Universidad Austral de Chile

Escuela de Electricidad y Electrónica

"REDES MPLS: FUNDAMENTOS, APLICACIÓN Y GESTIÓN DE RECURSOS"

Trabajo de Titulación para optar al
Título de Ingeniero Electrónico

PROFESOR PATROCINANTE:

Sr. Néstor Fierro Morineaud.

LUIS MIGUEL CORTÉS SALVIAT

VALDIVIA 2005

Profesor patrocinante:

Néstor Fierro Morineaud _____

Profesores Informantes:

Alejandro Villegas Macaya _____

Raúl Urra Ríos _____

DEDICATORIA

A mi Madre:

Cecilia del Carmen Salviat Barría. Quien con todo su amor, me brindó todo su apoyo y confianza e hizo posible que lograra este gran anhelo. A ella estaré eternamente agradecido y le dedico todo mi esfuerzo en mis estudios reflejados a través de este título. Doy gracias a Dios y a la vida por darme una madre tan maravillosa.

A mi Hermano:

Raúl Valdemar Cortés Salviat. Quien ha estado siempre brindándome cariño, fuerza y confianza para salir adelante.

AGRADECIMIENTOS

Este espacio agradezco de forma muy especial a mi tutor Don Néstor Fierro Morineaud, Académico de la Facultad de Ciencias de la Ingeniería, Instituto de Electrónica, quien me brindó toda su ayuda y experiencia, permitiéndome llegar a buen término en el desarrollo de este trabajo de titulación.

Agradezco a todos mis profesores por parte de la Escuela de Electricidad y Electrónica y del Instituto de Electrónica de la Universidad Austral de Chile, en especial a mis tutores, Don Raúl Urra Ríos y Don Alejandro Villegas Macaya.

También agradezco a toda mi familia, a mis amigos y compañeros que directa o indirectamente han logrado brindarme la posibilidad de obtener el título.

RESUMEN

El presente trabajo de tesis esta orientado a la entrega de información precisa y concisa sobre estándar MPLS o multiprocolo de etiquetas conmutadas. MPLS es una nueva tecnología orientada a redes de comunicación sobre Internet, la cual propone una nueva estrategia de encaminamiento para el tráfico que cursa a través de la misma. Aquí se describen las bases de dicha tecnología, mecanismo de operación, destacando las ventajas y diferencias con las tecnologías actuales, además sus principales aplicaciones.

La metodología que se utilizo para la trascripción de esta tesis fue la búsqueda y revisión de publicaciones producidas por la industria de telecomunicaciones, como son empresas operadoras de sistemas de comunicaciones, organismos de estandarización, proveedores de infraestructura de telecomunicaciones, foros de la industria, e información aparecida en la prensa tanto nacional como internacional, y universidades extranjeras, a través de las bases de datos propias de este tipo de instituciones, en el período 1990 a 2004. Complementariamente, se utilizó los principalmente buscadores como Google y Altavista de Internet.

Es importante destacar que este sistema, aunque nuevo, ya es implementado en países como Estados Unidos, España e Inglaterra con un gran nivel de expansión. Así entonces, adquiere mayor preponderancia el generar nuevas investigaciones en torno al tema.

ABSTRACT

The present work of thesis this oriented to the delivery of precise and concise information on standard MPLS or multiprocol label switching. MPLS is a new technology oriented to communication networks on Internet, which proposes a new strategy of routing for the traffic that attends through the same one. Here to the bases of this technology, mechanism of operation are described, emphasizing the advantages and differences with the present technologies, in addition their main applications.

The methodology that I am used for the trascripción of this thesis was the publication search and revision produced by the industry of telecommunications, as they are companies sysops of communications, organisms of standardization, infrastructure suppliers of telecommunications, forums of the industry, and information appeared in the press as much national as international, and universities, through the own data bases of this type of institutions, in period 1990 to 2004. Complementarily, it was used the mainly seeking ones like Google and Altavista de Internet.

It is important to emphasize that this system, although new, already is implemented in countries like the United States, Spain and England with a great level of expansion. Thus then, it acquires greater superiority generating new investigations about.

ÍNDICE

CAPITULO I.- “INTRODUCCIÓN A MPLS”

1.1 Introducción

Desde el inicio de la historia humana, el hombre ha buscado formas de comunicación para hacer más factible su supervivencia y como respuesta a sus instintos. Así entonces, se vieron obligados a transmitir a quienes les rodeaban, sus impresiones, sentimientos, emociones. Para ello se valieron de la mímica, de los gritos y las interjecciones, lo que constituyó un lenguaje biológico.

Posteriormente surgió el lenguaje hablado y las manifestaciones pictóricas. Aparecen las pinturas rupestres, los jeroglíficos; pudiendo así el hombre, por primera vez expresar su pensamiento de un modo gráfico.

El pensamiento humano ha evolucionado tornándose cada vez más complejo, por consiguiente, el ser humano se ha visto en la necesidad de generar una gran diversidad de cambios e inventos para optimizar el proceso comunicacional, entre estos se encuentran desarrollos tecnológicos que han sido sindicados como los precursores de la globalización de la información, así se hace mención de la Imprenta, el Teléfono, la Radiofonía, la Televisión, e Internet.

Con respecto al último medio de comunicación citado, este se inició como un proyecto de defensa de los Estados Unidos. A finales de los años 60, la ARPA (Agencia de Proyectos de Investigación Avanzados) del Departamento de Defensa definió el protocolo TCP/IP. Aunque parezca extraño, la idea era garantizar mediante este sistema la comunicación entre lugares alejados en caso de ataque nuclear. Ahora el TCP/IP sirve para garantizar la transmisión de los paquetes de información entre lugares remotos, siguiendo cualquier ruta disponible.

En 1975, ARPAnet comenzó a funcionar como red, sirviendo como base para unir centros de investigación militares y universidades, además se desarrolló protocolos más avanzados para diferentes tipos de ordenadores y tecnologías específicas. En 1983 se adoptó el TCP/IP como estándar principal para todas las comunicaciones, y en 1990 desapareció ARPAnet para dar paso junto a otras redes TCP/IP a Internet. Por aquel entonces también comenzaron a operar organizaciones privadas en la Red.

Así, Poco a poco, todos los fabricantes de ordenadores personales y redes han incorporado el TCP/IP a sus sistemas operativos, de modo que en la actualidad cualquier equipo está listo para conectarse a Internet. Internet une muchas redes, incluyendo como más importante la World Wide Web, de principios de los 90. Se calcula que actualmente hay varios miles de redes de todos los tamaños conectadas a Internet, más de seis millones de servidores y entre 40 y 50 millones de personas que tienen acceso a sus contenidos. Y estas cifras crecen sin cesar de un día a otro.

En la actualidad es imprescindible hablar de Internet, conectividad, e-mail, y en general de toda una serie de términos relacionados con esta revolución informática, en la que cada persona como individuo trabajador o estudiante se ve influenciado. Durante los últimos años esta revolución ha variado el estilo de vida de la raza humana como tal. Este es el medio que en la historia de la raza humana ha tenido el mayor crecimiento en el mercado global.

Sobre los últimos años, Internet ha inspirado el desarrollo de una variedad de nuevos usos en mercados de empresarios y consumidores. Estos nuevos usos han conducido a una demanda creciente de requisitos y junto con ello la garantía de ancho de banda en el núcleo de la red. Además de los servicios tradicionales de los datos proporcionados actualmente sobre el Internet, se están desarrollando y se están desplegando nuevos servicios voz y multimedia. El Internet ha emergido como la red de la opción para proporcionar estos servicios convergidos. Sin embargo, las demandas puestas en la red por estos nuevos usos y servicios, en términos de la

velocidad y de ancho de banda, han agotado los recursos de la infraestructura existente del Internet.

Consecuentemente a mediados de los 90, varias propuestas de distintos fabricantes proponen soluciones de tipo "conmutación IP" (IP switching) o "conmutación multinivel" (multilayer switching) para dar soluciones integrales y lograr satisfacer estas necesidades. Estas soluciones planteadas tales como: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba, condujeron finalmente a la adopción del actual estándar MPLS del IETF. [4]

MPLS (multiprotocol label switching) esta basada en el concepto de multiprocolo de etiquetas conmutadas. En donde la IETF o Engineering Task Force se forma como grupo de trabajo para estandarizar esta nueva tecnología, hoy en día MPLS es definida por un conjunto de la IETF Request for comments (RFCs) y una serie de especificaciones (bajo desarrollo).

MPLS desempeña un papel importante en el encaminamiento, el encaminamiento con protección (rutas de respaldo), establecimientos de circuitos, y el envío de paquetes a través de la red de próxima generación para resolver las demandas del servicio garantizados para los usuarios de la red.

Está claro que la migración a MPLS es de manera rápida y efectiva. Cada proveedor importante en los Estados Unidos, y muchos otros países, están migrando y compatibilizando sus redes hacia MPLS. Un estudio hecho el 2004 por la “Infonetics Research” muestra que el 86 por ciento de abastecedores de servicio, en el mundo entero, convergen sus redes de datos hacia IP/MPLS. Puesto que MPLS es una tecnología desarrollada para dar soluciones hacia redes de datos de servicios integrados en redes de banda ancha, otorgando así garantías de calidad de servicio [6].

1.2 Objetivos

1.2.1 Objetivos generales

- Realizar un trabajo orientado a la investigación sobre las redes MPLS, estableciendo así las bases de dicha tecnología.

- Dar a conocer las motivaciones que han llevado a la adopción del estándar MPLS.

- Adquirir los conocimientos necesarios sobre redes MPLS y de esta forma plantear las ventajas y diferencias con redes tradicionales.

1.2.2 Objetivos específicos

- Analizar los fundamentos de MPLS y sus mecanismos y componentes, describiendo claramente la separación entre las funciones de encaminamiento (routing) y envío (forwarding) en las redes IP.

- Describir los protocolos de distribución. LDP. RSVP.

- Dar a conocer las aplicaciones que permitan demostrar las potencialidades de las redes MPLS. tales como: redes privadas virtuales, ingeniería de tráfico, calidad de servicio.

- Describir el Balanceo de carga y sus mecanismos que la constituyen, y así comprender las formas de gestionar los recursos.

CAPITULO II.- "ANTECEDENTES GENERALES"

2.1 Glosario

A continuación se describen algunos conceptos básicos que se aplican a cualquier tecnología de conmutación y que son de gran ayuda para comprender este texto.

Enrutamiento.- Es un término utilizado para describir las acciones tomadas por una red para mover paquetes a través de ella (entre redes y subredes). El viaje de los paquetes se lleva a cabo a través de la red de máquina en máquina hasta llegar a su destino. Los protocolos de enrutamiento (ej: RIP, OSPF) permiten que cada maquina conozca cual máquina es el salto siguiente (next hop) para que el paquete llegue a su destino. Los enrutadores utilizan estos protocolos de enrutamiento para construir tablas de envío.

Conmutación (switching).- Es generalmente utilizado para describir la transferencia de datos de un puerto de entrada a un puerto de salida donde la selección del puerto de salida esta basado en información de la capa 2 (ej: VPI/VCI en ATM).

Componente de control.- Construye y mantiene la tabla de envío para el nodo a utilizar. Trabaja junto con los componentes de control de otros nodos para distribuir información de enrutamiento de forma consistente, también asegura que se utilicen los procedimientos locales adecuados para la creación de la tabla de envío.

Componente de envío (forwarding component).- Lleva al cabo el envío del paquete basándose en información de la tabla de envío (mantenida por el enrutador).

Tabla de envío.- Es un conjunto de campos en una tabla, los cuales proporcionan la información que ayuda al componente de envío a realizar su función de conmutación. La tabla de envío debe asociar cada paquete con un campo (tradicionalmente la dirección destino).

FEC (Forward Equivalent Class).- Es una representación de un grupo de paquetes que comparten los mismos requerimientos para su transporte.

Etiqueta.- Es un identificador corto de longitud fija de significado local el cual es utilizado para identificar un FEC. La etiqueta que se coloca en un paquete particular representa el FEC al cual el paquete es asignado.

Conmutación de Etiqueta (Label Switching).- Es una forma avanzada de envío de paquetes la cual reemplaza el algoritmo de envío convencional por un algoritmo mas eficiente de intercambio de etiqueta [1].

2.2 IP sobre ATM

La topología IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia. Cada router se comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM.

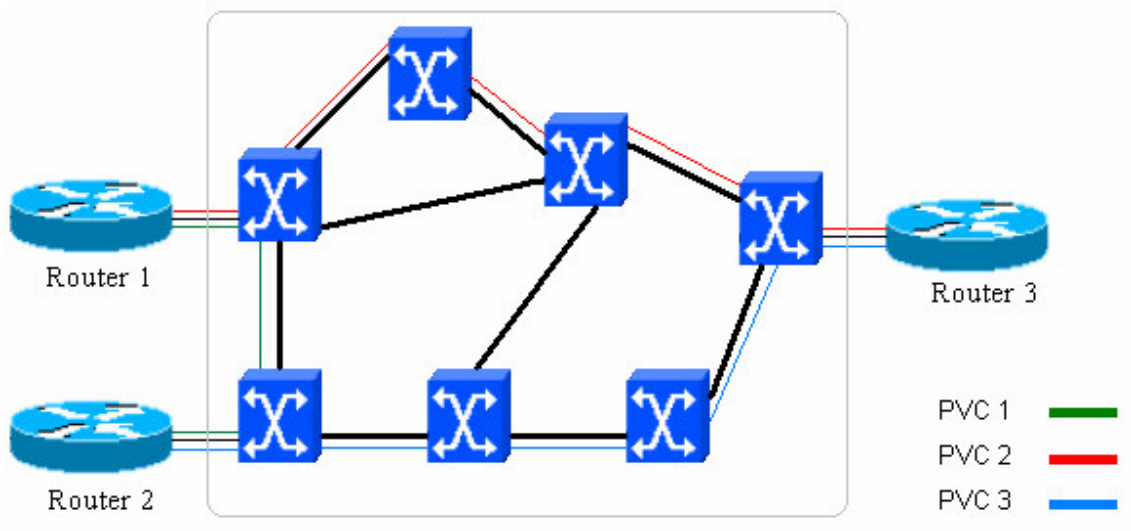

Figura 1.- Topología física (nivel 2).

Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la figura 1 y 2 se representa un claro ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM (figura 1) con la de la topología lógica IP superpuesta sobre la anterior (figura 2).

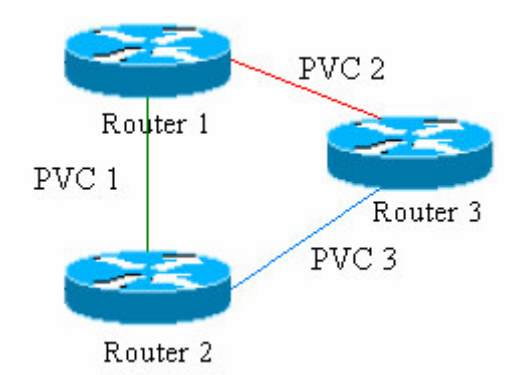

Figura 2.- Topología lógica (nivel 3).

La base de la tecnología IP/ATM [3] está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. (Más adelante se verá que el intercambio de etiquetas es uno de los componentes fundamentales en la arquitectura MPLS). Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas. La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del backbone; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software.

En la figura 2 se representa el modelo IP/ATM con la separación de funciones entre los que es routing IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

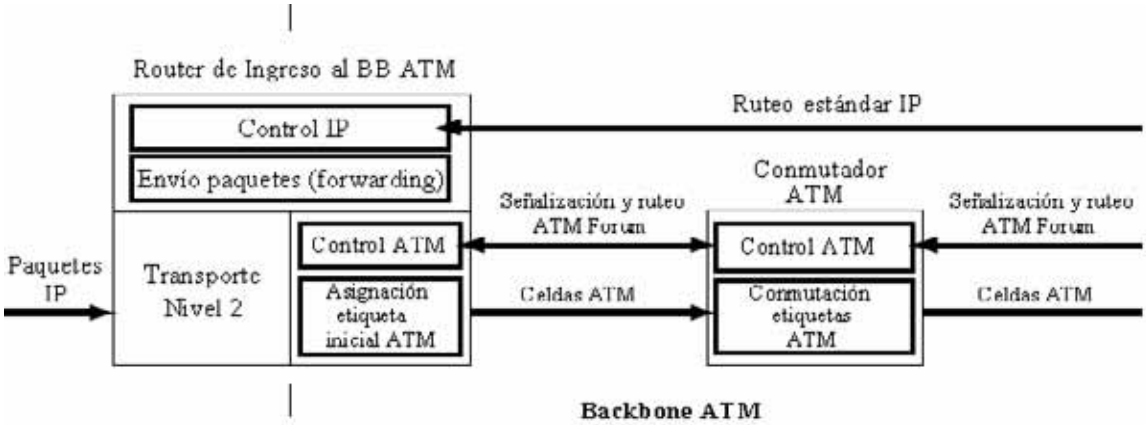

Figura 3.- Modelo IP sobre ATM [3].

