UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CÚAUTITLAN

MPLS

"Multiprotocol Label Switching"

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERA MECANICA ELECTRICISTA

P R E S E N T A:

MARCELA NAYELI ESTEVES MANZANO

ASESOR: ING. JOSE UBALDO RAMIREZ URIZAR

CUAUTITLAN IZCALLI, EDO. DE MEXICO 2004

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

ASUNTO: VOTOS APROBATORIOS.

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 28 del Reglamento General de Exámenes, nos permitimos comunicar a usted que revisamos la TESIS:

MPLS - "Multiprotocol Label Switching"

que presenta la pasante: Marcela Nayeli Esteves Manzano
con número de cuenta: 9132202-1 para obtener el título de :
Ingeniera Mecánica Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VOTO APROBATORIO.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 04 de Noviembre de 2003

PRESIDENTE	Ing. José Luis Rivera López	
VOCAL	Ing. José Ubaldo Ramírez Urizar	
SECRETARIO	Ing. Blanca de la Peña Valencia	
PRIMER SUPLENTE	Ing. Anselmo Angoa Torres	
SEGUNDO SUPLENTE	Ing. Marcelo Bastida Tapia	

En cada término de un proyecto encontré conocimiento, aprendizaje, satisfacción....después al iniciar nuevamente mi camino, expectante de nuevos objetivos, me sumergía en un orden distinto, desconocido, que provocaba confusión en mi corazón, pero mantenía vivo mi deseo de entenderlo, de agregarlo a mi vida y encontrar aunque solo fuese por un instante el equilibrio.....para después, seguir caminando por la vereda que he escogido.

Indice de Contenidos.

Capítulo IV. Aplicaciones de MPLS

OBJETIVOS DE TESIS.

- ***Analizar*** los hechos que demandaron el surgimiento de MPLS, su funcionamiento y las ventajas de su uso comparado con la solución de IP/ATM.

- ***Explorar*** las herramientas que nos proporciona le protocolo MPLS en la integración y optimización de sistemas de telecomunicaciones.

- ***Investigar*** las características de las aplicaciones comunes de MPLS (Ingeniería de tráfico, desarrollo de VPNs y CoS) y las ventajas que ellas suponen.

Introducción.

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

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

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

Con el objetivo de proporcionar ***Calidad de Servicio* (*QoS*)** a una red, el ***Internet Engineering Task Force* (IETF)** propuso como solución, a mediados de los años 90, el protocolo ***MPLS* (Multiprotocol Label Switching)** el cuál surge como

respuesta a los ***ISPs*** **(Internet Service Providers)** que en este contexto buscaban una solución a la compleja transmisión de datos IP sobre un backbone ATM, tendiendo a la convergencia de redes que les permitiría en un futuro, una administración más completa del estado de sus servicios.

MPLS es una tecnología que permite grandes ventajas para el transporte de cualquier tipo de datos sobre redes existentes **IP**, **ATM** ó **Frame Relay,** por lo que su implementación no resulta difícil. Al mismo tiempo proporciona servicios con niveles de **QoS** a través de su llamada ***«conmutación de etiquetas»*** o de rutas fijas. Además **MPLS** ofrece simples mecanismos para aplicaciones de paquetes orientados a ruteo, envío y conmutación para cualquier tipo de tráfico en una red a través de una de sus características principales: la separación de funciones de control y envío.

MPLS se puede presentar como un sustituto de la arquitectura **IP sobre ATM (IP/ATM),** ya que integra sin discontinuidades los niveles de capa 2 "enlace de datos" y de capa 3 "red" combinando eficazmente las funciones de control de ruteo con la simplicidad y rapidez de la conmutación de la capa 2.

Pero, ante todo y sobre todo, debemos considerar **MPLS** como el avance más reciente en la evolución de las tecnologías de ruteo y envío en las redes **IP**, lo que implica una evolución en la manera de construir y gestionar estas redes, las redes **IP** consideradas de ***"next generation"***. Los problemas que presentan las soluciones actuales de **IP/ATM**, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con **MPLS**. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del ruteo con la rapidez de la conmutación), **MPLS** ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de ***nuevos servicios de valor agregado.***

En una red **IP** tradicional, los routers conmutan los paquetes de una interfaz de entrada a una interfaz de salida al mismo tiempo que actualizan la información de enrutamiento. Para enviar los paquetes, se debe examinar la cabecera de cada paquete IP. Estas dos funciones, envío y enrutamiento, tienen lugar en cada salto que realiza un paquete para cada uno de los que atraviesan la red. A este respecto **MPLS** busca llevar las funciones de enrutamiento únicamente a los equipos exteriores del dominio **MPLS**, de forma que en el interior de dicho dominio no sea necesario realizar labores de enrutamiento, sino sólo de conmutación mediante la consulta de unas etiquetas añadidas a cada paquete en el momento de entrada al dominio, simplificando el envío y enrutamiento del mismo.

En resumen las principales ventajas que proporciona **MPLS** son:

- Envío de paquetes IP a gran velocidad de un modo simplificado y eficiente.
- Provisión de redes fácilmente escalables.
- Control de la Calidad de Servicio.
- Ingeniería de Tráfico y control del enrutamiento del tráfico.
- Redes Privadas Virtuales **(VPNs)**.

Capítulo I. Antecedentes de MPLS

1. Orígenes y Etapa Experimental de la Internet

Internet ha supuesto una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Los inventos del telégrafo, teléfono, radio y PC sentaron las bases para esta integración de capacidades nunca antes vivida. Internet es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus computadoras independientemente de su localización geográfica.

Internet hoy en día tiene una influencia que alcanza no solamente al campo técnico de las comunicaciones computacionales, sino también a toda la sociedad en la medida en que nos movemos hacia el incremento del uso de las herramientas ***online*** para llevar a cabo el comercio electrónico, la adquisición de información y la acción en comunidad.

Su origen se remonta a los años 60, como un experimento de la Agencia de Proyectos Avanzados de Investigación ***(ARPA, Advance Research Projects Agency)***, del Departamento de Defensa de los Estados Unidos ***(DARPA)***.

Una de las preocupaciones de las Fuerzas Armadas de los Estados Unidos era conseguir una manera en que las comunicaciones estuvieran descentralizadas, es decir, evitar un centro neurálgico de comunicaciones que pudiera ser destruido en un eventual ataque militar con armas nucleares y que así, aún sufriendo el ataque, las comunicaciones no se bloquearan, sino que solamente se perdiera un nodo.

Puede parecer en este punto que la única finalidad de la red que se estaba creando era la defensa de un ataque nuclear, pero hay que decir que la idea de los científicos que estaban trabajando en estas instituciones era crear una red para compartir recursos entre investigadores.

En 1969 la DARPA, junto con la compañía ***Rand Corporation*** desarrolló una red sin nodos centrales basada en conmutación de paquetes. La información se dividía en paquetes y cada paquete contenía la dirección de origen, la de destino, el número de secuencia y una cierta información, al llegar al destino se ordenaban según el número de secuencia y se juntaban para dar lugar a la información. Al viajar los paquetes por la red, era más difícil perder datos ya que, si un paquete concreto no llegaba al destino o llegaba defectuoso, la computadora que debía recibir la información sólo tenía que solicitar a la computadora emisora el paquete que le faltaba. El protocolo de comunicaciones se llamó ***NCP (Network Control Protocol)***.

En Diciembre de 1969, la red experimental inicio su operación con la conexión de una red de cuatro nodos interconectados vía enlaces de 56 kbps. DARPA conectó sus computadoras centrales vía ***"routers"***, que en ese entonces eran llamados ***Interface Message Processors (IMPs)***. El 1° de Septiembre de 1969 el primer ***IMP*** llegó a la UCLA. Un mes después el segundo fue instalado en Stanford, el tercero en la UC de Santa Bárbara y finalmente el cuarto en la universidad de UTAH. Esta nueva tecnología probó ser altamente confiable y motivó la creación de dos nuevas redes similares para la milicia: MILNET en los Estados Unidos y MINET en Europa.

Los años setenta transcurren con instituciones académicas y de gobierno conectándose directamente o conectando otras redes entre sí creando la "Internet" ***ARPA*** ó ***ARPAnet*** cuya política principal era la prohibición del uso de la red para fines comerciales.

Un ejemplo del interés de las instituciones por estas posibilidades de conexión lo represento la **NSF** ***(National Science Foundation)*** quién dio acceso a sus seis centros de cómputo a otras universidades a través de la ARPAnet. A partir de aquí se fueron conectando otras redes, evitando la existencia de centros para preservar la flexibilidad y la escalabilidad de la misma.

Al mismo tiempo los responsables de la administración de ARPAnet se encontraban desarrollando estándares y protocolos, como ***Telnet***, la especificación de transferencia de archivos o el protocolo de voz en redes ***(NVP, Network Voice Protocol)***. Pronto había muchas redes diferentes alrededor del mundo, pero no podían comunicarse con otras porque utilizaban protocolos o estándares diferentes entre sí para transmisión de datos.

Entonces, en 1974, **Vinton Cerf** ***(conocido por algunos como el padre de "Internet")***, junto con Bob Kahn, publican ***"Protocolo para Intercomunicación de Redes por paquetes"***, donde especifican en detalle el diseño de un nuevo protocolo, el **Protocolo de Control de Transmisión** ***(TCP, Transmission Control Protocol)***, que se convirtió en el estándar aceptado. La implementación de TCP permitió a las diversas redes conectarse en una verdadera red de redes, conectarse a **INTERNET**.

Vinton Cerf

En 1979 ARPAnet crea la primera comisión de control de la configuración de Internet y tras varios años de trabajo, por fin en 1981 se termina de definir el protocolo **TCP/IP** ***(Transfer Control Protocol / Internet Protocol)*** y ARPAnet lo adopta como estándar en 1982, sustituyendo a NCP. Internet es la abreviatura de

Interconnected Networks, es decir, Redes interconectadas, o red de redes.

En 1983 ARPAnet se separa de la red militar que la originó, de modo que ya sin fines militares se puede considerar esta fecha como el nacimiento de Internet. Es el momento en que el primer nodo, militar, se desliga dejando abierto el paso para todas las empresas, universidades y demás instituciones que ya por esa época poblaban la joven red.

1.2 La NSFNET y la Etapa de Consolidación de Internet

En 1985, al verse la ARPAnet altamente utilizada y congestionada, la National Science Foundation inició el desarrollo de un nuevo ***"backbone"***: la **NSFNET**.

La NSF estableció una red destinada a las comunicaciones entre científicos e ingenieros en los Estados Unidos. Esta red, se basó en ARPAnet e inició su infraestructura con 6 computadoras, localizadas en los centros de cómputo existentes, en ese entonces (San Diego CA, Boulder CO, Champaign IL, Pittsburgh PA, Ithaca NY y Princeton NJ). Figura 1.1.

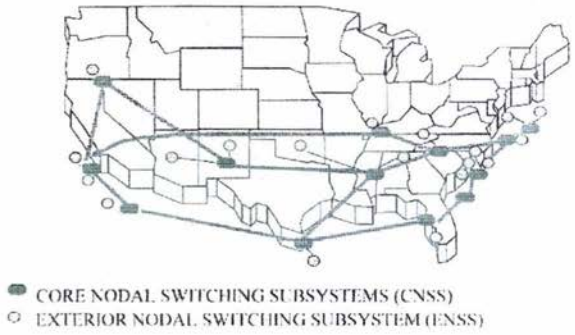

Figura 1.1. Backbone de la NSFNET (1993).

La NSFNET estaba integrada de múltiples redes regionales, conectadas a una red principal "*backbone*", la cual constituyó el núcleo de la NSFNET. En su forma temprana, la NSFNET creó una arquitectura de red jerárquica de tres niveles. La arquitectura conectaba campus universitarios y organizaciones de investigación a redes regionales, las cuales en turno se conectaban a una red principal o "*backbone*" enlazando nacionalmente los seis centros de supercómputo. Los enlaces originales eran a 56 kbps.

