DISEÑO DE UNA RED MPLS ORIENTADO A LA INGENIERÍA DE TRAFICO PARA UNA ISP EN TUNJA

YENY ANDREA MORENO MEJÍA

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR POR EL TITULO DE INGENIERO ELECTRÓNICO

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERÍA ELECTRÓNICA
TUNJA
2007

DISEÑO DE UNA RED MPLS ORIENTADO A LA INGENIERÍA DE TRAFICO PARA UNA ISP EN TUNJA

YENY ANDREA MORENO MEJÍA

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR POR EL TITULO DE INGENIERO ELECTRÓNICO

Director: Angélica María Salazar

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERÍA ELECTRÓNICA
TUNJA
2007

DISEÑO DE UNA RED MPLS ORIENTADO A LA INGENIERÍA DE TRAFICO PARA UNA ISP EN TUNJA

Nota de Aceptación:

_____

Aprobado por:

_____

Ing. Angélica María Salazar, Director

_____

Ing. Luis Fredy Sosa, Jurado

Camilo Ernesto Pardo Beainy

Ing. Camilo Ernesto Pardo, Jurado

Fecha de Aprobación_____

A MIS PADRES CRISANTO MORENO Y YANETH MEJÍA

A MI HERMANO FERNANDO MORENO

AGRADECIMIENTOS

A mis padres y hermano por acompañarme en este camino y haberme dado todo su apoyo incondicional para lograr alcanzar mis metas.

Quiero agradecer a Jairo Parra, Omar Rojas, Eduardo Avendaño, Fabián Ramírez y Magda Castro por el tiempo dedicado y las diversas orientaciones que me han dado a lo largo del desarrollo de la misma.

A Neo.Net Ltda. con quien he trabajado y han enriquecido mis conocimientos sobre el tema y este trabajo en diversos aspectos.

TABLA DE CONTENIDO

LISTA DE FIGURAS

RESUMEN

La realización de este proyecto esta contenida en un marco más amplio de trabajo, que cuenta con el financiamiento de Neo.Net Ltda., y que tiene por objeto la implementación de una red multi-servicio, utilizando su infraestructura con el objetivo de probar aplicaciones/servicios que pueda ser implantados en el futuro con garantías de calidad de servicio.

Esta se realiza por medio de un análisis a la red IP existente en la ISP en Tunja, determinando el tipo de enlace que utiliza, análisis de frecuencias, equipos instalados, protocolos que manejan, software de gestión, ventajas, desventajas y las diferentes aplicaciones que brindan al usuario final.

Como se vera mas adelante este libro se divide en 4 etapas las cuales reflejan el estudio a lo largo de este proyecto.

El capitulo I se encuentra la motivación que se lleva a cabo para la realización junto a los objetivos que enmarcan el proyecto.
El capitulo II relaciona una base teórica que es el fundamento de este estudio.
El capitulo III describe el funcionamiento de la red orientada hacia la Ingeniería de Trafico.
El capitulo IV muestra el diseño de esta propuesta con su respectivo análisis.

Finalmente se describen los aportes y conclusiones que trajo consigo el proyecto.

CAPITULO I

PRELIMINARES

El crecimiento actual de la Internet le da una oportunidad a los Internet Service Providers (ISPs) de ofrecer nuevos servicios como VoIP, Videoconferencia, etc., además de los ya tradicionales servicios de datos como email, ftp y web browsing. Todos estos nuevos servicios tienen grandes requerimientos en lo que a información, tasa de pérdida, delay y jitter se refiere.

La Internet no fue diseñada para trabajar con este tipo de requerimientos, trabajando desde sus comienzos, bajo el paradigma "Best Effort" de IP. Esto significa que el usuario manda paquetes a la red y la red va a tratar de hacerlos llegar a destino sin garantía alguna.

A pesar que protocolos como TCP han agregado mecanismos de reenvío que tratan de solucionar el problema de la pérdida de paquetes generado por el congestionamiento en la red, estos no solucionan las pérdidas en aplicaciones interactivas de tiempo real, donde no es posible esperar a que un paquete sea reenviado.

Es por ello que la comunidad de Internet ha hecho grandes esfuerzos en los pasados años para poder ofrecer garantías de calidad de servicio (QoS) a Internet, con el objetivo de transformarla en una red convergente para todos los servicios de telecomunicaciones. Entre los primeros modelos podemos destacar el de Servicios Integrados (IntServ) y el de Servicios Diferenciados (DiffServ). Debido principalmente a problemas de escalabilidad en el primer caso (IntServ) y al no poder ofrecer las suficientes garantías de QoS en el segundo (DiffServ), es donde se necesita de la Ingeniería de Tráfico en las redes IP para asegurar QoS. [30]

Los ISPs necesitan así de sofisticadas herramientas de gestión de redes que apunten a un uso óptimo de los recursos de la red que son compartidos entre clases de servicios con diferentes requerimientos de QoS [23]. La tecnología de Multi Protocol Label Switching (MPLS) es un buen ejemplo que ayuda a realizar ingeniería de tráfico en sistemas autónomos (AS). Se basa en la idea de enviar

paquetes a través de Label Switched Paths (LSPs) haciendo uso de etiquetas que son adjuntadas a los paquetes en los routers de ingreso de la red (puntos de interconexión entre la red MPLS y la red de acceso). Esas etiquetas son a su vez asignadas a los paquetes de acuerdo a su Forwarding Equivalence Class (FEC) (representación de un conjunto de paquetes que comparten los mismos requerimientos para su transporte) que son entonces mandados a través de uno de los LSPs asociado con esa FEC en particular.

La práctica de Ingeniería de Trafico (TE) hoy en día abarca el establecimiento y uso de esos LSPs como tuberías de determinado ancho de banda entre dos puntos. Dichos LSPs pueden ser configurados a través de varios routers, ya sea de forma manual por parte del usuario o en forma automática por parte del Administrador de Red. La Ingeniería de Tráfico (TE) intenta optimizar el desempeño de las redes, a través de tres actividades integradas: medición del tráfico, modelado de la red, y selección de mecanismos para el control del tráfico [2].

Desafortunadamente, grandes Proveedores de Servicios de Internet (ISPs) tienen pocos sistemas de software y herramientas que soporten la medición del tráfico y el modelado de la red, pilares básicos de una ingeniería de tráfico efectiva. De manera similar, preguntas sencillas sobre la topología, tráfico y ruteo son sorprendentemente difíciles de contestar en las redes IP de hoy en día. Una gran cantidad de trabajo ha sido dedicado al desarrollo de mecanismos y protocolos para el control del tráfico. Como ejemplo de ello, la mayor parte del trabajo de la Internet Engineering Task Force (IETF)[1] está relacionado al control del tráfico en lo que a la ingeniería de tráfico concierne.
Existen determinados factores que indican la necesidad de más y mejores herramientas de ingeniería de tráfico para las redes. Entre ellos se destacan la calidad del servicio, los parámetros ajustables interdependientes, el crecimiento de las redes y la variabilidad del tráfico.

En cuanto a la Calidad del Servicio, los clientes son cada vez más exigentes en el cumplimiento del desempeño, confiabilidad y seguridad, que se manifiestan en forma de Service Level Agreements (SLAs). Los clientes desarrollan más procedimientos de certificación y testeos continuos, para asegurar el cumplimiento de dichos SLAs.

Aplicaciones como Voz sobre IP, las cuales por su naturaleza, requieren del

[1] Organización internacional abierta de normalización que tiene como objetivos en contribuir a la ingeniería de Internet.

transporte de datos de alta calidad, medido por el retardo, tasa de pérdida de paquetes y jitter, están emergiendo hoy en día. Por eso es muy importante para los operadores de redes el coordinar cuidadosamente por dónde fluye el tráfico de cada demanda y ver si pueden o no tolerar la llegada de futuras nuevas demandas sin afectar las ya existentes y por ende, viendo comprometido el cumplimiento de los SLAs pertinentes.

En lo que a los Parámetros ajustables Interdependientes se refiere, hoy en día, los proveedores de equipos de red, proveen a los ISPs con poco o ningún control sobre los mecanismos básicos responsables de la coordinación de paquetes, gestión de buffers y selección de caminos. En su lugar, los proveedores de backbones[2] son forzados a entender una larga cantidad de parámetros interrelacionados que de una manera u otra afectan la configuración y operación. Hasta el día de hoy, un ISP debe gestionar su red de backbone, y sus complicadas relaciones de frontera con proveedores vecinos, ajustando los asuntos mencionados anteriormente a través de una combinación de intuición, testeo y pruebas de intento y error.

El Crecimiento de las Redes se ve reflejado en que por un lado, redes de backbones individuales están creciendo rápidamente en tamaño, velocidad y espectro abarcado; mientras que por otro lado, la industria intenta unir redes discordes entre sí, en redes integradas más grandes. Como resultado, las funciones de gestión de red que una vez pudieron ser manejadas por un grupo reducido de personas, basándose en la intuición y experimentación, deben ser ahora soportadas por herramientas efectivas de ingeniería de tráfico que unen información de configuración y de uso de una variedad de fuentes.

Por último, la Variabilidad del Tráfico. El tráfico de Internet es complejo. La carga ofrecida entre pares origen-destino es típicamente desconocida. Así mismo, la distribución del tráfico IP usualmente fluctúa ampliamente a través del tiempo. Esto introduce una gran complejidad a la ingeniería de tráfico sin aliviar las demandas de los clientes por un desempeño de comunicación predecible. Herramientas efectivas de TE deben soportar la identificación rápida de potenciales problemas de desempeño y un ambiente flexible para experimentar posibles soluciones. [31]

Es por los motivos expuestos anteriormente que se decidió realizar el diseño de una red MPLS orientada a Ingeniería de Tráfico para poder lograr un mejor desempeño en la red y una mejor calidad de servicio al usuario final.

[2] Se refiere a las principales conexiones troncales de Internet.

1.1 OBJETIVOS

1.1.1 Objetivo General

- Realizar un diseño que permita implementar a futuro las distintas prestaciones que se pueden obtener al aplicar Ingeniería de Tráfico sobre una red IP basada en Multi Protocol Label Switching (MPLS).

1.1.2 Objetivos Específicos

- Formar una sólida base teórica sobre MPLS y TE (Traffic Engineering), de esta manera entender la razón de su existencia y su principio de funcionamiento.
- Proponer una red MPLS para una ISP cuyo enfoque esta dirigido a brindar garantías de Calidad de Servicio (QoS), las cuales permiten asegurar al cliente el grado de servicio esperado en términos del ancho de banda solicitado.
- Diseñar una red MPLS orientado a la Ingeniería de tráfico, el cual le permitirá al ISP proporcionar la calidad de servicio y la confiabilidad necesarias para que su red IP maneje las redes basadas en MPLS y pueda satisfacer con eficiencia y seguridad los requisitos del cliente.
- Proponer una oferta competitiva en el mercado de servicios de telecomunicaciones. Ofreciendo al proveedor de servicio la posibilidad de generar fuentes de ingresos adicionales, además de la capacidad de resolver las necesidades de los clientes con nuevos servicios.
- Plantear el desarrollo de nuevas fuentes de ingresos, con los equipos implementados y la experiencia desarrollada para un servicio administrado que se pueden utilizar para lanzar otros servicios nuevos que usen la misma base de redes. Esta oportunidad de "una red y múltiples servicios" tiene un fuerte sentido financiero para el proveedor, pero requiere una red que tenga alta disponibilidad y calidad de servicio (QoS), además de otras funciones, porque los servicios administrados IP que funcionan en la red deben admitir las aplicaciones fundamentales de los clientes.

1.2 JUSTIFICACIÓN

La Ingeniería de Tráfico (TE) es una disciplina que procura la optimización del desempeño de las redes operativas. La Ingeniería de Tráfico abarca la aplicación de la tecnología y los principios científicos a la medición, caracterización, modelado, y control del tráfico que circula por la red.

Las mejoras del rendimiento de una red operacional, en cuanto a tráfico y modo de utilización de recursos, son los principales objetivos de la Ingeniería de Tráfico. El objetivo en este caso es optimizar la utilización de los recursos de la red de manera que no se saturen partes de la misma mientras otras permanecen subutilizadas.

Todo lo anterior apunta a un objetivo global, que es minimizar la congestión al mismo tiempo que intentar incrementar la eficiencia de la utilización de los recursos. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces.

La otra causa de congestión es la utilización ineficiente de los recursos debido al mapeado del tráfico. El objetivo básico de la Ingeniería de Tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén sobre-utilizados, creando cuellos de botella.

Con esto se quiere dirigir un flujo de paquetes IP a lo largo de un camino predeterminado a través de la red por medio del intercambio de etiquetas. Esas etiquetas son las que permiten que se establezcan las rutas que siguen los paquetes entre dos nodos de la red, conocidas con el nombre de ruta conmutada de etiquetas o LSPs.

CAPITULO 2

MPLS

2.1 Introducción

El protocolo MPLS (Conmutación de Etiquetas de Multiprotocolo) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP [1].

MPLS fue originalmente propuesto por un grupo de ingenieros de Cisco, con el nombre de "Tag switching", fue entregado a la IETF y luego del proceso de estandarización cambió de nombre. MPLS es un estándar multiprotocolo capaz de transportar diferentes tipos de tráfico por la misma vía.

MPLS combina el desempeño y velocidad de la capa de enlace de datos del modelo OSI con la escalabilidad y flexibilidad de la capa de red. Para hacer esto, en lugar de emplear el enrutamiento tradicional, es decir, no orientado a conexión, MPLS utiliza etiquetas cortas de longitud fija que son añadidas a los paquetes de datos en el momento en que éstos ingresan a la red MPLS. Las etiquetas asignadas a cada paquete son las que determinan las decisiones de enrutamiento dentro del dominio MPLS.

Una de las características más importantes que ofrece MPLS es su autonomía de otros protocolos ampliamente utilizados, de manera que protocolos de diferente naturaleza puedan coexistir dentro de la misma red, sin estar condicionados a uno de ellos en particular. De esta forma, MPLS no se limita a algún protocolo de la capa 2 ó 3 del modelo OSI, sino que además ofrece los beneficios más relevantes de ambas capas. Lo anterior es posible gracias a que las etiquetas utilizadas en MPLS son añadidas en un punto intermedio entre las capas 2 y 3 del modelo.

Debe señalarse también el papel que juega la calidad de servicio en las redes MPLS, aun cuando éstas puedan utilizarse para conducir, por ejemplo, paquetes IP. En la arquitectura MPLS, los ruteadores ubicados en el extremo por donde ingresa la información están encargados de asignar "etiquetas" dependiendo de las características de los propios paquetes. Las características específicas de un paquete están relacionadas a un nivel de calidad de servicio, mismo que indirectamente define una ruta de transmisión previa. Lo más interesante es que el análisis del encabezado de los paquetes IP se realiza en una sola ocasión, permitiendo que el direccionamiento de la información a través de los ruteadores MPLS se lleve a cabo a partir de la "etiqueta" insertada.[5]

2.2 Protocolo MPLS

El multiprotocolo de conmutación de etiquetas (MPLS) reduce significativamente el proceso de paquetes que se requiere cada vez más que un paquete ingresa a un enrutador en la red, esto mejora el desempeño de dichos dispositivos y del desempeño de la red general. Las capacidades más relevantes de este protocolo son 4:

- Soporte de calidad de servicio (QoS).
- Soporte para redes privadas virtuales (VPNs).

- Soporte multiprotocolo e Ingeniería de Tráfico.

Este último es el enfoque de la tesis el cual se hablara con más detalle [2].

2.2.1 Soporte de Calidad (QoS)

Este soporte de calidad le permite a los administradores de red la optimización de los recursos de sus redes haciendo un buen uso de las aplicaciones asignando diferentes recursos sin afectar el desempeño de la red con las demás aplicaciones lo que significa un manejo de costos y una mayor satisfacción hacia el cliente final [9].

La importancia que tiene QoS en una red se ve desde el punto de vista de la administración efectiva de los recursos que se tiene para poder dar al cliente final un mejor servicio y una mayor fluidez en su servicio sin necesidad de tener que limitar el ancho de banda para mejorar el trafico en la red. De esta calidad del servicio depende la transmisión cada vez más de información en menor tiempo.

QoS trabaja a lo largo de la red y se encarga de asignar recursos a las diferentes aplicaciones según se requieran, para asignar dichos recursos este se basa en prioridades. Algunas aplicaciones podrán tener más prioridad que otra, pero lo que si se garantiza es que todas las aplicaciones tengan los recursos necesarios y un tiempo aceptable para completar sus transacciones. Dichos recursos se refiere principalmente al ancho de banda en donde el administrador mejora la interacción entre el usuario y el sistema. A su vez se reducen costos, mejora el control sobre la latencia y genera una mayor confiabilidad sobre la red.

El problema inflexible de calidad de servicio no se da por el hecho de transmitir voz o video en línea sino por la interactividad del servicio. Es decir, si lo que se

pretende es por ejemplo escuchar radio en Internet, se esta frente a un servicio de voz en línea. Pero en este caso, el retardo no es relevante porque escuchar la radio con algunos segundos de atraso respecto de la emisión no es demasiado importante. En este caso las pérdidas pueden solucionarse con mecanismos tradicionales y se agrega un buffer en la aplicación destino que pre-memorice algunos segundos de transmisión. Sin embargo, en un servicio interactivo esto no es posible y las retransmisiones no aportan una solución a las perdidas.

