate-ttl* permite controlar la generación del campo TTL (time-to-live) en la cabecera de MPLS cuando las etiquetas son adicionadas a un paquete IP, por defecto esta habilitado. Para usar un valor TTL de 255 para la primera etiqueta del paquete IP debemos usar la forma negada de este comando.
En la figura 3.14 se muestra el proceso de configuración de MPLS en el router P1, como se observa primero se define CEF, luego se define en el modo de configuración global del enrutador que el protocolo por defecto sea LDP, se deniega el TTL, se activa interfase virtual Loopback 0 para el proceso LDP y finalmente se habilita MPLS en las interfaces GE 1/0 y GE 1/1 del enrutador P1 hacia P2 y PE1 respectivamente.

```
P1 (config) # configure terminal
P1 (config) # ip cef
P1 (config) # mpls ip
P1 (config) # mpls label protocol ldp
P1 (config) # no mpls ip propagate-ttl
P1 (config) # mpls ldp router-id Loopback 0
P1 (config) # interface GigabitEthernet1/0
P1 (config-if) # mpls ip
P1 (config) # interface GigabitEthernet1/1
P1 (config-if) # mpls ip
```

Figura 3.14 Configuración MPLS de P1

En las figuras siguientes 3.15, 3.16, 3.17 y 3.18 podemos observar la configuración de los enrutadores P1, P2, PE1 y PE2 que incluye la configuración del protocolo de enrutamiento OSPF, protocolo de distribución de etiquetas LDP (MPLS). Las configuraciones de P2, PE1 y PE2 se realizaron bajo el mismo procedimiento que el ejecutado en P1 según la figura 3.14.

Configuración OSFP LDP de P1

```
hostname P1
!
ip subnet-zero
!
ip cef
!
mpls label protocol ldp
no mpls ip propagate-ttl
mpls ldp router-id Loopback0
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.1 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS P1 >> P2 GE 1/0
 ip address 172.16.2.1 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427191B2E3E69797578
 mpls ip
!
interface GigabitEthernet1/1
 description Enlace MPLS P1 >> PE1 GE 1/1
 ip address 172.16.2.5 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427191B2E3E45857438
 mpls ip
 !
router ospf 1
 router-id 172.16.1.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.1 0.0.0.0 area 0
 network 172.16.2.0 0.0.0.3 area 0
 network 172.16.2.4 0.0.0.3 area 0
!
ip classless
```

Figura 3.15 Muestra la configuración OSPF LDP de P1

En la figura 3.15 podemos observar la configuración del enrutador P1, donde se ha definido que la interfase virtual Loopback0 con IP 172.16.1.1 será utilizada para el intercambio de enrutamiento OSPF con los demás enrutadores del backbone como son P2, PE1 y PE2. Como se indico antes de configurar el protocolo LDP de MPLS se debe habilitar primero un protocolo de enrutamiento que para nuestro caso es OSPF, que tiene por finalidad la publicación de todas las redes internas al backbone para que se establezca conexión entre los enrutadores. El intercambio de información de enrutamiento se realiza entre todas las interfaces virtuales definidas en los correspondientes enrutadores.

Configuración OSFP LDP de P2

```
hostname P2
!
ip subnet-zero
!
ip cef
!
mpls label protocol ldp
no mpls ip propagate-ttl
mpls ldp router-id Loopback0 force
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.2 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS P2 >> P1 GE 1/0
 ip address 172.16.2.2 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427345B2E3E69796134
 mpls ip
!
interface GigabitEthernet1/1
 description Enlace MPLS P2 >> PE2 GE 1/1
 ip address 172.16.2.9 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427345B2E3E61122135
 mpls ip
!
router ospf 1
 router-id 172.16.1.2
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.2 0.0.0.0 area 0
 network 172.16.2.0 0.0.0.3 area 0
 network 172.16.2.8 0.0.0.3 area 0
!
ip classless
```

Figura 3.16 Muestra la configuración OSPF - LDP de P2

En la figura 3.16 se tiene la configuración del enrutador P2, para habilitar el protocolo de distribución de etiquetas LDP se aplico el comando *mpls label protocol ldp* en el modo de configuración global del enrutador P2, de esta manera se habilita por defecto el protocolo LDP en todas las interfaces donde de active MPLS. MPLS se activa a nivel de interfaces, por ejemplo en el gráfico se habilita MPLS con el comando *mpls ip* dentro del modo de configuración de la interfase GE1/0 del enrutador P2, es decir se establece el intercambio de etiquetas MPLS con el enrutador P1, de manera similar se activa MPLS para la interfase GE1/1 que conecta con el enrutador PE2, se observa también la configuración del proceso OSPF.

Configuración OSPF LDP de PE1

```
hostname PE1
!
ip subnet-zero
!
ip cef
!
mpls label protocol ldp
no mpls ip propagate-ttl
mpls ldp router-id Loopback0
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.3 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS PE1 >> P1 GE 1/1
 ip address 172.16.2.6 255.255.255.252
 ip ospf message-digest-key 1 md5 7 152417345B2E3E68196154
 mpls ip
!
router ospf 1
 router-id 172.16.1.3
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.3 0.0.0.0 area 0
 network 172.16.2.4 0.0.0.3 area 0
!
ip classless
```

Figura 3.17 Muestra la configuración OSPF-LDP de PE1

En la figura 3.17 se muestra la configuración del enrutador PE1 donde podemos observar que para este enrutador solamente se habilita MPLS en la interfase GE 1/0, esto se debe a que solo tiene la conexión hacia el enrutador P1. De igual manera que en los otros enrutadores del backbone MPLS para el enrutador PE1 se utiliza la interfase virtual Loopback0 con IP 172.16.1.3 para el intercambio de información de enrutamiento OSPF, así mismo en el proceso OSPF se ha habilitado el intercambio de información de enrutamiento con autenticación, es decir antes de recibir rutas se ejecuta un proceso de autenticación con el enrutador vecino, en caso no se valide adecuadamente no se reciben las rutas. En la figura 3.18 se muestra la configuración del enrutador PE2 de igual manera solo se ha habilitado MPLS en la interfase GE1/0 que conecta hacia el enrutador P2. En ambas figuras 3.17 y 3.18 no se incluyen aun la configuración del enrutador PE1 hacia el enrutador CPE1, ni del enrutador PE2 hacia el enrutador CPE2, ya que se verán en el siguiente capítulo.

Configuración OPSF LDP de PE2

```
hostname PE2
!
ip subnet-zero
!
ip cef
!
mpls label protocol ldp
no mpls ip propagate-ttl
mpls ldp router-id Loopback0
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.4 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS PE2 >> P2 GE 1/1
 ip address 172.16.2.10 255.255.255.252
 ip ospf message-digest-key 1 md5 7 143427345B2E3E69796128
 mpls ip
!
router ospf 1
 router-id 172.16.1.4
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.4 0.0.0.0 area 0
 network 172.16.2.8 0.0.0.3 area 0
!
ip classless
```

Figura 3.18 Muestra la configuración OSPF-LDP de PE2

3.6 Verificación del funcionamiento del backbone MPLS

Para realizar la verificación del funcionamiento de una red MPLS, Cisco provee algunos comandos de interés que podemos utilizar en las diferentes etapas del proceso. A continuación se lista una serie de pasos que nos permitirán diagnosticar algún problema que pudiera presentarse en la red MPLS:

- Verificar que el protocolo de enrutamiento esta operando.
- Verificar el estado de CEF.
- Verificar el funcionamiento de MPLS.
- Verificar conectividad con los routers P y PE.
- Verificar la distribución de etiquetas.
- Verificar la asociación de etiquetas.
- Verificar que las etiquetas están siendo asignadas.

3.6.1 Verificación el funcionamiento del protocolo de enrutamiento

Para verificar el correcto funcionamiento del protocolo de enrutamiento IGP que esta corriendo en el backbone IP/MPLS podemos emplear los siguientes comandos:

- *show ip protocols.* Este comando nos permite visualizar la información del protocolo de enrutamiento IP que esta activo.

```
P1 # show ip protocols
Routing Protocol is "ospf 1"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Router ID 172.16.1.1
    Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Maximum path: 4
    Routing for Networks:
        172.16.1.1 0.0.0.0 area 0
        172.16.2.0 0.0.0.3 area 0
        172.16.2.4 0.0.0.3 area 0
   Reference bandwidth unit is 10000 mbps
    Routing Information Sources:
        Gateway         Distance      Last Update
        172.16.1.3           110      10:41:55
        172.16.1.2           110      10:41:55
        172.16.1.4           110      10:41:55
    Distance: (default is 110)
```

Figura 3.19 Muestra la salida del comando show ip protocols en P1

```
P1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O      172.16.2.8/30 [110/12952] via 172.16.2.2, 00:00:39, GigabitEthernet1/0
O      172.16.1.4/32 [110/12953] via 172.16.2.2, 00:00:39, GigabitEthernet1/0
C      172.16.2.4/30 is directly connected, GigabitEthernet1/1
C      172.16.1.1/32 is directly connected, Loopback0
C      172.16.2.0/30 is directly connected, GigabitEthernet1/0
O      172.16.1.3/32 [110/6477] via 172.16.2.6, 00:00:39, GigabitEthernet1/1
O      172.16.1.2/32 [110/6477] via 172.16.2.2, 00:00:39, GigabitEthernet1/0
```

Figura 3.20 Muestra la salida del comando show ip route en P1

- *show ip route*. Este comando nos permite visualizar la tabla de enrutamiento IP del router, donde debemos verificar que se encuentran presentes las redes asignadas y si los vecinos se encuentran presentes.

3.6.2 Verificación del estado de CEF

El comando *show ip cef summary* permite ver un resumen de la información contenida en la tabla FIB (*Forwarding Information Base*), se tienen también otros comandos como *show ip cef interface*, *show ip cef detail*, y *show ip cef* que muestra las entradas en la tabla BIF, como podemos observar en la figura 3.21 que muestra una parte de la tabla FIB de P1:

```
P1#show ip cef
Prefix              Next Hop        Interface
172.16.1.2/32       172.16.2.2      GigabitEthernet1/0
172.16.1.3/32       172.16.2.6      GigabitEthernet1/1
172.16.1.4/32       172.16.2.2      GigabitEthernet1/0
172.16.2.8/30       172.16.2.2      GigabitEthernet1/0
```

Figura 3.21 Muestra la salida show ip cef en P1

3.6.3 Verificación el funcionamiento de MPLS

Para la verificación del funcionamiento de MPLS tenemos el comando *show mpls interfaces* que nos asegura que MPLS esta globalmente habilitado. Este comando también verifica que tipo de protocolo esta corriendo en las interfaces, por ejemplo en la figura 3.22 podemos apreciar que el campo IP muestra que la interfase GigabitEthernet1/0 tiene configurado MPLS (protocolo LDP) y el campo *operational* muestra el estado del protocolo LDP.

```
P1# show mpls interfaces
Interface              IP         Tunnel   Operational
GigabitEthernet1/0     Yes (ldp)  No       Yes
GigabitEthernet1/1     Yes (ldp)  No       Yes
```

Figura 3.22 Salida de comando show mpls interfaces en P1

3.6.4 Verificación de la distribución de etiquetas

El comando *show mpls ldp discovery* y *show mpls ldp neighbor* muestra los vecinos descubiertos, y que protocolo se esta utilizando para la asociación de etiquetas con dichos vecinos (TDP o LDP). Si alguno de los vecinos no esta presente y verificamos que

no se tiene conectividad con el vecino, entonces se presenta un problema de conectividad y por consiguiente el LDP no corre, si el LDP corre correctamente este asigna una etiqueta por FEC. En las figuras 3.23 y 3.24 se muestran la salida de estos comandos, donde podemos observar por ejemplo que el enrutador P1 esta corriendo LDP a través de las interfaces GE1/0 y GE1/1 con los enrutadores P2 y PE1 respectivamente, utilizando como identificadores del proceso LDP las direcciones IP de las Loopback.

```
P1# show mpls ldp discovery
 Local LDP Identifier:
    172.16.1.1:0
    Discovery Sources:
    Interfaces:
       GigabitEthernet1/0 (ldp): xmit/recv
          LDP Id: 172.16.1.2:0
       GigabitEthernet1/1 (ldp): xmit/recv
          LDP Id: 172.16.1.3:0
```

Figura 3.23 Salida del comando show mpls discovery

```
P1#show mpls ldp neighbor
   Peer LDP Ident: 172.16.1.2:0; Local LDP Ident 172.16.1.1:0
      TCP connection: 172.16.1.2.58470 - 172.16.1.1.646
      State: Oper; Msgs sent/rcvd: 111/109; Downstream
      Up time: 01:27:17
      LDP discovery sources:
        GigabitEthernet1/0, Src IP addr: 172.16.2.2
      Addresses bound to peer LDP Ident:
        172.16.2.2      172.16.1.2      172.16.2.9
   Peer LDP Ident: 172.16.1.3:0; Local LDP Ident 172.16.1.1:0
      TCP connection: 172.16.1.3.60824 - 172.16.1.1.646
      State: Oper; Msgs sent/rcvd: 101/103; Downstream
      Up time: 01:20:06
      LDP discovery sources:
        GigabitEthernet1/1, Src IP addr: 172.16.2.6
      Addresses bound to peer LDP Ident:
        172.16.1.3      200.200.200.1   200.200.100.1   172.16.2.6
```

Figura 3.24 Salida del comando show mpls ldp neighbor en P1

3.6.5 Verificación de la asociación de etiqueta

El comando *show mpls ldp bindings* muestra la asignación de etiquetas a cada destino, también se puede utilizar el comando *show mpls forwarding-table* que nos permite verificar las diferentes rutas y las etiquetas asociadas con estas rutas. Las salidas a los comandos indicados se muestran en las figuras 3.25 y 3.26.

```
P1# show mpls ldp bindings
  tib entry: 172.16.1.1/32, rev 6
        local binding:  tag: imp-null
        remote binding: tsr: 172.16.1.2:0, tag: 16
        remote binding: tsr: 172.16.1.3:0, tag: 18
  tib entry: 172.16.1.2/32, rev 8
        local binding:  tag: 18
        remote binding: tsr: 172.16.1.2:0, tag: imp-null
        remote binding: tsr: 172.16.1.3:0, tag: 19
```

Figura 3.25 Salida del comando show mpls ldp bindings en P1

P1# show mpls forwarding-table

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
18	Pop tag	172.16.1.2/32	9416	Gi1/0	172.16.2.2
19	17	172.16.1.4/32	756	Gi1/0	172.16.2.2
20	Pop tag	172.16.2.8/30	0	Gi1/0	172.16.2.2
21	Pop tag	172.16.1.3/32	10272	Gi1/1	172.16.2.6

Figura 3.26 Salida del comando show mpls forwarding-table en P1

En el presente capitulo hemos desarrollo la configuración del protocolo de enrutamiento OSPF y configuración de MPLS en los enrutadores P1, P2, PE1 y PE2 de la red del backbone, como complemento se muestran algunos comandos que se pueden utilizar para la resolución de problemas tanto de enrutamiento como de MPLS.

El capitulo III nos ha servido para dejar lista la red del backbone MPLS para implementar y configurar el soporte para Redes Privadas Virtuales con Calidad de Servicio, tema que se trata en el siguiente capítulo.

IV
ANÁLISIS Y CONFIGURACIÓN DE UNA RED CORPORATIVA SOBRE LA RED MPLS/VPN CON CALIDAD DE SERVICIO

En el presente capítulo se desarrolla la red MPLS/VPN con calidad de servicio. Primero vamos a definir algunos requerimientos mínimos para la VPN Corporativa de un cliente al cual llamaremos BANCO PERU S.A.C, requerimientos en base a los cuales se ofrecerá una solución sobre la red MPLS/VPN. Para el soporte de VPNs sobre MPLS es necesario que el backbone tenga habilitado MPLS sobre algún protocolo de enrutamiento de estado de enlace como OSPF o IS-IS, dicho requisito se desarrollo en el capitulo III donde se configuro la red MPLS con LDP como protocolo de distribución de etiquetas y OSPF como IGP para el intercambio de rutas internas de la red del backbone.
Otro de los requisitos para el soporte de VPNs en MPLS es la configuración del protocolo MP-BGP para el enrutamiento de prefijos vpnv4 que son definidos en cada VPN con su respectivo VRF, RD y RT, temas que también se abordan en este capitulo así mismo se mencionan algunos comandos que podemos utilizar para la verificación en caso de presentarse algún problema. Se define y configura calidad de servicio en la red MPLS/VPN en integración con la arquitectura de servicios diferenciados (DiffServ). Culminando el capítulo se muestra el resultado de pruebas realizadas con la finalidad de validar las configuraciones que se desarrollaron en el presente informe.

4.1 Requerimientos de la red Corporativa

En las redes de clientes hoy en día se tiene una infinidad de aplicativos que cumplen diferentes funciones y que requieren ciertas condiciones para su buen funcionamiento. Para nuestro ejemplo vamos a suponer que se ha recibido los requerimientos de servicio de comunicaciones que necesita un cliente, al cual llamaremos BANCO PERU S.A.C. Los requerimientos mencionados por el cliente son:

- Interconectar las 2 sedes que tiene actualmente su empresa, a las cuales llamaremos Principal y Secundaria, ubicadas en diferentes distritos de Lima.
- Calidad de servicio, el cliente ha revisado el tráfico cursado en su red y los clasifica de 3 tipos: tráfico de Voz (utiliza telefonía IP), tráfico de datos crítico (transacciones comerciales) y tráfico no crítico (por ejemplo correo).

- Anchos de banda en función de los tipos de tráfico que menciona 128 K para Voz, 128 K para sus datos críticos y 128 K para su tráfico de datos no crítico.
- Seguridad en la comunicación entre sus dos sedes.

La red del núcleo MPLS/VPN que hemos desarrollado en el capitulo anterior se ha definido con 3 clases de servicio CoS3, CoS2 y CoS1, por lo que la solución a proponer al cliente BANCO PERU S.A.C consiste en ofrecerle servicios diferenciados que brindaran la calidad de servicio adecuada que requieren sus aplicativos y la seguridad de una red MPLS/VPN.

4.2.- Topología de la red

El backbone MPLS/VPN esta formado por 2 equipos P (Provider) y 2 equipos PE (Provider Edge). Los equipos CPE ubicados en los locales de los clientes se conectan a los equipos PE que están en el borde de la red MPLS. En nuestro ejemplo el cliente cuenta con 2 sedes, Principal y Secundaria, para las cuales se han asignado a los enrutadores CPE1 y CPE2 respectivamente. El router CPE1 estará conectado al router PE1 y el router CPE2 conectado al router PE2, como se muestra en la figura 4.1. En el capitulo 3 se menciono el modelo de los enrutadores que estamos trabajando 12406 XR (P), 7206 VXR (PE) y 2801 (CPE) correspondiente al fabricante Cisco Systems, las especificaciones técnicas de estos equipos se muestran en los anexos correspondientes.

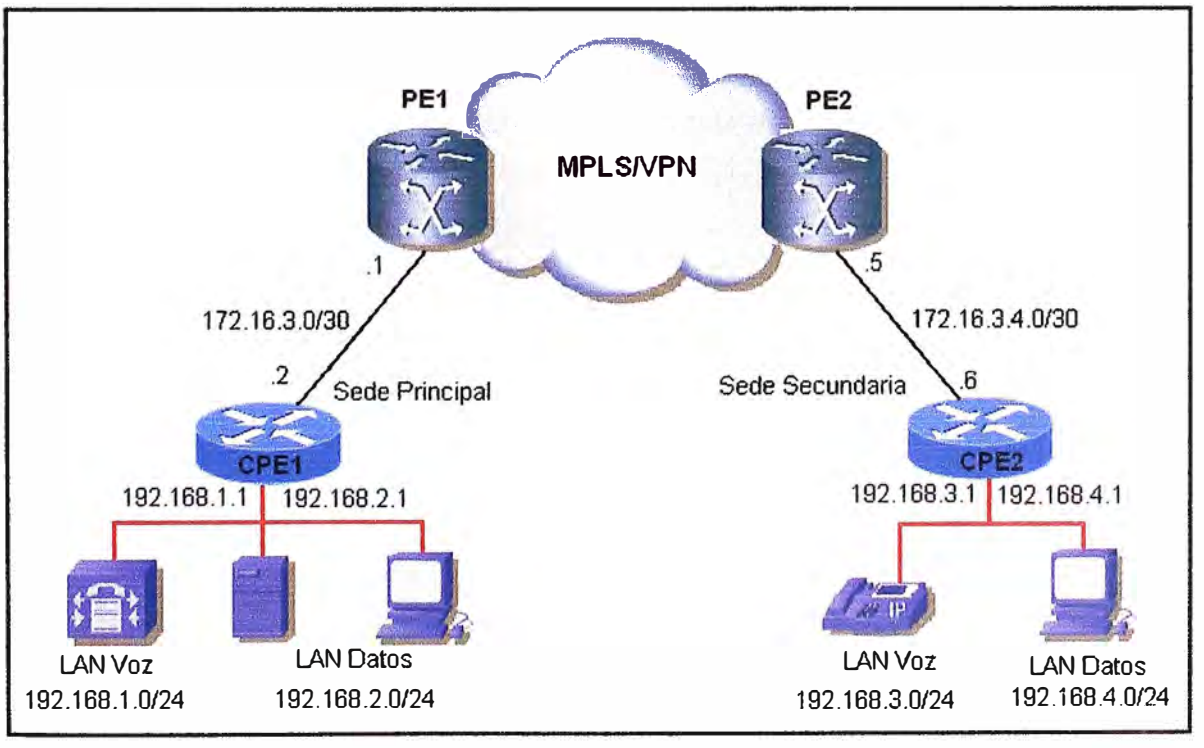

Figura 4.1 Topología de red

4.3 Protocolos de enrutamiento

Los protocolos de enrutamiento se utilizan para ofrecer el servicio hacia los clientes finales en función al tipo de enrutadores involucrados en la comunicación, estas clasificaciones son las siguientes:

4.3.1 Enrutamiento PE - PE

Para la implementación de la red MPLS/VPN es necesario configurar el protocolo de enrutamiento Interno MP-BGP, de esta forma la conectividad de los clientes se realiza con la exportación e importación de los valores correctos para Router Targets (RT). Los prefijos deben ser exportados de una VRF local (VPN Routing and Forwarding) a la sesión MP-BGP y importado nuevamente dentro de la VRF remota.

