UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

CLASES DE SERVICIO EN REDES MPLS Y SU APLICACIÓN PARA BRINDAR SERVICIOS DIFERENCIADOS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

THOMAS HENRY NECIOSUP RAMIREZ

PROMOCIÓN
2001- I

LIMA – PERÚ
2006

CLASES DE SERVICIO EN REDES MPLS Y SU APLICACIÓN PARA BRINDAR SERVICIOS DIFERENCIADOS

Dedico este trabajo a:

Mi madre, por sus sabios consejos y apoyo incondicional,

Mi padre, por el ejemplo de perseverar y luchar en la vida,

Y a mis hermanos por sus deseos de superación.

SUMARIO

El presente trabajo pretende describir el desarrollo de la calidad de servicio y sus aplicaciones en *backbones* con infraestructura MPLS. La tecnología MPLS es considerada una tecnología emergente y que esta siendo adoptada rápidamente por los principales proveedores de servicios del orbe. Se torna muy importante con los desarrollos realizados por el grupo IETF con respecto a ingeniería de tráfico, redes privadas virtuales y servicios diferenciados. También, entes externos a el IETF, como el fabricante CISCO, han desarrollado técnicas que apoyan aún más la implementación del protocolo MPLS en las redes que están a la vanguardia de la tecnología.

En el capitulo II se describe la arquitectura de la tecnología MPLS, sus funcionalidades y bondades.

En el capitulo III se toca el tema de ingeniería de tráfico sobre redes MPLS, lo cual es muy importante porque permite conocer la manera de cómo implementar la red para que, en caso de falla de algún enlace, los servicio de sus clientes soportados no se vea afectado.

En el capitulo IV se expone a detalle la arquitectura de calidad de servicio, ahondando en la arquitectura de servicios diferenciados y su impacto sobre MPLS en la clasificación de flujos de tráfico.

En el capitulo V se muestran los criterios de diseño e implementación de una red MPLS basándose en los desarrollos de ingeniería de tráfico y calidad de servicio.

ÍNDICE

CAPÍTULO V

MPLS: DISEÑO E IMPLEMENTACIÓN

PRÓLOGO

Desde la aparición de Internet y su incorporación a una red de tráfico comercial, en 1992, Internet ha crecido rápidamente, es decir, a pasado de ser una simple red de investigación a una red de datos comercial ampliamente difundida en el mundo.

Internet ha llegado a ser una herramienta muy importante en nuestro que hacer diario, en los campos de negocios empresariales, educación, comercio y entretenimiento. Como consecuencia de este crecimiento, los proveedores de servicios tienen la necesidad de crecer en capacidad de ancho de banda, cantidad de equipos de red y expansión geográfica.

Los nuevos desarrollos impulsan a converger la voz, video conferencia, televisión, etc. a la tecnología IP como medio de comunicación. Esto, impulsa a los proveedores de servicio a buscar mejores estándares de calidad de servicio. En esta búsqueda, se encuentra una tecnología emergente llamada MPLS (*MultiProtocol Label Switching*). El desarrollo paralelo en campos como ingeniería de tráfico, calidad de servicio, redes privadas virtuales y tecnologías de acceso como *Metro*

Ethernet, hacen posible que MPLS sea la tecnología preferida por los principales proveedores de servicio del orbe.

MPLS innova el paradigma de envío de paquetes, utiliza envío de paquetes basados en etiquetas. Las motivaciones que tienen los proveedores de servicio para migrar a MPLS son la alta escalabilidad, mayor velocidad en el envío de paquetes, integración con diferentes tecnologías de la capa de enlace, aplicación de ingeniería de tráfico, implementación de redes privadas virtuales, veloz enrutamiento en caso de falla de un recurso de red y principalmente la alta calidad de servicio que se puede brindar.

En un inicio las redes no brindaban calidad de servicio a sus usuarios, hoy en día con la aparición de aplicaciones de tiempo real, la calidad de servicio se hace estrictamente necesaria.

Este informe intenta dar a conocer las bondades que brindan los servicios diferenciados, es decir, la clasificación del tráfico y los beneficios que ofrece al ser implementado en redes con arquitectura MPLS para así brindar servicios diferenciados a sus usuarios.

CAPÍTULO I

DESCRIPCIÓN GENERAL

1.1 INTRODUCCIÓN

Desde el punto de vista tecnológico Internet ha impactado nuestras vidas más que cualquier otra tecnología en los últimos años. Hoy en día podemos observar equipos que manejan tecnología *wireless*, aplicaciones de Internet, Voz sobre IP, Telefonía IP, *webcast* video, PCs, *hosts* e incluso tráfico *Mainframe* sobre Internet. El rápido crecimiento de World Wide Web ha propalado la necesidad de redes IP para transportar la comunicación de datos.

Portadoras y proveedores de servicios están en una constante expansión de sus *backbones* para brindar mejores niveles de satisfacción a sus clientes. Recientemente, con la introducción del DWDM (*Dense Wavelength Division Multiplexing*) en el *backbone* de una red, se puede lograr enormes anchos de banda a través del existente par de fibra instalado, esto en base a la inyección de múltiples longitudes de onda en el cable de fibra óptica. Gracias a la disposición de estas grandes cantidades de ancho de banda se ha podido integrar el tráfico de redes públicas e Internet, con el de las redes privadas.

El factor económico siempre juega un papel fundamental a la hora de definir una nueva tecnología para el *backbone*, por tal motivo era necesario desarrollar una nueva tecnología de tal manera que la actualización a esta no debería de ser muy costosa. Las redes tradicionales fueron desarrolladas en base a circuitos privados virtuales como Frame-Relay y ATM (*Asynchronous Transfer Mode*). En los últimos años han sido iniciados varios esfuerzos y actividades en el desarrollo de MPLS (*MultiProtocol Label Switching*), muchos de los cuales ya han impactado considerablemente en las redes IP. La IETF formó un grupo de trabajo para MPLS, estandarizando una base tecnológica de "conmutación de etiquetas" y la implementación de LSP (*Label-Switched Path*) sobre varias tecnologías de la capa de enlace tales como: paquetes sobre SONET (POS), Frame Relay, ATM y Tecnologías LAN (como por ejemplo Ethernet y sus variantes, Token Ring, etc.).

Las Técnicas de conmutación de etiquetas están siendo implementadas en redes de portadoras y proveedores de servicios. Esto ha dado un nuevo giro para el rediseño en la arquitectura del *backbone* de los ISPs.

MPLS tiene la habilidad de poder influenciar en el rediseño de la arquitectura y reingeniería de Internet. MPLS es la tecnología que esta manejando el presente y futuro de las redes IP.

El desarrollo de la tecnología MPLS sobre *backbones* de los proveedores de servicios de Internet (ISPs) es posible debido a lo transparente que resulta para el usuario final. MPLS mejora el tradicional reenvió de paquetes usado por la arquitectura de Internet actual. Esta tecnología usa la información de las etiquetas adjuntas a los

paquetes IP, celdas ATM u otro *frame* de capa2, para tomar las decisiones de reenvió, lo cual impacta en la arquitectura de *routing* establecida.

1.2 NECESIDAD DE CALIDAD DE SERVICIO

Es un hecho que durante los últimos años el crecimiento de Internet ha sido exponencial y como consecuencia se han desarrollado nuevos servicios y aplicaciones cada vez más y más complejas, obviamente con grandes requerimientos de ancho de banda. A raíz de esto, la tecnología de Internet ha sufrido grandes cambios desde sus inicios, en los cuales los requerimientos de ancho de banda eran mínimos. Actualmente Internet es la manera más rápida de realizar transacciones entre las empresas y sus clientes minimizando los costos de operación por transacción y mejorando sus procesos.

Se puede decir que *calidad de servicio* es la habilidad que tiene una red para proporcionar el mejor servicio a un tráfico seleccionado sobre otros. Esta selección se puede realizar sobre diferentes tecnologías como Frame Relay, ATM, Ethernet y las variantes de 802.1, SONET y redes IP.

Por ejemplo, consideremos a un usuario que realiza una llamada usando un servicio de voz sobre IP (VoIP). Este usuario esperará que la llamada sea de la misma calidad que una llamada con tecnología tradicional. Si la llamada es de baja calidad lo más probable es que este usuario no vuelva a usar dicho servicio, esto dependerá de lo que pueda realizar el proveedor de servicios de VoIP para asegurar que la llamada de VoIP sufra un pequeño o ningún *jitter* (retardo variable), retardo en un sentido (*one-way*) de unos 150ms y que el ancho de banda para la llamada de VoIP esté garantizado entre 8 y 12 Kbps, asumiendo el CODEC de compresión G.729.

Es así que nace la necesidad de calidad de servicio para que pueda proporcionar un mejor y predecible servicio.

1.3 OBJETIVOS GENERALES

Este informe ha sido elaborado con la finalidad de hacer conocer la evolución de tecnologías emergentes así como el aporte a la nueva arquitectura de Internet que están implementando los principales proveedores de servicios de Internet. MPLS es la tecnología que están adoptando los principales ISPs del mundo para brindar un mejor servicio a sus usuarios finales, para esto se apoya de los desarrollos realizados en las áreas de calidad de servicio (QoS), ingeniería de trafico (TE), y protocolos de *routing*.

1.4 ORGANIZACIÓN DEL INFORME

En esta sección se muestra una sinopsis del contenido de los capítulos que conforman este informe para brindar una breve descripción de los temas que serán profundizados a partir del siguiente capítulo.

- Capitulo II "MPLS"

  MPLS es introducido como una tecnología que está manejando las futuras redes IP, incluso Internet. MPLS describe un nuevo paradigma de reenvío de paquetes para Internet, el cual afecta su ingeniería de tráfico y calidad de servicio. También, se describen los beneficios que brinda MPLS así como su arquitectura.

- Capitulo III "MPLS: Ingeniería de Trafico (TE)"

  Gracias al desarrollo de la ingeniería de tráfico, el flujo de tráfico a través del *backbone* de un proveedor de servicio puede ser optimizado. Esto incluye el

aprovisionamiento de una alta calidad de servicio, mejorando la utilización de los recursos de red al distribuir el tráfico de manera uniforme a través de los enlaces y proporcionando una rápida recuperación cuando un nodo o enlace de la red falla.

- Capitulo IV "MPLS: Calidad de servicio (QoS)"

Los proveedores de servicios que ofrecen servicios IP sobre un *backbone* MPLS deben necesariamente soportar calidad de servicio sobre su infraestructura MPLS diseñada. MPLS extrae lo mejor de la arquitectura de calidad de servicio para poder brindar a sus usuarios finales servicios IP garantizados.

- Capitulo V "MPLS: Diseño e Implementación"

Principalmente este capitulo expondrá los criterios a tomar en el diseño de una red MPLS. También, se incluirá implementaciones en redes MPLS usando los desarrollos de ingeniería de tráfico y calidad de servicio. Se comentará la implementación sobre la tecnología DWDM que consiste en *multiplexar* señales de diferentes longitudes de onda en una sola fibra.

CAPÍTULO II

MULTI PROTOCOL LABEL SWITCHING (MPLS)

2.1 MPLS: INTRODUCCIÓN

Multiprotocol Label Switching Protocol (MPLS) es una tecnología emergente que quiere solucionar muchos de los problemas existentes, asociados con el reenvió de paquetes. Miembros de la comunidad del IETF trabajaron arduamente para brindar los niveles básicos exigidos para marcar y evolucionar las ideas de muchos vendedores y usuarios respecto al concepto de "*label switching*" (conmutación de etiquetas). En el documento *draft-ietf-mpls-framework-05* [5], publicado por el IETF, se publica el marco que describe la meta principal. Este marco menciona lo siguiente:

La principal meta del grupo de trabajo MPLS es estandarizar una base tecnológica que integre el paradigma de intercambio y reenvío de etiquetas con el concepto de *routing*. Esta base tecnológica (intercambio de etiquetas) fue desarrollada para mejorar el costo y *performance* en la capa de red, mejorando las futuras proyecciones de la capa de red y proporcionar gran flexibilidad en el envío de (nuevos) servicios de *routing* (nuevos servicios de *routing* son permitidos sin un cambio en el paradigma de reenvío de paquetes).

La gran diferencia entre MPLS y las tradicionales tecnologías WAN es la forma en que las etiquetas son asignadas y la capacidad de cargar una pila de etiquetas

adjuntadas a un paquete. El concepto de una pila de etiquetas habilita nuevas aplicaciones, tales como TE, VPNs (V*irtual Private Networks)*, *Fast Rerouting* en caso de falla de un nodo o enlace, y demás.

El reenvío de paquetes en MPLS está en completo contraste a las redes no orientadas a conexión de hoy en día, donde cada paquete es analizado de un salto a otro, su cabecera capa 3 es revisado y una independiente decisión de reenvío (*fordwarding*) es hecha basada en la información extraída de el algoritmo de ruteo de la capa de red. Más adelante en la sección "2.5" se expondrá como se toman las decisiones de reenvío de paquetes MPLS.

2.2 ¿QUE ES MPLS?

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 (*Virtual 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 ruteo (*routing*) usada en la capa 3. El principal objetivo de MPLS es crear una red flexible y escalable que proporcione una mayor estabilidad y *performance* 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, *Edge LSR* (*Edge Label-Switched 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 ruteo (*routing*) 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 Edge LSR de salida, y paquete será enviado a su destino.

El termino *MultiProtocolo* indica que MPLS trabaja con cualquier protocolo de la capa de Red.

2.3 EVOLUCIÓN ES MPLS

La meta inicial de la conmutación de etiquetas fue traer la velocidad de la conmutación a nivel de capa 2 a la capa3. Esta inicial justificación para tecnologías como MPLS no es percibida como el principal beneficio, debido a los nuevos *switches* de capa 3, basado en la tecnología ASIC (*Application-eSspecific Integrated Circuit*), que pueden realizar búsquedas de rutas a suficientes velocidades para soportar más tipos de interfaces.

El inmenso interés en desarrollar la conmutación de etiquetas inicio la formación del grupo de trabajo del IETF MPLS en 1997.

MPLS se ha desarrollado gracias a otras tecnologías que le han antecedido, incluyendo versiones propietarias de implementaciones de conmutación de etiquetas tales como *Tag Switching* de CISCO, ARIS (*Agrégate Route-Based IP Switching*) de IBM, CSR (*Cell-Switched Router*) de Toshiba, *IP Switching* de IPSILON, e *IP Navigator* de LUCENT.

Tag Switching, inventada por CISCO, fue proporcionada a los usuarios en Marzo de 1998. Desde el inicio de *Tag Switching*, CISCO ha estado trabajando con el IETF para desarrollar y ratificar el estándar MPLS, el cual ha incorporado muchas de las características y beneficios del *Tag Switching*.

2.4 BENEFICIOS DE MPLS

El método de conmutación de etiquetas permite a los *routers* y switches ATM tomar decisiones de reenvío de paquetes basándose en el contenido de una simple etiqueta, no como en las complejas decisiones de ruteo basados en la dirección IP de destino. Esta técnica de conmutación de etiquetas trae muchos beneficios a las redes basadas en IP.

- VPNs— Con el uso de MPLS, los proveedores de servicios pueden crear VPNs de capa 3 a través del *backbone* de red para múltiples clientes, usando la misma infraestructura, y sin la necesidad de cifrar 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 portadoras o *carriers* emplean 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 *carriers* pueden migrar muchas de las funciones del *ATM control plane* 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.

Proveedores de servicio han aprovechado las mejoras de MPLS en comparación con redes IP sobre ATM convencionales. MPLS combina la *performance* y capacidad de *switching* de la capa 2 con la escalabilidad del *routing* 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.

Las más importantes características de MPLS son:

MPLS es soportado por todos los protocolos de la capa de red.

MPLS habilita eficientemente el envío de servicios IP sobre una red ATM.

MPLS soporta la creación de múltiples rutas entre una fuente y un destino en un *backbone* íntegramente conformado por *routers* de Internet.

Con la incorporación de MPLS en la arquitectura de red de un proveedor de servicios, reducen sus costos, incrementan sus ingresos y productividad, se puede proporcionar servicios diferenciados y se obtiene una gran ventaja sobre otros *carriers* que no ofrecen servicios MPLS tales como VPNs o ingeniería de tráfico.

2.5 ARQUITECTURA MPLS

Como en cualquier tecnología nueva, muchos términos nuevos son introducidos para describir los dispositivos que conforman tal arquitectura. Estos nuevos términos describen la funcionalidad de cada dispositivo y sus roles en la estructura MPLS.

2.5.1 MPLS y la arquitectura de Internet

Desde el desarrollo de ARPANET, el predecesor de la actual red de Internet, la arquitectura de Internet ha ido constantemente cambiando, esto en respuesta a los avances tecnológicos, crecimiento y ofertas de nuevos servicios. El más reciente cambio en la arquitectura de Internet es la adición de MPLS.

Una consideración especial es que el mecanismo de reenvío de paquetes "*forwarding*" de Internet, no ha cambiado desde los días de ARPANET. El mayor cambio ha sido la migración de EGP (*Exterior Gateway Protocol*) a BGPv4 (*Border Gateway Protocol versión 4*), la implementación de CIR (*Classless Interdomain routing*) y la constante ampliación de ancho de banda y la instalación de CPEs (*Customer Premise Equipment*), o *routers* de clientes, con más capacidades.

MPLS no solamente ha impactado el mecanismo de reenvío de paquetes IP, sino también, la determinación de rutas en cada salto. Esto implica una fundamental re-arquitectura de Internet. Como consecuencia, MPLS puede simplificar el desarrollo de IPv6 porque el mecanismo de *envío de paquetes* usado por MPLS para IPv4 puede ser aplicado a IPv6 con el uso de protocolos de *routing* que soportan direccionamiento IPv6.

MPLS esta siendo desarrollada rápidamente por el beneficio inmediato y directo a la red de Internet. El mayor beneficio inmediato de MPLS respecto al *backbone* convencional de un proveedor de servicios es la ingeniería de tráfico, que brinda la capacidad de manejar los enlaces en caso de congestión, y utilizar los enlaces en carga compartida sobre enlaces no utilizados, aprovechando los recursos de ancho de banda en el *backbone*. Esto se traduce en alta eficiencia y ahorro de costos.

Las actuales VPNs en Internet están implementadas usando túneles IPSec (*IP Security*) sobre Internet. Estas VPNs tienen una cabecera muy grande, como consecuencia del encabezamiento de un protocolo a otro, esto hace lento el servicio y se requiere equipos con gran capacidad de procesamiento. VPNs MPLS sobre Internet permite a los proveedores de servicio ofrecer niveles de servicio comparados a los servicios tradicionales de ATM o Frame Relay. Otra desventaja de los tradicionales túneles GRE (*Generic Routing Encapsulation*) e IPSec es que no son escalables. MPLS VPNs pueden ser implementadas sobre redes IP privadas.

2.5.2 MPLS: Modo de operación

La principal idea de MPLS es que usa etiquetas para reenviar paquetes. El nodo de ingreso a la red MPLS asigna un particular FEC (*Fordwarding Equivalence Class*) al paquete que ingresa a la red. La FEC asignada a un paquete es codificada como un valor conocido como *etiqueta*. Así los paquetes son etiquetados antes de ser reenviados. En los siguientes altos, no se analizará la cabecera de la capa de red del paquete. Esta etiqueta es usada como un índice en una tabla que contiene el siguiente salto y una nueva etiqueta. La antigua etiqueta es reemplazada con la nueva etiqueta, y el paquete es reenviado al siguiente salto.

En las redes MPLS, toda la capacidad de reenvío es manejada por las etiquetas. A continuación se describen las ventajas de usar este tipo de reenvío sobre los tradicionales métodos de reenvío de la capa de red.

- El reenvío de paquetes en MPLS puede ser manejado por *switches*, los cuales pueden hacer uso de búsquedas de etiquetas e incluso reemplazo de etiquetas pero no pueden hacer análisis de la cabecera de la capa de red. Los *switches* ATM implementan una función similar al conmutar celdas basadas en VPI/VCI encontradas en la cabecera ATM. Los *switches* ATM necesitarían ser controlados por un elemento de control IP basado en MPLS como el LSC (*Label Switch Controller*), lo cual forma la base de la integración de IP con ATM usando MPLS.
- Un paquete es asignado a una FEC cuando ingresa a la red. El *router* de ingreso puede usar alguna información que tiene del paquete, tal como puerto o interfaz de ingreso, aún si esta información no puede ser obtenida de la cabecera de la capa de red. Un paquete que ingresa a la red a través de un *router* específico puede ser etiquetado de manera diferente en el caso de que el mismo paquete ingrese por otro *router* diferente. Como resultado, las decisiones de reenvío que dependen del *router* de ingreso pueden ser tomadas fácilmente. Esto no puede hacerse con las decisiones de reenvío convencionales porque la identidad del *router* de ingreso no viaja en la cabecera de la capa de red. Por ejemplo, los paquetes que ingresan a la red por diferentes interfaces del CPE (*Customer Premise Equipment*) *router* podrían ser asignados a diferentes FECs. La etiqueta adjuntada representaría

la correspondiente FEC asignado al paquete. Esta funcionalidad forma la base del concepto de VPNs sobre MPLS (MPLS-VPN).

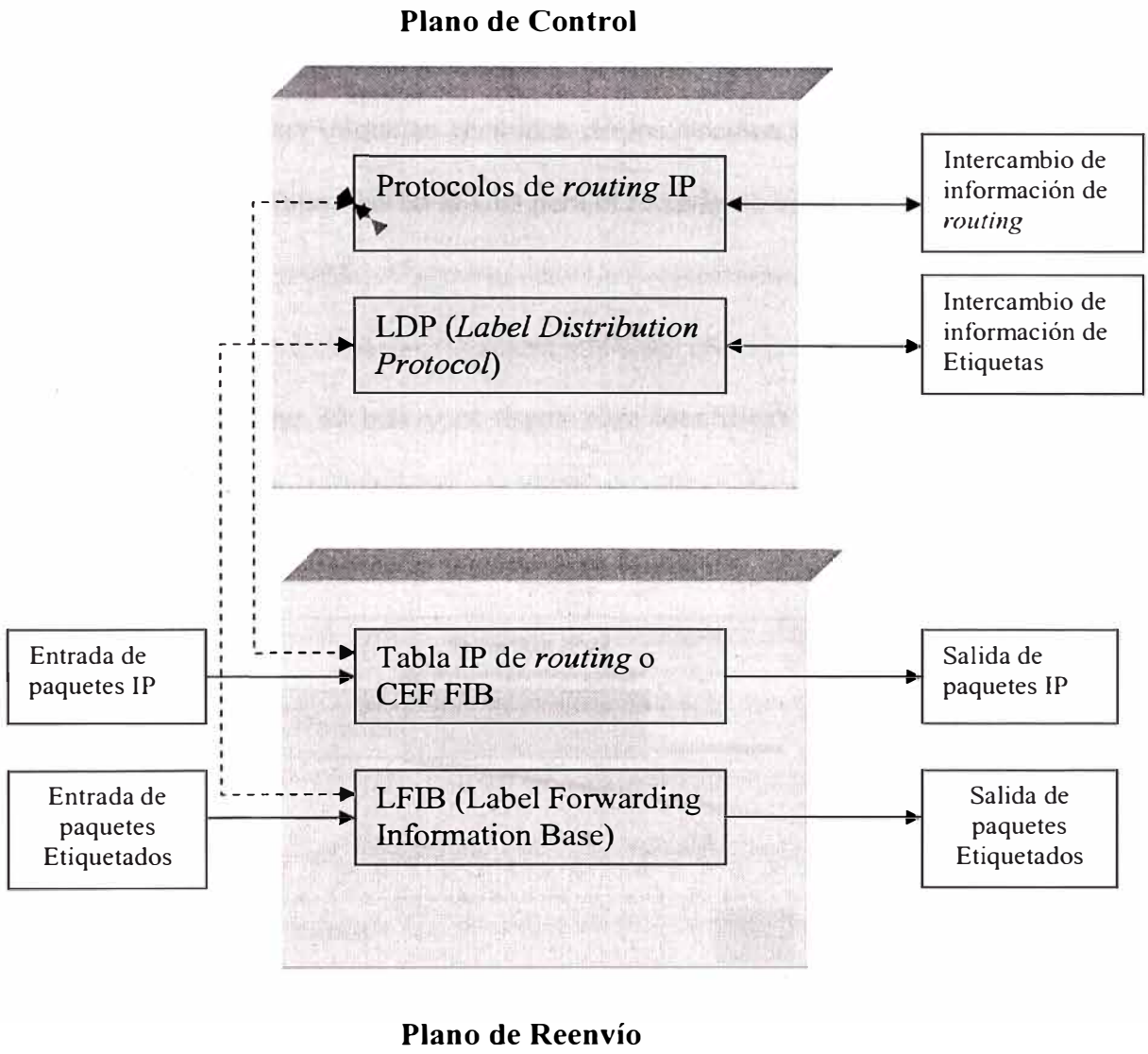
- La ingeniería de tráfico en la red fuerza al paquete a seguir una ruta particular, que podría ser una ruta subutilizada. Esta ruta es específicamente seleccionada cuando o antes de que el paquete ingrese a la red, en preferencia a ser seleccionado por el algoritmo de *routing* dinámico que indica como el paquete viajará por la red. En MPLS, una etiqueta puede ser usada para representar la ruta, entonces la identidad de la ruta explicita no será necesario que este dentro de la cabecera del paquete. Esta funcionalidad forma la base del concepto de ingeniería de tráfico en MPLS (MPLS-TE).
- La clase de servicio (CoS) de un paquete puede ser determinada por el nodo MPLS de ingreso (PE). Un nodo MPLS puede aplicar diferentes umbrales de descarte o políticas a diferentes paquetes. Los siguientes saltos reforzarán esta política usando un grupo de PHBs (*Per-Hop Behaviors*). MPLS permite (pero no requiere) la precedencia o clase de servicio a ser completamente o parcialmente deducida de la etiqueta. En este caso la etiqueta representa la combinación de un FEC y la precedencia o clase de servicio. Esta funcionalidad forma la base del concepto de Calidad de Servicio sobre MPLS (MPLS-QoS).

2.6 MPLS: ARQUITECTURA del NODO

El nodo MPLS es considerado a los dispositivos que manejen la tecnología MPLS para el envío de etiquetas. Pueden ser denominados P (*Provider core router*), PE (*Provider Edge router*), tanto el *router* P como el PE son LSRs. La arquitectura del

nodo está conformada por el plano de reenvío y el plano de control. Los nodos MPLS pueden funcionar en la capa 2 y la capa 3 (*switching* y *routing*) además de conmutar paquetes etiquetados. En la Figura 2-1 se muestra la arquitectura básica de un nodo MPLS.

FIGURA 2-1 *Arquitectura del Nodo MPLS*



2.6.1 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 tabla LIB (*Label Information Base*) y la tabla LFIB. La tabla 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.

- **Etiqueta**

Una etiqueta tiene 32 bits y es usada para identificar un FEC, usualmente de significado local. La etiqueta, la cual es adjuntada a un paquete particular, representa la FEC a la cual el paquete será asignado.

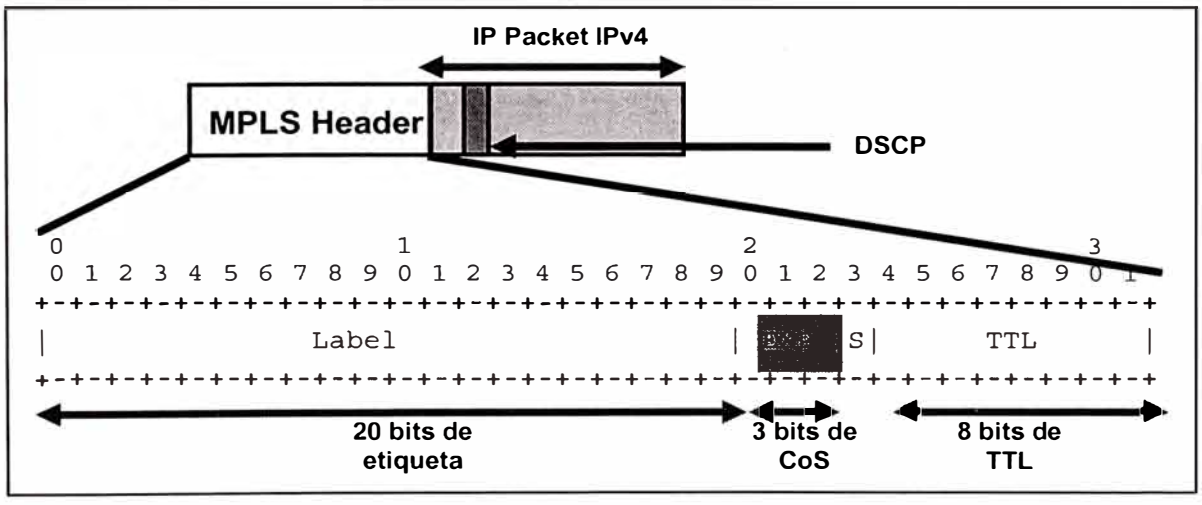


FIGURA 2-2 *Formato de Etiqueta MPLS*

Esta etiqueta esta dividida en los siguientes Campos: etiqueta (*label*) de 20 bits, clase de servicio (CoS) de tres bits, el campo S (*Stack*) de un *bit* que indica la

posición de la etiquetes, si el valor del *bit* es 1, entonces indicará la posición inferior, y finalmente el campo TTL (*time to live* o tiempo de vida) de 8 bits.

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.

Cabecera ATM

GFC	VPI	VCI	PTI	CLP	HEC	Data
	|------- **Etiqueta** ------|					

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 llamado *cabecera shim*. 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.

Cabecera Capa2	**Etiqueta**	Cabecera Capa3	Cabecera Capa4	Data

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 de 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.

En la siguiente tabla se listan los valores reservados para valores de etiquetas.