El otro parámetro que aunque es de segundo orden es muy importante en aplicaciones interactivas es el jitter. El jitter es la variación del retardo y tiene importancia porque por ejemplo, la reconstrucción de una señal de voz se debe hacer a la misma cadencia a la que fue muestreada. Si el retardo de los paquetes es variable esto no es posible. Para solucionar el problema del jitter se puede agregar retardo para absorber esta variabilidad, pero si el servicio es interactivo el margen de maniobra es muy pequeño.

La política 'Best Effort' (protocolo de máximo esfuerzo) implica que si existe más tráfico del que puede ser transportado por un enlace, el sobrante se envía a una cola de donde se irán sacando los paquetes para ser enviados. Si esta cola se llena, los paquetes son descartados.

En cuanto al retardo, el problema es similar. Existen tres fuentes fundamentales de retardo: el retardo de transmisión, el retardo de procesamiento en los enrutadores o switches, y el retardo de las colas de los enlaces. Los dos primeros con la tecnología existente son cada vez menos relevantes. Por ejemplo las transmisiones ópticas llevan a que una transmisión de Uruguay a Europa tienen un retardo de transmisión del orden de los 30 ms, es decir 5 0 6 veces menos que lo necesario para mantener una conversación de muy buena calidad. Por otra parte los retardos en enrutadores o switches vienen derivados fundamentalmente del procesamiento de los paquetes. Uno

de los procesamientos que genera un retardo es la búsqueda en las tablas de ruteo para decidir el próximo enrutador al que debe enviarse el paquete. Hoy en día estos procesos que antes se hacían por software pueden ser hechos por hardware y las velocidades de procesamiento están llegando al orden del milisegundo por paquete. Por más que el paquete deba atravesar 15 enrutadores esto no le agregara más de 15 ms en su retardo.[12]

La fuente de retardo que si es muy importante (y además a diferencia de las anteriores es variable de paquete a paquete) es la generada por el tamaño de la cola que encuentra el paquete en cada enlace que atraviesa. MPLS introduce un marco de trabajo orientado a conexión en un sistema basado en IP (protocolo de Internet) y facilita el tráfico de QoS exigente.

2.2.2 Soporte para 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 posee los enlaces. Las IP/VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. [18]

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 PVCs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas

clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los 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 NSPs, 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 unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP/VPN) ha sido la de construir túneles IP de diversos modos.

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

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

- En el nivel 3, mediante el protocolo IPSec del IETF
- En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un NSP.

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado 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, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios

routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado 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 de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. 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 cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles 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).
- 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.[32]

2.2.3 Soporte Multiprotocolo

MPLS puede ser utilizado con diversas tecnologías, por lo tanto no es necesario actualizar los router IP existentes. Los routers MPLS pueden trabajar con routers IP a la par, lo que facilita la introducción de dicha tecnología a redes existentes ya que esta diseñada para trabajar en redes ATM y Frame Relay. Al igual que los routers, los switches pueden trabajar con switches normales [3].

Esta tecnología puede trabajar con tecnologías puras como son IP Internet, ATM y Frame Relay. Todo esto con tener redes mixtas añadiendo QoS para optimizar y organizar los recursos. Lo que da lugar a una tecnología innovadora fácil de aplicar a redes nuevas como ya a existentes.

2.2.4 Ingeniería de Tráfico

Es la habilidad de definir rutas dinámicamente y planear la asignación de recursos con base en la demanda, así como optimizar el uso de la red. MPLS facilita la asignación de recursos en las redes para balancear la carga dependiendo de la demanda y proporciona diferentes niveles de soporte dependiendo de las demandas de tráfico de los usuarios. El protocolo IP provee una forma primitiva de Ingeniería de Tráfico al igual que el protocolo del Camino más Corto Primero (*OSPF*) que permite a los enrutadores cambiar la ruta de los paquetes cuando sea necesario para balancear la carga. Sin embargo, esto no es suficiente ya que este tipo de ruteo dinámico puede llevar a congestionar la red y no soporta QoS [2].

Todo tráfico entre dos puntos finales (*endpoints*) sigue la misma ruta y puede ser cambiada si ocurriera congestión, sin embargo, este cambio solo ocurre

solo cuando hay congestión que es algo que siempre se trata de evitar. En MPLS a diferencia de OSPF no se ve paquete por paquete sino flujos de paquetes con su respectivo QoS y demanda tráfico predecible. Con este protocolo es posible predecir rutas en base a flujos individuales, pudiendo haber diferentes flujos entre canales similares pero dirigiéndose a diferentes enrutadores.

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

2.2.4.1 Beneficios principales de ingeniería de trafico MPLS

• Permite al eje troncal (*backbone*) expandirse sobre las capacidades de la ingeniería de tráfico de las redes de Modo de Transferencia Asíncrona (*ATM*) y Frame Relay (*FE*) de Capa 2.

• La ingeniería de tráfico es esencial para los ejes troncales de proveedores de servicios. Dichos ejes deben soportar un uso elevado de su capacidad de transmisión.

• Utilizando MPLS las capacidades de ingeniera de tráfico son integradas a la Capa 3 (*OSI*) lo que optimiza el ruteo de trafico IP gracias a las pautas establecidas por la topología y las capacidades de la troncal.

• La ingeniería de trafico MPLS rutea el flujo de tráfico a lo largo de la red basándose en los recursos que dicho flujo requiere y en los recursos disponibles en toda la red.

• MPLS emplea la ruta más corta que cumpla con los requisitos del flujo de tráfico, que incluye: requisitos de ancho de banda, de medios y de prioridades

sobre otros flujos.[24]

2.2.4.2 Cómo funciona la Ingeniería de Trafico MPLS?

MPLS es básicamente una integración de tecnologías de Capa 2 a Capa 3, dicha integración permite manejar el tráfico a nuestra conveniencia. De esta manera el flujo de paquetes viaja a través de un túnel de datos en el eje troncal creado por el Protocolo de Reserva de Recursos (RSVP), la ruta de dicho túnel esta dada por los requisitos de recursos del túnel y de la red (constraint-based routing). El Protocolo de Enrutamiento Interno (*IGP*) rutea el tráfico a dichos túneles.

Con un buen manejo del tráfico en las redes, se pueden evitar congestionamientos, mejorar el desempeño general y reducir la latencia y el desechado de paquetes. En pocas palabras se maximiza la capacidad de la red y se minimizan los costos.

2.3 Funcionamiento de una red MPLS

MPLS utiliza RSVP como protocolo de señalización para la reserva de recursos. Hoy en día RSVP representa la forma más completa y sencilla para implementar técnicas de Ingeniería de Tráfico. Una ventaja fundamental que tiene MPLS sobre IPSec es en que las redes privadas virtuales implementadas con dicha tecnología solo se aplican al backbone del proveedor del servicio, lo que provee un escenario transparente para el usuario final.

RSVP provee otro tipo de ventajas además de la Ingeniería de Trafico ya que permite técnicas de protección de los caminos de MPLS. Si se diera un problema con el enlace del backbone del proveedor, no se apreciaría perdida de información ya que automáticamente se toma un camino físico alternativo.

MPLS crea una tabla de rutas distinta para cada VPN para permitir la reutilización del espacio de direcciones y para separar el trafico entre VPN's; ambas son ventajas para los clientes ya que pueden crear una VPN nueva sin necesidad de redireccionar.

Ambas tecnologías se están desarrollando a la par, MPLS por un lado se enfoca principalmente en los backbones e IPSec[3] por otro en los clientes. Por esta razón se busca hibridar ambas tecnologías en un futuro para que IPSec maneje la encriptación de la información y MPLS la provisión de servicios y de ruteo inteligente de tráfico.

2.4 Componentes de una red MPLS

Una red MPLS consiste de un conjunto de Enrutadores de Conmutación de Etiquetas (*LSR*) que tienen la capacidad de conmutar y rutear paquetes en base a la etiqueta que se ha añadido a cada paquete. Cada etiqueta define un flujo de paquetes entre dos puntos finales. Cada flujo es diferente y es llamado Clase de Equivalencia de Reenvío (*FEC*), así como también cada flujo tiene un camino específico a través de los LSR de la red, es por eso que se dice que la tecnología MPLS es "orientada a conexión". Cada FEC, además de la ruta de los paquetes contiene una serie de caracteres que define los requerimientos de QoS del flujo. Los routers de la red MPLS no necesitan examinar ni procesar el encabezado IP, solo es necesario reenviar cada paquete dependiendo el valor de su etiqueta. Esta es una de las ventajas que tienen los routers MPLS sobre los routers IP, en donde el proceso de reenvío es más complejo.

En un router IP cada vez que se recibe un paquete se analiza su encabezado IP para compararlo con la tabla de enrutamiento (*routing table*) y ver cual es el siguiente salto (*next hop*). El hecho de examinar estos paquetes en cada uno

[3] Es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y, de esta manera, asegurar las comunicaciones a través de dicho protocolo.

de los puntos de tránsito que deberán recorrer para llegar a su destino final significa un mayor tiempo de procesamiento en cada nodo y por lo tanto, una mayor duración en el recorrido.[11]

2.5 Diagrama de Operación MPLS [26].

Fuente: www.juniper.net/techcenter/mpls.html

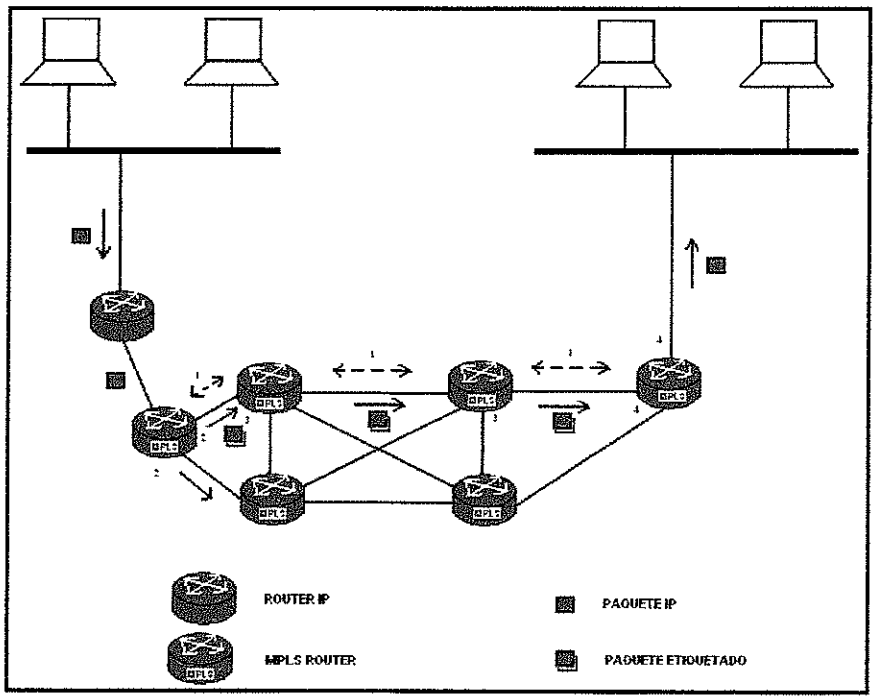

Figura 1: Diagrama de operación MPLS

A continuación los pasos que sigue el flujo de paquetes MPLS en la Figura 1:

1. Antes de mandar la información por el flujo es necesario establecer un Camino de Conmutación de Etiquetas (*LSP*) entre los routers que van a transmitir la FEC. Dichos LSP sirven como túneles de transporte a lo largo de la red MPLS e incluyen los parámetros QoS específicos del flujo. Estos parámetros sirven para determinar dos cosas:

a. La cantidad de recursos a reservar al LSP.
b. Las políticas de desechado y la cola de procesos en cada LSR.
Para lograr los puntos anteriores se utilizan dos protocolos para intercambiar información entre los routers de la red. Se le asignan etiquetas a cada flujo FEC particular para evitar el uso de etiquetas globales que dificultan el manejo y la cantidad de las mismas.

Por esta razón las etiquetas solo hacen referencia al flujo específico. La asignación de nombres y rutas se puede realizar manualmente o bien se puede utilizar el Protocolo de Distribución de Etiquetas (*LDP*) [1].

2. En esta sección el paquete entra al dominio MPLS mediante un LSR frontera que determina que servicios de red requiere, definiendo así su QoS. Al terminar dicha asignación el LSR asigna el paquete a una FEC y a un LSP particular, lo etiqueta y lo envía. Si no existe ningún LSP, el router frontera trabaja en conjunto con los demás LSRs para definirlo.

3. En este momento el paquete ya esta dentro del dominio MPLS, cuando los routers contiguos del LSR reciben el paquete se llevan acabo los siguientes procesos:

a. Se deshecha la etiqueta de entrada y se le añade la nueva etiqueta de salida al paquete.
b. Se envía el paquete al siguiente LSR dentro del LSP.

4. El LSR de salida "abre" la etiqueta y lee el encabezado IP para enviarlo al destino final.

2.6 Funcionamiento de un LER y un LSR

Los routers MPLS dividen su operación en dos partes: una de control y otra de datos. En el siguiente esquema se puede ver claramente la complejidad de la carga en los LER, es aquí donde se lleva a cabo el ruteo en la tabla de direcciones IP y quien se encarga de clasificar los paquetes a diferentes clases FEC. En la tabla de los LSR no se lee más que la tabla de etiquetas [23].

Los protocolos de ruteo pueden ser cualquiera de los mencionados anteriormente como el Protocolo de Información de Ruteo (*RIP*), OSPF. Sistema Integrado a Sistema Integrado (*IS-IS*), etc. Para los protocolos de distribución están RSVP-TE, CR-LDP, BGP, etc.

Fuente: ISP Network Structure, http:www.cisco.com

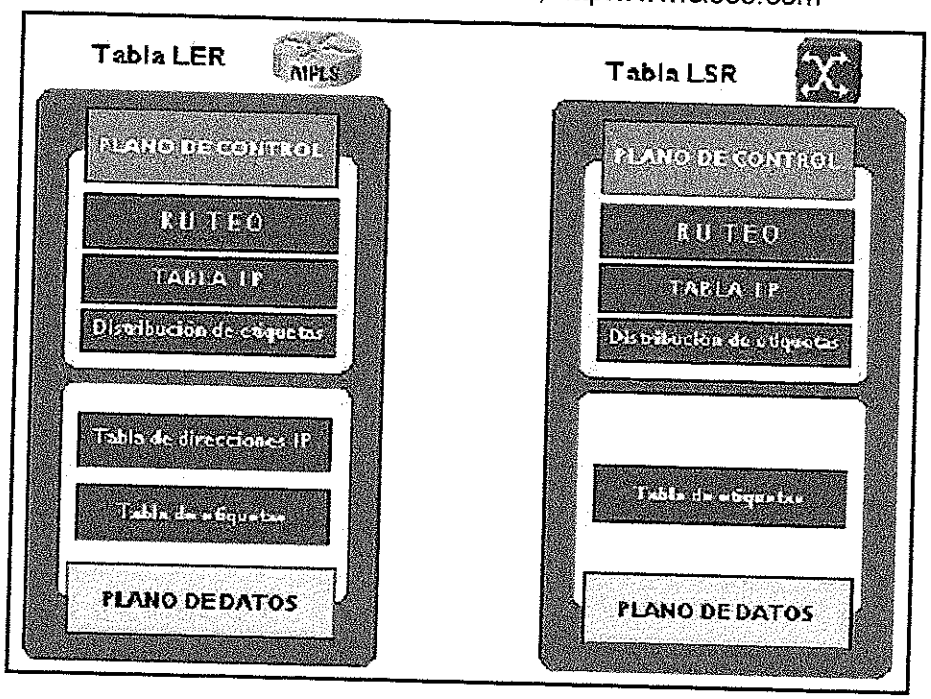

Figura 2. Tabla de Control y Datos

2.6.1 Plano de control

El plano de control esta compuesto por los protocolos y procedimientos que actúan de forma transparente y que mantienen las tablas de ruteo y las asociaciones de etiquetas y FECs como se muestra en la figura 2.

2.6.2 Plano de datos

El plano de datos esta formado por todo lo relacionado con procedimiento de asignaciones y modificaciones de las etiquetas y asignación de flujos a FEC como se muestra en la figura 2. Cuando llegan a un LSR más de un FEC con el mismo destino y procedencia dentro de la nube MPLS (esto se da cuando los FEC fueron creados por el mismo LER), se pueden juntar todos como si fueran una misma clase, con el fin de ahorrar tiempo en el intercambio y almacenamiento de etiquetas. En si, la agrupación es la capacidad de unir varios FEC en uno sólo.

Otro tipo de optimización se puede hacer mezclando etiquetas, esto se puede hacer cuando llegan diferentes tráficos por el mismo FEC. En este caso se ahorra espacio de almacenamiento y se ahorra tiempo en el plano de control al no tener muchas asociaciones de etiquetas. En este tipo de optimización existen algunas restricciones, por ejemplo, los flujos deben entrar y salir por la misma interfaz, no se puede realizar si van dirigidos al mismo LSP pero por diferentes interfaces de salida.