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte de datos que proporcionan los conmutadores. Los NSPs (proveedores de servicios) de primer nivel, poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de las necesidades del tráfico IP, utilizando la clase de servicio ATM UBR (Unspecified Bit Rate), ya que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes del ATM para control de la congestión y clases de servicio).

La ingeniería de tráfico se hace a base de proporcionar a los routers los PVCs necesarios, con una topología lógica entre routers totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los subinterfaces en los routers con los PVCs, a través de los cuales se intercambian los routers la información de encaminamiento correspondiente al protocolo interno IGP7. Lo habitual es que, entre cada par de routers, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal.

2.2.1 Limitaciones del modelo IP sobre ATM

La superposición de las dos topologías supone a los proveedores de servicio mayores costos para la implementación de sus redes. Sin embargo hay que destacar que al gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, supone a los proveedores de servicio que uno de los mayores costos se basa en la gestión sobre sus redes.

Existe, además, lo que se llama la "tasa impuesta por la celda", un overhead aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible.

Por otro lado, la solución IP/ATM presenta problemas de crecimiento exponencial nx(n-1) al aumentar el número de nodos IP sobre una topología completamente mallada. Por ejemplo, en una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM, son necesarios 5 x 4 = 20 PVCs (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura (6 x 5 = 30). Un problema adicional del crecimiento exponencial de rutas, es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP [4].

2.3 Convergencia hacia la Conmutación IP

Los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1994 a 1999) a que varios fabricantes desarrollaran técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señaladas anteriormente; con el fin de mezclar la alta velocidad de ATM basada en la conmutación y técnicas de encaminamiento IP. Esas técnicas se conocieron como "Conmutación IP" (IP switching) o "Conmutación Multinivel" (multilayer switching). La conmutación multicapas (multilayer switching), es la integración de la conmutación de la capa 2 y el ruteo de la capa 3. Los conmutadores de nivel 2 proveen la conectividad a grandes velocidades, mientras que los routers IP interconectados por los circuitos virtuales proveen de la inteligencia para enviar los paquetes IP. Es la convergencia de estas dos capas que genera el problema de mapear y realizar procesos complejos entre dos arquitecturas diferentes.

Así una serie de tecnologías privadas presentan soluciones que convergen en MPLS, entre las que merecen citarse:

- **Cell Switching Router (CSR).-** Fue desarrollado por Toshiba y presentado a la IETF en 1994. Fue una de las primeras propuestas para utilizar protocolos IP

para controlar infraestructura ATM. CRS se ha desarrollado en redes comerciales y académicas en Japón.

- **IP switching.-** Desarrollado por Ipsilon, se anunció en 1996. El objetivo básico de IP switching fue el de integrar conmutadores ATM de una manera eficiente (eliminando el plano de control ATM). Ipsilon utilizó la presencia de tráfico para controlar el establecimiento de una etiqueta.

- **Tag switching.-** Es la tecnología de conmutación de etiquetas desarrollada por Cisco Systems. A diferencia de las dos soluciones anteriores, tag switching es una técnica la cual no requiere de flujo de tráfico para la creación de tablas de etiqueta en un enrutador. En lugar de esto utilizaba protocolos de enrutamiento IP para determinar el siguiente salto.

- **Aggregate Route-based IP Switching (ARIS).-** Es desarrollado por IBM y es muy similar a Tag switching de Cisco. En ARIS la distribución de etiquetas comienza en el enrutador de salida y se propaga de forma ordenada hacia el enrutador de entrada.

Ya que múltiples soluciones independientes para el desarrollo de tecnologías basadas en conmutación de etiquetas es claramente una dirección no aceptable, se reconoció la necesidad de desarrollar estándares y se creó el grupo de trabajo de la IETF (Internet Ingineering task force) para este propósito, el cual fue creado en abril del año 1997.

Luego en enero del año 2001 la IETF (Internet Ingineering task force), establece las primeras bases de las redes MPLS y esto ha provocado la expansión de dicha tecnología.

2.4 La tecnología multinivel

Antes de comenzar a describir MPLS se debe entender que todas las soluciones de conmutación multinivel incluyendo MPLS deben cumplir con lo siguiente [6]:

- Separación de la componente de Control (routing) y de Envío (forwarding).

- Algoritmo de Intercambio de Etiquetas para el envío (Label-swapping forwarding algorithm).

2.4.1 Separación de las Componentes de Control y de Envío

Todas las soluciones de conmutación multinivel incluyendo MPLS, están compuestas por dos funcionalidades distintas (una componente de control y otra de envío), la componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros routers, para la construcción y el mantenimiento de las tablas de encaminamiento. La componente de envío examina la información contenida en la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y direcciona el paquete desde la interfaz de entrada a la interfaz de salida a través del correspondiente hardware de conmutación.

Específicamente, al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete.

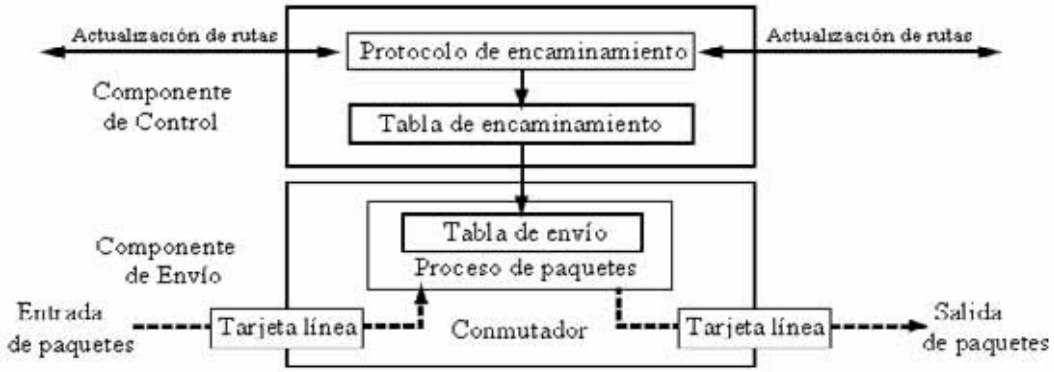

Figura 4.- Separación funcional del encaminamiento y envío [6].

Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ella se puede implementar y modificar independientemente. El único requisito es que la componente de encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información.

2.4.2 Algoritmo de Intercambio de Etiquetas para el envío (Label swapping forwarding algorithm).

El mecanismo de envío se implementa mediante el intercambio de etiquetas, Este algoritmo es el mismo usado para el envío de paquetes en switches ATM y Frame Relay. La señalización y distribución son fundamentales para el algoritmo de Intercambio de Etiquetas, la diferencia está en que ahora lo que se envía por la interfaz física de salida son paquetes "etiquetados".

De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento. En cuanto a la etiqueta que marca cada paquete, es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo y que identifica una "clase equivalente de envío" (Forwarding Equivalence Class, FEC). La FEC como se mencionó anteriormente es un conjunto de paquetes que

se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes.

Por ejemplo: en el encaminamiento convencional IP por prefijos de red (longest-match) una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo. Realmente, una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, asignando el tráfico a los correspondientes FEC. El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (Label-Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay. En el fondo, lo que hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la diferencia básica con el modelo IP/ATM. Al hablar de MPLS con más detalle se entenderán mejor estas peculiaridades.

El algoritmo de Intercambio de Etiquetas (LSF), requiere de la clasificación de los paquetes en el punto de entrada de la red, asignando una etiqueta inicial para cada uno. En la figura 5 el conmutador de etiquetas o label switch (LS) de ingreso recibe un paquete sin etiqueta con una dirección de destino 192.4.2.1. El Conmutador chequea la tabla de ruteo longest-match y mapea el paquete hacia una FEC 192.4/16.

El conmutador de etiquetas de ingreso o de borde le asigna entonces una etiqueta (con el valor 5) al paquete y lo envía al siguiente salto (hop) del LSP.

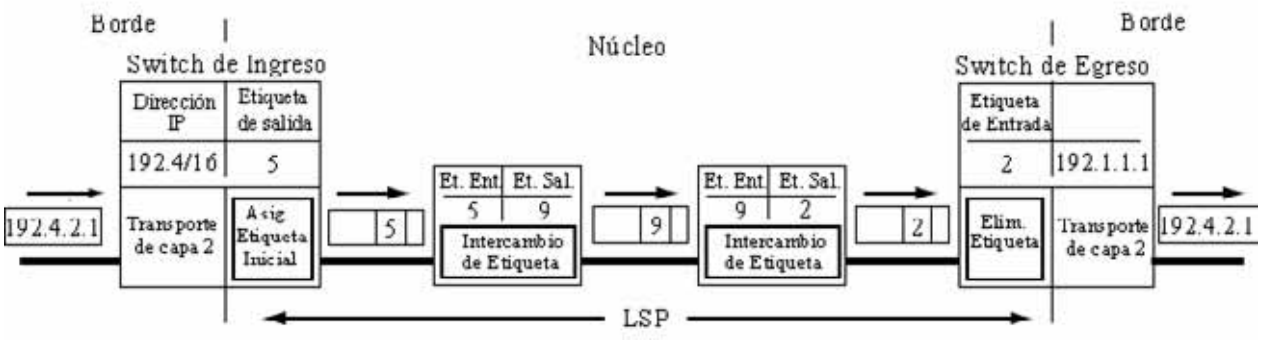

Figura 5.- Esquema de operación del algoritmo LSF. [6]

Un LSP es funcionalmente equivalente a un circuito virtual debido a que define las trayectorias de ingreso y egreso que van a ser seguidos por todos los paquetes que son asignados a una FEC específica.

En el núcleo de la red, los LS ignoran el encabezado del tipo capa de red y simplemente envían el paquete usando el algoritmo LFS. Cuando un paquete etiquetado llega a un conmutador, la componente de envío usa en número de puerto de entrada y la etiqueta, para ejecutar la búsqueda de concordancia exacta de su tabla de envío. Cuando esta concordancia es encontrada, la componente de envío recupera de la tabla de envió la etiqueta de salida, la interfase de salida, y la dirección del siguiente hop. La componente de envío intercambia o reemplaza entonces la etiqueta de entrada con la salida, y direcciona el paquete a la interfase de salida que se encarga de su transmisión al siguiente hop dentro del LSP.

CAPITULO III.- “DESCRIPCIÓN ESTRUCTURAL Y OPERACIONAL DEL MPLS”

3.1 Fundamentos de MPLS

El Multiprotocolo de conmutación por etiquetas (MPLS) es una solución versátil que surge de la evolución de la conmutación multicapas, y que confronta los principales problemas que presentan las redes de información de nuestros días: velocidad, escalabilidad, manejo de Calidad-de-Servicio (QoS), clase del servicio (CoS) e ingeniería de tráfico [9]. En este capítulo se presentan sus principales características, su arquitectura y su modo de operación.

La mayoría de los protocolos de enrutamiento desarrollados en la actualidad están basados en algoritmos diseñados para obtener el camino mas corto para el recorrido del paquete por la red y no toman en cuenta parámetros adicionales como son retardo, jitter, y congestión de tráfico, los cuales pueden afectar el desempeño de la red, por lo que la ingeniería de tráfico es un reto para los administradores de redes.

Examinando el viaje de un paquete donde se utiliza IP convencional, el cual viaja de un enrutador al siguiente, cada enrutador toma una decisión independiente del envío para ese paquete, lo que quiere decir que cada enrutador analiza el encabezado del paquete, asigna un FEC y corre un algoritmo de enrutamiento.

En MPLS la asignación de un paquete particular a un FEC particular se hace solo una vez y esto es cuando el paquete entra en la red MPLS. Aquí se le asigna a cada paquete (flujo de datos entrantes) una etiqueta FEC. Una vez que los paquetes son etiquetados por el enrutador de entrada, éste es enviado dentro de la red MPLS; en los enrutadores siguientes no hay un análisis del encabezado de la capa de red, y en lugar de esto, la etiqueta es utilizada como un índice en una tabla para especificar el siguiente salto enrutador y una nueva etiqueta (en cada salto se sustituye la etiqueta, de aquí el

término label switching). Esto trae una serie de ventajas en comparación con el enrutamiento convencional.

Las principales diferencias entre enrutamiento convencional y conmutación de etiquetas son:

	Enrutamiento Convencional	**Conmutación de Etiquetas**
Análisis completo del encabezado IP	Se realiza en cada nodo	Se realiza solo una vez en la periferia de la red, cuando la etiqueta es asignada.
Soporte de Unicast y Multicast	Requiere múltiples algoritmos de envío complejos	Se requiere solo un algoritmo de envío.
Decisiones de Enrutamiento	Se basa solo en direcciones	Se puede basar en un otros parámetros como son QoS, membresía a VPN, etc.

Tabla 1.- Comparación entre enrutamiento convencional y conmutación de etiquetas.

La adición del envío de paquetes basado en etiquetas complementa el enrutamiento convencional pero no lo reemplaza.

MPLS es un trabajo realizado y especificado por la Internet Engineering Task Force (IETF) que da los parámetros para la eficiente designación de ruteo, envío y conmutación de tráfico que fluye por la red [2]. MPLS realiza las siguientes funciones:

- Permite especificar mecanismos para la administración de flujos de tráfico de diferentes tipos (Ej.: flujos entre diferente hardware, diferentes máquinas, etc.).

- Permanece independiente de los protocolos de capa 2 y de capa 3.

- Dispone de medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes.

- Tiene interfaces con protocolos de ruteo existentes como el Resource ReSerVation Protocol (RSVP), Border Gateway protocol (BGP) y el Open Shortest Path First (OSPF).

- Soporta los protocolos de la capa de enlace usados tradicionalmente para IP. Además opera perfectamente sobre ATM y Frame Relay, dado el parecido en el mecanismo de transporte y conmutación.

- Diferentes tipos de tráfico requieren diferentes características de servicio, las cuales deben de ser garantizadas a lo largo de todo el camino a través de la red. MPLS permite la creación de caminos LSP (Label Switched Paths) con características de servicios diferentes.

Se le llama “Multiprotocolo” porque sus técnicas son aplicables a cualquier protocolo de capa 3 (Red). Algunos de los siguientes conceptos ya han sido definidos, pero se recalcarán para adecuarse a esta tecnología y comprender exactamente todo contexto del MPLS.

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen hacia un solo sentido el tráfico en cada punto de entrada a la red); para el tráfico dúplex se requieren dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Swiching Router) a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.

Las LSPs pueden ser establecidas previamente a la transmisión de datos (control-driven), o al momento en que se detecta un cierto flujo de datos (data-driven). Las etiquetas son distribuidas usando protocolos como el label distribution protocol (LDP) o el RSVP, o pueden ser sobrepuestas a protocolos de ruteo más comunes como el Border Gateway Protocol (BGP) o el OSPF. Cada paquete encapsula y acarrea las etiquetas a través de su paso por la trayectoria. La conmutación se efectúa a altas velocidades, debido a que las etiquetas son de una longitud fija, son insertadas al principio del paquete, y pueden ser manejadas por hardware para conmutar rápidamente los paquetes entre los enlaces correspondientes.

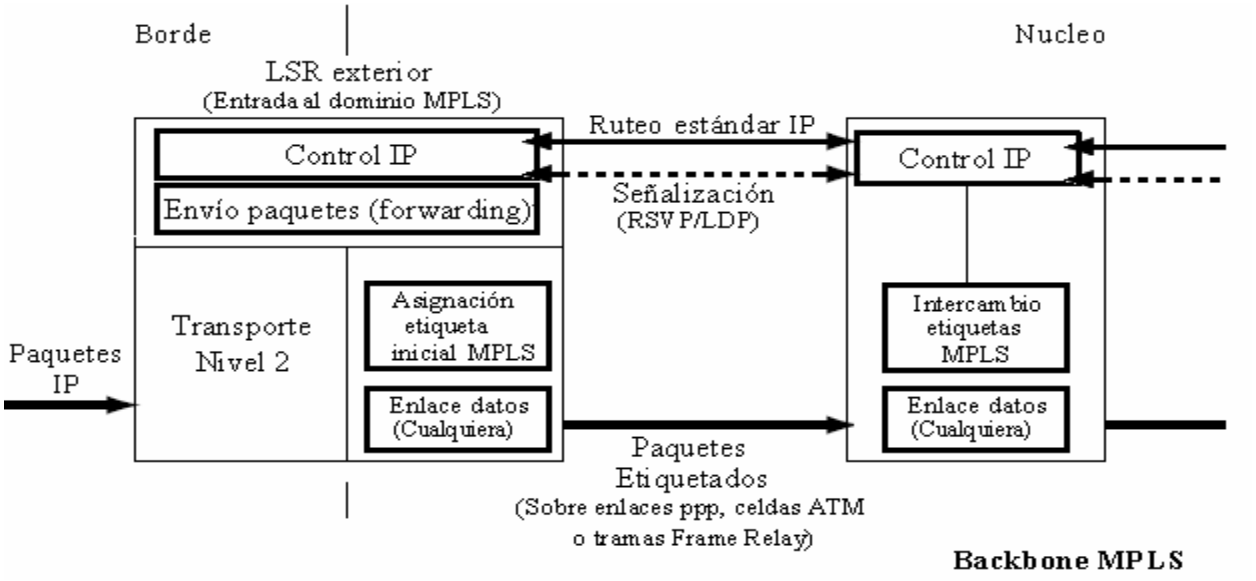

Figura 6.- Esquema funcional del MPLS.

