CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO (MPLS)

OSCAR ANDRÉS CARREÑO OYUELA
CESAR AUGUSTO ALARCON PRADA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DEINGENIERÍAS FISICOMECANICAS
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO (MPLS)

OSCAR ANDRÉS CARREÑO OYUELA
CESAR AUGUSTO ALARCON PRADA

Monografía presentada como requisito para optar al título de Especialista en Telecomunicaciones

DIRECTOR:
MAG. SANDRA CRISTINA SANGUINO GALVIS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DEINGENIERÍAS FISICOMECANICAS
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

AGRADECIMIENTOS

Los autores expresan su agradecimiento…

A nuestros padres por su entrega y apoyo incondicional durante nuestra formación como Especialistas en Telecomunicaciones.

A la Universidad Industrial de Santander por su formación a lo largo de los años.

A la directora de este trabajo Mag. Sandra Cristina Sanguino Galvis. Por sus valiosas orientaciones, enseñanza y colaboración.

A todos los familiares y amigos por el apoyo que nos brindaron durante el proceso de aprendizaje.

A todos los que de una u otra forma hicieron posible el desarrollo de este trabajo.

A mis padres Luis y Lilia

Quienes depositaron toda su confianza en mí

Y me dieron lo que soy.

A mi esposa Lina y a mi hijo Juan Diego

Por su apoyo, comprensión y amor

Durante estos años compartidos.

Este trabajo es tan mío como suyo y agradezco

al todo poderoso por permitirme bridarles esa satisfacción.

César Augusto

A mis padres, mi hermano y abuelos, los cuales me han dado siempre su apoyo incondicional, en los buenos y malos tiempos.

Gracias por la confianza depositada en mí la cual se ve reflejada en cada logro alcanzado.

Oscar Andrés

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

AAA (Authentication, Authorization, Acounting)-Son los tres pasos fundamentales en la seguridad de datos en informática: Autenticación, Autorización y Auditoria.

Aris – Protocolo de intercambio de etiquetas, propiedad de IBM.

ATM – Modo de Transferencia Asíncrona o Asynchronous Transfer Mode. Es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Bandwidth – (Ancho de Banda) Rango de frecuencias, expresadas en bits por segundo, disponibles para un medio de transmisión.

B-ISDN - Red Digital de Servicios Integrados de Banda Ancha.

Bps – Bytes por Segundo.

BGP – (Border Gateway Protocol) es un protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet, en la actualidad la mayoría de los ISPs intercambian sus tablas de rutas con este protocolo. Bysinc – (Comunicación Binaria Síncrona) Protocolo de IBM. Utiliza un conjunto definido de caracteres de control para transmisiones sincronizadas de datos codificados en binario entre estaciones de un sistema de comunicaciones.

CE router – router frontera del cliente que solicita el servicio VPN con MPLS.

CEF – (Cisco Express Forwarding) Es una técnica propietaria de Cisco para realizar switcheo a altas velocidades en WANs con garantía de velocidad y sin retraso.

CHAP (Challenge Handshake Authenticacition Protocol) – Es un método de autenticación remota o inalámbrica. Diversos proveedores de servidores y clientes de acceso a la red emplean CHAP.

Conectionless - Modelo de comunicaciones en el que las direcciones origen y destino están incluidas en cada paquete para que no sea necesaria la conexión directa entre dos nodos. Confiabilidad (Reliability) – Probabilidad y/o trabajo efectivo de la red.

CoS (Class of Service) – Es un algoritmo que compara los campos en los paquetes o las etiquetas CoS para clasificarlos y asignarlos a una cola, dependiendo de su prioridad.

CR-LDP – Protocolo de distribución de etiquetas que contiene extensiones del LDP para extender sus capacidades. Puede trabajar con explicit route constraints, QoS constraints, entre otras.

DiffServ – Se utiliza para establecer deferentes tipos de servicios a diferentes usuarios.

DOD - Downstream on demand

DOU - Downstream unsoliciteded

DSCP – (DiffServ Codepoint) Sirve para identificar la clase de tráfico.

ENCABEZADO SHIM – encabezado adicional agregado a los paquetes. se coloca entre los encabezados de capa de red y de capa de enlace del modelo OSI

Endpoint – Punto de salida o entrada de un domino o red.

ESP (Encapsulated Security Payload) – Es un encabezado de red diseñado para proveer los servicios de seguridad de IPv4 e IPv6

Ethernet - Tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI.
Explicit route – Se refiere al protocolo de selección de rutas que pasa por alto la ruta default y se enfoca en la ruta mas efectiva para el salto.

FEC – (Forwarding Equivalence Class) Nombre que se le da al tráfico que se reenvía bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

Frame Relay – **(*Frame-mode Bearer Service*)** Es una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de frames de datos, perfecto para la transmisión de grandes cantidades de datos.

Gigapops -(gigabit Point of Presence) Es un punto de acceso a Internet que admite, al menos, una conexión de un gigabit por segundo. Son los encargados de rutear el tráfico en redes de alta velocidad, además puede dar preferencia al tráfico y debe suministrar la seguridad requerida por algunas aplicaciones.

GRE – (Generic Routing Encapsulation) – Protocolo de conexión virtual mediante túneles.

HDLC – (High-Level Data Link Control) es un protocolo de comunicaciones de datos punto a punto entre dos elementos.

Hop-by-hop – método de selección de ruta que contiene los datos que deben ser examinados por cada nodo a través de la ruta de envió de un paquete.

Hop count – Numero de saltos entre el origen y el destino.

Hop limit – Limite de saltos entre el origen y el destino.

IANA – (Assigned Number Authority). La Agencia de Asignación de Números Internet era el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos.

ICMP – Es usado principalmente por los sistemas operativos de las computadoras en una red para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible ó que un router ó host no puede ser localizado.

IETF (Internet Engineering Task Force) – Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la Ingeniería de Internet. Se divide en áreas como: transporte, encaminamiento, seguridad, etc. Fue creada en USA en 1986.