Desde su construcción en 1985, el *"backbone"* de la NFSNET se ha venido modificando, principalmente en cuanto a la velocidad de sus medios de transmisión, cambiando desde los enlaces originales de 56 kbps, hasta enlaces basados en SONET OC3, en 1995, para constituir el actual "*backbone*" denominado **VBNs *(Very High Speed Backbone)***. Figura 1.2.

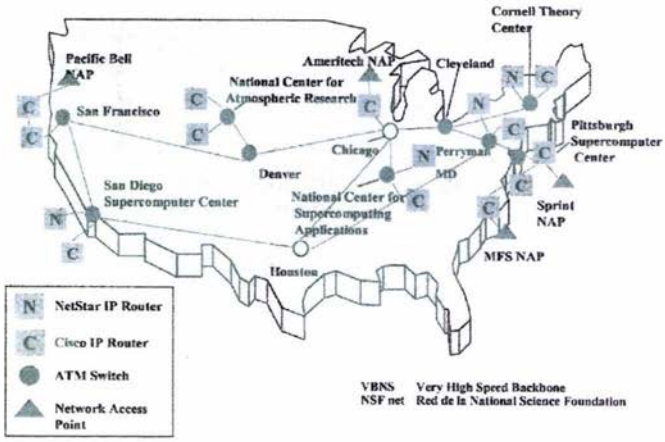

Figura 1.2. Mapa de la Topología del VBNS.

A finales de la década de los 90, la NSFNET estuvo reservada para aplicaciones de educación e investigación, sin embargo, la internet empezó a sentir presiones de organizaciones gubernamentales (en los Estados Unidos) y comerciales, para aplicaciones de esta índole y de propósito general. Por tal motivo la NSF se vio obligada a promover el desarrollo de un nuevo y más robusto modelo de la Internet y así acomodar el rol de los proveedores de servicios comerciales (de Internet), para esto se planteó la ejecución de cuatro proyectos:

- Crear un conjunto de Puntos de Acceso a la Red **(NAP, *Network Access Points*)**, donde grandes proveedores conectaran sus redes e intercambiarán tráfico.

- Implementar un proyecto para Arbitrar Rutas **(RA)**, para facilitar el intercambio de políticas y de direccionamiento de múltiples proveedores conectados a un NAP.

- Encontrar un proveedor de un Servicio de Red Principal de Muy Alta-velocidad **(VBNS, *Very High-Speed Backbone Network Service*)**, para propósitos gubernamentales y educativos.

- Transitar redes regionales para conectarlas a los NAP, ya sea directamente o por medio de un Proveedor de Servicios de Red **(NSP, *Network Service Provider*)**.

1.3 Arquitectura Actual de la Internet

Hoy en día, la estructura de la Internet se ha movido desde una arquitectura basada en un *"backbone"*, a una arquitectura distribuida operada por proveedores comerciales tales como **SPRINT**, **MCI**, **BBN** y otros, conectados vía puntos de intercambio de red. La Figura 1.3 ilustra la forma general de la Internet hoy día.

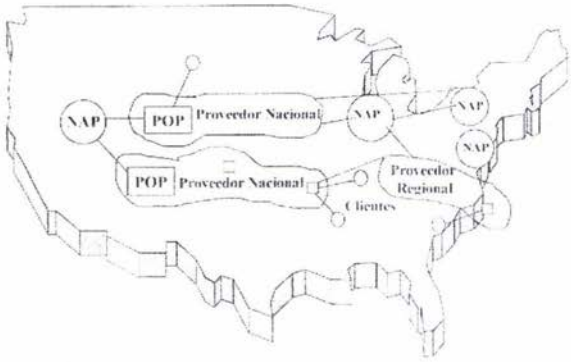

Figura 1.3. Estructura General de la Internet.

La Internet contemporánea es una colección de proveedores que tienen puntos de conexión llamados Puntos de Presencia **(POP, *Point of Presence*)**, sobre múltiples regiones. El conjunto de POP y la forma en la cual se interconectan, forman la red de un proveedor. Los clientes son conectados a la red de un proveedor vía los POP. Los clientes de proveedores de red pueden ser también proveedores a la vez.

Los proveedores que tienen POP a lo largo del territorio de un país, se les denomina comúnmente Proveedores Nacionales; de la misma manera se les

denomina Proveedores Regionales, a los proveedores que cubren una región específicamente.

Dentro de la nueva arquitectura de la Internet, se definieron puntos de interconexión denominados Puntos de Acceso a la Red (NAP), para permitir que clientes de un proveedor se comunicaran con clientes de otro proveedor. Figura 1.4.

Figura 1.4. Principales Puntos de Interconexión en EUA.

El término **ISP** ***(Internet Service Provider)***, es comúnmente utilizado para referirse a cualquiera que proporciona servicios de conexión a Internet, ya sea directamente a clientes finales o a otros proveedores. El término **NSP (Network Service Provider)**, es a menudo restringido a proveedores quienes reciben fondos de la NSF para administrar los NAP, como son **SPRINT**, **AMERITECH** y **MFS**. El término NSP, sin embargo, es también usado de manera más holgada para referirse a cualquier proveedor que se conecta a todos los NAP.

Un NAP es una red de alta velocidad o conmutador de datos (switch), al cual un número de enrutadores son conectados con propósitos de intercambio de

tráfico. Un NAP deberá operar al menos a 100 Mbps, y deberá ser capaz de ser actualizado como sea requerido, ya sea por demanda o por uso. Un NAP deberá ser tan simple como un Switch FDDI (100Mbps), o un switch ATM (155 Mbps), pasando tráfico desde un proveedor a otro.

Originalmente se implementaron cuatro NAP, auspiciados por la NSF:

- NAP Sprint, en Pennsauken, NJ.
- NAP Pacific Bell, San Francisco, CA.
- NAP Ameritech, Chicago, IL.
- MAP MFS, Washington, D.C.

1.4 Internet 2

La segunda principal iniciativa de NSF, antes de terminar la operación de su "backbone", fue el mantener vivo el espíritu innovador que caracterizó siempre a la internet, por lo que impulsó, mediante sus propios fondos, un proyecto de cómputo de alto desempeño al que se llamó ***Internet 2***.

La primera meta de este programa fue apoyar a las universidades para ganar acceso a la VBNS, típicamente vía puntos de conexión denominados **GigaPOP (*Gigabit Points Of Presence*)**.

La justificación para la creación de una nueva internet era que en ese momento ya no servía más a las necesidades de la comunidad educativa y de investigación debido a que su privatización había reducido las necesidades académicas y aumentado las comerciales, la nueva internet sería desarrollada para brindar un gran ancho de banda, seguridad y disponibilidad al área de investigación.

A finales de 1996 se reunieron 34 universidades ***(actualmente suman más de 160)*** de los Estados Unidos con el fin de acordar los pasos que deberían seguir para desarrollar una infraestructura, tanto en el plano físico (hardware), como en el lógico (definición de nuevos estándares, desarrollo del software necesario, etc.) en la que fuera posible explotar aplicaciones avanzadas. Una red de alta velocidad, que se estima entre 100 y 1,000 veces más rápida que la actual, donde la investigación y las experiencias avanzadas encuentren un verdadero desarrollo.

Internet 2 es un proyecto de la **UCAID (*University Corporation For Advanced Internet Development*)**, trabajando conjuntamente con la industria y el gobierno estadounidense. Este proyecto es financiado por los miembros de la UCAID y se estima que su costo es de aproximadamente 50 millones de USD por año.

Algunas de las principales aplicaciones de investigación de este proyecto son:

- Telemedicina
- Laboratorios virtuales
- Teleeducación
- Multimedia en tiempo real
- Software de colaboración

1.5 Crecimiento de Usuarios de Internet

El periodo comprendido entre las décadas de 1960 a 1980, puede ser descrito como la época de consolidación de las tecnologías de información e implementación de protocolos de red, la década de los 90's fue de gran relevancia tecnológica, registrando un dramático crecimiento del uso de la internet en ambos ámbitos, comercial y residencial. Tabla1.1.

USUARIOS DE INTERNET	1995	1998	2000	2005
Mundial	39,479	150,887	318,650	717,083
América del Norte	28,217	82,989	148,730	229,780
Este de Europa	8,528	34,741	86,577	202,201
Oeste de Europa	369	2,983	9,487	43,767
Asia	3,628	24,559	57,607	171,068
America Central y del Sur	293	2,722	10,766	43,529
Oriente Medio	444	2,893	7,482	26,708

Nota: Referencia en miles.

Tabla 1.1. Estadística de Usuarios de Internet a Nivel Mundial.

En resumen, la internet ha sido afectada por muchas fuerzas, que al empujar la idea de la supercarretera de la información, crearon nuevas oportunidades de negocios, la desregulación de mercados globales y una rica variedad de usos y nuevos servicios para todos, es por eso que se sigue manteniendo como una herramienta versátil y de fácil uso cuyo crecimiento va aumento.

Capítulo II. Inicios de MPLS

2. "Técnicas de Conmutación IP"

Entre los años 1997 y 1998 se produjo un explosivo crecimiento de Internet en términos de su volumen y capacidad, en conjunto con el incremento del uso de aplicaciones de tiempo real y multimedia, estos cambios produjeron una gran presión sobre las capacidades de la red para poder soportar un mayor ancho de banda y al mismo tiempo contar con garantías de calidad de servicio, además la creciente convergencia de las aplicaciones existentes hacia **IP**, junto a los problemas de rendimiento derivados de la solución **IP/ATM**, llevaron posteriormente a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva. Estas técnicas se conocieron como ***"conmutación IP"*** **(IP switching)** o ***"conmutación multinivel"*** **(multilayer switching).** Una serie de tecnologías privadas entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM y Cell Switching Router (CSR) de Toshiba, condujeron finalmente a la adopción del actual estándar **MPLS** del **IETF**. El problema que presentaban tales soluciones era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de capa 2 con el encaminamiento IP de capa 3.

Para poder entender mejor las ventajas de la solución MPLS, vale la pena revisar los esfuerzos anteriores de integración de los niveles 2 y 3 que han llevado finalmente a la adopción del estándar MPLS.

2.1 IP Switching

Esta tecnología fue desarrollada por ***Ipsilon Networks Inc***. El éxito de Ipsilon fue hacer la conmutación IP más rápida y al mismo tiempo ofrecer un soporte de calidad de servicio (QoS). Mientras la solución IP/ATM suponía la superposición de una topología virtual de routers IP sobre una topología real de conmutadores (switches) ATM presentándola como una gran nube transparente, el intento de Ipsilon fue descartar la conexión orientada al nivel de software de ATM y en su lugar implementar la conexión directa de los paquetes IP a la Interfaz física del switch ATM. Esta característica aumento la capacidad y velocidad de las conexiones IP y la escalabilidad de los switches ATM.

Un ***IP switch*** es básicamente un router IP que incluye hardware de conmutación y que tiene la capacidad de depositar las decisiones de ruteo o encaminamiento en el hardware de conmutación. Un IP switch se podría describir como un conmutador ATM con el hardware intacto pero sin el control del ***AAL-5 (ATM Adaptation Layer 5)*** este sería remplazado por el software standard de ruteo IP, el cuál trabajaría como un clasificador de flujo de tráfico de paquetes para decidir entre conmutar un flujo de datos o no y un driver de control de hardware de conmutación.

Un flujo es una secuencia de paquetes que viaja desde una fuente de origen hasta una de destino la cuál tiene el mismo tratamiento de envío en el router. Un flujo de datos IP siempre contiene los datos de dirección origen, dirección destino, número de puerto, etc. en su encabezado IP/TCP/UDP, Ipsilon define dos datos más, ***Flujo Par del Host*** para el tráfico entre la misma dirección IP de origen y destino. Y el ***Flujo Par de Puerto***, para el traficó entre el mismo puerto de origen y destino entre la misma dirección IP de origen y destino.