En la figura 6 se puede ver la funcionalidad del MPLS. Compárese con los esquemas vistos anteriormente en las figuras 3 y 4 para observar las analogías y diferencias. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (forwarding).

3.2 Definición y Arquitectura del sistema MPLS

3.2.1 Routers MPLS.

Los dispositivos que participan en los mecanismos del protocolo MPLS, pueden ser clasificados en ruteadores de etiqueta de borde o label edge routers (LERs), y en ruteadores de conmutación de etiquetas o label switching routers (LSRs).

Los LSR (Label Switched Router).- son los que representan el núcleo de la red (backbone), los LSR son Router de gran velocidad en el núcleo de la red MPLS. Sus principales funciones son: participar en el establecimiento de los circuitos extremo-extremo de la red o LSPs (Label Switched Path) usando un protocolo de señalización apropiado y conmutar rápidamente el tráfico de datos entre los caminos establecidos.

Los LER (Label Edge Router).- son dispositivos que operan en el borde de una red de acceso hacia una red MPLS. Un LER soporta múltiples puertos conectados a diferentes tipos de redes (frame relay, ATM, y Ethernet); y se encarga, en el ingreso de establecer una LSP para el tráfico en uso y de enviar este tráfico hacia la red MPLS, usando el protocolo o mecanismo de señalización de etiquetas, y en el egreso de distribuir de nuevo el tráfico hacia la red de acceso que corresponda. El la figura 7 se puede observar un esquema básico de una red MPLS.

El LER juega un papel muy importante en la asignación y remoción de etiquetas que se aplica al tráfico que entra y sale de una red MPLS, por ende los LERs se clasifican en nodos de entrada (ingress node) y nodos de salida (egress node) respectivamente.

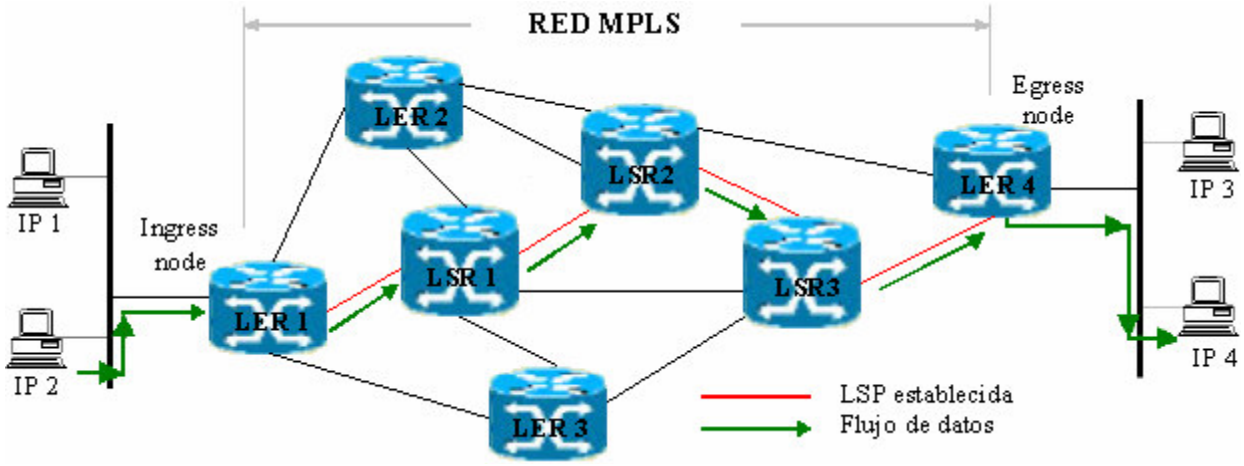

Figura 7.- Arquitectura de una red MPLS.

Un LSR puede tener dos tratamientos a un paquete que recibe. Cuando se encuentra con un paquete no etiquetado, el ruteo convencional usa un mapeo FEC-to-NHLFE (FTN) para enviar estos paquetes. Cuando se trata de un paquete etiquetado, el protocolo de distribución de etiquetas usa un mapeo Label-to-NHLFE (ILM) para enviar estos paquetes.

Una NHLFE (Next Hop Label Forwarding Entry).- es una entrada a una tabla de envío en la que se indica la etiqueta del siguiente hop. Por lo tanto, cuando un paquete entra a una red MPLS, se le asigna un determinado FEC.

Una clase de envío equivalente o forwarding equivalence class (FEC).- es una representación de un grupo de paquetes que comparten los mismos requerimientos para su transporte; todos los paquetes de este grupo tienen el mismo trato en la ruta hacia su destino. Al contrario de lo que pasa en el tradicional envío de paquetes en IP, en MPLS, la asignación de un paquete a una FEC en particular se realiza solo una vez, en el momento en el que paquete entra a la red. La definición de una FEC se basa en los requerimientos de servicio que posea un conjunto de paquetes dado, o simplemente por el prefijo de una dirección IP. Cada LSR construye una tabla para especificar que paquete debe ser enviado; esta tabla, llamada base de información de etiquetas (LIB),

la clase FEC a la cual se asigna el paquete se codifica como un valor corto de longitud corta y fija conocido como **etiqueta.**

Esta **etiqueta** es usada por los conmutadores de la red para encaminar el paquete hacia su siguiente nodo. Cuando un paquete se envía a su siguiente router, la etiqueta es enviada con él. La etiqueta se usa como un índice en la tabla que especifica el próximo salto y una nueva etiqueta. La etiqueta vieja es sustituida por la nueva, y el paquete es enviado al salto siguiente, este tema es de suma relevancia para la tecnología MPLS y es por eso que se discute con mayor profundidad en el punto 3.2.3.

Pila de etiquetas.- un conjunto apilado de etiquetas que pueden circular con el paquete.

3.2.2 Tipos de LSP

MPLS provee dos opciones para establecer una LSP:

Ruteo hop-by-hop.- Cada LSR selecciona independientemente el siguiente hop para una FEC dada. Esta metodología es similar a la que se usa en redes IP. El LSR usa cualquiera de los protocolos de ruteo disponibles, como OSPF, private network to network interface (PNNI), etc.

Ruteo explícito.- El LSR de ingreso especifica la lista de nodos por la cual viaja la trayectoria explícita. Sin embargo, la ruta especificada puede ser no óptima. A lo largo de su trayectoria, los recursos deben ser reservados para asegurar una calidad de servicio para el tráfico de datos. Esto se puede realizar mediante el concepto de ingeniería de tráfico.

3.2.3 Etiquetas

Una etiqueta, en su forma más simple, identifica la trayectoria que un paquete debe seguir. Una etiqueta es acarreada o encapsulada dentro de un encabezado de Capa 2 junto con el paquete. El ruteador que recibe el paquete, examina el contenido de la etiqueta para determinar el siguiente hop. Una vez que un paquete ha sido etiquetado, el resto del viaje del paquete a través de la red se basa en conmutación de etiquetas. El valor de una etiqueta es estrictamente de significado local, es decir, que pertenecen únicamente a saltos entre LSRs.

El primer proceso al que se somete un paquete al ingresar a un ruteador MPLS, es el de ser clasificado como una FEC nueva o una ya existente, y es entonces cuando se le asigna una etiqueta al paquete. El valor de las etiquetas se deriva de valores entregados por los protocolos de Capa 2. Para protocolos de capa de enlace de datos (como frame relay y ATM), se pueden emplear los identificadores de capa 2 directamente como etiquetas, los DLCIs en el caso de redes frame-relay, o los VPIs/VCIs en el caso de redes ATM. Entonces el envío de los paquetes se basa en el valor de estas etiquetas. La Figura 8 muestra el formato genérico de un encabezado MPLS o también llamado shim header, sus campos y como se interpone a los encabezados de las demás capas del modelo OSI [4].

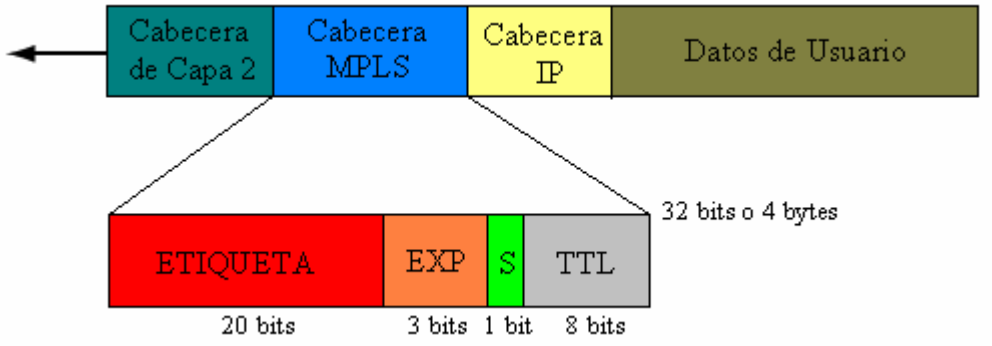

Figura 8- Estructura o formato de la cabecera genérica MPLS.

El shim header de la figura 3.3.1 se interpone entre los encabezados de capa 2 y el encabezado IP (de capa 3), por eso su nombre: shim o calzado. El encabezado es de 32 bits y se divide en los siguientes campos:

- **Etiqueta (20-bits).-** campo de 20 bits que acarrea el valor de la etiqueta MPLS.

- **EXP (3-bits).-** Antes se llamaba CoS (Class of Service), ahora se considera un rango experimental. Este campo se considera para consideraciones QoS (Quality of Service).

- **S (1-bit).-** se usa para indicar si esta presente una pila de etiquetas (label stack), entonces su valor será uno. Si la etiqueta es la única presente en la pila, entonces el valor será 0.

- **TTL (8-bit).-** el campo Time To Live provee funcionalidad IP TTL. Se usa para indicar el número de nodos MPLS por los que el paquete ha viajado hasta alcanzar su destino. El valor es copiado del encabezado del paquete cuando se ingresa a la LSP, y copiado de vuelta al encabezado del paquete IP cuando sale de la misma.

3.2.3.1 La Pila de etiquetas (Label Stack)

En un modelo más general, MPLS soporta la colocación de múltiples etiquetas a un solo paquete; en este caso, se soporta un diseño de ruteo jerárquico. Estas etiquetas se organizan en una pila o “stack” con una forma last-in, first-out (LIFO), y forma la llamada pila de etiquetas o label stack. El principal empleo de la pila de etiquetas se tiene cuando se emplea una operación MPLS llamada Tunneling.

3.2.3.2 Uniones a Etiquetas.

Las etiquetas son enlazadas a una FEC como resultado de algún evento o política que indica la necesidad por dicha etiqueta. Estos eventos de unión pueden ser divididos en dos categorías:

- **Uniones Data-Driven.-** ocurre cuando el tráfico comienza a fluir, éste es sometido al LSR y es reconocido como un candidato a label switching (usa la recepción de un paquete para disparar el proceso de asignación y distribución de etiquetas). Las uniones a etiquetas son establecidas sólo cuando son necesitadas y son asignadas a flujos individuales de tráfico IP, y no a paquetes individuales.

- **Uniones Control-Driven.-** se establecen como resultado de la actividad del plano de control y son independientes del flujo de datos. Las uniones pueden ser establecidas como respuesta a actualizaciones de ruteo (usa procesamiento de protocolos de ruteo como OSPF y BGP), o por la recepción de mensajes RSVP (usa procesamiento de control de tráfico basado en peticiones).

3.2.3.3 Distribución de Etiquetas.

En cuanto al proceso de distribución de etiquetas, se plantean conceptos que indican la dirección en que éste ocurre: upstream y downstrem. Por ejemplo: tenemos dos LSRs, R1 y R2, y estos concuerdan en atar la etiqueta L a la FEC Z, para paquetes mandados de R1 a R2. Entonces se dice que con respecto a esta unión, R1 es el LSR upstream y R2 es el LSR downstream. Cuando se dice que un nodo es upstream y otro es downstream con respecto a una unión, significa “únicamente” que etiqueta en particular representa a una FEC en paquetes que viajan del nodo upstream al nodo downstream (significancia local de la etiqueta). Esto “no” implica que todos los paquetes de tal FEC tengan que ser necesariamente ruteados del nodo upstream al nodo downstream [10].

La arquitectura MPLS no reconoce solamente a un método de señalización para la distribución de etiquetas. Protocolos existentes han sido extendidos, de manera que la información de etiquetas pueda ser "cargada a cuestas" dentro de los contenidos del protocolos (por ejemplo BGP, o túneles RSVP). El IETF ha definido en paralelo con la arquitectura MPLS, un nuevo protocolo conocido como el Protocolo de Distribución de Etiquetas (LDP), para un explícito manejo y señalización del espacio de etiqueta. También se han definido extensiones al protocolo LDP base, para soportar ruteo explícito basado en requerimientos QoS y CoS; estas extensiones se concentran en el protocolo Constraint-Based Label Distribution Protocol (CR-LDP). Los principales protocolos existentes y sus principales características son LDP, RSVP, CR-LDP, Protocol-Independent Multicast (PIM) y BGP (en el caso de VPNs).

Es una manera de manejar tráfico dentro de una red, al agrupar tipos similares de tráfico en clases, y asignarles a cada clase una prioridad en el nivel de servicio. Este tema se verá con mayor claridad en el capitulo V.

3.2.3.4 Control de distribución de etiquetas

MPLS define dos modos de control para la distribución de etiquetas entre LSRs vecinos:

- **Control independiente**.- en este modo, un LSR reconoce una FEC en particular y toma la decisión de unir una etiqueta a la FEC independientemente de distribuir la unión a sus LSR pares.

- **Control Ordenado.-** en este modo, un LSR une una etiqueta a una FEC dada, si y solo si se trata de un LER. Es decir, que el LER o también llamado label manager, es responsable de la distribución de etiquetas.

3.2.3.5 Esquemas de distribución de etiquetas.

En la arquitectura MPLS, la decisión de unir una etiqueta en particular a una FEC en particular se realiza por el LSR que es downstream con respecto a dicha unión. Entonces el LSR downstream informa al LSR upstream de la unión. Por lo tanto las etiquetas son asignadas en tendencia downstream, y las uniones de etiquetas son distribuidas en dirección downstream a upstream [1]. Con un control ordenado, la distribución de etiquetas puede ser disparada por el uso de dos posibles escenarios o esquemas:

- **Distribución de etiquetas Downstream (no solicitada) – DOU.-** en este método se permite que un LSR distribuya las uniones de etiquetas a LSRs que no los han requerido.

- **Distribución de etiquetas Downstream-on-Demand (solicitada) – DOD.-** permite a un LSR requerir explícitamente, al siguiente hop de una FEC en particular, una unión de etiqueta para dicha FEC.

3.2.3.6 Mecanismos de Señalización.

Petición de Etiquetas (label request): usando este mecanismo, un LSR hace una petición de etiqueta a su vecino downstream, de manera que la pueda unir a una FEC específica. Este mecanismo puede ser empleado por toda la cadena de LSRs hasta el LER de egreso.

Mapeo de Etiquetas (label mapping): En respuesta a una petición de etiqueta, un LSR downstream entonces manda (mapea) una etiqueta al LSR upstream correspondiente, usando este mecanismo de mapeo.

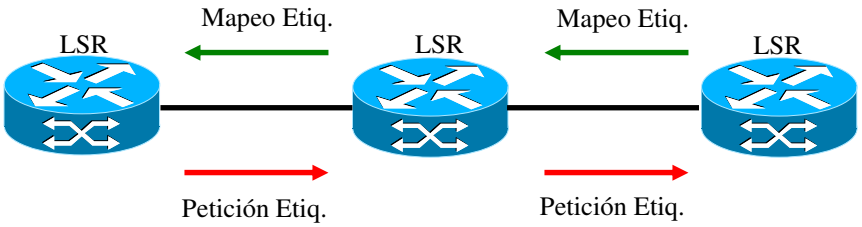

Figura 9.- Mecanismos de Señalización.

3.2.3.7 Proceso de Envío en MPLS y tablas que lo asisten.

Un ruteador MPLS tiene como primer obligación, el procesar paquetes con etiquetas entrantes. A veces a esta información se le llama tabla cross-connect (de interconexión), o en términos más adecuados y usados se le llama tabla NHLFE (Next Hop Label Forwarding Entry). Una tabla de este tipo se utiliza para el envío de paquetes etiquetados.

La principal ventaja de usar estas tablas en vez del tradicional ruteo, es que esta información puede ser procesada como datos de tipo Capa 2, donde el procesamiento es considerablemente más rápido que el ruteo.