TABLA 2-1 *Valores reservados de etiquetas*

Etiqueta	Descripción
0	Etiqueta NULL para IPv4. El valor de esta etiqueta es legal solo cuando esta en la parte inferior de la pila de etiquetas. Esto quiere decir que la pila de etiquetas debe de ser obviado y el reenvío de paquetes debe de ser basado en la cabecera IPv4.
1	Etiqueta de alerta. Esta etiqueta es análoga al uso de la opción "*router alert*" en el campo opciones del paquete IP. Este valor es legal en cualquier posición dentro de la pila con excepción de la posición inferior.
2	Etiqueta NULL para Ipv6. Concepto similar al usado para IPv4.
3	Etiqueta NULL implícita. Es la etiqueta que un nodo MPLS puede asignar y distribuir pero que nunca aparecerá en la actual encapsulación. Esta etiqueta es usada en el penúltimo salto.
4 -- 15	Reservado para uso futuro.

- **Pila de Etiquetas (S)**

El *bit* S (*stack*), dentro de la etiqueta, implementa el apilamiento de etiquetas en MPLS, es decir habilita que más de una etiqueta sea adjuntada a un paquete IP. El *bit* S tiene el valor de 1 cuando se indica la etiqueta inferior de la pila. Las

demás etiquetas tienen el valor de 0. En el caso que existan varias etiquetas adjuntadas al paquete IP, entonces la etiqueta superior estaría posicionada a la derecha de la cabecera de la capa2 y la etiqueta inferior estaría posicionada a la izquierda de la etiqueta de la capa3. El reenvío de paquetes es logrado usando el valor de la etiqueta superior en la pila. El *routing* de IP *unicast* no usa apilamiento de etiquetas, pero VPNs e Ingeniería de Tráfico en MPLS si lo usan en su operación.

- **TTL**

El campo TTL (*time to live*) es similar al campo usado en la cabecera IP. El nodo MPLS solo procesa el campo TTL de la etiqueta superior de la pila de etiquetas.

2.6.1.1 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.

FIGURA 2-3 *Estructura LFIB*

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.

2.6.1.2 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.

2.6.2 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 *routing*, entonces el nodo MPLS necesitará tener una tabla de *routing*. Para obtener una tabla de *routing*, se necesita un protocolo de *routing* (o se pueden usar rutas estáticas lo cual no es recomendable). Ahora que se tiene una tabla de *routing*, es necesario intercambiar las etiquetas. Este intercambio de etiquetas se puede lograr utilizando el protocolo LDP (*Label Distribution Protocol*) desarrollado por IETF, que es una versión del protocolo TDP (*Tag Distribution Protocol*) desarrollado por CISCO.

Protocolos l*ink-state* 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 *routers* convencionales, la tabla de *routing* 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 *routing* 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 *Routing Unicast*.- Construye la tabla FEC utilizando un convencional IGP tal como OSPF, IS-IS ú otro. La tabla de *routing* es usada para intercambiar la asociación entre etiquetas con los nodos MPLS adyacentes para las sub-redes que están contenidas en la tabla de *routing* IP. La distribución de la asociación entre etiquetas se hace usando el protocolo LDP o TDP para el caso de equipos CISCO.
- Módulo *Routing Multicast*.- Construye la tabla FEC usando un protocolo de *routing multicast* tal como PIM (*Protocol-Independent Multicast*). La tabla de *routing 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 *routing 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 *routing* 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 *routing* por VPN para las tablas FEC, las cuales son construidas usando protocolos de *routing* 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 *routing* 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 *routing* IP es usado para intercambiar la asociación entre etiquetas con los nodos MPLS adyacentes para sub-redes contenidas en la tabla de *routing* IP. La distribución de la asociación entre etiquetas es realizada usando el protocolo LDP o la versión propietaria de CISCO TDP.

2.7 ELEMENTOS MPLS

La descripción detallada de cada uno de los elementos de MPLS servirá para dar un entendimiento de la interacción entre los protocolos de la capa2, los protocolos de la capa3 y los dispositivos.

A continuación describiremos los siguientes elementos:

- LSR: *Label-Switched Router*
- LSP: *Label-Switched Path*
- LDP: *Label Distribution Protocol*

2.7.1 LSR (*Label-Switched Router*)

Una red MPLS o Internet consiste en un grupo de nodos, los cuales son llamados LSR (*router* de conmutación de etiquetas), los cuales son capaces de realizar la función de conmutación y *routing* de paquetes en base a la etiqueta que va adjuntada al paquete. Los LSRs son *routers* o *switches* MPLS que usan etiquetas para reenviar el tráfico.

Existe también el concepto de *Edge* LSR o LSR de borde, el cual principalmente etiqueta el paquete IP y lo reenvía a través de la red MPLS o remueve la etiqueta del paquete IP y lo reenvía fuera del dominio MPLS. Los *routers* que tienen todas sus interfaces manejando MPLS son llamados LSRs debido a que ellos comúnmente reenvían paquetes basados en etiquetas. Los *routers* que tienen algunas interfaces manejando MPLS están usualmente posicionados al borde del dominio MPLS. Estos *routers* también reenvían paquetes basados en la dirección IP destino y en base a etiquetas si la interfaz de salida maneja MPLS.

De manera similar para el caso de ATM se tiene los conceptos de LSR ATM y *Edge* LSR ATM.

2.7.1.1 Operación de LSR basado en paquetes

La operación de LSR basado en paquetes también es conocida como MPLS *frame mode (modo frame)*.

La operación básica de MPLS basado en paquetes que soporta *routing unicast* con un simple nivel de pila de etiquetas es ilustrada en la figura 2-4. El LSR1 hace la función de *Edge* LSR, el cual aplica la etiqueta inicial al paquete después de hacer una búsqueda convencional en la cabecera IP y asignar la correspondiente FEC al paquete. Parámetros como la interfaz de ingreso, para el caso de VPN o una ruta predeterminada definida por ingeniería de tráfico, puede también determinar la selección del FEC. Esta determinación es realizada una sola vez, al ingreso a la red MPLS.

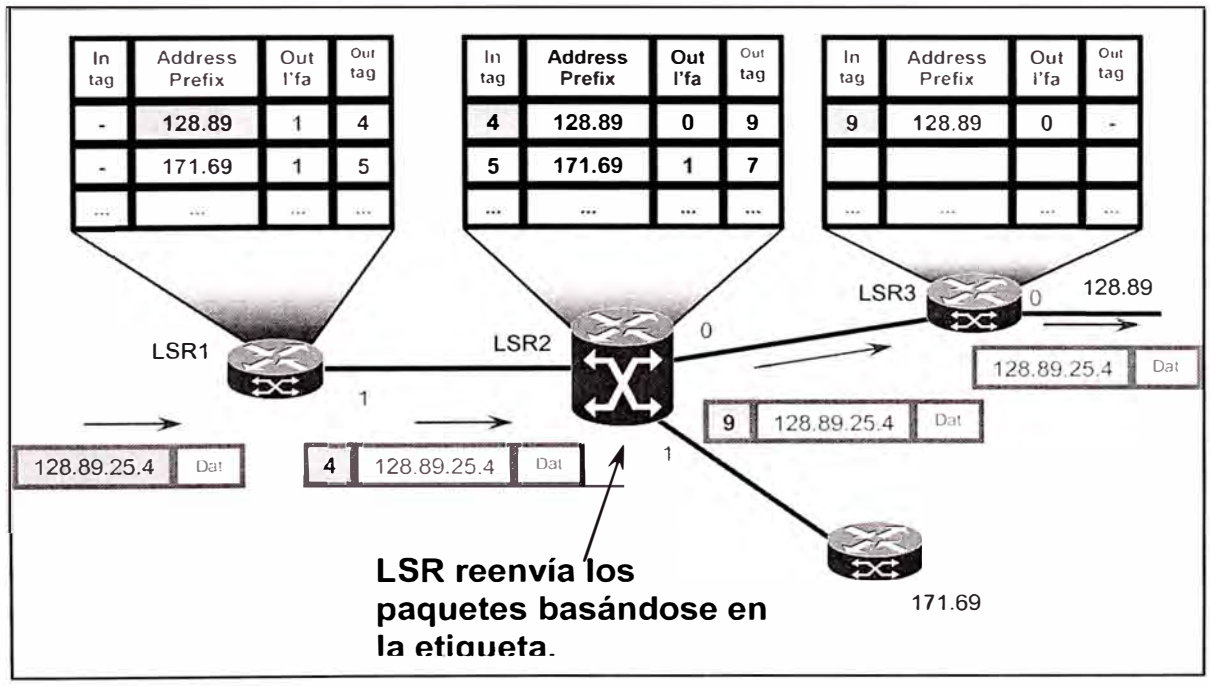


FIGURA 2-4 Operación de LSRs, simple nivel de apilamiento de etiquetas

Cada FEC está vinculada a una correspondiente etiqueta. Después que el paquete es etiquetado, los siguientes LSRs reenviarán el paquete usando solamente la etiqueta. LSRs usualmente reemplazan la etiqueta del paquete entrante con un nuevo valor que será reenviado. Al final, el LSR4 realizará una búsqueda de etiqueta, que indicará la remoción de la misma, y funcionará una búsqueda del siguiente salto a nivel de la capa3, finalmente el paquete será reenviado al siguiente salto externo.

La Figura 2-5 muestra la operación de LSR basado en paquetes con múltiples etiquetas. El LSR1 tiene la función de *Edge* LSR, el cual aplicará el inicial grupo de etiquetas al paquete después de hacer una búsqueda convencional en la cabecera IP y asignar la FEC correspondiente al paquete. LSR2 remueve la etiqueta superior 11 y de acuerdo a su tabla asigna una nueva etiqueta superior con valor 9. Al final el LSR4 buscara en su tabla las etiquetas adjuntas, removerá dichas etiquetas, y buscará a nivel de la capa3 para reenviar el paquete al siguiente salto externo.

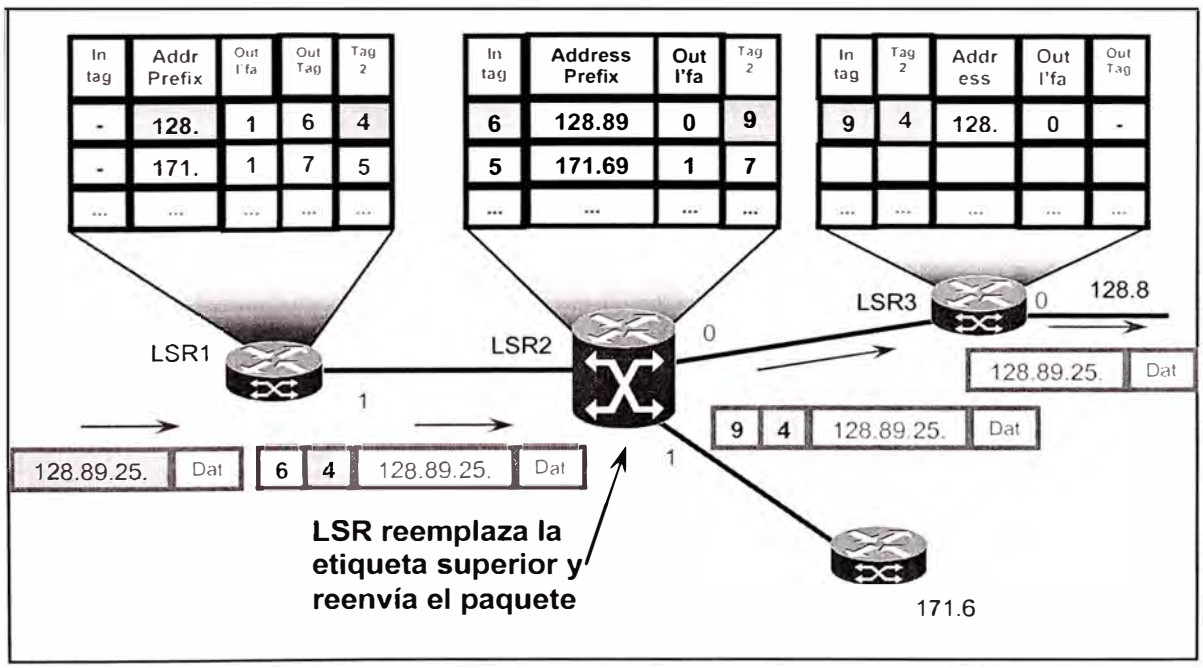


FIGURA 2-5: LSR Operación: con nivel de apilamiento múltiples etiquetas.

2.7.1.2 Operación en el penúltimo salto

La operación del LSR descrita anteriormente presenta ciertas desventajas asociadas a la doble búsqueda en el LSR3. El LSR3 necesitará examinar la pila de etiquetas y buscará la etiqueta en su LFIB, solo para saber que esta etiqueta será removida. Entonces se realizará una nueva búsqueda a nivel de la capa3 en la tabla global de *routing* o en la específica VPN asociada para poder reenviar el paquete correctamente al siguiente salto externo. La doble búsqueda en el LSR3 puede degradar el funcionamiento y la implementación del hardware de MPLS.

Para implementar el retiro de etiqueta en el penúltimo salto, el *edge* LSR3 requiere una operación de su vecino superior, LSR2, vía LDP o TDP usando una etiqueta especial conocida como *implicit-null.* Esta etiqueta toma el valor de 3 para LDP y el valor de 1 para TDP.

LSR2 remueve la etiqueta antes de enviar el simple paquete IP a LSR3. Entonces ahora sí LSR3 realiza una sola búsqueda pero solo a nivel de capa3 basado en la dirección de destino contenido en el paquete y envía el paquete al siguiente salto.

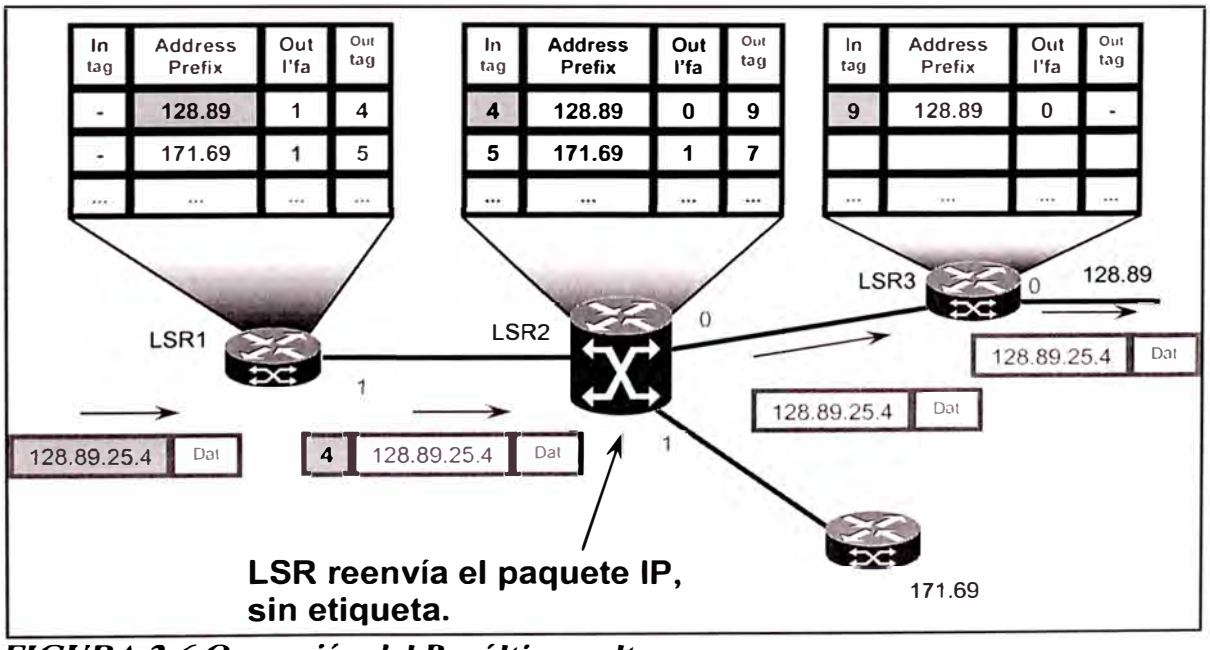


FIGURA 2-6 Operación del Penúltimo salto.

2.7.1.3 Operación del LSR ATM

Un LSR ATM usa el "Paradigma de reenvío basado en etiquetas" para transportar paquetes de capa 3 como si se trataran de celdas que son transportadas sobre una Red ATM. El concepto de MPLS sobre ATM también es conocido como MPLS *cell mode* (modo celda).

Un LSR ATM es un *switch* ATM, con la funcionalidad MPLS habilitado, que actúa como un *router* conmutador de etiquetas. ATM-LSR normalmente tienen un controlador LSC (*Label Switch Controller*), el cual realiza la función de *routing* IP con otros LSRs en la misma red MPLS.

El LSR ATM corre un protocolo de control MPLS en el plano de control y configura LVCs (*Label Virtual Circuits*), los cuales son en MPLS el análogo al convencional PVC de ATM. Es así que paquetes etiquetados son reenviados como celdas ATM. La matriz de conmutación del *switch* ATM es usado como una tabla de información de reenvío que MPLS llama LFIB (*Label Forwarding Information Base*).

El VC de control MPLS usa encapsulación LLC/SNAP de paquetes IP como es definido en el RFC 1483 [12]. El PVC de control 0/32 es usado para llevar tráfico de protocolo de ruteo IP entre un LSC y otros LSRs ATM.

2.7.2 LSP (*Label-Switched Path*)

El LDP es una conexión configurada entre dos LSRs en los cuales las técnicas de conmutación de etiquetas son usadas para reenviar etiquetas.

Un LDP es un camino específico por el cual pasa tráfico en una red MPLS. LSPs son aprovisionados usando un protocolo 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 ruteo tales como *MultiProtocolo* 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 ruteo y las rutas aprendidas de estos protocolos. LSRs pueden usar otros protocolos tal como RSVP, pero ya no son requeridos.

2.7.2.1 Establecimiento de un LSP

El establecimiento del LSP puede ser realizado de una o dos maneras:

- Control Independiente: Proporciona una rápida convergencia y establecimiento de LSPs, porque el LSR puede establecer y publicar la unión de etiquetas al mismo tiempo, sin el retraso de esperar un mensaje para recién propagar. Al establecimiento del LSP inmediatamente le sigue la convergencia del protocolo de ruteo.
- Control Ordenado: En este método, la unión de etiquetas son propagados a lo largo de la red antes de que el LSP sea establecido. Sin embargo, este método proporciona una mejor posibilidad de prevención de *loops* (Lazos).

2.7.3 LDP (Protocolo de Distribución de etiquetas)

El 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. LDP permite a un LSR distribuir etiquetas a su *peer* LDP usando el puerto TCP 646, mientras que 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.

TDP de Cisco y el Standard TDP 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 *peers* acerca de esta etiqueta y de su significado. LDP es usado para este propósito. *Un grupo de etiquetas del LSR de ingreso al LSR de egreso en un dominio MPLS definen un LSP*. Las etiquetas son usadas como mapas del *routing* 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 *peers* LSRs.

LDP proporciona a un LSR mecanismos de descubrimiento para permitir a los *peers* LSR ubicar uno al otro y establecer comunicación. LDP define cuatro clases de mensajes:

- DISCOVERY, corre sobre protocolo UDP y usa mensajes *multicast* HELLO para aprender sobre otros LSRs en los cuales LDP tiene una conexión directa. Entonces se establece una conexión TCP, una eventual sesión LDP con su peer. Las sesiones LDP son unidireccionales.

- ADJACENCY, corre sobre protocolo TCP y proporciona inicialización de sesión usando el mensaje de INITIALIZATION al inicio de la negociación de la sesión LDP. Esta información incluye el modo de asignación de etiquetas, valores de temporizador de sesión (*keepalive timer*) y el rango de etiquetas a ser usado entre los dos LSRs. Los *keepalives* para LDP son enviados periódicamente usando mensajes KEEPALIVE. La sesión LDP es terminada entre los *peers* LSRs si los mensajes KEEPALIVE no son recibidos en el intervalo de tiempo establecido.
- LABEL ADVERTISEMENT, proporciona publicación de unión de etiquetas usando mensajes LABEL MAPPING que publica la unión entre FECs y etiquetas. LABEL WITHDRAWAL son usados para revertir el proceso. Mensajes LABEL RELEASE son usados por LSRs que han recibido información de mapeo de etiqueta y quieren liberar la etiqueta porque ellos no tienen tanta necesidad de esta.
- NOTIFICATION, proporciona información de consulta y también información de error de señal entre *peers* LSRs que tienen una sesión LDP establecida entre ellos.

LDP corre sobre protocolo TCP, excepto el mensaje DISCOVERY que corre sobre UDP, para brindar intercambio de mensajes confiablemente.

La arquitectura MPLS permite a un LSR requerir explícitamente, de su siguiente salto para un particular FEC, una etiqueta y a que FEC esta asociada. Esto es conocido como distribución de etiquetas sobre demanda (*downstream on demand*). La arquitectura MPLS también permite a un LSR la distribución de etiquetas a LSRs

que no han solicitado explícitamente (*unsolicited downstream*). Estas técnicas de de distribución de etiquetas puede ser usada en la misma red y al mismo tiempo.

2.7.4 Routing *loops* en MPLS

Los *loops* ocurren cuando los LSRs disponen de una información acerca de la red y en lugar de enviar el tráfico a su destino, se pasan los paquetes entre ellos creyendo que el otro LSR conoce como alcanzar el destino. Como se indicó anteriormente, LSPs son construidos usando LDP, TDP o una extensión de protocolo de *routing* como BGP, PIM, o RSVP. LDP usa la información que proporciona la capa 3 y es susceptible a *routings loops* a menos que el protocolo de la capa 3 tenga mecanismo para evitar estos *loops*.

En protocolos de ruteo del tipo "Vector Distancia" como es el caso de RIP, los *routers* no tienen una vista topológica de toda la red. La métrica usada es el contador de saltos que podría llegar a infinito, para esto se define un número máximo.

En los protocolos de ruteo "l*ink-state*" tales como BGP, cada *router* tiene una visión entera de la topología de la red. En este tipo de redes, hay posibilidades de que se presenten *loops* si las bases de datos topológicas de los *routers* no están sincronizadas, esto puede pasar inmediatamente después de la falla de un enlace, por ejemplo:

Hay tres formas de controlar *loops* en MPLS:

- Supervivencia del *loop*. Minimiza el impacto de los *loops*. Permite que la red opere bien a pesar de la presencia de transitorios *loops* que se presentan por el protocolo de ruteo de capa 3.

- Detección del *loop*. Con este método *loops* también serán formados, sin embargo se eliminará la etiqueta asignada a este paquete
- Prevención del *loop*. Este es el control más eficaz, el de prevenir *loops* en la red. Este método se asegura de que no se formen ningún *loop* en la red. Las etiquetas no serán asignadas a ningún paquete hasta que se tenga la certeza de que *loops* no serán formados. La información del contador de saltos es incluida en los mensajes LDP o TDP de solicitud y respuesta.

CAPÍTULO III

MPLS: INGENIERÍA DE TRÁFICO

3.1 MPLS-TE: INTRODUCCIÓN

Debido al crecimiento geométrico de Internet y el requerimiento de mayor ancho de banda, calidad de servicio y confiabilidad de sus usuarios finales, los proveedores de Internet más importantes se ven en la necesidad de implementar tres iniciativas complementarias a la red de Internet existente: Una arquitectura de red escalable, Una red con capacidad de expansión, una red que soporte ingeniería de tráfico (TE). Hoy en día hay la necesidad de desarrollar diferenciación de servicios IP para que IPSs puedan proporcionar clases de servicios a diferentes tarifas. Para poder proporcionar tales posibilidades en la red, el reenvío de paquetes de la arquitectura de Internet convencional, debe de ser mejorado para soportar ingeniería de tráfico. Ingeniería de tráfico abarca muchos aspectos en el desempeño de la red. Esto incluye la implementación de alta calidad de servicio y mejoramiento de utilización de los recursos de red para la distribución eficiente de tráfico aún cuando un enlace o nodo falle o no este disponible.

En el *routing* de la capa 3, los paquetes son reenviados de un salto a otro. En cada salto la dirección destino del paquete es usada para hacer una tabla de *routing*. Estas

tablas son creadas por un protocolo de *routing* llamado IGP (*Interior Gateway Protocol*), el cual encuentra la ruta de menor costo de acuerdo a la métrica en cada destino en la red. En muchas redes este método trabaja bien pero en algunas redes este tipo de reenvió resulta en la sobre utilización de algunos enlace y en la baja utilización de otros. Este no balance de carga se dará cuando haya muchas posibles rutas a un destino y el IGP selecciona uno de ellos como la mejor ruta y usa solo esta ruta. En el caso extremo, la mejor ruta cargará un gran volumen de tráfico de paquetes y posiblemente descarte algunos mientras las otras "no mejores rutas" están disponibles.

Una solución a este problema sería ajustar el ancho de banda de los enlaces a un valor más apropiado. Reducir el ancho de banda de los enlaces no muy utilizados y ampliar el enlace que esta sobre utilizado. Sin embargo, este ajuste no siempre es posible porque el camino alternativo resulta ser la ruta *backup* y en caso falle el enlace principal será necesario disponer de un enlace *backup* capaz de soportar el tráfico que soporta el principal. Es decir el incremento de ancho de banda del enlace principal implicaría un costo adicional que de hecho incrementa el presupuesto de operación de la red.

Para mejorar el rendimiento de la red sin afectar el presupuesto, el administrador de red puede mover parte del tráfico del enlace principal sobre utilizado al enlace *backup* de baja utilización. En una operación normal de la red, este cambio daría como resultado menor cantidad de paquetes eliminados y mayor ancho de banda disponible para cursar tráfico. En el caso que uno de los enlaces falle entonces el otro enlace llegará a estar sobre utilizado.

Mover porciones de tráfico no puede ser realizado utilizando tradicionales protocolos de *routing* IGP. El *routing* del tráfico en la capa 3 resulta de un mapeo ineficiente de la disponibilidad de los recursos en la red.

Un buen mapeo del tráfico sobre los recursos de la red crea un mejor uso del dinero invertido.

Los costos ahorrados en un uso eficiente de los recursos de ancho de banda ayudan a reducir sobretodo el costo de operación de la red. Este ahorro permite al proveedor de servicios tener una ventaja sobre sus competidores. Esta ventaja es más importante cuando se obtienen más clientes y más competitividad.

Un eficiente uso de recursos de ancho de banda significa que el proveedor podría evitar una situación donde algunas partes de la red estén congestionadas, mientras otras partes no.

Ingeniería de tráfico no soluciona congestión temporal de la red debido a ráfagas de tráfico. Este tipo de problemas es manipulado de una mejor manera por técnicas como algoritmos de encolamiento, limitación de tráfico (*rate limit*) y descarte de paquetes de manera inteligente.

TE es usado cuando el problema es el mapeo del tráfico en los recursos de la red. En tales redes, una parte de la red sufre congestión por largos periodos de tiempo mientras que otras partes de la red tienen recursos disponibles.

Se debe de tener presente que utilizar TE implica en reducción de costos.

3.2 ¿QUE ES INGENIERÍA DE TRÁFICO?

El término TE es ampliamente utilizado en el mundo de la voz telefónica. TE significa que el tráfico es medido y analizado. Luego un modelo estadístico es

aplicado al patrón de tráfico para hacer pronósticos y estimaciones. Si el patrón de tráfico no está de acuerdo con los recursos de la red, el administrador de red remodelará el patrón de tráfico. Tal decisión puede ser usada para lograr una optima utilización de recursos o reducir costos al seleccionar un económico *carrier* de transito.

En las redes de datos del orbe, TE proporciona un enfoque integrado a la ingeniería de tráfico de la capa 3 del modelo OSI. El enfoque integrado significa que los *routers* son configurados para desviar tráfico de congestionadas partes de la red a no-congestionadas partes. Tradicionalmente esto se hacia usando las redes convencionales donde *routers* usan los PVCs ATM o Frame Relay para distribuir la carga de tráfico a nivel de capa 2.

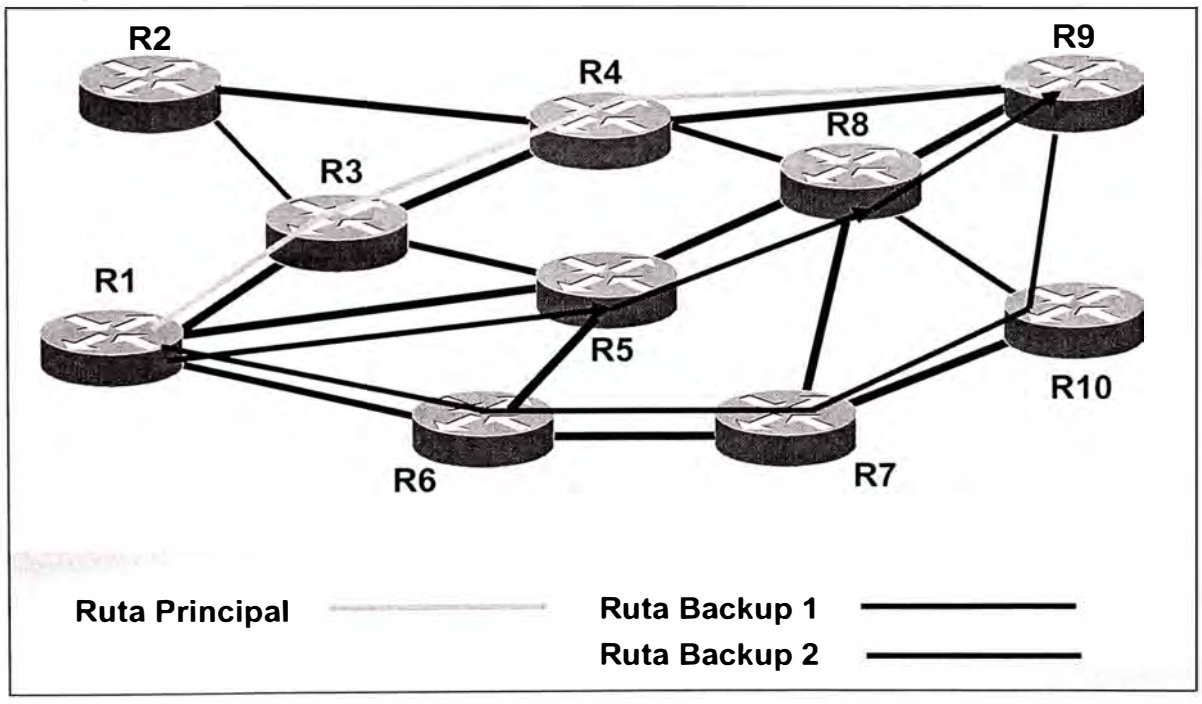


Figura 3.1 Establecimiento de una ruta principal y una de backup

En la figura se muestra que el proveedor de servicio define, basado en métricas del protocolo IGP, como mejor ruta R1-R3-R4-R9. Todo el tráfico que va de R1 a R9 va

por este camino. Sin embargo, se observa que las rutas backups R1-R5-R8-R9 y R1-R6-R7-R10-R9 no se están aprovechando. Es decir solamente si falla el enlace principal se utilizará el enlace backup 1 o de lo contrario el enlace backup 2.