A manera de resumen los componentes principales del plano de datos de un LER o LSR son:

- Etiqueta de entrada
- Una o más subentradas:
- Etiqueta de salida

• Interfaz de salida
• Dirección del siguiente salto[2[

2.7 Ruteo en los bordes y switcheo en el centro

La estructura general MPLS se basa en que los enrutadores de los extremos de la nube son los que realizan el mayor trabajo. Los Enrutadores de Etiquetas Frontera (*LER*) que realizan las labores de ruteo de paquetes con funciones de decisión de rutas manejan muchísima información, extremadamente complicada, que puede estar basada en la interfaz de entrada, en los valores del encabezado de red, en la red a la que pertenece, en el tipo de tráfico, etc.

Después tenemos los dispositivos internos LSR que hacen conmutación de paquetes a velocidades impresionantes y con eficacia incomparable, ya que solo es necesario leer la etiqueta del encabezado MPLS que define hacia donde va y de donde viene. Como se muestra en la Figura 3 los LER de los extremos añaden y quitan etiquetas y asignan FEC, los conmutadores trabajan basándose en las etiquetas MPLS [30].

Fuente: http: www.networkworld.com/topics/**mpls**.html

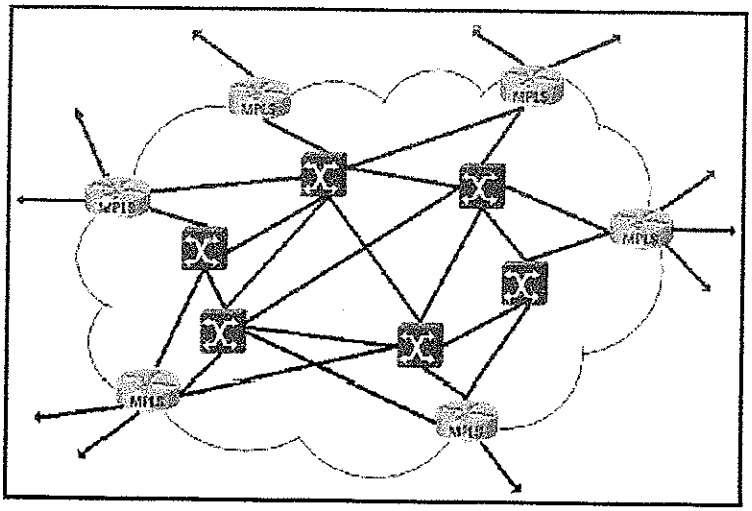

Figura 3. Dominio MPLS

2.8 Ventajas especificas de MPLS

En este momento ya es posible identificar algunas de las ventajas internas más importantes que MPLS presenta:

1. Un domino MPLS consiste de una serie de routers habilitados con MPLS continuos y contiguos. El tráfico puede entrar por un punto final físicamente conectado a la red, o por otro router que no sea MPLS y que este conectado a un red de computadoras sin conexión directa a la nube MPLS.

2. Se puede definir un Comportamiento por Salto (*PHB*) diferente en cada router de la FEC. El PHB define la prioridad en la cola y las políticas de desechado de los paquetes.

3. Para determinar el FEC se pueden utilizar varios parámetros que define el administrador de la red.

a. Dirección IP fuente o destino y/o las direcciones IP de la red.
b. Utilizar el ID del protocolo IP.
c. Etiqueta de flujo IPv6.
d. Numero de puerto de la fuente o del destino.
e. El punto de código (*codepoint*) de los servicios diferenciados (DSCP).

4. El reenvío de la información se lleva acabo mediante una búsqueda simple (*lookup*) en una tabla predefinida que enlaza los valores de las etiquetas con las direcciones del siguiente salto (*next hop*).

5. Los paquetes enviados de mismos endpoints pueden tener diferente FEC, por lo que las etiquetas serán diferentes y tendrán un PHB distinto en cada LSR. Esto puede genera diferentes flujos en la misma red. [33]

2.9 Procesando el TTL

Un elemento clave en el encabezado de un paquete IP es el campo TTL[4] y el Limite de Saltos (*Hop limit*). En un ambiente común de Internet (basado en IP), dicho campo va disminuyendo uno a uno hasta que llega a cero y se elimina el paquete. Esto es una medida de prevención de los paquetes se ciclen (*looping*) o estén demasiado tiempo en el Internet debido a un ruteo mediocre. En el ruteo MPLS no se lee el encabezado de los paquetes, es por eso que se añaden estos 8 bits que manejan el TTL para evitar que ocurra lo mencionado anteriormente.

2.9.1 Reglas para procesar el campo TTL:

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

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

2. Cuando un paquete MPLS llega a un LSR de salida, el valor del campo TTL

[4] Tiempo de vida e indica por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen.

en la etiqueta es disminuido (uno por uno) y posteriormente se quita la etiqueta de la pila, lo que deja una pila vacía. Entonces:

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

Es importante mencionar que cuando el valor del campo TTL llega a 0 y el paquete no ha llegado a su destino predefinido en el valor de la etiqueta, dicho paquete es desechado y se envía un mensaje del Protocolo de Control de Mensajes de Internet (*ICMP*) al remitente. Esto con el fin de evitar que un paquete no entregado se quede circulando en el Internet.

En teoría TTL esta medido en segundos, aunque cada equipo (*host*) que pase el paquete debe reducir el Tiempo de Vida en al menos una unidad. El campo TTL es disminuido en una unidad en cada salto, es por eso que en IPv6 a este decremento de unidades en cada salto se le llama Conteo de Saltos (*hop count*). [34]

2.10 Etiquetas.

Las etiquetas identifican el camino que un paquete puede atravesar. La etiqueta es encapsulada en la cabecera de la capa de enlace. Una vez el paquete ha sido etiquetado viajará a través del *backbone* mediante conmutación de etiquetas, es decir, cada *router* examinará la etiqueta, consultará en sus tablas de envío para saber con qué etiqueta y por qué interfaz debe salir, intercambiará las etiquetas y lo enviará por el interfaz correspondiente.

Pasos para la asignación de etiquetas:

1. Cada paquete se clasifica como un nuevo FEC o se le asigna un FEC ya existente.
2. Se asigna una etiqueta a cada paquete. Éstas se derivan de la capa de enlace, es decir, para redes Frame Relay, ATM o redes ópticas, los identificadores de la capa 2 (DLCIs, VPIs/VCIs y longitud de onda DWDM, respectivamente) pueden servir como etiquetas. Para redes como Ethernet y PPP (Point to Point Protocol), a la etiqueta se le añade una cabecera *shim* entre las cabeceras de la capa de enlace y la capa de red, que contendrá el campo TTL (Time To Live). Las decisiones de asignación de etiquetas pueden estar basadas en criterios de envío como encaminamiento unicast, multicast, ingeniería de tráfico, VPN (Virtual Private Network) y QoS (Quality of Service).[18]

2.10.1 Diagrama de Manejo de colas y etiquetas

Fuente: http: lightreadig.com/Multiprotocol label switching

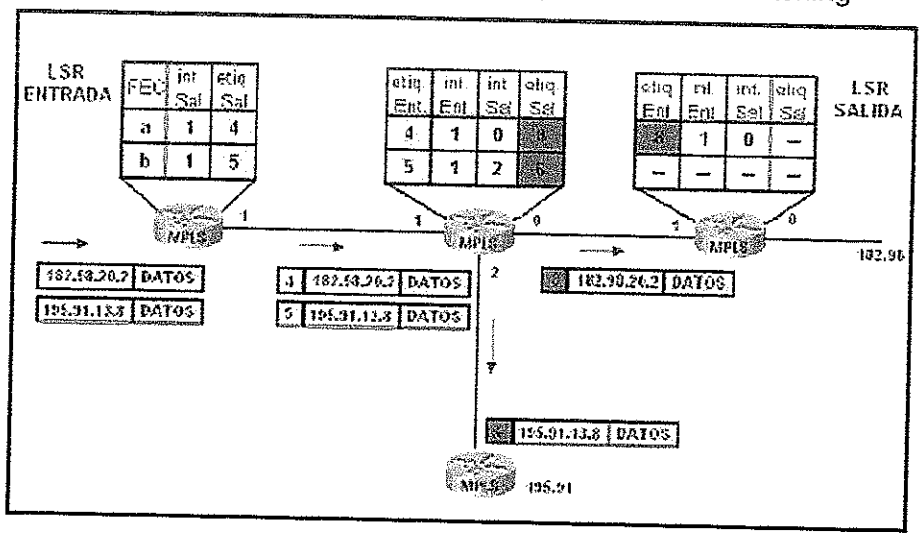

Figura 4. Diagrama de manejo de colas y etiquetas

Como se puede observar en la Figura 4 cada LSR tiene una tabla de reenvío

para cada LSP que pasa por sus interfaces. Dichas tablas manejan diferentes tipos de datos, la tabla del LSR de entrada maneja la FEC, la interfaz de salida y etiqueta de salida, los LSR siguientes manejan etiqueta e interfaz, ambas de entrada y de salida [21].

Posteriormente se muestra como llegan los datos (a y b) sin etiqueta al LSR de entrada, el cual les asigna una etiqueta de salida y lo manda al siguiente LSR (*next hop LSR*). El LSR siguiente deshecha las etiquetas de entrada y les añade nuevas y las manda a los LSR correspondientes, es aquí donde se ve la escalabilidad de la tecnología, ya que las etiquetas solo tienen significado local. Otra de las funciones del LSR de entrada es asignarle una FEC a cada paquete sin etiquetar que entra, y en base a esto asigna cada paquete a un LSP particular. En la Figura 4 tenemos dos FECs (a y b) cada uno con su LSP particular.

2.10.2 Formato de etiquetas MPLS

Fuente: MPLS, http: www.cisco.com

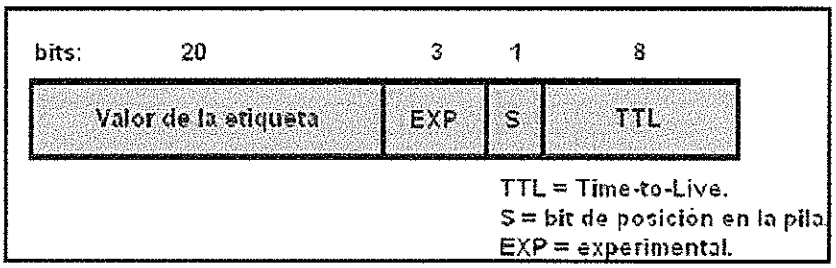

Figura 5. Formato de Etiqueta

Una etiqueta MPLS esta conformada por 32 bits, divididos como se muestra en la Figura 5, y contiene los siguientes elementos:

- Valor de la etiqueta: Etiqueta de 20 bits con valor local.
- Experimental: Son los 3 bits siguientes reservados para uso experimental.
- S: Es el bit de posición de pila:

- Cuando es 1 denota que es la entrada más antigua en la pila.
- Cuando es 0 denota que es cualquier otra entrada.

• Tiempo de Vida (*TTL*): Son los últimos 8 bits del paquete y se utilizan para codificar el valor del conteo de saltos (IPv6) o de tiempo de vida (IPv4).

Las etiquetas de la pila de etiquetas MPLS van después de los encabezados de la capa de enlace de datos (modelo OSI) [8], pero antes de los encabezados de la capa de red. A continuación una descripción gráfica de la ubicación del protocolo MPLS en cuanto al modelo OSI.

Fuente: http: www.wikipedia.org/modelo OSI

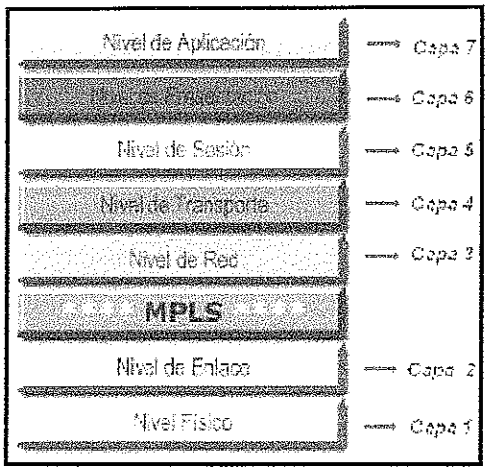

Figura 6. Modelo OSI-MPLS

En la Figura 6 se muestra el modelo OSI añadiendo el campo MPLS entre el Nivel de Enlace y el Nivel de Red. Para realizar el encaminamiento mediante túneles veamos un ejemplo:

Fuente: SEMERIA C, traffic engineering for the public network

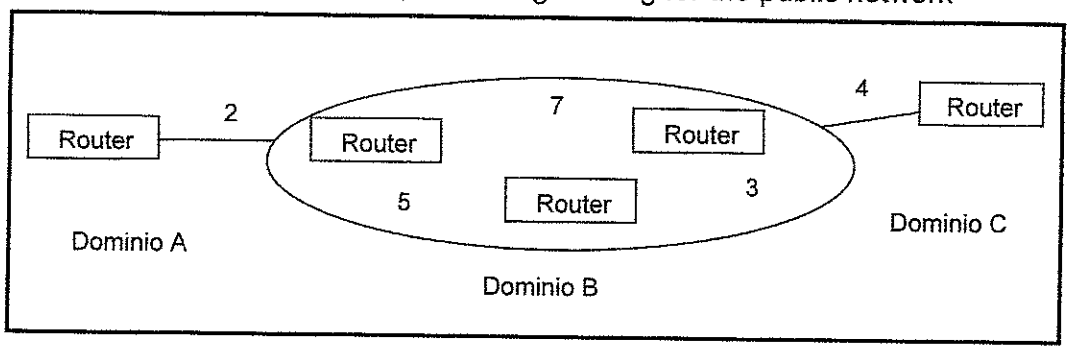

Figura 7. Rutas mediante túneles

Encaminamiento:

- La secuencia de etiquetas entre dominios es: 2-7-4
- La secuencia de etiquetas dentro del dominio B es: 5-3
- Las operaciones que se realizarán son:
  - Del dominio A al B el paquete llevará la etiqueta 2.
  - En el *router* de entrada al dominio B se intercambiará la etiqueta 2 por la 7, que identifica al nuevo dominio, y apila la etiqueta 5 que indica el siguiente salto en esa red.
  - En el siguiente *router* se intercambiará la etiqueta 5 por la 3.
  - En el *router* de salida se desapila 3 y ve que la etiqueta de entrada que tiene es 7, e intercambia ésta con 4 para llegar al siguiente dominio.[5]

2.10.3 Distribución de etiquetas

Para configurar el LSP cada LSR en el camino debe realizar una serie de operaciones:

1. Primero debe de asignar una etiqueta al LSP que sirve para identificar los paquetes que pertenecen a dicho FEC.

2. Posteriormente debe de informar a todos los nodos (computadoras,

servidores, routers IP, conmutadores, etc.) que mandan información, de la nueva etiqueta asignada por el LSR a la FEC en cuestión. Esto con el propósito de que dichos nodos etiqueten correctamente los paquetes con dirección al LSR que los contacto.

3. Por último debe saber cual es el siguiente salto para el LSP y la etiqueta que le asignó el next hop LSR. Este proceso permite la LSR mapear la etiqueta de entrada a una etiqueta de salida.

La primera operación se realiza localmente, sin embargo la segunda y la tercera se deben realizar manualmente o mediante un protocolo de distribución de etiquetas. La función principal de dichos protocolos es permitir a los LSR informar a los demás LSRs de las operaciones que realizó a las etiquetas del FEC. Adicionalmente, los protocolos de distribución informan las capacidades MPLS de cada LSR a los demás LSR. Extensiones a los protocolos RSVP y BGP (entre otros) pueden proporcionar funcionalidad a la distribución de etiquetas MPLS.

MPLS permite varios protocolos de señalización para la distribución de etiquetas entre LSRs, el uso de cada uno de ellos dependerá del hardware de la red MPLS y de las políticas de administración de ésta.

Protocolos de routing como BGP permiten llevar piggybacked información sobre las etiquetas entre los contenidos propios del protocolo, se utilizan para etiquetas externas en VPNs. RSVP también ha sido extendido para soportar intercambio de etiquetas piggybacked.

Además, MPLS tiene su propio protocolo LDP para señalización y gestión del espacio de etiquetas, a éste se le han añadido extensiones para soportar, también, requerimientos de QoS y CoS (Class of Service), así tenemos CR-LDP (Constraint-based – LDP). RSVP y CR-LDP se utilizan para la ingeniería

de tráfico y reserva de recursos. Para direcciones multicast tenemos PIM (Protocol-Independent Multicast) [1].

2.10.4 Asociación de etiquetas bajo demanda

La comunicación bajo demanda se da cuando un LSR pide a su siguiente salto que le informe de la etiqueta que debe usar y la interfaz de entrada para enviarle datos dirigidos a un destino definido. Según el destino el LSR del siguiente salto le envía la etiqueta que más le convenga para dicho destino.