La tabla NHFLE esta formada principalmente por todas las etiquetas que pueden ser encapsuladas dentro de los paquetes. Cada NHLFE contiene: el siguiente salto (next hop) del paquete, y la operación que la pila de etiquetas debe ejecutar, que es la siguiente:

- Reemplazar la etiqueta que se encuentra primera en la pila con una nueva etiqueta específica

- Ejecutar un “pop” en la pila.

- Repite el paso 1, y después ejecuta un “push” de una o varias nuevas etiquetas en la pila.

Después de ejecutar el pop en la pila, la etiqueta obtenida se agrega al paquete, y es entonces cuando el paquete es enviado al siguiente hop por medio de la interfase de salida.

Como la NHLFE se encuentra en la interfase de transmisión, la tabla no necesita almacenar información de la interfase de salida.

La estructura de datos (tabla) con la que un LSR interpreta etiquetas entrantes es llamada Mapa de Etiquetas Entrantes o Incomig Label Map (ILM). Una tabla ILM se forma de todas las etiquetas entrantes que un LSR o LER de egreso puede reconocer. El contenido de cada entrada ILM es: etiqueta, código de operación, FEC y un campo opcional que contiene un enlace a la estructura de salida utilizada para el envío de los paquetes (NHLFE). Cada interfase lógica del LSR almacena su propia tabla ILM.

En el caso de un LER de ingreso, existe una estructura que tiene el propósito de ayudarle al ruteador a decidir que etiquetas agregar a un paquete en particular. Esta estructura es llamada FEC-to-NHLFE (FTN), es decir un mapeo de cada FEC a un conjunto de NHLFEs. Se usa para enviar paquetes que llegan no etiquetados, y que van a serlo antes de ser enviados. Una entrada FTN esta formada por: una FEC y una entrada NHLFE. El procesamiento general que realiza esta tabla es la siguiente:

- Decide a que FEC pertenece un paquete.

- Encuentra la FEC dentro de la tabla FTN.

- Envía el paquete a la entrada NHLFE que corresponde a la FTN.

En resumen: un LSR usa el mapeo FTN para enviar paquetes no etiquetados, y usa mapeo ILM cuando se trata de enviar paquetes etiquetados.

En las Figuras 10 y 11 se muestra un ejemplo gráfico de cómo un LSR usa la tabla NHLFE para enviar paquetes a través de la LSP que va de LER1 a LER2. En la figura 10 se puede observar la dirección del mapeo, que como se ha dicho, se realiza por los LSPs downstream en dirección upstream. LER2 funciona como label manager, ya que se encarga de la requisición de etiquetas.

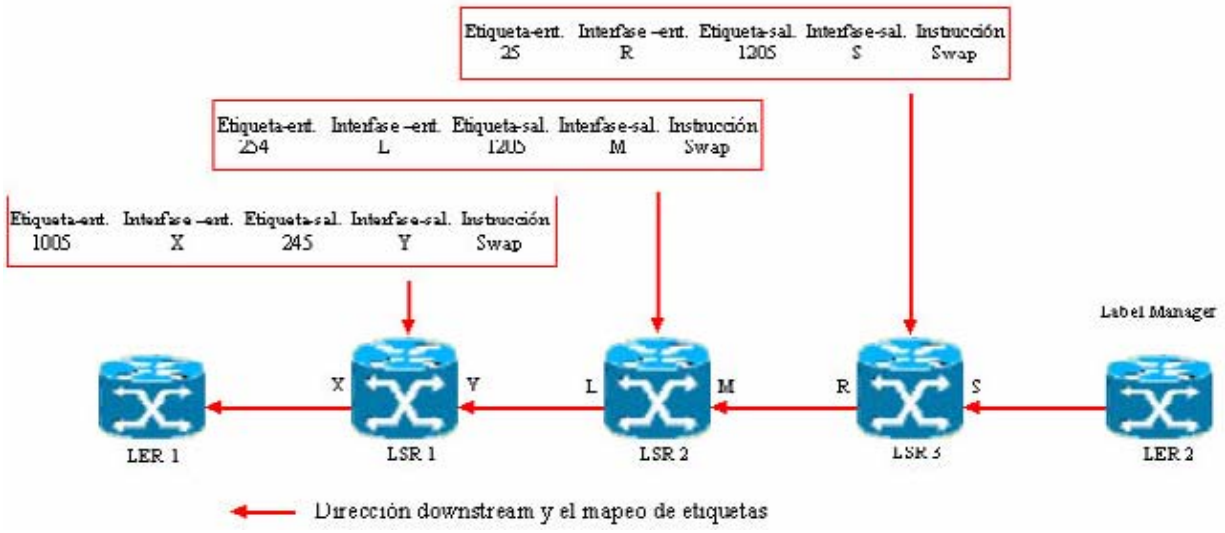

Figura 10.- Trayectoria de LSRs con tablas NHLFE [10].

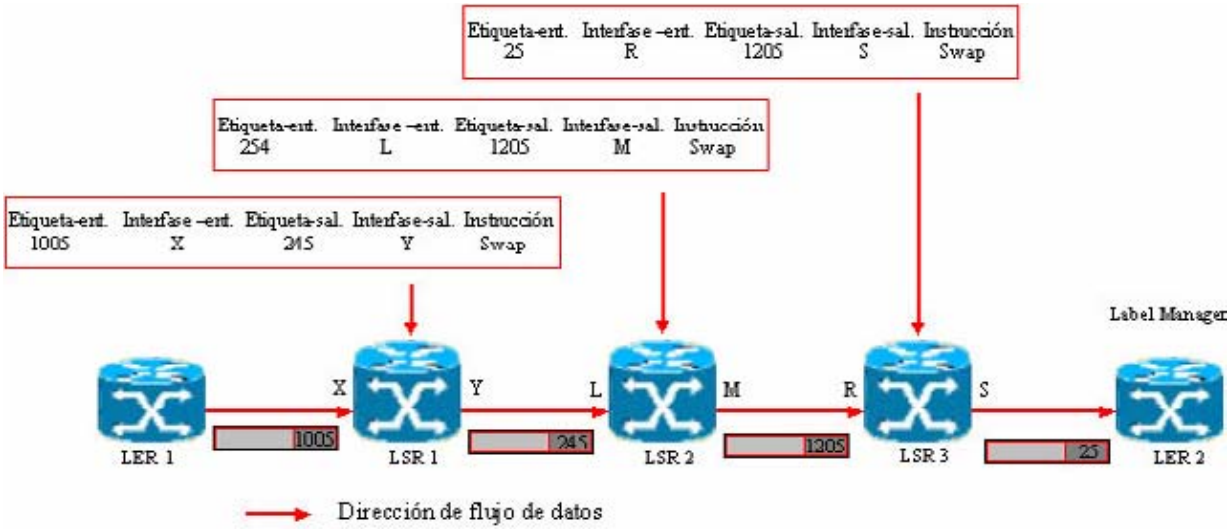

Figura 11.- Flujo de datos en dirección del mecanismo de petición [10].

3.2.3.8 Fusión de etiquetas (Label Merging).

Los flujos de tráfico entrantes a un ruteador provenientes de diferentes interfaces, pueden ser fusionados y conmutados usando una etiqueta en común, si y solo si están viajando rumbo a un mismo destino. Esto es conocido como una fusión de flujos o agregación de flujos.

3.2.3.9 Retención de etiquetas.

La arquitectura MPLS [10] define el tratamiento para uniones FEC/etiquetas en LSRs que no son el siguiente hop de una FEC en particular. Se definen dos modos:

- **Conservativo.**- en este modo, las uniones FEC/etiqueta recibidas por LSRs que no son el siguiente hop dentro de una FEC en particular son descartadas.

- **Liberal.-** en este modo, las uniones recibidas por LSRs que no son el siguiente hop de la FEC son retenidas.

3.3 Operación del MPLS.

Los paquetes que viajan a través de una red MPLS, en general, deben seguir los siguientes pasos:

- Creación y Distribución de etiquetas.
- Creación de tablas en cada LSR.
- Creación de LSP.
- Agregar etiquetas a los paquetes con la información de la tabla.
- Envío de paquetes.

En MPLS, no todo el tráfico es necesariamente transportado por la misma trayectoria. Dependiendo de las características de ingeniería de tráfico, se pueden crear diferentes LSPs para paquetes que tengan diferentes requerimientos QoS. En la figura 12 tenemos una red MPLS con cuatro LERs y tres LSRs, donde LER 1 es el de ingreso y LER 3 el de egreso.

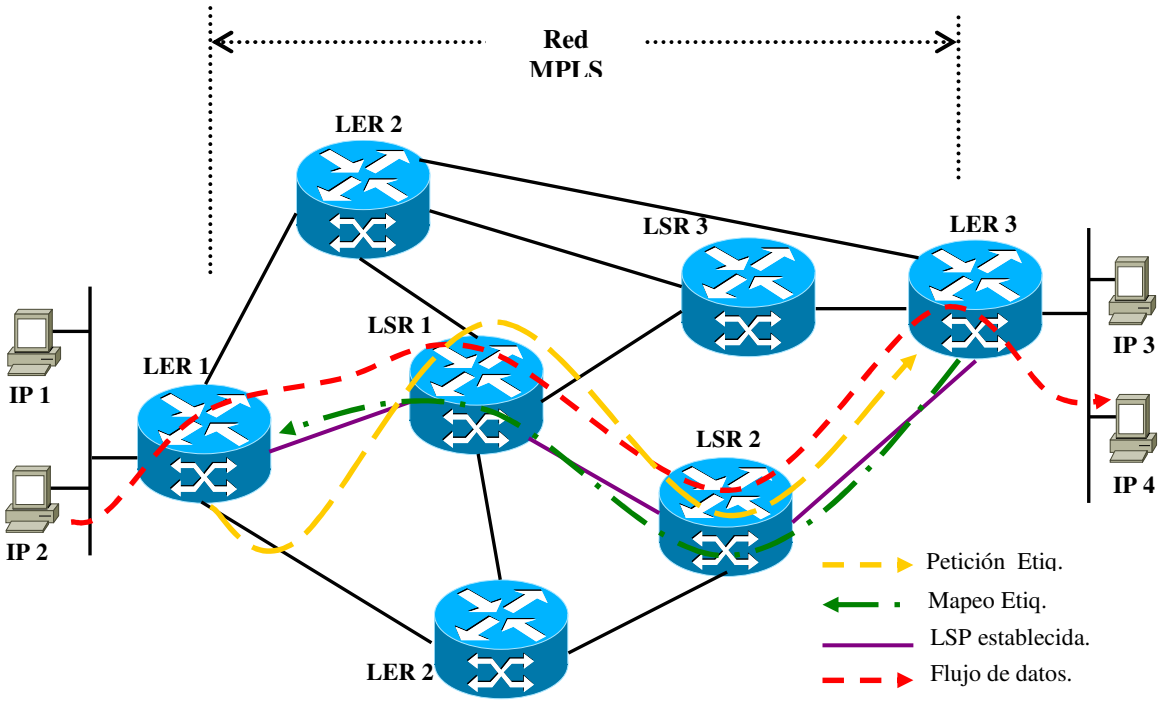

Figura 12.- Esquema de Operación de MPLS.

A continuación se especifica paso a paso las operaciones MPLS, que se realizan con respecto a un paquete que entra al dominio MPLS, esta descripción se realizará con respecto a la figura 12.

3.3.1 Creación de etiquetas y distribución de etiquetas

- Antes de que el tráfico empiece a fluir, los LSRs toman decisiones para unir una etiqueta a una FEC, y construir sus tablas.

- Con LDP, los routers downstream inician la distribución de etiquetas y de las uniones etiqueta/FEC.

- También LDP realiza las negociaciones de las características relacionadas con tráfico y de las capacidades MPLS.

- Se usa un protocolo de transporte ordenado y confiable como protocolo de señalización. El LDP usa TCP.

3.3.2 Creación de Tablas

- Cuando un LSR recibe las uniones a etiquetas crea entradas para la base de información de etiquetas (LIB). Los contenidos de la LIB especifican el mapeo entre una etiqueta y una FEC.

- El mapeo entre la tabla de puertos y etiquetas de entrada con la tabla de puertos y etiquetas d e salida.

- Las entradas son actualizadas cada vez que se efectúa una renegociación de las uniones a etiquetas.

3.3.3 Creación de la LSP

- Como se puede ver en la figura por la línea morada, las LSPs son creadas en sentido inverso de la creación de entradas LIB.

3.3.4 Inserción de etiquetas y chequeo de tablas

- El LER de ingreso usa la tabla LIB para encontrar el siguiente hop, y hace una petición de una etiqueta para una FEC en particular.

- Los LSRs subsecuentes solo usan la etiqueta para encontrar el siguiente hop.

- Una vez que un paquete llega al LER de egreso, la etiqueta es removida y el paquete es entregado a su destino.

3.3.5 Envío de paquetes

- Con referencia en la Figura 12 examinamos la trayectoria creada para los paquetes que viajan de LER1 a LER3, a través de LSR1 y LSR2.

- LER1 puede que no tenga ninguna etiqueta disponible, ya que es el primer request que se realizará. Así que lo que tiene que hacer el nodo es encontrar el siguiente nodo usando el algoritmo logest address match. Entonces especifica que LSR1 es su siguiente hop.

- LER1 iniciará entonces el request de etiqueta hacia LSR1. Entonces el request se propagará por la trayectoria en dirección a LER3 (egreso), como se observa en la figura.

- LER3 que funciona como manager de etiquetas, distribuirá las etiquetas en dirección upstream, pasando por cada nodo de la trayectoria. Es así como el protocolo LDP (u otro de los que se describen en el capitulo IV) realiza el establecimiento de trayectoria. LER1 insertará la etiqueta y enviará el paquete hacia LSR1.

- Cada LSR subsiguiente realizará el envío de paquetes realizando un intercambio de etiquetas (label swapping). Cuando el paquete llega a LER3, entonces le será retirada la etiqueta (pop), ya que el paquete saldrá del dominio MPLS y será entregado a su destino.

- El camino que siguen los paquetes desde IP2 hasta IP4 se observa en la Figura 12

La siguiente Tabla 3.2.2 muestra un ejemplo de la base de información (LIB) que se crea en un LSR para ayudar a la distribución de etiquetas y envío de paquetes.

Puerto de entrada	Etiqueta de entrada	Puerto de salida	Etiqueta de salida
3	2005	5	23
5	125	7	1005
6	10	2	9

Tabla 2- Ejemplo de una tabla LIB.

Si consideramos un ejemplo en particular, se comprende mejor la función de esta tabla. Tenemos tres tipos de flujos diferentes pasando por un LSR en particular, el primero se trata de una transferencia regular de información entre servidores (por ejemplo FTP), el segundo se trata de datos de voz, y el tercero es un flujo de video (estos dos últimos tipos de flujos generalmente requieren de la implementación de ingeniería de tráfico para su mejor transmisión). Cada flujo es asignado a una FEC en particular, ya que cada uno debe ser tratado de una manera en especial (ancho de banda, QoS, etc.).El mapeo asociado con cada flujo corresponde a las etiquetas 2005, 125 y 10 , con sus correspondientes puertos de entrada 3, 5 y 6. El LSR ejecuta un intercambio de etiquetas, por lo que para paquetes de la FEC1 se cambia la etiqueta 2005 por 23, para paquetes correspondientes a FEC2 se cambia 125 por 1005, y para FEC3 se cambia 10 por 9. Las interfaces de salida correspondientes para las 3 FECs son 5, 7 y 2.

Una característica única que presenta MPLS, es que puede controlar la trayectoria de un paquete sin que sea necesario que se especifiquen los ruteadores intermedios. Esto se realiza por la creación de túneles que pasen por ruteadores intermedios, los cuales pueden abarcar múltiples segmentos, se le llama tunneling.

CAPITULO IV.- “PROTOCOLO DE DISTRIBUCIÓN DE ETIQUETAS”

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por los cuales un LSR informa a otro de las uniones etiqueta/FEC que ha realizado. Dos LSRs que usan un protocolo de distribución de etiquetas para intercambiar información de las uniones, son conocidos como un par de distribución de etiquetas (label distribution peer) con respecto a la información que intercambian. Si se tiene un par de distribución de etiquetas, se puede hablar también de una adyacencia de distribución de etiquetas entre ellos [7]. Un protocolo LD también se encarga de las negociaciones en la que se busca el enganche entre dos pares LD, con el objetivo de que cada uno aprenda sobre las capacidades MPLS del otro.

Dependiendo de como se establezcan los LSP se pueden presentar diversas opciones: Si se utiliza la aproximación salto a salto (hop by hop) para el establecimiento de los LSP la IETF ha recomendado (no obligatorio) el uso del protocolo LDP (label Distribution Protocol) para la asignación de etiquetas, en este caso también se pueden utilizar los protocolos RSVP y CR-LDP. Si la estrategia utilizada es la “downstream unsolicited” donde el LER de salida distribuye las etiquetas que deben ser utilizadas para alcanzar un determinado destino, la única opción disponible es LDP. Cuando la estrategia es “downstream on demand” iniciada por el LER de entrada y no se desea seguir el camino calculado paso a paso, sino que se desea utilizar el que permita definir una ruta explicita, las opciones actualmente disponibles son CR-LDP y RSVP.