4.3.2 Enrutamiento PE – CPE

Este enrutamiento permite anunciar las redes del cliente hacia la Red MPLS/VPN local del proveedor de servicios. El intercambio de información de enrutamiento entre los enrutadores CPE y PE puede realizarse utilizando distintos protocolos de enrutamiento, estos pueden ser RIP v2, OSPF, EIGRP, BGP y rutas estáticas. Para nuestro esquema de 2 sedes, principal y secundaria (CPE1 y CPE2 respectivamente) se ha considerado utilizar como protocolo de enrutamiento a BGPv4 entre los enrutadores PE1 y CPE1, y rutas estáticas entre los enrutadores PE2 y CPE2, a continuación se mencionan algunos detalles:

- *Enrutamiento Estático.* En este caso debe configurarse una ruta estática por defecto (0.0.0.0) en el enrutador CPE2 teniendo como siguiente salto al equipo PE2, y configurar en el enrutador PE2 una ruta estática por cada red LAN que se utilice en el enrutador CPE2. PE2 integrará este prefijo a la tabla BGPv4 asociada con la VPN local del cliente utilizando la opción de distribución de redes conectadas y estáticas.
- *Enrutamiento Dinámico BGPv4.* En este caso las redes del cliente deberán ser anunciadas desde el equipo enrutador CPE1 utilizando la opción *network* del protocolo de enrutamiento BGPv4.

4.4 Plan de direccionamiento IP y asignación VPN

En base a los requerimientos de servicios que han sido solicitados por el cliente se ha definido el plan de direccionamiento IP, en la tabla 4.1 se muestran las redes LAN y WAN que se han sido designadas a ser configuradas en los enrutadores CPE1 y CPE2:

Equipo	Red	Mascara	Descripción
CPE1	172.16.3.0	255.255.255.252	Enlace WAN con PE1
	192.168.1.0	255.255.255.0	Red LAN de Voz
	192.168.2.0	255.255.255.0	Red LAN de Datos
CPE2	172.16.3.4	255.255.255.252	Enlace WAN con PE2
	192.168.3.0	255.255.255.0	Red LAN de Voz
	192.168.4.0	255.255.255.0	Red LAN de Datos

Tabla 4.1 Plan de direccionamiento IP

Como se ha definido previamente en los capítulos anteriores en la arquitectura MPLS/VPN se definen 3 elementos:

- *Virtual Routing Forwarding* (VRF). Un VRF es una instancia de enrutamiento y reenvió para una VPN, que puede ser entendido como un enrutador virtual que contiene su propia tabla de enrutamiento junto a su propia tabla envió/conmutación (FIB). Un VRF nos permite definir una VPN independiente para cada cliente, y se configura en los routers PE.
- *Route Distinguiher* (RD). Es un distintivo de ruta que es añadido a cada uno de los prefijos de red aumentando la longitud del prefijo de 32 a 96 bits, RD debe ser diferente para cada VRF.
- *Route Target* (RT). Es un indicador que se anexa a las rutas correspondientes a una VPN y es transportado junto con la información de ruta utilizando MP-BGP, tiene el mismo valor para todas las rutas anunciadas desde un VRF.

Para la implementación de la Red Privada del cliente es necesario que designemos los valores VRF, RD y RT que utilizaremos en la configuración de los equipos enrutadores.
Para nuestro ejemplo se ha definido que los valores de RD deben tener la siguiente sintaxis: RD = ASN:nn, donde ASN es el número de sistema autónomo del proveedor se servicios y nn debe identificar de manera única al cliente dentro de la red MPLS/VPN. Para el ejemplo se ha asignado el sistema autónomo 6500 (pertenece a los sistemas autónomos reservados por la IANA - Internet Assigned Numbers Authority), y 10 como valor de nn para identificar la VPN el cliente.

Descripción	Valor asignado
VRF	VPN_BANCO
RD	65000:10
RT	65000:10

Tabla 4.2 valores asignados a la VPN

Como se observa en la tabla 4.2 hemos definido que *vrf* tiene por nombre VPN_BANCO, el valor de *RD* es 65000:10 y el valor para *RT* también es 65000:10.

4.5 Configuración de la red MPLS/VPN

Para el soporte de VPN sobre la red MPLS es necesario antes implementar el protocolo Interno MP-BGP entre los PEs que nos permitirá el intercambio de prefijos vpnv4. Una vez que se ha habilitado MP-BGP entre los PEs se sigue el siguiente procedimiento para habilitar una VPN en MPLS:

- Se define la VPN en el PE (VRF, RD y RT).
- Se asocia la VPN a la interfase configurada en el PE que conecta al CPE.
- Se configura el enrutamiento PE-CPE.
- Se configura el router CPE que conecta al PE.

4.5.1 Configuración de MP-BGP en PE1 y PE2

El protocolo MP- BGP en un dominio MPLS, nos permite dejar la red preparada para crear servicios de redes privadas virtuales MPLS/VPN, la configuración de multiprotocolo IBGP se realiza entre los pares PE a PE, no es necesario realizarla en los enrutadores P. Sin embargo en redes reales como las de los proveedores de servicio que tienen varios equipos enrutadores P y una cantidad mayor de equipos enrutadores PE, se hace necesario configurar los equipos enrutadores P como reflectores de rutas MP-BGP, ya que no es escalable establecer sesiones BGP entre todos los pares PE (por ejemplo una red con 30 enrutadores PEs). Para nuestro ejemplo vamos a establecer la sesión MP-BGP solamente entre los enrutadores PE1 y PE2, para ello se requiere los siguientes pasos:

a) Configurar el proceso de enrutamiento del protocolo BGP con el número de sistema autónomo con el comando *router bgp*:

Router # configure Terminal
Router (config) # **router bgp** *autonomous-system*

b) Para la pareja de enrutadores PE1 y PE2, se tiene que definir en cada uno al vecino correspondiente y definir la interfaz loopback para la actualización de enrutamiento con el comando *neighbor.*

Router (config-router) # **neighbor** *ip-address* **remote-as** *autonomous-system*
Router (config-router) # **neighbor** *ip-address* **update-source** *loopback0*

c) Se debe activar el anuncio de prefijos IPv4 y vpnv4 con la opción *activate* del comando *neighbor*, previamente se tiene que ingresar al modo de configuración *address-family* correspondiente:

Router (config-router) # **address-family** [ipv4 | ipv6 | vpnv4 | vpnv6]
Router (config-router-af) # **neighbor** *ip-address* **activate**

El número de sistema autónomo que se define en la orden *router bgp* es el que le corresponde al proveedor de servicios, para nuestro caso vamos a utilizar el sistema autónomo 65000 que se encuentra dentro del rango de sistemas autónomos reservados por la IANA (64512 a 65535), a continuación en la figura 4.2 se muestra el procedimiento de configuración del protocolo de enrutamiento BGP en el equipo enrutador PE1 hacia el equipo enrutador PE2.

```
PE1 # configure terminal
PE1 (config) # router bgp 65000
PE1 (config-router) # bgp router-id 172.16.1.3
PE1 (config-router) # neighbor 172.16.1.4 remote-as 65000
PE1 (config-router) # neighbor 172.16.1.4 update-source Loopback0
PE1 (config-router) # neighbor 172.16.1.4 description enlace con PE2
PE1 (config-router) # address-family ipv4
PE1 (config-router-af) # neighbor 172.16.1.4 activate
PE1 (config-router-af) # neighbor 172.16.1.4 next-hop-self
PE1 (config-router-af) # neighbor 172.16.1.4 send-community both
PE1 (config-router-af) # exit
PE1 (config-router) # address-family vpnv4
PE1 (config-router-af) # neighbor 172.16.1.4 activate
PE1 (config-router-af) # neighbor 172.16.1.4 next-hop-self
PE1 (config-router-af) # end
```

Figura 4.2 Procedimiento de configuración de PE1

En la figura 4.2 podemos observar el proceso de configuración del protocolo de enrutamiento dinámico MP-BGP ejecutado en el enrutador PE1, donde se habilita como identificador de la sesión BGP con la dirección IP 172.16.1.3 que corresponde a su interfaz virtual Loopback 0 mediante el comando *bgp router-id*, *172.16.1.3*, para nuestro caso ambos enrutadores PE1 y PE2 deben pertenecen al mismo sistema autónomo 65000. Cuando se activa la sesión BGP con el enrutador vecino en el modo de configuración del *address-family vpnv4* automáticamente se activa el envió de comunidades estándar y extendidas entre ambos enrutadores PE1 y PE2. En las figuras 4.3 y 4.4 se muestran las configuraciones del protocolo de enrutamiento MP-BGP entre los enrutadores PE1 y PE2 luego de ejecutar el procedimiento indicado en la figura 4.2.

También podemos apreciar que por defecto aparece configurado el comando *no auto-summary*, que impide que se envíen rutas resumidas.

Configuración MP-BGP de PE1

```
router bgp 65000
 bgp router-id 172.16.1.3
 bgp log-neighbor-changes
 neighbor 172.16.1.4 remote-as 65000
 neighbor 172.16.1.4 update-source Loopback0
 neighbor 172.16.1.4 description enlace con PE2
 !
 address-family ipv4
 neighbor 172.16.1.4 activate
 neighbor 172.16.1.4 next-hop-self
 neighbor 172.16.1.4 send-community both
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 172.16.1.4 activate
 neighbor 172.16.1.4 next-hop-self
 neighbor 172.16.1.4 send-community both
 exit-address-family
```

Figura 4.3 Configuración MP-BGP de PE1

Configuración MP-BGP de PE2

```
router bgp 65000
 bgp router-id 172.16.1.4
 bgp log-neighbor-changes
 neighbor 172.16.1.3 remote-as 65000
 neighbor 172.16.1.3 update-source Loopback0
 neighbor 172.16.1.3 description enlace con PE1
 !
 address-family ipv4
 neighbor 172.16.1.3 activate
 neighbor 172.16.1.3 next-hop-self
 neighbor 172.16.1.3 send-community both
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 172.16.1.3 activate
 neighbor 172.16.1.3 next-hop-self
 neighbor 172.16.1.3 send-community both
 exit-address-family
```

Figura 4.4 Configuración MP-BGP de PE2

4.5.2 Configuración de VPNs

La arquitectura MPLS soporta la implementación de múltiples VPNs para una gran cantidad de clientes, una de las características que la hacen una solución extremadamente escalable. En la sección anterior se explico la configuración del protocolo de enrutamiento M-BGP, protocolo que es utilizado por la red MPLS para el intercambio de información de enrutamiento de las diferentes redes privadas virtuales entre los enrutadores PE1 y PE2, tener un protocolo de enrutamiento sobre la red MPLS es un requisito previo antes de iniciar la configuración de la VPN. Siguiendo con el desarrollo del capitulo a continuación se explica el procedimiento a seguir para la configuración de una Red Privada Virtual sobre la red MPLS:

a) Configuración de la VRF asociada a la VPN que vamos a configurar en los PE: Una VRF incluye las tablas de envío y enrutamiento de los sitios pertenecientes a una VPN. Los parámetros necesarios para crearla son el *Route Distinguisher* (RD) que permite identificar unívocamente un prefijo de VPN-IPv4 y Route-Target (RT) que identifica los enrutadores que deben recibir la ruta. Para definir una VRF se utiliza el comando *ip vrf*, donde *vrf-name* es el nombre asignado al VRF y debe ser único para identificar la VPN del cliente. En la red todos los enrutadores CPE del cliente deben tener definidas este VRF en los equipos enrutadores PE a donde se conectan.

Router # configure Tterminal
Router (config) # **ip vrf** *vrf-name*
Router (config-vrf) # **rd** *route-distinguer*
Router (config-vrf) # **route-target [import | export | both]** *route-target-ext-comunity*

b) Configuración del reenvió en las interfaces de los enrutadores PE que están conectados a los enrutadores CPE:

Router # configure terminal
Router (config) # **interface** *interfaz*
Router (config-if) # **ip vrf forwarding** v*rf-name*

c) Asignación de la dirección IP a la interfaz donde acabamos de configurar el reenvió dentro de la VPN, ya que pierde el direccionamiento de dicha interfaz. Después de ejecutar este último comando se mostrará un mensaje indicando que en la interfaz anterior se le ha quitado la configuración IP, por lo que habrá que volver a configurarla:

Router (config-if) # **ip address** *ip-address mask*

```
PE1 # configure terminal
PE1 (config) # ip vrf VPN_BANCO
PE1 (config-vrf) # rd 65000:10
PE1 (config-vrf) # route-target export 65000:10
PE1 (config-vrf) # route-target import 65000:10
PE1 (config-vrf) # exit
PE1 (config) # interface GigabitEthernet1/1
PE1 (config-if) # ip vrf forwarding VPN_BANCO
PE1 (config-if) # ip address 172.16.3.2 255.255.255.252
PE1 (config-if) # end
```

Figura 4.5 Procedimiento de configuración VRF en PE1

En las figura 4.5 se muestra el procedimiento realizado para configurar la VRF VPN_BANCO en el enrutador PE1, donde se define el RD 65000:10, la exportación e importación de rutas RT 65000:10 y la asignación de la VRF a la interfaz GE1/1 que se conecta al enrutador CPE2. En la figura 4.6 se muestra la configuración en los enrutadores PE1 y PE2 que se conectan a los enrutadores CPE1 y CPE2 respectivamente. Como se observa en las figuras indicadas se ha definido la misma VRF VPN_BANCO en ambos enrutadores PE1 y PE2, cabe recalcar que la VRF solo se configura en los enrutadores PE, en el caso de los enrutadores P no es necesario porque solo tienen conexiones troncales entre los enrutadores del núcleo MPLS.

Configuración VRF de PE1	Configuración VRF en PE2
ip vrf VPN_BANCO rd 65000:10 route-target export 65000:10 route-target import 65000:10 ! interface GigabitEthernet1/1 ip vrf forwarding VPN_BANCO ip address 172.16.3.2 255.255.255.252	ip vrf VPN_BANCO rd 65000:10 route-target export 65000:10 route-target import 65000:10 ! interface GigabitEthernet1/1 ip vrf forwarding VPN_BANCO ip address 172.16.3.5 255.255.255.252

Figura 4.6 Configuración de la VPN_BANCO en PE1 y PE2

4.5.3 Configuración del enrutamiento PE-CPE

Los enrutadores PE1 y PE2 necesitan ser configurados para intercambiar información de enrutamiento con los enrutadores CPE1 y CPE2 respectivamente, esto se realiza a través de las interfaces que conectan a los enrutadores CPE1 y CPE2 las cuales se encuentran asociadas a su correspondiente VRF. En nuestro caso vamos a configurar enrutamiento dinámico con el protocolo BGP entre los enrutadores PE1 y CPE1; y enrutamiento estático entre los enrutadores PE2 y CPE2 como se muestra en la figura 4.7.

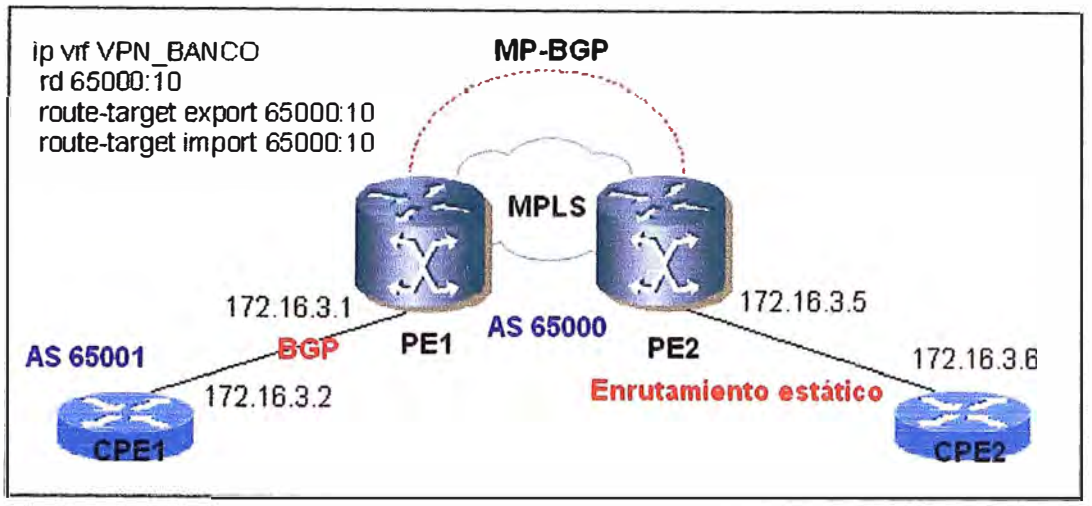

Figura 4.7 Enrutamiento PE-CPE

a) Configuración de enrutamiento BGP entre PE1 y CPE1

Algunos clientes prefieren el intercambio de rutas BGP4 con el proveedor de servicios. La redistribución entre la sesión EBGP del cliente y la sesión MP-iBGP son automáticas. Sin embargo se tiene algunos atributos de BGP como por ejemplo EBGP *multihop* que no son actualmente soportados por la sesión BGP entre los enrutadores PE y el CPE. Cuando realizamos la creación de la VRF automáticamente se crea el *address-family* dentro del proceso BGP del PE, por lo que para configurar el enrutamiento BGP necesitamos ingresar al *address-familiy* correspondiente para la VPN.

Es necesario definir un sistema autónomo para el proceso BGP de CPE1, vamos a asignar el sistema autónomo 65001 también perteneciente al segmento reservado por IANA (Internet Assigned Numbers Authority).

```
PE1 # configure terminal
PE1 (config) # router bgp 65000
PE1 (config-router) # address-family ipv4 vrf VPN_BANCO
PE1 (config-router-af) # neighbor 172.16.3.2 remote-as 65001
PE1 (config-router-af) # neighbor 172.16.3.2 activate
PE1 (config-router-af) # neighbor 172.16.3.2 send-community both
PE1 (config-router-af) # redistribute connected
PE1 (config-router-af) # redistribute static
PE1 (config-router-af) # end
```

Figura 4.8 Procedimiento de configuración BGP en PE1

En la figura 4.8 se observa el procedimiento de configuración de la sesión BGP entre los enrutadores PE1 y CPE1, dentro del address-family VPN_BANCO se define y activa como vecino a CPE2, y se activa el envió de comunidades, así mismo se configura la opción de redistribución de rutas directamente conectadas como es el caso de la WAN

PE1-CPE1. En la figura 4.9 se muestra el procedimiento de configuración del enrutador CPE1, en este caso solo se define el envió de rutas desde el enrutador CPE1 hacia el enrutador PE1, los cuales son prefijos IPv4.

```
CPE1 # configure terminal
CPE1 (config) # router bgp 65001
CPE1 (config-router) # neighbor 172.16.3.1 remote-as 65000
CPE1 (config-router) # address-family ipv4
CPE1 (config-router-af) # neighbor 172.16.3.1 activate
CPE1 (config-router-af) # neighbor 172.16.3.1 send-community both
CPE1 (config-router-af) # network 192.168.1.0 mask 255.255.255.0
CPE1 (config-router-af) # network 192.168.2.0 mask 255.255.255.0
CPE1 (config-router-af) # end
```

Figura 4.9 Procedimiento de configuración BGP de CPE1

En las figuras 4.10 y 4.11 se muestra las configuraciones obtenidas al ejecutar la orden show running-configuration en los enrutadores PE1 y CPE1. Se aprecia la parte de la configuración referida a la sesión BGP que se levanta entre los enrutadores PE1 y CPE1 luego de culminar el proceso de configuración indicado en las figuras 4.8 y 4.9. Como se observa el enrutador PE1 pertenece al sistema autónomo 65000 y establece la sesión BGP con su vecino el enrutador CPE1 que pertenece al sistema autónomo 65001. A diferencia del enrutador PE1 en el enrutador CPE1 no es necesario definir el address-family ipv4 vrf ya que solo es usado en los enrutadores PE que corren MPLS, en el enrutador CPE1 basta con definir la orden address-family ipv4.

Configuración BGP de PE1

```
interface GigabitEthernet1/1
 description Enlace WAN BGP PE1 >> CPE1
 ip vrf forwarding VPN_BANCO
 ip address 172.16.3.1 255.255.255.252
!
router bgp 65000
 !
 address-family ipv4 vrf VPN_BANCO
 redistribute connected
 redistribute static
 neighbor 172.16.3.2 remote-as 65001
 neighbor 172.16.3.2 activate
 neighbor 172.16.3.2 send-community both
 no auto-summary
 no synchronization
 exit-address-family
```

Figura 4.10 Configuración BGP de PE1 hacia CPE1

Configuración BGP de CPE1 hacia PE1

```
interface FastEthernet1/0
 description Enlace WAN BGP CPE1 >> PE1
 ip address 172.16.3.2 255.255.255.252
!
interface FastEthernet1/1
 description Red LAN
 ip address 192.168.1.1 255.255.255.0
 ip address 192.168.2.1 255.255.255.0 secondary
!
router bgp 65001
 bgp log-neighbor-changes
 neighbor 172.16.3.1 remote-as 65000
 !
 address-family ipv4
 neighbor 172.16.3.1 activate
 neighbor 172.16.3.1 send-community both
 no auto-summary
 no synchronization
 network 192.168.1.0 mask 255.255.255.0
 network 192.168.2.0 mask 255.255.255.0
 exit-address-family
```

Figura 4.11 Configuración BGP de CPE1 hacia PE1

b) Configuración de enrutamiento estático entre PE2 y CPE2

Entre PE2 y CPE2 vamos a realizar la configuración de enrutamiento estático, para esto en el enrutador PE2 debemos configurar una ruta estática para cada subred IP de destino que se encuentra en CPE2, las rutas estáticas deben ser definidas en su correspondiente VRF para nuestro caso VPN_BANCO. Así mismo debemos redistribuir las rutas estáticas y directamente conectadas dentro del address-family BGP en el PE2.