Este proceso suele ser el mas usual y uno de sus aspectos más interesantes es que la distribución de etiquetas se lleva acabo en sentido contrario al tráfico de datos. Las Figuras 8 y 9 muestran claramente el proceso:

Fuente: SEMERIA C, traffic engineering for the public network

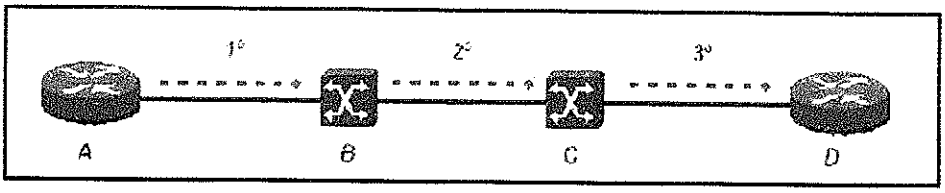

Figura 8. Solicitud de etiqueta bajo demanda

A continuación los pasos que sigue la Figura 8:

1. Primero el LER A pide una etiqueta de tráfico dirigido a la dirección 192.168.100.1. (Dirección IP ejemplo, no real)
2. Después el LSR B contesta que no es el LER de salida y que enviará la petición al siguiente vecino y posteriormente le envía la dirección a C.
3. El LSR C hace lo mismo que el LSR B pero ahora envía a D.
4. El LER D recibe la petición de etiqueta del LSR C y hace lo siguiente:

Fuente: SEMERIA C, traffic engineering for the public network

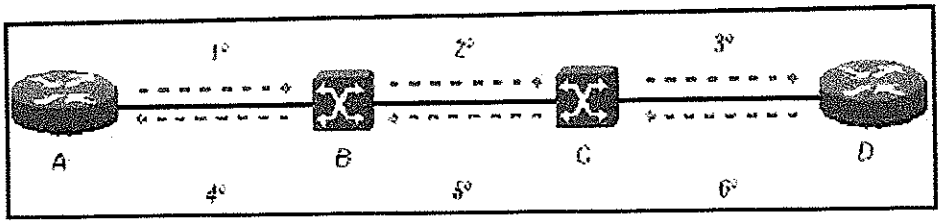

Figura 9. Respuesta a solicitud bajo demanda

A continuación se muestran los pasos que sigue la Figura 9:

5. El LER D confirma que es el LER de salida. Posteriormente dice que se utilice la etiqueta "57" (Tomamos el 57 como ejemplo) para el tráfico 192.168.100.1.
6. El LSR D toma el valor "57" como de salida y envía "45" al LSR B.
7. EL LSR B recibe el valor "45" como etiqueta de salida y envía "10" al LER A que solicito el valor.
8. Finalmente el LER de entrada A toma el valor "10" para el tráfico dirigido a 192.168.100.1 y envía la información.

En este último paso el LER de entrada recibe la etiqueta que pidió y en todo el camino ya están creadas las tablas de conmutación para cuando se envíe la etiqueta.

2.10.5 Asociación de etiquetas a múltiples destinos

Este método cada LSR realiza asociaciones de etiquetas y FEC para transmitirlas a sus vecinos para que las almacenen en sus tablas de etiquetas. En este caso la información de etiquetas para tráfico también viaja en sentido contrario al flujo de tráfico pero aquí la información la reciben todos los nodos, inclusive sin haberla pedido. Esta es una manera eficiente de mantener las tablas de todos los nodos actualizadas, el problema que esto representa es que el tráfico en la red se incrementa significativamente, sin embrago agiliza la creación de nuevos FECs.

2.10.6. Etiquetación frente a encapsulación

MPLS etiqueta la información, sin embargo algunos autores utilizan la palabra "encapsulación" para describir el funcionamiento de las etiquetas en dicha tecnología. Cuando se encapsula un protocolo en otro se forma una Unidad de Datos de Protocolo (*PDU*) o unidad de datos de protocolo de nivel N-1. Siendo el paquete la PDU de la capa de red, cada capa emisora de un protocolo toma la PDU de una capa superior, y lo codifica dentro del área de datos. A medida que se transmite, la capa recibe la PDU de su capa par, recupera el área de datos y la transmite a una capa superior, que procede de igual manera. Por esta razón las PDU tienen encapsuladas en su área de datos otras PDU [1].

MPLS toma la PDU de red y la transmite intacta, solo coloca una etiqueta MPLS entre el encabezado de red y el de enlace, esto deja intactas las tramas pequeñas de tamaño fijo del protocolo de red. Si el protocolo de red es IP las tramas son variables y comúnmente grandes, MPLS no modifica esta información y la trasmite intacta.

Fuente: SEMERIA C, traffic engineering for the public network

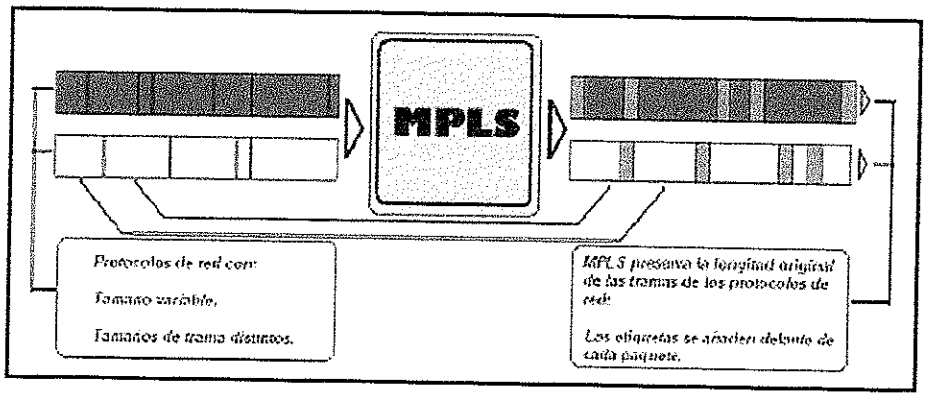

Figura 10. Longitud de trama fija en MPLS

En la imagen Figura 10 se puede ver la diferencia en el tamaño de las tramas de los protocolos de red, en MPLS la longitud de las tramas es fija lo que generaliza el proceso.[5]

2.11 Relación entre FECs, LSPs y Etiquetas.

Para entender el funcionamiento de la tecnología MPLS, es necesario comprender y analizar la importancia de la relación entre etiquetas, el LSP y la FEC. La característica principal de la funcionalidad de la tecnología MPLS es que el tráfico se divide en "canales privados" (Clase de Equivalencia de Reenvío). El tráfico de cada FEC viaja por medio de un LSP dentro del dominio MPLS. Los paquetes dentro de un FEC solo tienen validez en dicho canal, ya que las etiquetas son de significado local.

A lo largo de la nube MPLS en cada LSR se reenvían los paquetes etiquetados a la ruta especifica de la etiqueta, cada vez que entra el paquete al LSR este reemplaza el valor de la etiqueta de entrada con el nuevo valor de la etiqueta de salida. Esto se lleva acabo sucesivamente hasta que dicho paquete llega al router se salida.

2.12 Requisitos para el tráfico MPLS

Para que esto se lleve acabo satisfactoriamente se deben de cumplir los siguientes requisitos:

1. Todo tráfico debe de asignarse a un FEC específico.

2. Se necesita un protocolo de ruteo para determinar la topología y las condiciones del dominio para que las LSPs puedan ser asignadas a un FEC. Adicionalmente, el protocolo de ruteo debe de recolectar información y utilizarla para proveer los requerimientos de QoS del FEC.

3. Cada LSR debe de conocer las LSPs de cada FEC para poder asignarles una etiqueta de entrada y deben de comunicarla a todos los demás LSR en la ruta de dicho LSP.

Para poder entenderlo mejor se va a realizar un análisis de cada uno de los puntos mencionados anteriormente.[6]

2.13 Topología de LSPs.

El primer requisito se lleva acabo fuera de las especificaciones MPLS. La asignación del flujo de datos a una FEC específico se puede llevar acabo de diferentes maneras:

- Configuración manual.
- Protocolo de asignación.
- Análisis de paquetes de entrada en el LER.

La topología de la red MPLS tiene cuatro variantes, de las cuales la última sigue en etapa de desarrollo:

1. Un LSR de entrada y otro de salida. En este caso solo es necesario un camino a través del dominio MPLS.

2. Un LSR de salida y varios LSR de entrada. Este caso se da cuando se le asigna tráfico de diferentes fuentes a una sola FEC, el flujo de datos puede entrar por diferentes LSR de entrada. Un ejemplo claro es el caso de una intranet empresarial en una misma ubicación conectada a un dominio MPLS con varios LSR de entrada. Esto genera varios caminos dentro del dominio MPLS que comparten los últimos saltos (*hops*) antes de llegar al LER.

3. Varios LSRs de salida y tráfico unicast. En este caso la FEC puede requerir varios LSP a diferentes LERs, esto se da cuando el LSR de salida esta conectado a un cluster de redes. Todos los destinos del cluster de redes son alcanzables por el mismo LSR de salida. Este caso se da cuando un paquete no es asignado a la FEC por la dirección destino de la capa de red (como comúnmente sucede).

4. Varios LSR de salida para tráfico a múltiples destinos (*multicast*). El tráfico multicast en MPLS es la tecnología que dará funcionalidad a los servicios de banda ancha de la próxima generación de telecomunicaciones. De esta manera se pueden proveer servicios de transmisión de video de alta calidad y fiabilidad a multiusuarios ocupando un mismo canal. En un pasado para simular multicast se utilizaba un canal distinto (transmitiendo la misma información) para cada usuario, por ejemplo en una videoconferencia dirigida a destinos diferentes. Esto representaba un coste altísimo por el ancho de banda requerido, además de que no soportaba QoS ni Ingeniería de Tráfico. Multicast en MPLS es el futuro de la televisión vía IP y de la transmisión de streaming media dirigida a multiusuarios.[24]

2.13.1 Selección de rutas

El Multiprotocolo de Conmutación de Etiquetas maneja tres tipos de técnicas para la selección de rutas que toman los LSP dentro de un FEC específico:

- Ruteo de salto a salto (Hop-by-hop routing).
- Ruteo Explicito (Explicit routing).
- Algoritmo de Ruteo basado en restricciones (Constraint-based routing algorythm).

2.13.1.1 Ruteo Salto a Salto

En el ruteo de salto a salto cada LSR escoge el siguiente salto para cada FEC, independientemente de los demás LSRs. En esta opción se utiliza OSPF, siendo uno de los protocolos de ruteo más sencillos, provee sólo algunas de las ventajas de MPLS como son: conmutación y apilado de etiquetas, trato diferencial de paquetes de diferentes FEC pero con la misma ruta. Sin embargo no provee Ingeniería de Tráfico ni Políticas de Ruteo para el manejo de QoS.

2.13.1.2 Ruteo Explicito

En el ruteo explicito el LSR de entrada o de salida define todos o varios de los LSRs por los que va pasar el LSP dentro de un FEC determinado. Cuando el LER define todos los LSR se cumple completamente el ruteo explicito, si define solo algunos el ruteo explicito es parcial. Con cualquiera de las técnicas de ruteo explicito se manejan todos los beneficios de MPLS, tanto de ingeniería de tráfico como de QoS.

Las rutas explicitas se pueden definir de previamente o bien dinámicamente. Si las rutas se definen dinámicamente se mejora el alcance de las técnicas de Ingeniería de Tráfico. Para que esto sea posible el LER debe de tener información de la topología de la red y de los requisitos de QoS del dominio. El documento RFC 2676 sugiere que la información QoS debe de dividirse en dos categorías:

a) Un conjunto de atributos asociados con un FEC o con un conjunto de FECs similares que definen sus características de comportamiento a forma de grupo.
b) Un conjunto de atributos asociado con los recursos, como nodos y ligas, que obligan el paso de los LSPs a través de ellas. Las categorías se deben formar con el fin de cumplir con las especificaciones de la Ingeniería de Tráfico en MPLS.

2.13.1.3 Ruteo mediante un algoritmo

Por ultimo esta el ruteo mediante un algoritmo a base de restricciones en donde se toman en cuenta los requisitos de varios flujos de paquetes y los recursos disponibles en cada salto y en diferentes nodos. Una red MPLS que implementa esta técnica de selección de rutas esta consciente en todo momento de la utilización de los recursos, de la capacidad disponible y de los servicios proporcionados.

Las técnicas tradicionales de ruteo como OSPF y el Protocolo de Pasarela Externa (*BGP*) no cuentan con métricas de coste (*cost metrics*) suficientes para el manejar restricciones en sus algoritmos. La razón principal es que solo manejan una métrica de costo ya sea conteo de saltos, retraso (*delay*), etc. Para esta técnica es necesario contar con otro tipo de métricas, como: Proporción de pérdida de paquetes, reserva de capacidad actual, retraso de propagación y transferencia máxima de datos de la conexión. [35]

2.13.2 Protocolos de selección de rutas MPLS

Una de las funcionalidades que tiene MPLS, principalmente en la transmisión de video, es que asegura que siempre habrá recursos disponibles para mantener el canal de transferencia fluido; cuando se cumplen los requisitos de QoS. Esto es muy importante en videoconferencias multipunto, en donde se asegura ancho de banda suficiente para el video y se acota un retardo máximo para la voz. Para hacer esto se necesitan dos cosas:

1. Ruteo con QoS para determinar la métrica.

2. Algoritmo de distribución de etiquetas que permita reservar recursos para cada petición. CD-LDP o RSVP-TE

2.13.2.1 CR-LDP

El protocolo CR-LDP es muy parecido al protocolo Salto a Salto visto en secciones anteriores, sin embargo, tiene algunas particularidades, como son:

a. El mensaje *LDP_REQUEST* que envía el LER permite especificar explícitamente que rutas van a ser utilizadas.

b. La ventaja principal de manejar rutas explicitas es que pueden reservar recursos con diferentes características. Las características del camino están descritas por:

• Velocidad de Pico de Datos (*PDR*) – velocidad máxima de transferencia de datos.

• Velocidad de Datos Garantizada (*CDR*) – velocidad de transferencia de datos reservada.

• Tamaño Pico de la Ráfaga (*PBS*) – tamaño máximo de la traza.

• Tamaño de Ráfagas Garantizado (*CBS*) – tamaño máximo reservado de la traza.

• Frecuencia (*frecuency*) – especifica que tan frecuentemente se garantiza el CDR.

• Peso (*weigth*) – determina las prioridades relativas en cada LSR para múltiples LSP cuando amenaza congestión o hay poco ancho de banda disponible.

c. En CR-LDP los recursos requeridos pueden ser negociables. Cuando un LSR no tiene los recursos necesarios para satisfacer un parámetro negociable, realiza la reserva de los recursos disponibles y propaga el *LDP_REQUEST* con los nuevos valores al próximo LSR para que este complete la petición.

2.13.2.2 RSVP-TE

El protocolo RSVP-TE es una extensión del protocolo RSVP original, que fue diseñado para ejecutar la distribución de etiquetas sobre MPLS. RSVP-TE soporta además la creación de rutas explícitas con o sin reserva de recursos.

Una de las características adicionales más importantes de este protocolo es que permite el re-enrutamiento de los túneles LSP, con el fin de dar una solución ante caídas de red, congestión y cuellos de botella. Originalmente el IETF propuso a RSVP-TE como el protocolo de señalización principal, ya que este era utilizado por la mayoría de las compañías de Internet en MPLS y porque la tendencia es utilizar un protocolo de señalización RSVP. De aquí en adelante la IETF recomendó profundizar más en el protocolo RSVP y dejar a un lado CR-LDP.

A continuación (Figura 11) un escenario de funcionamiento del protocolo RSVP-TE, adaptado en este caso para tráfico multicast, en donde la videoconferencia es uno de los principales desafíos para el QoS.

Fuente: ROSEN E.C, Multiprotocol Label Switching and Protocol RSVP-TE

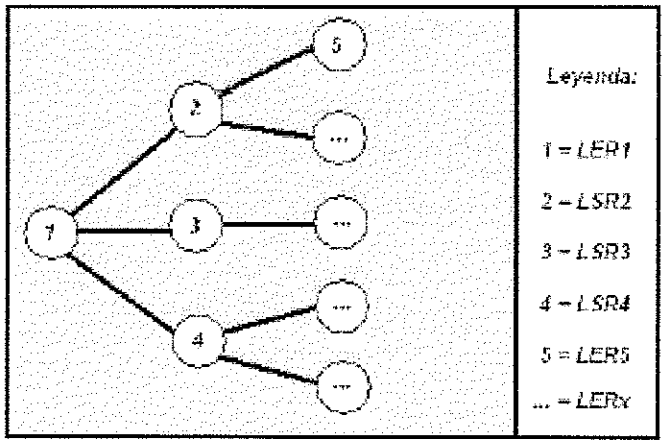

Figura 11. Funcionamiento RSVP-TE

1. Primero tenemos un nodo de entrada LER1 que determina que necesita establecer una nuevo LSP con un LER de salida. Es aquí donde por medio de políticas administrativas el LER1 determina las rutas para los nuevos LSPs. En este caso determina que el nuevo camino al LER5 debe establecerse por el nodo intermedio LSR2.

El LSR1 es el encargado de construir y mandar el mensaje *PATH* que contiene la ruta explicita (LSR2, LSR3). El mensaje se envía en forma de paquete IP y contiene los detalles de los parámetros de tráfico para la nueva ruta. Cuando el mensaje *PATH* llega al siguiente salto (LSR2) este contiene también el objeto *LABEL_REQUEST* pata la petición de las etiquetas.