4.1 Protocolo LDP (Label Distribution Protocol)

El LDP es un protocolo creado específicamente para la distribución de información concerniente a uniones FEC/etiqueta, dentro de una red MPLS. Es usado para mapear FECs a etiquetas, lo cual consecuentemente creará LSPs. Las sesiones LDP son creadas entre pares LDP de una red MPLS (pares no necesariamente adyacentes). Los pares intercambian los siguientes tipos de mensajes LSP [3]:

- **Mensajes de descubrimiento (discovery messages):** anuncian y mantienen la presencia de un LSR dentro de la red MPLS.

- **Mensajes de sesión (session messages):** establecen, mantienen y terminan sesiones entre pares LDP.

- **Mensajes de advertencia (advertisement messages):** crean, cambian y borran mapeos de etiquetas a FECs.

- **Mensajes de notificación (notification messages):** proveen de información de aviso y de información de error en la señal.

Los mensajes de descubrimiento anuncian la presencia de un LSR en la red, estos se realizan enviando el mensaje Hello periódicamente. Éste es transmitido como un paquete UDP por el puerto LDP en la dirección multicast del grupo todos los Routers de esta Subred. Cuando un LSR desea establecer una sesión con otro LSR, aprendido gracias al mensaje Hello, empleará el procedimiento de inicialización LDP sobre TCP. Si se lleva a cabo de forma correcta el procedimiento de inicialización LDP, los dos LSRs son ya pares LDP, y pueden intercambiar mensajes de anuncio.

Cuándo pedir cierta etiqueta, o anunciarla a un par, será una decisión local a cada LSR. En general, el LSR pide una etiqueta a su vecino cuando la necesita, y la anuncia cuando desea que el vecino la comience a utilizar.

El funcionamiento correcto del protocolo LDP requiere una recepción fiable y ordenada de mensajes. Para ello, se emplea el protocolo TCP para mensajes de sesión, de anuncio y de notificación. Es decir, para todo el proceso, excepto para los mensajes de descubrimiento, que viajan sobre UDP.

4.1.1 Estructura del mensaje LDP

El protocolo LDP utiliza el esquema de codificación de mensajes conocido como TLV (Tipo, Longitud, Valor), cada mensaje LDP tiene la siguiente estructura [3]:

- **U.-** Campo de un bit que indica el comportamiento en caso de recibir un mensaje desconocido. U=0 hay que responder con un mensaje de notificación al LSR origen, U=1 se ignora el mensaje y se continua procesando el PDU.

- **F.-** Campo de un bit. Este campo sólo se utiliza cuando el bit U esta en 1. Si se recibe un mensaje desconocido que debe propagarse y el bit F está en cero, este mensaje no progresa al siguiente LSR, en caso contrario sí lo hace.

- **Tipo.-** Campo de 14 bits que define el tipo de mensaje y, por lo tanto indica cómo debe ser interpretado el campo valor.

- **Longitud.-** Campo de 2 octetos que especifica la longitud del campo valor.

- **Valor.-** Campo de longitud variable que contiene la información del mensaje. La interpretación de la cadena de octetos de este campo depende del contenido del campo tipo.

4.2 RSVP (Resource reservation Protocol)

RSVP es un protocolo de señalización que permite el establecimiento y el control de los denominados Servicios Integrados. RSVP es el más complejo de todas las tecnologías de QoS, tanto para los sistemas finales como para los encaminadores de la red. También representa el mayor cambio con relación al servicio best-effort de IP, RSVP tiene el mayor nivel de calidad de servicio en términos de servicios garantizados. RSVP es un protocolo situado a nivel 3 o de transporte.

Para poder utilizar este protocolo en el entorno MPLS se le han agregado nuevas capacidades, estas se refieren a los objetos formatos de los paquetes y procedimientos necesarios para establecer los túneles LSP. Para el establecimiento de los túneles LSP el protocolo de señalización utiliza el modelo downstream on demand. Esto significa que la petición de asociación entre el FEC y una etiqueta para crear un túnel LSP es iniciada por el LSR de entrada, para lograr este objetivo hay que agregar uno objeto (LABEL_REQUEST) al mensaje del path propio de RSVP antes mencionado.

Un requisito adicional para este protocolo RSVP es que el dominio MPLS debe soportar el encaminamiento explicito (explicit routing) para facilitar la gestión de tráfico. Para lograr esto se añade el objeto (EXPLICIT_ROUTE) en los mensajes del path. Este nuevo objeto encapsula el conjunto de nodos ordenados que constituyen la ruta explícita que deben seguir los datos. Como la asignación de etiquetas se realiza desde el destino hacia el origen, en sentido contrario al flujo de datos, es necesario incrementar el mensaje resv con un objeto adicional (LABEL) capaz de transportar la nueva información requerida para este uso del protocolo. El funcionamiento de este protocolo para el establecimiento de túneles LSP se describe a continuación.

El funcionamiento de RSVP es el siguiente [7]:

- Cuando un LER de entrada al dominio MPLS (emisor) decide que necesita establecer un LSP hasta un determinado LER de salida, debe iniciar un procedimiento para establecerlo, mediante un mensaje denominado path, con su especificación de tráfico, hacia el destino o destinos. El propósito del mensaje PATH es el de marcar la ruta entre emisor y receptor además de recolectar información sobre la viabilidad de la solicitud a lo largo del camino (Cuando los LSR intermedios reciben el mensaje del path lo procesan de acuerdo con las especificaciones el protocolo y una vez reconocido que no son el extremo del FEC, transmiten el mensaje hacia el siguiente nodo de la ruta). La especificación anterior incluye los valores máximo y mínimo de ancho de banda, retardo y variación del mismo.

Cada encaminador va grabando la ruta por la que va circulando el mensaje de PATH, para que después pueda reconstruirse la ruta de vuelta. La ruta que debe seguir el LSP puede ser una ruta explícita determinada por el gestor de la red (esta ruta no puede coincidir con la calculada por los algoritmos de encaminamiento de la capa red). Al llegar el mensaje PATH al receptor o receptores, pueden medir que tipo de servicio puede soportar la red.

- Cuando el mensaje de path finalmente alcanza el LSE destino, éste procede a reservar los recursos internos, selecciona la etiqueta a utilizar para este túnel LSP y procede a propagarla hacia el anterior LSR mediante un mensaje de reserva (resv). Dicho mensaje incluye además de la especificación de tráfico recibida del emisor, la especificación requerida por el receptor, que consta del tipo de Servicio Integrado solicitado y un filtro que selecciona los paquetes con una determinada característica (por ejemplo protocolo y número de puerto) a los que se va aplicar la reserva. El identificador de sesión que utilizan los encaminadores está compuesto por el tipo de Servicio Integrado y el filtro.
- Cuando los LSRs intermedios reciben la asignación de la etiqueta con el mensaje de resv, usan el control de admisión para aceptar o no la reserva. En

caso positivo proceden a reservar los recursos internos necesarios y determinar la etiqueta a utilizar para el flujo. Una vez calculada la propagan hacia el LSR anterior de nuevo con ayuda del mensaje resv. . En caso contrario se envía un mensaje de error al emisor.

- Este proceso se repite hasta alcanzar el LSR origen donde también se realiza el proceso de reservar recursos internos, pero en este caso no es necesario asignar etiqueta y propagarla ya que se ha alcanzado el origen del FEC.

- Si el encaminador no soporta RSVP retransmite los mensajes RSVP de forma transparente. En estos enlaces no se puede garantizar la calidad de servicio, lo que implica que puede perderse la calidad de servicio extremo a extremo.

- Si el último encaminador efectúa la reserva envía un mensaje de confirmación al receptor. Cuando la sesión termina debe indicarse, para liberar los recursos de la reserva.

Se exponen, a continuación, las características más importantes de los mecanismos del protocolo RSVP:

- Las reservas no son permanentes y deben ser refrescadas periódicamente con mensajes PATH y RESV.

- Se necesita un interfaz para que las aplicaciones se comuniquen con RSVP. Las aplicaciones suministran la especificación de tráfico, inician el proceso de reserva y reciben la correspondiente notificación acerca de lo que ha ocurrido con la misma. También deben ser informadas de lo que pueda suceder a lo largo de la existencia de la sesión.
- Las reservas las efectúa el receptor, para soportar grandes y heterogéneos grupos receptores de multidifusión.

Como se ha indicado anteriormente, RSVP permite a una aplicación especificar la mayor calidad de servicio posible. El precio que hay que pagar por ello es una mayor complejidad y procesamiento, lo cual no es apropiado para muchas aplicaciones y partes de la red. Por ello se han propuesto métodos más sencillos, como el DiffServ que será descrito más adelante.

4.3 CR-LDP (Constraint-Based Routing label Distribution Protocol)

Es un encaminamiento basado en restricciones (Constraint-based routing). Esta extensión del LDP se basa en el calculo de trayectos que están sujetos a ciertas restricciones: ancho de banda, los requisitos de calidad de servicios QoS, demora (delay), variación de demora o jitter, o cualquier otro requisito asociado al trayecto que defina el operador de la red. Esta es una de las herramientas más útiles para controlar el dimensionado del tráfico y la QoS en la red que pueden ofrecer a sus clientes y/o usuarios.

Debido a ello, la IETF ha elaborado las extensiones necesarias para que el protocolo LDP pueda soportar este tipo de encaminamiento esta extensión es conocida como CR-LDP (Constraint-Based Routing label Distribution Protocol) y se ha definido expresamente para soportar el establecimiento y mantenimiento de LSP encaminados en forma explícita y las modificaciones de los LSP, pero no incluyen los algoritmos necesarios para calcular trayectos según los criterios definidos por el operador de la red [7].

Las principales limitaciones son las siguientes:

- Solo se soportan LSP´s punto a punto.
- Solo se soportan LSP´s unidireccionales.
- Sólo se soporta una única etiqueta por LSP.

4.4 Servicios Integrados (IntServ)

En 1994 la comunidad de Internet empezó a definir la Arquitectura de Servicios Integrados (Integrated Sevices Architecture, IntServ) que pretendía ampliar la arquitectura IP existente para soportar sesiones en tiempo real, manteniendo el servicio best-effort existente.

La arquitectura IntServ define un flujo como una corriente de paquetes con la dirección origen y destino, puerto origen y destino, iguales. IntServ sugiere que para dar QoS a un flujo, la red debe hacer un seguimiento del estado del flujo.

Los componentes básicos de la arquitectura IntServ son los siguientes:

- El control de tráfico, que a su vez incluye a otros tres. El primero es el control de admisión, que comprueba que existen recursos suficientes para soportar el servicio. El segundo es el clasificador de paquetes, el cual analiza los campos de direcciones y puertos para determinar la clase a laque pertenece el paquete. El tercero es el algoritmo de encolado que gestiona la transmisión de los paquetes por un enlace de salida.

- Las clases de tráfico, que ofrecen dos tipos de servicios: garantizados y de carga controlada, además del best-effort. Los primeros emulan a los circuitos dedicados, garantizando los parámetros de la especificación del tráfico del emisor. Los segundos son equivalentes al servicio best-effort en condiciones de red descargada. Suministran mejor servicio que el best-effort, pero no hay garantías como en los primeros.
- Un protocolo, para que una aplicación pida un determinado servicio a la red. El protocolo entrega la petición al control de tráfico de cada encaminador, que comprobará si es viable la petición.

4.5 Servicios diferenciados (DiffServ)

Los servicios diferenciados (Differenciated Services, DiffServ) son una forma sencilla y tosca de clasificar los servicios de las aplicaciones, aunque su simplicidad no da idea de su potencia y flexibilidad. Es una tecnología que trabaja a nivel 3.

Varios factores condujeron a su diseño, en primer lugar debía ser escalable, para ello se utiliza la agregación de varias sesiones en una que recibe el mismo tratamiento. También debía poder ser utilizada con todas las aplicaciones y no requerir un protocolo especial de control o un nuevo interfaz de programación como RSVP. Además hay que tener en cuenta, que los grandes avances en las velocidades de transmisión no aconsejan que los encaminadores centrales sean cargados con el seguimiento de cada sesión. Es más eficiente y escalable hacer un seguimiento de cada tipo de servicio.

El funcionamiento de DiffServ se basa en clasificar las sesiones a la entrada de la red en relación con un determinado servicio y después aplicarle el correspondiente tratamiento dentro de la red.

La clasificación a la entrada en la red está basada en el análisis de uno o varios campos de la cabecera del paquete. Después el paquete se marca, en algún campo de la cabecera, como perteneciente a una determinada clase de servicio.

Los encaminadores centrales sólo examinan el campo donde se marcó el paquete y le dan el tratamiento correspondiente a esa clase de servicio. Finalmente, antes de salir de la red se suprime la marca.

Al tipo de servicio se le denomina comportamiento del nodo (Per-Hop Behavior, PHB), que será el tratamiento que tenga cada paquete en cada nodo de la red. Un comportamiento agregado (Behavior Aggregate) se define para un grupo de paquetes

con el mismo CPDS. Un mismo PHB o servicio, es aplicado a cada comportamiento agregado dentro de la red.

Aunque hay más posibilidades, se han definido dos tipos de niveles de servicios:

- Reenvío rápido (Expedited Forwarding, EF), que tiene pérdidas, retardo y variación del mismo mínimos. Es un servicio similar a las líneas alquiladas. El tráfico que exceda el perfil declarado será descartado. Para ello el tráfico es conformado en los encaminadores de acceso, para no superar la máxima velocidad. Por supuesto esta velocidad debe ser menor que la mínima velocidad de los enlaces de salida de cada encaminador en la red. El EF PHB utiliza un solo bit CPDS para indicar que el paquete debe ser colocado en la cola de máxima prioridad.

- Reenvío asegurado (Assured Forwarding, AF), tiene 4 clases con 3 procedimientos en cada clase que determinan como descartar tráfico. Doce combinaciones CPDS definen las clases AF de precedencia a la hora de tirar los paquetes. Cuando hay congestión en un encaminador los paquetes con mayor precedencia son desechados primero. Las cuatro clases AF no definen un ancho de banda o retardo específico sino que la clase 1 es distinta de la clase 2 y así sucesivamente. El tráfico AF en exceso no es entregado con la misma probabilidad que el tráfico cumplidor, es decir puede ser degradado pero no necesariamente descartado.

DiffServ asume la existencia de un acuerdo entre el usuario y la red, en el nivel de servicio (Service Level Agreement SLA). El SLA establece el perfil del tráfico (ancho de banda, retardo, jitter y tasa de pérdidas) y la política (tiempo de disponibilidad, penalizaciones, etc.). Se espera que el tráfico sea conformado y espaciado en la entrada en la red con arreglo al SLA y cualquier tráfico no conforme no tendrá calidad de servicio.

DiffServ ha sido escogida como la tecnología para soportar la QoS en la Internet2 en la iniciativa conocida como QBone. Las razones que han llevado a esta decisión son las siguientes:

- Flexibilidad, para implementar los diferentes requerimientos de servicios de las aplicaciones avanzadas.

- Escalabilidad, al liberar al núcleo de la red de los procesos más complejos.

- Interoperabilidad, al estandarizar el comportamiento por nodo, más que servicios particulares o algoritmos de encolado.

CAPITULO V.- "APLICACIONES MPLS"

En este capitulo se abarca una de las mayores potencialidades que presenta MPLS, que corresponde a las aplicaciones de esta tecnología. Consecuentemente son tres las aplicaciones principales de MPLS que son las siguientes [2]:

- Ingeniería de tráfico.
- Calidad de servicio (QoS) y Clases de servicios (CoS).
- Redes virtuales privadas (VPNs).

5.1 Ingeniería de Tráfico

La Ingeniería de Tráfico (traffic engineering, TE) comprende a los aspectos necesarios para lograr la optimización del desempeño de una red en estado operativo. El principal objetivo de la TE es facilitar operaciones de red fiables y eficientes en tanto se optimiza simultáneamente el uso de los recursos disponibles y el rendimiento de tráfico.

En general la TE comprende la aplicación de la tecnología y de los principios científicos a la medición, modelado, caracterización y control del tráfico en Internet.

Los objetivos más importantes asociados con la TE pueden ser clasificados así [1]:

- **Objetivos de funcionamiento orientados al Tráfico.-** Comprende los aspectos que mejoran la calidad de servicio de los flujos de tráfico. En redes Best effort, estos parámetros de desempeño vienen dados por minimización del retardo, minimización de pérdidas, maximización del throughput, entre otros.

- **Objetivos de funcionamiento orientados a los Recursos.-** Se refiere a los aspectos que brinden una optimización en el uso de los recursos. Adicionalmente los mecanismos de la Ingeniería de Tráfico están clasificados en dos tipos básicos, acorde a la escala de aplicación que se quiere abarcar.

- **TE Dependiente de Tiempo.-** En este caso, los algoritmos de control de tráfico son utilizados para optimizar el uso de los recursos de la red en respuesta a variaciones de tráfico medidos en una escala de tiempo muy larga.