Con el desarrollo de Ingeniería de Tráfico, el flujo de tráfico a través del *backbone* del proveedor de servicios puede ser optimizado. Las rutas R1-R5-R8-R9 y R1-R6-R7-R10-R9 pueden ser utilizadas para balancear el tráfico que va de R1 a R9.

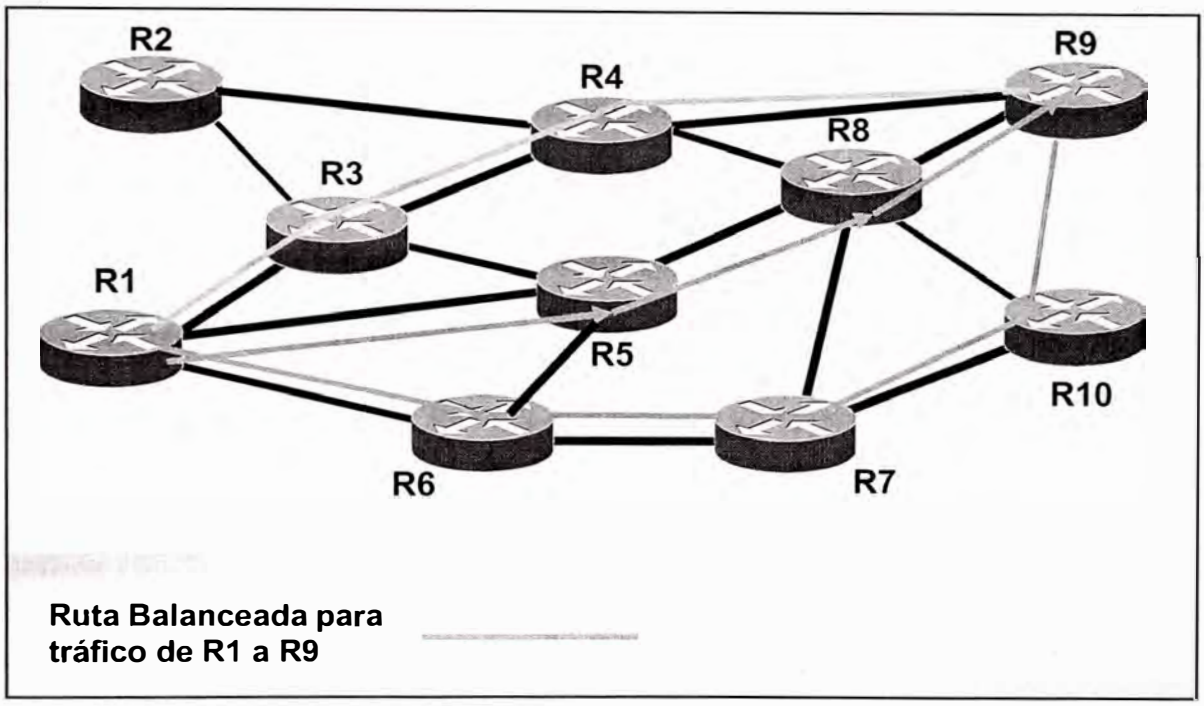


Figura 3.2 Establecimiento de rutas para balanceo de tráfico de R1 a R9

La figura muestra como se puede optimizar el flujo de tráfico de R1 a R9.

Dentro de los protocolos IGP se puede decir que EIGRP (*Enhanced Interior Gateway Routing Protocol*) no es un protocolo IGP que soporte TE. Hay solo dos protocolos l*ink-state* soportados por MPLS-TE y son IS-IS-IS y OSPF.

3.3 MANIPULACIÓN DE MÉTRICA VERSUS INGENIERÍA DE TRÁFICO.

En las redes IP convencionales se puede observar el pobre comportamiento del re-direccionamiento de tráfico. Este cambio es posible variando la métrica en el protocolo de *routing* IGP que puede ser OSPF. Este método no proporciona redundancia dinámica y no considera las características de tráfico que cursa cuando se toma la decisión de *routing*.

En MPLS-TE, los LSPs pueden cambiar dinámicamente de una ruta congestionada a una ruta alternativa. Esto significa una gran mejora respecto a redes IP convencionales, debido a que el administrador de la red puede disponer el uso de la más alta capacidad de recursos en condiciones normales y tener la tranquilidad que antes de una congestión, alguno de los tráficos pueden ser conmutados fácilmente a otro punto no congestionado. Es más, los administradores de red pueden hacer uso de algoritmos de optimización global que proporciona una relación de la demanda de tráfico con los enlaces físicos, lo cual no se lograría utilizando una optimización local. Como resultado el proveedor de servicios puede lograr un mayor grado de utilización de los enlaces en la red y esto reduciría los costos de los servicios proporcionados.

MPS-TE permite a los ISPs definir rutas explicitas a través de la red y llevar el tráfico por estas rutas. También, rutas explicitas de redundancia pueden ser configuradas.

3.4 VENTAJAS DE MPLS-TE

Las ventajas de la ingeniería de tráfico sobre MPLS son las siguientes:

- Con MPLS, las posibilidades de ingeniería de tráfico logran ser integradas a nivel de la capa 3, el cual optimiza el *routing* del tráfico IP dando restricciones impuestas por la topología y la capacidad del *backbone*.
- Permite al administrador de la red crear rutas explicitas especificando un camino físico exacto de un LSP.
- MPLS-TE brinda niveles de disponibilidad de red ante falla de nodos o enlaces los cuales cambian la topología de la red adaptando una nueva serié de restricciones aún si la ruta principal está ya predeterminada.
- Habilita carga compartida sobre rutas con diferentes costos y permite el uso de rutas que no son aprendidas por el IGP.
- Permite establecer estadísticas del uso del LSP. Esta información se puede utilizar para evaluar planes futuros de expansión en una red.
- Permite configurar *routing* restringido conocido como "*constraint-based routing*" (CBR). Esto permite al administrador de red seleccionar determinadas rutas para servicios especiales brindando diferentes niveles de calidad de servicio. Estos niveles de servicio pueden ser evaluados de acuerdo a las garantías brindadas en retardo, *jitter* (variación de retardo), perdida de paquetes, ancho de banda, etc.
- MPLS-TE elimina la necesidad de configurar manualmente los dispositivos de red configurando rutas. explicitas. La funcionalidad de MPLS-TE es muy confiable y permite comprender la topología del *backbone* y los procesos de señalización automatizados.

La principal ventaja de la ingeniería de tráfico sobre MPLS es que se puede aplicar sobre una Red IP, sin importar la plataforma sobre la que está, que puede ser ATM o

Frame Relay, de manera flexible, bajo costo de planificación y gestión y con una mayor calidad de servicio.

3.5 ELEMENTOS DE MPLS-TE

MPLS permite a los elementos de Ingeniería de Tráfico estar completamente bajo el control de IP. Esto permite ofrecer servicios IP que son brindados en redes convencionales en la capa 3 y capa 2. Esto proporciona una manera de lograr los mismos beneficios de ingeniería de tráfico del modelo convencional sin necesidad de configurar una red *full-mesh* (todos con todos) y sin la necesidad de implementar una nueva red.

MPLS-TE usa RSVP (*Resource Reservation Protocol*) para establecer y mantener automáticamente un túnel a través de la red. La ruta usada por un túnel, dado en algún punto en el tiempo, es determinada basándose en los requerimientos de recursos de túnel y de red, como ancho de banda. La información sobre la disponibilidad de los túneles es publicada por el protocolo de *routing* IGP (IS-IS u OSPF).

Los túneles son calculados en la cabecera del túnel (del *router* fuente), basado en una condición requerida entre el recurso solicitado y el recurso disponible CBR (*constraint-based routing*). Entonces el protocolo IGP re-envía el tráfico automáticamente en estos túneles. Por lo general, en un *backbone* con MPLS-TE, un paquete viaja en un simple túnel que conecta el punto de ingreso y de egreso.

A continuación se explicará los diversos elementos utilizados en MPLS-TE.

3.5.1 Túnel LSP

Este túnel proporciona un mecanismo de movilización de paquetes a través de la red MPLS, los cuales son creados usando un protocolo de señalización de servicios integrados tal como RSVP. Estos túneles son equivalentes a los VCs en ATM donde hay una ruta explícitamente configurada y un mecanismo de calidad de servicio asignada. El mensaje PATH RSVP lleva la ruta explicita a seguir usando una asignación provisional de recursos a lo largo del camino. El mensaje RESERVATION enviado en respuesta establece la operación de etiquetas y pasa de una asignación provisional a una reservación permanente. Cuando se usa RSVP, la calidad de servicio que ofrece Servicios Integrados (*IntServ*) está disponible. Los túneles LSP trabajan de forma unidireccional, es decir las rutas de reenvío y retorno para un flujo IP son independientes. Así, este comportamiento unidireccional se hace muy útil para TE en tráfico IP.

La cabecera MPLS contiene un campo EXP (*experimental bits*) de tres bits que son usados para diferenciación de servicios (*DiffServ* o DSCP). Esto significa que se tiene 8 (2^3) diferentes calidades de servicio disponibles sobre un túnel LSP.

3.5.2 Distribución de información de *routing* basado con restricciones (CBR)

La información de *routing* conocida como CBR (*Cronstaint-Based Routing*) debe de ser optimizada para encontrar rutas apropiadas a través de la red. Para este fin la información de restricciones debe ser distribuida por toda la red MPLS de manera que se cree una tabla de restricciones y reenvío integrada. Esta tabla es construida con la ayuda del protocolo IGP de *routing link-state* tales como: OSPF o IS-IS. Los

protocolos vector distancia no son útiles debido a que no brindan información suficiente para calcular rutas alternativas usadas por la ingeniería de tráfico.

Los protocolos IGP IS-IS y OSPF han sido extendidos para soportar MPLS-TE y llevar información de restricción de enlaces sin la necesidad de un protocolo de la capa 2 tal como PNNI (*Private Network Node Interface*) usado en ATM. En el Modelo convencional, un enlace físico incluye varios PVCs, la falla de este enlace significaría la falla de múltiples enlaces IP. En MPLS, la falla de un enlace físico significa la falla de un simple enlace, reduciendo así la perdida de flujo de tráfico y el tiempo de convergencia.

3.5.3 Asignación de tráfico a un túnel

El LSP es calculado por el *routing* basado en restricciones, CBR, el cual toma en consideración los requerimientos de recursos. Cuando un LSP es establecido, entonces el tráfico puede pasar a través de él. Desde la perspectiva IP un LSP es considerado un túnel.

Estos túneles creados solo pueden ser usados por el *routing* IP si los túneles son explícitamente especificados por el enrutamiento:

- Vía rutas estáticas que apuntan al túnel
- Por políticas de *routing* que asigna el siguiente salto a un túnel.

En la figura 3.3 se muestra la topología con dos túneles LSPs. Las direcciones *loopback* de cada *router* son i.i.i.i (donde i es el número del *router*) La métrica de cada *router* es asignada a 1. R1 tiene dos interfaces físicas I1 y I2 y dos *routers* vecinos (*neighbors*) con direcciones D1 y D2.

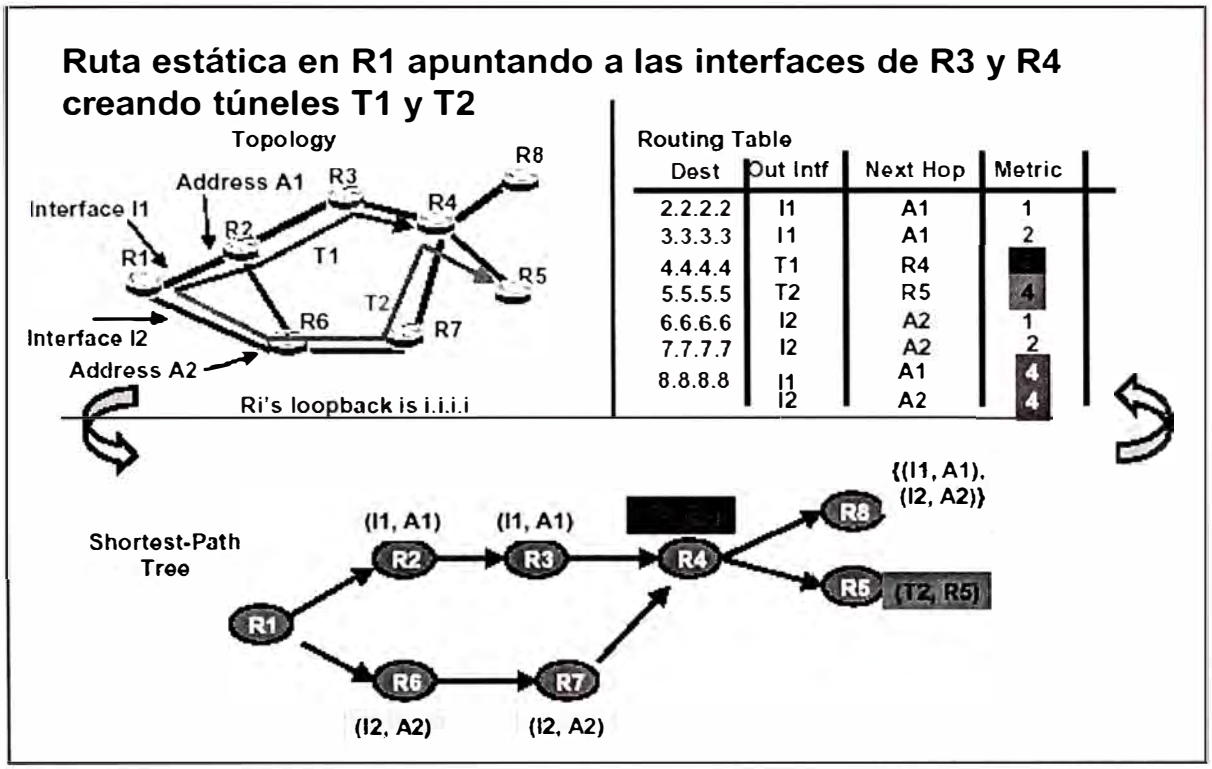


Figura 3.3. Creación de dos túneles: T1 (de R1 a R4) y T2 de (R1 a R5)

La tabla de *routing* del R1 muestra las rutas y la información asociada para llegar a cada *router* destino. Como se puede observar solo para llegar al *router* R4 y R5 hace uso del Túnel T1 y T2, respectivamente, los cuales son asociados como interfaces de salida del *router* R1. Para llegar a los demás destinos el protocolo IGP hace uso de métricas, que son calculadas por algoritmos en los que intervienen parámetros como la interface de salida y el número de saltos. Si el destino a alcanzar es por ejemplo R8, entonces necesariamente se hace uso del algoritmo de *routing* del protocolo IGP a menos que se defina una ruta estática a través de un túnel a este destino.

El algoritmo de *routing* SPF (*Shortest Path First*) calcula la mejor ruta a un destino con la excepción de rutas que involucren túneles, en este caso se hace uso de cálculo basado en CBR.

El flujo de tráfico también puede ser asignado a LSPs basados en *next-hop* BGP o usando parámetros de clases de servicio.

Rerouting

Redes con ingeniería de tráfico aplicada deben poder responder a cambios en la topología de la red y mantenerla estable. La falla de cualquier enlace o nodo no debe de alterar los servicios de red de alta prioridad, especialmente la clase de servicio más alta.

- *Fast Rerouting* (rápido re-direccionamiento),

  Es un mecanismo que minimiza la interrupción de servicio del flujo de tráfico. Re-*routing* re-optimiza el flujo de tráfico afectado por un cambio en la topología de la red.

  Para solucionar los problemas de configurar rutas estáticas en túneles MPLS-TE introduce el concepto de *re-route*. El túnel MPLS-TE es usado solamente por un IGP normal para calcular rutas, y no está incluido en el cálculo basado en CBR.

  El *fast re-routing* permite un *routing* temporal para re-optimizar el LSP cuando ocurre una falla en la red. Esto causa que el LSP sea re-enrutado a un túnel pre-configurado y así sortear el enlace fallado. La opción de *fast re-routing* es soportada activando los atributos de sesión que permiten protección del enlace.

  La figura 3.4 muestra el enlace de protección entre R2 y R4 y toma la ruta R2-R6-R7-R4 y usa todos lo mecanismos de MPLS-TE (asignación de etiquetas, reservación de recursos). Este túnel (*link protection* LSP) sirve como una ruta *backup* temporal en el caso que falle el enlace de R2 a R4.

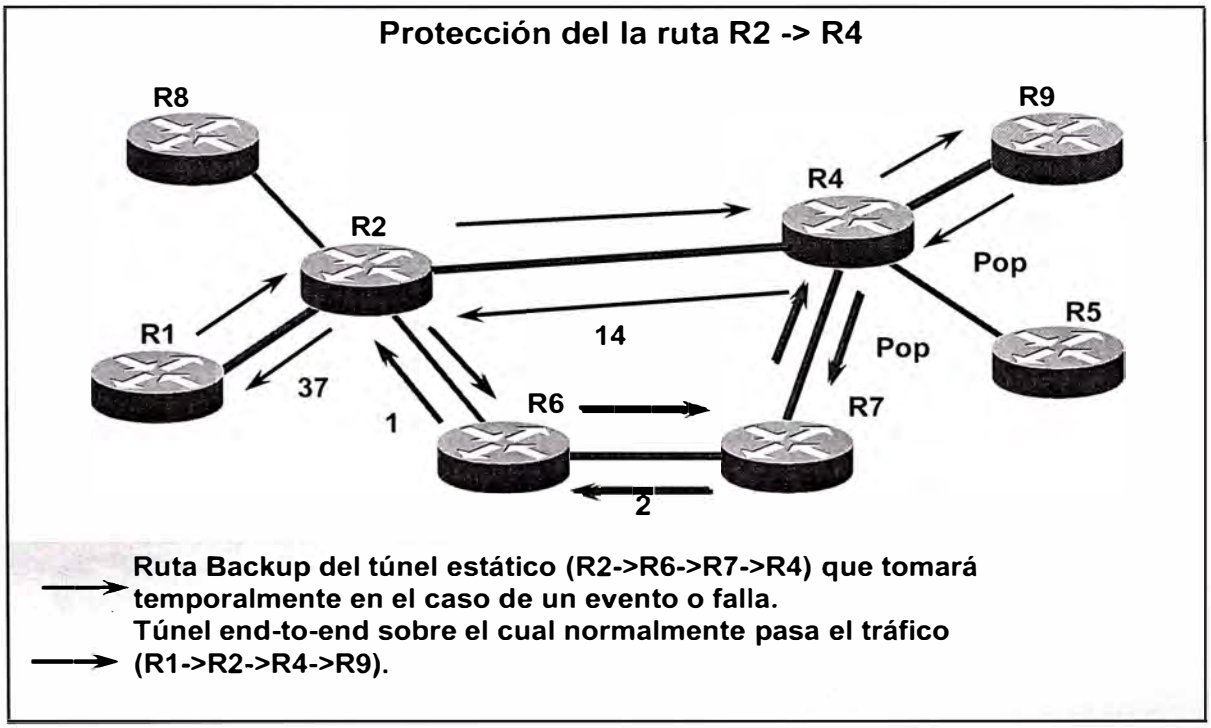


Figura 3.4. Ruta backup de protección a la ruta del R2-> R4

Cuando falla el enlace, R2-R4, el mensaje RSVP *PathErr* y los mecanismos del protocolo IGP son usados para notificar la falla a los extremos. El mensaje RSVP *PathErr* indica que hay un LSP *backup* a ser tomado en cuenta. El *re-routing* al túnel pre-configurado es casi instantáneo. Esto puede tomar algo menos de 50 milisegundos y este retardo es causado por el tiempo que toma detectar la falla del enlace y conmutar el tráfico al LSP *backup*.

Durante la fase del *re-routing,* las etiquetas del LSP deben ser también manipuladas. El *router* R2, a la cabeza del LSP, cambia la etiqueta original de salida por la etiqueta del LSP pre-establecido y une la original etiqueta a la pila de etiquetas.

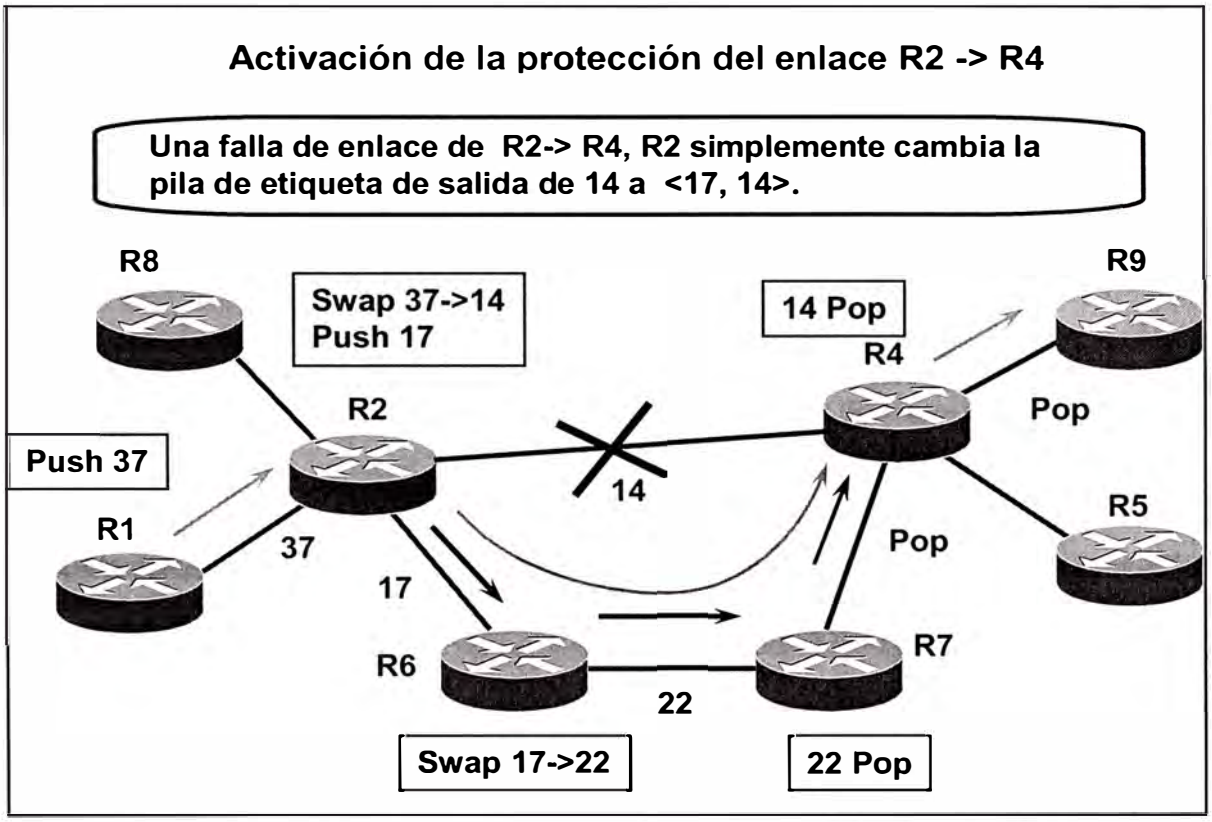


Figura 3.5. Se muestra la activación y el cambio de etiquetas del enlace backup.

En la figura 3.5 las etiquetas asignadas al LSP (del R1->R9) son: 37-14-POP (*Null* implícito). El único cambio ante una falla ocurre en R2 donde se cambia la etiqueta de 37 a 14. Sin embargo desde que el enlace con etiqueta 14 no está disponible, la ruta es movida al LSP de protección. La etiqueta original 14 es puesta en la pila de etiquetas del LSP de protección al cual le fue asignada la etiqueta de salida 17. Así, la ruta original LSP es efectivamente protegida ante una falla.

3.5.5 Ancho de Banda Garantizado TE (BG-TE)

GB-TE (*Guaranteed Bandwidth Traffic Engineering*) es una extensión de la actual funcionalidad de MPLS-TE. Introduce el concepto de una particular clase de tráfico, el cual es de ancho de banda garantizado. GB-TE permite al proveedor de servicio brindar una separada computación de ruta y control de admisión del ancho de banda

garantizado. GB-TE es otra característica de señalización del protocolo IGP y RSVP. Un tradicional MPLS-TE tiene un simple *pool* de ancho de banda en el enlace, cuando el ancho de banda es reservado a un túnel, en este caso el tráfico en el túnel es considerado como una clase simple. Por ejemplo, Cuando tráfico de voz y datos viajan por el mismo túnel, los mecanismos de calidad de servicio no pueden asegurar un mejor servicio para la voz. Normalmente, CB-WFQ (*Class Based Weighted-Fair Queuing*) puede ser aplicado en el túnel.

La idea de GB-TE es garantizar el ancho de banda para el túnel GB-TE en la red. En el caso de aplicaciones críticas como VoIP, un separado GB-TE túnel es creado. Así, dos *pool*s de ancho de banda son usados, uno para el tradicional túnel MPLS-TE y otro túnel GB-TE. Los mecanismos de Calidad de Servicio de Servicios Diferenciados (*DiffServ*) como LLQ (*Low Latency Queuing*) asegura que el ancho de banda para el túnel GB-TE sea dedicado a estos túneles. En la primera fase, el túnel GB-TE soporta una simple clase de ancho de banda garantizado. En siguientes fases se espera que GB-TE soporte múltiples clases de ancho de banda garantizado y una dinámica re-programación de mecanismos de encolamiento.

Túneles GB-TE son similares a túneles TE. Para soportar GB-TE, algunas modificaciones a los mecanismos de MPLS-TE fueron hechas:

- Hay dos tipos de ancho de banda por cada enlace en la red. Dos *pools* de ancho de banda, el pool global y el *sub-pool*.
- Ambos anchos de banda son anunciados en las actualizaciones del protocolo *link-state* que lleva la información de los recursos de la red.
- Los parámetros del túnel incluyen el tipo de ancho de banda que usara el túnel.

- El cálculo de la mejor ruta basado en Restricciones (CBR) es hecho de acuerdo a los requerimientos del tipo de ancho de banda del túnel. Los mensajes RSVP, siempre indican si el LSP es configurado como un túnel regular MPLS- TE o como un túnel GB-TE.
- Los nodos intermedios aplican el control de admisión y la asignación de ancho de banda en el apropiado *pool* de ancho de banda.

3.5.6 *Auto Bandwidth* (Ajuste automático de Ancho de Banda) TE

La asignación automática de ancho de banda proporciona un gran significado a la asignación de túneles basados en la carga de tráfico.

El Ajuste automático de ancho de banda (*Auto Bandwidth TE*) muestrea el promedio de la cantidad de tráfico para cada túnel que es marcado con ajuste automático de ancho de banda. En cada túnel marcado, se ajusta periódicamente (por ejemplo, un día) una asignación de ancho de banda del túnel del valor de la muestra mayor para el túnel desde el último ajuste.

La frecuencia con la que el ancho de banda del túnel es ajustado es configurable. Además, el intervalo de muestreo y el intervalo sobre el cual se promedia el tráfico del túnel para obtener la cantidad de tráfico promedio de salida, es configurable por el usuario en base a los túneles creados.

El beneficio de esta característica es la fácil configuración y monitoreo del ancho de banda para los túneles MPLS-TE. Si ancho de banda automático es configurado a un túnel, entonces automáticamente TE ajusta el ancho de banda del túnel.