2. Los nodos intermedios (LSR2, LSR3, LSR4) reciben el mensaje PATH, al ver que no son LERs, reenvían el mensaje a través de la ruta contenida en el mensaje, esto se repite hasta que el nodo que recibe el mensaje sea de salida.
3. Todos los nodos de salida contenidos en las LSPs asignan los recursos solicitados y seleccionan una etiqueta para cada una de las rutas. La etiqueta se envía y se distribuye dentro del mensaje *RESV* en el objeto *LABEL*. El mensaje se envía por el puerto donde llegó el mensaje *PATH*.

4. Cuando los nodos LSR 1, 2 y 3 reciben el mensaje *RESV*, determinan los recursos que deben reservar, guardan la etiqueta para cada LSP y agregan la información del valor de la etiqueta, el puerto de salida y el puerto de entrada en la tabla *LIB* (Figura 12) . Después de esta acción envía el mensaje *RESV* al nodo anterior.

Fuente: SEMERIA C, traffic engineering for the public network

LIB Nodo X		
Dir. IP Multicast	*Et. de Salida*	*Nodo new-hop*

Figura 12. Formato de tabla LIB

5. Cuando el mensaje RESV llega al nodo de entrada LER1, este solo actualiza la tabla LIB (Figura 12), no asigna una nueva etiqueta ni reenvía el mensaje *RESV*. En el tráfico multicast en RSVP-TE y CR-LDP se le llama Caminos Multicast de Conmutación de Etiquetas (*mLSP*) al conjunto de LSPs configurados. Una de las ventajas que tiene RSVP-TE sobre CR-LDP es que la operación de actualización de los mensajes *PATH* y *RESV* muestra los enlaces activos para identificar fácilmente cuando un LSP no puede ser establecido. Cuando esto pasa se generan los mensaje *PATHERR* y *RESVERR*. Otra forma de detectar errores, más sencilla y robusta, es mediante mensajes HELLO, para detectar fallas nodo a nodo.[19]

2.14 Protocolo LDP

Todo LSR que soporte el protocolo LDP debe mantener sesiones LDP con otros LSR o LER que hagan lo mismo. Durante una sesión LDP se generan diversos tipos de mensajes con la finalidad de dar a conocer a otros enrutadores que el enrutador esta vivo, mantener vivo dicho conocimiento, comunicar las asociaciones que el LSR haga de etiquetas o FECs, solicitar etiquetas a otros LSR, comunicar cuando una asociación ya no es válida, entre otras. En resumen el protocolo LDP mantiene el dominio MPLS en coherencia, en cuanto a las etiquetas y las relaciones que puedan tener con otros FECs en la red.

Los mensajes LSP son de suma importancia y deben de ser fiables al 100% ya que gracias a ellos es que MPLS funciona. Cuando se utiliza IP como protocolo de red, los LSRs anuncian su estado mediante UDP/IP; si utiliza IP lo hace mediante multicast a todos los routers suscritos al domino MPLS. Cuando los routers suscritos reciben el mensaje, que se comporta como un "*ping*" tradicional, estos los reenvían también. En los mensajes "*ping*" o "*hello*" vía UDP se transporta también la IP del servidor que se anuncia con el fin de que si alguno de los LSR desea establecer una sesión LDP, lo hará con el protocolo TCP y a la dirección IP anunciada. Si se da el caso, se establece la conexión y se inicia una sesión LDP entre los LSR interesados.

A continuación la representación gráfica del proceso de multicast a través de mensajes "*hello*" mediante sesiones LDP en un dominio MPLS.

Fuente: SEMERIA C, Multiprotocol Label Switching

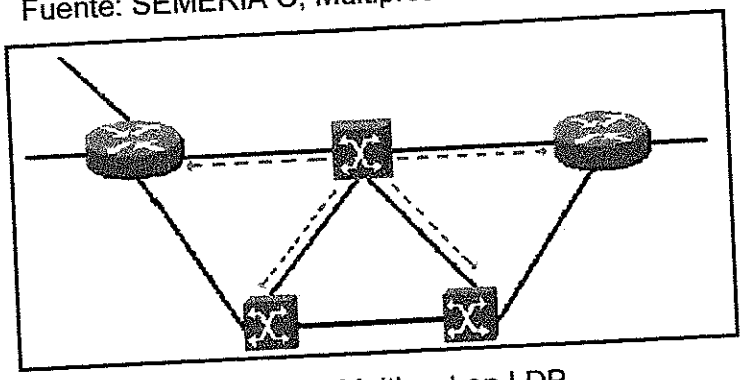

Figura 13. Multicast en LDP

En la Figura 13, el LSR enmarcado en rojo soporta LDP y envía mensajes "hello" periódicamente mediante el protocolo UDP para ver si algún vecino quiere establecer una conexión LDP.

Fuente: Fuente: SEMERIA C, Multiprotocol Label Switching

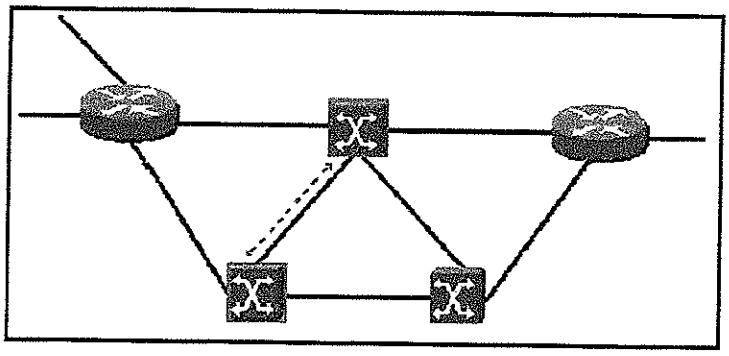

Figura 14. Sesión LDP entre nodos MPLS

En la Figura 14 todos los nodos reciben los mensajes "hello" del emisor, sin embargo, solo el LSR inferior izquierdo le interesa establecer una sesión LDP con el que LSR que envió el anuncio. Después abre una conexión TCP con el para establecer una sesión LDP. Cuando la sesión LDP esta abierta existen dos métodos por los cuales se comunican las asociaciones de: etiquetas, de la FEC con LSR y de la FEC con LER.

2.15 Modelo de Servicios Diferenciados (*DiffServ*)

El modelo DiffServ propuesto por el IETF se basa en clasificar el tráfico del dominio en clases, cada una con: políticas de cola y de reenvío independientes. Este modelo sustituye al modelo anterior propuesto por el IETF llamado Servicios Integrados (*IntServ*) que tenía problemas de escalabilidad ya el se trataba el tráfico por flujo y no por clase de tráfico, lo que impide el uso de políticas CoS. En este último modelo cuando el número de flujos aumenta el número de estados de los routers aumenta enormemente, lo que al final de cuentas genera una congestión insostenible en la red.

En MPLS los LSP pueden llevar uno o varios FEC y se pueden asignar numerosos flujos de información a cada FEC como sea necesario, el protocolo es tan manejable que se puede asignar, por así decirlo, que tráfico va a ser

enviado por que cable físico del dominio que forma el LSP. De esta manera se puede asignar que tipo de tráfico va a ser transportado por medios físicos ópticos o de cobre en el caso de Cable de Par Retorcido no blindado (*UTP*) de Categoría 5e (*CAT5e*), esto con el fin de agrupar diferentes tipos de servicio a diferentes medio físicos. Es por esto que la diferenciación de servicios es mucho más escalable que su predecesor servicios integrados.

La asignación de canales se puede hacer a nivel FEC o a un conjunto de FECs que a su vez pueden incluir cientos de flujos de información distintos, esto ayuda a disminuir la carga de estados en los routers. En la Figura 15 se muestra una nube MPLS con diferentes clases de servicio.

Fuente: Fuente: SEMERIA C, Multiprotocol Label Switching

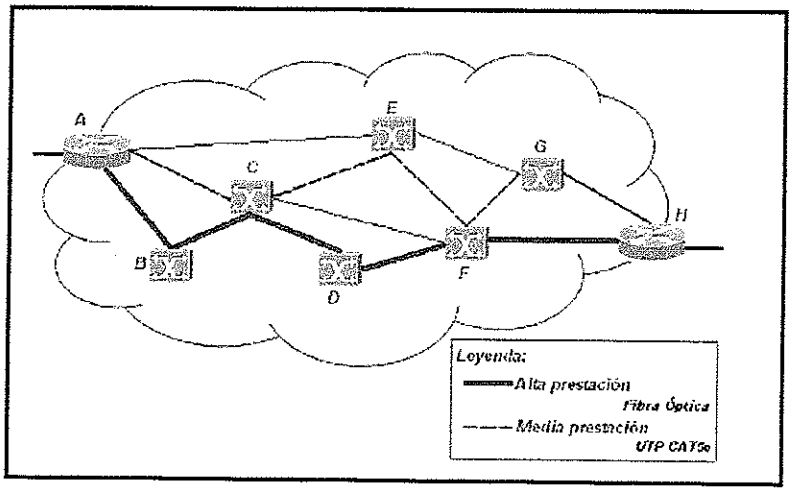

Figura 15. LSP con distintas prioridades

Este tipo de control de flujos es solo una de las opciones disponibles en la tecnología MPLS, ya que cuando la tecnología MPLS trabaja de la mano con DiffServ se puede especificar la clase de tráfico a la que pertenece cada paquete. Esto modifica la manera en que se mueve cada paquete a través de los LSR del dominio MPLS.[26]

2.15.1 Clase de Servicio

Con CoS cada paquete MPLS puede llevar en su encabezado de los 8 disponibles, solo hay 8 tipos de servicio porque solo hay 3 bits disponibles: xxx000 para designar la clase de servicio. Con esto podemos especificar que un LSP se transporte por cierto camino físico de fibra óptica con mayor rapidez y calidad y que otro LSP vaya por un camino físico distinto, como el cobre, con menor rapidez y prestaciones. A su vez se pueden asignar clases de servicio a paquetes dentro del mismo FEC, mismo LSP y mismo medio físico.

Ahora, con esta nueva característica cada LSR que soporte servicios diferenciados MPLS debe de conmutar en base a los 20 bits completos, incluyendo el nuevo campo CoS, un ejemplo de la tabla interna de un LSR es el siguiente:

Fuente: www.gams.com/mpls and Internetworks

Paquete MPLS de entrada			Paquete MPLS de salida		
Etiqueta de entrada	CoS	Interfaz de entrada	Etiqueta de salida	CoS	Interfaz de salida
50	1	1	51	1	2
50	5	1	51	5	2
75	0	2	75	0	3
...	...	...	...	...	...

Figura 16. MPLS con CoS

En la figura 16 se puede apreciar con facilidad como tráficos que entran por la misma interfaz física y con la misma etiqueta pueden tener deferente clase de servicio, pero deben de tener un trato distinto porque pertenecen a clases distintas. Esto se logra porque cada LSR que maneja DS (abreviación de DiffServ) clasifica todo el tráfico entrante dependiendo de su clase de servicio.

Para cada clase de servicio de los 8 disponibles se forma una cola gestionada por políticas que pueden ser distintas para cada tipo de servicio disponible. De

esta forma con DS se forman 8 colas, cada una con una clase de servicio distinta pero con diferentes tipos de datos como: Protocolo de Transferencia de Hipertexto (*HTTP*), Protocolo de Transferencia de Archivos (*FTP*), voz sobre IP (*VoIP*), etc. Cada cola tiene prioridades distintas en función del QoS que se quiera ofrecer para cada servicio. Para finalizar el proceso de CoS un algoritmo cíclico irá despachando cada una de las 8 colas.

El modelo de servicios diferenciados permite que MPLS proporcione QoS como una de sus ventajas principales y hoy en día es un punto clave en el entorno de la tecnología de conmutación de paquetes multiprotocolo.

CAPITULO 3

INGENIERÍA DE TRÁFICO

3.1 Introducción a la ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces.

La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura 17 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

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

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

Fuente: www.rediris.es/rediris/boletin/53/enfoque1.html

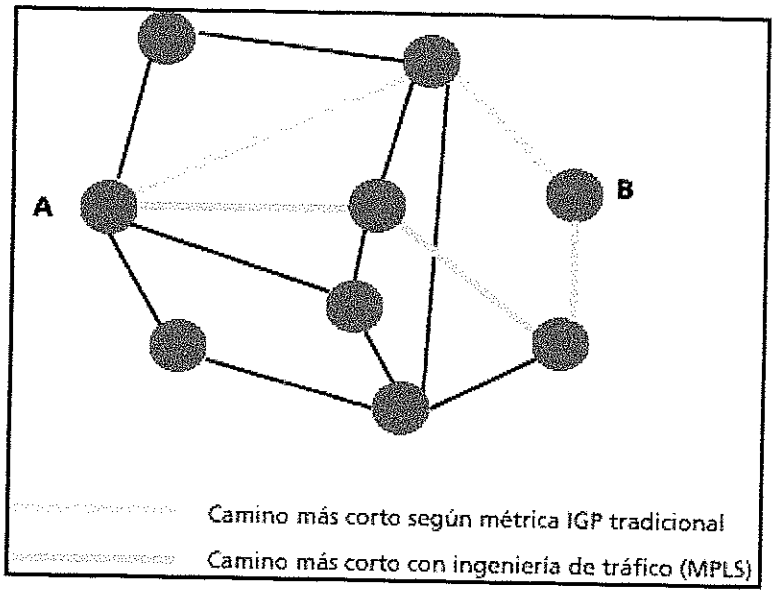

Figura 17. Diagrama de encaminamiento TE

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de

planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.[18]

La ingeniería de tráfico es el proceso que mejora la utilización de la red mediante la distribución del tráfico en ella de acuerdo con la disponibilidad de los recursos, el tráfico actual y el esperado. CoS y QoS pueden ser factores a tener en cuenta en este proceso.

Como resultado, tenemos que se evita la congestión en cualquier camino. La mejora de la utilización de la red no implica necesariamente que se obtenga el mejor camino, pero sí el mejor camino para un determinado tipo de tráfico.

La ingeniería de tráfico permite al proveedor hacer un mejor uso de los recursos y permitir reservar enlaces para determinadas clases de servicio o clientes. Aquí encontramos el caso de las **rutas forzadas**. La ruta que un LSP puede tomar puede forzarse para que cumpla unos requerimientos seleccionados en el LER de entrada (un caso particular de ellas son las rutas explícitas, donde el parámetro que fuerza este camino es el orden que debe seguir). Los parámetros que pueden ser utilizados para describir esas rutas son el ancho de banda, el retardo, la prioridad, etc., que se desea para un flujo de tráfico. Para calcular estas rutas existen dos métodos:

- Calcular en el LER de entrada toda la ruta basándose en información sobre el estado de la red.
- Calcular la ruta salto a salto con información local a cada LSR sobre la disponibilidad de los recursos.

Los dos métodos pueden combinarse si en alguna parte de la ruta la información no está disponible. Pero no basta sólo con obtener la ruta, es necesario reservar los recursos para poder satisfacer el servicio requerido.[6]

Existen dos aproximaciones: TE-RSVP y CR-LDP, ambas utilizan el encaminamiento explícito para crear los LSPs e introducen una sobrecarga de información adicional al crear, mantener y destruir un LSP, pero ésta, es mínima comparada con la generada al procesar la cabecera IP.

3.2 TE-RSVP.

TE-RSVP (Traffic Engineering – RSVP) es una extensión del protocolo RSVP. TE-RSVP es un protocolo de señalización *soft state* que utiliza UDP o datagramas IP para la comunicación entre compañeros LSR (LSR *peers*).

3.2.1 Creación de un ER-LSP

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.

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. 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.

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. 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.

3.3 CR-LDP

CR-LDP (Constraint-based LDP), a diferencia de TE-RSVP, no necesita de implementaciones adicionales ya que está basado en LDP y utiliza su misma estructura para los mensajes. Es un protocolo *hard state* y utiliza sesiones TCP entre compañeros LSR.

3.3.1 Creación de un ER-LSP

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.

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.

Una vez 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.

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. En cuanto llegue al LER de entrada se habrá

establecido el LSP.[2]

3.4 Comparación de ambos métodos

TE-RSVP es *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 *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 TE-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 refresco.

CR-LDP utiliza conexiones TCP lo que hace que éstas sean más fiables y seguras, mientras que TE-RSVP utiliza UDP o 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 oportunas sean iniciadas. Sin embargo, una conexión fallida en TE-RSVP será detectada cuando no se reciba un determinado mensaje de refresco y, dependiendo de cómo se haya configurado, detectar un fallo tardará segundos o minutos antes de que puedan iniciarse las acciones de recuperación.

Ambos protocolos soportan re-encaminamiento (*re-routing*):

TE-RSVP 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 refresco.

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.

La elección entre los diferentes protocolos se deberá a factores como la complejidad de la red, si las conexiones van a ser cortas o permanentes, qué grado de tolerancia a fallos se requiere, etc.