Para configurar el enrutamiento estático entre PE2 y CPE2, primero debemos definir las redes que deseamos publicar de CPE2 en PE2 con el comando *ip route vrf*:

Router (config) **# ip route vrf** vrf-name

Luego debemos definir dentro de la sesión BGP la redistribución de rutas estáticas y directamente conectadas, para lo cual utilizamos los comandos *redistribute static y redistribute connected*:

Router (config) **# router bgp** *autonomous-system*
Router (config-router) **# address-family ipv4 vrf** *vrf-name*
Router (config-router-af) **# redistribute static**
Router (config-router-af) **# redistribute connected**

```
PE2 # configure terminal
PE2 (config) # router bgp 65000
PE2 (config-router) # address-family ipv4
PE2 (config-router-af) # redistribute connected
PE2 (config-router-af) # redistribute static
PE2 (config-router-af) # exit
PE2 (config) # ip route vrf VPN_BANCO 192.168.3.0 255.255.255.0 172.16.3.6
PE2 (config) # ip route vrf VPN_BANCO 192.168.4.0 255.255.255.0 172.16.3.6
PE2 (config) # end
```

Figura 4.12 Procedimiento de configuración de rutas estáticas de PE2

En la figura 4.12 podemos observar el procedimiento de configuración de enrutamiento estático que se realiza en el enrutador PE2, donde se publican las 2 redes LAN del enrutador CPE2 (192.168.3.0/24 y 192.168.4.0/24) dentro de la VRF VPN_BANCO y tiene como siguiente salto la dirección IP WAN 172.16.3.6 del enrutador CPE2 que es la que se conecta con el enrutador PE2. En la figura 4.13 se configura en el enrutador CPE2 una ruta por defecto 0.0.0.0/0 que apunta hacia el enrutador PE2. En la figura 4.14 se muestra la configuración parcial terminada del enrutador PE2 respecto al enrutamiento que establece con el enrutador CPE2 y la redistribución hacia el protocolo MP-BGP.

```
CPE2 # configure terminal
CPE2 (config) # ip route 0.0.0.0 0.00.0 172.16.3.5
CPE2 (config) # end
```

Figura 4.13 Procedimiento de configuración de rutas estáticas de CPE2

Configuración PE2

```
interface GigabitEthernet1/1
 description Enlace WAN PE2 >> CPE2
 ip vrf forwarding VPN_BANCO
 ip address 172.16.3.5 255.255.255.252
!
router bgp 65000
 !
 address-family ipv4 vrf VPN_BANCO
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
ip route vrf VPN_BANCO 192.168.3.0 255.255.255.0 172.16.3.6
ip route vrf VPN_BANCO 192.168.4.0 255.255.255.0 172.16.3.6
```

Figura 4.14 Configuración de rutas estática en PE2 hacia CPE2

Configuración CPE2

```
interface FastEthernet1/0
 description Enlace WAN CPE2 >> PE2
 ip address 172.16.3.6 255.255.255.252
!
interface FastEthernet1/1
 description Red LAN
 ip address 192.168.3.1 255.255.255.0
 ip address 192.168.4.1 255.255.255.0 secondary
!
ip route 0.0.0.0 0.00.0 172.16.3.5
```

Figura 4.15 Configuración de rutas estáticas de CPE2

4.5. 4 Verificación del funcionamiento de la VPN-MPLS

Con los siguientes comandos podremos verificar que la red MPLS/VPN que hemos configurado hasta el momento está funcionando según lo esperado:

- **ping vrf** *vrf-name destinatión ip- address.* El funcionamiento es exactamente el mismo que el de un ping normal.
- **show ip vrf.** Muestra información acerca de las VRFs definidas y las interfaces a las que están asociadas.
- **show ip vrf** *vrf-name.* Muestra información de la *vrf-name* y las interfaces que están asociadas a esta *vrf-name*.
- **show ip route vrf** *vrf-name*. Muestra información de la tabla de enrutamiento para la VRF *vrf-name.*
- **show ip protocols vrf** *vrf-name*. Muestra información de los protocolos de enrutamiento activos en la VRF *vrf-name.*
- **show ip cef vrf** *vrf-name*. Nos muestra la tabla de reenvió asociada con el VRF.
- **show ip interface** *interface-number* **vrf** *vrf-name*. Muestra la tabla VRF asociada con la interfase indicada.
- **show ip bgp vpnv4 all.** Muestra la información de enrutamiento de la tabla de prefijos BGP VPN.
- **show ip bgp vpnv4 vrf** vrf-name. Muestra información acerca de BGP VPN asociada con el VRF que se indica. Podemos utilizar las extensiones de este comando para verificar las rutas que estamos enviando o recibiendo desde los CPEs o PEs.
- **show mpls ip forwarding vrf** *vrf-name*. Muestra información del reenvió de etiquetas que corresponden a las rutas anunciadas por el router.

4.6 Calidad de Servicio

La filosofía de una red MPLS/VPN orientada a ofrecer calidad de servicio se basa en la agrupación de los distintos Tipos de Tráfico en un cierto número de clases de servicio con diferentes prioridades. Los paquetes pertenecientes a una misma clase de servicio tienen en común los mismos requerimientos de tratamiento en cuanto a ancho de banda necesario, retardo, variación del retardo (jitter) y pérdida de paquetes, es decir, de calidad de servicio (QoS).

La arquitectura MPLS/DiffServ tiene la capacidad de diferenciación del tráfico a través de toda su trayectoria, en consecuencia las aplicaciones de los clientes deberán ser clasificadas en algunas de las clases de servicios que se van a definir en la red.

Teniendo en consideración que la red MPLS/VPN que estamos implementando es una red administrada, es decir donde se tiene la gestión de los equipos CPE (Customer Premise Equitment), la identificación y marcado del tráfico de cliente deberá realizarse en el equipo CPE. Cada clase de servicio tiene una política de tráfico asociada, por medio de la cual es posible ofrecer los parámetros de SLA asociados al servicio. La capacidad de tener una red que pueda soportar diferentes clases de servicio permite a los proveedores de servicio de telecomunicaciones ofrecer una variedad de combinaciones dependiendo de los requerimientos del cliente, por ejemplo un ancho de banda de 384Kbps dividido en 128 Kbps para CoS3, 128 Kbps para CoS2 y 128 Kbps para CoS1, de esta manera los costos se aplican en base al tipo de servicio y ancho de banda del tipo de servicio.

4.6.1 Tipos y políticas de tráfico

Los tipos de tráfico definidos en la red MPLS/VPN y las políticas aplicables a cada una de ellas son mostradas a continuación:

Descripción	CoS3	CoS2	CoS1
Tipo de datos	Voz y Video	Datos Críticos	Datos no críticos
Prioridad	Máxima	Media	Normal
Precedencia /IP DSCP	P5 / IP DSCP 40	P2 / IP DSCP 16	P1 / IP DSCP 8
Política aplicable al tráfico excedente	Se descarta	Se remarca con P1	No aplica

Tabla 4.3 Tipos y políticas de tráfico

Como se observa en la tabla 4.3 se han definido 3 tipos de clases de servicios CoS3, CoS2 y CoS1. La clase de servicio CoS3 definida para aplicaciones en tiempo real como por ejemplo Multimedia, voz y videoconferencia. La clase de servicio CoS2 asociada a aplicaciones de datos sensibles al retardo y críticas para el negocio como SNA, SAP,

ERP y finalmente la clase de servicio CoS1 para aplicaciones de base de datos, transaccionales, transferencia de archivos.

A continuación se mencionan algunas consideraciones que se tendrán presentes para el aprovisionamiento del servicio:

- En la clase de servicio CoS1, P1 es el valor por defecto para el servicio, en ausencia de tráfico de clase 3 y clase 2, el tráfico asociado con precedencia P1 puede ocupar la totalidad del ancho de banda contratado. En caso de sobrepasar este valor los paquetes será descartados.
- Los anchos de banda de cada una de las clases de servicio (CoS) se ofrecerán como múltiplos de 32Kbps.
- La suma de los anchos de banda asignados para Precedencia 5 (Cos3), Precedencia 2 (CoS2) y Precedencia 1 (CoS1), debe ser igual al ancho de banda del acceso contratado.

4.6.2 Identificación de las clases de servicios

A continuación en la tabla 4.4 se presenta las equivalencias DSCP y Precedencia IP que son utilizadas para identificar el tipo de servicio:

Clase de servicio	Tráfico	IP Precedente (3 bits)	IP DSCP (6 bits)	IP TOS (8 bits)
CoS3	Voz/Video	5 (101)	40 (101000)	160 (10100000)
CoS2	Datos críticos	2 (010)	16 (010000)	64 (01000000)
CoS1	Datos no críticos	1 (001)	8 (001000)	32 (00100000)

Tabla 4.4 Equivalencias Precedencia IP, IP DSCP y IP TOS

4.7 Configuración de calidad de servicio

La arquitectura MPLS/DiffServ permite la creación de diferentes clases de servicios sobre las cuales se aplican diferentes políticas de calidad, en base a diferentes métodos como una estrategia de manejo de los paquetes en caso de congestión, o el evitar que la red alcance este estado, descartando paquetes a medida que estos ingresan a la red. El manejo de congestión es un término general usado para nombrar los distintos tipos de estrategia de encolamiento que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red, controlando la inyección de tráfico a la red, para que ciertos flujos tengan prioridad sobre otros.

Entre los métodos que hacen posible la implementación de calidad de servicio en equipos Cisco tenemos:

- *Condicionamiento del tráfico (traffic policing y traffic shaping).* El condicionamiento del tráfico se lleva a cabo en los extremos del dominio de la red MPLS/DiffServ Los condicionadores de tráfico ejecutan modelado de tráfico y funciones de políticas para asegurar que el tráfico entrante al dominio MPLS/DiffServ cumpla las reglas especificadas.
- *Clasificación de paquetes.* Utiliza un descriptor de tráfico (por ejemplo, DSCP) para categorizar un paquete en un determinado grupo, lo que permite particionar el tráfico en diferentes clases de servicio y niveles de prioridad. Después de que se defina el paquete, se hace accesible para los manejadores de QoS de la red.
- *Marcado de paquetes.* Está relacionado con la clasificación de paquetes. Permite clasificar un paquete basado en un descriptor de tráfico específico (como el valor DSCP). Esta clasificación se puede usar para aplicar servicios diferenciados definidos por el usuario al paquete, y para asociar el paquete con un grupo local de QoS.
- *Gestión de la congestión.* Se consigue con la planificación de tráfico y con la gestión de colas. Cuando hay congestión, un mecanismo como CBWFQ se usa para proporcionar un ancho de banda garantizado a los distintos tipos de tráfico.
- *Evitar la congestión.* Las técnicas para evitar la congestión se centran en los cuellos de botella más comunes, la técnica más usada es WRED. Con WRED y DIffServ, se puede habilitar WRED para usar el valor DSCP cuando WRED calcula la probabilidad de un paquete.

Para la implementación de calidad de servicio en una red MPLS/VPN primero vamos a configurar las clases de servicio para asociar el tráfico de paquetes IP a la clase a la cual corresponda, luego debemos configurar las políticas de servicio que se van a aplicar a cada clase de servicio y finalmente se tiene que asociar la política de servicio a la interfase correspondiente. En los enrutadores CPE adicionalmente se va a configurar el marcado de paquetes en la interfase LAN en base a la clasificación que se realice en la misma interfase, esto con la finalidad que el tráfico desde la red del cliente llegue a la red MPLS/VPN marcado y clasificado.

4.7.1 Configuración de clases de tráfico

CB-WFQ nos permite crear clases de tráfico que consiste en agrupar un tipo de tráfico de la red bajo un mismo concepto, de tal manera que los paquetes agrupados en esa clase pueden tener un mismo tratamiento cuando llegan al router.

Para la creación de clases de tráfico se utiliza el comando *class-map*. Al crear una clase de tráfico conteniendo criterios de equiparación, el comando *class-map* es usado para especificar el nombre de la clase de tráfico, y el comando *match* es usado en el modo de configuración de mapa de clase, para asociar el tráfico a la clase. A continuación se muestra la sintaxis del comando *class-map*:

Router (config) **# class-map [match-any | match-all]** *class-map-name*
Router (config-cmap) **# match** *criteria*

El comando *class-map match-all*, especifica que todos los criterios de equiparación deben darse en el tráfico entrante para poder ser clasificado como parte del tráfico de la clase. El comando *class-map match-any,* especifica que uno de los criterios debe darse para poder clasificar el tráfico entrante como tráfico de clase.
El comando *match* puede tener los siguientes criterios:

- **match ip dscp** *dscp-value*. Configura el criterio de correspondencia para un mapa de clase basado valor IP DSCP. Pueden ser definidos hasta 8 valores DSCP en una sola declaración *match ip dscp.* El rango de valores DSCP es desde 0 a 63.
- **match mpls experimental topmost** *number.* Configura el criterio de correspondencia para un mapa de clase basado en el valor del campo EXP de MPLS. El rango de valores EXP es desde 0 a 7.

Se han definido 3 clases de servicio CoS3_EXP, CoS2_EXP y CoS1_EXP que van a asociarse a las interfaces de los enlaces P – P y P – PE, las cuales clasifican el tráfico en base a los valores del campo EXP de MPLS. Las clases CoS3_EXP, CoS2_EXP y CoS1 EXP están asociadas a los valores EXP 5, 2 y 1 respectivamente. En la figura 4.16 se muestra el procedimiento de configuración de las clases mencionadas en P1.

```
P1 # configure terminal
P1 (config) # class-map match-any CoS3_EXP
P1 (config-cmap) # match mpls experimental topmost 5
P1 (config-cmap) # exit
P1 (config) # class-map match-any CoS2_EXP
P1 (config-cmap) # match mpls experimental topmost 2
P1 (config-cmap) # exit
P1 (config) # class-map match-any Cos1_EXP
P1 (config-cmap) # match mpls experimental topmost 1
P1 (config-cmap) # end
```

Figura 4.16 Procedimiento de configuración de clases en P1

Configuración de clases de servicio en P1 y P2

```
class-map match-any CoS3_EXP
  match mpls experimental topmost 5
class-map match-any CoS2_EXP
  match mpls experimental topmost 2
class-map match-any CoS1_EXP
  match mpls experimental topmost 1
```

Figura 4.17 Configuración de clases de servicio en P1 y P2

También se ha definido las clases de servicio CoS3_DSCP, CoS2_DSCP y CoS1_DSCP que van a asociarse a las interfaces de los enlaces entre los enrutadores PE – CPE. En realidad la clase de servicio CoS3_EXP mencionada anteriormente y la clase de servicio CoS3_DSCP son utilizadas por el mismo tipo de tráfico, sin embargo se han definido con nombres diferentes porque se van a aplicar en interfaces con funciones de clasificación diferentes (CoS3_EXP utiliza el campo EXP mientras CoS3_DSCP utiliza el campo IP DSCP). En la figura 4.18 podemos observa el procedimiento de configuración de las clases mencionadas en el enrutador PE1 y en la figura 4.19 las configuraciones de los enrutadores PE1 y PE2.

```
PE1 # configure terminal
PE1 (config) # class-map match-any CoS3_DSCP
PE1 (config-cmap) # match ip dscp cs5
PE1 (config-cmap) # exit
PE1 (config) # class-map match-any CoS2_DSCP
PE1 (config-cmap) # match ip dscp cs2
PE1 (config-cmap) # exit
PE1 (config) # class-map match-any CoS1_DSCP
PE1 (config-cmap) # match ip dscp cs1
PE1 (config-cmap) # end
```

Figura 4.18 Configuración de clases en PE1

Para la configuración de las clases de servicio en los equipos enrutadores CPE1 y CPE2 ubicados en el local del cliente, hemos llamado a estas mismas 3 de clases de servicio con nombres diferentes de las que se han configurado en los enrutadores P y PE, ya que son las únicas que se definen en los enrutadores CPE1 y CPE2: CoS3, CoS2 y CoS1 que realizan clasificación en base al valor DSCP. En la figura 4.20 podemos observar la configuración de clases de servicio de los enrutadores CPE1 y CPE2, CoS3 (dscp cs5), CoS2 (dscp cs2) y CoS1 (dscp cos1).

Configuración de clases de servicio en PE1 y PE2

```
class-map match-any CoS3_EXP
 match mpls experimental topmost 5
class-map match-any CoS2_EXP
 match mpls experimental topmost 2
class-map match-any Cos1_EXP
 match mpls experimental topmost 1
!
class-map match-any CoS3_DSCP
 match ip dscp cs5
class-map match-any CoS2_DSCP
 match ip dscp cs2
class-map match-any CoS1_DSCP
 match ip dscp cs1
```

Figura 4.19 Configuración de clases de servicio en PE1 y PE2

Clases en CPE1 y CPE2

```
class-map match-any CoS3
 match ip dscp cs5
class-map match-any CoS2
 match ip dscp cs2
class-map match-any CoS1
 match ip dscp cs1
```

Figura 4.20 Configuración de clases de servicio en CPE1 y CPE2

4.7.2 Configuración de políticas de servicio

Para configurar una política de servicio, se usa el comando *policy-map*, que nos permite especificar un nombre a la política de servicio, y a la que se asocian clases de tráfico, definidas previamente. Todo el tráfico que no se equipara con los criterios de las clases, pertenecen a la clase de tráfico por defecto. A continuación se muestra la sintaxis del comando *policy-map*:

Router (config) # **policy-map** *policy-map-name*
Router (config-pmap) # **class** *class-map-name*
Router (config-pmap-c) #

A continuación se mencionan las opciones de configuración en el sudmodo *policy map class* (Router (config-pmap-c) #):

- **bandwidth** [*bandwidth-kbps* | **percent** *percent*]. Especifica un ancho de banda mínimo que se garantiza a una clase de tráfico en periodos de congestión.

- **fair-queue** *number-of-queues*. Especifica un número de colas reservadas para una clase de tráfico (WFQ).
- **police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action*. Especifica un ancho de banda máximo utilizable por una clase de tráfico usando el algoritmo ticket bucket. Las acciones que se pueden tomar son descartar el paquete, cambiar el valor de precedencia y reenviar el paquete, cambiar el valor dscp y reenviar, o solamente reenviar el paquete.
- **priority** [*kbps* | **percent** *percent*] [*bytes*]. Especifica el ancho de banda permitido y garantizado por prioridad de tráfico.
- **random-detect**. Habilita la política WRED (Weighted Random Early Detection) para una clase de tráfico que tiene un ancho de banda garantizado.

En la figura 4.21 se muestra el procedimiento de configuración de las políticas de servicio en P1 realizado en base a los comandos indicados. Como se observa se ha definido la política de servicio policy-map Core-MPLS que se va a aplicar al flujo de tráfico en los enlaces troncales P – P y P- PE. A la clase 3 se ha asignado una cola de prioridad estricta LLQ (*Low Latency Queueing*) reservando el 35% del ancho de banda. Para la clase 2 se ha reservado el 20% del ancho de banda disponible, en situaciones de congestión, activamos un mecanismo de descarte inteligente (*WRED*) que esta asociado. La clase 1 también tiene reservado un 20% del ancho de banda disponible y *WRED* activado. Finalmente, a la clase por defecto se aplica *WFQ* y además activamos *WRED* para descarte inteligente de paquetes.

```
P1 # configure terminal
P1 (config) # policy-map Core-MPLS
P1 (config-pmap) # class CoS3_EXP
P1 (config-pmap-c) # priority percent 35
P1 (config-pmap-c) # exit
P1 (config-pmap) # class CoS2_EXP
P1 (config-pmap-c) # bandwidth percent 20
P1 (config-pmap-c) # random-detect precedence 2
P1 (config-pmap-c) # exit
P1 (config-pmap) # class CoS1_EXP
P1 (config-pmap-c) # bandwidth percent 20
P1 (config-pmap-c) # random-detect precedence 1
P1 (config-pmap-c) # exit
P1 (config-pmap) # class class-default
P1 (config-pmap-c) # fair-queue
P1 (config-pmap-c) # random-detect precedence 0
P1 (config-pmap-c) # end
```

Figura 4.21 Procedimiento de configuración en P1

Configuración de políticas de servicio de P1 y P2

```
policy-map Core-MPLS
 class CoS3_EXP
  priority percent 35
 class CoS2_EXP
  bandwidth percent 20
  random-detect precedence 2
 class CoS1_EXP
  bandwidth percent 20
  random-detect precedence 1
 class class-default
  fair-queue
  random-detect precedence 0
```

Figura 4.22 Configuración de políticas de servicio en P1 y P2

Configuración de políticas de servicio en PE1 y PE2

```
policy-map Core-MPLS
 class CoS3_EXP
  priority percent 35
 class CoS2_EXP
  bandwidth percent 20
  random-detect precedence 2
 class CoS1_EXP
  bandwidth percent 20
  random-detect precedence 1
 class class-default
  fair-queue
  random-detect precedence 0
!
policy-map VPN_BANCO_CPE_IN
 class class-default
  shape average 384000
!
policy-map VPN_BANCO_CPE_OUT
 class CoS3_DSCP
  priority 128
  police 128000 24000 48000 conform-action transmit exceed-action drop
 class CoS2_DSCP
  bandwidth 128
  police 128000 24000 48000 conform-action transmit  exceed-action set-dscp-transmit cs1
 class CoS1_DSCP
  bandwidth 128
 class class-default
  fair-queue
```

Figura 4.23 Configuración de políticas de servicio de PE1 y PE2

Para PE1 y PE2 se van a configurar adicionalmente las políticas de servicio que están asociadas a las clases definidas como CoS3_DSCP, CoS2_DSCP y CoS1_DSCP.