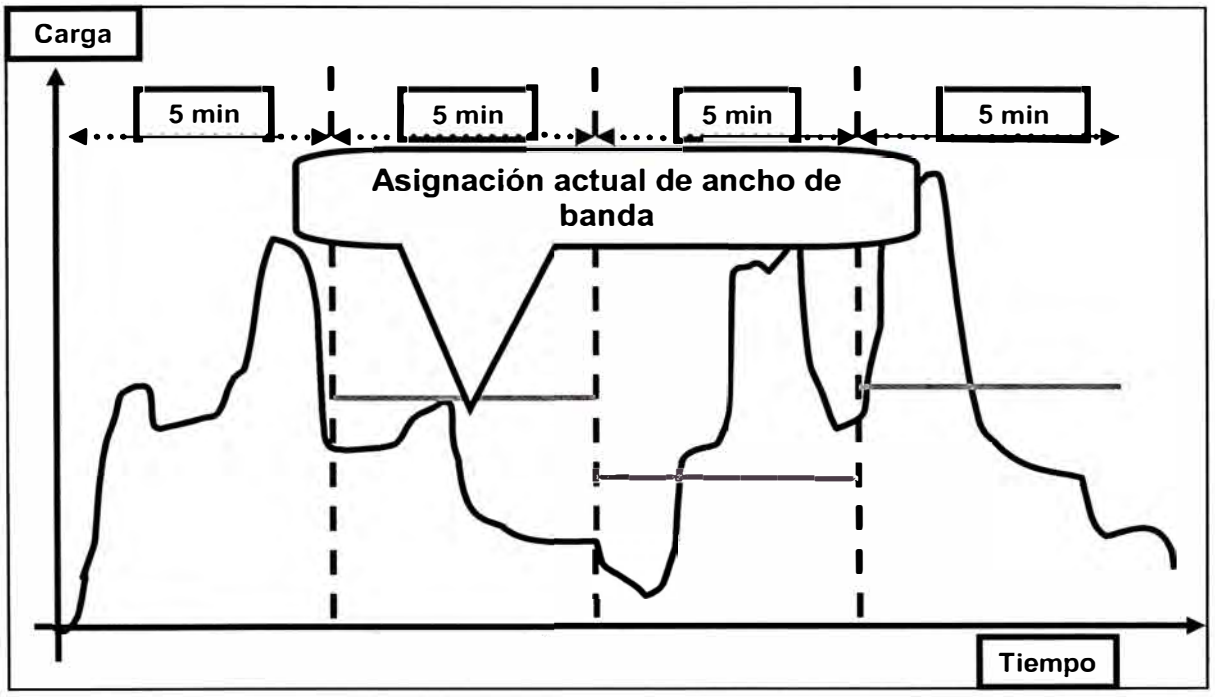


Figura 3.6: Ejemplo de Ajuste de Ancho de banda automático.

La característica de ajuste de ancho de banda automático trata independientemente cada túnel que ha sido habilitado. Así, el ajuste de ancho de banda para cada túnel es de acuerdo a la frecuencia de ajuste configurada en el túnel y la cantidad de tráfico de salida muestreada al túnel desde el último ajuste, sin considerar ajustes previamente hechos o pendientes en otros túneles.

En la figura 3.6 se muestra la carga en el túnel y los intervalos de medición. El tráfico de entrada y salida en la interface del túnel son promediados sobre un intervalo predefinido (*load-interval*). En el ejemplo, el intervalo es 5 minutos.

Los ajustes automáticos de ancho de banda se hacen periódicamente, por ejemplo, una vez al día. Cuando el ajuste de ancho de banda es hecho, la actual asignación de ancho de banda (línea horizontal en la figura) es reiniciada al valor máximo.

CAPÍTULO IV

MPLS: CLASE DE SERVICIO (QoS)

4.1 MPLS-QoS: INTRODUCCIÓN

El crecimiento exponencial de Internet hace que las comunicaciones en el mundo cambien día a día. Esto se manifiesta en la forma de estudiar, de trabajar y de entretenerte. Las formas de acceso universal hacia Internet hacen de esta una herramienta de uso masivo. La utilización de Internet va desde enviar un simple correo electrónico hasta hacer el uso de aplicaciones en tiempo real con calidad de servicio garantizado.

Servicios como llamadas VoIP, video en tiempo real, televisión sobre Internet, educación a distancia, transacciones seguras de dinero y otros, necesitan tener una alta calidad de servicio. Para esto, es necesario obtener valores apropiados de retardo, *jitter* (variación de retardo), ancho de banda, perdida de paquetes y disponibilidad. Estos parámetros forman la base de la calidad de servicio. Una red IP debe estar diseñada para poder soportar calidad de servicio requerida por las aplicaciones que cursan sobre esta red.

Muchos proveedores de servicios ofrecen calidad de servicio a través de acuerdos a nivel de servicios (SLAs: *Service Level Agreements*) para garantizar el tráfico de datos de sus clientes o de sus aplicaciones.

La calidad de servicio en redes IP brinda a los dispositivos, *routers* o *switches*, la inteligencia necesaria para manipular los paquetes de tal manera de dar preferencia al tráfico que se desea priorizar que está contemplado en el SLA.

La calidad de servicio (QoS) es definida como los mecanismos que permiten controlar la mezcla de anchos de banda, del retardo, de la variación del retardo y de la perdida de paquetes en la red. Es decir, QoS no es una característica de un dispositivo sino es una arquitectura de extremo a extremo. La calidad de servicio IP permite priorizar clases de servicios, asignar ancho de banda y evitar congestión de tráfico.

Aquellos proveedores de servicios que brindan servicios IP sobre una red MPLS deben soportar calida de servicio IP sobre su infraestructura MPLS. Esto significa soportar calidad de servicio sobre MPLS-VPNs o sobre rutas MPLS-TE. El IETF (*Internet Engineering Task Force*) ha definido dos modelos para la implementación de calidad de servicio: Servicios Integrados (*IntServ*) y Servicios Diferenciados (*DiffServ*). En *IntServ*, el usuario final indica a la red la reservación de los recursos de ancho de banda que usará. *DiffServ* trabaja sobre una aprovisionada calidad de servicio, en la cual los elementos de red están configurados a múltiples clases de servicios de tráfico con diferentes requerimientos, es decir la red reconoce que clases requieren un trato especial.

4.2 ARQUITECTURA DE CALIDAD DE SERVICIO SEGÚN CISCO

La arquitectura de calidad de servicio está implementada por varios mecanismos. Estos mecanismos son usados por la arquitectura de servicios integrados y servicios diferenciados para poder brindar soluciones de acuerdo a los recursos disponibles y los requerimientos solicitados.

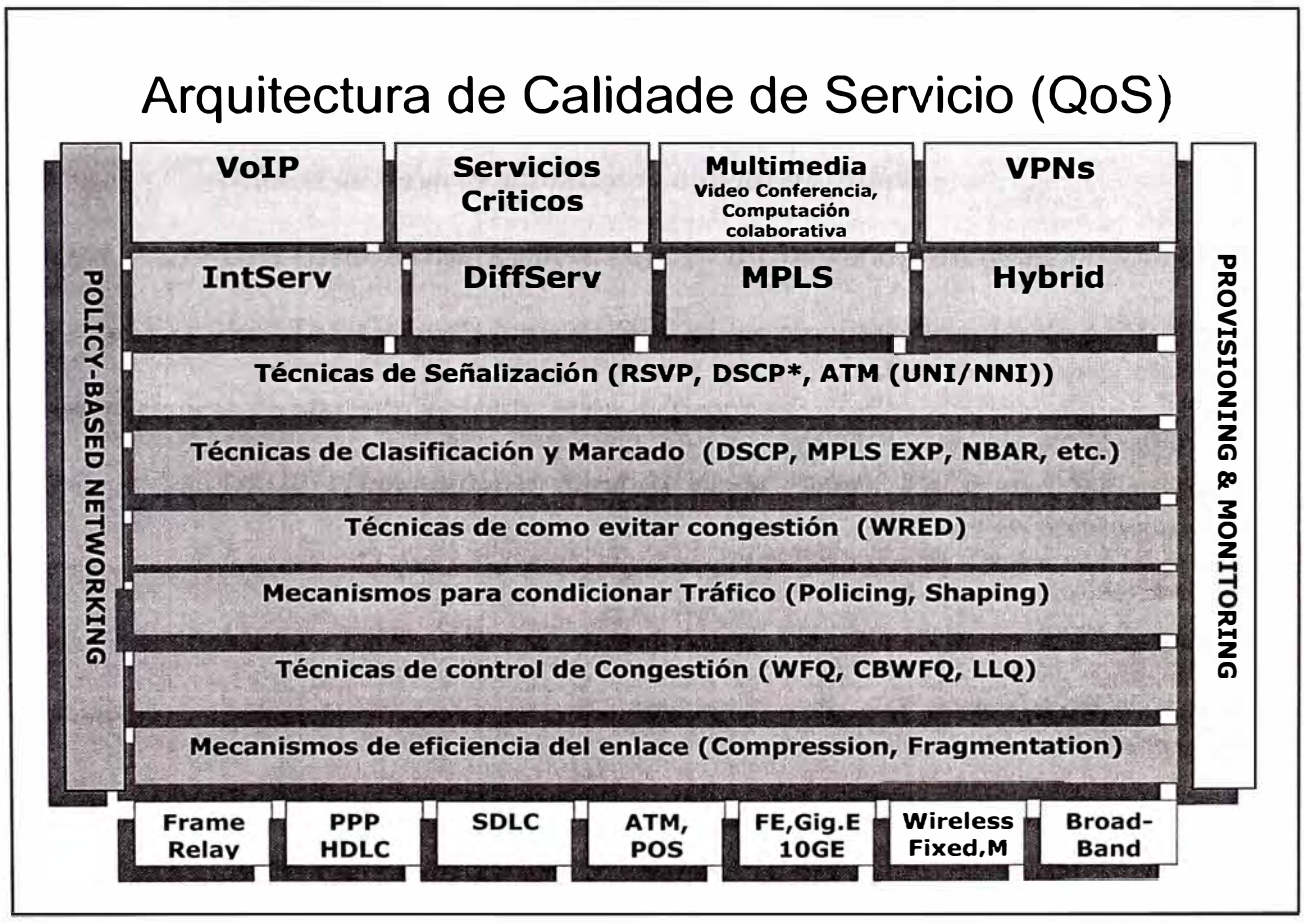


Figura 4.1: Arquitectura de QoS según CISCO.

CISCO ha desarrollado técnicas que permiten a los proveedores manejar mejor la confiabilidad de sus enlaces, el ancho de banda, el retardo y la variación del retardo. También ha implementado equipos de última generación como son los *router* 7500 y

12000 usados principalmente en el *backbone* de la red, con módulos o tarjetas que soporten las técnicas de calidad de servicio desarrolladas.

En la figura 4.1 se muestra las técnicas usadas en la arquitectura de QoS establecida por CISCO.

A continuación se dará una breve descripción de cada una de estás

- Técnicas de señalización
  - RSVP (*Resource Reservation Protocol*). *Definido en RFC 2205 [6], es un protocolo que reserva recursos en la red para proporcionar calidad de servicio garantizado a flujos de tráfico*
  - UNI (*User Network Interface*) / NNI (*Network-to-Network Interface*) de ATM. *Controladores de flujo en los circuitos virtuales de ATM.*
- Técnicas de marcado y clasificación de paquetes
  - DSCP (*Differentiated Services Code Point*). *Valor que indica la preferencia que tendrá el paquete que viaja a través de una red IP.*
  - MPLS EXP. *Campo experimental de la etiquete MPLS que generalmente copia el valor DSCP en este campo EXP de MPLS.*
- Técnicas de cómo evitar congestión
  - WRED (*Weighted Random Early Detection*). *Algoritmo que permite manejar la cola de la interface (como número de paquetes en cola), de tal manera que la cola no este llena continuamente.*
- Mecanismos para condicionar tráfico
  - CAR (*Commited Access Rate*). *Limitador de capacidad de ancho de banda del flujo de tráfico. El exceso de tráfico es descartado automáticamente.*

- GTS (*Generic Traffic Shaping*). *Limitador de capacidad de ancho de banda del flujo de tráfico. Cierto tráfico de exceso es almacenado en la cola de espera hasta que haya disponibilidad de ancho de banda. El tráfico que excede aún el valor máximo en cola de espera es descartado automáticamente.*
- FRTS (*Frame Relay Traffic Shaping*). *Similar a GTS pero FRTS solo es aplicable a redes Frame Relay.*

- Mecanismos de control de congestión
  - FIFO *Queuing* ((FIFO: *First Input First Ouput*)). *La mas básica técnica de encolamiento. Los paquetes son enviados fuera de la interface en el orden que llegaron al buffer.*
  - PQ (*Priority Queuing*). *Crea 4 colas de prioridad. Los paquetes que se encuentran en el buffer de la interface de salida son separados en estas 4 colas de prioridad. Los paquetes de la alta prioridad siempre tendrán preferencia sobre los otros. Es decir, es necesario que no haya paquetes de alta prioridad para que paquetes de prioridad media sean enviados.*
  - CQ (*Custom Queuing*). *Adicional a la creación de colas de PQ, CQ asigna ancho de banda y cantidad de paquetes a cada una de las 4 colas que son definidas. La configuración es manual.*
  - WFQ (*Weighted Fair Queuing*). *Es la técnica de encolamiento default en los routers CISCO. Es similar a CQ con la diferencia que esta técnica no requiere configuración de asignación de ancho de banda*

a cada cola. La asignación actual de ancho de banda depende del número de flujos, los cuales pueden cambiar constantemente.

- CB-WFQ (*Class-Based Weighted Fair Queuing*). *Utiliza lo mejor de CQ y WFQ. Es decir asigna ancho de banda a cada cola creada, cada cola es una clase, tal como CQ.*
- LLQ (*Low Latency Queuing*). *Adicionalmente a CB-WFQ, se asigna una prioridad a cada clase creada. LLQ también es conocida como PQ-CB-WFQ.*

- Mecanismos de eficiencia del enlace
  - CRTP (*Compresión Real-Time Protocol*). *Este protocolo permite la compresión de la cabeceras: IP (20 bytes), UDP (8 bytes), RTP (12 bytes) y mantiene el payload sin compresión. Finalmente el paquete CRTP queda con una cabecera CRTP (2- 4 bytes) y el payload.*
  - LFI (*Link Fragmentation Interleaving*). Opción de fragmentación de paquetes que puede ser usado dependiendo del tipo de enlace WAN:
    - Frame Relay FRF.12. *Fragmenta el tamaño del frame Frame Relay. Con esto se logra obtener calidad de servicio para servicios como VoFR (Voz over Frame Relay).*
    - ML-PPP (*MultiLink Point-to-Point Protocol*). *Definido en RFC1990 [13], ML-PPP permite fragmentación de paquetes los cuales son reensamblados en el siguiente salto. También proporciona el uso de múltiples enlace físicos, lográndose redundancia de enlace entre dos puntos.*

4.3 ARQUITECTURA DE SERVICIOS INTEGRADOS (*IntServ*)

La Internet estaba basada inicialmente en servicio de envío de paquetes del mejor esfuerzo (*best effort*). Hoy en día Internet provee muchas aplicaciones diferentes que en sus inicios, algunas aplicaciones tienen especiales requerimientos de ancho de banda y retardo. El modelo de Servicios Integrados (RFC 1633 [9]) fue introducido por el IETF para garantizar el comportamiento predecible de estas aplicaciones.

IntServ proporciona una solución de calidad de servicio extremo a extremo por ruta de señalización de origen a destino. También especifica un número de clases de servicio diseñados para conocer las necesidades de los diferentes tipos de tráfico de las aplicaciones. RSVP es uno de los varios protocolos de señalización en esta arquitectura de servicios integrados.

IntServ ha definido especificaciones Tspec (tráfico esperado) y Rspec (recurso especificado):

- Tspec (*tráfico esperado*)

  Especifica el tipo de tráfico que ingresa a la red. Para esto se requiere elementos de red como *routers* y *switches* que proporcionen políticas para comprobar que el tráfico esté dentro del valor Tspec. El tráfico que exceda el valor de Tspec será eliminado.

- Rspec (recurso especificado)

  Solicita niveles de calidad de servicio y reservación de recursos de red. En este caso y al igual que Tspec, IntServ requiere elementos de red como *routers* y *switches* para realizar funciones de control de admisión (*admission control*), el cual verifica si hay suficientes recursos en la red para la calidad de servicio

solicitada. Si los recursos son escasos entonces la solicitud de calidad de servicio es denegada.

4.3.1 Clases de servicios integrados

IntServ define dos clases de servicio: servicio garantizado y carga controlada. Estas clases de servicio pueden ser solicitadas vía RSVP, esto si se asume que todos los elementos de red en la ruta especificada soportan este protocolo de señalización.

- Servicio Garantizado: proporciona bajos retardos de extremo a extremo asegurando el ancho de banda del tráfico que se ajusta a la reservación especificada. Servicio garantizado requiere que cada flujo use colas separadas, lo cual implica baja utilización de la red.
- Carga Controlada: proporciona servicios con bajo retardo sobre redes con moderada carga. Así, es posible brindar calidad de servicio por cada flujo en la red, para esto se debe de tener recursos disponibles y usar señalización RSVP.

4.3.2 RSVP (*Resource Reservation Protocol*)

El Protocolo de Reservación de Recursos RSVP fue desarrollado para comunicar las necesidades de recursos entre los elementos de red. Es descrito en los RFCs del 2205 [6] al 2215 [14].

RSVP es el protocolo de señalización de Servicios Integrados que permite señalar los requerimientos de QoS a la red. Una vez que la red reconoce una solicitud de QoS entonces esta es admitida o denegada. En el caso de ser admitida, el *router* solicitante envía un mensaje RESV y el *router* solicitado responde con un mensaje PATH. En el

mensaje de RSVP se incluye informaciones como las direcciones IP de los elementos extremos, puertos UDP a usar y el requerimiento de QoS. También incluye la información de los valores de Tspec y Rspec.

La reservación de recursos RSVP es unidireccional, para que sea bi-direccional debe de ser solicitada en ambos sentidos.

La reservación de recursos se debe hacer en cada elemento de red, así los mensajes de RESV y PATH son intercambiados entre cada dispositivo. También, la reservación se hace por tipo de tráfico, es decir, la señalización entre los *routers* en todo el camino, la revisión del tráfico a reservar en cada salto, hace que sea compleja la reservación de la ruta en todos los elementos de red de la ruta. Adicionalmente se suma el incremento de consumo de recursos de memoria y CPU en cada elemento para soportar largos números de reservaciones.

Sin embargo, RSVP puede hacer reservación de tráfico para un tráfico específico. Esto forma la base de la implementación de MPLS. Si paquetes pertenecen a un flujo reservado, este puede ser definido tal que pertenezca una FEC (*Forwarding Equivalence Class*) particular. Etiquetas adjuntadas pueden ser creadas para que se asocien etiquetas con instancias FEC. Estas etiquetas pueden ser distribuidas usando LDP o un protocolo de *routing*.

En la figura 4.2, se muestra una red implementada con servicios integrados usando RSVP y WFQ. Se reserva un ancho de banda en toda la ruta, cada ancho de banda esta dividido en flujos de diferentes prioridades, así se garantiza que los paquetes de alta prioridad siempre sean priorizados. La configuración de RSVP y WFQ debe de hacerse en todos los elementos de red en la ruta.

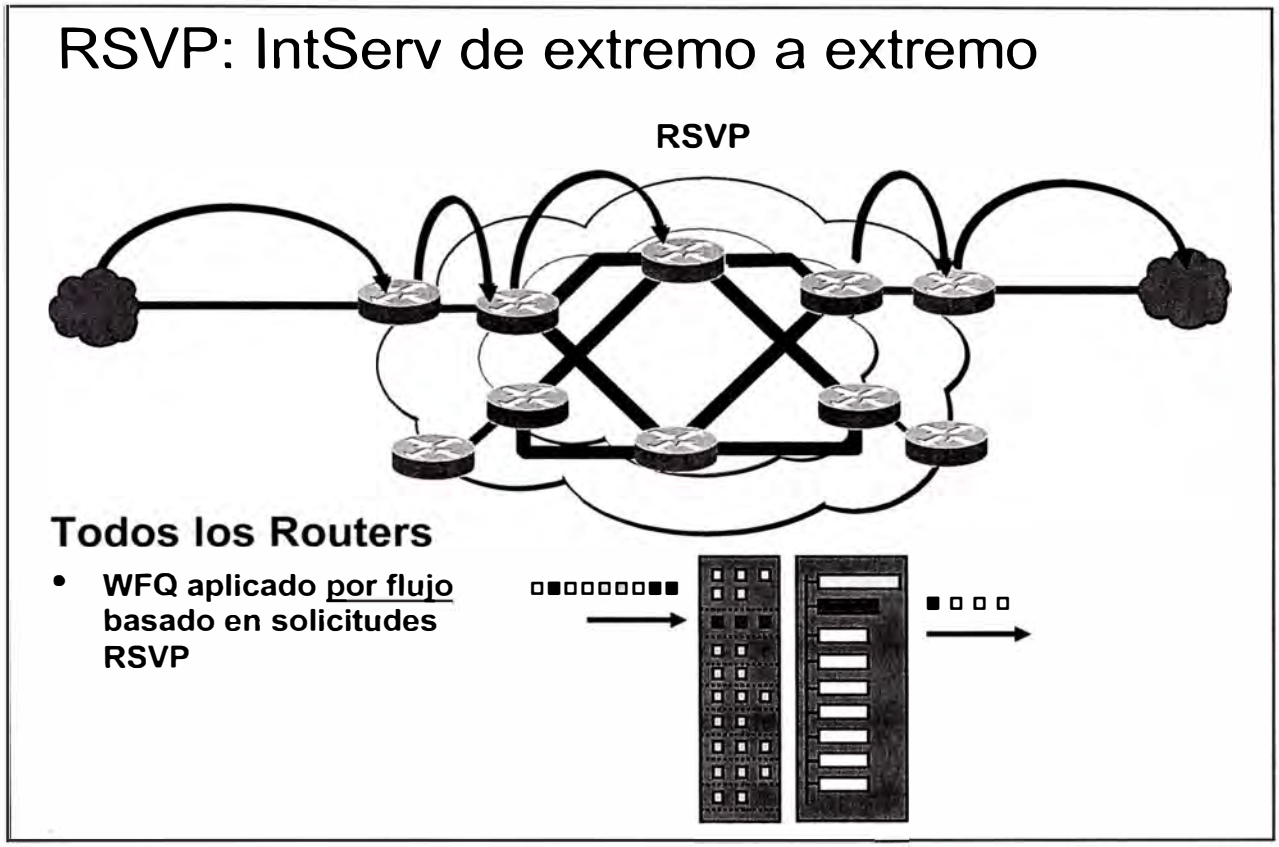


Figura 4.2: Reservación en un sentido usando RSVP y WFQ en cada router.

4.3.3 Implementación de MPLS usando servicios integrados (*IntServ*)

MPLS pude ser habilitado en LSRs al asociar etiquetas a flujos que tienen reservación RSVP.

Los paquetes que tienen una reservación RSVP pueden ser considerados como FECs. Una etiqueta puede identificarse con una FEC. Las etiquetas creadas y el flujo RSVP deben ser distribuidos entre los LSRs.

Como se muestra en la figura 4.3, un *host* envía un mensaje de RSVP PATH y el receptor responde con un mensaje RSVP RESV.

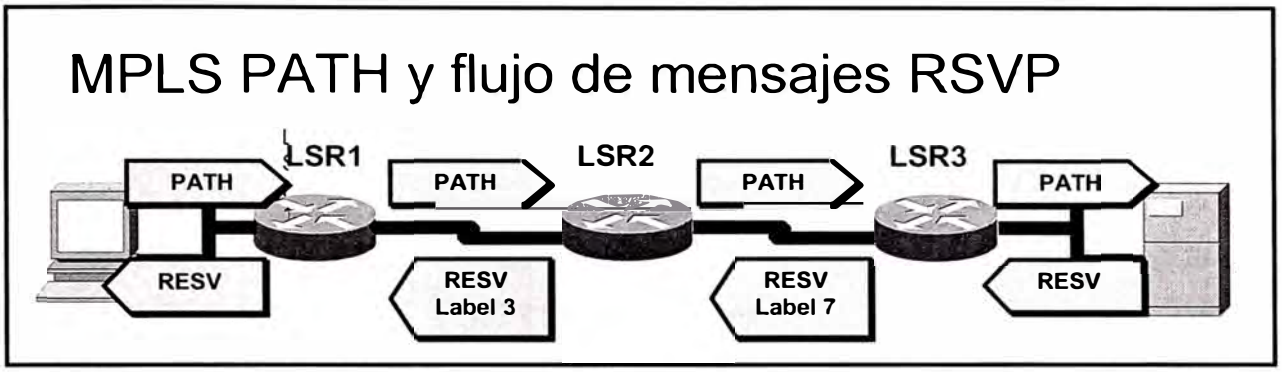


Figura 4.3: MPLS usando RSVP en IntServ.

El LSR3 recibe el mensaje RESV, asigna una etiqueta de su pool y envía a LSR2 el mensaje RESV con la etiqueta asignada (7). También esta etiqueta 7 es asignada a la tabla LFIB del LSR3. LSR2 crea una entrada con etiqueta 7 en su tabla LFIB, entonces este asigna una nueva etiqueta (3) y es enviado a LSR1. Como los mensajes respuesta RESV han sido enviados de extremo a extremo entonces se puede decir que un LSP ha sido establecido y cada LSR puede asociar recursos de calidad de servicio en el LSP.

El LSR1 puede asociar todos los paquetes asociados en una FEC y asignarlos a un particular LSP. Por ejemplo, todos los paquetes destinados a un particular prefijo destino pueden ser asignados a un particular LSP. De esta manera, un simple LSP puede proporcionar una calidad de servicio garantizada ante una gran cantidad de flujos de tráfico. MPLS también define un objeto LABEL_REQUEST, el cual podría ser llevado en un mensaje RSVP PATH. Según la figura se iniciaría en LSR1. Este objeto puede decirle a LSR3 que responda con un mensaje RESV para establecer el LSP al igual que configurar el LSP de extremo a extremo.

Antes de empezar con la arquitectura de Servicios Diferenciados hablaremos de IP *Precedence* para comprender lo que significa DSCP (*Differentiated Services Code Point*)

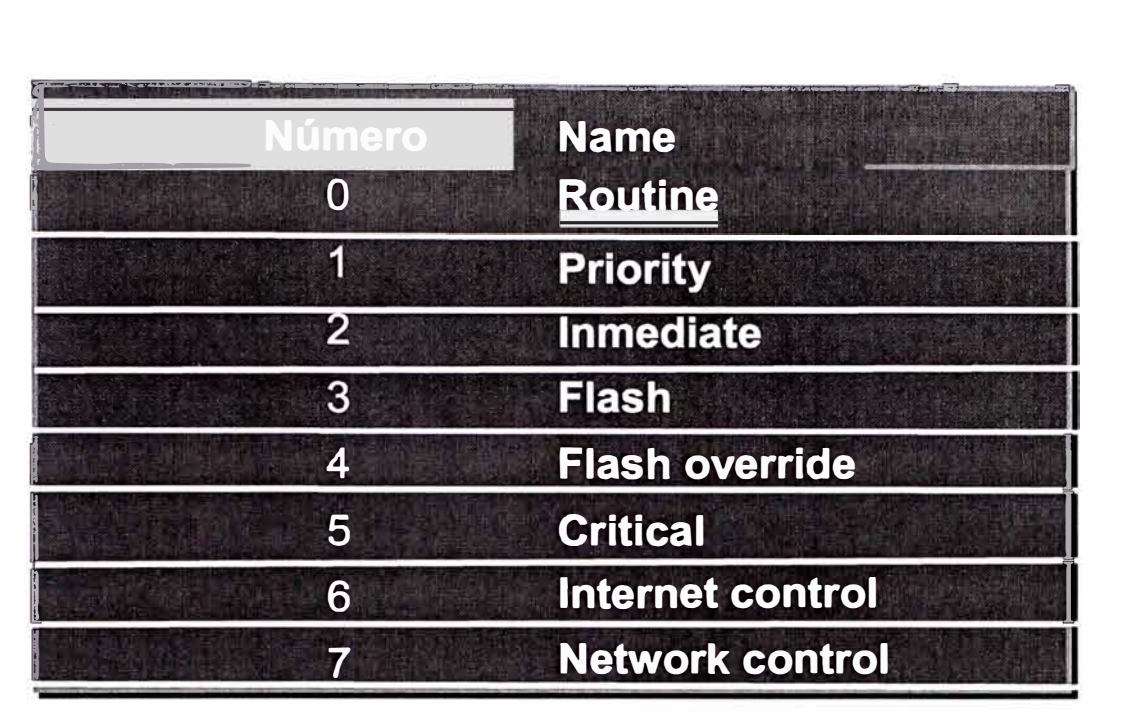
4.4 IP PRECEDENCE

Como hemos podido observar en la sección anterior, la implementación de RSVP en servicios integrados es muy compleja lo cual lo hace no escalable. IP *Precedence*, definido por el lIETF en los RFCs 781 y 1812 [15,1812], ha simplificado el aprovechamiento de calidad de servicio IP al adoptar un modelo de clasificación de flujos de tráfico en clases y proporcionando la apropiada calidad de servicio a cada flujo clasificado.

Los paquetes pueden ser clasificados en los elementos de borde de la red y pueden pertenecer a 8 clases diferentes. Esto se obtiene al cambiar los bits de precedencia en el campo ToS (*Type of Service*) de la cabecera IPv4.

En caso de congestión los paquetes de baja prioridad son eliminados para dar paso a los paquetes de mayor prioridad. Sin embargo, el RFC 1349 [17] redefine estos tres bits y adhiere un séptimo *bit* en el *byte* para designar la solicitud de ToS del paquete, en adición a su prioridad. Luego de que los paquetes son marcados con el apropiado bit IP *Precedence*, los elementos de la red a lo largo de la ruta que toma el paquete conocen el relativo nivel de precedencia del paquete y pueden aplicar un reenvío de paquetes preferencial en un alto nivel de prioridad.

En la figura 4.4 se muestra los valores de *IP precedence* y los nombres que toman los tres bits de Precedencia (ToS). Por ejemplo, el valor de 5 indica prioridad crítica.



Número	Name
0	Routine
1	Priority
2	Inmediate
3	Flash
4	Flash override
5	Critical
6	Internet control
7	Network control

Figura 4.4: Valores de IP Precedence

El *IP Precedence* solo permite especificar una relativa prioridad al paquete. Este no proporciona una diferencia específica de eliminación de paquetes para paquetes de similar nivel de prioridad. Por ejemplo, si tráfico TELNET y SNMP son asignados a la misma clase, en caso de congestión no se descartaran paquetes de TELNET a favor de paquetes SNMP, se descartarán ambos tipos de paquetes.