CAPITULO 4

PROPUESTA

4.1 INTRODUCCIÓN

En este capitulo se propone un diseño que permite a una red IP implementar MPLS para realizar Ingeniería de trafico haciendo un uso eficiente de los recursos de la red. Este diseño se basa en la experiencia adquirida en la empresa Neo. Net Ltda. La cual es una empresa de comunicaciones pionera en el desarrollo de redes WIMAX, la cual permite implementar sistemas inalámbricos metropolitanos extendidos de banda ancha escalables de última generación para Internet y transmisión de datos.

Con esta red de alto desempeño, confiable, segura y propia se logra ofrecer soluciones de acceso inalámbrico (LAN) y enlaces digitales a Internet garantizando calidad y disponibilidad del trafico cursado, priorizando datos, voz y video.

La idea es usar esta experiencia como administradora de la red para realizar el diseño de esta red MPLS orientada a la ingeniería de trafico sobre una red IP como la es Neo.Net Ltda. Hay que tener en cuenta que el rápido crecimiento de las empresas, expansión de negocios y fusiones de otras empresas han permitido el desarrollo de redes mas seguras y flexibles, para lo cual Neo.Net Ltda. Esta a la vanguardia en tecnología para brindar una conectividad de alta velocidad proporcionando una calidad de servicio superior creando una fuerte competencia en el mercado como es Telefónica/Telecom y ETB.

4.2 METODOLOGÍA

4.2.1 ANÁLISIS PRELIMINAR

En la infraestructura de una ISP se tiene que tener en cuenta la calidad de servicio y la rápida conectividad, el diseño tiene que ser apropiado para soportar una elevada redundancia en todos los elementos y múltiples enlaces de alta capacidad.

Al crecer las redes los elementos propios se especializan, la misma estructura de la red permite usar caminos redundantes y rutas optimas lo cual llevan a facilitar la separación de los dominios de broadcast. Tenemos los routers los cuales los podemos dividir en dos grupos:

- Router de concentración: son los que permiten realizar el acceso a la red a los clientes individuales. Su énfasis está en un número elevado de puertos de baja velocidad.
- Router de backbone: permiten el transporte óptimo entre nodos de la red. Su énfasis esta en las mayores tasas de transmisión sobre las interfaces más rápidas disponibles.

La propuesta esta basada en un backbone IP de un ISP en Tunja, para el cual vamos a analizar sus componentes, su funcionalidad y el criterio que se utilizo para la elección de los mismos.

4.2.2 COMPONENTES Y FUNCIONALIDAD

- Router CISCO 3640: router multiservicio flexible que soporta altas densidades y brinda un rendimiento de 50 a 70 Kbps. Es una solución rentable que se adapta a las necesidades y requisitos de la red. Posee características de calidad de servicio y la priorización de tráfico

necesaria para una robusta plataforma multiservicio, brindando una gran solución para redes privadas virtuales a través de características de tunneling avanzadas.

- Switch CISCO 2950: conmutador de 48 puertos, Fast Eth 10 Base-T, 10 Base-TX, posee alto rendimiento que permite pasar de forma sencilla de las redes LAN[5] compartidas tradicionales a redes completamente conmutadas. Ofrece un amplio espectro para aplicaciones de usuarios. Además ofrece escalabilidad y adaptación modular teniendo en cuenta las necesidades de la red.

- KYPUS: es un appliance de Linux, diseñados específicamente para ser robusto, de fácil actualización, administración remota, menor consumo eléctrico, inmune a virus, menor ruido, facilidad de uso, mayor seguridad, tolerancia a fallos y flexibilidad. Esta máquina contiene los siguientes servicios: File Server, WEB Server, Mail Server, IDS/IPS, NAT/DNS/Print Server, DHCP, FTP, LDAP, RAS, PPTP, VPN Client Pass Though, PPPoE, Policy Based Traffic Shaping, Backup/Restore, Content Filtering entre otros. Es robusto, de fácil actualización, administración remota, menor consumo eléctrico, inmune a virus, menor ruido, facilidad de uso, mayor seguridad, tolerancia a fallos y flexibilidad.

- Router CISCO 2800: proporciona una infraestructura que les permite un acceso rápido y seguro a las aplicaciones con una seguridad optimizada. El 2800 incorpora desde el origen, el hardware de encriptación y aceleración para construir VPNs (virtual private networks) incorporada. Como características destacadas de seguridad integra funcionalidad de firewall y la funcionalidad del sistema de prevención de intrusión en línea (IPS - intrusión prevention system). Disponen de DSPs integrados en la plataforma para proporcionar funciones como voz segura, gateway de

[5] Red de Área Local o simplemente Red Local. Una red local es la interconexión de varios ordenadores y periféricos.

voz, audio-conferencias, y transcodificación, combinadas con el proceso de llamadas integrado en Cisco IOS software.

- Router CISCO 2611: router modular de alto rendimiento que tienen la capacidad de integrar varios servicios e integrarlos en uno. Ofrece un rendimiento cinco veces mayor que otras soluciones ya que admite enrutamiento LAN a LAN a velocidad de cable, comprensión de datos de alto rendimiento basadas en hardware y comprensión de datos basados en software. A su vez ofrece interoperatividad y compatibilidad con varios protocolos. Permite su gestión y monitoreo por un protocolo simple que es el SNMP o Telnet.

- BCU: es una unidad de control de ancho de banda, contiene 3 puertos configurables a las necesidades de la red, permite el control por medio de direcciones de MAC controlando la asimetría y reuso de la misma. Por medio de esta se da un menor manejo a la capacidad de la red. No tiene limite en el ancho de banda pero si en el numero de mac la cual soporta hasta 2048 MAC.

- Nodos: Estos permiten la concentración y distribución de la señal al usuario final. Cada una contiene una base, una antena omnidireccional y el punto a punto respectivo.

- CPE: Es la antena del usuario final que trabaja con línea de vista dependiendo a la base que se quiera orientar.

- Centro de Gestión: es donde se realiza el monitoreo y gestión de la red, manteniéndola estable y garantizando el servicio. A su vez se realiza el control y activación de todos los clientes.[29]

4.2.3 CRITERIOS DE DISEÑO

Para poder plantear la infraestructura se tienen que plantear la red en 4 niveles:

- Red de Acceso
- Red de concentración
- Red Troncal
- Red de Gestión, Radius

Para la elección de estos equipos se tuvieron en cuenta los siguientes criterios:

- Escalabilidad y el alto ancho de banda que pueden soportar
- La alta densidad de puertos para una futura aplicación
- Procesador optimizado para agregación de tráfico de gran volumen.
- Prestaciones de valor añadido: VPN, seguridad con listas de acceso extendidas y firewalls, diferenciación de calidades de servicio, soporte multicast, etc.
- Flexibilidad en velocidades de acceso permitidas: PPP, PMP.
- Los routers concentradores de acceso disponen en ambos extremos de interfaces Fast Ethernet o Gigabit Ethernet que permiten una mayor velocidad de transmisión.

Con estos criterios se proyecta que a medida que el tráfico de Internet siga creciendo los router tendrán una mayor densidad de tráfico, el cual será controlado con la misma infraestructura. A parte del backbone se realizo un estudio de sitio en cada uno de los nodos para el desarrollo del backhaul y se tuvo en cuenta los siguientes criterios:

- Plano o mapa de la localidad
- Inspección visual de la localidad
- Identificación áreas de usuario
- Determinación preliminar de las ubicaciones de los Puntos de Acceso Inalámbricos
- Verificación de la ubicación de los Punto de Acceso Inalámbrico
- Estudio de radiofrecuencia
- Posición geográfica

Según estos criterios se obtuvo el siguiente diagrama el cual es manejado actualmente y será utilizado para la propuesta de la red MPLS.

Fuente: [Autor] [Neo.Net Ltda.]

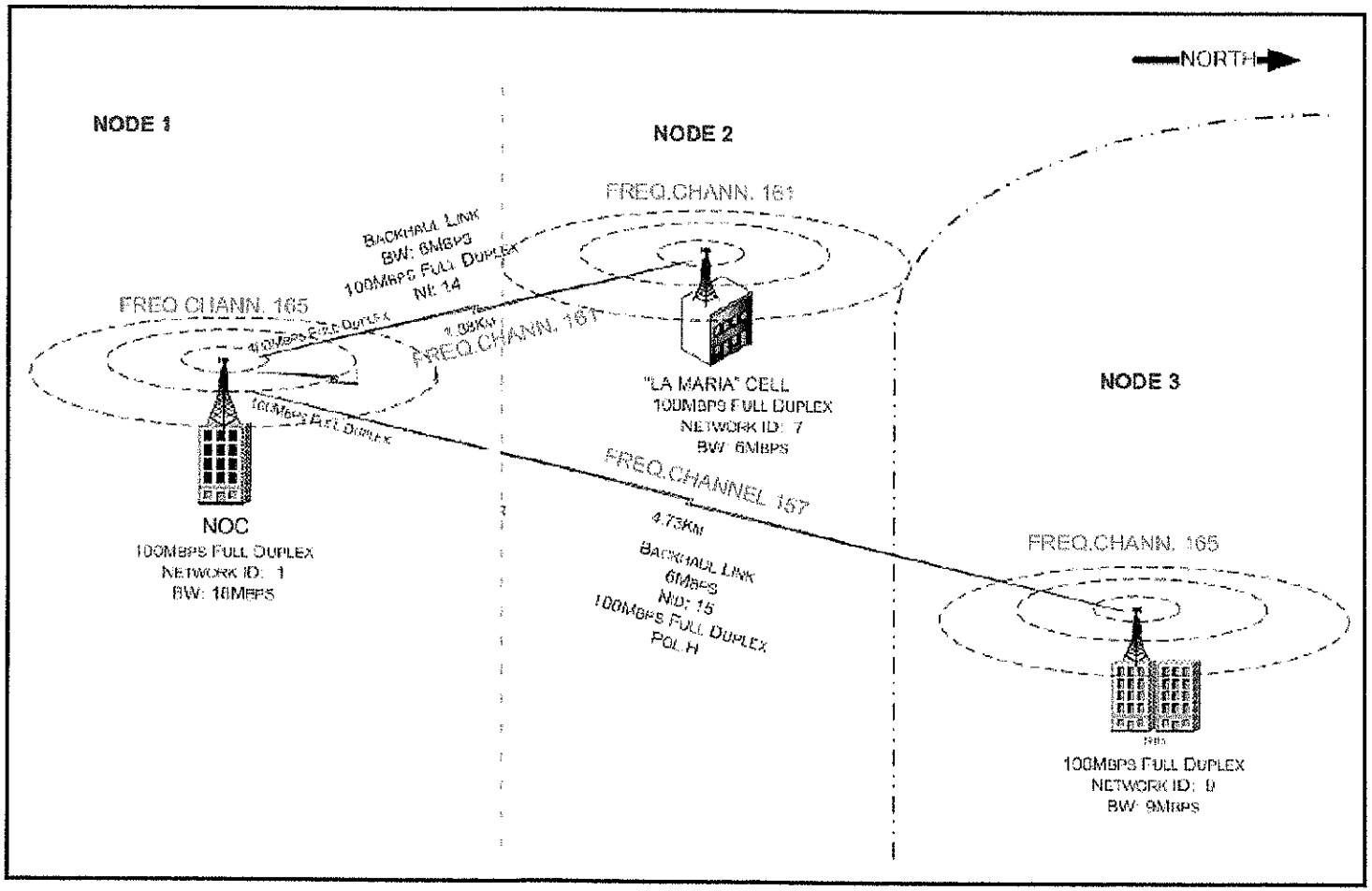

Figura 18. Análisis de Frecuencias de los nodos de la red IP en Tunja

4.2.4 VENTAJAS DE LA RED IP

- Flexibilidad, dado que se puede adecuar el servicio de acuerdo a la necesidad del cliente.
- Escalabilidad para poder crecer sin perder la calidad en su servicio.
- Implementación de servicios de valor agregado según la necesidad del cliente.
- Fácil instalación
- Cobertura
- Control remoto

4.2.5 DESVENTAJAS DE LA RED IP

- Interoperabilidad entre diferentes tecnologías
- Inconvenientes de potencia en los radios ya que se toma de una fuente no regulada.
- Descargas eléctricas.
- Congestión en la red.

Fuente: [Autor] [Neo.Net Ltda.]

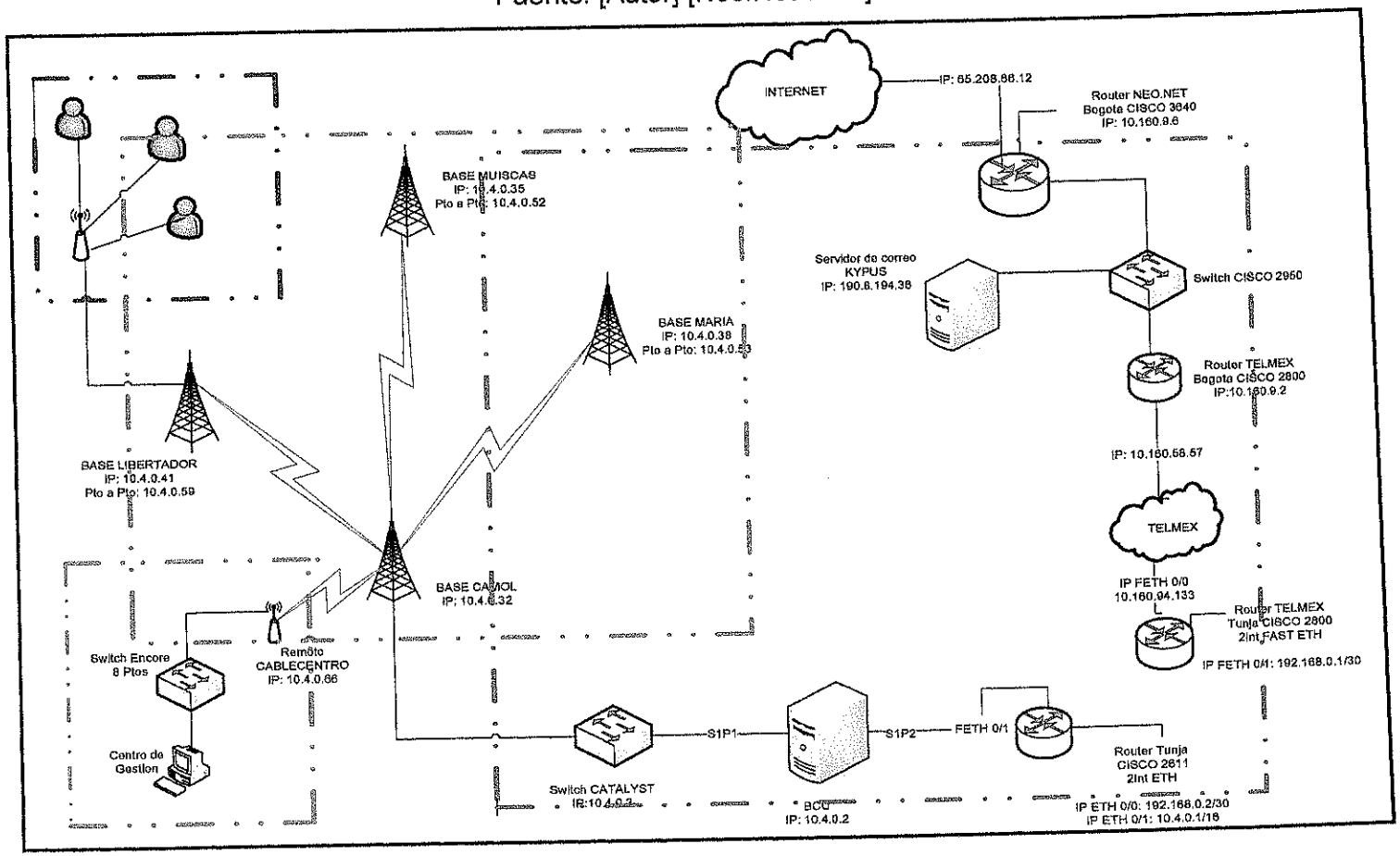

Figura 19. Core IP de la ISP en Tunja

4.3 DISEÑO DE UNA RED MPLS ORIENTADA A LA INGENIERÍA DE TRÁFICO PARA UN ISP EN TUNJA

El diseño de la red MPLS se base en el diseño mencionado anteriormente. En este se agrega el backbone MPLS que será descrito posteriormente con sus diferentes componentes, funcionalidades y desarrollo de la misma.

4.3.1 COMPONENTES

4.3.1.1 COMPONENTES FISICOS

- LER: Es el nodo de borde donde se clasifica el trafico que ingresa al domino MPLS.
- LSR: Es el nodo de núcleo el cual es el especializado en el intercambio de etiquetas.

4.3.1.2 COMPONENTES FUNCIONALES

- FEC: clase en la cual se agrupan todos aquellos tráficos con similares requerimientos.
- LSP: Es el camino que siguen todos los paquetes de una misma FEC.[4]

4.3.2 FUNCIONAMIENTO

Se tiene el LER el cual recibe el trafico a la entrada del dominio MPLS, este clasifica el trafico (origen, destino, tipo de trafico,..etc). Luego asigna una FEC y envía el tráfico por el LSP asignado a la FEC. Dentro del LSP cada LSR se limita a intercambia etiquetas.