IGP – (Interior Protocol Gateway) Hace referencia a los protocolos usados dentro de un sistema autónomo. Los protocolos IGP más utilizados son RIP y OSPF.

IKE (Internet Key Exchange) – Se utiliza para establecer una SA en el protocolo IPSec. Su utilización es obligatoria en el estándar IPv6 Ingeniería de tráfico – Utiliza datos estadísticos como la teoría de colas para predecir el comportamiento de las redes de telecomunicaciones.

IOS – (Internetwork Operating System) Sistema operativo creado por Cisco Systems para programar y mantener equipos de interconexión de redes informáticas como switches y routers.

IP – (Internet Protocol) Es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados (switched).

IPSec – (Internet Protocol Security) es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado y, de esta manera, asegurar las comunicaciones a través de dicho protocolo.

IPv4 – IPv4 usa direcciones de 32 bits, limitándola a 232 = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales. IPv6 – Estándar destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet.

IS-IS (Intermediate System to Intermediate System) - Es un protocolo utilizado por los enrutadores para determinar el mejor camino para reenviar paquetes a lo largo de la red. Compite directamente con OSPF.

ISO (International Standarization Organization) – Es una organización internacional no gubernamental compuesta por representantes de los Organismos de Normalización (ONs) nacionales, que produce Normas Internacionales industriales y comerciales.

IPX – (Internetwork Packet Exchange) Protocolo de nivel del red que se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo.

Jitter – El “jitter” es la variación aleatoria de la latencia, reduce las capacidades de la red y provoca que los paquetes lleguen en un orden distinto al que fueron emitidos.

L2TP (Layer 2 Tunneling Protocol) – Fue diseñado por el IETF para corregir las deficiencias de PPTP y L2F y establecerse como un estándar aprobado por el IETF.

L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado.

L2F (Layer 2 Forwarding) – Fue creado en las primeras etapas de desarrollo de las VPN y esta diseñado para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas. El establecimiento de túneles no de depende de IP por lo que soporta protocolos como Frame Relay o ATM.

Latencia (Latency) – Es el lapso necesario para que un paquete de información viaje desde la fuente hasta su destino.

LDP – (Label Distribution Protocol) Protocolo de distribución de etiquetas, utilizado principalmente en MPLS, la extensión CR-MPLS permite el uso de ingeniería de tráfico.

LEAP (Lightweight Extensible Authentication Protocol) – Es un protocolo desarrollado por CISCO para la autenticación den redes inalámbricas. Funciona con llaves WEP y autenticación entre el servidor inalámbrico y el servidor RADUIS.

LER – (Label Edge Router) Elemento que inicia o termina el túnel (pone y quita encabezados). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router.

LIB: (label información base) o tabla de conectividad

LIFO – (Last In First Out) Es un algoritmo utilizado en teoría de colas. Funciona como una pila de platos, en la que los platos van poniéndose uno sobre el otro, y si se quiere sacar uno (pop), se saca primero el que se puso último.

Looping – Paquete ciclado a lo largo de un segmento de la red.

LSP – (Label Switched Path) Nombre genérico de un camino MPLS (para cierto FEC), es decir, del túnel MPLS establecido entre los extremos.

LSR – (Label Switched Router) Elemento que conmuta etiquetas.

Modelo OSI – Modelo definido por la Organización Internacional de Normalización, es uno de los más importantes y el más utilizado. Se divide en 7 capas sucesivas: Física, Enlace de Datos, Red, Transporte, Sesión, Presentación y Aplicación.

MPLS – (Multiprotocol Label Switching) Es un mecanismo de transporte de datos estándar creado por la IETF. 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.

MTU (Maximum Transfer Unit) - Es un término informático que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones. El tamaño común es de 1500 bytes para Ethernet, para ATM es de 8190 bytes.

Multicast – Es el envío de 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.

NAT – (Network Address Translation) Estandar creado por la IETF el cual utiliza una o más direcciones IP para conectar varios computadores a otra red, por lo general Internet.

NetFlow – Es una de las características del software IOS de Cisco, es también el nombre de un protocolo abierto (Propietario de Cisco) que recupera información de tráfico IP.

Next hop – Se refiere al siguiente salto, el router que sigue en el LSP.

OSPF – (Open Shortest Path First) Propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red con información sobre sistemas locales y vecinos, esto con el fin de conocer la ruta mas corta.

P2P – (Peer-to-peer) una red informática que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan a la vez como clientes y como servidores de los demás nodos de la red.

P router – Router interno del proveedor del servicio VPN con MPLS

Payload – Carga de transmisión.

PDU – Es la unidad de datos de protocolo de la capa de red. Las PDU tienen encapsuladas en su área de datos otras PDU.

PE router – Router frontera del proveedor del servicio VPN con MPLS.

PHB – (Pero Hop Behavior) Es la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión.

PING -Utilidad que comprueba el estado de la conexión con uno o varios equipos remotos. Lo hace por medio de paquetes de solicitud y respuesta de eco para determinar si un sistema IP específico es accesible en una red.

Pop – Saca paquetes de la pila o stack.

PPP (Point to Point Protocol) – El protocolo PPP permite establecer una comunicación a nivel de enlace entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un modem telefónico.

PPPoE (Point to Point Protocol over Ethernet) – Es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizado mayormente para proveer conexión de banda ancha mediante servicios de cable módem y xDSL. Este ofrece las ventajas del protocolo PPP como son la autenticación, encriptación y compresión.

PPTP (Point-to-Point Tunneling Protocol) – es un protocolo para implementar redes privadas virtuales desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum. Actualmente PPTP ya no se utiliza.

PREC (Precedence) – Es el antecesor IP del campo EXP en IP-MPLS, son 3 bytes que definen la clase de servicio.

Push – Introduce paquetes a la pila o stack. PVC – (Permanent Virtual Circuits) Conexión que reemplaza las líneas privadas por un sólo enlace a la red.

QoS – (Quality over Service) Es la capacidad de las tecnologías de conmutación de paquetes (tag-switching) de proveer todos los recursos necesarios a cada aplicación en un momento determinado dentro de la red.