Estos tres bits restringen las posibles clases de prioridad a ocho. Hay que considerar que se reservan dos prioridades para control de red y control de Internet. Entonces las clases de prioridad se reducen a seis.

Así, el RFC-1349 [17] redefine el sub-campo ToS para utilizar los bits 3, 4, 5 y 6, y elimina el concepto descrito en el RFC 791 [18] que solo señalaba dos clases de prioridad.

En la figura 4.5 se detalla el formato de la cabecera IP para identificar el campo ToS. El ToS permite la interoperabilidad para brindar calidad de servicio de extremo a extremo.

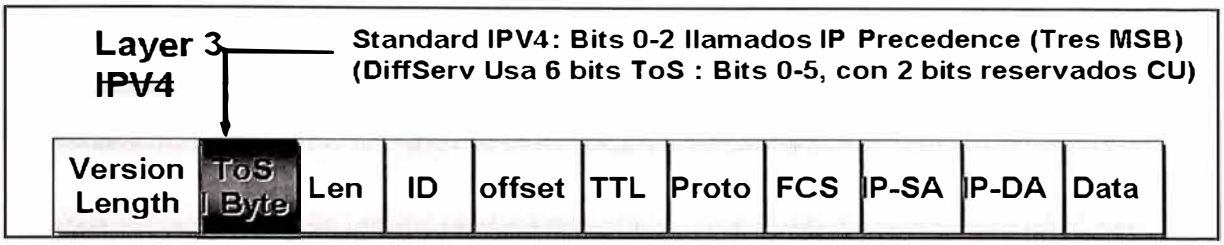


Figura 4.5: Detalle del datagrama IPv4

4.5 ARQUITECTURA DE SERVICIOS DIFERENCIADOS (*DiffServ*)

El modelo *DiffServ* divide el tráfico en pequeños números de clases que asignan recursos por clase. Este modelo es similar al modelo *IP Precedence*. Usa seis bits en la cabecera IP los cuales son llamados DSCP (*Differentiated Services Code Point*). Estos 6 bits pueden implementar 64 diferentes clases, sin embargo, en la práctica solo pocas clases son implementadas.

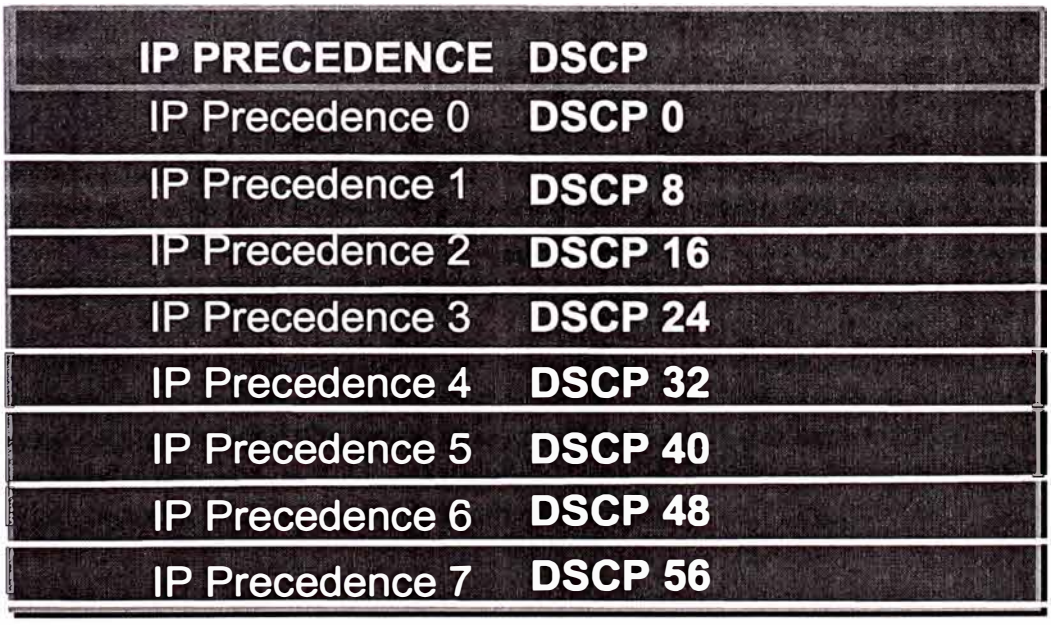


Figura 4.6: Match entre IP Precedence y DSCP

La figura 4.6 muestra la comparación de valores de los campos ToS y DSCP. Cabe señalar que el valor de ToS=5 es el mismo valor de DSCP=40, ambos indican que el paquete requiere alta calidad de servicio.

Los RFCs 2474 y 2475 [11,12] definen la arquitectura de servicios diferenciados y el uso general de bits en el campo DS. DS es el nuevo campo que define la clase de servicio, antes era definido por el campo ToS según el RFC 1349 [17].

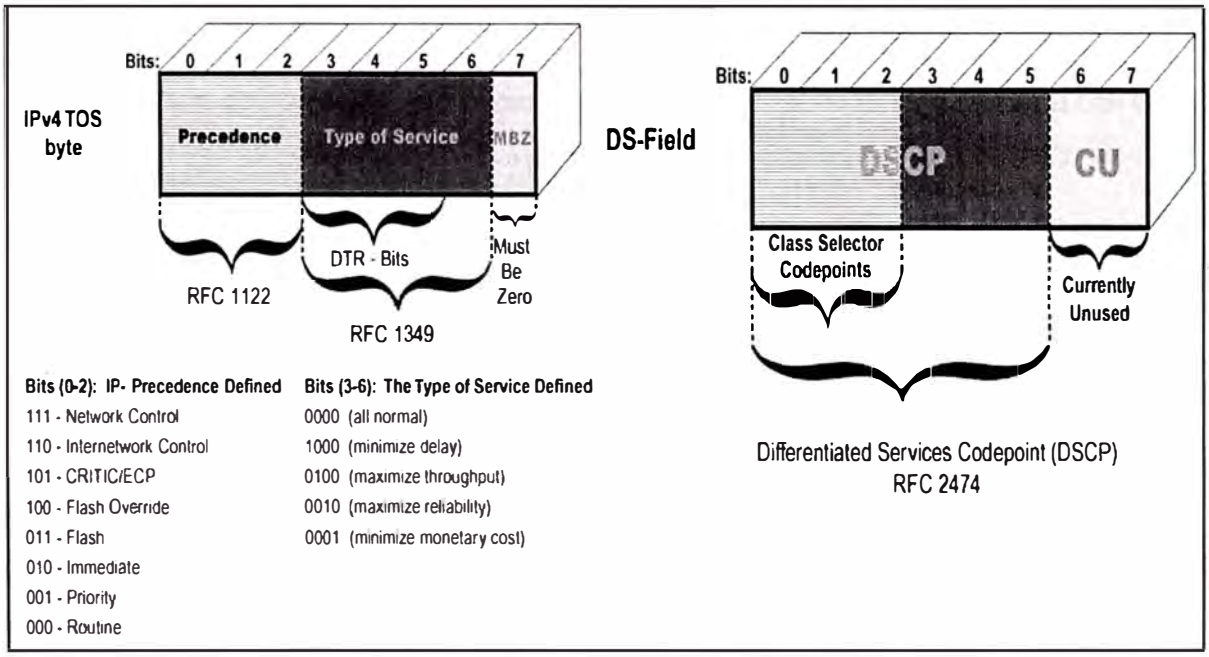


Figura 4.7: Comparación entre ToS IPV4 y el campo DS

Al valor del campo DS se le conoce como DSCP que es usado para marcar paquetes y así poder luego seleccionar un comportamiento por salto (*Per-Hop Behavior*). Tal como se muestra en la figura 4.7, los 6 primeros bits del campo DS forman el DSCP y dan su valor, los otros dos bits no son usados y son denominados CU (*Currently Unused*).

4.5.1 Comportamiento de las clases por salto PHB (*Per-Hop Behavior*)

Cada elemento de red o salto examina el valor de DSCP y determina la QoS requerida por el paquete. A estos requerimientos se le conoce como *Per-Hop Behavior*. Cada elemento de red tiene una tabla que relaciona el DSCP encontrado en un paquete a un PHB que determina como el paquete será tratado. El DSCP es un número o valor que llevará el paquete y el PHB son comportamientos bien especificados que se aplicarán a los paquetes.

Una colección de paquetes que tienen el mismo valor de DSCP y cruzan a través de la red en una dirección particular, es llamado *Behavior Agrégate* (BA).

Están disponibles 4 tipos de implementaciones de PHB en Servicios Diferenciados: *Default* PHB, *Class-selector* PHB, *Expedited Forwarding* (EF) PHB y *Assured Forwarding* (AF) PHB.

- *Default* PHB: indica un envío de paquetes usando mejor esfuerzo (*Best Effort*). Los paquetes son marcados con el valor DSCP de 000000y obtienen servicio *"best effort"* (sin calidad de servicio). También, si el paquete no coincide con algún DSCP de la tabla del nodo entonces se asigna al paquete el *Default* PHB.
- *Class-Selector* PHB: Actualmente muchas implementaciones usan *IP Precedence* debido a su simplicidad y fácil implementación. Para preservar la compatibilidad con *IP Precedence*, se definen valores de DSCP de la forma *xxx*000 (donde x puede ser 0 ó 1). Estos valores de DSCP son llamados *class-selector*. El *default codepoint* es un *class-selector*, 000000. El PHB asociado al *class-selector codepoint* es un class-selector PHB. Estos PHBs también tienen el mismo comportamiento de reenvío de paquetes como si este

implementado *IP Precedence* en los nodos. Por ejemplo, paquetes que tienen como valor de DSCP 101000 (IP *Precedence* 101) tienen un tratamiento preferencial de reenvío de paquetes comparado con paquetes que tienen valores de DSCP de 01100 (IP *Precedence* 011). Estos PHBs aseguran que coexistan los campos DS con los de *IP Precedence* en los diferentes nodos.

- *Expedited Forwarding* (EF) PHB: Los paquetes que son marcados con este tipo de PHB son priorizados sobre otros, con mínimos retardos y bajo costo. EL EF PHB en la arquitectura *DiffServ* proporciona baja perdida de paquetes, bajo retardo, bajo *jitter* (variación del retardo) y servicio garantizado de ancho de banda. Las aplicaciones como VoIP, video, *online e-commerce*, requieren estas garantías. El EF PHB implementa un servicio *premium* a ciertas aplicaciones. Estas aplicaciones deben de ser específicamente etiquetadas como aplicaciones críticas y en caso de existir congestión solamente este tipo de tráfico tendrá una alta prioridad. Según el RFC 2474 [11], el valor de DSCP recomendado para EF PHB es 101110.
- *Assured Forwarding* (AF) PHB: El marcado del DSCP como AF especifica una clase o una preferencia de *drop* para paquetes IP. Los paquetes con diferentes preferencias de *drop* en la misma clase AF son *dropeados* o descartados basados en sus relativos valores de precedencia de *drop* en la clase AF. El RFC 2587 [19] recomienda 12 AF PHBs representando 4 clases AF: AF1y, AF2y, AF3y y AF4y. Cada clase es asignada a cierta cantidad de *buffers* en memoria y ancho de banda, dependiendo del SLA que acuerda el proveedor de servicios. En cada clase AFx, es posible especificar 3 valores de precedencia de *drop*. Si existe congestión y paquetes de la clase AFx

necesitan ser descartados, entonces estos paquetes serán descartados en la siguiente precedencia tal que dp(AFx1) <= dp(AFx2) <= dp(AFx3), donde dp(AFxy) es la probabilidad de que el paquete sea eliminado de la clase AFxy. Por lo tanto, cada clase AF usa tres valores DSCP.

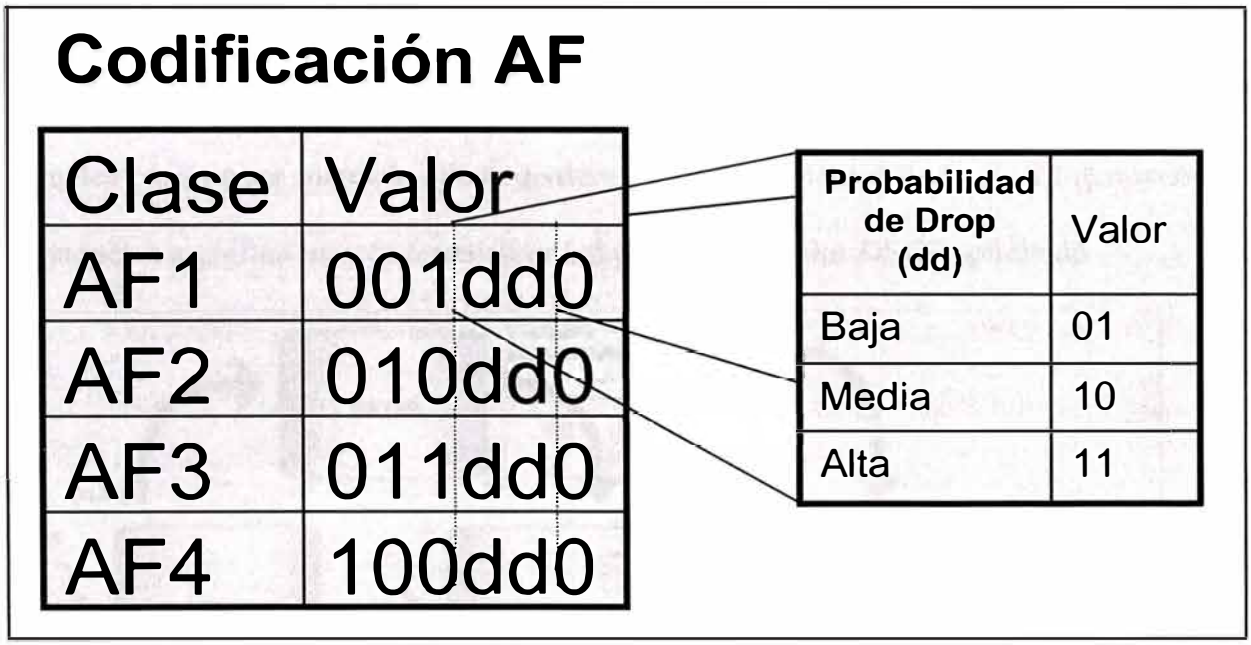


Figura 4.8: Cada clase AF (4) puede manejar tres probabilidades de descarte de paquetes

En la figura 4.8 se muestra que la clase AF PHB puede ser de 4 clases (AF1, AF2, AF3 y AF4) y cada clase puede manejar tres probabilidades de descarte de paquetes (baja, media y alta).

4.5.2 Condicionadores de tráfico en servicios diferenciados.

La región *DiffServ* (DS) esta compuesta por uno o más dominios DS. Cada dominio es configurado usando los diferentes tipos de PHBs como valor de DSCP. Debe de habilitarse *DiffServ* en toda la ruta del paquete IP. Asimismo, en un dominio DS se

configura DS en los nodos de ingreso, en los nodos de *backbone* y en los nodos de egreso de la red MPLS.

Por lo general en un dominio de servicios diferenciados se sigue el proceso que se muestra en la figura 4.9. Primero se clasifica el paquete, es decir los paquetes se agrupan en flujos de tráfico, clases, de acuerdo a la información de la cabecera del paquete. Segundo, se chequea los paquetes clasificados de acuerdo a su precedencia o valores DSCP a nivel de encolamiento en la interface (*Token Bucket*). Tercero, los paquetes pasan a ser marcados de acuerdo a los requerimientos de QoS. El marcado de paquetes significa marcar ó remarcar los paquetes al valor DSCP solicitado.

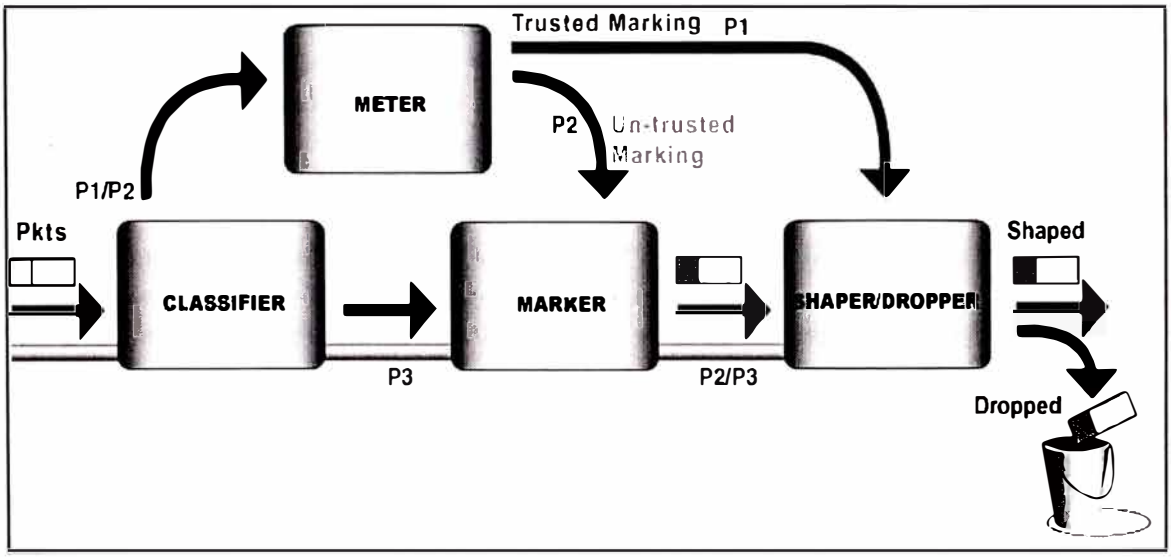


Figura 4.9: Condicionadores de tráfico en Servicios Diferenciados.

Finalmente los paquetes pasan a un *shaper* o limitador de ancho de banda por donde los paquetes priorizados tendrán trato preferencial y los demás serán descartados en caso de congestión. En la figura 4.9 se muestra los procesos por los cuales pasa un paquete antes de abandonar la interface de salida o de ser descartado.

4.5.3 Mecanismos de servicios Diferenciados

El modelo de Servicios Diferenciados solo define el uso del DSCP y PHBs. Los PHBs simplemente describen el comportamiento de envío de paquetes de un nodo. El modelo no especifica como estos PHBs pueden ser implementados. Una variedad de técnicas de encolamiento, medición y modelación de tráfico pueden ser usadas para ofrecer el condicionamiento de tráfico y PHB deseados.

A continuación se describen dos políticas para el manejo del flujo de tráfico:

- Políticas de tráfico (*Traffic Policing).* Las Listas de Acceso de Cisco o más conocidas como CAR (*Commited Access Rate*) pueden ser usadas como condicionadores de tráfico y para proporcionar PHB con clases AF en los bordes y el núcleo de un dominio DS. Los paquetes son medidos y diferentes acciones pueden ser tomadas dependiendo en si el paquete esta dentro del ancho de banda especificado (Bc: *Commited Burst*), esta en exceso (Be: *Excess Burst*) o excede inclusive el exceso de tráfico configurado (Bc +Be). Los paquetes que están dentro del ancho de banda especificado Bc están permitidos. El tráfico que esta entre Bc y Be es tráfico en exceso. El tráfico que es mayor a Bc + Be es descartado. Un paquete puede ser transmitido, descartado o remarcado con un diferente valor DSCP (para pasar a otra clase de prioridad AF) dependiendo de cómo sea configurada la política.
- Conformación de tráfico (*Traffic shaping*): GTS (*Generic Traffic shaping*) y FRTS (*Frame Relay Traffic Shaping*) son mecanismos que simplemente descartan los paquetes en congestión. Esto puede ser configurado definiendo simplemente una promedio de tráfico Bc y un exceso Be.

4.5.4 Acuerdo para clases PHB

El PHB es importante en *routers* del núcleo dependiendo del valor de DSCP marcado en los paquetes. EF es implementado usando LLQ (*Low Latency Queuing*), y AF puede ser implementado usando una combinación de CBWFQ (*Class-Based Weighted Fair Queuing)* y WRED (*Weighted Random Early Detection*) o CAR (*Commited Access Rate*):

- LLQ para AF PHB: LLQ ofrece una prioridad estricta de encolamiento para tráfico sensible a los retardos tal como VoIP a lo largo de la ruta de los daos. LLQ debe de ser implementado en cada salto. Esta cola de prioridad es definida tal que el exceso de trafico sensible al retardo no interfiera con las otras clases.
- CBWFQ y WRED para AF PHB: CBWFQ permite partir el ancho de banda en varias clases definidas. Un ancho de banda puede ser definido a cada clase o un porcentaje del ancho de banda de la interface para el cual esta política será aplicada. En una clase AF, los paquetes pueden ser descartados basados en el campo de precedencia de *drop* usando WRED.
- Políticas de tráfico para AF PHB: CAR puede ser usado para implementar el PHB en el núcleo y también para condicionar tráfico y proporcionar PHB para clases AF en el núcleo del dominio DS. Los paquetes son medidos, y diferentes acciones son tomadas, dependiendo de si el paquete en cuestión esta dentro del tráfico definido, excede o viola el ancho de banda configurado.

En resumen podemos decir que los servicios diferenciados pueden brindar clases de servicio que pueden ser por ejemplo, *premium, gold, silver, bronce.* Cada clase representa diferentes flujos de tráfico con diferentes requerimientos de calidad de servicio. Como se muestra en la figura 4.10, a los paquetes al ingresar a la red se les aplica técnicas de marcado, clasificación, políticas, etc. (TCB: *TrafficCondition Block*). Para que finalmente tengan el tratamiento esperado en todo el dominio *DiffServ* de la red.

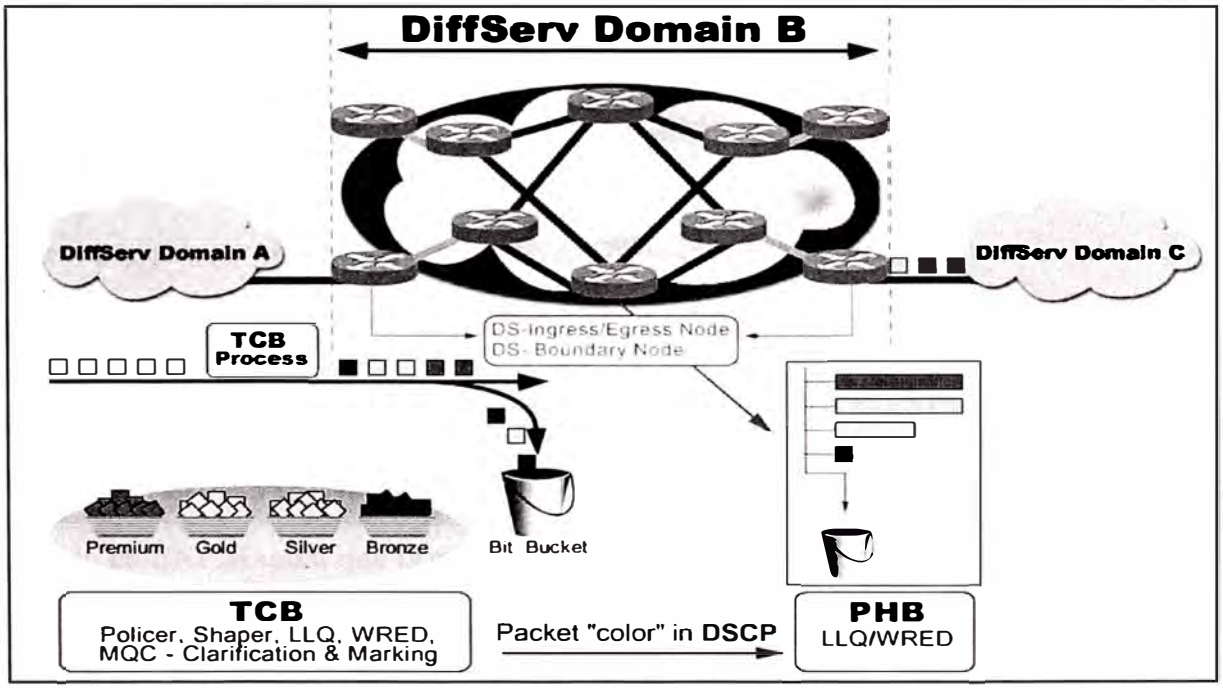


Figura 4.10: Arquitectura de Servicios Diferenciados.

4.5.5 Implementación de MPLS usando servicios diferenciados

Los LSRs de MPLS no examinan el contenido de la cabecera IP y el valor de DSCP como es requerido en *DiffServ*. Esto significa que el apropiado PHB debe ser determinado del valor de la etiqueta. La cabecera *shim* de MPLS tiene un campo de tres bits llamados Exp. Este campo fue originalmente definido para uso experimental.

Puede soportar 8 diferentes valores y es usado por MPLS en ocho diferentes clases de servicios diferenciados. El campo de DSCP es de 6 bits y puede soportar hasta 64 clases de servicio (CoS).

La información del campo DSCP no es visible para los LSRs, ellos solo leen la cabecera MPLS. La información de *DiffServ* es visible usando el campo EXP de la etiqueta. Es decir, los 3 primeros bits de DSCP son copiados al campo EXP de MPLS en el equipo de borde de la red. Cada LSR, en el LSP de un paquete, analiza el campo EXP y lo asocia a una clase PHB. El proveedor de servicio también puede variar el campo EXP para brindar la calidad de servicio solicitada por el cliente. Esta característica es diferente a sobre-escribir del campo *IP Precedence* del paquete, esto permite mantener intacto el campo *IP Precedence* para uso del cliente. La clase de servicio configurada al cliente no es cambiada mientras el paquete viaja por la red MPLS. Los LSP creados de esta forma son conocidos como E-LSPs o Exp-LSPs. Un E-LSP puede soportar hasta 8 diferentes clases PHB, es decir el encolamiento es basado en EXP al igual que la prioridad al descartar paquetes.

Los L-LSPs o *Label*-LSP son usados en caso se requiera más de 8 clases PHB en la red. En este caso la clase PHB es asignada de acuerdo a la información en la etiqueta. Para el caso de ATM, donde la cabecera *shim* no es usada, la clase PHB es asociada según el campo VCI. Solamente una clase PHB es posible por L-LSP, excepto para la clase AF. Es decir, el encolamiento es basado en la etiqueta y la prioridad al descartar paquetes es según el campo EXP [7].

En la figura 4.11 se muestra como un paquete IPv4 es encapsulado con una cabecera MPLS. También se describe el proceso de agrupación de paquetes en clases BA para luego marcarlos en el campo EXP.

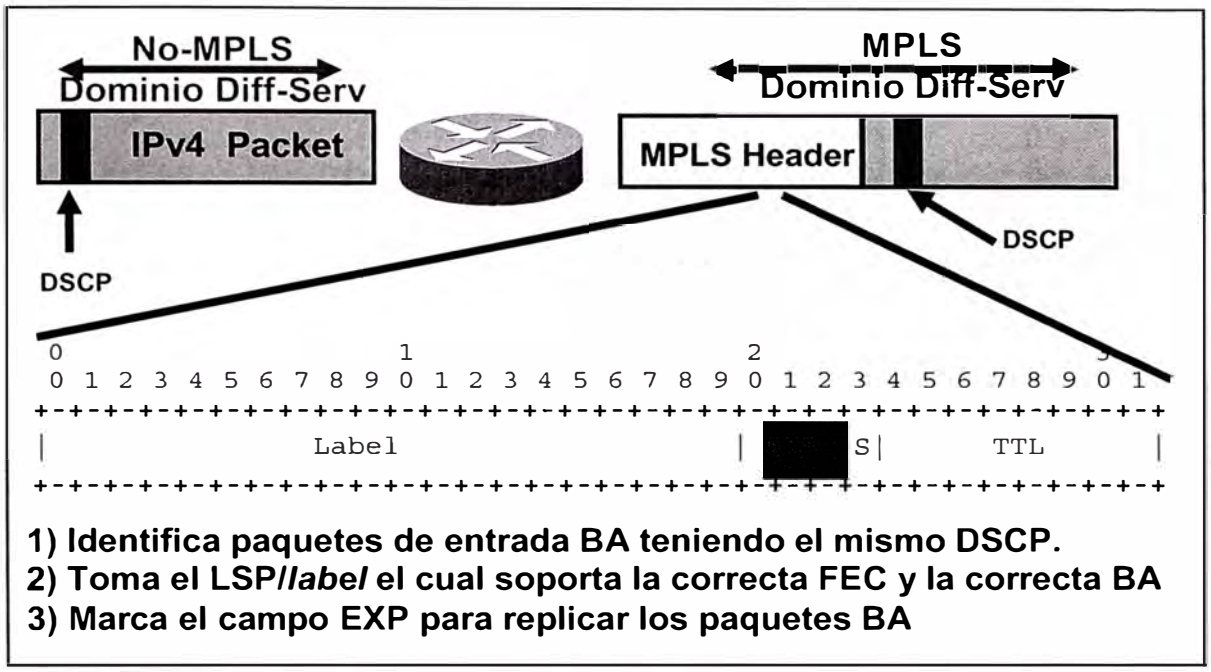


Figura 4.11: LSR de borde formando L-LSP. Haciendo uso de DSCP.

4.6 QoS sobre MPLS VPN

Una VPN (*Virtual Private Network*) es definida como un grupo de usuarios compartiendo una misma infraestructura de red publica con ciertas políticas que controlan la conectividad y la calidad de servicio entre las sedes remotas.

Las calidades de servicio y las clases de servicio CoS) están disponibles en los *peers* VPN creados. Por ejemplo, una aplicación de tiempo real como VoIP podría recibir una CoS preferencial sobre una simple transferencia de archivos. Para describir QoS sobre VPNs se muestra dos modelos: tubería (*pipe*) y manguera (*hose*).