La operación se basa en dos componentes esenciales el envío y el control de paquetes, lo cual lo veremos a continuación:

4.3.2.1 Envío de Paquetes MPLS

Fuente: http://www.juniper.com

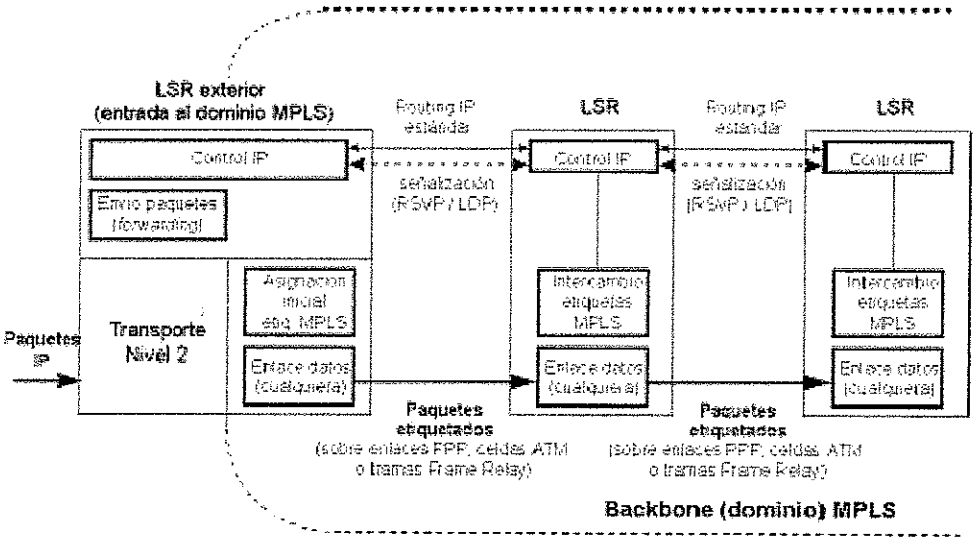

Figura 20. Envío y control de paquetes a través del backbone MPLS

- Se tiene el paquete IP que entra por el nivel 2 del modelo OSI.
- Se realiza la asignación e intercambio de etiquetas que permiten el establecimiento de los caminos LSP.
- Se crea cada LSP (circuito virtual que siguen por la red todos los paquetes asignados FEC) con el fin de conectar uno o más saltos en los que se intercambian las etiquetas, de modo que cada paquete se envía de un LSR a otro a través del dominio MPLS.
- Se insertan las etiquetas en cabeceras MPLS entre los niveles 2 y 3 del modelo OSI.

Fuente: http://www.juniper.com

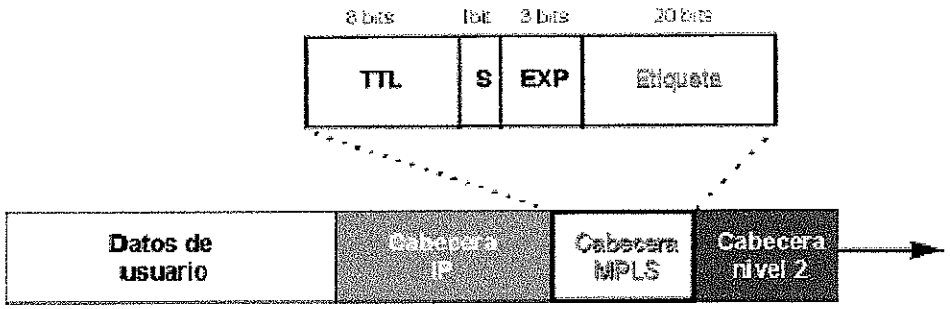

Figura 21. Cabecera MPLS

- Los LSR interiores intercambia las etiquetas a partir de una tabla de envío. La tabla de envío se construye a partir de la información de encaminamiento que proporciona la componente de control.
- Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada la cual se utiliza para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta.

4.3.2.2 Control de Paquetes MPLS

- Al generarse las tablas de envío se realizan sobre la información que se tiene de la red: topología, patrón de trafico, características de enlace,..etc. A su vez se utiliza para establecer los caminos virtuales los protocolos internos IGP para establecer estas tablas.
- Se crea para cada ruta IP un camino de etiquetas uniendo las entrada/salida en cada tabla de los LSR´s.
- El protocolo interno se encarga de distribuir la información necesaria.
- Luego se realiza la señalización para marcar el camino cada vez que se requiera crear un circuito virtual, para lo cual se utiliza el protocolo LDP.
- El protocolo LDP lo que hace es generar diversos tipos de mensajes con el fin de dar a conocer a los router que esta activo y mantiene al dominio

MPLS en coherencia en cuanto a las etiquetas y relaciones que puedan tener con otros FECs en la red.

- Una vez abierta la sesión se puede realizar de 2 formas según tenga la configuración:
    - Bajo demanda: donde el primer LSR solicita la etiqueta y la interfaz que debe utilizar para llegar a su destino.
    - Múltiples destinos: el primer LSR asocia etiquetas y FECs y las envía a múltiples nodos donde estos los almacenan y el que le interese establece la comunicación.
- Los flujos de tráfico siguen el camino mas corto calculado por el algoritmo IGP correspondiente.
- Pero MPLS con su ingeniería de tráfico tiene una ruta alterna no con menores saltos sino la más optimo para evitar cuellos de botella, con garantías explicitas según el requerimiento del cliente.

4.3.3 DISPOSITIVOS UTILIZADOS

Se utilizan router de la familia CISCO ya que MPLS fue propuesto originalmente por unos Ingenieros de CISCO y después de ser implementada por la IETF estuvieron trabajando hasta convertirse en los proveedores con la mejores soluciones multiaplaience en redes MPLS.

Para esto se tienen las siguientes series de router que según las características que quiera ofrecer la ISP serán las ajustables a su red:

- Serie 7000: es un sistema altamente escalable y versátil, que ofrece servicios Capa 2 y Capa 3 de alto alcance para agregación en el edge de una red de área amplia (WAN), agregación en el Ethernet de área metropolitana, Centros Internet de Datos y aplicaciones finales de clase empresarial. Además del nuevo módulo OC-48c/STM-16 POS (Packer over SONNET)/DTP (Dynamic Packet Transport) de Servicios Ópticos

(OMS) con dos puertos, para aplicaciones Metro IP, existe también un módulo canalizado OC-12/STM-4 OSM de un puerto y el nuevo OC-48/STM-16 OSM de un puerto, que ofrecen ahorros en costos en el capital y la operación a través del aprovisionamiento de eficiencia y densidad de puertos con circuitos mejorados. Los proveedores de servicio estarán en capacidad de implementar distintos paquetes de servicios de nueva generación con efectividad en sus costos. Las empresas podrán introducir una avanzada Calidad de Servicio (QoS), alta disponibilidad y los servicios de seguridad necesarios para dar soporte a aplicaciones de red de misión crítica para incrementar la productividad de los negocios.

- Serie 10000: posee Dynamic Bandwith Selection (DBS), que permite a los usuarios finales, de manera independiente, cargar sus conexiones de banda ancha instantáneamente, incrementando la demanda de aplicaciones de alta banda ancha como video en demanda (VoD). Otra presentación ofrecida en el portafolio de Cisco es Service Selection Gateway (SSG), que permite a los carriers entregar portales a la medida a los usuarios finales, y así, entregar una experiencia en línea más rica y más personalizada, a la vez que se promueve el acceso a los servicios, tales como películas o juegos. Y en respuesta a la necesidad creciente de seguridad de red, Cisco entrega capacidades Per User Network-based Firewall, que le dan a las familias o a los clientes finales empresariales la habilidad de seleccionar fácilmente niveles diferentes de protección de firewalls para miembros individuales de la familia o empleados.

- Serie 12000: servicios tales como virtualización segura, operatividad continua y escalabilidad de multiservicio, la serie 12000 de Cisco ofrece soluciones de routing inteligentes que varían desde 2.5 gigabits por segundo (gbps) hasta *n* X 10 gbps por ranura. Con su exclusivo diseño

ServiceFlex y su Arquitectura de Separación de Servicios, la serie XR 12000 de Cisco permite a las operadoras de telecomunicaciones aislar los servicios públicos de los privados a través de una virtualización segura de un router en dominios de enrutamiento físicos y lógicos. La operatividad continua del sistema se basa en las capacidades de auto recuperación y auto defensa del software IOS XR, que están diseñadas para estar siempre activas y ser escalables para añadir nuevos servicios o características. Con inteligencia de procesamiento distribuida y una gran calidad de servicio y mecanismos de multiemisión, lo cual permite a los proveedores escalar de puntos vinculados a servicios como FR/ATM, L2/L3 VPN y de puntos vinculados a clientes como colas y listas de control de acceso, al tiempo que se escala el rendimiento. [29]

Fuente: [Autor]

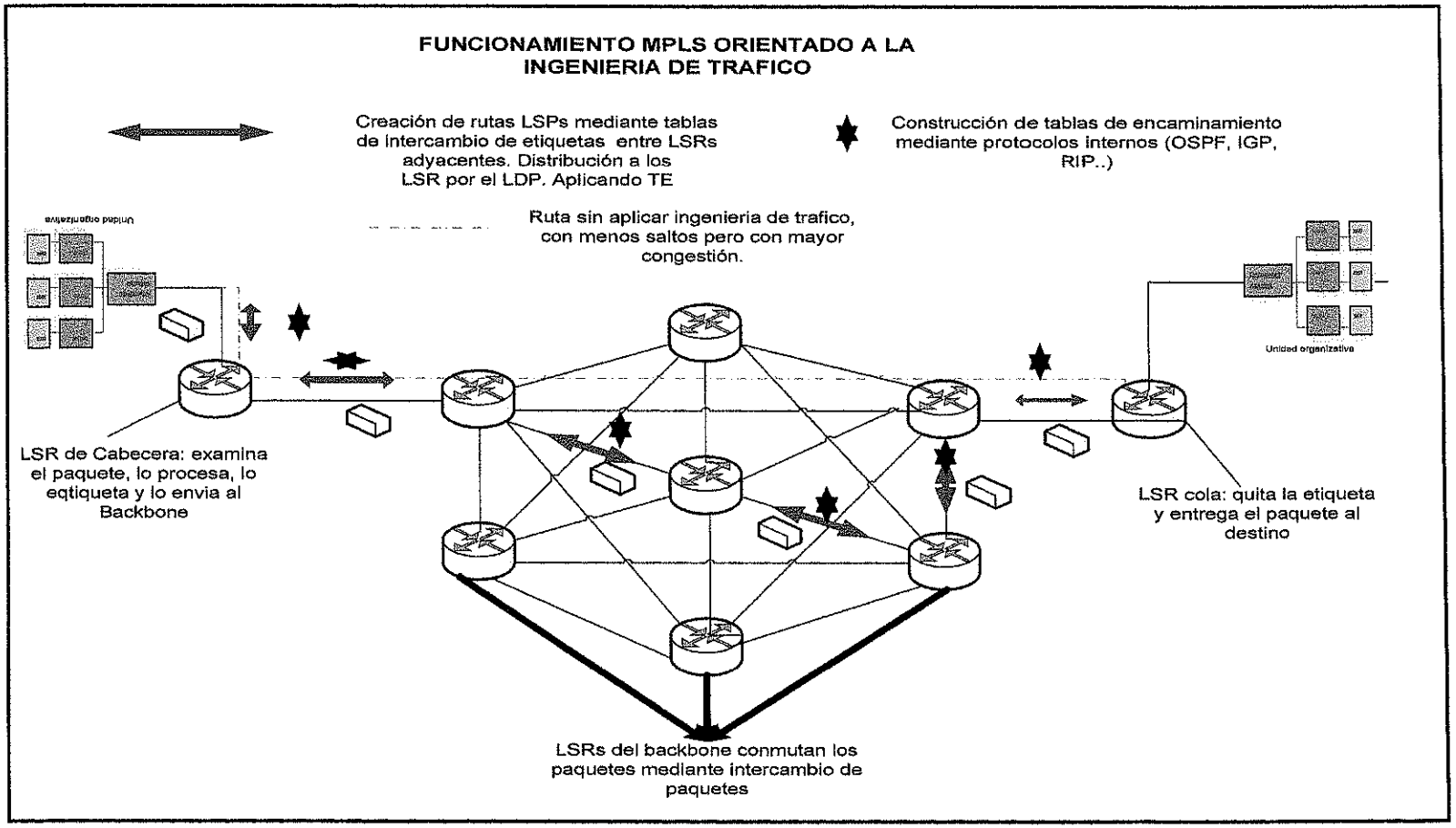

Figura 22. Backbone MPLS orientado a la Ingeniería de Trafico

4.3.4 VENTAJAS DE LA RED MPLS

- Flexibilidad frente al usuario ya que permite según sus necesidades poder adaptarlo en la red.
- Escalabilidad para manejar el crecimiento continuo en la red, sin llegar a una saturación y así lograr adaptarse a las circunstancias cambiantes en la red sin afectar el servicio.
- Accesibilidad con la que puede ser usado o accedido en general por el propio administrador de la red o el mismo usuario.
- Eficiencia con respecto a la capacidad que tiene para producir un máximo de resultados con los recursos necesarios, ofreciendo una alta calidad de servicio.
- Calidad de Servicio a los clientes en cuanto a la transmisión de datos garantizando un buen servicio.
- Administración en cuanto a que se puede controlar el tráfico que pasa por la red.
- Fácil Migración a la red IP ya que no necesita cambiar infraestructura solo agregar.
- Seguridad ya que la red IP existente maneja protocolos propios del fabricante los cuales serán aplicados a la red MPLS el cual garantiza una alta confiabilidad al acceso.
- Convergencia ya que tiende a ser la red mas segura, fiable y utilizada para lograr ofrecer un servicio con calidad.
- Control sobre la red
- Rapidez en el transporte de datos ya que se descongestiona la red al crear rutas explicitas que vienen del TE.
- Funciona sobre cualquier tecnología de transporte.
- Permite el crecimiento constante de Internet.
- Es compatible en cuanto a operación, administración y mantenimiento de las redes IP.
- Se tiene un mejor aprovechamiento de la red existente.

4.4 ANÁLISIS FINANCIERO

CORE IP			CORE MPLS		
EQUIPO	**CANTIDAD**	**PRECIO**	**EQUIPO**	**CANTIDAD**	**PRECIO**
Router CISCO 3640	1	1424,05	Router CISCO 3640	1	1424,05
Switch CISCO 2950	1	1295	Switch CISCO 2950	1	1295
KYPUS	1	1800	KYPUS	1	1800
Router CISCO 2800	1	2065,95	Router CISCO 2800	1	2065,95
Router CISCO 2611	1	2929,95	Router CISCO 2611	1	2929,95
BCU	1	1500	BCU	1	1500
Nodos	1	1500	Nodos	1	1500
CPE	1	800	CPE	1	800
			Router Serie 7000	1	3795
			Router Serie 10000	1	5975,63
			Router Serie 12000	1	7749
Costos de Ingeniería		1000	Costos de Ingeniería		2000
TOTAL		14314,95	**TOTAL**		32834,58

Según el análisis financiero se puede observar que según la calidad de servicio que quiera ofrecer el ISP varía el costo en la infraestructura. Además el costo de Ingeniería es más alto debido a que el análisis es mayor. La infraestructura manejada en el Core IP es la misma utilizada en el Core MPLS añadiendo sus equipos. Con respecto al análisis Costo-Beneficio es evidente que al tener un Core MPLS el costo aumenta pero el beneficio es mayor en cuanto a rentabilidad y servicio garantizado, ya que los clientes empresariales acrecentara a la hora de la implementación y según el mercado atacado, la inversión será amortiguada en muy poco tiempo y el aumento de ingresos para la empresa va a ser mayor después de esto garantizando un sostenimiento sin ninguna inversión.

Para concluir el proyecto es viable económica y técnicamente ya que el análisis Costo-Beneficio que se aprecia es muy alto. La recuperación de la inversión seria a corto plazo y el aumento de ingresos se vería reflejado inmediatamente.

APORTES Y CONCLUSIONES

- La red MPLS provee un servicio sencillo, una nueva conexión afecta a un solo Router para la comunicación entre el backbone y el usuario.
- La Ingeniería de tráfico permite mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.
- La red MPLS 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.
- Los proveedores de servicio tienen ante sí el enorme reto de gestionar redes cada vez más complejas y extensas, con una mayor gama de servicios y con creciente demanda de ancho de banda, calidad y garantías.
- MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel (o conmutación IP). La idea básica de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles 3 y 2, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura.
- MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino). Además de poder hacer ingeniería de tráfico IP, MPLS permite mantener clases de servicio 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.

- La propuesta de este diseño para una ISP en Tunja basada en MPLS con tráfico de ingeniería es viable económica y técnicamente debido a que ofrece calidad de servicio y seguridad para los usuarios, rendimiento en la red y rentabilidad económica para la empresa.
- El análisis que se realizo hacia la red MPLS fue basado en el estudio de la ISP en Tunja, donde inicialmente se observaron desventajas en el desempeño de la red como congestión en la red e interoperabilidad con otras tecnologías las cuales fueron cubiertas con esta propuesta de diseño por medio de la Ingeniería de Trafico se crean rutas alternas en caso de presentarse congestiones en la red.