RFC – (Request for Comments) Conjunto de notas técnicas y organizativas donde se describen los estándares de Internet, comenzado en 1969.

SNA – (System Network Arquitecture) Es una arquitectura de red diseñada y utilizada por IBM para la conectividad con sus hosts o mainframes. La integran grandes ordenadores y servidores muy robustos que soportan millones de transacciones. Comúnmente utilizada en bancos.

RC4 (Rivest Chipre 4) – Es un algoritmo de cifrado de flujo utilizado en protocolos SSL y WEP, fue diseñado por Ron Rivest en 1984.

RD – (Route Distinguisher) Es una clasficador de direcciones utilizado por MPLS para distinguir rutas VPN de diferentes clientes que se conectan al proveedor del servicio.

RSA -Es un sistema criptográfico desarrollado por : Ronald Rivest, Adi Shamir y Leonard Adleman. Todo usuario de dicho sistema hace pública una clave de cifrado y oculta una clave de descifrado.

RSVP – Protocolo que se encarga de reservar recursos para que estén disponibles cuando las aplicaciones lo necesiten.

RSVP-TE – Extensión al protocolo RSVP original para el manejo de rutas explicitas con o sin reserva de recursos.

SA (Security Association) – Describe un flujo unidireccional seguro de datos a través de dos puertas de enlace. Se utiliza en IPSec con IKE.

SLA - arreglo de nivel de servicio

Spoofing – en términos de seguridad informática hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

SSL (Security Sockets Layer) - Es un protocolo criptográfico que proporciona comunicaciones seguras en Internet. Proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía Streaming media – transmisión de datos multimedia: voz, video, etc.

TACACS (Terminal Access Controller Access Control System) – Es un protocolo de autenticación remota que se usa para comunicarse con un servidor de autenticación (Comúnmente UNIX). TACACS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red.

Tag Switching – Protocolo de intercambio de etiquetas, propiedad de CISCO.

TOS (Type of Service) – Son los 6 bytes en el encabezado IPv4 que determinan el DSCP.

TTL – (Time to Live) Indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen. Este valor va disminuyendo cada vez que un router recibe y reenvía el paquete. Cuando este valor llega a cero, el paquete deja de ser reenviado.

UDP (User Datagram Protocol) – Es un protocolo que opera en el nivel de transportare del modelo OSI que se basa en intercambio de datagramas. Permite enviar los datagramas sin establecer previamente una conexión ya que su encabezado contiene suficiente información de direccionamiento. Unicast – En el tráfico unicast la transmisión de información se dirige a un solo punto con una dirección que solamente puede ser reconocida por un sistema anfitrión.

VC (Virtual Circuit) – Conexiones virtuales que utiliza ATM para reemplazar las líneas privadas por un solo enlace de red, pueden ser permanentes o conmutadas (PVC, SVC).

VPLS (Virtual Private LAN Service) – Es un forma de proveer comunicación multipunto a multipunto basado en Ethernet para redes IP/MPLS. VPN (Virtual Private Network) – Red privada que utiliza túneles virtuales para conectarse entre nodos físicamente separados.

VPWS (Virtual Private Wired Service) – Es un circuito de enlace punto a punto que conecta dos enrutadores CE.

VRF (Virtual Routing and Forwarding) – Es una tecnología utilizada en redes de computadoras que permite la coexistencia de múltiples instancias las tablas de ruteo de un mismo router. Esta tecnología es utilizada comúnmente en MPLS VPNs de capa 3.

WAN – (Wide Area Network) Es una red muy extensa que abarca computadoras separadas físicamente. Opera en la capa física y de enlace del modelo de referencia.

WEP (Wired Equivalent Privacy) – Sistema de cifrado incluido en el estándar 802.11 como protocolo para redes inalámbricas. Permite el cifrado de la información que se transmite. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64bits, de 128bits o de 256 bits. Proporciona cifrado a nivel 2.

X.25 – Red de conmutación de paquetes basada en el protocolo HDLC. Establece mecanismos de direccionamiento entre usuarios, negociación de características de comunicación y técnicas de recuperación de errores.

RESUMEN

TITULO: Estado del arte de la conmutación de etiquetas multiprotocolo (MPLS)[*]

AUTORES: Oscar Andrés Carreño O, César Augusto Alarcón Prada[**]

PALABRAS CLAVES: MPLS, routers, etiquetado de tramas

DESCRIPCIÓN

El trabajo realizado hace referencia al análisis de la conmutación de etiquetas multiprotocolo (MPLS)[***] y su implementación en la empresa COPETRAN LTDA, utilizando datos reales tomados en sitio, bases teóricas y simuladores que permiten describir estas redes y plantear recomendaciones para la interconexión de las principales sedes remotas.

El término MPLS (Conmutación de etiquetas multiprotocolo) representa un conjunto de especificaciones definidas por el *IETF* (*Grupo de Trabajo de Ingeniería de Internet*) que le asigna a las tramas que circulan por la red una identificación que le indique a los routers la ruta que deben seguir los datos. Además, , MPLS sirve para la administración de la calidad de servicio al definir 5 *clases de servicios*, conocidos como *CoS (Clase de servicio)*.

MPLS es hoy día una solución clásica y estándar al transporte de información en las redes. Ha sido hasta hoy una solución aceptable para el envío de información, utilizando enrutamiento de paquetes con ciertas garantías de entrega.

A su vez, los avances en el hardware y una nueva visión a la hora de manejar las redes, están dando lugar al empleo creciente de las tecnologías de Conmutación, encabezadas por la tecnología ATM. Aportando velocidad, calidad de servicio y facilitando la gestión de los recursos en la red.

[*] Monografía

[**] Facultad de Ingenierías FísicoMecánicas. Escuela de Ingeniería Eléctrica, Electrónica y de Telecomunicaciones. Director: SANDRA CRISTINA SANGUINO GALVIS. Magíster en Administración de Tecnología de Información - ITESM (México).