4.6.1 QoS sobre MPLS VPN: Modelo tunería (*pipe*)

En este modelo el proveedor de servicio proporciona al cliente VPN cierta calidad de servicio garantizada para el tráfico entre un *router* del cliente (CE: *Customer Edge router*) y otro en la misma VPN. Este modelo puede ser representado como una

tubería entre dos *routers* CE. Cualquier tráfico que ingresa a esta tubería recibe QoS garantizada. El *router* PE al final de la tubería puede especificar el tráfico específico que usará esta tubería. Este modelo es similar a ATM o Frame Relay. Sin embargo ATM o Frame Relay tienen conexiones bi-direccionales y el modelo *pipe* o tubería es unidireccional. Esta naturaleza unidireccional permite tener patrones de tráfico asimétrico, lo cual permite diferentes velocidades de tráfico en cualquier dirección entre los *routers* CE del cliente.

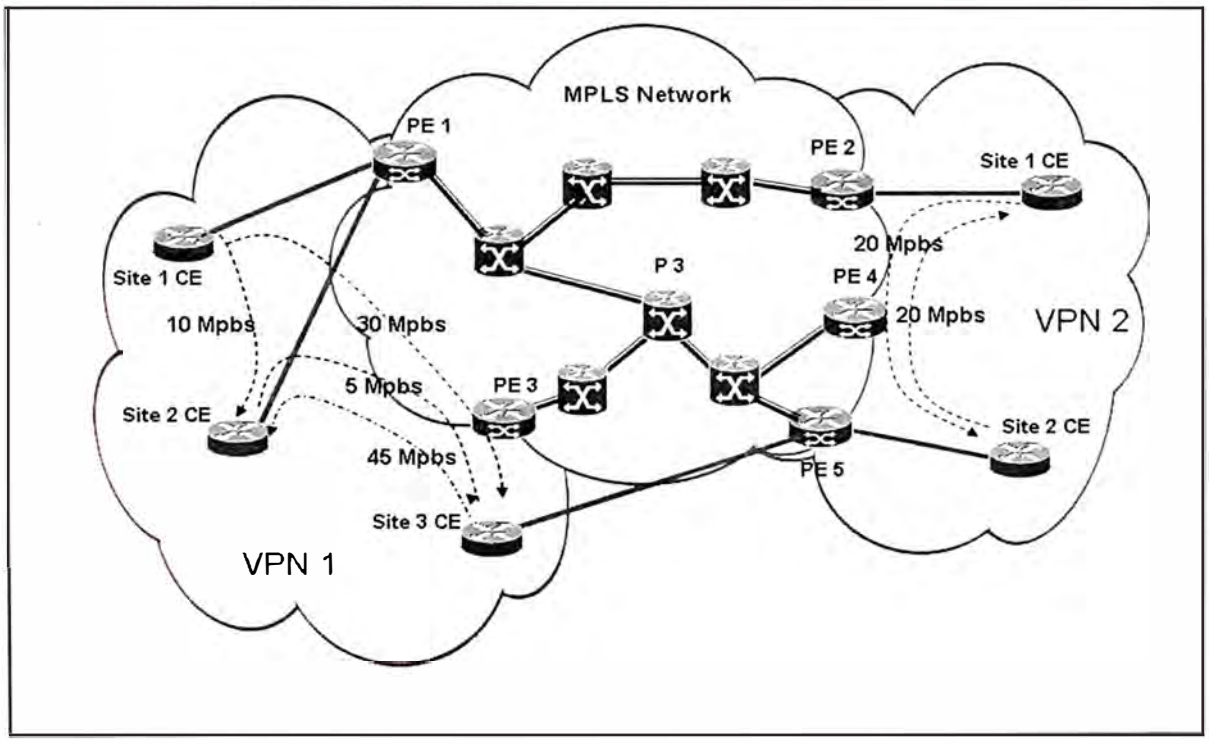


Figura 4.12: QoS sobre MPLS VPN – Modelo Tubería (pipe)

Como se observa en la figura 4.12, el proveedor de servicios proporciona una VPN1 con una tubería que garantiza 30 Mbps para tráfico del site1 al site3, otra tubería que garantiza el tráfico de 10 Mbps del site1 al site2 y aún otra tubería que garantiza tráfico de 5Mbps del site2 al site3. Hay también otra tubería que garantiza 45Mbps de flujo de tráfico del site3 al site2. Esta asimetría es debido a la naturaleza

unidireccional de la calidad de servicio en tuberías MPLS y a que se tiene conexiones con diferentes CEs (sedes remotas). La VPN2 tiene tuberías simétricas que garantizan 20Mbps en ambos sentidos.

Para una apropiada implementación de este modelo y su respectiva aplicación de QoS, es conveniente conocer a detalle la cantidad de tráfico que existe entre las tuberías. De esta manera se tendrá una visión de los recursos necesarios en la red. Por ejemplo, la asignación de ancho de banda a los LSP formados entre los *routers* PE (*Provider Edge router*) debe tener un valor de acuerdo a la suma de los tráficos de las diferentes tuberías que circulan por el LSP.

La característica principal de una MPLS VPN es la autonomía en calidad de servicio, *routing*, reservación de ancho de banda, etc. Esto se logra con la aplicación de VRFs (*VPN Routing and Forwarding*), cada VRF es aplicado a una VP. Por ejemplo, en la figura 4.12, se muestra que el Site1, Site2 y Site3 pertenecen a la VPN-1. Estas sedes remotas podrán conocer las rutas de las demás sedes, también permite la aplicación de QoS y reservación de ancho de banda de acuerdo a lo solicitado por el cliente en cada sede. Es decir, los VRFs permiten el establecimiento de VPNs que compartirán la misma infraestructura de red pero con absoluta independencia a las demás VPN coexistentes en el *backbone*. Los VRFs solamente son aplicados en los *routers* PE.

4.6.2 QoS sobre MPLS VPN: Modelo manguera (*hose*)

En este modelo, el proveedor de servicio brinda al cliente ciertas garantías al tráfico que un particular *router* CE enviaría y recibiría de otros *routers* CEs en la misma VPN. Para el cliente, es mucho más fácil la implementación de este modelo pues, por

lo general, el cliente no tiene el análisis o capacidad de planeamiento del tráfico entre sus sedes.

Los dos parámetros usados en este modelo son el ICR (*Ingress Commited Rate*) y el ECR (*Egress Commited Rate*)

- ICR (*Ingress Commited Rate*). Es la cantidad de tráfico que los *routers* CEs, en la misma VPN, pueden recibir de un particular *router* CE.
- ECR (*Egress Commited Rate*). Es la cantidad de tráfico que los *routers* CEs, en la misma VPN, pueden enviar a un particular *router* CE.

Los valores de ICR y ECR son independientes uno del otro y no necesariamente tiene que ser el mismo.

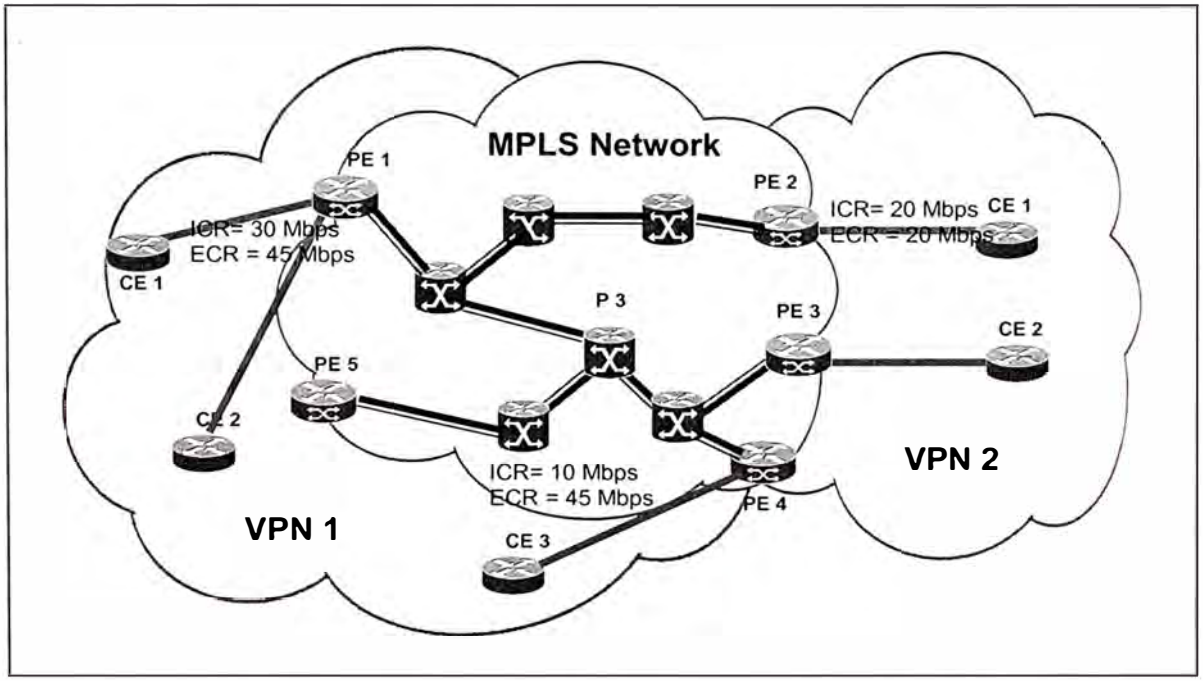


Figura 4.13: QoS sobre MPLS VPN – Modelo manguera (hose)

En la figura 4.13, el proveedor de servicios brinda ciertos valores de ICR y ECR en cada VPN. En la VPN1, los *router* CE2 y CE3 pueden recibir hasta 30Mbps del

router CE1 (CE1 ICR=30Mbps). Este tráfico puede ser dirigido al *router* CE1, al *router* CE2 o de manera distribuida. De igual forma, los *router* CE2 y CE3 pueden enviar hasta 45 Mbps al *router* CE1 (CE1, ECR=45 Mbps). En la VPN2 cierto tráfico garantizado de hasta 20Mbps para tráfico enviado desde CE1 a CE2 (CE1 ICR=20). El router CE1 también tiene un ECR de 20Mbps, esto significa que el *router* CE2 puede enviar hasta 20 Mbps al *router* CE1

El modelo *hose* soporta múltiples clases de servicio, esto lo hace semejante a *DiffServ*. Las diferentes clases de servicio en el modelo *hose* son soportadas usando mecanismos implementados en *DiffServ*.

Un proveedor de servicio puede ofrecer a sus clientes VPNs del modelo *pipe*, *hose* o una combinación de ambas. El *router* de ingreso a la red MPLS (PE), determina que tráfico recibe una determinada clase de servicio, dependiendo de la interface de entrada, la dirección IP origen o destino, el *IP Precedence*, el número de puerto TCP o una combinación de estos valores. El *router* de ingreso (PE) puede también aplicar políticas al tráfico de entrada y marcar los paquetes basados en los acuerdos, SLAs, establecidos con los clientes. Estos paquetes pueden ser marcados de manera diferente y eliminados en caso de congestión.

4.7 QoS sobre MPLS

En un escenario real, con *backbone* MPLS (*routers* P y PE), MPLS VPNs creadas, y *routers* de clientes (CE) conectados a la red MPLS, podemos decir que un paquete enviado por un *router* CE al *backbone* es enviado con una precedencia (3 primeros bits del campo DSCP) que le permitirá al paquete recibir el tratamiento deseado.

Estos bits de precedencia son copiados en el campo EXP de la cabecera MPLS en el *router* PE de ingreso. Sin embargo, el proveedor de servicio podría querer cambiar el campo EXP para brindar, o en todo caso asegurarse, que la calidad de servicio del paquete es la ofrecida al cliente.

Esta característica permite a los proveedores de servicio variar el valor del campo EXP en lugar de sobrescribir el valor de la precedencia en el paquete enviado por el cliente. De esta forma la cabecera IP permanece inalterable desde el momento en que es enviado por el cliente.

QoS Sobre MPLS permite a los proveedores de servicio clasificar paquetes de acuerdo a su tipo, interface de entrada, y otros factores para marcar cada paquete en el campo EXP de la cabecera MPLS sin variar el campo de IP *Precedence* o DSCP. Por ejemplo, los proveedores de servicio pueden clasificar paquetes con o sin considerar la velocidad de los paquetes que ingresan al *backbone* a través del PE. Los clientes pueden diferenciar tráfico en sus redes y así no necesitarán comprar múltiples clases de servicio al proveedor de servicio. Los bits del campo Exp de MPLS permiten especificar la QoS de un paquete MPLS y el valor de IP *Precedence* o DSCP especifican la QoS en un paquete IP.

El fabricante Cisco actualmente ha implementado las siguientes funcionalidades en MPLS QoS:

- CAR (*Commited Access Rate*). *Clasifica los paquetes de acuerdo a las tasas de transferencia de entrada y salida. Esto permite marcar el campo EXP o IP precedence / DSCP a un valor apropiado.*
- WRED (*Weighted Random Early Detection*). *Cumple la función de monitoreo de tráfico en la interface para evitar congestión descartando*

paquetes basándose en IP precedence/DSCP o el campo EXP de la cabecera MPLS.

- CBWFQ (*Class-Based Weighted Fair Queuing*). *Una técnica automatizada de encolamiento que usa un algoritmo de encolamiento para asegurar la asignación de ancho de banda a las diferentes clases de tráfico en la red.*

4.7.1 Campo EXP de MPLS.

La configuración de valores del campo EXP de la cabecera MPLS llena las expectativas de los proveedores de servicio quienes no quieren alterar el valor del campo *IP precedence* de los paquetes IP que son transportados a través de la red. Con la selección de diferentes valores del campo EXP, se pueden marcar paquetes basados en sus características deseadas, de tal manera que tendrán el tratamiento de prioridad correspondiente durante congestión del tráfico.

4.7.2 Priorizar paquetes

Los paquetes IP pueden ser clasificados de acuerdo a los campos de dirección IP origen, dirección IP destino, puerto utilizado, tipo de protocolo o clase de servicio. La clasificación de paquetes es importante, porque de ello dependerá su prioridad. La prioridad de los paquetes indicará como será tratado durante periodos de congestión de tráfico. Por ejemplo, los proveedores de servicio tienen acuerdos, SLAs, con sus clientes. Los acuerdos especifican ancho de banda garantizado, calidad de servicio de determinados servicios y diversas aplicaciones.

CAPÍTULO V

MPLS: DISEÑO E IMPLEMENTACION

5.1 CRITERIOS PARA EL DISEÑO DE UNA RED MPLS.

A continuación se mencionan los criterios de diseño en la elección de una arquitectura de red MPLS para el *backbone*.

5.1.1 Criterio en la elección del tipo de Red de la capa2

La red puede ser basada en celdas (ATM), basada en paquetes (Ethernet, Frame Relay, etc.) o híbrida. Esta elección depende de si se tiene ya una red implementada y lo que se desea es migrarla a MPLS o si se trata de una nueva red en la cual se escogerá también la tecnología de capa2. **En nuestro caso elegiremos una basada en paquetes.**

5.1.2 Criterio en la elección del NODO PE

A continuación se menciona 4 consideraciones al elegir un equipo PE:

- El tipo de servicio que será ofrecido. Pueden ser servicios IP y servicios ATM. En nuestro caso se brindará servicios IP.
- Los diferentes tipos de acceso. El *router* deberá de soportar tarjetas de las diferentes tecnologías de acceso como: serial, serial/Frame Relay, E1/T1,

Ethernet, *Fast Ethernet*, *Gigabit Ethernet*, HSSI, ATM, *packet over* SONET/SDH, y entre otras.

El número de líneas de acceso y la concentración de estas líneas. Por ejemplo, un *router* puede soportar 6 *slots* y otro 13 *slots*. En cada *slot* pueden ingresar tarjetas de diferentes tecnologías y con determinados números de puertos. Este punto indicará la capacidad de crecimiento en el acceso a la red.

- Requerimientos de redundancia y capacidad. Otro factor que influye en la elección del PE incluye funcionalidades como OIR (*Online Insertion and Renoval*). Con esta funcionalidad se puede reemplazar una tarjeta sin necesidad de apagar el equipo y por ende afectar los demás servicios que brinda dicho PE.

5.1.3 Criterio en la elección del NODO P

Las principales consideraciones en esta elección son:

- Los diferentes tipos de *troncales* que puede soportar el nodo P.
- El número de *troncales* soportadas.
- El número de conexiones soportadas.
- Requerimientos de redundancia y confidencialidad.

5.2 DISEÑO DE UNA RED MPLS

El diseño de una red MPLS debe de ser considerada antes de la implementación de la red o antes del proceso de migración a MPLS para asegurar que la red funcione de manera confiable y óptima. El tráfico generado por los clientes debe de ser estimado, porque IP es no orientado a conexión entonces el cliente le dirá al proveedor de

servicios el tráfico exacto que enviará. Esto lleva a pensar en el dimensionamiento y escalabilidad de la red.

Se deben de tomar en cuenta los siguientes pasos en el diseño:

- Diseño del POP (*Point-Of-Presence*). Incluye la elección del equipo y las interfaces a usar. La ubicación del POP también es importante, debe ubicarse en un punto de concentración de tráfico.
- Capacidad del enlace del *backbone* MPLS. Incluye los siguientes pasos:
    - Diseño de los puntos de presencia (POPs)
    - Estimación del tráfico de cada POP.
    - Estimación del tráfico unidireccional con la matriz de *routers* en el *backbone*.
    - Estimación del tráfico bi-direccional. Con la matriz.
    - Diseño de la topología del *backbone*.
    - Cálculo estimado del ancho de banda en los enlaces.
    - Asignación de capacidad en el enlace.
    - Ajuste de redundancia.
    - Verificar la selección de los equipos constantemente.
- Diseño del *routing* en la capa 3. MPLS usa protocolos *link-state* como OSPF o IS-IS para determinar las rutas de su tráfico IP. Diseñar el *routing* IP en redes MPLS es similar al diseño de *routing* IP en redes tradicionales.
- Ajustes de diseño en la evolución de la red. Luego que la red MPLS es desarrollada, continuos ajustes de diseños son requeridos para verificar el diseño original. La red también evolucionará con la creación de nuevos POPs

durante el proceso de crecimiento de la red. Se requiere procesos que realicen los siguientes pasos:

- Analizar y medir el tráfico en la red y compararlo con la capacidad de los enlaces.
- Continuamente evolucionar los modelos de tráfico en la red. La distribución de tráfico en el *backbone* MPLS debe de ser constantemente revisada.

- Plan de numeración: Se debe considerar los siguientes planes:
  - Plan de direccionamiento del *backbone*.
  - Plan de direccionamiento de los clientes conectados a los POPs.
  - Plan de numeración de las VPNs de cada cliente.

Una vez que ya se han dado los alcances para el diseño en implementación de una red MPLS, el siguiente paso es el proceso de ejecución de los consideraciones que se han tomado en cuenta en los puntos anteriores.

A continuación se citan tres escenarios que pasaremos a desarrollar.

- Implementación de una red metropolitana MPLS con servicios diferenciados.
- Implementación de una red MPLS con ingeniería de tráfico, modo normal.
- Implementación de una red MPLS con ingeniería de tráfico, modo protección.
- Implementación de una red MPLS con ingeniería de tráfico y calidad de servicio.

5.3 IMPLEMENTACIÓN DE UNA RED METROPOLITANA MPLS CON SERVICIOS DIFERENCIADOS.

Basándonos en los puntos anteriores diseñaremos una red de acuerdo a lo que se expone en la figura 5.1. Se desea implementar una red MPLS con topología estrella en la cual el *router* de núcleo (P) conecte y distribuya las rutas a todos los *routers* de borde (PE). Se trata de una implementación simple, en la cual no se necesita crear túneles pues el punto intermedio de paso siempre será el núcleo central P y no existirá otra ruta alternativa entre un *router* de ingreso (PE) y otro.

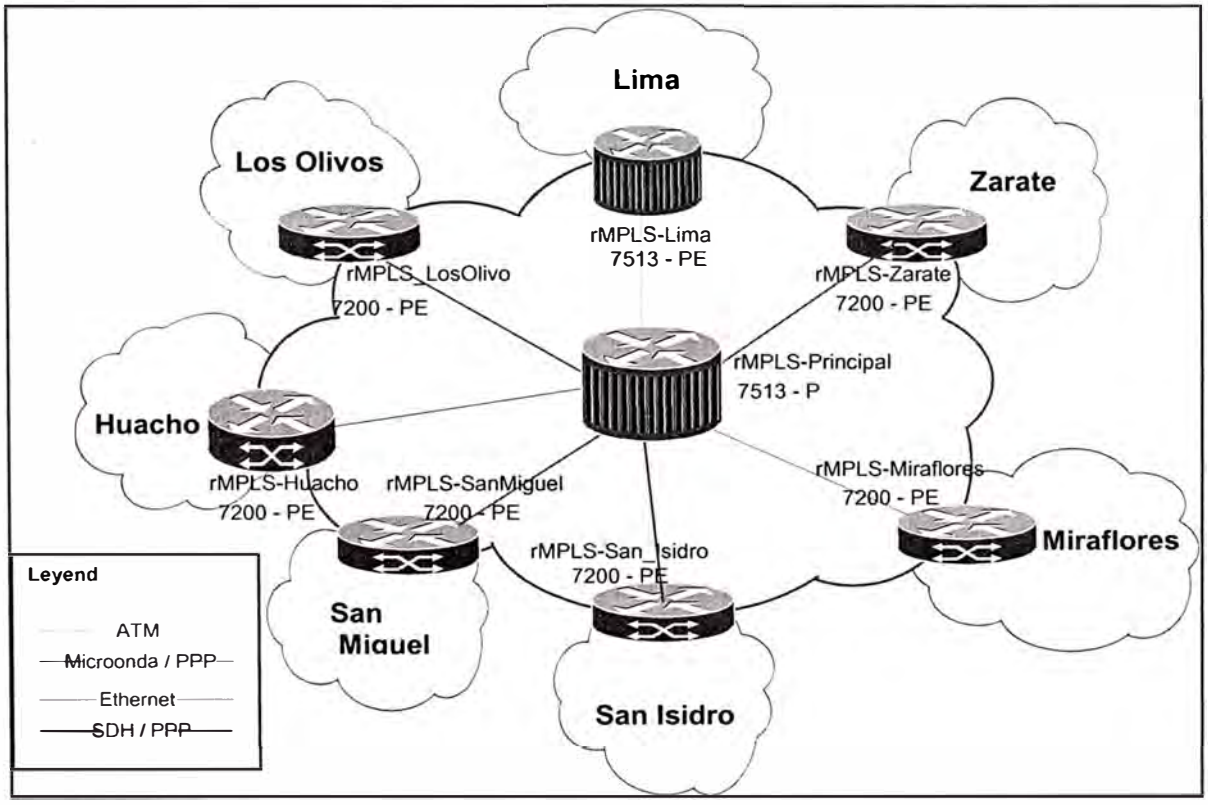


Figura 5.1: Topología de una red Metropolitana MPLS.

Asumiremos que se trata de una red metropolitana y cada nodo PE esta distribuido en las zonas más importantes de la ciudad de Lima. El *router* principal del núcleo (P)

tendrá enlaces con cada uno de los *routers* PE con diferentes tecnologías de interconexión.

5.3.1 Implementación de las tecnologías de acceso y del equipamiento a utilizar

En la tabla 5.1 se muestra los criterios de diseño sobre los *routers* PEs y el nodo P.

Nombre del Nodo	Troncal hacia el nodo P	Tipo de Router	Servicios de Acceso	Tecnología de Acceso	Redundancia de Troncal
Principal	----	7513 - P			
Huacho	Microondas / PPP	7200VXR -PE	IP	Serial PPP / Serial FR / Ethernet	NO
Lima	ATM	7513 - P	IP	Serial PPP / Serial FR / Ethernet	NO
Los Olivos	SDH/ E1 / PPP	7200VXR -PE	IP	Serial PPP / Serial FR / Ethernet	NO
Miraflores	SDH/ E1 / PPP	7200VXR -PE	IP	Serial PPP / Serial FR / Ethernet	NO
San Isidro	SDH/ E1 / PPP	7200VXR -PE	IP	Serial PPP / Serial FR / Ethernet	NO
San Miguel	SDH/ E1 / PPP	7200VXR -PE	IP	Serial PPP / Serial FR / Ethernet	NO
Zarate	Fast Ethernet	7200VXR -PE	IP	Serial PPP / Serial FR / Ethernet	NO

Tabla 5.1. Detalle de los servicios brindados por los routers PEs.

La elección del nodo PE es una tarea muy importante. Como se muestra en la tabla 5.1, se utilizarán *routers* cisco 7200VXR como *routers* PEs, a excepción de Lima que usará un 7513. El *router* de núcleo será un cisco 7513.

Los *routers* PE 7200VXR tendrán las siguientes características:

- Sistema operativo: IOS Cisco 12.3(10) *Service Provider Vip.*
- Procesador del *router*: procesador NPE400
- Cantidad de memoria: 512 Mb de memoria RAM / 64 Mb de memoria Flash.
- Tarjetas: 8 interfaces E1, 8 interfaces seriales y 2 puertos Fast Ethernet.

Los *routers* P 7513 tendrá las siguientes características:

- Sistema operativo: IOS Cisco 12.3(10) *Service Provider Vip.*
- Procesador del *router*: procesador RSP4+

- Cantidad de memoria: 256 Mb de memoria RAM / 128 Mb de memoria Flash.
- Tarjetas: 24 interfaces E1, 2 interfaces ATM, 8 interfaces seriales y 4 puertos Fast Ethernet.

5.3.2 Elección del protocolo de *routing* para el *backbone* MPLS.

Por lo general se utiliza el protocolo BGP. En nuestro caso usaremos, también, BGP. Por tratarse de una topología estrella se aprovechará la funcionalidad de BGP llamada *router-reflector*. Su habilitación permite que el *router* P reciba las rutas de un nodo PE específico y lo distribuya automáticamente a todos los demás nodos PEs, es decir, todos los *routers* PEs tendrán en su tabla de *routing* las redes de los otros PEs respetando las diferentes VPNs creadas.

Para nuestro caso definiremos el sistema autónomo número 20005 a ser usado por BGP. El plan de numeración es como se muestra en la tabla 5.2

Nombre del Nodo	Dirección IP WAN	Mascara de Red	Dirección IP Loopback	Mascara de Red
Huacho	200.62.188.42	255.255.255.252	200.62.188.8	255.255.255.255
Lima	200.62.188.34	255.255.255.252	200.62.188.2	255.255.255.255
Los Olivos	200.62.188.70	255.255.255.252	200.62.188.5	255.255.255.255
Miraflores	200.62.188.102	255.255.255.252	200.62.188.9	255.255.255.255
San Isidro	200.62.188.66	255.255.255.252	200.62.188.4	255.255.255.255
San Miguel	00.62.188.98	255.255.255.252	200.62.188.7	255.255.255.255
Zarate	200.62.188.74	255.255.255.252	200.62.188.6	255.255.255.255

Tabla 5.2: Direccionamiento IP en los nodos PE

5.3.3 Elección del protocolo de *routing* para transportar las rutas de los clientes.

Como se trata de una topología estrella y no hay necesidad de la creación de túneles se elegirá la configuración por rutas estáticas.

5.3.4 Configuración del *router* PE

En primer lugar se define el protocolo de interconexión. Para el caso de Los Olivos las interfaces son E1 a través de un enlace SDH. Se implementará *MultiLink* PPP en las interfaces E1 del PE de Los Olivos y del nodo P para habilitar dicho enlace.

Para levantar las *troncales* desde el *router* P a los *routers* PEs es necesario configurar lo siguiente:

Configuración en el *router* PE (ejemplo, rMPLS-LosOlivos)

```
! configuración en el router Los Olivos
card type e1 6
ip cef
no tag-switching ip propagate-ttl
tag-switching tdp router-id Loopback0
frame-relay switching
!
interface Loopback0
 description Loopback BB MPLS
 ip address 200.62.188.5 255.255.255.255
 no clns route-cache
!
controller E1 6/0
 clock source internal
 channel-group 0 timeslots 1-31
 description LosOlivos- E1 SDH >> rMpls_Principal controller
4/0/4
! configuración de la interface virtual MultiLink.
interface Multilink1
 description LosOlivos- E1 SDH >> rMpls_Principal controller
4/0/4
 ip address 200.62.188.70 255.255.255.252
 load-interval 30
 ntp broadcast
 tag-switching mtu 1508
 tag-switching ip
 ppp multilink
 ppp multilink fragment disable
 ppp multilink group 1
 no clns route-cache
!
! Asociación de la interface controller con la interface serial
y esta a su vez con !la interface Multilink PPP.
interface Serial6/0:0
 description LosOlivos- E1 SDH >> rMpls_Principal controller
4/0/4
 no ip address
 encapsulation ppp
 load-interval 30
 no fair-queue
```

```
 ppp multilink
 ppp multilink group 1
 no clns route-cache
!
! Configuración de la sesión BGP con funcionalidad router
! reflector
router bgp 20005
 no synchronization
 bgp log-neighbor-changes
 redistribute static
 neighbor Client-rr peer-group
 neighbor Client-rr remote-as 20005
 neighbor Client-rr update-source Loopback0
 neighbor Client-rr next-hop-self
 neighbor Client-rr send-community both
 neighbor Client-rr soft-reconfiguration inbound
 neighbor 200.62.188.1 peer-group Client-rr
 no auto-summary
```

En los demás *routers* PE se tendrá que repetir la configuración implementada en Los Olivos de tal manera de tener todos los enlaces activos.