En la figura 4.23 se observa que se ha configurado las políticas de servicio VPN_BANCO_CPE_IN y VPN_BANCO_CPE_OUT que se van a aplicar al tráfico entrante y saliente en las interfaces de los enrutadores PE1 y PE2 que conectan a los enrutadores CPE1 y CPE2 respectivamente. En la figura 4.24 se muestra la configuración de las políticas de servicio aplicadas en los enrutadores CPE1 y CPE2.

Configuración de políticas de servicio en CPE1 y CPE2

```
policy-map wan
 class CoS3
  priority 128
   police 128000 24000 48000 conform-action transmit  exceed-action drop
 class CoS2
  bandwidth 128
   police 128000 24000 48000 conform-action transmit  exceed-action set-dscp-transmit cs1
 class CoS1
  bandwidth 128
 class class-default
  fair-queue
policy-map Shape384
 class class-default
  shape average 384000
  service-policy wan
```

Figura 4.24 Configuración de políticas de servició en CPE1 y CPE2

4.7.3 Configuración de la política de servicio asociada a la interfaz

Para asociar una política de servicio a una interfaz, y especificar la dirección en la cual debe aplicarse la política (paquetes entrantes o paquetes salientes), se utiliza el comando *service-policy* en el modo de configuración de la interfaz.

Router (config) # interface *interface-type*
Router (config-if) # **service-policy {input | output}** *policy-map-name*

En la configuración siguiente de la figura 4.25 se muestra las políticas de servicios asociadas a las interfaces del enrutador PE1. Por ejemplo la política de servicio llamada Core-MPLS ha sido asignada y configurada a la interfase GE1/0 del enrutador PE1 (aplicada solamente para el tráfico saliente que fluye en dirección del enrutador PE1 hacia el enrutador P1) y las políticas de servicios llamadas VPN_BANCO_CPE_IN y VPN_BANCO_CPE_OUT han sido asociadas al tráfico entrante y saliente de la interfase GE 1/1 del enrutador PE1 que se conecta con el enrutador CPE1.

```
PE1 (config) # configure terminal
PE1 (config) # interface GigabitEthernet1/0
PE1 (config-if) # service-policy output Core-MPLS
PE1 (config-if) #exit
PE1 (config) # interface GigabitEthernet1/1
PE1 (config-if) # service-policy input VPN_BANCO_CPE_IN
PE1 (config-if) # service-policy output VPN_BANCO_CPE_OUT
```

Figura 4.25 Procedimiento de configuración en la interfaces de PE1

4.7.4 Marcado de paquetes en el CPE

El marcado de paquetes se va a realizar en los equipos CPE1 y CPE2 en el tráfico de entrada a la interfase LAN. Para el ejemplo se ha asumido que las redes de Voz (CoS3) 192.168.1.0/24 y 192.168.3.0/24 en la sede principal y secundaria respectivamente, se marcaran con DSCP 5. El tráfico de datos crítico (CoS2) se ha considerado como el tráfico desde cualquier PC hacia el servidor con IP 192.168.2.2 ubicado en la sede principal, será marcado con DSCP 2. Finalmente el tráfico que no cumpla con ninguna de las características mencionadas será considerado como tráfico CoS1 y será marcado con DSCP 1. En la figura 4.26 se muestra la configuración de marcado de paquetes de CPE1.

Configuración de marcado de paquetes en CPE1

```
class-map match-any P3
 match access-group name CoS3
class-map match-any P2
 match access-group name CoS2
!
policy-map SetDscpLan
 class P3
  set ip dscp cs5
 class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1
!
interface FastEthernet1/1
 description RED LAN
 ip address 192.168.2.1 255.255.255.0 secondary
 ip address 192.168.1.1 255.255.255.0
 service-policy input SetDscpLan
!
ip access-list extended CoS3
 permit ip 192.168.1.0 0.0.0.255 any
ip access-list extended CoS2
 permit ip host 192.168.2.2 any
```

Figura 4.26 Configuración de marcado de paquetes en CPE1

4.7.5 Verificación de la configuración de calidad de servicio

Par la verificación de la configuración y funcionamiento de las políticas aplicadas se tiene los siguientes comandos:

- **show class-map**. Muestra la información de las clases de tráfico
- **show policy-map**. Muestra todas las políticas de servicio configuradas.
- **Show policy-map** *interface.* Muestra la configuración y estadísticas de entrada y salida asociadas a una interfase en particular, el comando show policy-map tiene muchas otras opciones mas especificas, que podemos consultarla con el signo de interrogación a continuación del comando *show policy-map.*

4.8 Configuración final de los equipos P, PE y CPE

A continuación se muestra la configuración final de los equipos P1, P2, PE1, PE2, CPE1 y CPE2, incluyendo la configuración OSPF, MPLS, BGP, VPN y Calidad de Servicio.

4.8.1 Configuración final de P1

```
hostname P1
¡
ip subnet-zero
¡
ip cef
¡
class-map match-any CoS3_EXP
 match mpls experimental topmost 5
class-map match-any CoS2_EXP
 match mpls experimental topmost 2
class-map match-any CoS1_EXP
 match mpls experimental topmost 1
¡
policy-map Core-MPLS
 class CoS3_EXP
  priority percent 35
 class CoS2_EXP
  bandwidth percent 20
  random-detect precedence 2
 class CoS1_EXP
  bandwidth percent 20
  random-detect precedence 1
 class class-default
  fair-queue
  random-detect precedence 0
¡
mpls label protocol ldp
no mpls ip propagate-ttl
mpls ldp router-id Loopback0 force
¡
interface Loopback0
```

```
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.1 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS P1 >> P2 GE 1/0
 ip address 172.16.2.1 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427191B2E3E69797578
 mpls ip
 service-policy output Core-MPLS
¡
interface GigabitEthernet1/1
 description Enlace MPLS P1 >> PE1 GE 1/1
 ip address 172.16.2.5 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427191B2E3E45857438
 mpls ip
 service-policy output Core-MPLS
¡
router ospf 1
 router-id 172.16.1.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.1 0.0.0.0 area 0
 network 172.16.2.0 0.0.0.3 area 0
 network 172.16.2.4 0.0.0.3 area 0
¡
ip classless
```

4.8.2 Configuración final de P2

```
hostname P2
¡
ip subnet-zero
¡
ip cef
¡
class-map match-any CoS3_EXP
 match mpls experimental topmost 5
class-map match-any CoS2_EXP
 match mpls experimental topmost 2
class-map match-any CoS1_EXP
 match mpls experimental topmost 1
¡
policy-map Core-MPLS
 class CoS3_EXP
  priority percent 35
 class CoS2_EXP
  bandwidth percent 20
  random-detect precedence 2
 class CoS1_EXP
  bandwidth percent 20
  random-detect precedence 1
 class class-default
  fair-queue
```

```
 random-detect precedence 0
¡
mpls label protocol ldp
no mpls ip propagate-ttl
mpls ldp router-id Loopback0 force
¡
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.2 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS P2 >> P1 GE 1/0
 ip address 172.16.2.2 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427345B2E3E69796134
 mpls ip
 service-policy output Core-MPLS
!
interface GigabitEthernet1/1
 description Enlace MPLS P2 >> PE2 GE 1/1
 ip address 172.16.2.9 255.255.255.252
 ip ospf message-digest-key 1 md5 7 132427345B2E3E61122135
 mpls ip
 service-policy output Core-MPLS
!
router ospf 1
 router-id 172.16.1.2
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.2 0.0.0.0 area 0
 network 172.16.2.0 0.0.0.3 area 0
 network 172.16.2.8 0.0.0.3 area 0
¡
ip classless
```

4.8.3 Configuración final de PE1

```
hostname PE1
¡
ip subnet-zero
¡
ip cef
¡
ip vrf VPN_BANCO
 rd 65000:10
 route-target export 65000:10
 route-target import 65000:10
¡
class-map match-any CoS3_EXP
 match mpls experimental topmost 5
class-map match-any CoS2_EXP
 match mpls experimental topmost 2
class-map match-any CoS1_EXP
 match mpls experimental topmost 1
```

```
!
class-map match-any CoS3_DSCP
 match ip dscp cs5
class-map match-any CoS2_DSCP
 match ip dscp cs2
class-map match-any CoS1_DSCP
 match ip dscp cs1
!
policy-map Core-MPLS
 class CoS3_EXP
  priority percent 35
 class CoS2_EXP
  bandwidth percent 20
  random-detect precedence 2
 class CoS1_EXP
  bandwidth percent 20
  random-detect precedence 1
 class class-default
  fair-queue
  random-detect precedence 0
!
policy-map VPN_BANCO_CPE_IN
 class class-default
  shape average 384000
!
policy-map VPN_BANCO_CPE_OUT
 class CoS3_DSCP
  priority 128
  police 128000 24000 48000 conform-action transmit exceed-action drop
 class CoS2_DSCP
  bandwidth 128
  police 128000 24000 48000 conform-action transmit  exceed-action set-dscp-transmit
cs1
 class CoS1_DSCP
  bandwidth 128
 class class-default
  fair-queue
!
mpls label protocol ldp
no mpls ip propagate-ttl
mpls ldp router-id Loopback0 force
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.3 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS PE1 >> P1 GE 1/1
 ip address 172.16.2.6 255.255.255.252
 ip ospf message-digest-key 1 md5 7 152417345B2E3E68196154
 mpls ip
 service-policy output Core-MPLS
!
interface GigabitEthernet1/1
```

```
 description Enlace MPLS PE1 >> CEP1 FE 1/0
 ip vrf forwarding VPN_BANCO
 ip address 172.16.3.1 255.255.255.252
 service-policy input VPN_BANCO_CPE_IN
 service-policy output VPN_BANCO_CPE_OUT
!
router ospf 1
 router-id 172.16.1.3
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.3 0.0.0.0 area 0
 network 172.16.2.4 0.0.0.3 area 0
!
router bgp 65000
 bgp router-id 172.16.1.3
 bgp log-neighbor-changes
 neighbor 172.16.1.4 remote-as 65000
 neighbor 172.16.1.4 update-source Loopback0
 neighbor 172.16.1.4 description enlace con PE2
 !
 address-family ipv4
 neighbor 172.16.1.4 activate
 neighbor 172.16.1.4 next-hop-self
 neighbor 172.16.1.4 send-community both
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 172.16.1.4 activate
 neighbor 172.16.1.4 next-hop-self
 neighbor 172.16.1.4 send-community both
 exit-address-family
 !
 address-family ipv4 vrf VPN_BANCO
 redistribute connected
 redistribute static
 neighbor 172.16.3.2 remote-as 65001
 neighbor 172.16.3.2 activate
 neighbor 172.16.3.2 send-community both
 neighbor 172.16.3.2 description enlace con CPE1
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
```

4.8.4 Configuración final de PE2

```
hostname PE2
!
ip subnet-zero
```

```
ip cef
!
ip vrf VPN_BANCO
 rd 65000:10
 route-target export 65000:10
 route-target import 65000:10
!
class-map match-any CoS3_EXP
 match mpls experimental topmost 5
class-map match-any CoS2_EXP
 match mpls experimental topmost 2
class-map match-any CoS1_EXP
 match mpls experimental topmost 1
!
class-map match-any CoS3_DSCP
 match ip dscp cs5
class-map match-any CoS2_DSCP
 match ip dscp cs2
class-map match-any CoS1_DSCP
 match ip dscp cs1
!
policy-map Core-MPLS
 class CoS3_EXP
  priority percent 35
 class CoS2_EXP
  bandwidth percent 20
  random-detect precedence 2
 class CoS1_EXP
  bandwidth percent 20
  random-detect precedence 1
 class class-default
  fair-queue
  random-detect precedence 0
!
policy-map VPN_BANCO_CPE_IN
 class class-default
  shape average 384000
!
policy-map VPN_BANCO_CPE_OUT
 class CoS3_DSCP
  priority 128
  police 128000 24000 48000 conform-action transmit exceed-action drop
 class CoS2_DSCP
  bandwidth 128
  police 128000 24000 48000 conform-action transmit  exceed-action set-dscp-transmit
cs1
 class CoS1_DSCP
  bandwidth 128
 class class-default
  fair-queue
!
mpls label protocol ldp
no mpls ip propagate-ttl
mpls ldp router-id Loopback0 force
```

```
!
interface Loopback0
 description Proceso BGP – OSPF - MPLS
 ip address 172.16.1.4 255.255.255.255
!
interface GigabitEthernet1/0
 description Enlace MPLS PE2 >> P2 GE 1/1
 ip address 172.16.2.10 255.255.255.252
 ip ospf message-digest-key 1 md5 7 143427345B2E3E69796128
 mpls ip
service-policy output Core-MPLS
!
interface GigabitEthernet1/1
 description Enlace MPLS PE2 >> CEP2 FE 1/0
 ip vrf forwarding VPN_BANCO
 ip address 172.16.3.5 255.255.255.252
 service-policy input VPN_BANCO_CPE_IN
 service-policy output VPN_BANCO_CPE_OUT
!
router ospf 1
 router-id 172.16.1.4
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 0 authentication message-digest
 network 172.16.1.4 0.0.0.0 area 0
 network 172.16.2.8 0.0.0.3 area 0
!
router bgp 65000
 bgp router-id 172.16.1.4
 bgp log-neighbor-changes
 neighbor 172.16.1.3 remote-as 65000
 neighbor 172.16.1.3 update-source Loopback0
 neighbor 172.16.1.3 description enlace con PE1
 !
 address-family ipv4
 neighbor 172.16.1.3 activate
 neighbor 172.16.1.3 next-hop-self
 neighbor 172.16.1.3 send-community both
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 172.16.1.3 activate
 neighbor 172.16.1.3 next-hop-self
 neighbor 172.16.1.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf VPN_BANCO
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
```

```
!
ip classless
ip route vrf VPN_BANCO 192.168.3.0 255.255.255.0 172.16.3.6
ip route vrf VPN_BANCO 192.168.4.0 255.255.255.0 172.16.3.6
```

4.8.5 Configuración final de CPE1

```
hostname CPE1
!
ip subnet-zero
!
ip cef
!
class-map match-any CoS3
 match ip dscp cs5
class-map match-any CoS2
 match ip dscp cs2
class-map match-any CoS1
 match ip dscp cs1
class-map match-any P3
 match access-group name CoS3
class-map match-any P2
 match access-group name CoS2
!
policy-map SetDscpLan
 class P3
  set ip dscp cs5
 class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1
policy-map wan
 class CoS3
  priority 128
   police 128000 24000 48000 conform-action transmit  exceed-action drop
 class CoS2
  bandwidth 128
   police 128000 24000 48000 conform-action transmit  exceed-action set-dscp-transmit
cs1
 class CoS1
  bandwidth 128
 class class-default
  fair-queue
policy-map Shape384
 class class-default
  shape average 384000
  service-policy wan
!
interface FastEthernet1/0
 description Enlace WAN BGP CPE1 >> PE1
 ip address 172.16.3.2 255.255.255.0
 service-policy output Shape384
!
interface FastEthernet1/1
```

```
 description RED LAN
 ip address 192.168.2.1 255.255.255.0 secondary
 ip address 192.168.1.1 255.255.255.0
 service-policy input SetDscpLan
!
router bgp 65001
 bgp log-neighbor-changes
 neighbor 172.16.3.1 remote-as 65000
 neighbor 172.16.3.1 description enlace con PE1
 !
 address-family ipv4
 neighbor 172.16.3.1 activate
 neighbor 172.16.3.1 send-community both
 no auto-summary
 no synchronization
 network 192.168.1.0 mask 255.255.255.0
 network 192.168.2.0 mask 255.255.255.0
 exit-address-family
!
ip classless
!
ip access-list extended CoS3
 permit ip 192.168.1.0 0.0.0.255 any
ip access-list extended CoS2
 permit ip host 192.168.2.2 any
```

4.8.6 Configuración final de CPE2

```
hostname CPE2
!
ip subnet-zero
!
ip cef
!
class-map match-any CoS3
 match ip dscp cs5
class-map match-any CoS2
 match ip dscp cs2
class-map match-any CoS1
 match ip dscp cs1
class-map match-any P3
 match access-group name CoS3
class-map match-any P2
 match access-group name CoS2
!
policy-map SetDscpLan
 class P3
  set ip dscp cs5
 class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1
policy-map wan
 class CoS3
```

```
  priority 128
   police 128000 24000 48000 conform-action transmit  exceed-action drop
 class CoS2
  bandwidth 128
   police 128000 24000 48000 conform-action transmit  exceed-action set-dscp-transmit
cs1
 class CoS1
  bandwidth 128
 class class-default
  fair-queue
policy-map Shape384
 class class-default
  shape average 384000
  service-policy wan
!
interface FastEthernet1/0
 description Enlace WAN BGP CPE2 >> PE2
 ip address 172.16.3.6 255.255.255.0
 service-policy output Shape384
!
interface FastEthernet1/1
 description RED LAN
 ip address 192.168.4.1 255.255.255.0 secondary
 ip address 192.168.3.1 255.255.255.0
 service-policy input SetDscpLan
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.3.5
!
ip access-list extended CoS3
 permit ip 192.168.3.0 0.0.0.255 any
ip access-list extended CoS2
 permit ip any host 192.168.2.2
```

4.9 Pruebas de verificación de la red MPLS

Con la finalidad de validar las configuraciones realizadas previamente para la implementación de la red MPLS y su aplicación para el soporte de Calidad de Servicio se han realizado algunas pruebas que nos permiten corroborar el tratamiento que recibe el tráfico de las diferentes aplicaciones del cliente en la red.

En el inicio del capitulo IV se definieron algunos requerimientos mínimos para la VPN Corporativa del cliente BANCO PERU S.A.C que son los siguientes:

- Interconectar las 2 sedes a través de la red MPLS, llamadas sedes Principal y Secundaria, ubicadas en diferentes distritos de Lima.
- Calidad de servicio, en base al análisis del tráfico cursado en la red del cliente, que se clasifica de 3 tipos: tráfico de Voz (utiliza telefonía IP), tráfico de datos críticos

(transacciones comerciales) y tráfico no crítico (por ejemplo correo y acceso a Internet).

• Anchos de banda en función de los tipos de tráfico que utiliza 128 Kbps para Voz (CoS3), 128 Kbps para sus datos críticos (CoS2) y 128 Kbps para su tráfico de datos no crítico (CoS1).

Las configuraciones realizadas en los enrutadores de la red del núcleo MPLS así como en los enrutadores CPE nos permiten cubrir los requerimientos solicitados por el cliente aplicando políticas de calidad a las 3 clases de servicios que hemos definido en base a la integración de la arquitectura MPLS y DiffServ, a continuación se menciona el comportamiento de las políticas de calidad de servicio que se aplica a las 3 clases de servicio solicitas CoS3, CoS2 y CoS1:

- CoS3 (128 K): La red MPLS asigna la más alta prioridad al tráfico de esta clase, su tratamiento esta priorizado sobre cualquier otro tipo de tráfico, durante la congestión la red garantiza que el cliente puede llegar a utilizar los 128 Kbps contratados manteniendo los mismos tiempos de respuesta que en una situación normal, requisito importante para el buen establecimiento de una comunicación de telefonía IP o una video conferencia. Una característica importante a resaltar se presenta cuando el trafico CoS3 del cliente excediera los 128 K contratados, será descartado, como sabemos en una comunicación de telefonía IP es posible tolerar un porcentaje mínimo de perdida de paquetes no así el retardo. En ausencia de tráfico CoS3 el ancho de banda es aprovechado por las otras clases de servicio.
- CoS2 (128 K): A diferencia del tráfico CoS3 puede tolerar mayores retardos, sin embargo son más sensibles a la pérdida de paquetes, por lo cual el tratamiento que reciben en la red tiene otro comportamiento. Para el caso del CoS2 se ha configurado garantizar un mínimo de 128 K, es decir durante la congestión el cliente puede utilizar los 128 K contratados, sin embargo podría percibir que los tiempos de respuesta se elevan. Cuando se excede los 128 K garantizados para el tráfico CoS2, este se remarca como tráfico CoS1 y pasa a utilizar el ancho de banda reservado para el CoS1 pudiendo llegar a copar el ancho de banda total del enlace.
- CoS1 (128 K): Son menos sensible al retardo y la pérdida de paquetes, como es el caso del correo, acceso a Internet, etc. Para este tipo de tráfico de igual manera se ha garantizado un mínimo de 128 K, en ausencia de tráfico tipo CoS3 y CoS2 puede llegar a utilizar el ancho de banda total del enlace es decir la suma del CoS3, CoS2 y CoS1 (384 K).

Durante las pruebas para la generación de tráfico se utilizó la herramienta ping de los enrutadores Cisco que permite enviar paquetes de diferentes tamaños y marcar el campo Tipo de Servicio del paquete IP dependiendo del tipo de clase de tráfico que deseamos generar, CoS3 (160), CoS2 (32) y CoS1 (16). Como se observará en las gráficas posteriores las pruebas se realizaron por aproximadamente 4 horas, dividiéndolas en 5 escenarios A, B, C, D y E. Cabe mencionar que el muestreo realizado para la construcción de las gráficas se realiza cada 5 minutos, siendo las gráficas un aproximado del tráfico real, ya que entre cada muestra fluye gran cantidad de tráfico que no se captura.