[***] Multiprotocol Label Switching

ABSTRACT

TITLE: state of the art about Multiprotocol label switching (MPLS)[*]

AUTHORS: Oscar Andrés Carreño O, César Augusto Alarcón Prada[**]

KEY WORDS: mpls, routers, frame tagging

DESCRIPTION

The work refers to the multiprotocol label switching (MPLS)[***] and the implementation on COPETRAN LTDA enterprise, using the real data taken on the field. Theoretical data and simulator can we describe the network and give recommendations for the interconnection of the principals remotes venues.

The term MPLS (Multiprotocol Label Switching) represents a set of specifications defined by the IETF (Internet Engineering Task Force) assigned to the frames circulating the network identification to indicate to routers that the route should follow the data. Therefore, MPLS is used for quality management service defines 5 classes of service, known as CoS.

MPLS is now a standard classic solution to the transport and information networks. Has hitherto been an acceptable solution for sending information using packet routing with certain delivery guarantees.

In turn, advances in hardware and a new vision when managing networks is leading to increasing use of switching technologies, led by ATM technology. Providing speed, service quality and facilitating the management of network resources.

[*] Monograph

[**] Physical –mechanical Engineering Faculty. Electrical, Electronical and Telecommunications School. Advisor: SANDRA CRISTINA SANGUINO GALVIS. Master of Information Technology Management - ITESM (México).

[***] Multiprotocol Label Switching

1 INTRODUCCIÓN

Este trabajo examina los componentes básicos de la redes MPLS (Conmutación de etiquetas multiprotocolo), entendiendo y explorando el transporte de datos, funciones de equipos, y desarrollos que ayudan a hacer de esta tecnología, una tendencia en el mundo de las telecomunicaciones.

MPLS es una tecnología estable que ha madurado con el tiempo a través de nuevos desarrollos y nuevas características[1].. Actualmente MPLS es bueno según los indicadores obtenidos en las pruebas hechas en el laboratorio, pero su economía no. La economía es lenta, sin embargo, aproximadamente 70 proveedores en todo el mundo ya han adoptado a MPLS en algunos servidores. Con tantos proveedores mayoritarios, (incluyendo British Telecom and Quest) ya se vienen ofreciendo servicios MPLS al mercado de los proveedores de redes y las empresas de redes. Implementándose rápidamente MPLS en las empresas privadas y en las redes privadas virtuales o VPNs.

Tanto grandes como medianas empresas y redes privadas están examinando los beneficios de MPLS. El mayor y el que hace que esta tecnología sea exitosa es el ahorro que ésta promete a través de la convergencia y servicios adicionales. MPLS ofrece la habilidad para construir una red escalable que permite llevar en una red cualquier tipo de tráfico, empezando por trafico IP hasta Voz IP, posibilitando servicios de transmisión de datos, voz, transmisión de video en línea y por demanda, transmisión de video conferencia entre otros servicios.
MPLS puede consolidar el ATM, Frame Relay, Voz IP y redes IP dentro de una infraestructura, generando una gran ventaja de costo.

[1] http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

El protocolo de conmutación de etiquetas (*MPLS*) integra el ancho de banda, la latencia y la utilización de Capa 2 en la Capa3 del modelo de referencia OSI[1] para mejorar y simplificar el intercambio de paquetes. Es decir, es una técnica que utiliza la inteligencia del ruteo y el desempeño de los conmutadores para disminuir el tráfico de rutas, la congestión, las fallas de conexión y los cuellos de botella.

MPLS proviene de tecnologías ya existentes, como son "*Tag Switching*" de CISCO y "*ARIS*" de IBM. En 1997 fue creado el primer grupo de trabajo de MPLS por el Grupo de Trabajo en Ingeniería de Internet (*IETF*). Hoy en día es un tema de actualidad y se ha convertido en un estándar de calidad y desempeño completo que permite formar sistemas de redes muy robustos.

En este proyecto se pretende formar una base sólida que muestre las especificaciones y características de la tecnología MPLS, siendo un tema de actualidad y de gran futuro. Esto con el fin de proveer un pilar preliminar para cualquier análisis y/o implementación del protocolo en un futuro.

[1] OSI (open system interconnection) Modelo de interconexión de sistemas abiertos. Es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Analizar la conmutación de etiquetas multiprotocolo (MPLS) y su implementación en la empresa COPETRAN LTDA, utilizando datos reales tomados en sitio, bases teóricas y simuladores que permitan describir estas redes y plantear recomendaciones para la interconexión de las principales sedes remotas.

2.2 OBJETIVOS ESPECÍFICOS

1. Estudiar el comportamiento de la tecnología MPLS en los enlaces de datos de la empresa COPETRAN LTDA con el fin de observar los beneficios que esta tecnología genera en la red de la empresa.

2. Realizar un estudio sobre la comunicación multiprotocolo mediante etiquetas (MPLS), en bases de datos y medios alternos que puedan dar una base teórica con el fin de realizar un escrito de estudio en esta tecnología.

3. Describir las ventajas y desventajas que ofrece la comunicación multiprotocolo mediante etiquetas (MPLS) y analizar algunas soluciones de última milla, previas a la llegada de esta tecnología.

3 PLATEAMIENTO DEL PROBLEMA

La creciente demanda de utilización de Internet para aplicaciones en tiempo real tales como teleconferencias, aplicaciones en línea, telefonía, etc., necesita satisfacer requerimientos de retardo, probabilidad de pérdida de paquetes y ancho de banda. Existe también un gran interés en poder realizar servicios diferenciados, donde aquél que quiera una mayor calidad de servicio pueda contratar el servicio que desea y tener prioridad sobre aquel que no lo contrate.

En este marco surge una nueva tecnología, que está siendo estudiada y discutida: MPLS (Multiprotocol Label Switching). El término MPLS representa un conjunto de especificaciones definidas por el *IETF*[1] () que le asigna a las tramas que circulan por la red una identificación que le indique a los routers la ruta que deben seguir los datos. Además, MPLS sirve para la administración de la calidad de servicio.