- **TE Dependiente del Estado.-** En este caso, los algoritmos o mecanismos de control de tráfico se deben adaptar a los cambios de estado que sufre la red en forma casi instantánea.

Entendido de otra forma, se adaptan a cambios en los estados de la red que ocurren en escalas de tiempo muy cortas.

En redes tradicionales Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos).

En el esquema de la figura 13 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

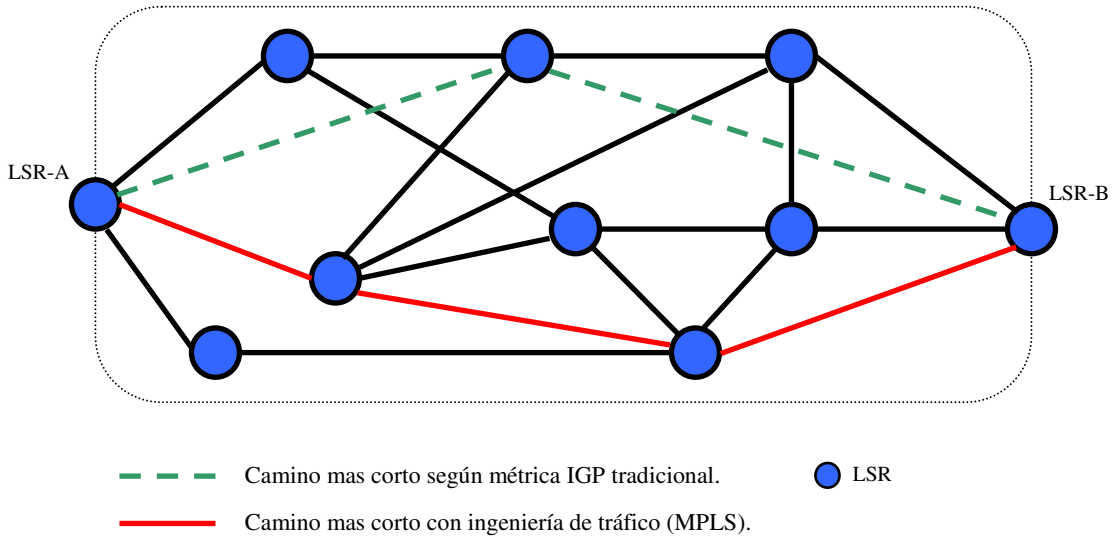

Figura 13.- Comparación de caminos IGP v/s TE [2].

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes haga aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

- Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

- Se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

5.1.1 Balanceo de carga

El Balanceo de Carga es un aspecto clave en los esquemas de TE aplicados a las redes IP. Es utilizado como un mecanismo para la asignación adaptativa de tráfico a los enlaces de salida disponibles, dicha asignación se realiza de acuerdo al estado actual de la red; el conocimiento de dicho estado puede estar basado en la utilización, retardo del paquete, pérdida del paquete, etc. Por tal razón, la eficiencia de cualquier mecanismo de balanceo de carga depende crucialmente del proceso de medidas del tráfico que ingresa a la red y se requiere una gran habilidad para controlarlo de forma precisa, dada la naturaleza dinámica del mismo.

Por regla general, las decisiones y operaciones relacionadas con el balanceo de carga se realizan en los nodos de ingreso, quienes tienen, un mejor conocimiento del tráfico que se inyecta a la red. Los nodos intermedios se encargan de realizar funciones de re-envío y en ciertos casos de recolectar información sobre el tráfico en la red y enviarla al nodo de ingreso.

El Balanceo de Carga (Load Balancing), también conocido como Compartición de Carga (Load Sharing) o División de Tráfico (Traffic Splitting) es un mecanismo importante para mejorar el funcionamiento (en aspectos de caudal, retardo, jitter y pérdidas) y las prestaciones de la red.

Un sistema de balanceo de carga comprende regularmente un Divisor de Tráfico (Traffic Splitter) y múltiples enlaces de salida (Outgoing Links), como se ve en la figura 14.

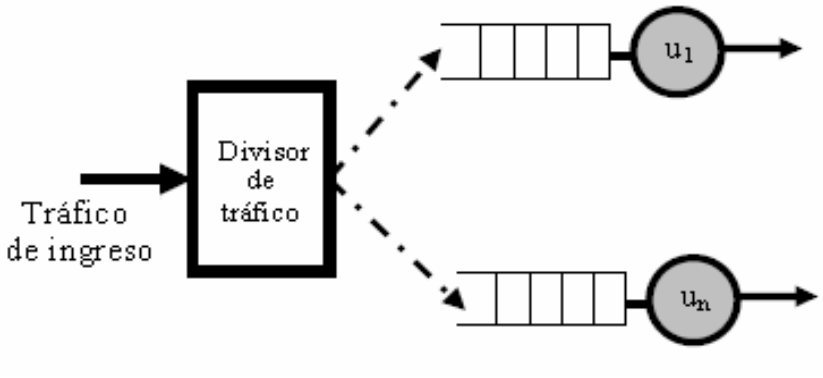

Figura 14.- Modelo básico de referencia para balaceo de carga.

De un modo más específico, un mecanismo de balanceo de carga comprenderá funcionalmente dos aspectos, como se observa en la figura 15.

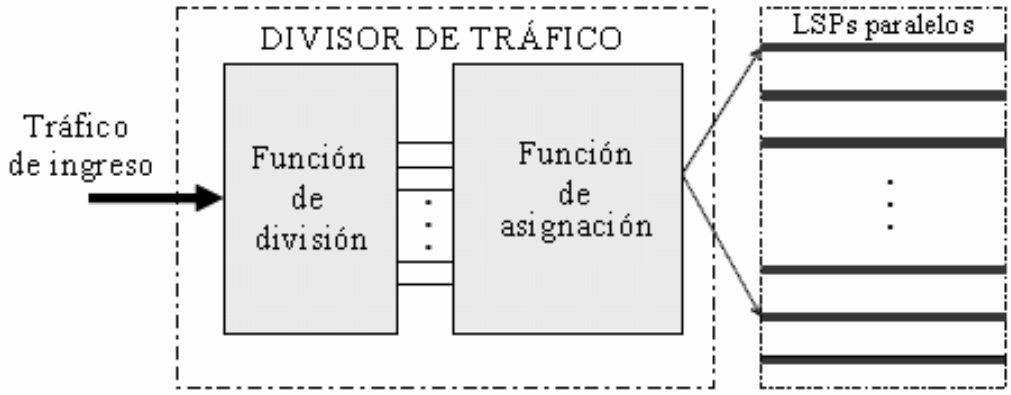

Figura 15.- Modelo funcional para balanceo de carga.

- **La función de división.-** encargada de repartir el tráfico entrante en porciones adecuadas y acorde a las capacidades de los enlaces de salida y garantizando mantener la secuencia de los paquetes.

- **La función de asignación.-** constituye la parte del mecanismo de balanceo de carga encargada de determinar a cuál LSP y en qué momento entregarle la porción de tráfico que debe transportar.

Los mecanismos de balanceo de carga son clasificados de forma aproximada en dos grupos principales:

- **Basados en Conexión.** Donde los flujos de datos son representados con un reducido número de parámetros, y las decisiones de encaminamiento y reenvío afectan a todo el flujo.

- **Basados en Paquetes.** Se aplican cuando la división de carga trabaja a nivel de paquete, la cual esta bien adaptada a la naturaleza no orientada a conexión de las redes IP.

Un buen sistema de balanceo de carga deberá ser capaz de dividir el tráfico entre múltiples enlaces de salida de forma equitativa o mediante alguna proporción predefinida.

Los requerimientos básicos que los esquemas de división de tráfico deben satisfacer para poder realizar balanceo de carga son:

- **Baja Sobrecarga.-** Los algoritmos de división de tráfico deben ser muy simples y preferiblemente no tener estados o que estos sean reducidos, pues el procesamiento de cada paquete generaría demasiada sobrecarga.

- **Alta Eficiencia.-** Una distribución de tráfico muy desigual, puede resultar en una utilización poco uniforme del enlace y en pérdida de ancho de banda.

- **Conservar el orden de los paquetes en los flujos.-** Los paquetes mal ordenados dentro de un flujo TCP pueden producir señales de congestión erróneas y hacer que se produzca una degradación del throughput.

Los algoritmos de balanceo de carga en MPLS, se desarrollan en base a que MPLS es por naturaleza una tecnología de backbone para redes IP que conectaría a muchos ISP (Internet Service Provider).

Dado que entre los ISP´s de hoy existen múltiples trayectos con el fin de garantizar un buen nivel de redundancia y tener un buen nivel de disponibilidad, los trayectos paralelos pueden ser aprovechados para realizar una división adecuada del tráfico que entra en la red y repartirlo correctamente entre todos aquellos enlaces disponibles. Ver figura 16.

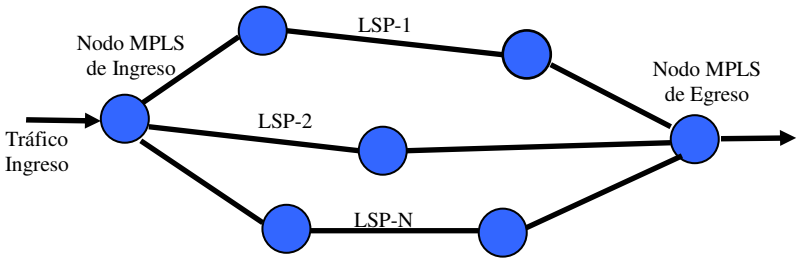

Figura 16.- Red MPLS con LSPs paralelos.

5.1.2 Algoritmos de Balanceo de Carga

Los inconvenientes presentes en las redes actuales que impiden lograr un adecuado balanceo de carga tienen relación con el algoritmo de encaminamiento que utilizan, el cual fundamentalmente es el algoritmo del Camino más Corto (Shortest Path). Con este algoritmo, cada paquete que entra en la red buscará el camino de

menor número de saltos que le permita alcanzar el destino, el cual regularmente para todos los paquetes es el mismo, así existan en la red otros caminos con mayor número de saltos pero mucho mas rápidos.

Esto degrada el funcionamiento de la red en aspectos como: la congestión que se produce sobre el enlace del camino mas corto, disminución del throughput efectivo de la red, entre otros.

Dentro de las propuestas de balanceo de carga que se pueden encontrar en la literatura, destacan las siguientes:

5.1.2.1 MATE (MPLS Adaptive Traffic Engineerin)

El objetivo principal de MATE es evitar la congestión en la red mediante el balanceo adaptativo de la carga entre múltiples trayectos, basado en medidas y análisis de la congestión.

Algunas de sus características:

- Control extremo a extremo entre los nodos de ingreso y egreso.
- No se requiere nuevo hardware o protocolo en los nodos intermedios.
- No se requiere conocer la demanda de tráfico.
- Las decisiones de optimización están basadas en la medida de congestión del trayecto.
- Mínimo re-ordenamiento de paquetes.

El diagrama funcional de MATE se representa en la Figura 17.

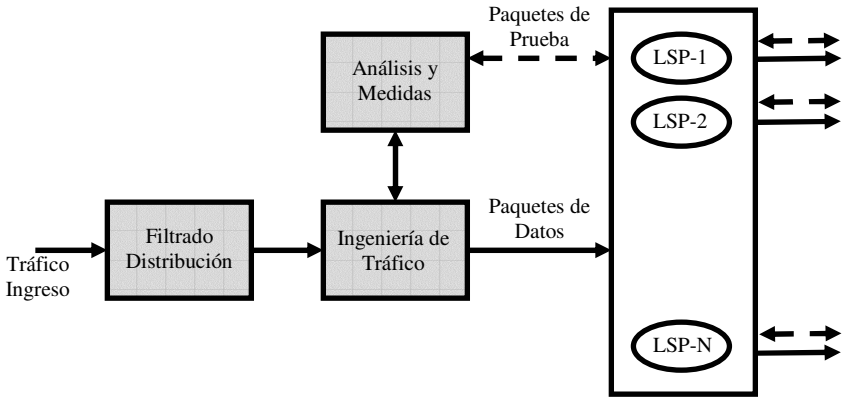

Figura 17.- Esquema funcional de MATE [2].

La red MATE define Engineered Traffic como el tráfico que requiere ser balanceado y Cross Traffic como el tráfico que ingresa a la red a través de los nodos intermedios y sobre los cuales no se tienen ningún tipo de control, figura 18.

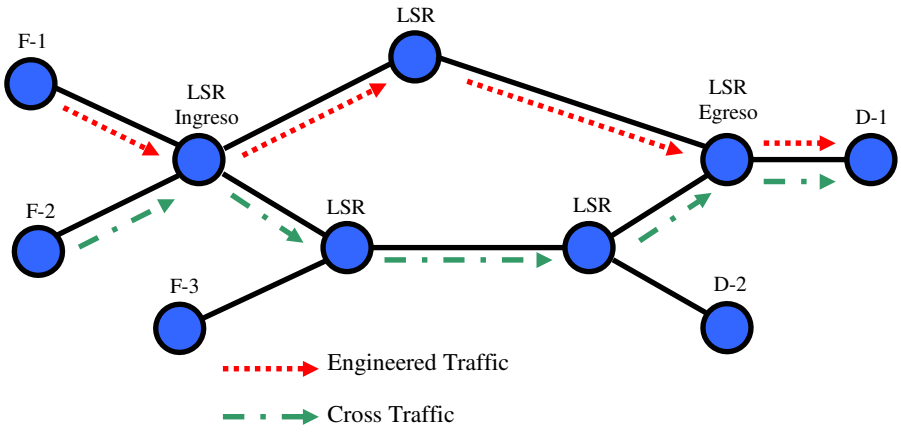

Figura 18.- Clases de tráfico definidos por MATE.

Estas funciones están ubicadas en el nodo de ingreso de la red MPLS y se describen brevemente a continuación.

- Los paquetes entrantes al nodo de ingreso de la red MPLS llegan al bloque funcional de Filtrado y Distribución, quien es el responsable de distribuir el tráfico entre los diferentes LSP´ s, de tal forma que se evite que los paquetes que llegan al destino lo hagan fuera de secuencia.

- La función de Ingeniería de Tráfico, consiste de dos fases, Monitorización y Balanceo de Carga. Es responsable de decidir cuándo y cómo se conmuta el tráfico entre los LSP´ s. Esto se realiza mediante estadísticas, las cuales son obtenidas de las medidas realizadas sobre los paquetes de prueba.

- La función de Análisis y Medidas, es responsable de obtener estadísticas de los LSP´ s (en un solo sentido) tales como el retardo y la pérdida de paquetes. Esto se logra mediante el envío periódico de paquetes de prueba desde el nodo emisor hasta el nodo receptor y la devolución posterior del mismo.

5.1.2.2 Topology-based Static Load BalancingAlgorithm (TSLB)

Este algoritmo es una mejora del camino más corto (Shortest Path). En este algoritmo, un nuevo tráfico es encaminado en primer lugar a través del camino mas corto; si dicho camino tiene la capacidad suficiente para satisfacer el ancho de banda solicitado por el nuevo tráfico el camino se establece. Si este primer camino no cumple con las necesidades del tráfico entrante se buscará el siguiente trayecto hasta encontrar un camino que satisfaga el requerimiento. Si no se encuentra un camino que cumpla con el requerimiento el algoritmo falla.

El principal inconveniente radica en que dado que las fuentes de tráfico transmiten aleatoriamente, un tráfico bajo tomará el camino mas corto aunque éste tenga una capacidad muy superior a la requerida, distribuyendo por tanto el tráfico de forma poco razonable y disminuyendo la utilización de los recursos de la red y el throughput. Ver figura 19.

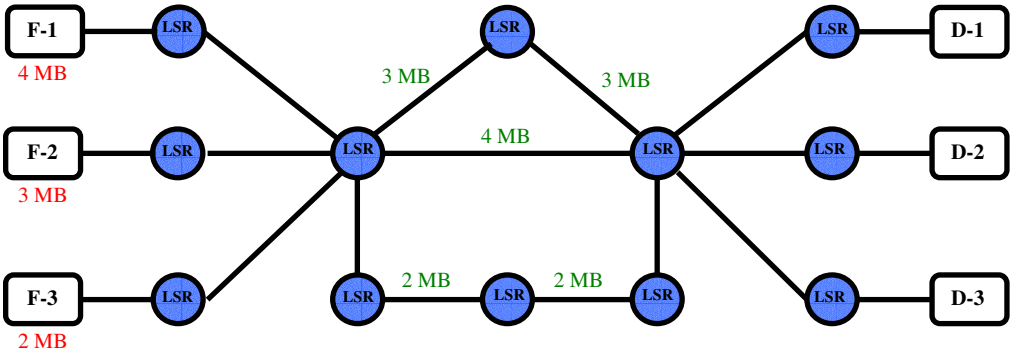

Figura 19.- Topología de referencia para los algoritmos TSLB, RSLB, DLB.