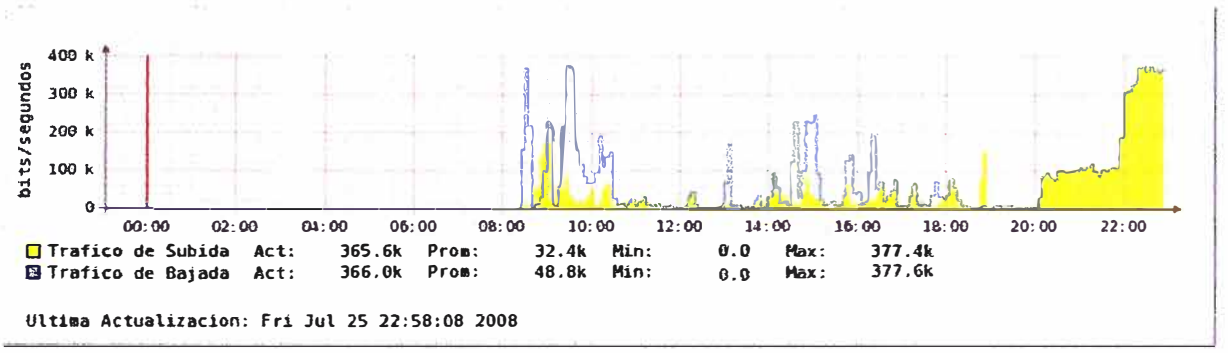

Figura 4.27 Tráfico total cursado en el enlace

La primera gráfica que se presenta de las pruebas realizadas se muestra en la figura 4.27 donde se puede observar el tráfico cursado en ambos sentidos durante las pruebas, las cuales se iniciaron a las 20:00 horas, inicialmente observamos que se mantiene constante por algún tiempo en aproximadamente 100K (en la practica se llego a saturar el CoS3 con 128K sin embargo como se menciono anteriormente se toman muestras cada 5 minutos lo que genera una gráfica aproximada), tiempo en el que se genero únicamente tráfico de clase CoS3, luego se aprecia que el tráfico se elevada llegando al valor máximo del ancho de banda total 384K, en esta parte se genero tráfico de clase de servicio CoS3, CoS2 y CoS1.

El programa que crea la gráfica del tráfico cursado que se observa en la figura 4.27 obtiene los valores utilizando el comando show interfaces en los enrutadores Cisco que nos permite visualizar el comportamiento del trafico en una interfase especifica, por ejemplo en la figura 4.28 se observa la salida del comando show interfaces aplicado a la interfase FE1/0 del enrutador CPE1, donde podemos apreciar que la parte sombreada indica el trafico de entrada y salida de la interfase en bits por segundo o paquetes por segundo que esta cursando al momento de la captura, adicionalmente indica otros valores que nos permiten detectar posibles problemas en la interfase.

```
CPE1 # show interfaces FastEthernet1/0
FastEthernet1/0 is up, line protocol is up
  Hardware is AmdFE, address is 0012.4311.3f61 (bia 0012.4311.3f61)
  Description: Enlace WAN BGP CPE1 >> PE1
  Internet address is 172.16.3.2/23
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 3d21h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 15000 bits/sec, 15 packets/sec
  30 second output rate 8000 bits/sec, 8 packets/sec
     26822578 packets input, 893787195 bytes
     Received 563109 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     22229762 packets output, 452528810 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Figura 4.28 Muestra la salida del comando show interfaces

A continuación en la figura 4.29 se muestra también una gráfica del tráfico total cursado en el enlace, pero con mayores detalles ya que se observa el trafico diferenciado por clase de servicio, en la parte superior del eje horizontal se muestra el trafico saliente o de subida que fluye en sentido CPE1 a CPE2 (sede principal a sede secundaria), y en la parte inferior del eje el tráfico que fluye de retorno o bajada de CPE2 a CPE1 (sede secundaria a sede principal), así mismo indica los valores actuales del tipo de tráfico en el momento de la captura, mínimo, promedio y máximo registrado durante el periodo de pruebas. En las figuras 4.30, 4.31 y 4.32 se muestra el tráfico de clase CoS3, CoS2 y CoS1 respectivamente cursado en la red privada del cliente.

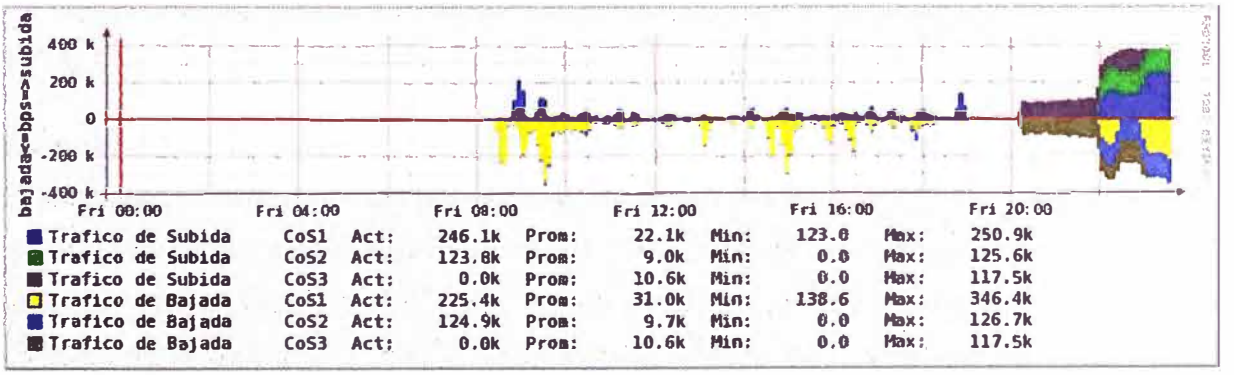

Figura 4.29 Tráfico total diferenciado por clase de servicio

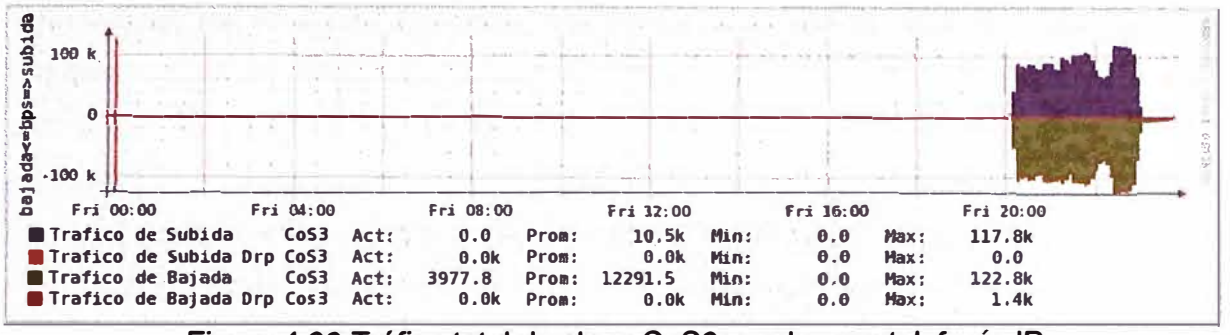

Figura 4.30 Tráfico total de clase CoS3 usado para telefonía IP

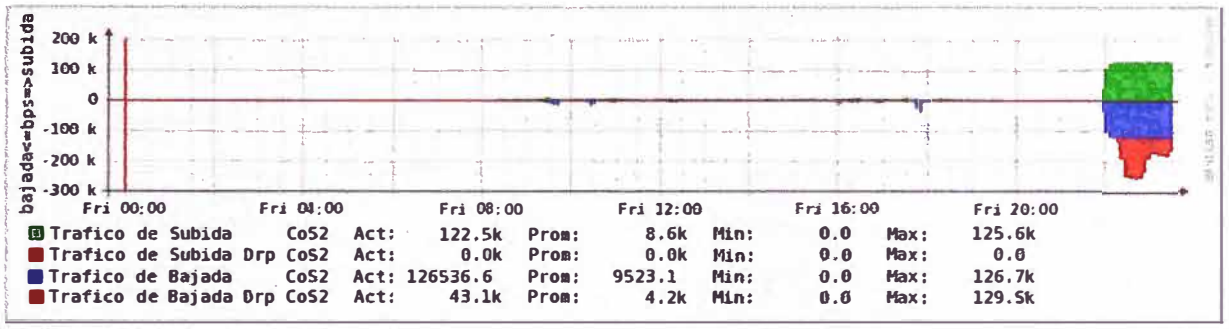

Figura 4.31 Tráfico total de clase CoS2 usado para datos críticos

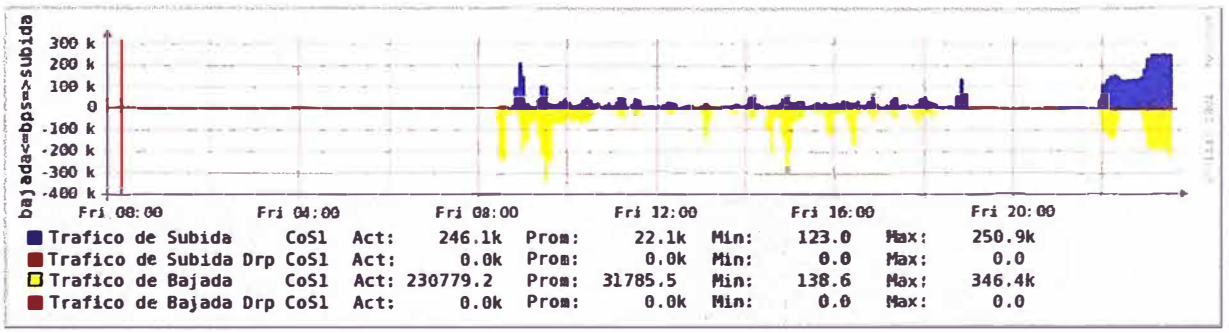

Figura 4.32 Tráfico total de clase CoS1 usado para datos no críticos

Con la finalidad de mostrar más a detalle el comportamiento que presento las clases de tráfico generado durante las pruebas se ha ampliado la figura 4.29 obteniendo la figura 4.33 donde podemos apreciar los escenarios de pruebas A, B, C, D y E, escenarios en los cuales hemos realizado diferentes pruebas para validar el funcionamiento de la red MPLS y su aplicación de calidad de servicio y redes privadas virtuales.

Escenario A

El escenario A tiene por finalidad verificar el comportamiento de la red MPLS para la red privada del cliente cuando se tiene solamente tráfico de clase CoS3 sin presencia de tráfico de clase CoS2 y CoS1. Para ello se genero únicamente tráfico de CoS3 (tráfico utilizado para telefonía IP) marcando el campo Tipo de Servicio de los paquetes IP con valor 160 que es el equivalente para el campo DSCP y EXP que se utiliza en los

enrutadores de la red MPLS para clasificar el tráfico de clase CoS3, y aplicarle las políticas de calidad correspondiente. Se realizaron 2 tipos de pruebas, generando tráfico sin llegar a la capacidad total de 128K y saturando los 128 K, resultados que se comentan a continuación:

- Inicialmente se realizaron pruebas de envío de tráfico de clase CoS3 a través de la red privada del cliente sin llegar a saturar el ancho de banda contratado de 128K, observando que no se registran pérdidas de paquetes, no se presenta encolamiento y los tiempos de respuesta se mantienen estables y con niveles óptimos. En la figura 4.34 se presenta la salida de ejecutar el comando ping en el enrutador CPE1 ubicado en la sede principal del cliente, con una muestra pequeña de solo 500 paquetes enviados hacia la dirección IP 192.168.3.1 de la red LAN del enrutador CPE2, paquetes que están siendo marcados para ser del tipo de clase de servicio CoS3, se puede observar que el éxito de la llegada de paquetes es del 100 % (0 % de pérdida de paquetes) y los tiempos respuesta se mantiene en promedio en 3 milisegundos, con un máximo de 8 milisegundos en algunos paquetes.

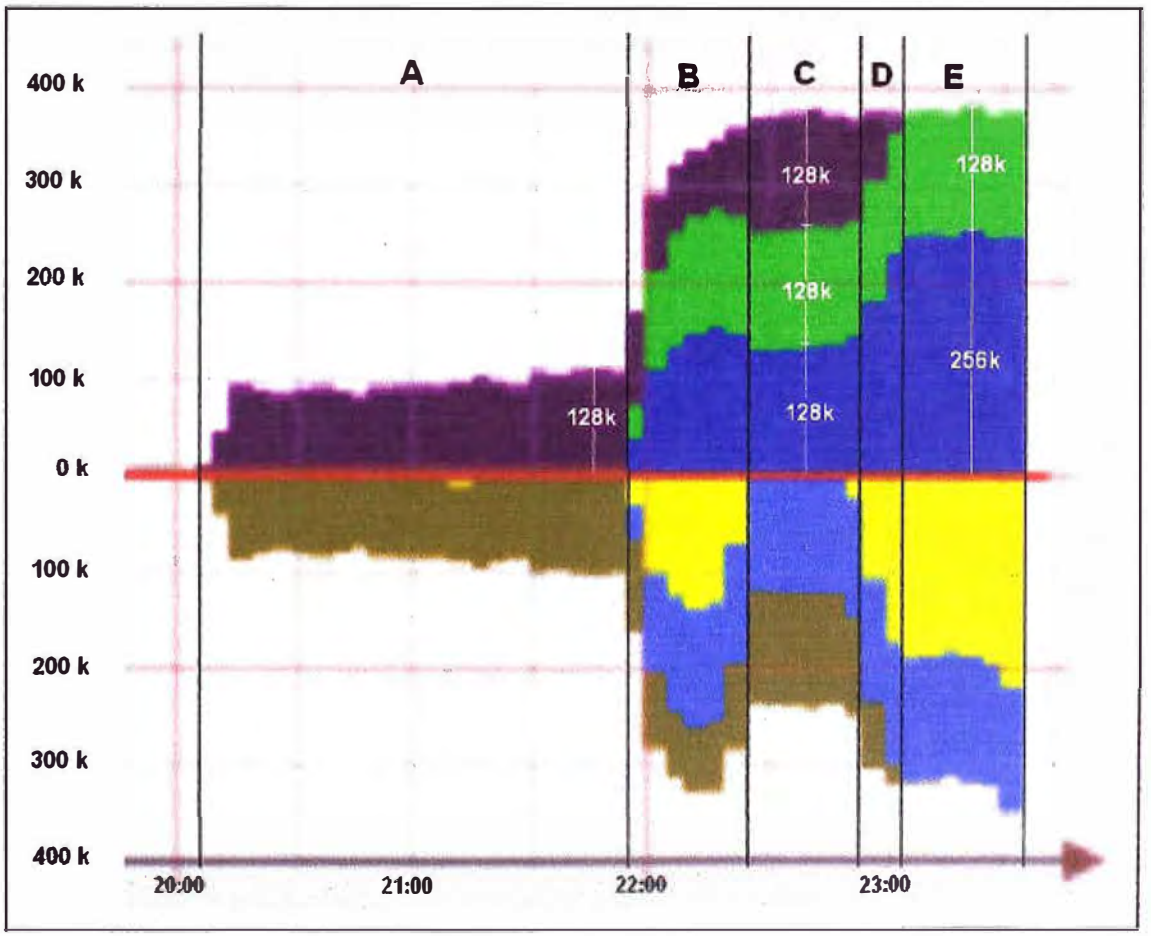

Figura 4.33 Tráfico por clases cursado durante las pruebas

- En la gráfica 4.35 se presenta una parte de la salida del comando show policy-map interface FastEthemet 1/0 ouptput aplicado al enrutador CPE1, donde podemos verificar que la velocidad llega a 101kbps en el momento que se captura los resultados, no se observan paquetes que hayan estado en la cola de espera y menos paquetes descartados, así mismo comentar que el tráfico de clase CoS2 es 0, ya que solo se esta generando tráfico de clase CoS3, el tráfico CoS1 observado es el que se genera por la gestión al ingresar a los equipos.