Debido a la flexibilidad de esta tecnología para el control de la calidad de servicio, surge el interés de analizar las ventajas que ofrece una red de conmutación de etiquetas multiprotocolo (MPLS) para la COOPERATIVA SANTANDEREADA DE TRANSPORTADORES – COPETRAN LTDA que en la actualidad utiliza MPLS para interconectar las principales sedes remotas utilizando como proveedor de servicios principal a la empresa ETB[2]

[1] IETF: (Internet Engineering Task Force) – *Grupo de Trabajo de Ingeniería de Internet. Es una o*rganización internacional abierta de normalización.

[2] ETB (Empresa de Telecomunicaciones de Bogotá, antiguamente Empresa de Teléfonos de Bogotá) es una de las más grandes compañías de telecomunicaciones en Colombia

4 JUSTIFICACIÓN

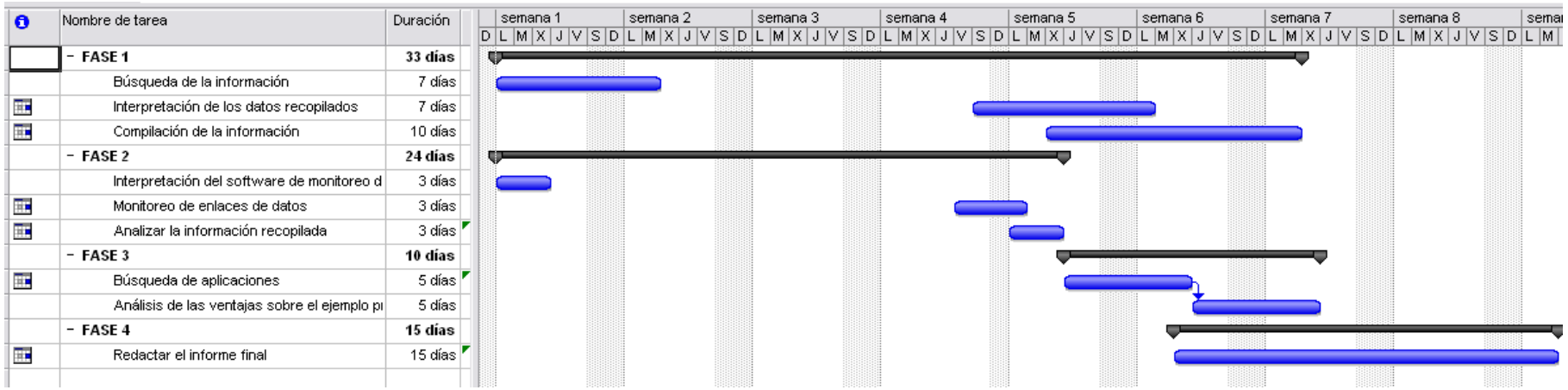
Como tecnología, MPLS está madurando más allá de sus raíces como un mecanismo de reenvío de utilidad para un avanzado y altamente funcional de tecnología que permite a los proveedores de servicios activar nuevas fuentes de ingresos y nuevas funciones de red para sus clientes. Es esta capacidad para soportar las nuevas características y servicios la que ha asegurado el éxito de MPLS en el campo de las redes proporcionando mayor velocidad y menor costo en el reenvío de paquetes[1].

Por medio de esta monografía, los autores pondrán en práctica los conocimientos obtenidos en la Especialización en Telecomunicaciones de la Universidad Industrial de Santander, específicamente en las áreas de redes de telecomunicaciones y comunicación multiprotocolo mediante etiquetas (MPLS), estudiando los beneficios importantes que ofrece este tipo de comunicación, conociendo el estado actual de la tecnología y sus diversas funciones como lo es la utilidad para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

En esta monografía se pretende formar una base sólida que muestre las especificaciones y características de la tecnología MPLS, siendo un tema de actualidad y de gran futuro. Esto con el fin de proveer un pilar preeliminar para cualquier análisis y/o implementación del protocolo. También ofrecerá una guía teórica para la empresa COPETRAN LTDA que le permita analizar las bondades de MPLS para expandir sus canales de comunicaciones y garantizar una mejor calidad de servicio a sus usuarios finales.

[1] http://urania.dis.eafit.edu.co/cursos/st0059/material/RedesLanWan/lans/mpls.pdf

5 CRONOGRAMA



Nombre de tarea	Duración
FASE 1	**33 días**
Búsqueda de la información	7 días
Interpretación de los datos recopilados	7 días
Compilación de la información	10 días
FASE 2	**24 días**
Interpretación del software de monitoreo d	3 días
Monitoreo de enlaces de datos	3 días
Analizar la información recopilada	3 días
FASE 3	**10 días**
Búsqueda de aplicaciones	5 días
Análisis de las ventajas sobre el ejemplo pi	5 días
FASE 4	**15 días**
Redactar el informe final	15 días

6 MARCO REFERENCIAL

Antes de MPLS, los protocolos mas populares de una red WAN eran Frame Relay y ATM. Por efectos de costos las redes WAN fueron construidas para llevar varios protocolos. Con la popularidad de internet, IP se convirtio en el protocolo mas popular siendo las VPNs creadas sobre los protocolos WAN; los consumidores arredaron a los proveedores de servicio enlaces ATM y enlaces Frame Relay para construir su propia red privada.

Debido a que el envió de paquetes convencional del protocolo de Internet (IP) tiene un número de limitaciones, los proveedores de servicio se enfrentan a muchos desafios al intentar resolver la demanda de los clientes. Los proveedores de servicio (ISP[1]) se deben referir a proteger su infraestructura existente y a encontrar maneras de generar los nuevos servicios actualmente no soportados con tecnologias existentes y se dan cuenta de que es necesario un nuevo método.

Es por eso que MPLS fue diseñado para incorporarse y sustituir a las antiguas tecnologías Frame Relay[2] y ATM[3]. A diferencia de estas, pero al igual que IP, MPLS es un estándar multiprotocolo capaz de transportar diferentes tipos de tráfico por la misma vía.