Cuando un paquete es montado y enviado al controlador del IP switch antes de ser encaminado al siguiente router también es clasificado su flujo. Dependiendo de

su clasificación el switch puede decidir si envía o conmuta el paquete de ese flujo.

Los servicios que pueden ser proporcionados por el modelo ***IP Switching*** son:

Point to Point: IP Switching aboga por un modelo de red para ATM punto a punto más que por un modelo lógico compartido como lo propuesto por otros competidores.

Multicast: En el caso de multicast un flujo entrante al IP Switch puede ramificarse en múltiples destinos, cada ramificación puede ser redireccionada.

Quality of Service: Un IP Switch puede tomar decisiones de calidad de servicio (QoS) de acuerdo con la configuración local del dispositivo. La información de QoS se incluye en el proceso de clasificación de flujo, adicional a ello la configuración individual de QoS en cada flujo puede realizarse utilizando el protocolo **RSVP**.

Latency: Esta característica puede hacerse bajo la conexión orientada a protocolos TCP. En la configuración de TCP se puede establecer un canal virtual aún antes de que el primer paquete de datos sea enviado. En caso de una parte de la ruta falle el IP Switch puede regresar a la dirección del envió del paquete utilizando una ruta distinta.

2.2 Tag Switching

Tag Switching fue desarrollado por ***Cisco Systems Inc***. para mejorar el enrutamiento en términos de ancho de banda, escalabilidad, soporte a nuevas funcionalidades de ruteo, multicast, jerarquía de enrutamiento y flexibilidad en el control de enrutamiento. Esta utiliza la etiqueta de conmutación para capa 3

"envío de paquetes". La tecnología de Tag Switching consiste en el envió y control de los siguientes componentes:

Forwarding Component (Componente de envío): esta utiliza las etiquetas llevadas por los paquetes y la etiqueta de información de envío en el Tag Switch para realizar el envío del paquete. Los paquetes que pasan por el Tag Switch pueden llevar etiquetas en una de las siguientes formas:

- Como un pequeño encabezado de etiqueta insertado entre las capas 2 y 3.
- Como parte del encabezado de capa 2
- Como parte del encabezado de capa 3

Tag Information Base (Base de Información de etiquetas): Los routers y conmutadores (switches) que soportan la conmutación de etiquetas son llamados Tag Switches. Un Tag Switch guarda la información de envió de etiquetas en una base de datos llamada Tag Information Base (TIB). Cada consulta en el TIB se realiza a través de una etiqueta de entrada con una ó más subentradas (etiqueta saliente, interfaz saliente, etc.).

Forwarding Procedure (Procedimiento de envío): Cuando un Tag Switch recibe un paquete con etiqueta, este la utiliza como un índice de búsqueda en el TIB. En caso de encontrar una entrada con una etiqueta igual a la etiqueta del paquete, el switch la sustituye por la etiqueta de salida y dirige al paquete a la interfaz de salida.

Control Component (Componente de control): En la conmutación de etiquetas hay una liga entre la etiqueta y la capa de ruteo (capa 3). Una etiqueta puede ser ligada a una aplicación de flujo de datos, una ruta específica, un grupo de rutas ó multicast, etc. La principal función de la componente de control es crear ligas de etiquetas y distribuir la información de la etiqueta ligada entre las conexiones de

los Tag Switches. Algunas de las funciones de ruteo que soporta la conmutación de etiquetas son descritas a continuación:

Destination Based Router (Router Basado en Destino): Un Tag Switch puede participar en los protocolos de la capa de ruteo y con esta información construir su ***Base de Datos de Información de Envío (Forwarding Information Base, FIB)***. Luego podría utilizarse cualquiera de los siguientes tres métodos para la asignación de etiquetas y la creación del TIB:

1. ***Downstream Tag Allocation***: Aquí el downstream switch (es el switch que recibe paquetes de información de otro switch en una ruta) realiza el trabajo de asignación y ligado de etiquetas en una ruta en particular o un grupo de rutas.
2. ***Downstream Tag Allocation on Demand***: El dowstream switch asigna y liga las etiquetas con un prefijo en su dirección, pero solo cuando le es solicitado por un upstream switch (es el switch que envía paquetes de información a otro switch en una ruta).
3. **Upstream Tag Allocation**: El upstream switch se permite asignar y ligar una etiqueta con un prefijo de dirección.

Una vez que la asignación de etiquetas esta hecha y las ligas son creadas, el switch distribuye esta información a otros switches interconectados en la red. Cuando un paquete sin etiqueta se incorpora a la red de Tag Switches una etiqueta es añadida a su encabezado por el primer Tag Switch en su ruta. Luego el paquete es conmutado a través de la red hasta pasar por el último Tag Switch en su ruta, este remueve la etiqueta. Puesto que la existencia de un paquete de entrada realiza una consulta en el FIB para la asignación de una etiqueta de encabezado, podemos decir que la conmutación de etiquetas conduce a la topología de entrega del paquete.

Hierarchy of Routing Knowledge (Jerarquía de la Ruta Conocida): El ruteo IP concibe a la red como una configuración de dominios de ruteo. Aunque separe el ruteo del intra-dominio del ruteo del inter-dominio, todos los routers dentro del dominio de una ruta de tráfico mantienen la misma cantidad de información que va degradando el desempeño de la red e incrementa el tiempo de convergencia del ruteo. Para reconocer los límites del dominio la conmutación de etiquetas configura un paquete de datos para llevar un arreglo de etiquetas, así dentro de un ambiente IP un paquete tendrá 2 etiquetas, una para la conmutación del Inter.-dominio y otra para la del intra-dominio.

Multicast Forwarding (Envío en modo Multicast): Para soportar la función de Multicast la conmutación de etiquetas asocia una etiqueta con un grupo de información (multicast). Cuando un Tag Switch crea una entrada de envío en modo multicast en su TIB, este crea una etiqueta de salida local y una subentrada para cada interfaz de salida.

Flexible Routing (Ruteo Flexible): El ruteo basado en destino no soporta ningún parámetro a excepción de la dirección de destino para asignar la ruta. Esto limita la capacidad de la red para balancear las cargas. La conmutación de etiquetas supera esta limitación permitiendo ligar las etiquetas de rutas específicas que pueden ser diferentes de las rutas establecidas por la dirección de destino.

Quality of Service (Calidad de Servicio): Para soportar una selección de calidad de Servicio un router debe de ser capaz de clasificar los paquetes de información pertenecientes a una clase en particular y enviarlos satisfaciendo la selección de la calidad de servicio configurada. La conmutación de etiquetas permite a la calidad de servicio asignar una etiqueta a una clase de paquetes una vez que se haya hecho la clasificación. Esto elimina la necesidad de reclasificar el paquete en cada router.

2.3 Aggregate Route-Based IP Switching (ARIS)

El concepto de ***ARIS*** fue introducido por ***IBM***. Su principal logro fue mejorar el procesamiento de IP y otros protocolos de capa 3 (red) utilizando una conmutación de datagramas acelerando la velocidad de los medios de transmisión.

Un ***Integrated Switched Router (ISR)***, es un switch que soporta el ruteo standard de capa 3. Una ruta conmutada es una ruta a lo largo de la red en la cual los datos pueden ser conmutados en un medio de transmisión. En una red que utiliza el envío convencional de datos, ARIS utiliza los ISR's en lugar de los switches/routers y las rutas de conmutación preestablecidas en los nodos de la red. Estos nodos son reconocidos por ARIS gracias a la información que proveen los protocolos ***OSPF*** y ***BGP***. Las rutas conmutadas son establecidas por el intercambio de mensajes en los ISR's. Al recibir un una serie de datos el ISR realiza las operaciones de búsqueda detallada para encontrar dentro de su base de información de envío la ruta conmutada asociada a su destino y transmitirla a esta. Si no es encontrada ninguna información asociada es enviada al siguiente dispositivo utilizando la ruta de envío standard.

A continuación se mencionan las principales características de ARIS:

Loop Prevention: ARIS previene la creación de loops en rutas conmutadas enviando una lista de ***"ISR ID"*** para establecer mensajes mientras las rutas son creadas, de esta manera ARIS puede hacer cambios en la ruta de una series de datos si encuentra un loop en la misma.

Explicit Routes: ARIS puede soportar la creación de rutas conmutadas a través de rutas explícitas en el caso de rutas bidireccionales o multicast.

Multicast: ARIS es capaz de establecer rutas conmutadas en configuración de punto-multipunto.

Label Conservation: ARIS permite la combinación de rutas conmutadas conservando su información traz haber sido utilizadas varias veces por la misma salida para un mismo destino.

Flexibility: A diferencia de otras tecnologías similares, ARIS puede funcionar aun en redes que contengan una combinación de routers convencionales y algunos ISR's.

L2 Tunneling: ARIS permite la creación de túneles de información, permitiendo que las etiquetas de encabezado establezcan mensajes hacia el ISR de entrada.

2.4 Cell Switching Router (CSR)

Esta tecnología fue introducida por ***Toshiba Corporation***, Japón. Toshiba basó su propuesta analizando las limitaciones de la solución IP/ATM, se dio cuenta que esta solución no podía trabajar con protocolos como RSVP y que tan solo el uso de reservación de recursos y flujos de tráfico IP tenía básicas limitaciones comparado con el mecanismo de conmutación de celdas de ATM. Fue entonces que propuso el CSR el cuál esta basado en una arquitectura de red que intenta combinar ambos aspectos ampliando las capacidades de los routers actuales para manipular la reservación de recursos y el flujo de información IP usando el esquema de capacidades de la conmutación de celdas de ATM.

Cell Switched Router es un router con la funcionalidad de la conmutación de celdas de ATM en adición a las capacidades de envío de datos convencional IP. Tal como en un grupo de datos IP ambas opciones el encabezado IP y los VPI/VCI de la conmutación de celdas están disponibles en el CSR. Un CSR puede permitir el paso de datos ensamblados o no concatenando la salida o entrada de VC's

(Virtual Containers) ATM. Existen dos diferentes tipos de VCs definidos entre uno o varios CSRs adyacentes y su host o router final.

1. ***Default VC:*** Para datos que son ensamblados o desensamblados en un CSR.
2. ***Dedicated VCs:*** Estos llevan flujo de información IP y pueden concatenarse con otros VC's.

La ruta para el envío de datos es definida en base a la tabla de ruteo de entrada de cada CSR. La ruta para VC's entre dos CSR's adyacentes se determina utilizando protocolos de ruteo ATM como ***PNNI (Network Node Interface Protocol)***. Al ingresar a un router/host se realiza el trabajo de clasificación de flujo. Aquí se examina el encabezado de cada flujo de datos y se toma la decisión de si es enviado como default o dedicated VC. Los CSR's intermedios examinan el VPI/VCI de las celdas de entrada y si existe una entrada en la tabla de ruteo de ATM entonces las celdas son conmutadas, si no, se ensamblan nuevamente y se envían en base a la entrada de la tabla de ruteo IP.

Como características principales se debe mencionar su capacidad para brindar servicios multicast y la flexibilidad de cambiar de ruta dinámicamente en caso de que encuentre un problema o error sobre la misma.

2.5 Resumen de Soluciones

En resumen todas las soluciones de conmutación IP (incluido MPLS) se basan en dos componentes básicos comunes:

- la separación entre las funciones de control (ruteo) y de envío (forwarding)
- el paradigma de intercambio de etiquetas para el envío de datos

En la figura 2.1 se representa la separación funcional de esas dos componentes, una de control y la 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 enrutamiento. 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. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde el interfaz de entrada al de salida a través del correspondiente hardware de conmutación.