5.3.5 Configuración del router P

La configuración de este *router* se hace tomando en cuenta que las interfaces que son usadas como *troncales* son interfaces E1.

```
! router rMPLS_Principal
card type e1 4 0                ← definiendo el tipo de tarjeta
ip cef distributed              ← siempre debe de estar activo
no tag-switching ip propagate-ttl
tag-switching tdp router-id Loopback0

interface Loopback0
 description Source for BGP, and MPLS
 ip address 200.62.188.1 255.255.255.255
 no clns route-cache

controller E1 4/0/4
 channel-group 0 timeslots 1-31
 description Enlace a Olivos - E1 SDH >> controller E1 6/0
!
interface Serial4/0/4:0
 description Enlace a Olivos - E1 SDH >> controller E1 6/0
 no ip address
 encapsulation ppp              ← tipo de encapsulacion capa2
 load-interval 30
 tx-queue-limit 26
 ppp multilink                  ← uso de eficiencia del enlace
 ppp multilink group 3
```

```
 no clns route-cache
!
interface Multilink3
 description Enlace a Olivos - E1 SDH >> controller E1 6/0
 ip address 200.62.188.69 255.255.255.252
 load-interval 30
 ntp broadcast
 tag-switching mtu 1508
 tag-switching ip
 ppp multilink
 ppp multilink fragment disable
 ppp multilink group 3
 no clns route-cache
!
! Creación de la sesión BGP con funcionalidad de router
reflector
router bgp 20005
 no synchronization
 bgp log-neighbor-changes
 neighbor Client-rr peer-group
 neighbor Client-rr remote-as 20005
 neighbor Client-rr update-source Loopback0
 neighbor Client-rr route-reflector-client
 neighbor Client-rr next-hop-self
 neighbor Client-rr send-community both
 neighbor Client-rr soft-reconfiguration inbound
 neighbor 200.62.188.2 peer-group Client-rr
 neighbor 200.62.188.4 peer-group Client-rr
 neighbor 200.62.188.5 peer-group Client-rr
 neighbor 200.62.188.6 peer-group Client-rr
 neighbor 200.62.188.7 peer-group Client-rr
 neighbor 200.62.188.8 peer-group Client-rr
 neighbor 200.62.188.9 peer-group Client-rr
no auto-summary
!
address-family vpnv4
 neighbor Client-rr activate
 neighbor Client-rr route-reflector-client
 neighbor Client-rr next-hop-self
 neighbor Client-rr send-community both
 neighbor 200.62.188.2 peer-group Client-rr
 neighbor 200.62.188.4 peer-group Client-rr
 neighbor 200.62.188.5 peer-group Client-rr
 neighbor 200.62.188.6 peer-group Client-rr
 neighbor 200.62.188.7 peer-group Client-rr
 neighbor 200.62.188.8 peer-group Client-rr
 neighbor 200.62.188.9 peer-group Client-rr
exit-address-family
!
ip classless
```

Comprobación de la activación del enlace

Si aplicamos el comando “show ip bgp summary” en Los Olivos se tendrá:

```
rMPLS_Principal#sh ip bgp summary
...
Neighbor        V AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
200.62.188.5    4 20005  202103  255549       12    0    0 2d17h           0
```

Si aplicamos "*sh ip bgp sumary*" en rMPLS-Los-Olivos se obtendrá:

```
PE_LosOlivos#sh ip bgp summary

Neighbor        V AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
200.62.188.1    4 20005    5577    4086        4    0    0 2d18h           1
```

Para concluir la prueba, una prueba de ping será necesaria.

```
rMPLS_Principal#ping 200.62.188.5
!!!!
successfull (100/100%)
```

Con estas salidas se comprueba la habilitación de la troncal entre el *router* P y el PE.

En los demás *routers* se implementará de manera similar a la realizada en el POP Los Olivos.

Finalmente el *router* P (rMPLS_Principal) tendrá la siguiente tabla de sesiones BGP:

```
rMPLS_Principal#sh ip bgp summary
Neighbor        V AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
200.62.188.2    4 20005  201655  257553       12    0    0 19w2d           1
200.62.188.4    4 20005  201707  255653       12    0    0 2d19h           0
200.62.188.5    4 20005  202103  255549       12    0    0 2d17h           0
200.62.188.6    4 20005  201456  254635       12    0    0 11w0d           0
200.62.188.7    4 20005  201415  254558       12    0    0 12w5d           0
200.62.188.8    4 20005  250936  256562       12    0    0 19w6d           1
200.62.188.9    4 20005  201849  255700       12    0    0 5w5d            0
200.62.188.10   4 20005  190299  242835       12    0    0 18w6d           0
200.62.188.11   4 20005  118717  165612       12    0    0 1w5d            1
rMPLS_Principal#
```

3.5.6 Implementación de las VPNs de los clientes.

Según la figura 5.2 se describen dos VPNs: VPN1 para el cliente *Bank* y VPN2 asignada al cliente *Market*. Se observa que el cliente *Bank* tiene presencia en todos los POPs mientras que el cliente *Market* solo está presente en tres POPs.

Se asigna en VPN1 el número de VRF de 00123 y en la VPN2 el número de VRF 00124.

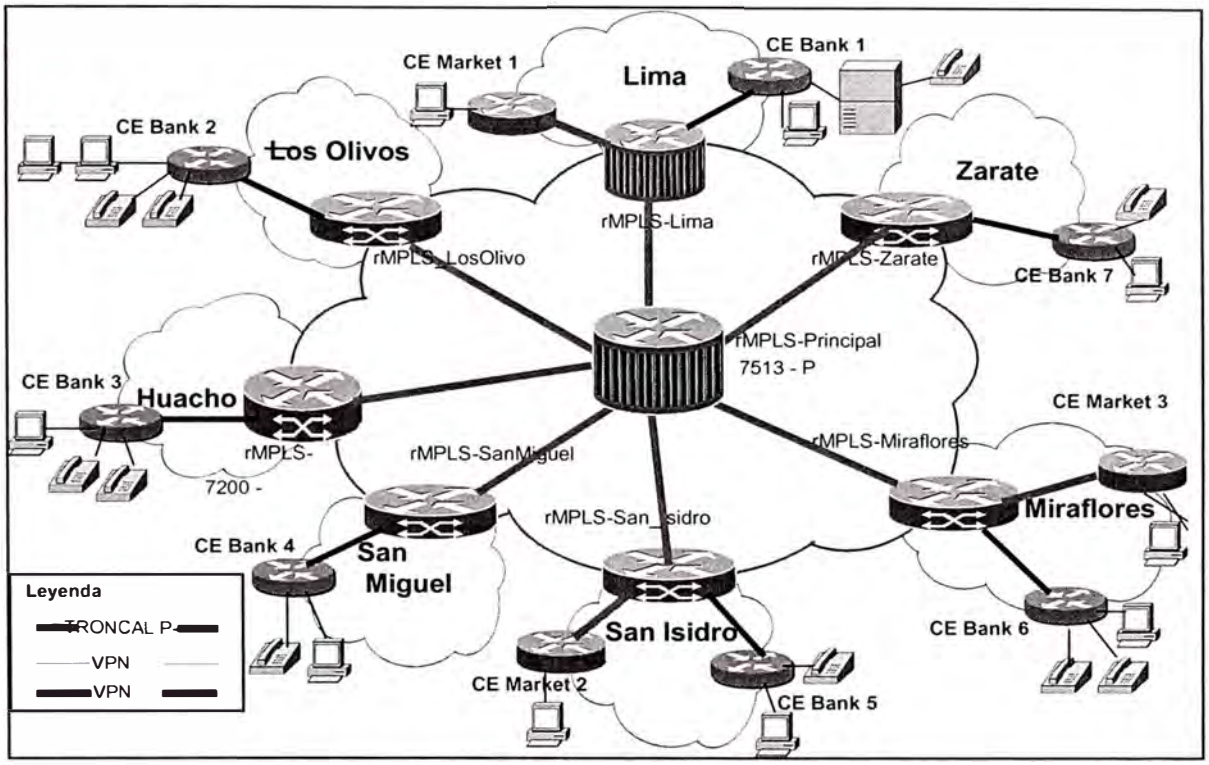


Figura 5.2. Muestra dos VPNs creadas, cada VPN corresponde a un cliente.

De acuerdo a la figura superior, se expondrá las configuraciones en dos POPs, en los demás POPs se configurará de manera similar. En el nodo PE no es necesario configurar nada adicional, las rutas son reflejadas mediante la funcionalidad de BGP usada, "*router-reflector*".

En la tabla 5.3 se muestra el detalle del plan de numeración de las sedes del cliente *BANK*:

Sede del cliente Bank en:	Dirección IP WAN	Mascara de Red	Dirección IP LAN	Mascara de Red
Huacho	10.225.16.226	255.255.255.252	172.22.16.0	255.255.255.0
Lima	10.225.8.34	255.255.255.252	172.22.9.17	255.255.255.0
Los Olivos	10.225.4.26	255.255.255.252	172.22.16.0	255.255.255.0
Miraflores	10.225.20.26	255.255.255.252	172.22.20.0	255.255.255.0
San Isidro	10.225.0.42	255.255.255.252	172.22.18.0	255.255.255.0
San Miguel	10.225.8.22	255.255.255.252	172.22.19.0	255.255.255.0
Zarate	10.225.12.22	255.255.255.252	172.22.17.0	255.255.255.0

Tabla 5.3. Detalle del plan de numeración del cliente BANK.

Configuración en el *router* rMPLS_Los-Olivos

```
! creación de VPN
ip vrf 00123
 description Bank
 rd 20005:123
 export map Loopback
 route-target export 20005:1000000123
 route-target import 20005:1000000123
 route-target import 20005:1100000001
!
router bgp 20005
.....
address-family ipv4 vrf 00123
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
! Adición del protocolo IGP, es este caso ruta estática
ip route vrf 00123 172.22.16.0 255.255.255.0 10.225.4.26
```

Comprobación de las rutas aprendidas dentro de la VPN desde el PE de Los Olivos:

```
PE_Los-Olivos#sh ip route vrf 00123
Routing Table: 00123
B       172.22.9.0/24 [200/0] via 200.62.188.2, 2d18h
B       172.22.18.0/24 [200/0] via 200.62.188.4, 2d18h
B       172.22.19.0/24 [200/0] via 200.62.188.7, 2d18h
S       172.22.16.0/24 [1/0] via 10.225.4.26
B       172.22.17.0/24 [200/0] via 200.62.188.6, 1d03h
B*   0.0.0.0/0 [200/0] via 200.62.188.2, 2d18h
```

Configuración en el PE *router* rMPLS_SanIsidro

```
ip vrf 00123
 description Bank
 rd 20005:123
 export map Loopback
 route-target export 20005:1000000123
 route-target import 20005:1000000123
 route-target import 20005:1100000001
!
router bgp 20005
address-family ipv4 vrf 00123
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
!publicación de la red LAN a las demás sedes
ip route vrf 00123 172.22.18.0 255.255.255.0 10.225.0.42
```

Comprobación de las rutas aprendidas dentro de la VPN desde el PE de San Isidro:

```
rMPLS_San-Isidro#sh ip route vrf 00123

B        172.22.15.0/24 [200/0] via 200.62.188.8, 2d19h
B        172.22.19.0/24 [200/0] via 200.62.188.7, 2d19h
B        172.22.16.0/24 [200/0] via 200.62.188.5, 2d12h
B        172.22.17.0/24 [200/0] via 200.62.188.6, 1d03h
B        10.225.8.20/30 [200/0] via 200.62.188.7, 2d19h
B        10.225.4.24/30 [200/0] via 200.62.188.5, 2d12h
B        200.62.131.240 [200/0] via 200.62.188.2, 2d19h
B*    0.0.0.0/0 [200/0] via 200.62.188.2, 2d19h
```

Configuración en el *router* rMPLS_Lima (*ruta default de las demás sedes*)

```
ip cef distributed
ip vrf 00123
 description Bank
 rd 20005:123
 route-target export 20005:1000000123
 route-target import 20005:1000000123
tag-switching tdp router-id Loopback0
no tag-switching ip propagate-ttl
!
! Interface que será conocida por los demás neighbors BGP
interface Loopback0
 description Loopback BB MPLS
 ip address 200.62.188.2 255.255.255.255
!
! Interface que da cara al router P
interface ATM9/1/0.102 point-to-point
 description Enlace router P
 ip address 200.62.188.34 255.255.255.252
 pvc PE-P 100/500
  abr 13208 13208
  oam-pvc manage
  encapsulation aal5snap
 !
router bgp 20005
.....
 !
 address-family ipv4 vrf 00123
 redistribute connected
 redistribute static
 !!! Publicación de la ruta default a las demás sedes
 default-information originate
 no auto-summary
 no synchronization
 exit-address-family
 !
```

3.5.7 Implementación de QoS sobre la VPN del cliente *BANK*.

Para iniciar esta parte de la configuración es necesario conocer la distribución de tráfico de cada sede remota, es decir, el ancho de banda contratado y el ancho de banda a priorizar. La tabla 5.4 muestra los anchos de banda de cada sede del cliente *Bank* y a su vez los requerimientos de ancho de banda de alta prioridad y de media prioridad.

Sede del cliente *Bank* en:	Ancho de Banda	Canales de VOZ	Alta Prioridad (P3) (Kbps)	Media Prioridad (P2) (Kbps)
Huacho	256 Kbps	4	88	100
Lima	1.5 Mbps	24	528	600
Los Olivos	256 Kbps	4	88	100
Miraflores	256 Kbps	4	88	100
San Isidro	256 Kbps	4	88	100
San Miguel	256 Kbps	4	88	100
Zarate	256 Kbps	4	88	100

Tabla 5.4 Muestra la distribución de prioridad de ancho de banda.

Como se ha definido Lima como sede principal de la red del cliente, entonces empezaremos a configurar la calidad de servicio en el *router* rMPLS_Lima.

Clasificación y marcado de paquetes

Se definen 3 clases de servicio

- Prioridad P1, tráfico que no requiere exigencias en QoS (http, mail, etc.).
- Prioridad P2, tráfico sensible a retardos (SAP, SNA, etc.)
- Prioridad P3, tráfico de tiempo real que requiere alta QoS (Multimedia, VoIP, video conferencia, etc.)

Se asume que los paquetes ya llegan marcados a la red MPLS, de no ser así se debe de marcar el campo DSCP del paquete que ingresa a la red. En este caso aplicaremos el marcado, clasificación y aplicación de QoS en el *router* de acceso.

Configuración de QoS en el *router* PE de acceso principal, rMPLS Lima:

```
  Clasificación y marcado de paquetes
 !!
  Clasificación en clases de servicio
class-map match-all Trafico-P3
  match ip dscp cs3
class-map match-all Trafico-P2
  match ip dscp cs2
class-map match-all Trafico-P1
  match ip dscp cs2
!!!
! Definiendo la política de entrada para marcado de paquetes
policy-map police_Bank-Lima
  class Trafico-P3
    police 528000 conform-action transmit exceed-action drop
  class Trafico-P2
    police 600000 conform-action transmit exceed-action set-
dscp-transmit cs1
  class class-default
    police 408000 conform-action transmit exceed-action
transmit
!!!
! Definiendo la política de salida para manejo de congestión
policy-map Bank-Lima_QoS_1536
  class Trafico-P3
    priority 528
  class Trafico-P2
   bandwidth 600
  class class-default
   bandwidth 408
 !!
  Aplicación de las políticas en la interface del cliente.
  La sede Lima es la sede principal.
  El ancho de banda a configurar debe de ser la suma de las
  sedes remotas.
interface ATM9/1/0.142 point-to-point
 description Bank-Lima >> Sedes Remotas
 ip vrf forwarding 00123
 ip address 10.225.8.33 255.255.255.252
 atm route-bridged ip
 pvc Bank-Lima 0/142
  vbr-rt 2641
  tx-ring-limit 10
  encapsulation aal5snap
    service-policy input police_Bank-Lima
    service-policy output Bank-Lima_QoS 1536
```

Configuración de QoS en el *router* PE de acceso remoto, rMPLS_Los-Olivos:

De igual manera se configurara en cada uno de los *routers* de acceso remoto. En este caso tomaremos como ejemplo rMPLS_Los-Olivos.

```
! Clasificación y marcado de paquetes
!!!
! Clasificación en clases de servicio
class-map match-all Trafico-P3
  match ip dscp cs3
class-map match-all Trafico-P2
  match ip dscp cs2
class-map match-all Trafico-P1
  match ip dscp cs2
!!!
!Definiendo la política de entrada para marcado de paquetes
policy-map police_Bank-Los-Olivos
  class Trafico-P3
    police 88000 conform-action transmit exceed-action drop
  class Trafico-P2
    police 100000 conform-action transmit exceed-action set-
dscp-transmit cs1
  class class-default
    police 68000 conform-action transmit exceed-action transmit
!!!
!Definiendo la política de salida para manejo de congestión
policy-map Bank-Los-Olivos_QoS_256
  class Trafico-P3
    priority 88
  class Trafico-P2
   bandwidth 100
  class class-default
   bandwidth 68
!!!
! Aplicación de las políticas en la interface del cliente.
! La sede Los Olivos es una sede remota.
! El ancho de banda a configurar debe de ser la suma de las
! sedes remotas (256 Kbps).
interface FastEthernet0/0
 description CPE Bank-LosOlivos
 ip vrf forwarding 00123
 ip address 10.225.4.25 255.255.255.252
 duplex full
 speed 100
 no clns route-cache
 service-policy input police_Bank-Los-Olivos
 service-policy output Bank-Los-Olivos_QoS_256
```

A continuación expondremos casos de configuraciones con aplicaciones MPLS-TE y MPLS-DS-TE y MPLS-TE-QoS

5.4 IMPLEMENTACIÓN: MPLS-TE NE MODO NORMAL

Implementando túneles de acuerdo a lo mostrado en la figura 5.3.

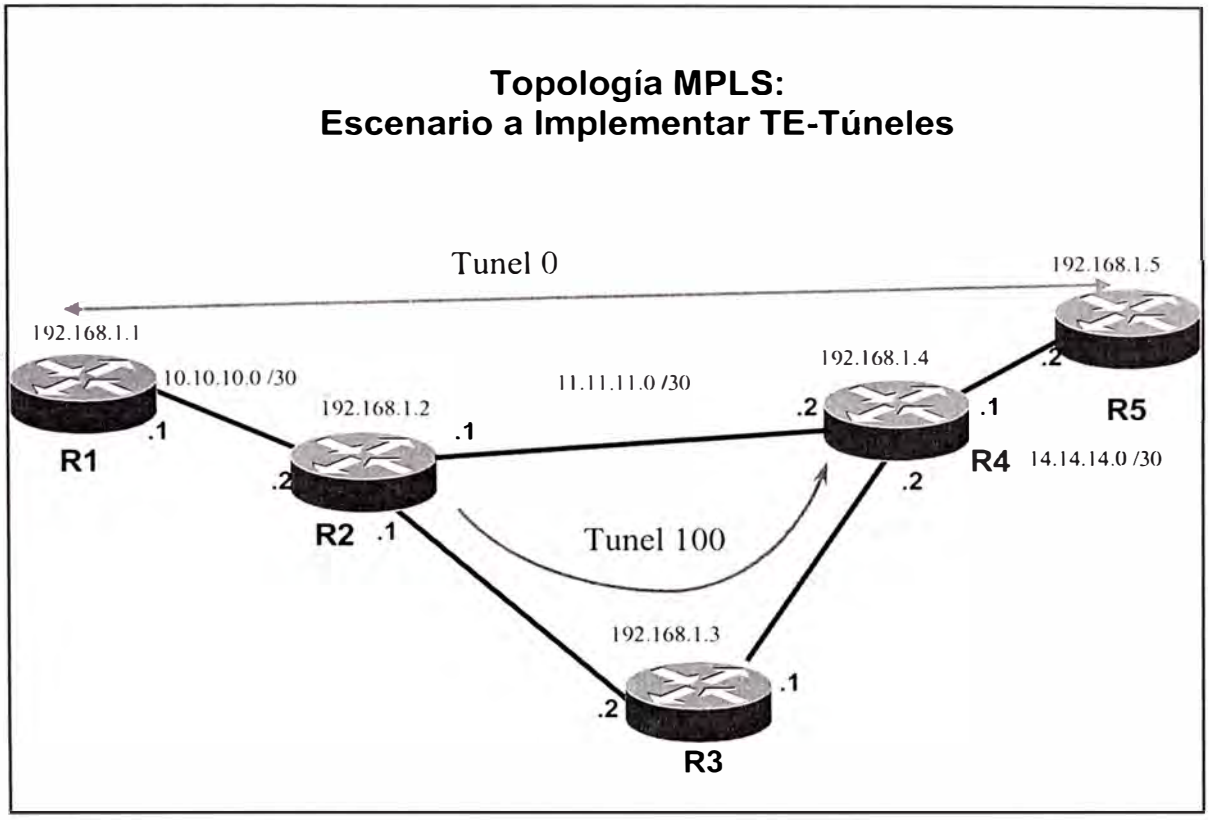


Figura 5.3: Topología de una red MPLS con túneles TE. Operación normal.

Antes de comenzar con la configuración de los túneles TE, debemos asegurarnos que todos los *routers* en el dominio soporten MPLS, RSVP-TE y un protocolo de *routing* IGP que puede ser IS-IS o OSPF con extensiones TE.

En estas configuraciones se asume que todos los *routers* participantes pertenecen a una simple área o dominio que concierne al protocolo IGP. Hay implementaciones que se pueden realizar con *routers* que pertenecen a diferentes áreas.

5.4.1 Requerimientos básicos para configurar TE:

Activación del CEF (*Cisco Express Forwarding*).

Los *peers* IGP deben apuntar a las interfaces *loopback* de los *routers*.

- Túnel siempre debe ser unidireccional

Asumiremos el uso del protocolo IS-IS. La implementación con OSPF es muy similar y solo requiere pocos cambios.

5.4.2 Estableciendo el Túnel 0 entre el *router*s: R1 - R5.

```
!!!...configuración en R1:
mpls traffic-eng tunnels
!
interface loopback0
  ip address 192.168.1.1 255.255.255.255
  ip router isis
!
interface R1-R2
  ip address 10.10.10.1 255.255.255.252
  ip router isis
  !!! … habilitando el tunnel TE
  mpls traffic-eng tunnels
  !!!.. habilitando RSVP en un sentido
  ip rsvp bandwidth 100000 100000
!
!!!
! creando el proceso IS-IS en el router
router isis
  metric style wide
  mpls traffic-eng level-2
  mpls traffic-eng router-id loopback0
```

5.4.3 Configuración del túnel: R1 - R5

Usaremos una ruta dinámica, la mayor ruta encontrada por el algoritmo CBR. También se puede configurar rutas explicitas. El identificador del *router* y la interface deben ser especificados.

```
interface tunnel0
  ip unnumbered loopback0
  no ip direct-broadcast
  tunnel destination 192.168.1.5
  tunnel mode mpls traffic-eng
!!!.. anuncia al peer remoto que puede pasar tráfico por este
!!! túnel
  tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng bandwidth 100
  tunnel mpls traffic-eng priority 1 1
!!!... Define como se calcula la ruta
  tunnel mpls traffic-eng path-option 1 dynamic
  tunnel mpls traffic-eng record-route
```

5.4.4 Configuración del *router* intermedio: R2

```
ip cef
mpls traffic-eng tunnels

interface loopback0
  ip address 192.168.1.2 255.255.255.255
  ip router isis

interface R2-R1
  ip address 10.10.10.2 255.255.255.252
  ip router isis
  mpls traffic-eng tunnels
  ip rsvp bandwidth 1000 1000

 interface R2-R4
   ip address 11.11.11.1 255.255.255.252
   ip router isis
   mpls traffic-eng tunnels
   ip rsvp bandwidth 100000 100000

!!!…habilitando el túnel TE en las interfaces
interface R2-R3
  ip address 12.12.12.1 255.255.255.252
  ip router isis
  mpls traffic-eng tunnels
  ip rsvp bandwidth 100000 100000
router isis
 metric style wide
 mpls traffic-eng level-2
 mpls traffic-eng router-id loopback0
```

5.4.5 Configuración en el *router peer* remoto (R5).

Debe tener la misma configuración que el *router* intermedio.

```
ip cef
mpls traffic-eng tunnels

interface loopback0
  ip address 192.168.1.5 255.255.255.255
  ip router isis

interface R5-R4
  ip address 14.14.14.2 255.255.255.252

ip router isis
  mpls traffic-eng tunnels
  ip rsvp bandwidth 100000 100000
  metric style wide
  mpls traffic-eng level-2
  mpls traffic-eng router-id loopback0
```

Con esta configuración el túnel debería de estar operativo.

5.4.6 Asignación de tráfico al túnel

Para habilitar la asignación de tráfico a este túnel o configurar rutas cstáticas para alcanzar algún destino detrás del *router* remoto R5, usaremos el comando "*tunnel mpls traffic-eng autoroute announce*".

5.4.7 Verificación de funcionamiento del túnel TE

Los siguientes comandos pueden ser utilizados para comprobar que el tráfico esta siendo ruteado por este túnel.

```
show mpls traffic-eng tunnel
show ip route 192.168.1.5
show mpls traffic-eng autoroute
ping 192.168.1.5
show interface tunnel0 accounting
show interface r1-r2 accounting
```

5.4.8 Creación de una ruta explicita de R1 a R5

Para crear una ruta explicita de R1 a R5, la configuración en el *router* R5 debe de ser ligeramente cambiada.

```
! Definiendo la ruta explicita
ip explicit-path identifier-explicit-path-name
  next-address 10.10.10.2
  next-address 11.11.11.2
  next-address 14.14.14.2

!sobre la interface tunnel 0 se adhiere:
tunnel mpls traffic-eng path-option 1 explicit name identifier-
explicit-path-name
```

Nota: Para cada LSP, una ruta explicita o dinámica puede ser especificada simultáneamente. El *router* escogerá la mejor ruta.

5.5 IMPLEMENTACIÓN: MPLS-TE EN MODO PROTECCIÓN

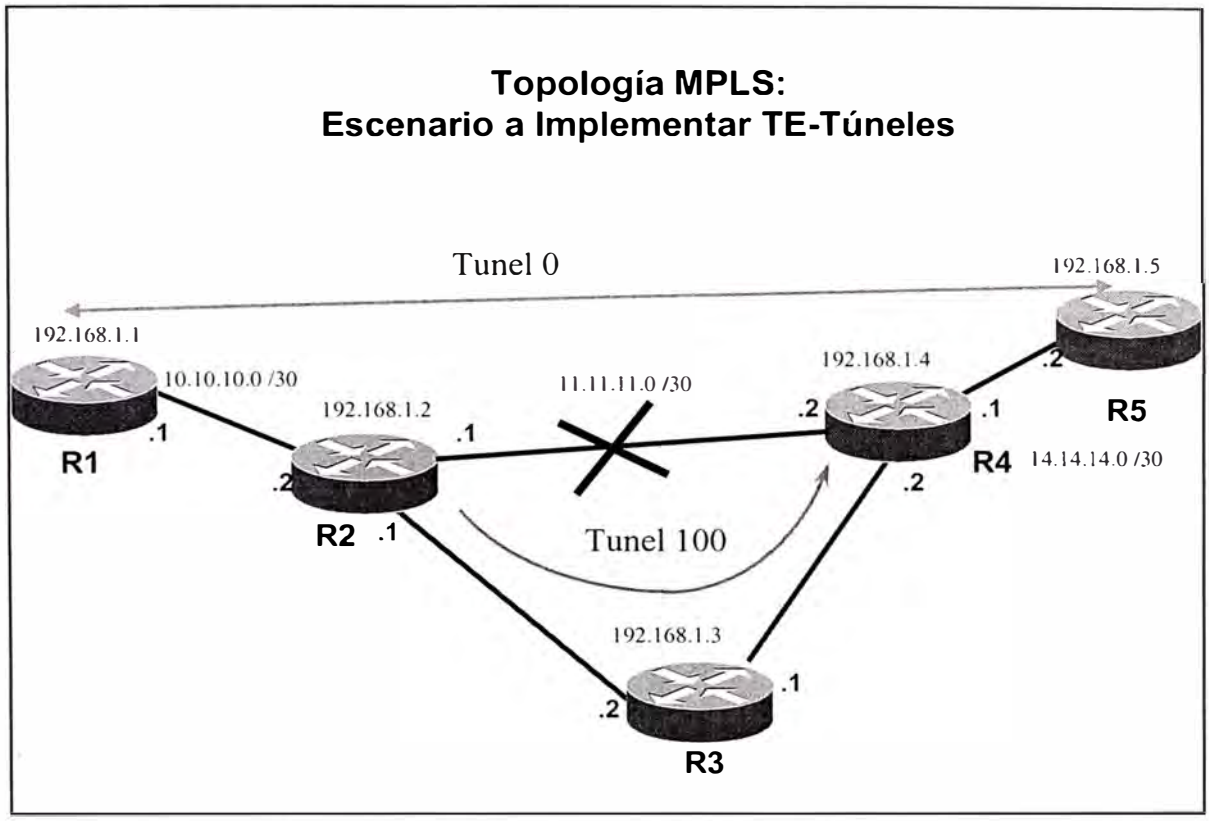


Figura 5.5: Topología de una red MPLS con túneles TE. Operación con falla.

Como se muestra en la figura 5.5, asumamos que la ruta principal es el LSP R1-R2-R4-R5. Se desea proteger el enlace entre R2 y R4 con una ruta backup R2-R3-R4, vía el Túnel 100.

Algo muy importante que resaltar es que solamente las interfaces POS soportan Fast Re-route.