Mediante MPLS se une la inteligencia del direccionamiento con el rendimiento de conmutar y suministrar beneficios importantes a la red con la arquitectura IP pura tanto como aquellas con IP y ATM o mezcla de otras tecnologías de capa 2. La tecnología MPLS resulta clave para las redes privadas virtuales escalables

[1] ISP: (Internet Services Provider). Proveedor de servicios de Internet

2 (*Frame-mode Bearer Service*) Es una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de frames de datos, perfecto para la transmisión de grandes cantidades de datos.

[3] Modo de Transferencia Asíncrona o Asynchronous Transfer Mode. Tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones

(VPNs), permitiendo crear un enlace eficiente entre dos o más puntos terminales fijos dentro de la red existente. La tecnología también ayuda a repartir y a diferenciar los servicios en redes IP punto a punto con la configuración y la dirección más simple. Haciéndola clave para los proveedores de internet como para suscriptores. No es frecuente el uso de esta tecnología cuando se requiere una conectividad entre emplazamientos geográficamente distantes y tampoco resulta práctico para aplicaciones de conectividad remota y móvil. En cambio, sí suele utilizarse para conectar múltiples divisiones corporativas o sucursales grandes ubicadas en una región geográfica definida.

Como herramienta de marketing, MPLS ha resultado muy útil a los proveedores de servicios, deseosos de seguir ofreciendo los lucrativos contratos de servicios gestionados. No obstante, debido a la demanda disminuida de servicios de voz tradicionales y a la migración de los clientes de servicios Frame Relay y ATM (de márgenes altos), a las VPN IPSec (de márgenes reducidos) que utilizan Internet como red *backbone*, muchos proveedores están experimentando una importante reducción de sus ingresos. A diferencia del estándar IPSec, MPLS utiliza la red propietaria del proveedor de servicios y se comercializa normalmente como servicio gestionado. Por ello, MPLS resulta mucho más rentable para los proveedores de servicios.

6.1 DEFINICIÓN DE LA CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO (MPLS).

MPLS es una tecnología de red que utiliza etiquetas adjuntadas a paquetes de datos como mecanismo de transporte de datos para enviarlos a través de una red. Creado por la IETF y definido en el RFC 3031, esta tecnología ha permanecido por alrededor de 10 años. 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.

6.2 FUNCIONAMIENTO DE LA CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO MPLS.

En una red simple IP usando MPLS, las etiquetas MPLS son anunciadas entre los routers de forma que estos puedan construir un mapa de etiqueta a etiqueta. Estas etiquetas se adjuntan a cada paquete IP permitiendo a los routers que transmiten el trafico mirar la etiqueta y no el destino IP.

En la red MPLS, el enrutador final de etiquetas es llamado LER, (Label Edge router) y es el encargado de asignar una etiqueta MPLS a cada paquete IP. Los paquetes se envían a través de una ruta de conmutación de etiquetas (LSP), donde el enrutador de conmutación de etiquetas o LSR (Label Switch Router), retransmite los paquetes basándose en las etiquetas que tienen asignadas. En cada salto, el LSR elimina la etiqueta existente y aplica una nueva, que indica al siguiente LSR adónde debe enviar el paquete.

En caso de congestiones o fallos de enlaces, el LSP resulta útil para asegurar un enrutamiento eficaz entre los emplazamientos de una red gestionada y garantizar los correspondientes niveles de rendimiento, sin que tenga que intervenir el usuario final.

Con la tecnología LSP, el proveedor de servicios puede enrutar el tráfico según tipos de datos o categorías de clientes. Gracias a la función de etiquetado, la red se encarga de separar el tráfico de alta prioridad, (p.ej., voz o vídeo) en diferentes flujos de datos. Sin embargo, aunque MPLS resulta útil a la hora de conectar emplazamientos, no es para crear enlaces entre clientes y ubicaciones, ni para establecer prestaciones de teletrabajo. Dado que MPLS sólo funciona en la red del proveedor de servicios, no es posible conectar todas las ubicaciones a menos que

la red del proveedor de servicios se extienda hasta dichas ubicaciones. MPLS no fue diseñado para establecer conexiones entre trabajadores móviles remotos y las oficinas centrales. Para establecer este tipo de entorno de teletrabajo corporativo, es preferible una VPN IPSec o SSL. Además, mientras MPLS resulta útil para la creación de un canal multiprotocolo, por sí mismo, no ofrece muchas ventajas en cuanto a transporte seguro de los datos. Una VPN MPLS aísla el tráfico de la misma forma que ATM o Frame Relay, pero no incluye ninguna función para el cifrado, a no ser que se utilice IPSec. Si bien este escenario, con la configuración adecuada, es poco probable, bien puede darse con una configuración deficiente y los intrusos están precisamente al acecho de estas oportunidades. El objetivo de sus creadores era desarrollar una forma de etiquetar paquetes para conseguir una transferencia más eficaz. Sin embargo, MPLS no encripta dichos paquetes, por lo que pueden resultar muy vulnerables a la intrusión, las intervenciones y otros tipos de ataques nefastos. También es posible falsificar el espacio de dirección del cliente o la propia etiqueta MPLS. Esto no significa que MPLS sea una tecnología deficiente, sino simplemente que no se debe implementar MPLS sin una función de seguridad añadida, como puede ser un punto de seguridad en el emplazamiento del cliente (p.ej., cortafuegos con VPN IPSec). MPLS ofrece una topología de malla completa en todos los puntos de la red. Aunque la interconexión de todos los emplazamientos puede que presente ventajas, estas son mínimas si se comparan con una red de alta velocidad y ancho de banda adecuado. Las tecnologías anteriores a MPLS, como Frame Relay, utilizaban una arquitectura en estrella (hub-andspoke). El modelo en estrella presenta una clara ventaja, que MPLS no tiene en cuenta: ofrece una mayor facilidad para implementar medidas de seguridad centralizadas contra la infiltración de amenazas (p.ej., virus, gusanos o spyware).

6.3 FUNDAMENTOS SOBRE MPLS, CONSTRUCCIÓN DE UNA RED MPLS.

En una red IP, sin los routers, no habría posibilidad de marcar, clasificar o monitorear los datos (como lo muestra la figura 1), pero también no habría posibilidad para que el trafico tenga una ruta especifica.