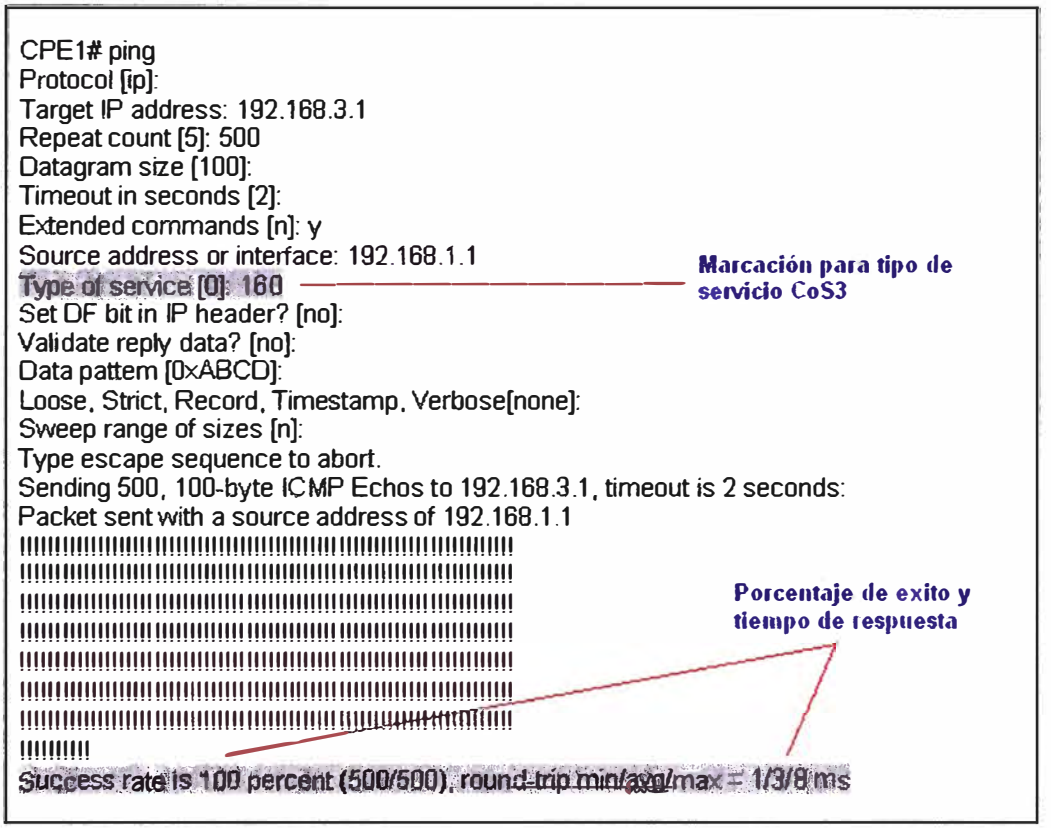

Figura 4.34 Generación de tráfico CoS3

- Continuando con las pruebas se incremento el tráfico de clase CoS3 con el objetivo de saturar el ancho de banda de 128K y observar el tratamiento que recibe el tráfico de clase CoS3. Pudimos corroborar que al generar más tráfico de clase CoS3 aparecen paquetes que ingresaron a la cola de espera y luego al exceder el umbral permitido se descartaron, como se muestra en la figura 4.36. La presencia de paquetes descartados en la salida del comando show policy-map de la figura 4.36 se traduce en pérdida de paquetes, lo cual afecta la calidad de las llamadas, sin embargo si esta pérdida es eventual y pequeña no será percibida durante la comunicación, podemos observar gráficamente en la figura 4.37 que es la ampliación de la figura 4.30.

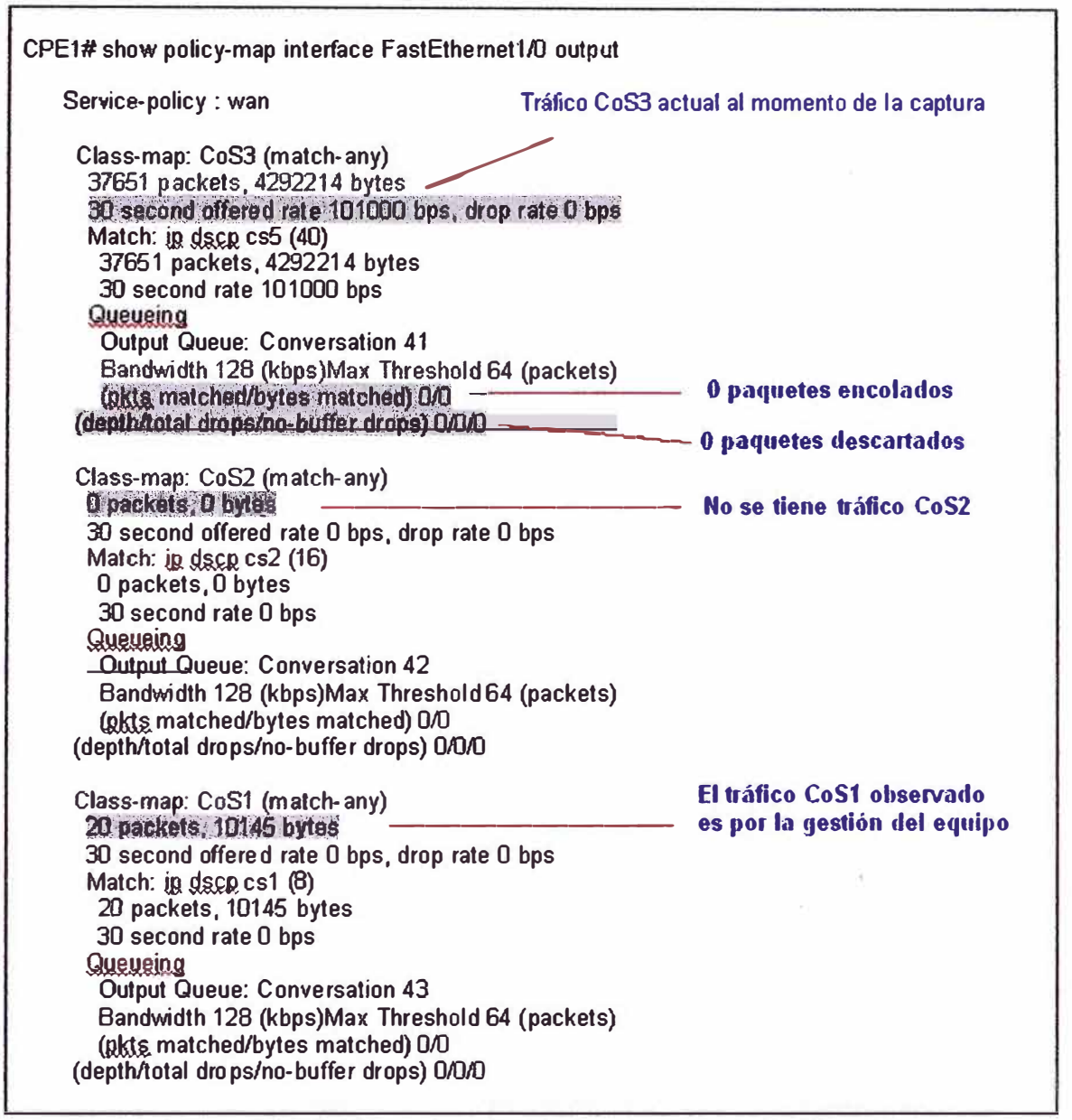

Figura 4.35 Políticas de calidad sin saturar el CoS3 de 128K

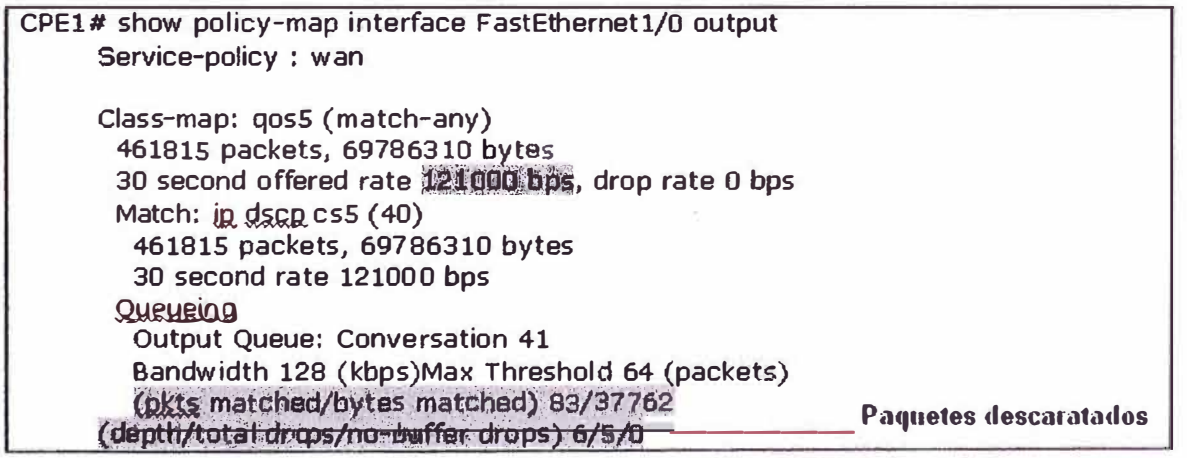

Figura 4.36 Políticas de calidad saturando el CoS3 de 128K

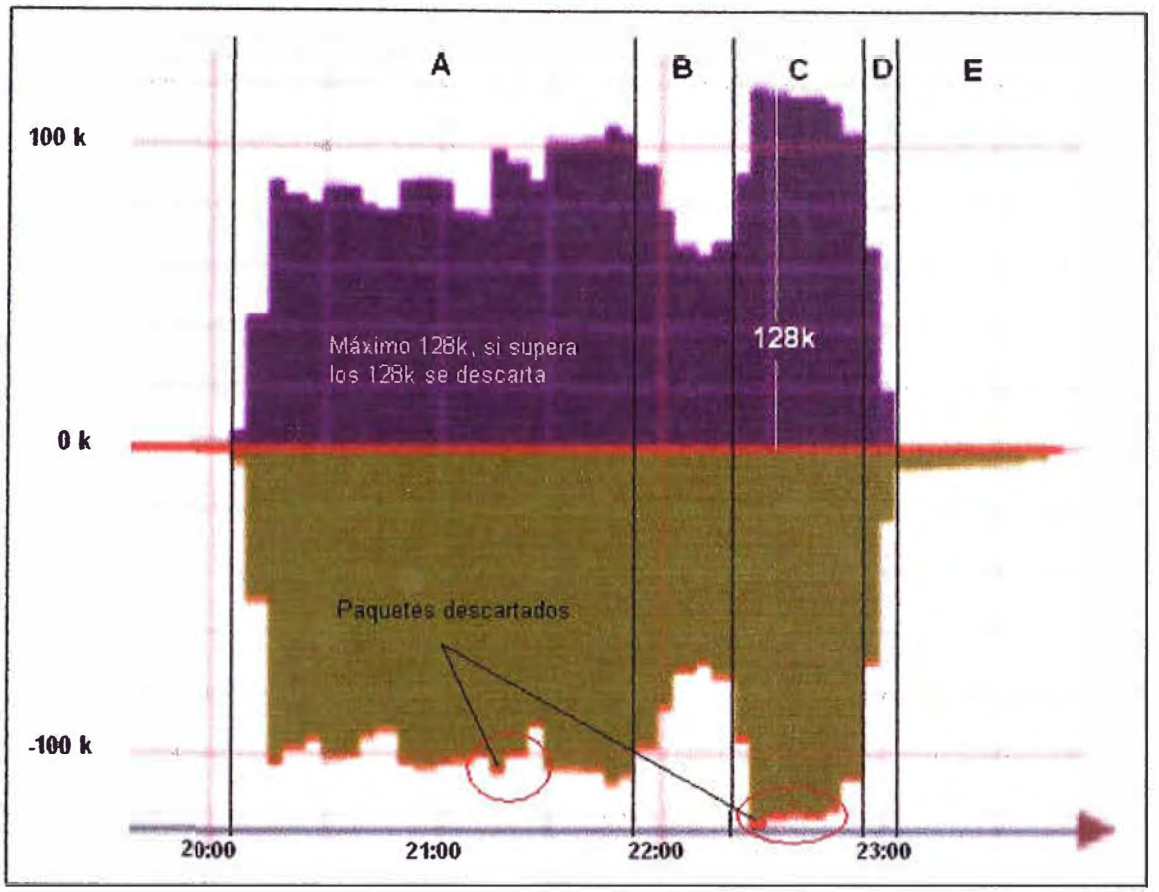

Figura 4.37 Tráfico de clase CoS3

Escenario B

Para el escenario de pruebas B se genera tráfico de clase CoS3, CoS2 y CoS1, en la figura 4.33 podemos verificar que al desminuir el tráfico de clase CoS3 la suma del tráfico de clase CoS2 y CoS1 puede incrementarse por encima de los 256K, aprovechando el ancho de banda disponible que no se utiliza por el tráfico de clase CoS3. No vamos a entrar en detalles en este escenario debido a que es el escenario de transición para las pruebas a realizar en el escenario C donde se satura el ancho de banda total y verificamos el comportamiento de los diferentes tipos de tráfico.

Escenario C

En el escenario de pruebas C se genero tráfico de clases CoS3 y CoS2 utilizando el ancho de banda total del enlace de 384K, con el cual se comprueba el comportamiento del tráfico de clase CoS3 en congestión y el comportamiento de remarcado de paquetes cuando se excede el tráfico de clase CoS2.

- Como se indica la idea era utilizar el enlace de 384K totalmente, en la figura 4.33 y 4.37 pudimos verificar que el ancho de banda total del enlace llega al tope sin afectar el ancho de banda reservado para el tráfico de clase CoS3, en todo

momento puede llegar a los 128K garantizados. Cuando no se tiene tráfico tipo CoS3 el tráfico restante puede utilizar el tráfico reservado para el tráfico de clase CoS3, pero inmediatamente ingresa tráfico de clase CoS3 se libera la capacidad necesaria para garantizar el flujo del tráfico de clase CoS3.

- En la figura 4.38 (ampliación de la figura 4.31) podemos observar el tráfico de clase CoS2 cursado en el enlace durante las pruebas, el tráfico de clase CoS2 tiene un mínimo garantizado de 128K en caso de congestión y puede alcanzar hasta el ancho de banda total de 384K en caso de ausencia de tráfico de tipo CoS3. Como se verifica en la figura 4.38 el tráfico de clase CoS2 llega a 128K (color verde) y luego se genera el tráfico de color rojo, que es el tráfico que se remarca con clase de servicio CoS1, es decir llega a ocupar el ancho de banda del tipo de servicio CoS1 alcanzando los 256K, cuando se genera mas tráfico CoS2 y sobrepasa los 256K este tráfico excedente se descarta ya que no puede utilizar mas de los 256K, debido a que se tiene tráfico de clase CoS3 que esta utilizando 128K restantes. El tráfico remarcado también puede observarse en la figura 4.40 que es la gráfica del tráfico de tipo CoS1.

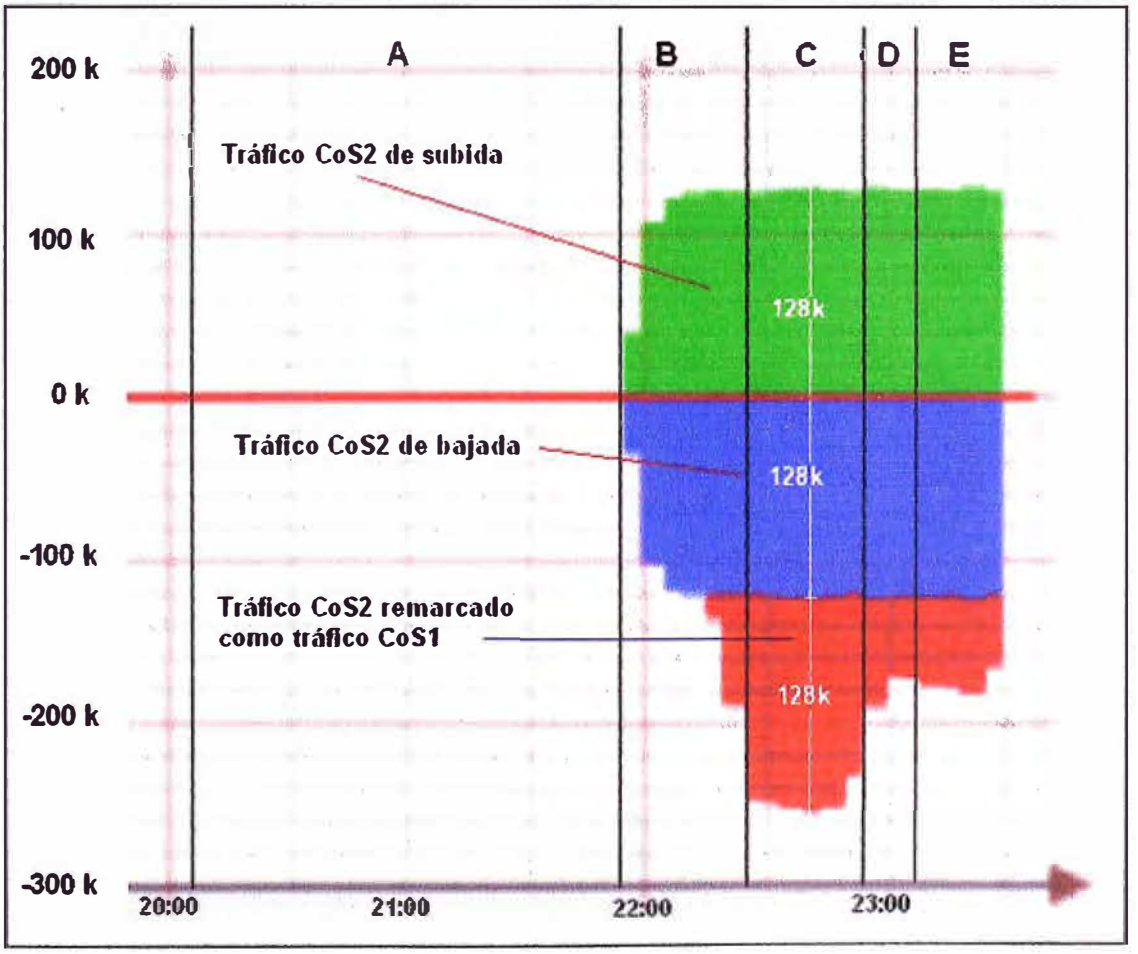

Figura 4.38 Tráfico de clase CoS2

- En la figura 4.39 se muestra una parte de la salida del comando show policy-map interface FastEthemet1/0 ouput para este caso podemos verificar en el momento de la captura que el tráfico de clase CoS3 llega a 119kbps mientras que el tráfico de clase CoS2 llega a 264kbps (383kbps en total). De los 264kbps de tráfico de clase CoS2 que se observa, se tiene 135kbps de tráfico que excedió los 128kbps garantizados para el tráfico de clase CoS2 y que fue remarcado como tipo CoS1, valores que se reflejan en la gráfica 4.38. De manera similar que para el CoS3 mientras no se sature el ancho de banda no se registran pérdidas de paquetes y los tiempos se mantienen estables, en cuanto se comienza a saturar el enlace se registran pérdidas de paquetes y elevación de los tiempos de respuesta.

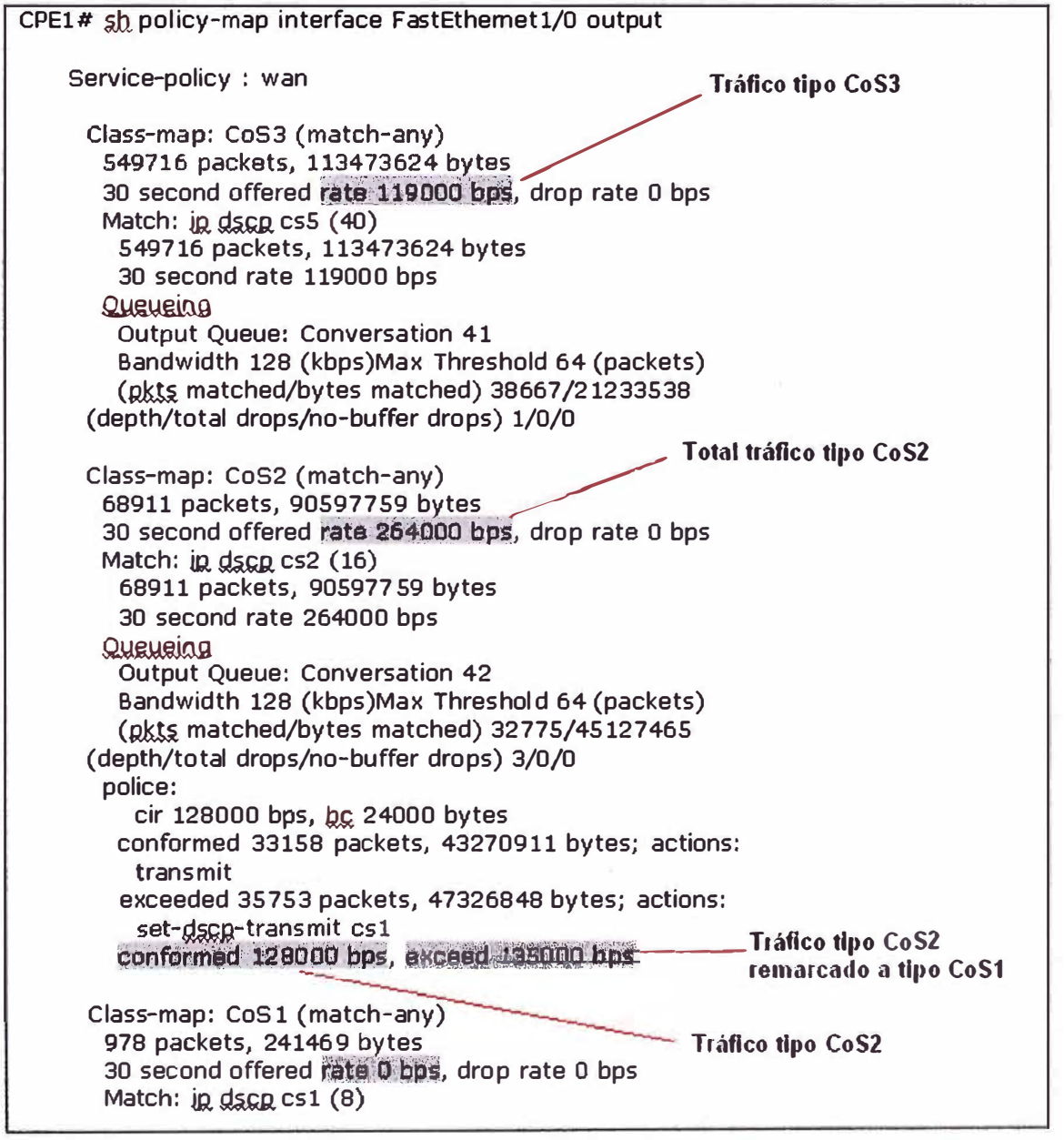

Figura 4.39 Políticas de calidad con tráfico de clase CoS3 y CoS2

Escenario D

En este escenario de pruebas se inicia la generación progresiva de tráfico de tipo CoS1 y disminuye paulatinamente la generación del tráfico de tipo CoS3 pero manteniendo el consumo total del ancho de banda de 384K, con lo cual podemos observar en la figura 4.33 como el ancho de banda que se deja de utilizar por el tráfico tipo CoS3 es aprovechado por el tráfico tipo CoS1 validando nuevamente los comportamientos descritos al inicio del capitulo.

Escenario E

Para este escenario de pruebas se dejo de generar tráfico de tipo CoS3, se generó tráfico de tipo CoS2 y CoS1 de igual manera llegando a utilizar el enlace total de 384K como se puede apreciar en la figura 4.33. En este caso observamos que el tráfico de clase CoS2 gráfica valores de 128K como máximo ya que el tráfico de clase CoS2 que excede los 128K se gráfica como tráfico de tipo CoS1, razón por la cual se muestra que el tráfico de clase CoS1 llega a 256 K, en caso de ausencia de tráfico de clases CoS3 y CoS2 el tráfico de tipo CoS1 puede aprovechar todo el ancho de banda. En la figura 4.41 podemos apreciar el tráfico de tipo CoS1 generado durante las pruebas, en el escenario C no se generó tráfico tipo CoS1 es el tráfico remarcado de tipo CoS2. En la figura 4.40 se muestra la salida del comando show policy-map interface FastEthernet 1/0 output con los valores de 131kbps de tráfico de clase CoS2 y 252kbps de tráfico de clase CoS1, así mismo se verifica la suma total 383kbps.