ANEXO 1

CONFIGURACIÓN ROUTER

Para que un router pueda trabajar en un domino MPLS se deben tener en cuenta los siguientes comandos:

- **CONFIGURACION DE UNA INTERFAZ LOOPBACK**

Esta Interfaz nos permite identificar el router. Se configura de la siguiente manera:

Usuario# configure Terminal
Usuario(config)# interface loopback <numero de la interfaz>
Usuario(config-if)# ip address <dirección IP><mascara>

- **CONFIGURACION DE OSPF:**

En el backbone MPLS se habrá de configurar OSPF como protocolo de routing
dinámico. OSPF es un protocolo de routing interno (IGP) del tipo estado de enlace. Los equipos anuncian toda la información al arrancar el protocolo. Se enviarán entre sí paquetes cuando se detectan fallos en algún enlace.

Por lo tanto, todos los routers actualizan la base de datos topológica, se copian los paquetes e inundan a los vecinos. Por tanto, sólo se van enviando las nuevas actualizaciones de rutas.

Entonces, se tiene el siguiente comando que comprueba las cercanías OSPF:

show ip ospf neighbors

El comando:

show ip route

Permite ver la tabla de rutas del router donde se ejecuta el comando y si el router aprende las rutas por OSPF.

Para comprobar el estado de OSPF por interfaz se utiliza el siguiente comando:

show ip ospf interface

- **CONFIGURACION DE MPLS**

Una vez establecidos los protocolos de routing se configura las funcionalidades
MPLS en los routers. Para esto se comienza por el protocolo de distribución de
etiquetas en las distintas interfaces.

La configuración de MPLS requiere los siguientes pasos:

- Configurar el CEF (Cisco Express Forwarding) en todos los routers con funcionalidad "PE" y "P". CEF es el conjunto de funcionalidades que reúnen los equipos para poder trabajar en un entorno MPLS.

Los comandos que hay que ejecutar para activar CEF en un router que soporte estas funcionalidades son:

Usuario# configure terminal
usuario(config)# ip cef

Para comprobar si se ha activado CEF se utiliza el siguiente comando:

show ip cef summary

- Activación del protocolo de distribución de etiquetas LDP:

Hay que realizar la siguiente configuración en cada interfaz que vaya a hablar MPLS:

usuario (config)# interface <nombre de la interfaz>
usuario (config-if # mpls ip
usuario (config-if)# mpls label protocol ldp

Para realizar la verificación del funcionamiento de MPLS, se utilizan los siguientes comandos:

- show mpls interfaces

Muestra las interfaces en las que está funcionando MPLS-LDP.

- show mpls ldp parameters

Muestra los parámetros que está utilizando el protocolo en el equipo donde se ejecuta el comando.

- show mpls ldp neighbor

Muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando.

- show mpls ldp binding

Muestra la tabla de etiquetas que está utilizando el router donde se ejecuta el comando.

- show mpls Forwarding-table

Muestra la tabla de Forwarding del router donde se ejecuta el comando.[29]

BIBLIOGRAFÍA

[1] ANDERSSON L. et al., "LDP Specification", Internet Draft, <draft-ietf-mpls-ldp-05.txt>, junio 1999

[2] AWDUCHE D.O. et al., "Requirements for Traffic Engineering Over MPLS", Internet Draft, <draft-ietf-mpls-traffic-eng-01.txt>, junio 1999

[3] CALLON R. et al., "A Framework for Multiprotocol Label Switching", Internet Draft, <draft-ietf-mpls-framework-04.txt>, Julio 1999

[4] ROSEN E.C., VISWANATHAN A., CALLON R., "Multiprotocol Label Switching Architecture", Internet Draft, <draft-ietf-mpls-arch-06.txt>, agosto 1999

[5] SEMERIA C., "Multiprotocol Label Switching: Enhancing Routing in the New Public Network", Juniper Networks Inc., White Paper, http://www.juniper.net/techcenter/techpapers/mpls/mpls.html, marzo 1999

[6] SEMERIA C., "Traffic Engineering for the New Public Network", Juniper Networks Inc., White Paper, enero 1999, http://www.juniper.net/techcenter/techpapers//TE_NPN.html

[7] SEMERIA C., Stewart III J.W., "Optimizing Routing Software for Reliable Internet Growth", Juniper Networks Inc., White Paper, Julio 1999, http://www.juniper.net/techcenter/techpapers/optimizing-routing-sw.fm.html

[8] http: //www.wikipedia.org/modeloOSI

[9] Over MPLS". IETF RFC 2702, September 1999R.

[10] B. Jamoussi et al. "Multiprotocol Label Switching Arquitecture". IETF RFC 3031, January 2001.

[11] E. Rosen, A. Viswanathan, R. Callon. "Multiprotocol Label Switching Architecture". Internet Draft <draft-ietfmpls- arch-06.txt>, August 1999.

[12] S. Chen, K Nahrtedt. "An overview of quality of service Routing for Next Generation High Speed Networks: problems and solutions". IEEE Network, pp.64-71 November -December.1998

[13] K. Ahuja, T. L. Magnanti, and J. B. Orlin. "Network Flows: Theory, Algorithms and Applications". Prentice- Hall, Inc., Englewood Cliffs, NJ 1993. ISBN: 0-13- 617549-X

[14] P. Chardaire, A. Lisser. "Minimum Cost Multicommodity flow". November 1999. http://www.sys.uea.ac.uk/people/pc/hbook.pdf

[15] Löbel " Solving Large–Scale Real–World Minimum- Cost Flow Problems By a network Simplex Method"

[16] http://citeseer.nj.nec.com/lobel96solving.html

[17] http://www.gams.com

[18] http://www.rediris.es/rediris/boletin/53/enfoque1.html

[19] B.Jamoussi, et al. "Constraint – Based LSP setup Using LDP". Internet Draft <draft-ietf-mpls-cr-ldp-05.txt>. January 2002.

[20] T.Ott, T. Bogovic, T.Carpenter, "Algorithms for Flow Allocation for Multiprotocol label Switching". Telecordia, Technical memorandum,

[21] http:\\www.lightreading.com

[22] Designing Large-Scale IP Internetworks, http://www.cisco.com

[23] ISP Network Structure, http://www.cisco.com

[24] Traffic Engineering for the new public network, http://www.juniper.com

[25] Migration Strategies for IP Service Growth : Cell-Switched MPLS or IP-routed MPLS,

[26] www.juniper.net/solutions/literature/white_papers/200048.pdf

[27] Positioning and Developing a Migration Strategy to Offer Advanced IP Services Based on MPLS, http://www.cisco.com

[28] ISP Policy Implementation Case Study, http://www.cisco.com

[29] http://www.cisco.com/en/product/hw/routersmpls/index

[30] www.iaik.tugraz.at/teaching/03_advanced%20computer%20networks/ss2005/vo2/DiffServ%20IntServ%20MPLS.pdf

[31] www.ciscopress.com/articles/article.asp?p=426640

[32] www.opalsoft.net/qos/MPLS

[33] www.bt.es/perspectives/ip.html

[34] www.riverstonenet.com/support/mpls/encoding_mpls_labels.htm

[35] www.idg.es/pcworldtech/mostrarArticulo.asp?id=293659430&seccion=comunicaciones

GLOSARIO

- **Apple Macintosh:** es el nombre de una serie de ordenadores fabricados y comercializados por Apple Computer desde 1984.
- **AppleTalk:** Es el protocolo de comunicación para ordenadores Apple Macintosh y viene incluido en su sistema operativo, de tal forma que el usuario no necesita configurarlo.
- **Arpanet:** fue creada por encargo del Departamento de Defensa de los Estados Unidos como medio de comunicación para los diferentes organismos del país. El primer nodo se creó en la Universidad de California y fue la espina dorsal de Internet hasta 1990, tras finalizar la transición al protocolo TCP/IP en 1983.
- **Backbone:** se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos entre países, continentes y océanos del mundo.
- **Best Effort:** Protocolo de máximo esfuerzo por que hace todo lo posible para transmitir hacia la aplicación pero no puede garantizar que la aplicación lo reciba.
- **BGP:** El BGP o Border Gateway Protocol es un protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet. Actualmente la totalidad de los ISP intercambian sus tablas de rutas a través del protocolo BGP.
- **CPE:** El CPE es un equipo de telecomunicaciones usado en interiores como en exteriores para originar, encaminar o terminar una comunicación.

- **DECnet:** Es un protocolo de red propio de Digital Equipement Corporation (DEC), que se utiliza para las conexiones en red de los ordenadores y equipos de esta marca y sus compatibles.
- **Delay:** Tiempo que tarda un paquete de red llegar a destino.
- **DiffServ:** Arquitectura de la ingeniería de tráfico que busca agregar trafico en conjuntos grandes y diferenciar servicios de manera escalable y gestionable.
- **DLCI:** Data Link Connection Identifier (DLCI) es el identificador de canal del circuito establecido en Frame Relay. Este identificador se aloja en la trama e indica el camino a seguir por los datos, es decir, el circuito virtual establecido.
- **DSCP:** Punto de código de servicios diferenciados, es un campo de un paquete IP que permite la asignación de distintos niveles de servicio de tráfico de red.
- **Ethernet:** es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos.
- **DWDM:** Multiplexación por división en longitudes de onda densas. es una técnica de transmisión de señales a través de fibra óptica.
- **Ethertalk**. Es la versión para Ethernet y otra variante de appletalk. Esto aumenta la velocidad y facilita aplicaciones como por ejemplo la transferencia de archivos.
- **FEC:** es un tipo de mecanismo de corrección de errores que permite su corrección en el receptor sin retransmisión de la información original.
- **FTP:** es uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Ficheros) y es el ideal para transferir grandes bloques de datos por la red. Su comportamiento está definido por la recomendación RFC 959
- **Gopher:** Servicio de Internet consistente en el acceso a la información a través de menús. La información se organiza de

forma arborescente: sólo los nudos contienen menús de acceso a otros menús o a hojas, mientras que las hojas contienen *simplemente información textual.*

- **HTTP:** El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW).
- **ICMP:** Es el subprotocolo de diagnóstico y notificación de errores del protocolo de Internet (IP).
- **IETF:** Grupo de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en EE.UU. en 1986.
- **IGP:** Interior Gateway Protocol (IGP, protocolo de pasarela interno) hace referencia a los protocolos usados dentro de un sistema autónomo. Los protocolos IGP más utilizados son RIP, OSPF y IS-IS. Interior Gateway Protocol (IGP, protocolo de pasarela interno) IGP es un protocolo que genera tablas de enrutamiento dentro de un sistema autónomo.
- **Inetd**: Inetd pertenece a un grupo de programas llamados TSR (Terminate and stay resident). Dichos programas siempre están en ejecución, a la espera de que se produzca algún suceso determinado en el sistema. Cuando dicho suceso ocurre, el TSR lleva a cabo la tarea para la que está programado. su finalidad es estar a la espera de que se produzca alguna solicitud de conexión del exterior. Cuando esto ocurre, inetd evalúa dicha solicitud determinando que servicio está solicitando la máquina remota y le pasa el control a dicho servicio.
- **IntServ:** Arquitectura de la ingeniería de tráfico que procura la reserve de recursos de punta a punta para flujos individuales.

- **IP**: Se encarga de repartir los paquetes de información enviados entre el ordenador local y los ordenadores remotos. Esto lo hace etiquetando los paquetes con una serie de información, entre la que cabe destacar las direcciones IP de los dos ordenadores. Basándose en esta información, IP garantiza que los datos se encaminarán al destino correcto. Los paquetes recorrerán la red hasta su destino por el camino más corto posible gracias a unos dispositivos denominados encaminadores o routers.
- **IPSEC:** (la abreviatura de Internet Protocol security) es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y, de esta manera, asegurar las comunicaciones a través de dicho protocolo.
- **IPv6:** es la versión 6 del Protocolo de Internet (Internet Protocol), un estándar del nivel de red encargado de dirigir y encaminar los paquetes a través de una red.
- **IPX/SPX:** es un protocolo de Novell que interconecta redes que usan clientes y servidores Novell Netware. Es un protocolo orientado a paquetes y no orientado a conexión lo cual significa que no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino.
- **ISP:** Proveedor de servicio de Internet dedicada a conectar a Internet a usuarios o distintas redes.
- **Jitter:** Es el retardo que tiene la señal en llegar a su destino.
- **LAT:** (Local Area Transport, transporte de área local), se utiliza para conectar periféricos por medio de la red y tiene una serie de características de gran utilidad como la asignación de nombres de servicio a periféricos o los servicios dedicados.
- **LocalTalk**: Es una variante de appletalk y la comunicación se realiza a través de los puertos serie de las estaciones. La velocidad de transmisión es pequeña pero sirve por ejemplo para compartir impresoras.

- ***LSP (Label Switched Paths):*** es una ruta sobre una red MPLS, establecida por un protocolo de señalización como LDP, RSVP o CR-LDP.
- **LSR:** es un dispositivo que implementa la conmutación de etiquetas.
- **Modelo OSI:** El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconection) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial. (Para la descripción detallada del modelo OSI con todos sus niveles se puede remitir al siguiente enlace http://es.wikipedia.org/wiki/Modelo_osi).
- **MPLS:** es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI.
- **Multicast:** Es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.
- **NetBEUI:** NetBIOS Extended User Interface o Interfaz de Usuario para NetBIOS es una versión mejorada de NetBIOS que sí permite el formato o arreglo de la información en una transmisión de datos. También desarrollado por IBM y adoptado después por Microsoft, es actualmente el protocolo predominante en las redes Windows NT, LAN Manager y Windows para Trabajo en Grupo.
- **NetBIOS:** NetBIOS (Network Basic Input/Output System) es un programa que permite que se comuniquen aplicaciones en diferentes ordenadores dentro de una LAN.

- **NSPs:** Proveedor de servicio de red, es una organización que vende ancho de banda o acceso directo proporcionado por un backbone a Internet y generalmente el acceso a sus puntos de acceso a la red.
- **Novell Netware:** es un sistema operativo de red producido por la empresa Novell. NetWare es una de las plataformas de servicio más fiable para ofrecer acceso seguro y continuado a la red y los recursos de información, sobre todo en cuanto a servidores de archivos.
- **OSPF:** Open Shortest Path First (frecuentemente abreviado OSPF) es un protocolo de encaminamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible.
- **PDU:** Protocolo de unidad de datos. Se utiliza para el intercambio entre unidades pares, dentro una capa del modelo OSI.
- **PIM:** Pertenece a los protocolos de encaminamiento multicast, que puede proveer la distribución de datos de uno a uno o de uno a muchos sobre internet.
- **Puertos**: La mayoría de las aplicaciones TCP/IP tienen una filosofía de cliente-servidor. Cuando se recibe una solicitud de conexión, inetd inicia un programa servidor que se encargará de comunicarse con la máquina cliente. Para facilitar este proceso, a cada aplicación se le asigna una única dirección. Dicha dirección se llama puerto. Cuando se produce una solicitud de conexión a dicho puerto, se ejecutará la aplicación correspondiente.
- **PVCs:** Son circuitos virtuales que proporcionan un ancho de banda garantizado que se reserve a través de la red y soporta aplicaciones de datos de altas prestaciones.
- **RFC:** Es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet, que se explica con todo

detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

- **RIP** (Protocolo de Información de Ruteo) Es un protocolo de pasarela interior utilizado por los routers, aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.
- **RSVP:** Es un protocolo de reservación de recursos de control de la red que permite que los programas que van a trabajar en Internet puedan obtener la calidad de servicio que sus flujos de datos puedan requerir.
- **Sistemas Autónomos (As):** Es un conjunto de redes y dispositivos que se encuentran administrados por una sola entidad que cuentan con una política común de definición de trayectorias para Internet.

- **SLA (Service Level Agreements):** Acuerdo de Nivel de Servicio y a veces se abrevia como ANS. Un SLA es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a prestar el mismo bajo unas determinadas condiciones y con unas prestaciones mínimas.
- **Streaming:** es un término que se refiere a ver u oír un archivo directamente en una página web sin necesidad de bajárselo antes al ordenador o computador.
- **Switch:** Es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.
- **TCP**: Controla la división de la información en unidades individuales de datos (llamadas paquetes) para que estos paquetes sean encaminados de la forma más eficiente hacia su punto de

destino. En dicho punto, TCP se encargará de reensamblar dichos paquetes para reconstruir el fichero o mensaje que se envió.

- **Telnet:** es el nombre de un protocolo (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella.
- **Throughput:** Se llama así al volumen de trabajo o de información que fluye a través de un sistema.
- **Token Ring:** Arquitectura de red desarrollada por IBM en los años 70's con topología lógica en anillo y técnica de acceso de paso de testigo.
- **Tokentalk**: Es la versión de Appletalk para redes Token Ring.
- **UDP:** ser Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.
- **Unicast:** Es un envío de información desde un único emisor a un único receptor.
- **X.25:** Es un protocolo utilizado principalmente en WAN y, sobre todo, en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, que los bloques de datos contienen información del origen y destino de los mismos para que la red los pueda entregar correctamente aunque cada uno circule por un camino diferente.