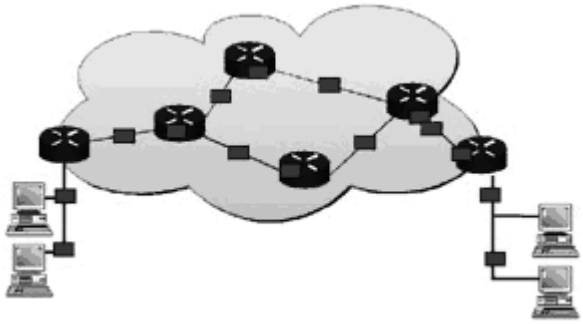


Figura 1. Red IP sin ruta específica *(Fuente propia)*

En orden de designar diferentes clases de servicio o de servicio prioritario, el tráfico debe ser marcado con etiquetas especiales para que entren en la red. Un router especial llamado enrutador de etiquetas de Borde (o LER por su nombre en inglés *label Edge router*) el cual provee esta función (figura 1).

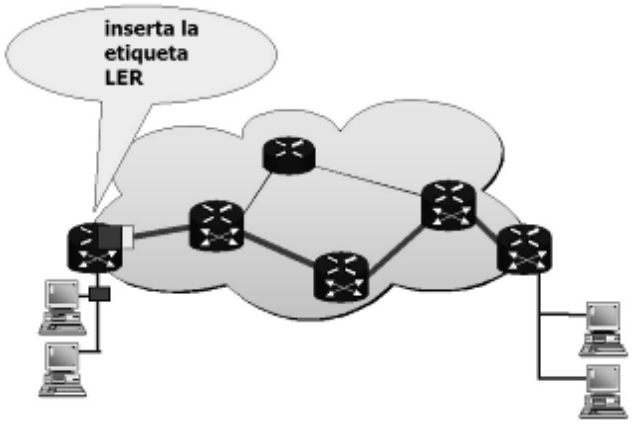


Figura2. Red IP con ruta específica *(Fuente propia)*

El LER convierte ambos paquetes IP en paquetes MPLS dentro de los paquetes IP. En el lado de entrada, el LER examina el paquete que entra y determina si el paquete debe estar etiquetado. Una base de datos especial en el LER marca la dirección en la etiqueta y el encabezado de MPLS (figura 2) es adjuntado al paquete que va ser enviado en esa ruta. El LSP funciona de forma similar a las rutas de conmutación de circuitos que utilizan las redes ATM. Sin embargo, a diferencia de ATM, MPLS soporta distintos protocolos, entre los que se incluyen IPv6 e IPSec, IPv4, ATM, Frame Relay y Ethernet. Al igual que ATM, MPLS ofrece una garantía de ancho de banda para varios flujos de tráfico, por lo que resulta ideal para tráfico sensible a la latencia.

Para entender el encabezado de MPLS se va a mirar el modelo OSI (open Systems interconexión). Las etiquetas de la pila de etiquetas MPLS van después de los encabezados de la capa de enlace de datos pero antes de los encabezados de la capa de red; cuando un paquete IP es presentado en el LER, el pone la etiqueta de encabezado entre las capas 2 y 3 (Figura 3).

Figura 3. Modelo OSI[1] (fuente Multiprotocol Label Switching Architecture. Network Working Group)

[1] El **modelo de interconexión de sistemas abiertos**, también llamado **OSI** (en inglés *open system interconnection*) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones

El encabezado o la etiqueta MPLS consiste en cuatro bytes (32 bits) ; 20 bits son usados para la etiqueta, tres bits para funciones experimentales, y un bit para la función de pila, y ocho bits para tiempo de vida (TTL). El encabezado shim[1] permite la interoperabilidad entre ATM (protocolo de capa 2) e IP (protocolo de capa 3).

Figura 4. Encabezado MPLS (fuente Multiprotocol Label Switching Architecture. Network Working Group)

La función de LSR[2] es de examinar los paquetes que llegan. Siempre si la etiqueta está presente, el LSR va a buscar y a seguir las instrucciones de la etiqueta y va a reenviar el paquete de acuerdo a estas. En general, el LSR realiza una etiqueta de función de intercambio (figura 5)

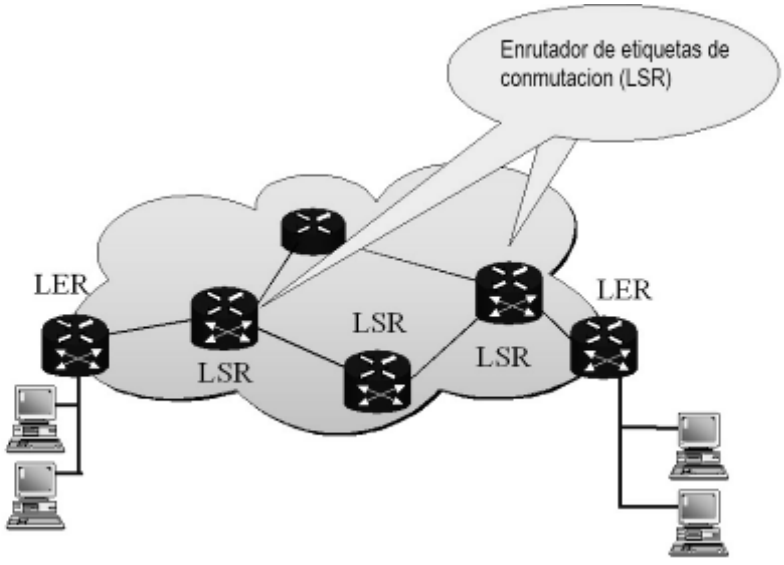


Figura **5 LSR realiza una etiqueta de función de intercambio (Fuente propia)**

[1] Encabezado adicional agregado a los paquetes. se coloca entre los encabezados de capa de red y de capa de enlace del modelo OSI

[2] (Label Switched Router) Elemento que conmuta etiquetas

Los caminos son establecidos entre el LER y el LSR. Estos caminos son llamados LSPs (label switch paths). Estos caminos han sido designados para las características de tráfico, como tal, ellos son muy similares a la ingeniería de caminos de ATM. La capacidad de manejo de trafico de cada camino es calculado. Estas características pueden incluir carga tope de tráfico, variación Inter-paquetes y cálculo de porcentaje de paquetes caídos.