5.1.2.3 Resource-based Static Load Balancing Algorithm (RSLB)

Cuando un tráfico nuevo llega al encaminador de entrada, este seleccionará la ruta cuya capacidad disponible sea un tanto mayor a la solicitada por el nuevo flujo. Por tanto, este algoritmo podrá reservar las rutas de mayor capacidad para tráficos futuros que la requieran.

El inconveniente de este algoritmo aparece con fuentes de tráfico que puedan tener una tasa de envío inestable, fluctuando en un rango especial. Esta fluctuación en el tráfico puede conducir a pérdida de paquetes, especialmente cuando la tasa de ráfagas de la fuente excede la capacidad del enlace.

5.1.2.4 Dynamic Load Balancing Algorithm (DLB)

En este caso se parte del conocimiento que el ancho de banda de la ruta, esta dividido en: Capacidad en Uso (UB: Used Bandwidth) y Capacidad Libre (FC: Free Capacity), de tal forma que el algoritmo buscará la ruta que tenga el menor ancho de banda en uso, pero que su capacidad disponible (UB + FC) sea mayor que la solicitud de ancho de banda del tráfico entrante.

DLB toma en cuenta la topología de red y los requerimientos de ancho de banda simultáneamente. En condiciones de baja carga, los flujos de tráfico pueden ser repartidos sobre la ruta disponible mas corta y de mayor capacidad; cuando la carga de la red cambie y se torne el tráfico mas pesado, los flujos pequeños pueden ser re-encaminados a otras rutas apropiadas y así reservar los enlaces de alta capacidad para los flujos que lo requieran.

El inconveniente presentado por este algoritmo se da por el hecho de que los tiempos de reencaminamiento de los flujos previamente establecidos que se deben acomodar nuevamente deben ser muy rápidos ya que de lo contrario existirán pérdidas de información.

5.0.2.5 DYLBA (DYnamic Load Balancing Algorithm)

Es un algoritmo que implementa una técnica debúsqueda local, donde el proceso básico es la modificación de la ruta para un único LSP. La idea fundamental que utiliza es la de reencaminar eficientemente LSP´ s de los enlaces más congestionados.

Para los enlaces establecidos se definen procedimientos para monitorear su capacidad y se definen umbrales de congestión. Los LSP´ s mas congestionados son identificados por la mínima capacidad disponible en la red. Para realizar el cálculo de la ruta explícita y ejecutar el algoritmo de balanceo de carga, cada encaminador en la red necesita conocer la topología actual y las capacidades residuales de cada enlace, para

determinar e identificar los enlaces más congestionados. Se asume que cada encaminador en la red MPLS ejecuta el algoritmo Estado del Enlace (Link State) con extensiones para conocimiento de ancho de banda residual (Residual Bandwidth Advertisements).

Cuando el establecimiento de un nuevo LSP produce la detección de congestión sobre uno de los enlaces de la red (cuando solo se dispone de una cantidad x de ancho de banda residual) el algoritmo de balanceo y el proceso de reencaminamiento entran en funcionamiento.

Un parámetro crítico en el algoritmo es la definición del umbral usado para detectar los enlaces congestionados.

5.2 Calidad de servicio (QoS) y clases de servicios (CoS)

Una de las características clave de MPLS, comparado con redes tradicionales como Frame Relay y ATM, es que está diseñado para proveer servicios garantizados. Es decir, que según los requisitos de los usuarios, permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva.

MPLS esta orientada a conexión por naturaleza garantizando el tráfico IP. Mientras que QoS y clases de servicios factores fundamentales de esta tecnología, estos pueden ser implementados a través de ingeniería de tráfico. Esta capacidad permite proveer a los distintos usuarios un servicio de nivel estable (Service level Agreements, SLAs) en aspectos como: ancho de banda, tiempo de demora, y variación del mismo. Generando un valor agregado a los prestadores de servicios y proponiendo a estos últimos la migración hacia estas redes.

5.2.1 InterServ y DiffServ

Varios mecanismos son los que utiliza MPLS para dar estabilidad de QoS y CoS dentro de su red. En el modelo InterServ (Integrated Services), RSVP obtiene los requerimientos para establecer un flujo de tráfico con QoS, permitiendo a los distintos LSR las negociaciones necesarias para generar un tráfico garantizado y además parámetros o recursos como ancho de banda y latencia end to end. El modelo DiffServ (Differentiated Services) del IETF. Define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio (CoS), otorgando un servicio no necesariamente garantizado para el curso del tráfico con diferentes prioridades. Para ello se emplea el campo ToS (Type of Service), en la cabecera de paquete IP para proveer esta clasificación.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP.

De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.

Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

Mientras que InterServ ofrece ancho de banda garantizado para el tráfico, no provee escalabilidad u operabilidad en grandes redes, por otro lado la arquitectura DiffServ, es una alternativa escalable pero no provee de una garantía total.

Recientemente la IETF workgroup se ha enfocado en la combinación de elementos de DiffServ e ingeniería de tráfico, para dar servicios garantizados de flujos de datos MPLS dentro de la red. La información DiffServ en la cabecera IP es mapeada e introducida dentro de la etiqueta de información de los paquetes MPLS.

Qos puede ser y es generalmente implementado en el borde de la red MPLS donde el usuario comienza con la transmisión de los paquetes que requieren un tráfico en tiempo real.

5.3 Redes virtuales privadas MPLS

5.3.1 El concepto de VPN

Una VPN (Virtual Private Network) es una tecnología en la que se establecen canales seguros de comunicación que ofrecen protección a los datos transmitidos mediante el uso de algoritmos de encriptación y/o autentificación criptográfica. Una VPN es virtual porque es físicamente un red distinta, es privada porque la información que transita por los túneles es encriptada para brindar confidencialidad, y es una red porque consiste de computadoras y enlaces de comunicación, pudiendo incluir enrutadores, switches y gateways de seguridad.

VPN es una tecnología punto a punto, ampliamente adoptada en ambientes de transacciones financieras, y/o redes que requieren confidencialidad permanente, tanto en redes privadas como entre proveedores de Servicio de Internet y sus clientes. En el mercado existe una gran variedad de soluciones VPN, sin embargo aquí solo se discutirá VPN MPLS. La figura 20 ilustra un ejemplo de interconexión de oficinas y

sucursales de un entorno corporativo, interconectadas vía VPN usando la Internet como backbone de su red. Cada oficina tiene un gateway de seguridad que provee una interfaz con Internet y la red interna del corporativo. Los gateways de seguridad se configuran para definir las políticas de control de acceso para cada oficina. Los servicios de seguridad de IPSec (Internet Protocol Security) son ampliamente utilizados para la implementación de VPNs.

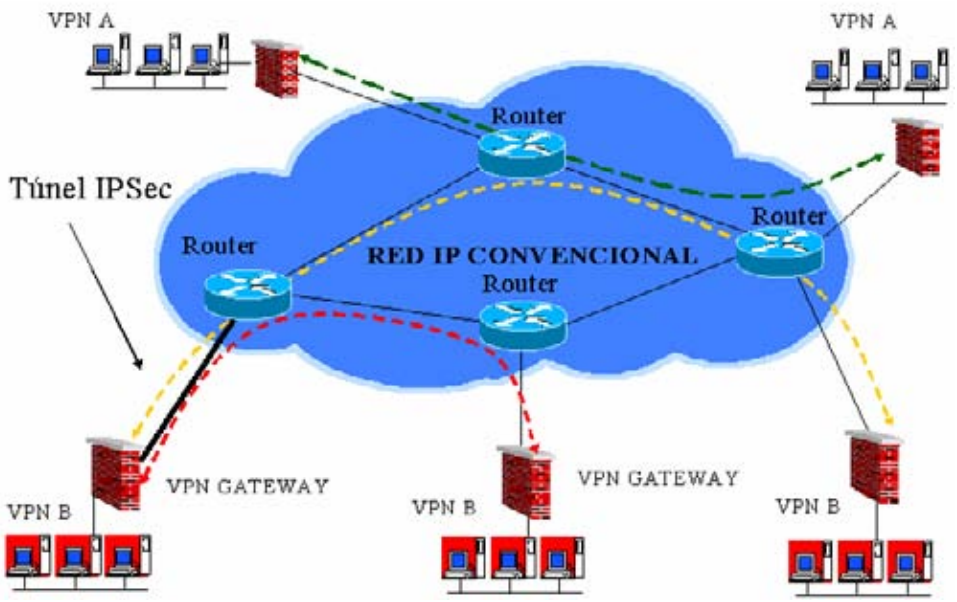

Figura 20.- Ejemplo de una Red Privada Virtual o VPN.

5.3.2 IPSec

IPSec (Internet Protocol Security) es un conjunto de extensiones al protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa de Red, de tal forma que su funcionamiento es completamente transparente al nivel de aplicaciones. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores.

La arquitectura de IPSec define la granularidad con la que el usuario puede especificar su política de seguridad. Permite que cierto tráfico sea identificado para recibir el nivel de protección deseado como se muestra en la figura 21.

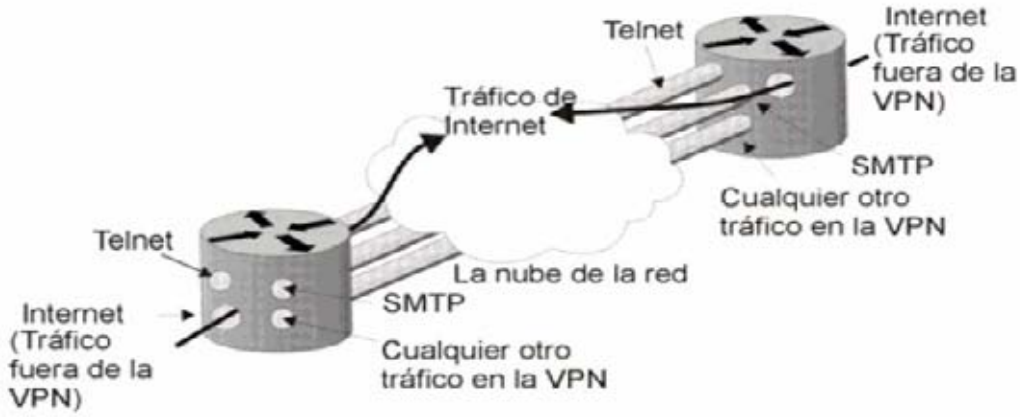

Figura 21.- Túneles de comunicación protegidos por IPSec entre redes separadas.

IPSec hace posible la creación de "túneles" seguros entre dos gateways (típicamente un router, cortafuegos o, incluso, software sobre un PC conectado a la red privada del usuario) a través de redes públicas. Los túneles IPSec son establecidos dinámicamente y libera d o s cuando no están en uso. Para establecer un túnel, los dos gateways IPSec han de autenticarse entre sí y definir cuáles serán los algoritmos de seguridad y las claves que utilizarán. Así, IPSec proporciona comunicaciones seguras y la separación lógica entre los flujos del tráfico de la red privada virtual (VPN) frente al resto de las transmisiones que cursan la red IP compartida.

5.3.3 Redes privadas virtuales MPLS

Las redes VPN pueden ser organizadas en dos categorías [4]:

- Basadas en clientes.- La VPN es configurada en equipos exclusivamente localizados en el cliente y usando protocolos de túneles para el curso de tráfico sobre redes publicas. Como se muestra en la figura 20. IPSec agrega seguridad y capacidad de encriptación para IP. Este es típicamente manejado donde se encuentra el clientes, es decir, fuera del proveedor de servicio.

- Basadas en redes.- Aquí la VPN es configurada en equipos de los proveedores de servicios y manejadas por los mismos. MPLS VPN es un ejemplo de estas redes.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los lazos del cliente y restablecer todos los nuevos PVCs.

La popularización de las aplicaciones TCP/IP, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y menores costes de gestión y provisión de

servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN.

Sin embargo, el problema real que plantean estas IP VPNs, es que están basadas en un modelo topológico superpuesto sobre la topología física existente, es decir, basados en túneles extremos a extremo (o circuitos virtuales permanentes) entre cada par de routers de clientes en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes.

MPLS VPN es mantenida y manejada por el proveedor de servicio, con lo cual puede proveer al consumidor ahorros muy significativos, además de una gran escalabilidad de crecimiento comparado con otras tecnologías VPN. MPLS VPN lleva diferentes tipos de tráficos del cliente, de forma única y separada para el envío de flujo de datos por cada VPN establecida. Este método de funcionamiento evita la necesidad de establecer y mantener circuitos virtuales permanentes, algo que, junto con la aplicación de técnicas de priorización de tráfico, hace de MPLS una solución ideal para crear redes VPN IP completamente malladas**.**

Estos mecanismos además de proveen la separación del tráfico y es totalmente transparente en el usuario final, que pertenece a un grupo VPN. MPLS VPN provee seguridad inherente, llevando trafico IP seguro, como Frame Relay o ATM reduciendo la necesidad de encriptación. Miercom, una empresa independiente de consultaría y evaluación e investigación de redes, evaluó la seguridad de una red VPN en varios

routes y concluyo que (2001): “Nuestros resultados de las pruebas demostraron que VPN basadas en MPLS ofrece la misma seguridad que Frame Relay o ATM.”

5.3.4 VPN MPLS de capa 3

MPLS VPN se clasifica en dos categorías, aquellas que operan sobre capa 3 y las que operan sobre capa 2.

Las VPN de capa 3 fueron las primeras investigaciones y estandarizado en la RFCs. Las VPN sobre capa 3 esta estandarizada por la RFC 2547, donde existe un completo desarrollo de la configuración de la misma.

Las VPN RFC 2547 basadas en capa 3, utilizan extensiones del protocolo BGP (Border Gateway Protocol), específicamente el multiprotocolo interno BGP (MP-iBGP); para la distribución de la información de ruteo dentro de la VPN o backbone provisto. El estándar MPLS utiliza sus mecanismos (previamente discutidos) para el envío de tráfico sobre el backbone VPN. En redes virtuales MPLS de capa 3, la arquitectura se conforma principalmente por un par de routers que son el CE (Customer edge) y el PE (Provider Edge), como se muestra en la figura 22. El router CE provee información al router PE de los clientes que pertenecen a la red privada que se encuentra detrás de este. En cambio el router PE almacena información privada de ruteo, la cual es formulada a través de una tabla virtual de ruteo e información (Virtual Routing Forwarding table, VRF); cada VRF es esencialmente una red privada IP. El router PE mantiene y separa tablas VRFs por cada VPN, consecuentemente esta provee un adecuado aislamiento y seguridad. Y a su vez cada usuario de una VPN tiene acceso solo a sitios o host que pertenecen a la misma VPN. Además de la tabla VRF, el router PE también almacena la información de ruteo normal que necesita para el envió de tráfico sobre la red publica.

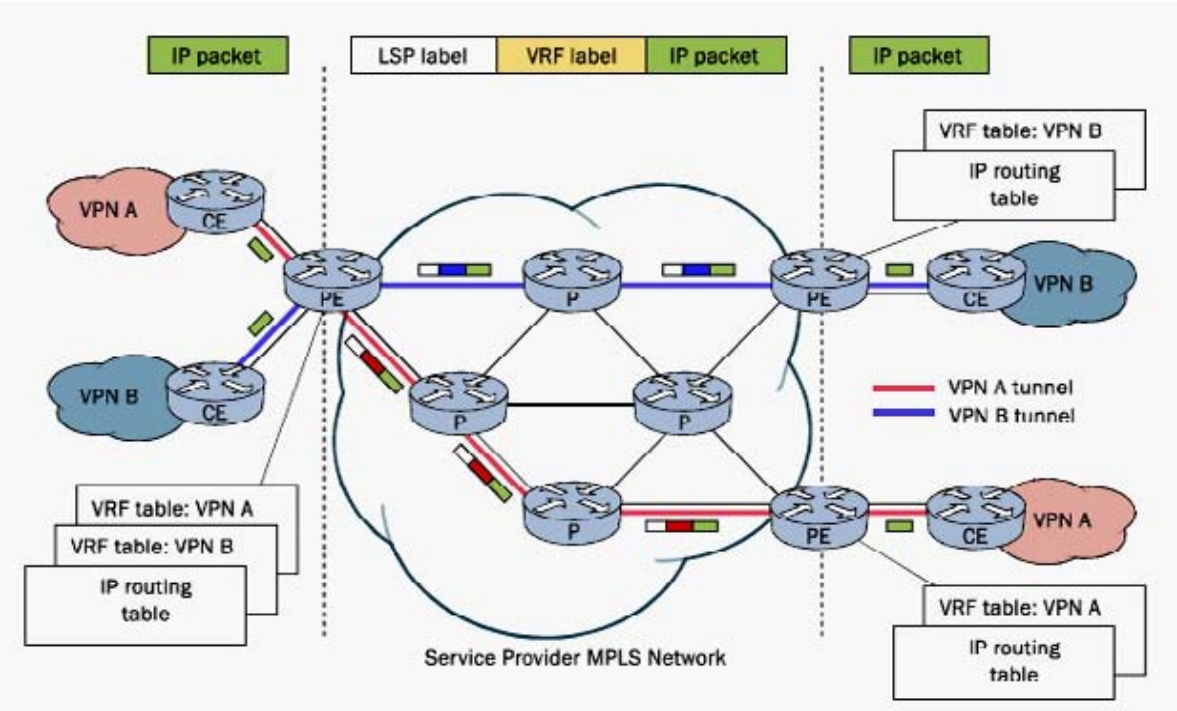

Figura 22.- Red VPN MPLS sobre capa 3 [4].