5.5.1 Construcción de la ruta *backup*: R2-R4 a través de R3.

```
!!!...configurando la ruta backup en R2
interface tunnel100
  ip unnumbered loopback0
  mpls traffic-eng tunnels
  tunnel destination 13.13.13.2
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng priority 0 0
  tunnel mpls traffic-eng path-option 1 explicit backup-
tunnel1000
```

```
  ip rsvp bandwidth 1 1
!
ip explicit-path backup-tunnel100
  next address 12.12.12.2
  next address 13.13.13.2
! Configuración de protección del enlace en R2: Protección del
! enlace es solo soportado por interfaces POS.
interface R2-R4
  ip address 11.11.11.1
  mpls traffic-eng tunnels
  mpls traffic-eng backup tunnel100
  pos ais-shut                        <-- se asume interface POS
  pos report lrdi                     <-- se asume interface POS
  ip rsvp bandwidth 2480000 2480000
```

En el *router* R1, el túnel 1 debe saber que tiene un túnel backup listo para ser tomado en caso de falla. Esto configurará la bandera local de protección de enlace a 0x01 entonces el *router* R1 será señalado como túnel1 del LSP.

5.5.2 Activando *fast re-routing*

Sobre la "interface Tunnel0" se adhiere "*tunnel mpls traffic-eng fast-reroute*"

```
interface tunnel0
  ip unnumbered loopback0
  no ip direct-broadcast
  tunnel destination 192.168.1.5
  tunnel mode mpls traffic-eng
  !!!.. anuncia al peer remoto R5 que puede pasar tráfico por
  !!! este túnel
  tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng bandwidth 100
  tunnel mpls traffic-eng priority 1 1
  !!!... define como se calcula la ruta
  tunnel mpls traffic-eng path-option 1 dynamic
  tunnel mpls traffic-eng record-route
  tunnel mpls traffic-eng fast-reroute
```

5.6 IMPLEMENTACIÓN: MPLS-TE + QoS

Se desea implementar calidad de servicios con servicios diferenciados (*DiffServ*) sobre la arquitectura MPLS que se muestra en la Figura 5.6.

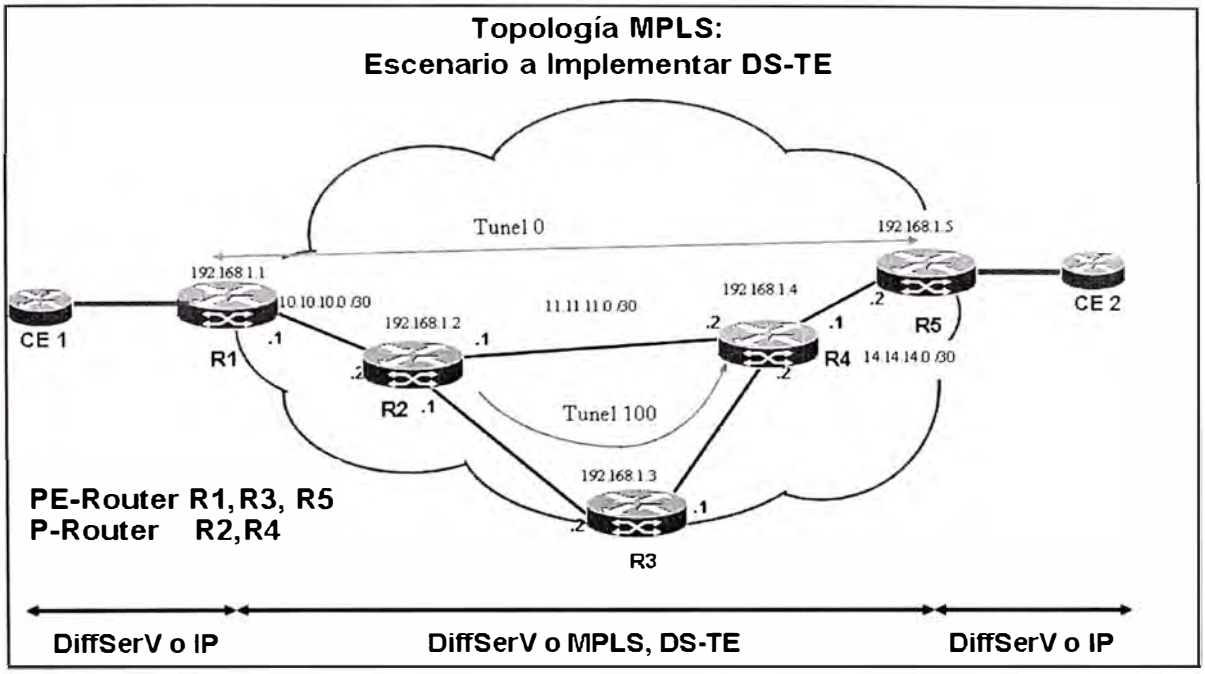


Figura 5.6: Ejemplo de implementación MPLS-TE + QoS

La solución más fácil y natural, cuando un limitado número de clases son creadas, es marcar directamente el campo EXP, de la etiqueta MPLS, con el valor de DSCP del paquete IPv4 que ingresa a la red MPLS a través del *router* PE. En el *router* de egreso PE de la red MPLS, se retira la etiqueta y con esto se asegura que *DiffServ* sea aplicado en toda la ruta.

5.6.1 Asignando *DiffServ* al campo EXP.

En el *router* de ingreso.

- Se marca y aplica la política de tráfico de acuerdo a lo contratado.
- Se define el IP Precedente / DSCP y se asocia al campo Exp de MPLS.

```
class-map match-all DATOS-P3
  match ip dscp ef
class-map match-all DATOS-P1
  match ip dscp af31 af32 af33
!
policy-map IN-POLICY
  class DATOS-P3
```

```
    police 1280000 32000 32000 onform-action set-mpls-exp-
transmit 5 exceed-action drop
  class DATOSP-1
    police 22000000 550000 550000 conform-action set-mpls-exp-
transmit 4 exceed-action set-mpls-exp-transmit 3
  class default
    set mpls experimental 0
```

La política IN-POLICY debe ser aplicada en la interface de entrada a la red MPLS.

La interface de salida del paquete da cara a la red MPLS:

• El tráfico es clasificado de acuerdo al campo EXP.

• LLQ (MDDR) para encolamiento de paquetes MPLS

• WRED basado en EXP para implementar precedencia de descartar paquetes.

• IP *Precedence* es copiado a MPLS EXP si no se define otra acción en la política.

La política OUT-POLICY es aplicada en la interface de salida (interface que da cara al núcleo MPLS).

En la nube MPLS, para los *routers* P:

• Servicio de Tráfico basado en el marcado campo EXP.

• LLQ (MDRR) para paquetes MPLS.

• WRED basado en EXP

```
!Se define grupos de colas CoS,"OUT-POLICY"
cos-queue-group OUT-POLICY
  precedence 0 queue 0
  precedence 3 queue 1
  precedence 4 queue 1
  precedence 5 queue low-latency
  precedence 0 random-detect-label 0
  precedence 3 random-detect-label 1
  precedence 4 random-detect-label 2
  random-detect-label 0 300 500 1
  random-detect-label 1 100 300 1
  random-detect-label 2 300 500 1
  queue 0 50
  queue 1 50
  queue low-latency strict-priority
 !
! Aplicar esta politica a la interface de salida del
¡ router P
interface POS2/0
```

```
ip addr X.X.X.X 255.255.255.252
tx-cos OUT-POLICY
```

5.6.2 Configurando DS-TE

DS-TE proporciona la posibilidad de dedicar específicos LSPs para tráfico de alta prioridad (muy sensibles) donde una alta calidad de servicio es requerida (en términos de retardo, *jitter* o pérdida de paquetes).

Para configurar DS-TE es necesario mencionar dos componentes importantes:

Configurar dos *pools* de ancho de banda en el núcleo (*global-pool* y *sub-pool*): usa el *sub-pool* para túnel que lleva tráfico altamente sensible, el otro pool, global-pool, se usará para túnel que lleva tráfico con requerimientos solo de Servicios Diferenciados o *Best Effort*. En el núcleo MPLS debe asegurarse que el tráfico enviado al LSP *sub-pool* es ubicado en la cola de "Alta Prioridad / Baja Latencia" en la interface de salida de cada LSR a lo largo del LSP. Es necesario asegurarse que esta cola no será sobre-suscrita para evitar descarte de paquetes.

En el *router* PE se limitará el ancho de banda del túnel LSP *sub-pool*. El total de tráfico enviado a este túnel debe ser menor o igual a la capacidad del ancho de banda del *sub-pool*. El exceso de tráfico será descartado.

La configuración de MPLS DS-TE es ligeramente diferente comparada con el mostrado en Ingeniería de Tráfico (TE). DS-TE es habilitado en los *routers* de núcleo usando versiones extendidas de los comandos "*tunnel mpls traffic-eng bandwidth sub-pool xxxxx*" y "*ip rsvp bandwidth xxxxx yyyyy sub-pool zzzzz*"

5.6.3 Configuración en el *router* PE

Solo se indicarán los cambios

```
interface R1-R2
  ip address 10.10.10.1 255.255.255.0
  ip router isis
  mpls traffic-eng tunnels <-- enable TE
  ip rsvp bandwidth 100000 100000 sub-pool 60000
!
router isis
  metric style wide
  mpls traffic-eng level-2
  mpls traffic-eng router-id loopback0
........
```

5.6.4 Configurando el túnel: R1 - R5

El túnel 10 es un túnel DS-TE usado para tráficos que necesitan altos requerimientos de QoS. Usaremos una ruta dinámica. La mejor ruta encontrada por CBR.

```
interface tunnel100
  ip unnumbered loopback0
  no ip direct-broadcast
  tunnel destination 192.168.1.5
  tunnel mode mpls traffic-eng
  !no se anuncia el tunnel vía un IGP
  no tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng bandwidth sub-pool 40000
  tunnel mpls traffic-eng priority 0 0
  !definiendocomo la ruta sera calculada
  tunnel mpls traffic-eng path-option 1 dynamic
  tunnel mpls traffic-eng record-route
```

Como los destinos detrás de R5 no son anunciados por el comando "a*utoroute announce*" sería necesario ingresar una ruta estática la cual usara el Túnel 10 como siguiente salto. Así se asegurará que el tráfico deseado pase por el túnel 10.

En la interface de Entrada.

- Creación de un lista de acceso (ACL) 100 llamada "ds-te-class" y aplicarlo a todos los paquetes destinados a "OUR-DESTINATION".
- Creación de la política *ds-te-input-policy*, donde:
    - Los paquetes en la clase ds-te-class son limitados a:
        - 8 millones de bits por segundo.
        - *Burst* normal de 01 millon de bytes.
        - *Burst* máximo de 02 millones de bytes.
    - Paquetes dentro del ancho de banda limitado son marcados con el valor de 5 en el campo EXP y son enviados.
    - Paquetes que exceden el tráfico limitado serán descartados.
    - Los demás paquetes son marcados con el valor de 0 en el campo EXP y son enviados.

5.6.5 Configurando la interface del *router* R1-R2.

- Todos lo paquetes MPLS marcados en el campo EXP con el valor de 5 serán ubicados en la cola de "alta prioridad / baja latencia".
- La configuración del PE varia de acuerdo a si se trata de un router de la familia cisco 7500 o 12000.

Configurando R1 como si se tratara de un *router* Cisco 7500

```
class-map match-all ds-te-class
  match access-group 100
!
access-list 100 permit ip any host "our-destination"
!
policy-map ds-te-input-policy
  class ds-te-class
        police 8000000 1000000 2000000 conform-action set-mpls-
exp-transmit 5
```

```
        exceed-action drop
    class class-default
        set-mpls-exp-transmit 0
```

Aplicando la política en la interface de entrada.

```
interface "inbound"
 service-policy input ds-te-input-policy
.....
```

Definición de la clase de alta prioridad /baja latencia con EXP=5.

```
class-map match-all exp5-traffic
 match mpls experimental 5

policy-map output-interface-policy
 class exp5-traffic
 priority 32

interface R1-R2
 service-policy output output-interface-policy
....
```

Configurando R1 como sise tratará de un *router* Cisco 12000

```
!
access-list 100 permit ip any "our-destination" 0.0.0.255
!
!!!...en la interface de entrada
interface "ingress"
    rate-limit input access-group 100 8000000 1000000 2000000
    conform-action set-mpls-exp-transmit 5 exceed-action set-mpls-
    exp-transmit 0
!!!
!!!...en la interface de salida (R1-R2)
interface R1-R2
    ....
    tx-cos exp-class-ds-te
```

Donde "*exp-class-ds-te*" es definido como:

```
cos-queue-group exp-class-ds-te
  precedence 0 random-detect-label 0
  precedence 5 queue low-latency
  precedence 5 random-detect-label 5
  random-detect-label 0 100 200 1
  random-detect-label 5 2000 3000 1
  queue low-latency strict-priority
```

5.6.6 Configuración en los *routers* intermedios (P).

Ambas interfaces de entrada y de salida en los *routers* intermedios son idénticamente configurados a la interface de salida del router PE, R1.

5.6.7 Configuración en el *router* remoto R5 (PE).

La configuración de las interfaces (que ve a la nube MPLS) del *router* PE son configurados idénticamente a las interfaces de los *routers* intermedios (P).

En el ejemplo anterior, solo tráfico DS-TE está circulando en el núcleo MPLS. Imaginemos una configuración, donde el tráfico de destino a "*our-destination*" use DS-TE y los otros tráficos tomen ventaja de MPLS-TE.

Como se comenta en las configuraciones anteriores, el LSP DS-TE creado continuará usando la cola de "alta prioridad / baja latencia". El tráfico TE usará encolamiento "normal". Así, en todas las interfaces de entrada, donde los LSP DS-TE y LSP TE podrían correr concurrentemente, una política de limitación de tráfico necesitará ser establecida. Esta política permitirá asegurar que el ancho de banda del tráfico DS-TE este siempre disponible en caso de congestión en la red MPLS.

CONCLUSIONES

El presente informe expone las principales características de los servicios diferenciados y su aplicación sobre MPLS. Este desarrollo es posible gracias a diversas tecnologías que hacen de MPLS una plataforma de red muy robusta en términos de seguridad, ingeniería de tráfico y calidad de servicio. A continuación mencionan las conclusiones que nos deja la aplicación de servicios diferenciados sobre MPLS:

1. Los avances en aplicaciones de tiempo real de hoy en día, requieren alta disponibilidad y sobre todo calidad de servicio. Esto impulsa a desarrolladores, como el IETF y fabricantes, como CISCO, a evolucionar las tecnologías existentes e investigar en nuevas tecnologías. MPLS extrae lo mejor de desarrollos realizados y los usa para implementar una infraestructura de red de nueva generación, con bondades que son necesarias para las aplicaciones en tiempo real de hoy en día y con la más alta confiabilidad.

2. La evolución de tecnologías como ingeniería de tráfico (TE), calidad de servicio (QoS), protocolos de *routing* (IGP), y avances en arquitecturas de hardware

y software de equipos de red, han aportado de manera significativa en la evolución de MPLS. Esto permite que MPLS sea una tecnología de *backbone* privilegiada respecto a otras tecnologías.

3. Inicialmente no se brindaba calidad de servicio y los paquetes eran enviados de acuerdo al mejor esfuerzo (*Best Effort*); luego, el grupo IETF desarrolló la arquitectura de servicios integrados (*Intserv*) y finalmente la arquitectura de servicios diferenciados (*DiffServ*). Estas arquitecturas son la base de fundamentos y definiciones que los fabricantes de tecnología deben tener en cuenta en el desarrollo de sus productos.

4. Lo más importante para brindar calidad de servicio es identificar el paquete que se requiere priorizar para luego clasificarlo y asociarlo a una clase para darle un trato especial, según la clase marcada. De acuerdo a esto, en una red convencional, se puede usar la interface de entrada, la dirección IP fuente o destino, el *IP precedence*, el puerto, o la combinación de estos valores. También, se debe tener en cuenta los recursos de *hardware* y *software* implementados en la red tal que puedan realizar esta labor de marcado, clasificación y aplicación de políticas de calidad de servicio. En tal sentido, se han desarrollado diversas técnicas y mecanismos que hacen posible la implementación de calidad de servicio basándose en la aplicación de los servicios diferenciados.

5. Actualmente la mejor técnica de manejo de congestión usada es LLQ (*Low Latency Queuing*). Con esto se logra obtener alta calidad de servicio para aplicaciones sensibles a retardos, perdida de paquetes, *jitter* (variación de retardo) y otros factores que puedan degradar el servicio. Estas aplicaciones pueden ser VoIP,

Videoconferencia IP, Tráfico SNA (servidores, cajeros automáticos, etc.) y otras aplicaciones de tiempo real.

6. Es importante mencionar que MPLS no reemplaza la tecnología IP. El plano de control IP forma parte de la arquitectura MPLS y es un componente fundamental.

7. Con el desarrollo de MPLS, servicios diferenciados e ingeniería de tráfico, se logran altos niveles de calidad de servicio no sólo a nivel de capa3 sino también a nivel de capa2. MPLS implementa un nuevo paradigma de envío de paquetes, conmutación de etiquetas, en la cual solo asocia las decisiones de envío a la información de la etiqueta. Con esto se logra una mayor eficiencia de los recursos de red, bajo procesamiento de memoria y CPU en condiciones de alto tráfico. El campo EXP de la etiqueta MPLS indicará la preferencia del paquete, es decir como será tratado en la red MPLS, y este puede ser alterado sin alterar el campo DSCP del paquete original. Esta flexibilidad permite al proveedor de servicio manejar clases de servicio y calidad de servicio a cada una de estas clases, variando el campo EXP para estos fines pero sin alterar el paquete original del cliente. El *router* de ingreso a la red MPLS, realiza la labor de marcado y clasificación para aplicar al paquete las características de calidad de servicio contratadas por el cliente y acordadas en el SLA (*Service Level Agreement*) establecido entre el proveedor de servicios y el cliente.

7. MPLS también 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.

8. Actualmente los más importantes proveedores de servicios del mundo están migrando sus redes a MPLS para obtener mejores estándares de calidad de servicio. Por ejemplo, en Marzo del presente año (2005), la empresa Telmex Latin America ha implementado en Chile la primera red IP Metropolitana 10Gigabit de ese país, basada en tecnologías DWDM, Metro *Ethernet* y MPLS. Esta red implementa lo mejor de las tecnologías de acceso y lo mejor de las redes de *backbone* (MPLS). En el Perú actualmente tanto las empresas Telmex como Telefónica tienen implementadas la tecnología MPLS en sus *backbones*, con accesos Serial, *Ethernet*, ADSL, etc. Telmex Perú también piensa lanzar una red 10 *Gigabit* con similares características a la implementada en Chile.

9. Finalmente podemos decir que la evolución de nuevas tecnologías como MPLS, LLQ, Metro *Ethernet*, DWDM, dan la posibilidad al proveedor de servicio de implementar una red robusta en su *backbone* que brinde optimización de los recursos de su red con una significativa reducción de costos. Esto permite la convergencia sobre IP, ganando además en calidad de servicio, velocidad, seguridad y flexibilidad.

10. En mi opinión, he podido observar las notables diferencias de tener una red MPLS respecto a otras redes como ATM. Las principales diferencias son definitivamente la calidad de servicio y la mayor velocidad de reenvió de paquetes. Además con MPLS se evita el exceso de *padding* que tiene ATM que consiste en llenar el *payload* (información útil) de la celda hasta obtener el valor estándar de 48bytes. MPLS evita esto usando diversos protocolos de la capa 2 que tienen variable valor de *payload*. Puedo decir, que un cliente que tiene como red WAN la

arquitectura MPLS tiene definitivamente un mejor funcionamiento que un cliente que tiene como red WAN la tecnología ATM.

11. MPLS se suma al desarrollo de la red metropolitana llamada "*metro ethernet*", la cual intercoecta redes LAN a grandes distancias dentro de una misma ciudad para implementar una red de nueva generación. El principal problema de las redes metropolitanas es el cuello de botella en el acceso a la red WAN pero con el apoyo MPLS en el *core* se puede diferenciar servicios y manejar mejor la distribución de ancho de banda. Otros beneficios del uso de estas tecnologías son: el bajo costo pues ethernet es ampliamente usado y los costos de administración, operación y funcionamiento son bajos, a cambio se obtiene acceso de banda ancha de 10Mbps, 100Mbps, 1Gbps y 10Gbps. Las redes implementadas con Ethernet permiten modificar y manipular de una manera más dinámica, versátil y eficiente, los anchos de banda y cantidad de usuarios en corto tiempo.

12. En suma, el valor fundamental que obtienen los proveedores de servicios al implementar una red IP MPLS es la habilidad de ofrecer conectividad en capa 2 y capa 3 y compartir servicios (como DHCP, NAT, etc.) sobre una misma red con altos grados de optimización y utilización del ancho de banda disponible en la red usando ingeniería de tráfico y calidad de servicio para brindar servicios diferenciados.

APENDICE

GLOSARIO MPLS

AAL: ATM *Adaptation Layer*. Capa de Adaptación ATM

Admisión control: control de admisión. Es un grupo de acciones tomadas por una red para admitir o denegar determinados flujos de tráfico.

AF: *Assured Forwarding*, Una clasificación de servicios diferenciados para paquetes que especifican la precedencia de descarte de paquetes.

ATM: *Asynchronous Transfer Mode*, Modo de Transferencia Asíncrono

ATM-LSR: ATM *Label Switching Router*. *Router* conmutador de etiquetas ATM.

BA: *Behavior Aggregate.* Una colección de paquetes que tienen el mismo valor de DSCP.

Backbone: Línea de transmisión de datos de alta velocidad o una serié de conexiones que juntas una vía con gran ancho de banda.

BGP: *Border Gateway Protocol*. Un protocolo de *routing* entre dominios que intercambia información de rutas con otros sistemas BGP. Definido en el RFC 1163.

Capa 2: capa de enlace de datos.

Capa 3: capa de red.

CAR: *Committed Access Rate*. Es utilizado como una forma de condicionar tráfico y separarlo en clases dentro del dominio DS.

CBR: *Constraint-Based Routing*. Es un protocolo y a la vez procedimiento que determina la ruta de la etiqueta a través de la red.

CBWFQ: *Class-Based weighted Fair Queuing*. Permite definir clases que están basadas en ciertos criterios.

CE-router: *Customer Edge router*. El *router* CE es un equipo que es parte de la red del cliente.

CEF: *Cisco Express Forwarding*. Una avanzada tecnología de conmutación de la capa 3. El CEF optimiza el funcionamiento de la red y la hace escalable durante el paso de gran cantidad de tráfico.

CoS: *Class of Service*. Es una característica que proporciona tipos de servicio diferenciado a través de la red MPLS.

CPE: *Customer Premisse Equipment*. Equipo que se encuentra dentro de la red edl cliente.

CR-LDP: *Constraint-based Routing Label Distribution Protocol*. Un grupo de extensiones para LDP que habilita CBR y QoS en una red MPLS.

DiffServ: *Differenciated Services*. Servicios diferenciados

DLCI: *Data-Link Connection Identifier*. Es una etiqueta usada en Frame Relay para identificar un circuito.

Dominio MPLS: Son nodos continuos que operan bajo un mismo protocolo de *routing* MPLS.

DSCP: *Differentiated Services Code Point*. Se refiere a los 06 primeros bits del campo ToS en la cabecera IP.

DWDM: *Dense Wavelength Division Multiplexing*. Método de transmisión óptica de múltiples señales sobre una misma fibra.

Edge LSR: Es un LSR que aplica o remueve la etiquete al ingresar o egresar de la red respectivamente.

EF: *Expedited Forwarding*. Paquete marcado que garantiza mínimo retardo y baja perdida de paquetes.

Etiqueta MPLS: Es la etiqueta que lleva el paquete IP y que representa el FEC al que pertenece el paquete.

FEC: *Forwarding Equivalente Class*. Es un grupo de paquetes de la capa 3 que son enviados de la misma manera sobre la misma ruta y con el mismo tratamiento de envío.

FRTS: *Frame Relay traffic Shapping*. Mecanismo usado para modelar tráfico sobre Frame Relay.

GTS: *Generic Traffic Shapping*. Proporciona un mecanismo para controlar el flujo de tráfico en una particular interface.

IGP: *Interior Gateway Protocol*. Es un protocolo de Internet usado para intercambiar información de *routing* en un mismo sistema autónomo.

IETF: Internet Engineering Task Force. Grupo de desarrollo de estándares de nuevas tecnologías.

IntServ: *Integrated Services*. Servicios integrados.

IP: *Internet Protocol*. Protocolo de Internet

IP Precedence: Valor de 03 bits del campo Tos de la cabecera IP.

IS-IS: *Intermediate System-Intermediate System.* Es un protocolo de routing del tipo *link-state.*

ISP: *Internet Seviche Provider.* Proveedor de servicios de Internet.

Label: Es un identificador usado para identificar un FEC.

LAN: *Local Area Network.* Red de Área Local.

LDP: *Label Distribution Protocol.* Es el protocolo usado para distribuir etiquetas entre los LSRs tal como lo define el IETF.

LFIB: *Label Forwarding Information Base.* Es una estructura de datos usada por etiquetas para mantener información de las etiquetas de entrada y salida, interfaces y los FECs.

LIB: *Label Information Base.* Es una base de Datos usada por un LSR para almacenar etiquetas aprendidas de otros LSRs.

LLQ: *Low Latency Queuing.* Método que aplica una prioridad estricta a colas CBWFQ.

LSP: *Label-Switched Path.* Es el camino por el que viaja un paquete a través de uno o más LSRs en la red MPLS.

LSR: *Label-Switching Router.* Es un nodo MPLS que envía paquetes a nivel de la capa 3.

LVC: *Label switch controlled Virtual Circuit.* Son circuitos virtuales ATM que son configurados a través de LDP en los ATM LSR.

MPLS: *MultiProtocol Label Switching.* Es un grupo de estándares desarrollados por el IETF diseñados para permitir el flujo de paquetes basados en conmutación de etiquetas.

P-router: *Provider core router*. El *router* P es un LSR que no esta conectado a los clientes. Se trata de un LSR netamente conmutador de etiquetas.

PE-router: *Provider Edge router*. El LSR Pe es parte de la red del proveedor de servicios. Los *routers* PE son usados para que los clientes puedan acceder a la red MPLS.

PHB: *Per-Hop Behavior*. Hace referencia al comportamiento de los paquetes que están organizados, encolados, y que pertenecen a un mismo BA

POS: *Packet over SONET/SDH*. Tecnología en la cual los paquetes IP son mapeados en *frames* SONET o SDH sin la intervención de una capa ATM.

PVC: *Permanent Virtual Circuit*. Es un circuito virtual configurado permanentemente para tecnologías de la capa 2 como ATM o Frame Relay.

QoS: *Quality of Service*. Forma de medir el funcionamiento en sistemas de transmisión de datos que reflejan su calidad de transmisión y disponibilidad de servicio.

Router: Es un dispositivo que conecta dos o más redes. Asegura que estas redes puedan mantener una comunicación constante basándose en un protocolo de *routing* para tomar decisiones de envío de paquetes.

Routing: Es la capacidad que tienen los dispositivos como *routers* o LSRs para reenviar paquetes a un destino en particular. Para tomar estas decisiones hacen uso de un protocolo de *routing* d la capa 3.

RSVP: *Resource reSerVation Protocol*. Es un protocolo que reserva recursos de red para proporcionar calidad de servicio garantizado a flujos de tráfico.

SDH: *Synchronous Digital Hierarchy*. Es un estándar europeo que define velocidades y estándares de transmisión de señales ópticas sobre fibra óptica usando ATM y SONET.

SONET: *Synchronous Optical NETwork*. Es un estándar desarrollado por *Bellcore* y ampliamente usado por las industrias de telecomunicaciones para transportar altas velocidades sobre fibra óptica.

TDP: *Tag Forwarding Protocol*. Protocolo propietario de Cisco usado para distribuir etiquetas a través de los LSRs.

TE: *Traffic Engineering*. Técnica y proceso usado para hacer circular el tráfico por la ruta más optima de acuerdo al protocolo de *routing* estándar que ha sido aplicado.

TE-túnel. Es un túnel usado por ingeniería de tráfico.

UDP: *User Datagram Protocol*. Protocolo de Datagrama de Usuario

VoIP: Voz sobre IP.

VPN: *Virtual Private Network*. Un grupo seguro y cerrado de usuarios a nivel de la capa 3 que comparten recursos de una o más redes de la capa 2.

VRF: *VPN Routing/Forwarding*. Una VRF incluye la información de routing que define un cliente VPN que esta conectado al router PE.

WAN: *Wide Area Network*. Red de area extensa.

WFQ: *Weighted Fair Queuing*. Técnica de encolamiento que garantiza a cada cola una porción del total de ancho de banda disponible.

WRED: *Weighted Random Early Detection*. WRED proporciona un trato preferencia a los paquetes de la cola de alta prioridad.

BIBLIOGRAFÍA

1. Alwayn, Vivek, "*Advanced MPLS Design and Implementation*", CISCO Press", 2002.

2. Keagy, Scott, "*Integrating Voice and Data Networks*", CISCO Press, 2000.

3. Halabi, "*Internet Routing Architecture*", CISCO Press, 2000.

4. Guichard-Pepelnjak, "*MPLS and VPN Architectures",* CISCO Press 2001.

5. R.Callon, "*A Framework for MultiProtocol Label Switching*", Internet *draft-ietf-mpls-framework-05,* Set. 1999.

6. R Braden, "*Resource ReSerVation Protocol (RSVP)*", RFC 2205, Set. 1997.

7. Le Faucheur, "*MPLS Support for Differentiated Services*", Internet *draft-ietf-mpls-diff-ext-08.txt*

8. E. Rosen, "*MultiProtocol Label Switching Architecture*", RFC 3031, Jun. 2001.

9. R. Braden, "*Integrated Services in the Internet Architecture: an Overview*", RFC 1633, Jun. 1994.

10. D. Awduche, "*Requirements for Traffic Engineering over MPLS*", RFC 2702, Set.1999.

11. K. Nichols, "*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*", RFC 2474, Dic. 1998.

12. S. Blake, "*An Architecture for Differentiated Services*", RFC 2475, Dic. 1998.