```
CPE1 # show policy-map interface FastEthernet1/0 output
 Service-policy output: Shape384
  Class-map: class-default (match-any)
   733890 packets, 335097652 bytes
   30 second offered rate 383000 bps, drop rate 0 bps

   Service-policy : wan
    Class-map: CoS5 (match-any)
     573352 packets, 125388328 bytes
     30 second offered rate 0 bps, drop rate 0 bps

    Class-map: CoS2 (match-any)
     117003 packets, 158580452 bytes
     30 second offered rate 131000 bps, drop rate 0 bps

    Class-map: CoS1 (match-any)
     36281 packets, 50092430 bytes
     30 second offered rate 252000 bps, drop rate 0 bps
```

Figura 4.40 Políticas de tráfico de clase CoS2 y CoS1

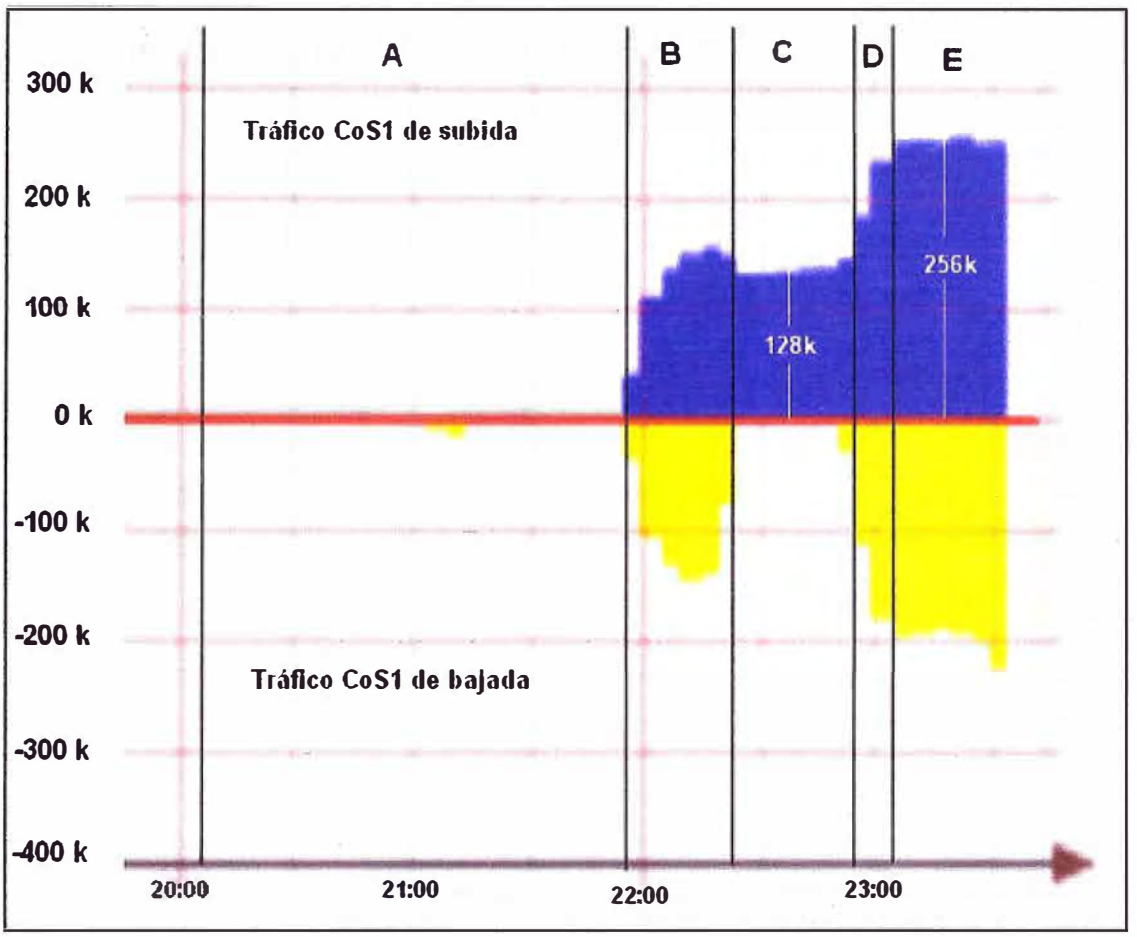

Figura 4.41 Tráfico de clase CoS1

Podemos concluir que los 5 escenarios anteriormente descritos nos han permitido observar y comprobar el funcionamiento de las diferentes configuraciones implementadas en la red MPLS que se diseño para el desarrollo del presente informe, se ha validado algunas de las aplicaciones que nos brinda la tecnología MPLS como son el soporte de multiplataforma (Hemos trabajado MPLS sobre Ethernet), Red Privada Virtual (se ha verificado conectividad extremo a extremo de la red Privada del cliente) y Calidad de Servicio sobre las 3 clases definidas y utilizadas.

Finalmente resumir que las ventajas que ofrece MPLS sobre otras arquitecturas la ha convertido en la tecnología ampliamente utilizada hoy en día en la gran mayoría de las redes de operadores de telecomunicaciones del mundo, lo que motivo al desarrollo del presente informe, esperando que sirva de ayuda y motivación a todos aquellos que se encuentran en la búsqueda de conocimientos sobre esta tecnología.

CONCLUSIONES

1. Al combinar un uno solo lo mejor de cada nivel (la inteligencia del enrutamiento con la rapidez de la conmutación), MPLS se ha convertido en el último paso de la conmutación multinivel, que permite ofrecer nuevas posibilidades de gestión de backbones.
2. MPLS soporta enrutamiento IP Unicast que es la aplicación mas utilizada ya que sirve de base para algunas otras aplicaciones. Esta aplicación permite crear una malla completa de túneles LSP para la conexión hacia los posibles destinos de enrutamiento.
3. El enrutamiento IP Multicast puede utilizar una red MPLS, por ejemplo a través de uno de los protocolos de enrutamiento multicast como PIM, con extensiones para MPLS. Actualmente sobre MPLS se corre IP Multicast Nativo, es decir el tráfico multicast no lleva etiquetas.
4. El soporte multiprotocolo de MPLS permite la coexistencia con ATM, lo que ha facilitado enormemente realizar la migración de los backbones tradicionales ATM de los proveedores de servicio a sus actuales backbones MPLS, como es el caso de algunos operadores en Perú como Telmex o Telefónica. Así mismo ha permitido de esta manera la versatilidad de redes de acceso en los proveedores de servicio. Hoy en día se tienen backbones MPLS conectados en simultáneo a redes de acceso como ATM, Frame Relay, Metro Ethernet y otras.
5. MPLS provee un mecanismo eficiente para el manejo de redes privadas virtuales. De esta manera el tráfico de una red privada atraviesa la red eficazmente y de manera transparente para el usuario, eliminando cualquier tráfico externo y protegiendo la información. Los niveles de seguridad brindados por una red MPLS/VPN son comparables con los entregados por los circuitos virtuales de Frame Relay y ATM. Sin embargo, en escenarios donde estos niveles no son suficientes, como por ejemplo en transacciones de entidades financieras, una red MPLS/VPN puede también ser combinada con la encriptación y autenticación que brinda IPSec, elevando aún más la seguridad de la VPN.

6. La escalabilidad de una red MPLS nos permite realizar cambios de conectividad y capacidad de forma muy ágil. MPLS ofrece conectividad todos contra todos (full-mesh), lo que la convierte en una red realmente flexible con unos requerimientos de configuración mínimos a la hora de añadir un nuevo extremo a la VPN, pues sólo hay que configurar el nuevo extremo, sin tener que tocar la configuración del resto de extremos.

7. MPLS soporta arquitecturas como IntServ e DiffServ lo que le permite ofrecer una red con calidad de servicio, asegura la priorización del tráfico crítico o sensible al retardo sin despreciar tampoco el resto del tráfico gestionando el ancho de banda asignado a cada tipo de tráfico. MPLS soporta la diferenciación de tráfico de una forma estandarizada y permite garantizar SLAs para dichos tipos de tráfico, pudiéndose implementar herramientas, incluso vía Web, que permitan a los usuarios controlar el funcionamiento de su red en todo momento.

8. MPLS es considerado estratégicamente una solución para la ingeniería de tráfico porque puede potencialmente proveer más funcionalidad de manera integrada y con bajo coste. Ofrece aspectos automáticos de la ingeniería de tráfico como la posibilidad de establecer un LSP explicito que permite emular un circuito conmutado en un modelo de enrutamiento.

9. MPLS ofrece ahorros significativos en materia de implementación porque es soportado por la mayoría de protocolos de la capa2. Esto resulta en una relativa facilidad de migrar a esta tecnología. También con la ingeniería de tráfico se logra reducir los costos de mantenimiento de los enlaces, pues TE ofrece la optimización de los recursos en la red MPLS.

10. Finalmente podemos concluir que MPLS es la tecnología por la que la mayoría de los proveedores de servicios en la industria de las telecomunicaciones han apostado, ello asegura un futuro prometedor y un constante desarrollo.

ANEXOS

ANEXO A. ESPECIFICACIONES TÉCNICAS DEL ROUTER CISCO 12406 XR

The Cisco® XR 12000 Series and Cisco 12000 Series routers compose a portfolio of intelligent routing solutions that scale from 2.5- to n x10 Gbps capacity per slot, enabling carrier-class IP/Multiprotocol Label Switching (MPLS) networks and accelerating the evolution to IP Next-Generation Networks. Built upon a foundation of investment protection, this portfolio delivers up to 1.28-terabits-per-second switching capacity with wire-speed feature performance, scalability, and graceful hardware and software upgrade paths.

CISCO XR 12000 AND 12000 SERIES PRODUCT PORTFOLIO OVERVIEW

This portfolio of routers delivers capacity and services with its fully distributed forwarding architecture and high-efficiency crossbar switch fabric (Figure 1). The combination of a centralized scheduler and unique virtual output queuing (VOQ) technology is aimed at maximizing the use of the switch fabric bandwidth, minimizing latency, and providing nonblocking performance. Cisco Systems® uses the latest in high-performance application-specific integrated circuit (ASIC) technology to provide line-rate forwarding with an extensive feature set, while maintaining the strict control of jitter and latency required for real-time services. Offering a comprehensive set of quality-of-service (QoS), IP/MPLS, and high-availability features, the Cisco XR 12000 Series and 12000 Series routers can help ensure maximum bandwidth usage and traffic differentiation while meeting even the strictest customer service-level agreements (SLAs).

The Cisco XR 12000 Series and 12000 Series routers use Cisco IOS® XR Software and Cisco IOS Software, respectively, to deliver numerous service possibilities for network operators. With the addition of the Cisco XR 12000 Series to its high-end routing product lines, Cisco Systems gives providers a graceful upgrade path for their installed base of Cisco 12000 Series routers as they transition toward a converged IP Next-Generation Network infrastructure. For a detailed list of feature support, software capabilities, compatibility, and release notes for Cisco IOS XR and Cisco IOS Software on these routers, visit: http://www.cisco.com/go/12000.

The Cisco XR 12000 Series and 12000 Series routers product specifications are detailed in Table 1.

Table 1. Product Specifications

Product Specification	Cisco XR 12000 and 12000 Series 16-Slot Chassis	Cisco XR 12000 and 12000 Series 10-Slot Chassis	Cisco XR 12000 and 12000 Series 6-Slot Chassis	Cisco XR 12000 and 12000 Series 4-Slot Chassis
Slot capacity	16 slots	10 slots	6 slots	4 slots
Aggregate switching capacity	Cisco 12016: 80 Gbps Cisco 12416: 320 Gbps Cisco 12816: 1280 Gbps	Cisco 12010: 50 Gbps Cisco 12410: 200 Gbps Cisco12810: 800 Gbps	Cisco 12006: 30 Gbps Cisco 12406: 120 Gbps	Cisco 12404: 80 Gbps
Full-duplex throughput per slot	Cisco 12016: 2.5 Gbps/slot Cisco 12416: 10 Gbps/slot Cisco 12816: 40 Gbps/slot	Cisco 12010: 2.5 Gbps/slot Cisco 12410: 10 Gbps/slot Cisco 12810: 40 Gbps/slot	Cisco 12006: 2.5 Gbps/slot Cisco 12406: 10 Gbps/slot	Cisco 12404: 10 Gbps/slot
Physical	Chassis height 71.5 in. (181.6 cm) 72.5 in. (184.2 cm)1 Chassis width 17.25 in. (43.8 cm) 18.75 in. (47.6 cm)2 Chassis depth 22.0 in. (55.9 cm) 24.0 in. (61.0 cm)3 Weight 140 lb (64 kg)[4] 390 lb (177 kg)[5]	Chassis height 37.5 in. (95.25 cm) Chassis width 19 in. (48.26 cm) Chassis depth 22.0 in. (55.9 cm) 24.0 in. (61.0 cm) weight 125 lb (57 kg) 275 lb (125 kg)	Chassis height 18.5 in. (47.0 cm) Chassis width 17.3 in. (43.9 cm) 18.9 in. (48.0 cm) Chassis depth 28.0 in. (71.1 cm) Weight 140 lb (64 kg) 205 lb (94 kg)	Chassis height 8.75 in. (22.23 cm) Chassis width 17.39 in. (44.15 cm) 18.9 in. (48.01 cm) Chassis depth 27.5 in. (69.85 cm) Weight 73 lb (33.18 kg) 103 lb (46.82 kg)
Chassis per rack	One	Two	Four	Eight

Electrical specifications for the AC input power				
Total AC input power[1]	4651 VA (max) per chassis	2790 VA (max) per chassis	Low Line 1708 VA (max) High Line 1950 VA (max) per chassis	1341 VA (max) per chassis
Rated input voltage[2]	200–240 VAC nominal (range: 180–264 VAC)	200–240 VAC nominal (range: 180–264 VAC)	100–120 VAC (Low Line) 200–240 VAC (High Line) nominal (range: 85–264 VAC)	100–120 VAC or 200–240 VAC nominal (range: 85–264 VAC)
Rated input line frequency	50–60 Hz nominal (range: 47–63 Hz)	50–60 Hz nominal (range: 47–63 Hz)	50–60 Hz nominal (range: 47–63 Hz)	50–60 Hz nominal (range: 47–63 Hz)
Input current rating (For any line cord)	10.3A maximum @ 240 VAC	11.6A maximum @ 240 VAC	17.2A (max) @ 100 VAC 10A (max) @ 200 VAC	6A maximum @ 240 VAC
Source AC service requirement	20A North America; 16A international	20A North America; 16A international	20A North America; 16A international	20A North America; 16A international
Electrical specifications for DC input power				
Total DC input power	4212 W (max)	2430 W (max)	1630 W (max)	1280 W (max)
Rated input voltage	-48 VDC nominal in North America	-48 VDC nominal in North America	-48 VDC nominal in North America	-48 VDC nominal in North America
	-60 VDC nominal in the European community (range: -40.5 to -75 VDC)	-60 VDC nominal in the European community (range: -40.5 to -75 VDC	-60 VDC nominal in the European community (range: -40.5 to -75 VDC	-60 VDC nominal in the European community (range: -40.5 to -75 VDC
Input current rating For any DC input pair	52A maximum @ 40.5 VDC[3]	60A maximum @ 40.5 VDC	45A maximum @ 40.5 VDC	35A maximum @ 40.5 VDC
Source DC service requirement	60A	60A	60A	60A
Environmental conditions				
Temperature	Operating: 32 to 104°F (0 to 40°C) Nonoperating: -4 to 149°F (-20 to 65°C)	Operating: 32 to 104°F (0 to 40°C) Nonoperating: -4 to 149°F (-20 to 65°C)	Operating: 32 to 104°F (0 to 40°C) Nonoperating: -4 to 149°F (-20 to 65°C)	Operating: 32 to 104°F (0 to 40°C) Nonoperating: -40 to 158°F (-40 to 70°C)
Humidity	Operating: 10–90% noncondensing Nonoperating: 5–95% noncondensing	Operating: 10–90% noncondensing Nonoperating: 5–95% noncondensing	Operating: 10–90% noncondensing Nonoperating: 5–95% noncondensing	Operating: 5–90% noncondensing Nonoperating: 5–95% noncondensing
Altitude	Operating: 0–10,000 ft. (0–3000m) Nonoperating: 0–15,000 ft. (0–4570m)	Operating: 0–10,000 ft. (0–3000m) Nonoperating: 0–15,000 ft. (0–4570m)	Operating: 0–10,000 ft. (0–3000m) Nonoperating: 0–15,000 ft. (0–4570m)	Operating: 0–14,000 ft. (0–4267m) Nonoperating: 0–16,000 ft. (0–4877m)
Heat dissipation	DC (max): 4212 VA @ 14372 Btu/hr AC (max):4651 VA @ 15870 Btu/hr	DC (max): 2430 VA @ 8291 Btu/hr AC (max):2790 VA @ 9519 Btu/hr	DC (max): 1630 VA @ 5562 Btu/hr low line AC (max): 1708 VA @ 5828 Btu/hr high line AC (max): 1950 VA @ 6654 Btu/hr	DC (max): 1280 VA @ 4367 Btu/hr AC (max): 1341 VA @ 4575 Btu/hr
Acoustic noise	70 dBa maximum	70 dBa maximum	70 dBa maximum	70 dBa maximum
Shock	Operating (halfsine): 21 in./sec (0.53m/sec) Nonoperating (trapezoidal pulse): 20g, 52 in./sec (1.32 m/sec)	Operating (halfsine): 21 in./sec (0.53m/sec) Nonoperating (trapezoidal pulse): 20g, 52 in./sec (1.32 m/sec)	Operating (halfsine): 21 in./sec (0.53m/sec) Nonoperating (trapezoidal pulse): 20g, 52 in./sec (1.32 m/sec)	Operating (halfsine): 5g (11 m/sec) Nonoperating (trapezoidal pulse): 15g (11 m/sec)
Vibration	Operating: 0.35 grms[4] from 3 to 500 Hz Nonoperating: 1.0 grms from 3 to 500 Hz	Operating: 0.35 grms from 3 to 500 Hz Nonoperating: 1.0 grms from 3 to 500 Hz	Operating: 0.35 grms from 3 to 500 Hz Nonoperating: 1.0 grms from 3 to 500 Hz	Operating (sinusoidal): 3–500 Hz @ 0.15 gpk (random): 2.5–200 Hz @ 0.33 grms Storage (sinusoidal): 10–500 Hz @ 0.8 gpk (random): 2.5–200 Hz @ 1.05 grms

Hardware components (per base system)	• 4 DC power supplies, or 3 AC supplies, or 4 AC power supplies • 1 performance router processor • 16 line-card slots with 15 line cards and 1 route processor or 14 line cards and 2 route processors (1:1 redundant) • 3 switch fabric cards (SFCs) • 2 clock scheduler cards (CSCs) • 2 alarm cards • Air filters • 2 blower assemblies • 2 cable-management trays • Country-specific power cords	• 2 DC power supplies or 2 AC supplies • 1 performance router processor • 10 line-card slots with 9 line cards and 1 route processor or 8 line cards and 2 route processors (1:1 redundant) • 5 SFCs • 2 CSCs • 1 alarm card • Air filter • 1 blower assembly • 1 cable-management tray • Country-specific power cords	• 2 DC power supplies or 2 AC supplies • 1 performance router processor • 6 line-card slots with 5 line cards and 1 route processor or 4 line cards and 2 route processors (1:1 redundant) • 3 SFCs • 2 CSCs • 1 alarm card • Air filter • 1 blower assembly • 1 cable-management tray • Country-specific power cords	• 2 DC power supplies or 2 AC supplies • 1 performance router processor • 4 line-card slots with 3 line cards and 1 route processor or 2 line cards and 2 route processors (1:1 redundant) • 1 consolidated switch fabric, clock scheduler, and alarm card • Air filter • 1 blower assembly • 1 cable-management tray • Country-specific power cords
Software components (per base system)	• Cisco IOS XR or Cisco IOS Software Operating System • Cisco Express Forwarding for distributed packet forwarding	• Cisco IOS XR or Cisco IOS Software Operating System • Cisco Express Forwarding for distributed packet forwarding	• Cisco IOS XR or Cisco IOS Software Operating System • Cisco Express Forwarding for distributed packet forwarding	• Cisco IOS XR or Cisco IOS Software Operating System • Cisco Express Forwarding for distributed packet forwarding
Compatibility	Cisco 12800: Line cards that support 2.5-, 10-, or 20-Gbps capability Cisco 12400: Line cards that support 2.5- or 10-Gbps capability Cisco 12000: Line cards that support 2.5-Gbps capability			
Protocols	IPv4, MPLS, Border Gateway Protocol Version 4 (BGPv4), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First Version 2.0 (OSPFv2.0), Routing Information Protocol Version 2 (RIPv2), Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), and Protocol Independent Multicast dense mode/sparse mode (PIM DX/SX)			
Connectivity	Packet over SONET/SDH (POS), Ethernet, ATM, copper (DS-3/E3), Channelized (CT3, ChOC-3/CHSTM1, ChOC-12/CHSTM4, ChOC-48/CHSTM16); see Cisco IOS XR Software release notes for specific connectivity support on the Cisco XR 12000 Series			
Reliability	System redundancy: • Fabric card redundancy 4:1 • CSC redundancy 1:1 • Power supply redundancy (1:1 for DC; AC is load balancing) • Blower redundancy 1:1 • Route processor redundancy 1:1 • Alarm card redundancy 1:1 • Dual homing through line cards • Supports automatic protection switching (APS) ASICs Mean time between failure (MTBF): • CSC = 240,078 hr • SFC = 276,062 hr			
Management interfaces	Cisco XR 12000 and Cisco 12000 Series Performance Route Processor (PRP) supports two serial ports (console and auxiliary) and one 10/100 Ethernet port			
Indicators and interfaces	Visual alarms for critical, major, and minor states on CSCs, SFCs, and on or error condition for system alarm boards			

ANEXO B. ESPECIFICACIONES TÉCNICAS DEL ROUTER CISCO 7206 VXR

The Cisco 7200 VXR Series Router delivers exceptional performance/price, modularity, and scalability in a compact form factor with a wide range of deployment options.

Cisco 7200 VXR Series Router

With processing speeds up to 2 million packets per second, port- and service adapters ranging from NxDS0 to Gigabit Ethernet, and OC-3 as well as an unparalleled number of high-touch IP services, the Cisco 7200 VXR series is the ideal Services Aggregation WAN/MAN edge device for enterprises and service providers deploying any of the following solutions:

- **WAN edge**—Award-winning quality-of-service (QoS) feature performance
- **Broadband aggregation**—Up to 16,000 Point-to-Point Protocol (PPP) sessions per chassis
- **Multiprotocol Label Switching provider edge (MPLS PE)**—Number one choice for provider edge deployment today
- **Voice/video/data integration**—Time-division multiplexer (TDM)-enabled VXR chassis and voice port adapters
- **IP-to-IP Gateway Support**—Direct IP-interconnections
- **IP Security virtual private networking (IPSec VPN)**—Scalable to 5,000 tunnels per chassis
- **High-End Customer Premises Equipment (CPE)**—For managed WAN services saving equipment, transport and administrative cost

Table 1. Cisco 7200 VXR Features and Benefit

Features	Benefits
Up to 2 Mpps Processing Capability	Provides high-performance routing and processing performance
Maximum Connectivity Options	Meets a variety of topology requirements with the widest range of port densities and interface options
Breadth of Services	Supports QoS, security, MPLS, broadband, multiservice, voice, IP-to-IP Gateway and management features for next-generation networks
Investment Protection	Low initial investment with upgrade and redeployment capability

Product Specifications

Table 2. Cards, Ports, Slots

	Cisco 7204 VXR	Cisco 7206 VXR
Configurable Slots without Port Adapter Jacket Card	4	6
Configurable Slots with Port Adapter Jacket Card	5	7
Ethernet (10BASE-T) Ports	32	48
Ethernet (10BASE-FL) Ports	20	30
Fast Ethernet (TX) Ports	4	Up to 6
Fast Ethernet (FX) Ports	4	Up to 6
EtherSwitch Port Adapters	2	2

100VG-AnyLAN Ports	4	Up to 6
FDDI (FDX, HDX) Ports	0	0
ATM Ports (T3, OC-3)	4, 4	Up to 6, 4
Packet over SONET	4	6
ATM-CES Port Adapters (Data, Voice, Video), Dual-Wide	1	1
Token Ring (FDX, HDX) Ports	16	24
Synchronous Serial Ports	32	48
ISDN BRI Ports (U, S/T)	16, 32	24, 48
ISDN PRI, Multichannel T1/E1 Ports	32	48
Multichannel T3 Ports	Up to 4	Up to 6
HSSI Ports	Up to 8	Up to 12
Packet over T3/E3 Ports (Integrated DSU)	Up to 10	Up to 14
IBM Channel Interface Ports (ESCON and Parallel)	6	6
VPN Acceleration Module	1	1

Components

Table 3. Chassis

Feature	Cisco 7204 VXR	Cisco 7206 VXR
Chassis/Rack	• 16 with side-to-side air flow • 9 with RDS mounting system for front-to-back airflow	Same as Cisco 7204 VXR
I/O Card Slots	1	Same as Cisco 7204 VXR
Port Adapter Slots	4	6
Midplane	2 independent 32-bit, 50-MHz PCI buses with an aggregate bandwidth of 1.2 Gbps when used with NPE-400. 3 independent 32-bit, 50-MHz PCI buses with an aggregate bandwidth of 1.8 Gbps when used with NPE-G1 or NPE-G2	Same as Cisco 7204 VXR
Online Insertion and Removal (OIR)	Yes	Same as Cisco 7204 VXR
Field-Replaceable Components	Processor, memory, power supply, I/O card, and port adapters	Same as Cisco 7204 VXR
Additional Standard Components	AC power supply, AC power cord	Same as Cisco 7204 VXR

Table 4. Environmental Conditions

	Cisco 7204 VXR	Cisco 7206 VXR
Operating Temperature	32 to 104°F (0 to 40°C)	Same as Cisco 7204 VXR
Storage Temperature	-4 to 149°F (-20 to 65°C)	Same as Cisco 7204 VXR
Operating Humidity	10 to 90% (noncondensing)	Same as Cisco 7204 VXR

Table 5. Memory

	Cisco 7204 VXR	Cisco 7206 VXR