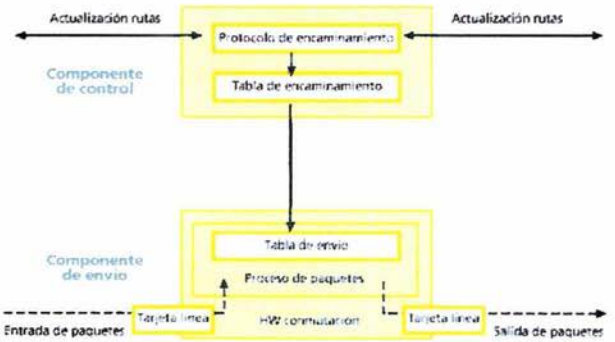

Figura 2.1. Separación entre las funciones de control (Routing) y de envío (Forwarding).

Al separar la componente de control (enrutamiento) de la componente de envío, cada una de ellas se puede implementar y modificar independientemente. El único requisito es que la componente de enrutamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a ATM. 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.

2.6 Origen de la solución IP/ATM

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI...). Por otro lado, los ***backbones IP*** que los Proveedores de Servicio de Red (NSP) habían comenzado a desplegar en esos años, estaban construidos a base de routers conectados por líneas dedicadas ***T1/E1*** y ***T3/E3***. El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los NSPs fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los NSPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces, se dieron cuenta que con los protocolos habituales de enrutamiento basados en métricas del menor número de saltos, no era posible optimizar efectivamente el ancho de banda global en las redes por lo que había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar las capas 2 y 3 estaba el hecho de las infraestructuras de redes ATM desplegadas por los operadores de telecomunicaciones. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los NSPs. Por un lado, proporcionaban mayores velocidades (155 Mpbs) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red IP/ATM

pronto ganó adeptos entre la comunidad de NSPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento 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 comunica con el resto mediante los ***circuitos virtuales permanentes*** **(PVCs, *Permanent Virtual Circuits*)** que se establecen sobre la topología física de la red ATM. 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 2.2 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

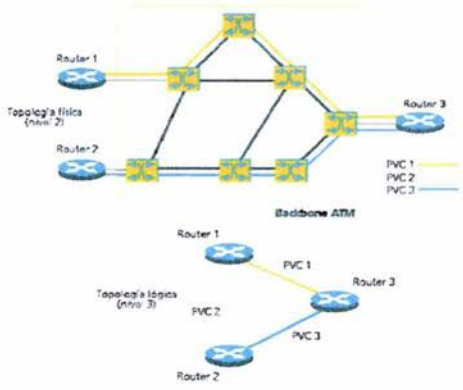

Figura 2.2. Topología Física de una Red ATM vs Topología Lógica IP.

La base del modelo IP/ATM 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 años 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En la figura 2.3 se representa el modelo IP/ATM con la separación de funciones entre lo que es ***routing IP en capa 3 (control y envío de paquetes) y lo que es conmutación en capa 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.

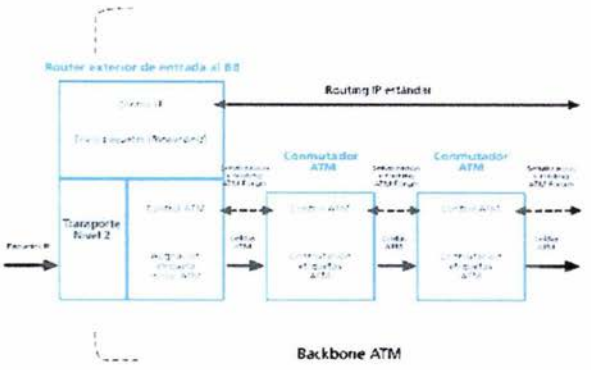

Figura 2.3. Modelo IP/ATM, separación de capas 3 y 2.

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. En los casos de los NSPs de primer nivel, ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de la 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 sus subinterfaces en los routers con los PVCs, a través de los cuales los routers se intercambian la información de encaminamiento correspondiente al protocolo interno ***IGP (Interior Gateway Protocol)***. Lo habitual es que, entre cada par de routers, haya un PVC principal y otro de respaldo, que entre automáticamente en funcionamiento cuando falle el principal.

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costos de gestión global de sus redes. Además, existe 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 los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada.

De lo anterior podemos concluir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de capas 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas a diferencia de MPLS que logra esa integración de niveles sin discontinuidades, como se verá en el siguiente capítulo.

Capítulo III. Descripción Funcional de MPLS

3. Descripción funcional de MPLS

MPLS ***(Multiprotocol Label Switching)*** significa ***Multiprotocolo de Conmutación de Etiquetas***, multiprotocolo porque sus técnicas son aplicables a **CUALQUIER** protocolo de capa de red. MPLS es un estándar emergente del IETF que surgió para condensar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90.

Los problemas que presentan las soluciones actuales de IP/ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS al combinar en uno solo lo mejor de cada nivel ***(la inteligencia del routing con la rapidez del switching)***.

3.1 Insuficiencias del protocolo IP

La tendencia tecnológica actual consiste en la consolidación de los tipos de tráfico más importantes en el protocolo IP. Las soluciones de telefonía, vídeoconferencia y las aplicaciones científicas de banda ancha están cada día más solicitadas. Además, los flujos de audio y vídeo corresponden a servicios en tiempo real. Por ello exigen tiempos de transporte muy cortos y una transferencia con muy poca inestabilidad, es decir, regular. Las aplicaciones tradicionales (web, correo electrónico, transferencia de archivos) admiten plazos más importantes pero, en cambio, requieren una tasa de pérdida de paquetes confiable. Junto a los servicios de punto a punto tradicionales también empiezan a aparecer servicios multipuntos,

servicios de difusión y servicios de redes privadas virtuales **(VPNs)** para los que hay que gestionar la calidad del servicio **(QoS)**.

Dado este contexto, el principio de ***"best effort"*** propio de la pila de protocolos **TCP/IP** no ofrece ya garantías suficientes. Para hacer frente a las nuevas condiciones y ofrecer una calidad de servicio adecuada, los ingenieros pueden recurrir a redes de mayor tamaño. No obstante, ésta es una solución a corto plazo ya que el tráfico no para de aumentar y, como un gas perfecto, tiende a ocupar rápidamente toda la banda de paso disponible. Incluso en los enlaces muy poco cargados, los picos de tráfico muy cortos ocasionan a veces degradaciones del rendimiento inaceptables para las aplicaciones en tiempo real. Por último, la expansión y la interconexión de las redes hacen que los cuadros de encaminamiento sean cada vez más complejos de gestionar.

3.2 Definición de Conceptos

Antes de comenzar la descripción de las funciones del protocolo MPLS, es útil clarificar algunos de los conceptos que serán utilizados a lo largo de este capítulo, algunos de ellos serán mencionados a detalle más adelante.

DLCI	Nombre usado en Frame Relay para la identificación de circuitos.
FEC (Forwarding Equivalence Class)	Conjunto de paquetes que se envían sobre el mismo camino a través de una red, aún cuando sus destinos finales sean diferentes.
Label	Es un identificador corto de longitud fija, el cuál es utilizado para identificar una clase de FEC, usualmente de relevancia local.

(LSP) Label Switched Path	La ruta unidireccional que se establece mediante la conmutación de etiquetas a través de uno o más LSR en un dominio MPLS.
(LSR) Label Switching Router	Es un nodo MPLS con capacidades de envío y conmutación de paquetes de capa 3 nativos.
Capa 2	Es la capa de enlace (envío) de protocolo OSI por debajo de la capa de ruteo ó capa 3 que ofrece los servicios usados por el nivel de capa 3. Cuando el envío se hace por intercambio de etiquetas de longitud corta y fija ocurre en capa 2 aún cuando la etiqueta examinada sea un VPI/VCI de ATM, un DLCI de Frame Relay ó una etiqueta de MPLS.
Capa 3	Es la capa de protocolo OSI en el que operan IP y sus protocolos de ruteo asociados con los sinónimos de nivel de enlace y capa 2.
Label Stack	Conjunto ordenado de etiquetas.
Dominio MPLS	Configuración de un grupo de nodos contiguos los cuales operan funciones de ruteo y envío MPLS y pertenecen también a un mismo dominio de Ruteo o Administración.
LER	Es un nodo MPLS que conecta un nodo fuera de dominio (ya sea porque este no corra en MPLS o porque pertenezca a un dominio diferente) al dominio MPLS. Por ejemplo un nodo frontera sería aquel LSR que tenga un host vecino que no funcione con MPLS.
LER de salida	Es aquel nodo de frontera MPLS que maneja el tráfico saliente de un dominio MPLS.
LER de entrada	Es aquel nodo de frontera MPLS que maneja el tráfico entrante a un dominio MPLS.

MPLS Label	Es la etiqueta que es transportada en un paquete de encabezado y que representa la FEC de un paquete.
Nodo MPLS	Es un nodo que puede correr en un ambiente MPLS. Un nodo MPLS tendrá los protocolos de control MPLS, deberá operar uno o más protocolos de ruteo de capa 3, y ser capaz del envío de paquetes basado en la conmutación de etiquetas. Opcionalmente un nodo MPLS debe poder enviar paquetes nativos de capa 3.
VPI/VCI	Es una etiqueta usada en redes ATM para identificar circuitos.

A continuación se enlista una serie de acrónimos y abreviaturas utilizados para definir algunos conceptos de este capítulo.

ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
DLCI	Data Link Circuit Identifier
FEC	Forwarding Equivalente Class
IGP	Interior Gateway Protocol
BGP	Border Gateway Protocol
IP	Internet Protocol
LDP	Label Distribution Protocol
LSP	Label Switched Path
LSR	Label Switching Router
MPLS	Multi-Protocol Label Switching
TTL	Time To-Live
VCI	Virtual Circuit Identifier
VPI	Virtual Path Identifier

3.3 Elementos básicos de MPLS

3.3.1 MPLS Label

Una etiqueta o ***"label"*** MPLS es un identificador corto de longitud fija, el cuál es utilizado para identificar una clase de **FEC**. La etiqueta que se pone en un paquete determinado representa la clase FEC asignada al paquete.

Un paquete es asignado a una FEC en base (completamente o parcialmente) a su dirección de destino de nivel de red. Sin embargo, la etiqueta asignada a ese paquete nunca es una codificación de esta dirección.

La MPLS label (Figura 3.1) está formada por 20 bits, además contiene los campos **EXP** ***(Experimental)*** de 3 bits utilizados para diferenciar **Clases de Servicio** ***CoS*** y propagarlas a través de su correspondiente LSP, **S** ***(Stacking bit)*** de un bit para poder apilar etiquetas de forma jerárquica y el campo **TTL** ***(Time to Live)*** de 8 bits el cuál indica durante cuanto tiempo se considera válido el paquete, si este es excedido el paquete será descartado.

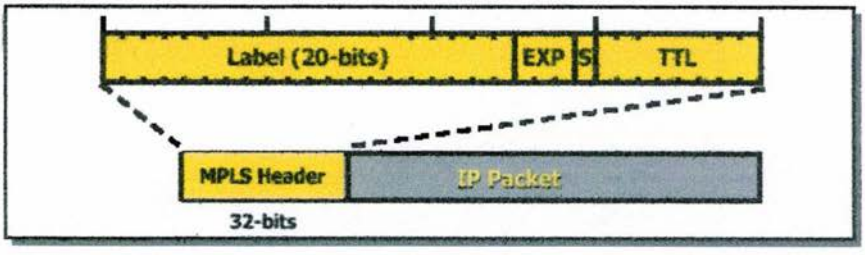

Figura 3.1. MPLS Label.

La MPLS label es también conocida como ***"shim header"***. Debido a su estructura la cuál encapsula los paquetes IP (capa 3) para su envío (capa 2). El protocolo MPLS se ubica insertado entre la capa 2 y la capa 3 del modelo OSI como lo indica la figura 3.2.