Las VPN de capa 3 usa dos niveles de almacenamiento MPLS, como se ve en la parte superior de la figura 22; la etiqueta en el interior del paquete que especifica la información de la VPN desde PE a PE y la etiqueta exterior del paquete que contiene la información de envío hop-by-hop MPLS. El router P, que se encuentra en el núcleo de la red MPLS ignora lo que sucede y por lo tanto solo lee e intercambia la etiqueta externa (LSP Label) del paquete que pasa por el y viaja a través de la red. Es importante destacar que este no actúa sobre la etiqueta interna del paquete (VRF label), esta información viaja oculta a través de la red (túnel).

Las VPN de capa 3 presentan varias ventajas:

- El cliente maneja un amplio espacio de direcciones IP, de esta manera puede agregar o quitar algún usuario de acuerdo a sus necesidades, la forma en que se pueden configurar a los usuarios dentro su red, es significativamente simple.

- Una nuevo sitio VPN es fácilmente conectado y manejado por el proveedor de servicio, las VPN de capa 3 también tiene la ventaja de soportar auto descubrimiento debido a la capacidad de ruteo dinámico del protocolo BGP para la distribución de los routers en la VPN.

- Evita la complejidad de túneles y PVCs

- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.

- Permite aprovechar las posibilidades de ingeniería de tráfico para las poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación, etc.), lo que es necesario para un servicio completo VPN.

5.3.5 VPN MPLS de capa 2

Las redes VPN MPLS sobre capa 2, son VPN de reciente generación que se ha venido desarrollando a fines del 2003. Las VPN MPLS de capa 2 se encuentra en plena fase de estandarización. Pero la industria se ha centralizado en el anteproyecto de Martini de la IETF, denominado así por su primer autor Luca Martini. Estos diseños definen la metodología para establecer túneles VPN de capa 2 a través de redes MPLS que maneja todo tipo de tráfico de capa 2 incluyendo Ethernet, Frame Relay, ATM, TDM, y PPP/HDLC.

Existen dos tipos de VPN MPLS sobre capa 2 que define la metodología Martini:

- Punto a punto.- o point-to-point, similar a ATM y Frame Relay, la conexión punto a punto atraviesa toda la red (LSPs).

- Multipunto.- que soporta diferentes jerarquías de topologías, VPLS (Virtual Private LAN Services) es un modelo multipunto que ha generado bastante interés últimamente.

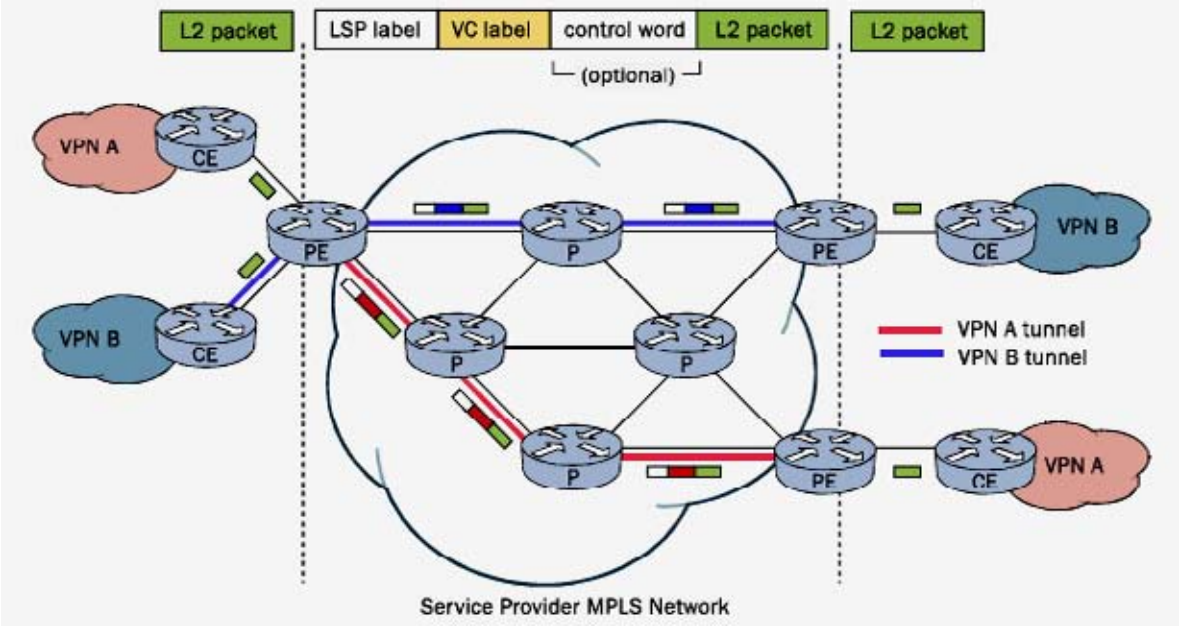

Figura 23.- Red VPN MPLS sobre capa 2 [4].

En VPN de capa 2, los routers PE y CE no tienen necesidad de ruteo como las VPN de capa 3, en lugar de eso, solo necesitan que exista una conexión entre PE y CE, así el router PE simplemente conmuta el tráfico entrante hacia los túneles configurados de uno o mas routers PE distintos y pertenecientes a la misma red. Una VPN MPLS de capa 2 determina la accesibilidad mediante un plano de datos, aprendiendo las

direcciones correspondientes. Al contrario de VPN de capa 3, el cual determina la accesibilidad mediante un plano de control que intercambian los router con BGP.

Las En VPN de capa 2 usa de manera similar el almacenamiento de etiquetas de las VPN de capa 3, aquí la creación de túneles a través de etiquetas externas determina el hop-by-hop sobre el camino a través de la red. Ver figura 23

La etiqueta interior Virtual Circuit (VC), identifica la Vlan, VPN o conexión hacia el punto final, además existe la opción de agregar una etiqueta de control o Control Word label, para llevar la información sobre el encapsulado del paquete de capa 2.

Las VPN MPLS de capa 2, distintas ventajas para el transporte de datos, según los requerimientos de la empresa, cualquier cosa porta es transparente en las redes MPLS. Ellas también pueden correr cualquier medio de transporte incluyendo ATM, Frame Relay, Packet sobre SONET, y Ethernet, habilitando la integración de redes IP orientadas a conexión con redes orientadas a conexión.

Por otro lado, las VPNs de capa 2 no son escalables como las VPNs de capa 3. La red mallada de LSPs debe ser instalada entre todas las VPN, un requerimiento que no es aconsejable para un gran numero de Vlans. Además estas redes no tienen la ventaja de descubrimiento automático de ruteo que ofrece las VPN de capa 3, por lo tanto solo satisface situaciones en donde el número de miembros que pertenecen a una VPN son pequeños y estáticos.

CONCLUSIONES

En el momento actual, todos los proveedores de servicios tienen ante sí el enorme reto de gestionar redes cada vez más complejas y extensas, con una mayor gama de servicios y con creciente demanda de ancho de banda, calidad y garantías. MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino).

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel. La idea básica de separar el plano de control y el de envío (mediante el algoritmo de intercambio de etiquetas), permite que cada una de ellas se pueda implementar y modificar de manera independiente, lo que crea una poderosa herramienta para poder gestionar de mejor forma las redes y a su vez permite que pueda funcionar sobre cualquier tecnología de transporte (no sólo sobre infraestructuras ATM) facilitando de modo significativo la migración para las redes de próxima generación.

Los operadores disponen ya de redes basadas en MPLS, aunque todavía no dejan de lado a ATM. Al menos durante unos años, estas tecnologías convivirán, y la gestión de recursos entre ellas serán aspectos fundamentales.

He podido observar que un aspecto importante considerado por la TE es el Balanceo de carga (Load Balancing), mecanismo que contribuye a la reducción de la congestión en las redes y a mejorar el uso de los recursos disponibles en la red. Otorgando escalabilidad, soporte de Calidad de Servicio, Clases de Servicios, entre otras y consecuentemente mejorando el rendimiento y la operabilidad de la red.

Los esquemas de Balanceo de Carga en Internet y en particular en MPLS, están desarrollados para que dicho proceso se realice en los nodos de ingreso, pues se considera el punto mas apropiado para hacerlo, dado que ahí se pueden realizar de forma más efectiva el control sobre el tráfico entrante.

En la actualidad existen mecanismos de balanceo de carga implementados en los encaminadores Cisco ® a través de su Cisco IOS, se recomienda usar balanceo de carga por destino; los sistemas de Juniper Networks a través de su sistema JUNOS®, y en redes experimentales de alta velocidad como la JGN (Japan Gigabit Network).

Es importante destacar que las redes privadas virtuales es una aplicación fundamental para los proveedores de servicios, ya que hoy en día, las grandes empresas quieren establecer una comunicación total, fluida y privada entre sus distintas sedes; mejorando la rentabilidad de estas mismas.

MPLS es una red bastante segura ya que no se permite que los datos entren o salgan del LSP por lugares que no han sido establecidos por el administrador de la red, además, cuando los datos entran en el dispositivo para conmutarse no son vistos por capas superiores más que por el módulo de envío MPLS (que intercambiará la etiqueta conforme a la tabla de envío del LSR), esto crea un entorno riguroso y a la vez flexible con lo cual se puede implementar redes virtuales y privadas MPLS, mediante la construcción de túneles con etiquetas apiladas.

BIBLIOGRAFÍA

- **Libros**

[1]. Eric Osborne, “Traffic Engineering with MPLS”, Cisco Press, July 17, 2002.
[2]. Gallear R “An Introduction to MPLS”, Vol. 1, 1999.

- **Papers**

[3]. B. Thomas, “LDP Applicability”. IETF 3037, junio 2001.
[4]. María Sol Canalis, “MPLS: Una arquitectura de backbone para la Internet del siglo XXI”. Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina, octubre 2003.
[5]. Jaeger R. Jupiner Networks, “Transitioning from IP-over-LANE to IP/MPLS Networks”. White paper 2001.
[6]. Jaeger R. Juniper networks, “MPLS: Enhancing Routing in the New Public Network”. White paper 2004.
[7]. Rob Redford, Juniper Networks, “RSVP Signaling Extensions for MPLS Traffic Engineering”. white paper 2000.
[8]. Rosen E, “Multiprotocol Label Switching Architecture”. RFC 3031, Enero 2001.
[9]. Xavier Hesselbach, Mónica Huerta, Oscar Calderón, “Problemas abiertos en MPLS”. Dpto. de Ingeniería Telemática, Universidad Politécnica de Catalunya, Barcelona – España 2002.

- **Sitio Web**

[10]. http://www.cisco.com/warp/public/cc/so/neso/vvda/ipatm/mpls_wp.htm
[11]. http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/ievpn_rg.htm
[12]. http://www.ietf.org/html.charters/mpls-charter.html 2
[13]. http://www.iec.org/online/tutorials/mpls

ANEXO

GLOSARIO

- **Algoritmo.-** Es un procedimiento o fórmula para resolver un problema, en los codecs están implementados sobre hardware de procesamiento digital de señales.

- **Ancho de banda.-** Es el ancho del espectro de frecuencias de la señal, es una medida de la velocidad de la señal. En los sistemas digitales se expresa en la cantidad de bits por segundo. Se intenta minimizar el ancho de banda por dos razones, reducir la susceptibilidad al ruido permitir mayor información sobre el mismo.

- **ATM (Asynchronous Transfer Mode).-** Es una tecnología de conmutación dedicada a conexión que organiza los datos en celdas de 53 bytes.

- **Backbone.-** Es el cableado central que interconecta redes dispersas dentro de un mismo predio o edificio.

- **Best effort.-** Servicios ATM sin calidad garantizada.

- **Bridge (puente).-** Unidad Funcional que interconecta dos redes de área local que utilizan el mismo protocolo de control de enlace lógico pero distintos protocolos de control deacceso al medio dentro del nivel 2 de OSI.

- **Byte.-** Agrupación fundamental de información binaria formada por 8 bits. Es la unidad mínima que puede direccionarse, pero no la unidad mínima que puede tratarse.

- **Calidad de servicio (Quality of Service).-** Es el mecanismo por el cual las características de una red como ancho de banda, retardo y pérdida de paquetes pueden ser medidas, mejoradas y garantizadas en un nivel determinado.

- **Congestión.-** Es el efecto indeseado al compartir un único medio de transmisión por varios usuarios.

- **Datagrama.-** Entidad de datos autocontenida e independiente que transporta información suficiente en orden de ser encaminada desde su ordenador de origen a su ordenador de destino sin tener que depender de que se haya producido anteriormente tráfico algunos entre ambos o la red de transporte.

- **Encabezado.-** Es la información de señalización, origen – destino, que antecede a la carga útil.

- **IETF Internet Engineering Task Force.-** Es el grupo que define los estándares para Internet y los protocolos operativos como TCP/IP. Está supervisado por una sociedad llamada IAB (Internet Architecture Board) y los resultados los publican en documentos llamados RFC (Request for Comments).

- **Frame Relay.-** Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.

- **Gateway (Puerta de acceso, pasarela).-** Unidad de interfuncionamiento. Dispositivo de comunicaciones que interconecta sistemas diseñados conforme a protocolos propietarios, o entre un sistema con un protocolo propietario y un sistema abierto o una red RAL, teniendo lugar una conversión completa de protocolos hasta la capa 7 del modelo de referencia OSI.

- **Host.-** En una red informática, es un ordenador central que facilita a los usuarios finales servicios tales como capacidad de proceso y acceso a bases de datos, y que permite unciones de control de red.

- **IGP (Protocolo de gateway interior).-** Protocolo de Internet que se utiliza para intercambiar información de enrutamiento dentro de un sistema autónomo. IGRP, OSPF y RIP son ejemplos de IGP de Internet comunes.

- **Internet.-** Es una red pública de computadoras de alcance mundial que cuenta con millones de usuarios y utiliza el protocolo TCP/IP.

- **Intranet.-** Es una red privada que se extiende dentro del ámbito de una empresa.

- **IP (Internet Protocol).-** Es el protocolo que se encarga de realizar el direccionamiento de los paquetes. Ver TCP/IP

- **IPSec (Internet Protocol Security).-** IP Seguro. Estándar abierto para garantizar seguridad en comunicaciones privadas en redes IP.

- **ISP (Internet Service Provider) —** Organización que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas o por líneas conmutadas. Es una entidad, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, les ofrece una serie de servicios (hospedaje de páginas web, consultoría de diseño e implantación de webs e Intranets, etc.).

- **Latencia.-** Es el tiempo que tarda un paquete de datos entre dos puntos determinados. Ver retardo.

- **Modelo de referencia OSI (Open system Interconection).-** Es un estándar que especifica como se deben transmitir los datos entre dos puntos de una red de telecomunicaciones. Consta de 7 niveles: físico, enlace, red, transporte, sesión y aplicación.

- **Retardo (delay).-** Es el tiempo que tarda un paquete de datos entre dos puntos determinados, se incluyen los tiempos de propagación, transmisión y procesamiento. Ver latencia.

- **Router.-** Es el equipo que interconecta redes LAN y redes WAN, también traduce protocolos.

- **RSVP (Protocolo de reserva de recursos).-** Protocolo que hace posible la reserva de recursos a través de una red IP. Las aplicaciones que se ejecutan en los sistemas finales IP pueden usar RSVP para indicarle a los otros nodos la naturaleza (ancho de banda, fluctuación de fase, ráfaga máxima, etc.) de los flujos de paquetes que desean recibir.

- **Throughput.-** Es la cantidad de datos transmitidos exitosamente desde un dispositivo hasta otro en un período de tiempo.

- **TCP/IP Transmission Control Protocol** / **Internet Protocol.-** Es una serie de protocolos y servicios que abarcan el nivel 2 y el 3 del mdelo de referencia OSI.

- **Tunneling.-** Arquitectura diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulación punto a punto estándar.

- **Protocolo de Datagramas de Usuario (UDP).-** Protocolo que no pide confirmación de la validez de los paquetes enviados por la computadora emisora. Este protocolo es actualmente usado para la transmisión de sonido y vídeo a través de Internet. El UDP está diseñado para satisfacer necesidades concretas de ancho de banda y como no reenvía los datos perdidos, es ideal para el tráfico de voz digitalizada debido a que un paquete perdido no afecta la calidad del sonido. Entre las aplicaciones que utilizan este protocolo encontramos a Real Audio.

- **UDP.-** Acrónimo de User Datagram Protocol. Protocolo dentro del TCP/IP que convierte mensajes de datos en paquetes para su envío vía IP pero no verifica que hayan sido entregados correctamente.