Processor Memory	• 128 MB (default for NPE-225) • 256 MB (default for NPE-400 and NPE-G1, max for NPE-225) • 512 MB (max for NPE-400) • 1 GB (max for NPE-G1 and default for NPE-G2); in future: optional upgrade to 2 GB for NPE-G2)	Same as Cisco 7204 VXR

PCMCIA Flash Disk Memory Card (optional, up to 2 slots available)	• 48 MB, expandable to 128 MB for I/O controllers • 64 MB, expandable to 256 MB for NPE-G1 and NPE-G2	Same as Cisco 7204 VXR
Compact Flash Disk Memory Card (optional for NPE-G1 and NPE-G2)	• 64 MB, expandable to 256 MB for NPE-G1 • 256 MB for NPE-G2	Same as Cisco 7204 VXR

Table 6. Physical Specifications

	Cisco 7204 VXR	Cisco 7206 VXR
Height	5.25 in. (13.34 cm)	5.25 in. (13.34 cm)
Width	16.8 in. (42.67 cm)	16.8 in. (42.67 cm)
Depth	17 in. (43.18 cm)	17 in. (43.18 cm)
Weight	Chassis is fully configured with a network processing engine, I/O controller, four port adapters, two power supplies, and a fan tray: ~50 lb (22.7 kg)	Chassis is fully configured with a network processing engine, I/O controller, six port adapters, two power supplies, and a fan tray: ~50 lb (22.7 kg)

Table 7. Power (The Cisco 7200 VXR is available with single and dual power supply options for both AC and DC.)

	Cisco 7204 VXR	Cisco 7206 VXR
AC-Input Power	370W max. (single or dual power supply configuration)	Same as Cisco 7204 VXR
AC-Input Voltage Rating	100-240 VAC wide input with power factor correction	Same as Cisco 7204 VXR
AC-Input Current Rating	Not to exceed 5A max. at 100 VAC and 2.5A max. at 240 VAC with the chassis fully configured	Same as Cisco 7204 VXR
AC-Input Frequency Rating	50/60 Hz	Same as Cisco 7204 VXR
AC-Input Cable	18 AWG 3-wire cable, with 3-lead IEC-320 receptacle on the power supply end, and a country-dependent plug on the power source end	Same as Cisco 7204 VXR
DC-Output Power	280W max. (single or dual power supply configuration)	Same as Cisco 7204 VXR
DC-Input Power	370W max. (single or dual power supply configuration)	Same as Cisco 7204 VXR
DC-Input Voltage Rating	-24 to -60 VDC for global DC power requirements	Same as Cisco 7204 VXR
DC-Input Current Rating	• Not to exceed 13A max. at -48 VDC (370W/-48 VDC = 7.7A typical draw) • Not to exceed 8A max. at -60 VDC (370W/-60 VDC = 6.2A typical draw)	Same as Cisco 7204 VXR
DC Voltages Supplied and Maximum Steady-State Current Ratings	• +5.2V at 36OA • +12.2V at 9A • -12.0V at 1.5A • +3.5V at 13A	Same as Cisco 7204 VXR
DC-Input Cable	14 AWG recommended minimum, with at least 3 conductors rated for at least 140°F (60°C)	Same as Cisco 7204 VXR
Frequency	50/60 Hz	Same as Cisco 7204 VXR
Airflow	~80 cfm	Same as Cisco 7204 VXR
Power Dissipation	~370W max. configuration	Same as Cisco 7204 VXR
Heat Dissipation	370W (1262 BTUs)	Same as Cisco 7204 VXR
Noise Level	• Front (I/O Controller and PA side): 44.2 db • Back (Power supply side): 43.7 db • Left (Fan side): 47.2 db • Right: 44.8 db	Same as Cisco 7204 VXR

ANEXO C. ESPECIFICACIONES TÉCNICAS DEL ROUTER CISCO 2801

The Cisco 2800 Series comprises four platforms (refer to Figure 1): the Cisco 2801, the Cisco 2811, the Cisco 2821, and the Cisco 2851. The Cisco 2800 Series provides significant additional value compared to prior generations of Cisco routers at similar price points by offering up to a fivefold performance improvement, up to a tenfold increase in security and voice performance, embedded service options, and dramatically increased slot performance and density while maintaining support for most of the more than 90 existing modules that are available today for the Cisco 1700, Cisco 2600, and Cisco 3700 Series.

The Cisco 2800 Series features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1/xDSL connections. The routers offer embedded encryption acceleration and on the motherboard voice digital-signal-processor (DSP) slots; intrusion prevention system (IPS) and firewall functions; optional integrated call processing and voice mail support; high-density interfaces for a wide range of wired and wireless connectivity requirements; and sufficient performance and slot density for future network expansion requirements and advanced applications.

Table 1. Architecture—Features and Benefits

Feature	Benefit
Modular Architecture	• A wide variety of LAN and WAN options are available. Network interfaces can be upgraded in the field to accommodate future technologies. • Several types of slots are available to add connectivity and services in the future on an "integrate-as-you-grow" basis. • The Cisco 2800 supports more than 90 modules, including WICs, VICs, network modules, PVDMs, and AIMs (Note: the Cisco 2801 router does not support network modules).
Embedded Security Hardware Acceleration	• Each of the Cisco 2800 Series routers comes standard with embedded hardware cryptography accelerators, which when combined with an optional Cisco IOS Software upgrade help enable WAN link security and VPN services.
Integrated Dual Fast Ethernet or Gigabit Ethernet Ports	• The Cisco 2800 Series provide two 10/100 on the Cisco 2801 and Cisco 2811 and two 10/100/1000 on the Cisco 2821 and Cisco 2851
Support for Cisco IOS Software	• The Cisco 2800 helps enable end-to-end solutions with full support for the latest Cisco IOS Software-based QoS, bandwidth management, and security features. • Common feature and command set structure across the Cisco 1700, 1800, 2600, 2800, 3700 and 3800 series routers simplifies feature set selection, deployment, management, and training.
Optional Integrated Power Supply for Distribution of Power Over Ethernet (PoE)	• An optional upgrade to the internal power supply provides in-line power (802.3af-compliant Power-over-Ethernet [PoE] and Cisco standard inline power) to optional integrated switch modules.
Optional Integrated Universal DC Power Supply	• On the Cisco 2811, 2821, and 2851 routers an optional DC power supply is available that extends possible deployments environments such as central offices and industrial environments (Note: not available on the Cisco 2801).
Integrated Redundant-Power-Supply (RPS) Connector	• On the Cisco 2811, 2821, and 2851 there is a built in external power-supply connector that eases the addition of external redundant power supply that can be shared with other Cisco products to decrease network downtime by protecting the network components from downtime due to power failures.

Table 2. Modularity—Features and Benefits

Feature	Benefit
Enhanced Network-Module (NME) Slots	• The NME slots support existing network modules (Note: NM and NME support on Cisco 2811, 2821, and 2851 only) • NME Slots offer high data throughput capability (up to 1.6Gbps) and support for Power over Ethernet (POE). • NME slots are highly flexible with support for extended NMEs (NME-X on Cisco 2821 and 2851 only) and enhanced double-wide NMEs (NME-XDs) (Note: Cisco 2851 only).

Feature	Benefit
High-Performance WIC (HWIC) Slots with Enhanced Functionality	• Four integrated HWIC slots on Cisco 2811, 2821, and 2851 and two integrated HWIC slots on Cisco 2801 allow for more flexible and dense configurations. • HWICs slots can also support WICs, VICs, and VWICs • HWIC slots offer high data throughput capability (up to 400 Mbps half duplex or 800 Mbps aggregate throughput) and Power over Ethernet (POE) support. • A flexible form factor supports up to two double-wide HWIC (HWIC-D) modules.
Dual AIM Slots	Dual AIM slots support concurrent services such as hardware-accelerated security, ATM segmentation and reassembly (SAR), compression, and voice mail (Refer to Table 7 for more details on specific platform support).
Packet Voice DSP Module (PVDM) Slots on Motherboard	Slots for Cisco PVDM2 Modules (DSP Modules) are integrated on the motherboard, freeing slots on the router for other services.
Extension-Voice-Module (EVM) Slot	The EVM supports additional voice services and density without consuming the network-module slot (Note: available only on Cisco 2821 and 2851).
USB Support	Up to two USB ports are available per Cisco 2800 series router. The routers' Universal Serial Bus (USB) ports enable important security and storage capabilities.

Table 3. Secure Networking—Feature and Benefits

Feature	Benefit
Cisco IOS Software Firewall	• Sophisticated security and policy enforcement provides features such as stateful, application-based filtering (context-based access control), per-user authentication and authorization, real-time alerts, transparent firewall, and IPv6 firewall.
Secure Sockets Layer (SSL)	• SSL provides security for web transactions by handling authentication, data encryption and digital signatures. The 2800 Series supports SSL VPNs and SSL acceleration via the AIM-VPN/SSL-3.
Onboard VPN Encryption Acceleration	• The Cisco 2800 Series supports IPSec Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) 128, AES 192, and AES 256 cryptology without consuming an AIM slot.
Network Admissions Control (NAC)	• A Cisco Self-Defending Network initiative, NAC seeks to dramatically improve the ability of networks to identify, prevent, and adapt to threats by allowing network access only to compliant and trusted endpoint devices.
Multiprotocol Label Switching (MPLS) VPN Support	• The Cisco 2800 Series supports specific provider edge functions plus a mechanism to extend customers' MPLS VPN networks out to the customer edge with virtual routing and forwarding (VRF) firewall and VRF IPSec. For details on the MPLS VPN support on the different versions of the Cisco 2800 Series, please check the feature navigator tool on http://www.cisco.com.
USB eToken Support	• USB eTokens from Aladdin Knowledge Systems (available at http://www.aladdin.com/etoken/cisco/) provides secure configuration distribution and allows users to store VPN credentials for deployment
AIM-Based Security Acceleration	• Support for an optional dedicated security AIM can deliver 2 to 3 times the performance of embedded encryption capabilities with Layer 3 compression.
Intrusion Prevention System (IPS)	• Flexible and high performance support is offered through Cisco IOS® Software or an intrusion-detection-system (IDS) network module. • The ability to load and enable selected IDS signatures in the same manner as Cisco IDS Sensor Appliances
Advanced Application Inspection and Control	• Cisco IOS Firewall includes HTTP and several email inspection engines that can be used to detect misuse of port 80 and email connectivity.
Cisco Easy VPN Remote and Server Support	• The Cisco 2800 Series eases administration and management of point-to-point VPNs by actively pushing new security policies from a single headend to remote sites.
Dynamic Multipoint VPN (DMVPN)	• DMVPN is a Cisco IOS Software solution for building IPSec + generic routing encapsulation (GRE) VPNs in an easy and scalable manner.
Group Encrypted Transport (GET) VPN	• GET VPN is a Cisco IOS Software solution that simplifies securing large Layer 2 or MPLS networks requiring partial or full-mesh connectivity by providing tunnel-less VPN connectivity.
URL Filtering	• URL filtering is available onboard with an optional content-engine network module or external with a PC server running the URL filtering software.
Cisco Router and Security Device Manager (SDM)	• This intuitive, easy-to-use, Web-based device-management tool is embedded within the Cisco IOS Software access routers; it can be accessed remotely for faster and easier deployment of Cisco routers for both WAN access and security features.

Table 4. IP Telephony Support—Features and Benefits

Feature	Benefit
IP Phone Support	• Optional support for Cisco in-line power distribution to Ethernet switch network modules and HWICs can be used to power Cisco IP phones.
EVM Module Slots	• Extension Voice Module Slots, available only on the Cisco 2821 and Cisco 2851, provide support for the Cisco High-Density Analog and Digital Extension Module for Voice and Fax, providing support for up to 24 total voice and fax sessions without consuming a Network Module Slot.
PVDM (DSP) Slots on Motherboard	• DSP (PVDM2) modules deliver support for analog and digital voice, conferencing, transcoding, and secure Real-Time Transport Protocol (RTP) applications.
Integrated Call Processing	• Cisco CME is an optional solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones. Cisco CME delivers telephony features similar to those that are commonly used by business users to meet the requirements of the small to medium-sized offices.
Integrated Voice Mail	• Support for up to a 250 mailboxes using the Cisco Unity® Express voice messaging system is possible with the integration of an optional voice-mail AIM or network module.
Broad Range of Voice Interfaces	• Interfaces for public switched telephone network (PSTN), private branch exchange (PBX), and key system connections include FXS; FXO; analog direct inward dialing (DID); ear and mouth (E&M); Centralized Automated Message Accounting (CAMA); ISDN Basic Rate Interface (BRI); and T1, E1, and J1 with ISDN Primary Rate Interface (PRI); QSIG; E1 R2; and several additional channel-associated-signaling (CAS) signaling schemes.
Survivable Remote Site Telephony (SRST)	• Branch offices can take advantage of centralized call control while cost-effectively providing local branch backup using SRST redundancy for IP telephony.

Table 5. Wireless Support—Features and Benefits

Feature	Benefit
WLAN Connectivity	• The 802.11b/g or 802.11a/b/g HWIC access point interface card can be used to provide integrated WLAN connectivity to mobile clients at sites requiring a single access point, resulting in mobility and enhanced productivity for users. • Dual RP-TNC connectors enable diversity and allow for optimum coverage through the use of external antennas.
Wireless Infrastructure Services	• Telephony support for wired and WLAN IP phones is delivered by Cisco CallManager Express (CCME) or by Survivable Remote Site Telephony (SRST) with Cisco CallManager. Cordless WLAN IP phones allow users to be mobile and more productive. • Integrated switch modules with Power over Ethernet (POE) enable support for Cisco Aironet access points (for larger sites) as well as wired IP phones. • Mobility for clients from WLAN to cellular networks is enabled by Mobile IP home agent support. • IEEE 802.1x local authentication using LEAP provides enhanced reliability through survivable authentication for WLAN clients during WAN failures. • Customizable guest access is enabled with the service selection gateway features, along with the Subscriber Edge Services Manager.
Land Mobile Radio Over IP	• LMR over IP support allows radio users (e.g., security personnel, maintenance personnel, police officers, etc.) to communicate via IP with phone and PC users, delivering improved communications and productivity.
Wi-Fi Hotspot Services	• The access zone router and service selection gateway services features can be used to deploy secure public WLAN access services with an integrated HWIC-AP for small sites or with Cisco Aironet access points for larger sites. Wi-Fi hotspot services can be offered for additional revenue for public locations (e.g., restaurants, hotels, airports, etc.) or a value-added service for customer satisfaction.

Table 6. Chassis Specifications

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Product Architecture				
DRAM	• Default: 128 MB • Maximum: 384 MB	• Default: 256 MB • Maximum: 768 MB	• Default: 256 MB • Maximum: 1 GB	

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Compact Flash	• Default: 64 MB • Maximum: 128MB	• Default: 64 MB • Maximum: 256 MB		
Fixed USB 1.1 Ports	1	2		
Onboard LAN Ports	2-10/100		2-10/100/1000	
Onboard AIM (Internal) Slot	2			
Interface Card Slots	• 4 slots; 2 slots support HWIC, WIC, VIC, or VWIC type modules • 1 slot supports WIC, VIC, or VWIC type modules • 1 slot supports VIC or VWIC type modules	4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules		
Network-Module Slot	No	1 slot, supports NM and NME type modules	1 slot, supports NM, NME and NME-X type modules	1 slot, supports NM, NME, NME-X, NMD and NME-XD type modules
Extension Voice Module Slot	0		1	
PVDM (DSP) Slots on Motherboard	2		3	
Integrated Hardware-Based Encryption	Yes			
VPN Hardware Acceleration (on Motherboard)	DES, 3DES, AES 128, AES 192, and AES 256			
Optional Integrated In-Line Power (PoE)	Yes, requires AC-IP power supply			
Console Port (up to 115.2 kbps)	1			
Auxiliary Port (up to 115.2 kbps)	1			
Minimum Cisco IOS Software Release	12.3(8)T			
Rack Mounting	Yes, 19-inch	Yes, 19- and 23-in. options		
Wall Mounting	No	Yes	No	No
Power Requirements				
AC Input Voltage	100 to 240 VAC, autoranging			
AC Input Frequency	47-63 Hz			
AC Input Current	2A (110V) 1A (230V)		3A (110V) 2A (230V)	
AC Input Surge Current	50A maximum, one cycle (-48V power included)			
AC-IP Maximum In-Line Power Distribution	120W	160W	240W	360W
AC-IP Input Current	4A (110V) 2A (230V)		8A (110V) 4A (230V)	
AC-IP Input Surge Current	50A maximum, one cycle (-48V power included)			
DC Input Voltage	No DC Power Option available	24 to 60 VDC, autoranging positive or negative		
DC Input Current	• No DC Power Option available	• 8A (24V) • 3A (60V) • Startup current 50A<10 ms	• 12A (24V) • 5A (60V) • Startup current 50A<10 ms	

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Typical Power Dissipation (No Modules)	42W (143 BTU/hr)	32W (109 BTU/hr)	54W (184 BTU/hr)	58W (197 BTU/hr)
Power Dissipation-AC without IP Phone Support	150W (511 BTU/hr)	170W (580 BTU/hr)	280W (955 BTU/hr)	280W (955 BTU/hr)
Power Dissipation-AC without IP Phone Support	150W (511 BTU/hr)	170W (580 BTU/hr)	280W (955 BTU/hr)	280W (955 BTU/hr)
Power Dissipation-AC with IP Phone Support-System Only	150W (511 BTU/hr)	210W (717 BTU/hr)	310W (1058 BTU/hr)	370W (1262 BTU/hr)
Power Dissipation-AC with IP Phone Support-IP Phones	180W (612 BTU/hr)	160W (546 BTU/hr)	240W (819 BTU/hr)	360W (1128 BTU/hr)
Power Dissipation-DC	Not applicable	180W (614 BTU/hr)	300W (1024 BTU/hr)	300W (1024 BTU/hr)
RPS	No	Ext emalonly, connector for RPS provided by default		
Recommended RPS Unit	No RPS option	Cisco RPS-2300 Redundant Power System		
Environmental Specifications				
Operating Temperature	32°to 104°F (0°to 40°C)			
Non-Operating Temperature	-4°to 149°F (-20°to 65°C)	-40°to 158°F (-40°to 70°C)		
Maximum Operating Temperature at Altitude	• 40°C @ sea level • 31°C @ 6,000 ft (1800 m) • 25°C @ 10,000 ft (3000 m) Note: Derate 1.5°C per 1000 ft	• 40°C @ sea level • 40°C @ 6,000 ft (1800 m) • 30°C @ 13,000 ft (4000 m) • 27.2°C @ 15,000 ft (4600 m) Note: Derate 1.4°C per 1,000 ft above 6,000 ft		
Operating Humidity	10 to 85% non-condensing	5 to 95%, non-condensing		
Dimensions (H x W x D)	• 1.72 x 17.5 x 16.5 in. • (43.7 x 445 x 419 mm)	• 1.75 x 17.25 x 16.4 in. • (44.5 x 438.2 x 416.6 mm)	• 3.5 x 17.25 x 16.4 in. • (88.9 x 438.2 x 416.6 mm)	
Rack Height	1 rack unit (1RU)		2RU	
Weight (Fully Configured)	13.7 lb (6.2 kg)	14 lb (6.4 kg)	25 lb (11.4 kg)	
Noise Level (Min/Max)	• 39 dBA for normal operating temperature (<90°F/32.2°C) • 53.5 dBA (@ maximum fan speed)	• 47 dBA for normal operating temperature (<90°F/32.2°C) • 57 dBA (@ maximum fan speed)	• 44 dBA for normal operating temperature (<90°F/32.2°C) • 53 dBA (@ maximum fan speed)	

BIBLIOGRAFÍA

1. Vivek Alwayn, "Advanced MPLS Design and Implementation", Cisco Press – USA, 2002.

2. Luc De Ghein, "MPLS Fundamentals", Cisco Press – USA, 2007.

3. Ivan Pepelnjak, Jim Guichard, Jeff Apcar, "MPLS and VPN Architectures, Volume II", Cisco Press – USA, Junio 2003.

4. Lancy Lobo, "MPLS Configuration on Cisco IOS Software", Cisco Press – USA, Octubre 2005.

5. William Stallings, "The Internet Protocol Journal, MPLS", Cisco Systems, Inc. – USA, Setiembre 2001.

6. Daniel Diaz, "MultiProtocol Label Switching, MPLS", Universidad de Ingenieria – Perú, Octubre 2007.

7. E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture", IETF Standards Track RFC 3031, Enero 2001.

8. L. Andersson, P. Doolan, N. Feldman, A. Fredette, B. Thomas, "LDP Specification", IETF Standards Track RFC 3036, Enero 2001.

9. F. Le Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen R. Krishnan, P. Cheval, J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services", IETF Standards Track RFC 3270, Mayo2002.

10. María Sol Canalis, "MPLS Multi Protocol Label Switching: Una Arquitectura de Backbone para la Internet del Siglo XXI", Universidad Nacional del Nordeste – Argentina, 2003.

11. Martha Arellano, Julian Hernández, "Seminario de Tecnología MPLS", Instituto Tecnológico de Telefonos de Mexico S.C – Uruguay, 2004.

12. Anette Donnell, "Deploying MPLS Traffic Engineering", Junniper Networks, Inc. – USA, Octubre 2005.