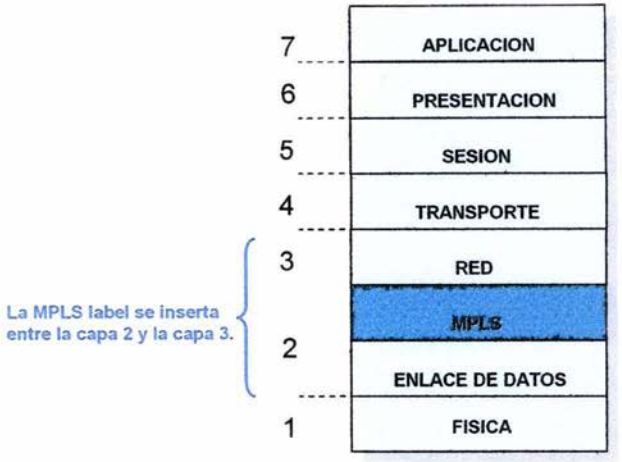

Figura 3.2. Ubicación de la MPLS label en el modelo OSI.

Alternativamente la MPLS label, puede funcionar sobre cualquier tipo de transporte: PPP, Ethernet, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas, se utilizan estos campos nativos, por ejemplo los campos DLCI de Frame Relay y VPI/VCI de ATM. Sin embargo, si la tecnología de capa 2 empleada no soporta un campo para etiquetas, por ejemplo enlaces de PPP o LAN, entonces se emplea un encabezado genérico MPLS de 32 bits, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del capa 2 y la del paquete de capa 3, ver figura 3.3.

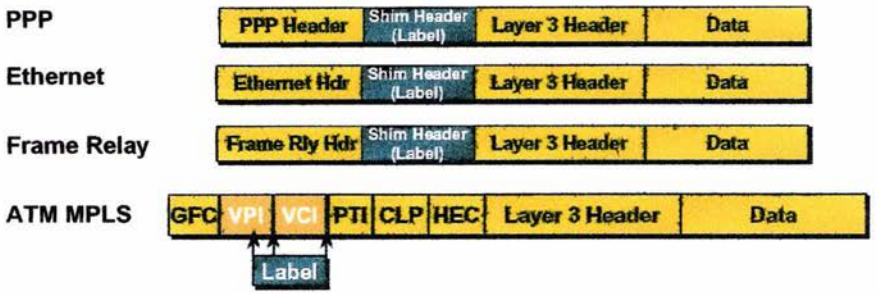

Figura 3.3. Ejemplos de encapsulación del *"shim header"* ó MPLS label en diferentes tipos de transporte.

3.3.2 Dominio MPLS

Un dominio MPLS se puede definir como un conjunto contiguo de nodos con funcionalidad MPLS y que pertenecen a un mismo dominio de enrutamiento IP.

Tal como se muestra en la figura 3.4 un dominio MPLS puede contener los siguientes elementos:

***LER* (Label Edge Router)**. En un nodo MPLS capaz de conectar un dominio MPLS con nodos externos al dominio (comúnmente porque éstos no soporten MPLS o porque pertenezcan a otro dominio MPLS diferente).

***LSR* (Label Switch Router)**. Es un nodo interno de un dominio MPLS que conmutan los paquetes en función de la etiqueta. En algunos casos dependiendo de la implementación y configuración, pueden conmutar también en función de la cabecera IP.

***LSP* (Label switched Path)**. Se denomina así cada uno de los caminos unidireccionales que se establecen mediante conmutación de etiquetas en un dominio MPLS.

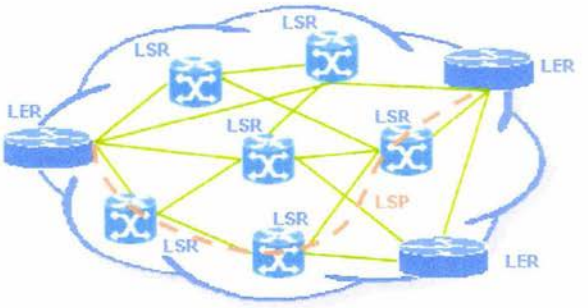

Figura 3.4. Elementos de un Dominio MPLS.

3.3.3 Retención de etiquetas

A continuación se describen los modos de distribución y retención de etiquetas que los LSRs utilizan para identificar las interfaces y etiquetas donde están conectados a otros LSRs a través de la red.

Teniendo en cuenta las posiciones relativas de dos LSRs para un determinado **FEC** (Figura 3.5) se define como ***Upstream LSR*** (LSR de ascenso) a aquel ruteador que envía los paquetes, mientras que el que los recibe es identificado como ***Dowstream LSR*** (descenso).

Figura 3.5. LSR Upstream y LSR downstream.

La arquitectura MPLS permite dos métodos para relacionar LSRs vecinos para la asignación de etiquetas.

El primero de ellos es el ***downstream on demand***, el cuál permite que un LSR Upstream haga una petición explícita de una etiqueta para un determinado FEC al LSR downstream del siguiente salto en la ruta. (Figura 3.6)

Figura 3.6. Downstream on Demand.

El segundo método es el ***unsolicited downstream***, este permite que un LSR downstream asigne una etiqueta sin que haya recibido una petición explícita. (Figura 3.7)

Figura 3.7. Unsolicited Downstream.

Una vez que un LSR ha recibido la asignación de una etiqueta para un determinado FEC, puede adoptar dos estrategias distintas para la retención o conservación de dicha asignación.

Si el LSR monitoriza la asignación y conoce cuando deja de estar activa y por tanto dicha asignación ha dejado ser válida y se puede descartar, su comportamiento se conoce como ***Modo Conservador de Retención de Etiquetas (Conservative Label Retention Mode)***. Este modo de operación tiene el inconveniente de que si se quiere volver a establecer la relación entre FEC y etiqueta es necesario repetir el procedimiento de asignación; pero al mismo tiempo tiene la ventaja que sólo permanecen asignadas aquellas etiquetas que realmente están en uso.

La segunda aproximación consiste en que una vez que el LSR ha recibido una asignación la mantiene indefinidamente. Este modelo, conocido como ***Modo Liberal de Retención de Etiquetas (Liberal Label Retention Mode)***, tiene el inconveniente del alto consumo de etiquetas; mientras que tiene la ventaja de que si se quiere volver a establecer la relación entre FEC y etiqueta no es necesario repetir el procedimiento de asignación.

3.4 Rutas Explícitas

Un concepto asociado a los LSPs es el conocido como ***Ruta Explícita***, la cuál es básicamente una secuencia de LSRs en un dominio MPLS. No es estrictamente necesario que se defina completamente desde un LER de entrada a un LER de salida, ya que una ***Ruta Explícita*** puede contener solamente la especificación de una parte del camino dentro del dominio.

Si la ***Ruta Explícita*** se define desde la entrada hasta la salida del dominio no es necesario utilizar ningún algoritmo de enrutamiento, pero si la ***Ruta Explícita*** sólo incluye una parte del camino (por ejemplo, desde el LER de entrada hasta un LSR en el interior del dominio), el resto (del último LSR de la **Ruta Explícita** hasta el LER de salida) se obtiene con ayuda de los algoritmos de enrutamiento.

3.5 Operación de MPLS

En esencia el procedimiento de operación de la arquitectura MPLS se puede describir en cinco puntos:

1. Las tablas de enrutamiento se construyen mediante los algoritmos de enrutamiento interiores como ***OSPF (Open Shortest Path First)*** o ***RIP (Routing Information Protocol)*** o exteriores como ***BGP***. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de enrutamiento que proporciona el protocolo de distribución de etiquetas. Cada entrada de la tabla contiene un par de etiquetas de entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LERs sólo hay

una etiqueta, de salida o de entrada de acuerdo al flujo de datos). En la figura 3.8 se ilustra un ejemplo del funcionamiento de un LSR de un dominio MPLS. A un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

Figura 3.8. Ejemplo de tabla de intercambio de etiquetas en un LSR.

2. Las rutas LSP se construyen mediante tablas de intercambio de etiquetas entre LSRs adyacentes. Los LSPs se establecen para un sentido del tráfico en cada punto de entrada a la red, para el tráfico bidireccional 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 LSR a otro, a través del dominio MPLS. Las etiquetas se distribuyen mediante un protocolo de distribución de etiquetas. No se especifica ninguno obligatoriamente y, a tales efectos, se puede utilizar el protocolo denominado **LDP**, definido específicamente para MPLS u otros protocolos como **RSVP** ***(Resource Reservation Protocol)*** o **CR-LDP** ***(Constraint-Based Routing – Label Distribution Protocol)***.

3. Cuando un paquete entra en el dominio MPLS a través del LER de entrada, éste lo etiqueta y lo envía al backbone por la ruta LSP correspondiente al FEC identificado por la etiqueta.

4. Los LSRs del backbone reenvían los paquetes a través del LSP mediante intercambio de etiquetas, no siendo necesario procesar las cabeceras del protocolo de la capa de red (dentro de un dominio MPLS los LSR ignoran la cabecera IP), solamente analizan la etiqueta de entrada, consultan la tabla de conmutación de etiquetas y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP.

5. Al llegar el paquete al LER de salida, ve que el siguiente salto lo saca del dominio MPLS, al consultar la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.

En la figura 3.9 se representa la transferencia de un paquete de datos a través de un dominio MPLS; el LER de entrada recibe un paquete IP (sin etiquetar) cuya dirección de destino es 212.95.193.1. Los LSR del backbone intercambian etiquetas sin analizar el encabezado IP y asignan etiquetas a diferentes clases FEC (en el ejemplo: 16, 20, 11, 9) a través de toda la LSP, para, finalmente, llegar al LER de salida donde la etiqueta es extraída y el paquete IP es enviado a su nodo destino.

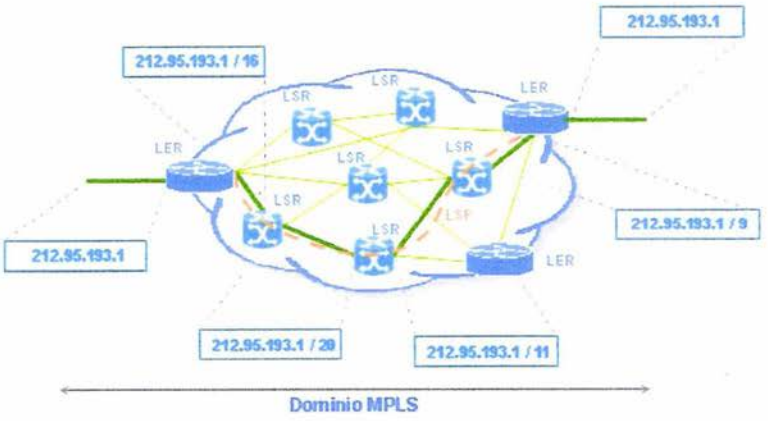

Figura 3.9. Transferencia de un paquete a través de un dominio MPLS.

3.6 Protocolos de Distribución de Etiquetas

Para establecer un LSP es necesario que cada elemento de un dominio MPLS tenga conocimiento de las etiquetas de entrada y salida de cada LSR en un dominio MPLS, el intercambio de esta información se realiza a través de los ***LDPs***, los cuáles generan toda la información de las tablas de enrutamiento en cada LSR en base a la topología, el patrón de tráfico de la red, las características de los enlaces, etc. Para construir las tablas de enrutamiento se utiliza la propia información de enrutamiento que manejan los protocolos ***IGP*** como ***OSPF, IS-IS, RIP***, etc.

En resumen podemos decir que MPLS crea un "camino de etiquetas" para cada "ruta IP" en la red a base de concatenar las etiquetas de entrada o salida en cada

tabla de los LSRs, después el protocolo interno correspondiente se encarga de pasar la información necesaria a través de la red.

3.6.1 Label Distribution Protocol (LDP)

Para que un LSR upstream intercambie la etiqueta de un paquete de entrada y lo envíe a su correspondiente LSR dowstream, el LSR upstream debe tener un método para identificar que valor debe tener la etiqueta que su LSR downstream esta esperando, este método es llamado protocolo de distribución de etiquetas.

Actualmente, existen varios protocolos tales como ***LDP***, ***CR-LDP***, ***RSVP*** ó ***BGP*** que pueden ser utilizados para la distribución de etiquetas entre LSRs.

El ***RFC 3031*** del IETF que describe la arquitectura de MPLS no establece el uso específico de un protocolo de distribución de etiquetas en particular, de hecho, el uso de cualquier protocolo dependerá de los requerimientos que deba cumplir para cada tipo de red.

El LDP fue diseñado con una única función: ***la distribución de etiquetas***, por lo que no realiza funciones de ***quality of service (QoS)***. Es decir no esta habilitado para seleccionar o reservar recursos para un LSP. Por tal motivo es necesario sumar a sus capacidades las de un protocolo de reservación de recursos o utilizar un protocolo que pueda realizar funciones de distribución de etiquetas y pueda soportar reservación de recursos como el protocolo RSVP. Los protocolos de distribución que pueden extender sus capacidades para reservar recursos son LDP y BGP.

El IETF define al LDP como la configuración de procedimientos y mensajes con los que se establece un LSP a través de la red utilizando la información de ruteo

de capa 3 directamente sobre las rutas conmutadas de la capa 2 de transmisión de enlace. Sin embargo es necesario asegurarse que estos LSPs puedan soportar funciones de ingeniería de tráfico ***(TE)*** y definir clases de servicio ***(CoS)***. Como en el caso anterior el LDP por si solo no tiene estas capacidades por lo que ha sido extendido para obtener funciones de ruteo basado en restricciones ***(constrain based routing)*** de allí el nombre de ***CR-LDP***.

CR-LDP no es el único protocolo que ofrece esta funcionalidad; RSVP puede proporcionar casi los mismos beneficios que el CR-LDP, pero además añade a sus capacidades la ingeniería de tráfico, es por eso que también se le conoce como ***RSVP-TE***. En resumen podemos afirmar que cada protocolo de señalización funciona para lograr el mismo resultado final en la red, por lo que utilizar cualquiera de ellos dependerá de las necesidades particulares de cada red.

3.6.2 CR-LDP

El protocolo ***CR-LDP*** esta basado en el cálculo de trayectos o caminos que están sujetos a ciertas restricciones de ancho de banda, los requisitos de ***CoS*** (demora, variación de demora o jitter) o cualquier otro requisito asociado al trayecto que defina el operador de red. El protocolo CR-LDP se ha desarrollado expresamente para soportar el establecimiento y mantenimiento de LSPs enrutados en forma explícita.

El protocolo CR-LDP es una de las herramientas más útiles de las que disponen los operadores para controlar el dimensionamiento de tráfico de red y ofrecer las ventajas de las clases de servicio ***CoS*** para sus clientes o usuarios.

Las extensiones actuales del protocolo CR-LDP incluyen los elementos de información necesarios para soportar el enrutamiento explícito y la modificación de los LSPs, pero carecen de los algoritmos necesarios para computar los trayectos según los criterios definidos por el operador de red.

Las principales limitaciones de este protocolo son las siguientes:

- Sólo se soportan LSPs punto a punto.
- Sólo se soportan LSPs unidireccionales.
- Sólo es soportada una única etiqueta por LSP.

A continuación se detalla el proceso de creación de un LSP (en una ruta explícita (ER)), bajo el protocolo ***CR-LDP***, ver figura 3.10:

1. El LER de entrada quiere establecer un nuevo LSP hacia el LER de salida. Los parámetros de tráfico determinan por dónde debe pasar la ruta, así que el LER de entrada reserva los recursos que necesita y envía un mensaje ***LABEL_REQUEST*** con la ruta explícita hacia el LER de salida y con los parámetros de tráfico que requiere la sesión.
2. Cada nodo de la ruta que recibe el mensaje reserva los recursos y determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje ***LABEL_REQUEST*** eliminándose de la ruta. Puede reducir la reserva si los parámetros de tráfico están marcados como negociables.
3. Una vez que llega al LER de salida, éste realiza cualquier negociación final sobre los recursos y hace la reserva. Asigna una nueva etiqueta al nuevo LSP y la distribuye en un mensaje ***LABEL_MAPPING*** que contiene los parámetros de tráfico finales reservados para el LSP.
4. Los LSRs intermedios emparejan los mensajes ***LABEL_REQUEST*** y ***LABEL_MAPPING*** que han recibido según el identificador de LSP,

asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje ***LABEL_MAPPING***.

5. En cuanto llegue al LER de entrada se habrá establecido el LSP.

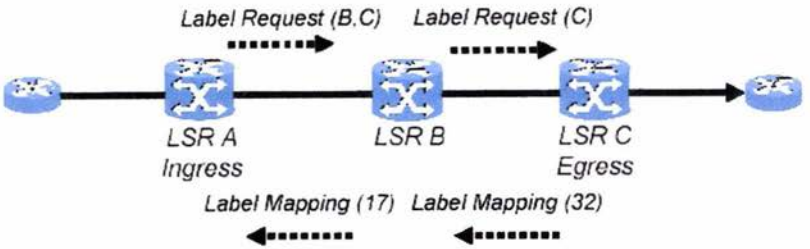

Figura 3.10. Protocolo CR-LDP.

3.6.3 RSVP-TE

Otra de las opciones actualmente consideradas para la distribución de etiquetas es el protocolo ***RSVP.*** También es conocido como ***RSVP-TE***, este es una extensión del protocolo original RSVP que proporciona ingeniería de tráfico ***(TE)***. Como su nombre lo indica su característica principal es la de reservar recursos a través de la red para el envió de datos.

El funcionamiento del protocolo RSVP consiste en el establecimiento de ***"túneles LSP"*** para la reservación de recursos. Se define como túnel LSP a aquel flujo de datos asociado a un LSP que es introducido virtualmente a un túnel y que como característica principal no utiliza los procedimientos de enrutamiento y filtrado IP.

A continuación se detalla el proceso de creación de un LSP, bajo el protocolo RSVP ver figura 3.11:

1. El LER de entrada quiere establecer un nuevo LSP hacia el LER de salida. Los parámetros de tráfico determinan por dónde debe pasar la ruta, así que el LER de entrada envía un mensaje ***PATH*** con la ruta explícita hacia el LER de salida y con los parámetros de tráfico que requiere la sesión.

2. Cada nodo de la ruta que recibe el mensaje determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje ***PATH*** eliminándose de la ruta. En cualquier caso cada LSR creará una nueva sesión.

3. Una vez llega al LER de salida, éste determina qué recursos ha de reservar y devuelve un mensaje ***RESV*** que distribuirá la etiqueta que ha elegido para ese LSP y contendrá los detalles de la reserva.

4. Los LSRs intermedios emparejan los mensajes ***PATH*** y ***RESV*** que han recibido según el identificador de LSP, reservan los recursos que indica ***RESV***, asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje ***RESV***.

5. El LER de entrada, cuando lo recibe, enviará un mensaje de confirmación ***RESVConf*** para indicar que se ha establecido el LSP.

Después de haberse establecido el LSP se enviarán mensajes periódicos para mantener el camino y las reservas.

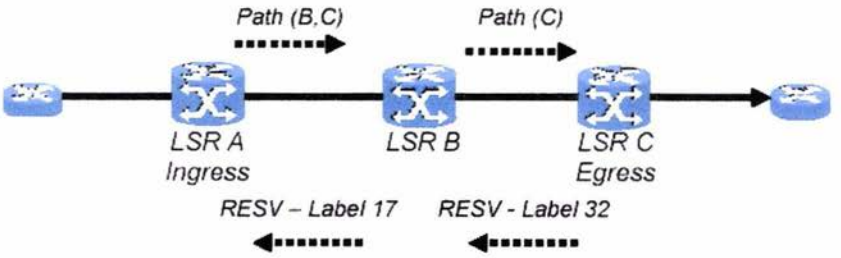

Figura 3.11. Protocolo RSVP.

3.6.4 Comparación de ambos protocolos de señalización

- ***RSVP*** es un protocolo ***soft state***, lo cual significa que la información es intercambiada cuando se establece el LSP, pero se deben enviar mensajes periódicos para notificar que la conexión todavía se requiere. Por el contrario, ***CR-LDP*** es del tipo ***hard state***, es decir, toda la información se intercambia al iniciar la conexión y no se produce más información adicional hasta que el LSP se elimine.
- El hecho que ***RSVP*** sea ***soft state*** e introduzca una sobrecarga adicional hace que no sea escalable ya que esta sobrecarga crecerá proporcionalmente con el número de sesiones RSVP. Para evitar esto se intenta resumir la información y aprovechar un único mensaje para enviar varios mensajes de refresh.
- ***CR-LDP*** utiliza conexiones TCP lo que hace que éstas sean más fiables y seguras, mientras que RSVP utiliza ***UDP (Universal Distribution Protocol)*** ó datagramas IP para establecer las comunicaciones, lo que supone mayor vulnerabilidad aunque puede utilizar ***IPSec*** o algún otro esquema de encriptación.
- Las conexiones TCP de CR-LDP permiten detectar un fallo mediante notificaciones propias de TCP. Esta notificación se procesa rápidamente así que las acciones se realizan oportunamente. Sin embargo, una conexión fallida en RSVP será detectada cuando no se reciba un determinado mensaje de refresh y, dependiendo de cómo se haya configurado, detectar un fallo puede tardar segundos o minutos antes de que puedan iniciarse las acciones de recuperación.
- RSVP-TE puede crear una nueva ruta a partir de un salto diferente en un LSR, así, en el momento en que se detecte el fallo refrescará esta nueva ruta que pasará a ser operativa y, la antigua se eliminará cuando deje de recibir mensajes de refresh.

- Otra alternativa que soportan ambos protocolos es crear una ruta completa alternativa mientras se usa la antigua, en el momento que se produzca un fallo la nueva ruta será operativa y se eliminará la antigua.
- CR-LDP soporta que un LSP dé servicio a muchos hosts mediante la designación de FECs, mientras que RSVP sólo reserva ancho de banda a una única dirección IP.

En resumen la elección entre los diferentes protocolos de distribución de etiquetas se deberá a factores como la complejidad de la red, la longitud de las conexiones, el grado de tolerancia a fallas, etc.

3.6.5 IGP

IGP's son protocolos de ruteo utilizados dentro de ***sistemas autónomos (AS)*** para proveerlos de las capacidades de ruteo dentro de estos sistemas. La mayoría de los protocolos de ruteo utilizados actualmente están basados en dos modelos diferentes: ***distante vector*** y ***link state***.

Comúnmente los protocolos de tipo link state son ***OSPF*** y ***IS-IS***. En la plataforma MPLS estos son utilizados para soportar la construcción de LSPs reuniendo requerimientos específicos de ***QoS***.

Los protocolos ***IGP*** también son utilizados en MPLS para determinar el ***next hop label fowarding entry (NHLFE)***. El NHLFE es utilizado en MPLS cuando un paquete etiquetado es enviado con la información de su siguiente salto y contiene el detalle de que hacer con los datos del paquete recibido.

3.6.6 BGP

BGP es un protocolo de ruteo que normalmente es utilizado entre ***(AS)*** para proveerlos de las capacidades de ruteo entre estos sistemas. Actualmente esta siendo ampliamente desarrollado para interconectar a los grandes proveedores de servicios de red dentro de Internet. En la plataforma MPLS también puede utilizarse para distribuir la información de anuncio de etiquetas para cada ruta.

Capítulo IV. Aplicaciones de MPLS

4. Aplicaciones de MPLS

Las aplicaciones de MPLS pueden resumirse en una sola frase:

"Flexibilidad de ingeniería y calidad de servicio."

TE, MPLS facilita el enrutamiento de paquetes para rutas configuradas previamente, en función de criterios como, por ejemplo, la baja tasa de carga, el reparto de la carga por varias rutas o la necesidad de restaurar un enlace en menos de 60 milisegundos en caso de avería de circuito, etc. Los sistemas intermedios situados en el backbone de la red tratan las informaciones primarias que contienen las etiquetas mucho más rápidamente ya que la decisión de enrutamiento está establecida previamente. Por ello, los paquetes circulan más rápido y los recursos de los ruteadores y de los conmutadores están menos solicitados.

CoS, Una etiqueta MPLS puede asociarse a un flujo aplicativo específico, lo cual permite distinguirlo de los otros, todo lo contrario a el protocolo IP, que no diferencia las aplicaciones. Las aplicaciones que exigen una banda de paso garantizada y estable, como vimos antes, pueden recibir un trato prioritario.

VPN, Una etiqueta MPLS puede asociarse a un origen o destino y con ello se facilita la creación de circuitos virtuales privados (VPN), que comparten una infraestructura física común. Como ya veremos más adelante, estos VPN permiten agregar tipos de tráfico que presentan características comunes, lo cual tiene ventajas tanto en lo que se refiere a los recursos de la red como a la seguridad y a la gestión de la facturación. Además, la jerarquía de las etiquetas MPLS permite construir VPNs que no necesitan ninguna modificación en el espacio de la

dirección IP de los clientes y que coexisten con la red MPLS que algunos clientes podrían establecer entre sus diferentes sitios.

De manera general, la implantación de MPLS en una red permite a los ingenieros mejorar el rendimiento del backbone de la red y controlar la calidad del servicio, dejando al mismo tiempo que sus miembros gestionen su propio tráfico como deseen.

MPLS refuerza los servicios que se ofrecen en cualquier red de nueva generación, sus principales aplicaciones son:

- Ingeniería de tráfico ***(TE)***.
- Clases de servicio ***(CoS)***.
- Servicio de redes privadas virtuales ***(VPN)***

4.1 Ingeniería de tráfico

Ingeniería de tráfico es el proceso donde los datos son enrutados a través de la red de acuerdo a la disponibilidad de sus recursos físicos. La idea es mejorar el rendimiento global de la misma equilibrando de forma óptima el uso de sus recursos y evitado saturaciones de tráfico en un sector de esta mientras otros se encuentren subutilizados. Un factor importante para la Ingeniería de Tráfico es determinar ***clases de servicio*** y ***calidades de servicio*** las cuales serán detalladas adelante en este mismo capítulo.

La ingeniería de tráfico puede administrarse a través de operadores manuales, ellos pueden administrar el estado de la red, enrutar manualmente el tráfico o aprovisionar recursos adicionales para compensar los problemas que detecten en cualquier momento.

Otra alternativa es dejar que la ingeniería de tráfico sea manejada por procesos automatizados que reaccionen de acuerdo a una retroalimentación del estado de la red a través de los protocolos de ruteo.

La ingeniería de tráfico provee a la red del mejor uso de sus recursos, extendiendo la carga sobre enlaces de capa 2 y permitiendo reservar algunos de estos enlaces para cierta clase de tráfico o para un cliente en particular. En la actualidad uno de los principales usos de MPLS es mejorar el desempeño de los backbones de redes de ***ISPs*** a través de la ingeniería de tráfico.

La ingeniería de tráfico tiene la habilidad de mover flujos de tráfico a través de la ruta más corta seleccionada por el protocolo ***IGP*** hacia una ruta potencialmente menos congestionada a través de la red (ver figura 4.1).

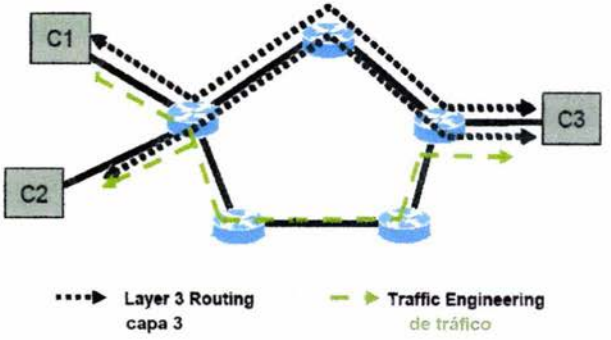

Figura 4.1. Ingeniería de tráfico.

La ingeniería de tráfico es capaz de proveer las siguientes características:

- Enrutar rutas primarias rodeando puntos altamente congestionados en la red.
- Proveer de controles precisos de información cuando es necesario reenrutar el tráfico debido a fallas en su ruta primaria.

- Proveer de un uso eficiente el ancho de banda disponible en agregados y en fibra óptica de larga distancia asegurándose de que ningún sector de la red este sobreutilizado mientras otros se encuentren subutilizados.
- Maximizar la eficiencia operacional de la red.
- Reforzar las características de la orientación de tráfico, minimizando la pérdida de paquetes, los periodos de congestión, etc.
- Mejorar estadísticamente las características de comportamiento de la red (tales como: proporción de pérdidas, variación de retardos, retardo de transferencias, etc.), requeridas para soportar las aplicaciones multiservicio de Internet.

La ingeniería de tráfico es esencial para los backbones de proveedores de servicios y para los ISPs. Cada backbone debe soportar una alta carga de transmisión de servicios, por lo que las redes deben ser lo suficientemente flexibles para poder mantener su funcionamiento aún cuando existan nodos o enlaces dañados en la misma.

Las características de ingeniería de tráfico en MPLS están integradas en la capa 3, la cuál optimiza el enrutamiento de tráfico IP, de acuerdo a las restricciones de la topología y capacidad del backbone en la red.

La ingeniería de tráfico en MPLS enruta flujos de tráfico a través de la red de acuerdo a los recursos necesarios del flujo enrutado y a los recursos disponibles en la red. MPLS utiliza el ruteo basado en restricción (constrain-based routing) para encontrar la ruta más corta que reúna los requerimientos del flujo de tráfico. Estos requerimientos pueden ser: ancho de banda, medio de transmisión, prioridad sobre otros flujos, etc.

MPLS puede adaptarse hábilmente a los cambios que pueda sufrir una red, ajustándose a una cambiante serie de restricciones basadas en fallas en la red, tales como enlaces o nodos dañados.

4.1.1 Funcionamiento de la ingeniería de tráfico en redes MPLS

La ingeniería de tráfico en MPLS establece y mantiene automáticamente túneles LSP a través del backbone usando el protocolo RSVP. La ruta utilizada por cualquiera de ellos estará definida de acuerdo a los requerimientos de sus recursos y a los recursos mismos de la red.
El protocolo IGP, automáticamente enruta el tráfico dentro de estos túneles LSP. Típicamente, un paquete que cruce una red MPLS viajará en un único túnel que conecte su punto de entrada con el de salida.

La Ingeniería de Tráfico en MPLS se construye bajo los siguientes mecanismos:

- Túneles LSP, estos son señalizados con el protocolo RSVP-TE.
- Un enlace IGP (por ejemplo un enlace IS-IS ó OSPF).
- Un modulo de cálculo de rutas, que determine los caminos que deben utilizar los túneles LSP.
- Un módulo de administración de enlaces que se encargue de la admisión y respaldo de información de los recursos disponibles.
- Envío de etiquetas, el cual proporciona a los routers de capa 2 la capacidad de direccionar tráfico a través de múltiples saltos de acuerdo a un algoritmo de recursos de ruteo.

Una aproximación al diseño del backbone de una red con ingeniería de tráfico, sería definir una malla de túneles desde cada LER de entrada a cada LER de salida. El protocolo IGP que opera en el LER de entrada determina cuál flujo de tráfico debe enrutarse con cuál LER de salida. Los módulos de cálculo y señalización de rutas MPLS bajo el diseño de ingeniería de tráfico determinan la ruta tomada por el túnel LSP, este procedimiento esta sujeto a la disponibilidad de recursos y estado dinámico de la red.

Algunas veces, el flujo de tráfico es tan grande que no es posible enviarlo sobre un mismo túnel LSP. En este caso es posible enviar el flujo de datos en cargas compartidas a través de múltiples túneles LSP configurados entre el LER de entrada y el de salida.

4.1.2 Mapeo de tráfico dentro de Túneles LSP

Los protocolos IGP de enlace como el ***IS-IS ((intermediate System – Intermediate System)*** utilizan un algoritmo llamado ***Dijkstra's shortest path first (SPF)*** para identificar las rutas más cortas entre todos los nodos de una red y obtener las tablas de ruteo correspondiente. Estas tablas contienen toda la información de destinos y de ***"primer salto"*** para cada router. La expresión ***"primer salto"*** se refiere a la interfaz física más próxima desde el router destino.

Otros algoritmos utilizados en ingeniería de tráfico calculan rutas explícitas ***(ER)*** para uno o más routers en la red. El router de origen identifica las rutas explícitas como sus propias interfaces lógicas.

En adelante nos referiremos a las rutas explícitas únicamente como ***ER-LSP*** y como ***túneles TE*** a los túneles LSP de ingeniería de tráfico.

4.1.3 Identificación de SPF

Durante la identificación de ***SPFs (Shortest Path Found)***, el router encuentra la ruta más corta a un nodo específico en la red. Si ese nodo esta directamente conectado al router la información del "primer salto" se obtiene de la base de datos. Si la conexión no es directa al router, el nodo hereda la información del "primer salto" de otros nodos conectados a él. Cada nodo tiene uno o más nodos

conectados entre sí por lo que esta información puede derivarse de cualquier otra conexión.

Existen 3 formas para que un router determine la información de "primer salto":

1. Examinar la lista de routers de salida directamente alcanzables por la ruta de un túnel TE. Si existe un túnel TE hacia este nodo, debe utilizarse como información de "primer salto".
2. Si no hay un túnel TE y el nodo esta directamente conectado al nodo, se debe utilizar la información de la base de datos para determinar el "primer salto".
3. Si el nodo no está directamente conectado y no es alcanzable por algún túnel TE, la información de "primer salto" será copiada de cualquier nodo conectado a él.

Como resultado de esta identificación, el flujo de tráfico hacia nodos que están al final de la ruta de túneles TE fluye sobre estos. Tráfico de nodos en descenso hacia los nodos de salida también fluye a través de túneles TE. Si hay más de un túnel TE a diferentes nodos intermedios en la ruta al nodo de destino, el tráfico fluye sobre el túnel TE cuyo nodo de salida sea el más cercano al nodo de destino.

En resumen podemos decir que MPLS se adapta a la ingeniería de tráfico ya que permite:

- Que el administrador de red establezca ER-LSP por LSRs concretos.
- Obtener estadísticas de uso de cada LSP en detalle, es decir, cuánto tráfico se enruta por ellos y de qué tipo. Con esta información, se puede replanificar la red de forma que ofrezca un uso más eficiente de los recursos.
- Hacer Encaminamiento Restringido (*CBR, Constraint-Based Routing*), de modo que se pueden seleccionar rutas específicas para transportar el

tráfico de un tipo en concreto con unos requerimientos específicos. Esta posibilidad está directamente ligada a los Acuerdos de Nivel de Servicio ***(SLAs, Service Level Agreements)*** que un proveedor acuerde con el cliente, al que puede facturar así de un modo mucho más flexible y adaptable a sus necesidades. La ventaja de la Ingeniería de Tráfico MPLS es que se puede aplicar directamente sobre una red IP, independientemente de la infraestructura que le de soporte, con un mayor nivel de detalle y de forma más sencilla y eficiente que como se venía haciendo hasta el momento.

4.2 Clases de servicio (CoS)

La entrega de Clases de Servicio se ha convertido en una función indispensable para los más grandes proveedores de servicios de red debido a la estructura competitiva de la internet y a las diversas necesidades de sus clientes y usuarios.

La filosofía de una red orientada a ofrecer Calidad de Servicio se basa en la agrupación de los distintos tipos de tráfico, en un cierto número de Clases de Servicio, con diferentes prioridades.

Los paquetes pertenecientes a una misma Clase de Servicio tienen en común los mismos requerimientos de tratamiento en cuanto a ancho de banda, retardo, variación del retardo ***(jitter)*** y pérdida de paquetes, es decir, de Calidad de Servicio ***(QoS)***.

La capacidad de poder asegurar que un paquete en concreto recibirá, a lo largo de todo el dominio, el tratamiento requerido, se apoya en dos posibilidades, ambas estandarizadas por el IETF:

- ***IntServ (Integrated Services)***: apoyándose en el protocolo ***RSVP***, se reservan los recursos necesarios asociándose a LSPs concretos.
- ***DiffServ (Differenciated Services)***: orientado al tráfico IP, basa su funcionamiento en la clasificación del tráfico a la entrada de la red y en la asignación de prioridades mediante el campo de 8 bits ***DSCP (DiffServ Code Point)***. En función de este campo, cada nodo intermedio tratará el paquete de la forma adecuada. A este comportamiento se le denomina ***PHB (Per Hop Behaviour)***, implementado mediante diferentes algoritmos de cola como ***PQ (Priority Queuing)***, ***WPQ (Weighted Priority Queuing)***, etc.

Como se comenta en el párrafo anterior las clases de servicio permiten que los operadores de red puedan ofrecer ***Servicios Diferenciados*** a través de una red MPLS. Además pueden satisfacer un amplio rango de requerimientos de red especificando la clase de servicio aplicable a cada paquete IP transmitido. Diferentes clases de servicio pueden establecerse para paquetes IP, configurando un bit de precedencia IP en el encabezado de cada paquete.

Las clases de servicio de MPLS pueden soportar los siguientes servicios diferenciados.

- Clasificación de paquetes.
- Anulación de congestión.
- Administración de congestión.

La tabla 4.1 describe las clases de servicio MPLS y sus funciones:

SERVICIO	FUNCION DE CoS	DESCRIPCION
Clasificación de Paquetes	CAR (Commited access rate), Mecanismo de ancho de banda comprometido basado en la clasificación de paquetes al final de la red antes de que las etiquetas sean asignadas.	CAR utiliza bits de ToS (Type of service) en el encabezado IP para clasificar paquetes de acuerdo a la proporción de transmisiones de entrada y salida. El CAR es comúnmente configurado en interfaces al final de una red con la función de controlar el flujo de tráfico a la entrada o salida de una red. El CAR puede utilizar comandos para clasificar o reclasificar un paquete IP.
Anulación de congestión	Weighted random early detection ((WRED). Las clases de paquetes IP son diferenciadas de acuerdo a la probabilidad de disminución.	WRED monitorea el tráfico en la red para anticipar y prevenir congestiones en los cuellos de botella de la red. WRED puede descartar tráfico de baja prioridad cuando una interface empieza a congestionarse. WRED puede configurarse para diferentes clases de servicio.
Administración de congestión	Weighted fair queueing (WFQ). Las clases de paquetes IP se basan en los requerimientos de ancho de banda y sus características de retardo.	WFQ es un sistema automatizado que asegura una asignación de ancho de banda justa para toda la red. WFQ define prioridades para determinar cuanto ancho de banda debe asignar a cada clase de tráfico.

Tabla 4.1. Servicios diferenciados MPLS.

4.2.1 Beneficios de CoS en redes MPLS

Utilizando clases de servicio en una red de dominio MPLS, se pueden obtener los siguientes beneficios:

- Asignación eficiente de recursos
- Diferenciación de paquetes
- Mejoras a servicios futuros

- Mejoras en la ingeniería de tráfico en MPLS
- Contabilidad del flujo de tráfico de salida del dominio MPLS
- Transporte de AAL5 sobre MPLS
- Construcción de VPNs

4.2.2 Configuración del valor de CoS en MPLS

Cuando tráfico IP entra en un túnel LSP, el LER de entrada marca todos los paquetes IP con un valor de clase de servicio, el cual es utilizado en la transmisión de prioridad de cola. El valor de CoS es encriptado formando parte del encabezado MPLS, hasta que es removido a su salida del dominio MPLS por el LER de salida.

Las clases de servicio de MPLS trabajan en conjunto con las funciones de CoS comunes a los routers en general. Si los parámetros de CoS no son configurados, se utilizaran los valores predeterminados por el fabricante.

Existen dos formas de configurar los bits de clase de servicio en el encabezado MPLS:

- Con el número de la cola de rendimiento como el valor del paquete de CoS en conjunto con el ***packet lost priority (PLP)***.
- Configurando valores arreglados en todos los paquetes entrantes a un túnel LSP, esto quiere decir que todos ellos recibirán la misma clase de servicio.

El valor de CoS representa un valor decimal entre 0 y 7. Este número corresponde a tres dígitos binarios, los 2 bits de mayor valor representan cuál cola de transmisión será utilizada en la interface de salida.

El bit de menor valor representa el bit de PLP y se usa para seleccionar el perfil de la función RED. 0 no utiliza PLP, 1 utiliza PLP.

En la tabla 4.2 se observan los valores de CoS para MPLS.

VALOR DE CoS	BITS	TRANSMISIÓN DE COLA	BIT PLP
0	000	0	Not Set
1	001	0	Set
2	010	1	Not Set
3	011	1	Set
4	100	2	Not Set
5	101	2	Set
6	110	3	Not Set
7	111	3	Set

Tabla 4.2. Servicios diferenciados MPLS.

Como el CoS forma parte del encabezado MPLS, su valor es asociado a los paquetes mientras ellos viajan a través del túnel LSP. Este valor nunca permanece en el encabezado IP cuando sale del dominio MPLS.

4.3 Redes Privadas Virtuales (VPNs)

Una red privada virtual ***(VPN)*** se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones ***intra/extranet***, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y ***"privada"*** indica que el usuario ***"cree"*** que

solo el tiene acceso a los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet.

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 costos asociados. Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs.

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los ISPs, 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 costos 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.

Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:

- en el nivel 3, mediante el protocolo ***IPSec*** (IPsec es un protocolo de encriptación)del IETF.
- en el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un ISP.

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el encriptado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos ISPs que sigan el estándar IPSec. Pero como el encriptado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles IP de capa 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del ISP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede encriptar la información para mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles IP de nivel 2 está condicionada a un único proveedor.

A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

- están basadas en conexiones punto a punto (PVCs o túneles IP).
- la configuración es manual.

- la provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.
- plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.
- la gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremo a extremo (o circuitos virtuales) entre cada par de routers de cliente 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 ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una ***"nube común"*** en las que solamente pueden entrar los miembros de la misma VPN. Las ***"nubes"*** que representan las distintas VPNs se implementan mediante túneles LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los túneles LSPs son similares a los túneles IP en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles IP se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de enrutamiento IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar

técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

En la figura 4.2 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los túneles LSP está en que éstos se crean dentro de la red, a base de LSPs, y no de extremo a extremo a través de la red.

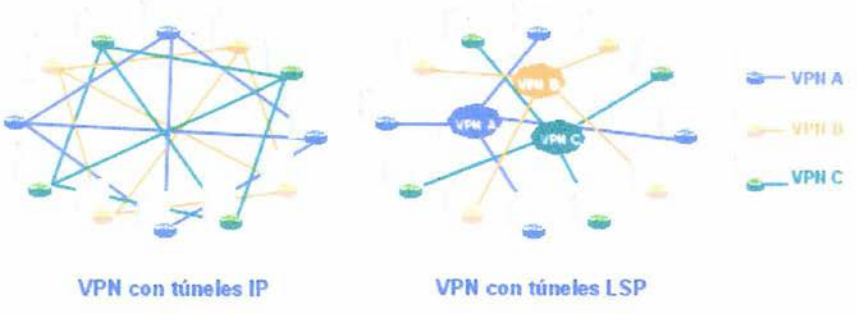

Figura 4.2. Comparación entre diferentes tipos de VPNs.

Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

- proporcionan un modelo ***"acoplado"*** o ***"inteligente"***, ya que la red MPLS ***"sabe"*** de la existencia de VPNs (lo que no ocurre con túneles IP ni PVCs).
- evita la complejidad de los túneles IP y PVCs.
- la provisión de servicio es sencilla: una nueva conexión afecta a un solo router.
- tiene mayores opciones de crecimiento modular.

- permiten mantener garantías ***QoS*** extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes ***clases de servicio***.
- permite aprovechar las posibilidades de ***ingeniería de tráfico*** para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo ***VPN***.

CONCLUSIONES

En los últimos años el desarrollo de las redes de comunicación ha creado grandes necesidades en el mercado, los requerimientos de servicios a menor costo al igual que la competencia son cada vez mayores.

A pesar de que hace varios años están presentes en el mercado tecnologías como ATM que satisfacen los requerimientos del mercado en el campo de las redes de alto desempeño y permiten ofrecer parámetros de calidad de servicio, los costos de estas tecnologías son muy elevados y en muchos casos su arquitectura no es lo suficientemente flexible para adaptarse a las necesidades de los clientes, además su integración con las redes existentes es muy complicada, como es el caso de las redes IP, siendo esta la tecnología de más amplio uso en este momento.

MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de enrutamiento IP (típicamente limitadas a encaminar por dirección de destino). Además de poder hacer ingeniería de tráfico, MPLS permite mantener clases de servicio (CoS) y soporta con gran eficacia la creación de VPNs. Por todo ello, MPLS aparece ahora como la gran promesa y esperanza para poder mantener el ritmo actual de crecimiento de la Internet.

Las principales soluciones que ofrece la tecnología MPLS para redes IP se pueden resumir en los siguientes puntos:

- Garantías de calidad de servicio (QoS).
- Fácil integración con redes existentes de diferentes tecnologías como ATM, Frame Relay, etc.
- Creación flexible de Redes Privadas Virtuales (VPNs).

- Soporte a soluciones de Ingeniería de Tráfico.
- Bajo costo de implementación, ya que en la mayoría de los casos permite la utilización de los equipos y tecnologías existentes.

MPLS proporciona una solución con grandes posibilidades de éxito gracias a la facilidad que presenta migrar cualquier red actual (FR, ATM, Ethernet...) a esta plataforma, siendo este el primer paso para la coexistencia entre ellas mediante software añadido a equipos actuales.

Una importante ventaja es la simplificación en cuanto a la administración de redes, MPLS permite crear sobre una misma red tantas redes virtuales VPNs como sea necesario. Esto facilitará enormemente la labor a los proveedores de servicio al tiempo que les permitirá ofrecer servicios de valor añadido, pues es lo que en definitiva acabará marcando la diferencia entre ellos.
A la fecha, ya existen importantes operadores migrando sus redes a esta solución tal es el caso de, por ejemplo, ***Cable & Wireless***, ***Equant***, ***Genuity*** y ***MCI World-Com***, etc.

Al mismo tiempo los fabricantes de equipos con facilidades MPLS se han volcado de lleno en el desarrollo del software necesario para la migración y del equipamiento propio de esta plataforma. Tanto ***CISCO*** como ***Nortel Networks***, ***Juniper Networks*** o ***Nokia*** (entre otros) disponen de grupos de trabajo especializados desarrollando este nuevo estándar. Éste es el punto clave para que los proveedores de servicio puedan comprobar la aceptación de MPLS en el mercado, dando así el primer paso hacia una nueva etapa para las redes de comunicaciones. Una etapa, si todo evoluciona siguiendo la trayectoria actual, muy prometedora.

Bibliografía

http://www.ati.es

http://www.entenderinternet.com

http://www.interware.com.mx

http://www.isoc.org

http://www.digitalnetworks.net

http://www.ietf.org

http://www.webopedia.internet.com

http://www.mplsrc.com

http://www.pulsewan.com

http://www.tonetbarna.com/

http://www.rediris.es

RFC 3031 Multiprotocol Label Switching Architecture