La figura 6 muestra el establecimiento entre LSP y dispositivos de alerta MPLS. MPLS trabaja como un protocolo de superposición IP, los dos protocolos pueden coexistir en la misma nube sin interferencia.

Figura 6. Establecimiento LSP y dispositivos de aleta MPLS *(Fuente propia)*

6.3.1 Flujo de datos en redes MPLS

La forma simple del flujo de datos ocurre cuando los paquetes IP están presentados al enrutador de entrada, el cual está actuando como el LER (figura 7)

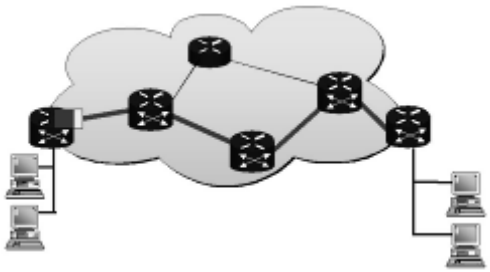


Figura 7. LER de ingreso adjunta el encabezado Shim *(Fuente propia)*

El LER clasifica el tráfico de entrada IP, relativo a la etiqueta correspondiente. En MPLS este proceso de clasificación es llamado FEC (por sus siglas en ingles Forward equivalent class). El LERs usa diferentes modos de etiquetar el tráfico. En un simple ejemplo, el paquete IP es insertado con una etiqueta y un FEC utilizando tablas pre-programadas como se muestra en la tabla número 1.

Tabla 1. Set de instrucciones de LER

Destino/IP	Numero de puerto	FEC	Proximo salto	Etiqueta	Instrucción
199.50.5.1	80	B	47.5.10.100	80	Push
199.50.5.1	443	A	120.8.4.100	17	Push
199.50.5.1	25	IP	100.5.1.100		(Do nothing; native IP)

Cuando el paquete MPLS deja el LER, está destinado por el LSR, donde será examinado en busca de la presencia de etiquetas. El LSR busca estos en la tabla de re-envíos llamada LIB (label información base) o tabla de conectividad, por instrucciones. La LSR saltara etiquetas de acuerdo con las instrucciones LIB como se muestra en la tabla numero 2.

Tabla número 2. Base de información de etiquetas de cambio de router

Etiqueta de entrada	Puerto de entrada	Etiqueta de salida	Puerto de salida	FEC	instruccion para el siguente salto
80	B	40	B	B	Swap
17	A	18	C	A	Swap

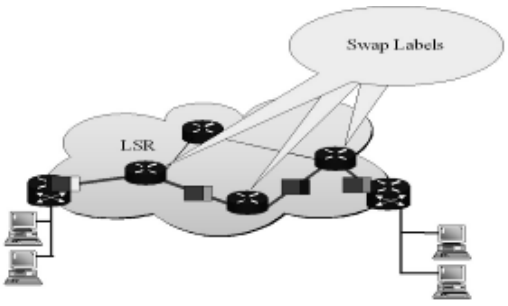


Figura 8. Demostración del funcionamiento del LSR funciones de salto por etiquetas. *(Fuente propia)*

A la salida de la red MPLS el LER remueve el encabezado MPLS del paquete y reenvía este a la red IP. La etiqueta de salto simplifica el flujo del paquete MPLS.

El paquete de LER realiza muchas funciones de análisis: mapeando la capa 2 a MPLS, mapeando MPLS para la capa 3, y clasificando el tráfico. En adición, el LER decide que paquetes del tráfico se convierten en paquetes MPLS.

Un método de decisión es llamado *modo disparo* (triggered mode). Usando este método, el router determina si hay un flujo de tráfico y cuando un predeterminado número de paquetes son dirigidos a una única localización y son programados para llegar dentro de un plazo determinado. Una vez el router ha realizado esta determinación, será re-enrutado el flujo del tráfico del procesamiento MPLS. Incluso nuevas mejoras y la flexibilidad están disponibles para MPLS usando el método de etiqueta-apilado, como se muestra en la figura 9

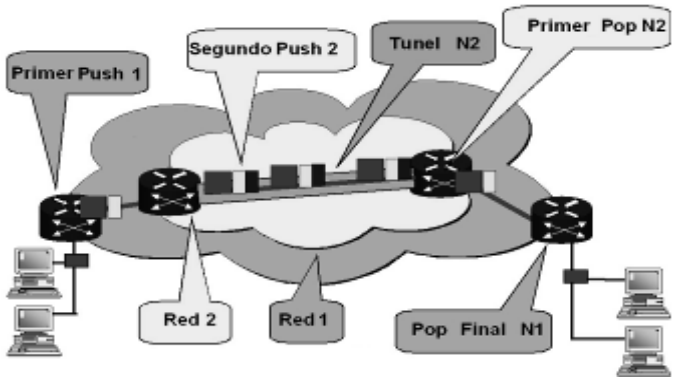


Figura 9. Etiquetas apiladas con túnel de red *(Fuente propia)*

Considerando el siguiente escenario. Usted tiene su propia red 1; sin embargo el tráfico va a ser procesado a través de una red 2, la cual no es dueña su compañía. Usted tiene que estar seguro que la red 2 maneja su tráfico de acuerdo con su arreglo de nivel de servicio (SLA), pero el dueño de la red 2 no está usando el mismo criterio de etiquetas como su compañía. En este caso usted debe tener una pila de etiquetas y construir un túnel a través de la red 2. Esta

configuración le permitirá preservar la integridad de sus etiquetas de red mientras permite a la otra re operar independientemente.

Los routers MPLS, como los telefonistas de la antigüedad, deben ser entrenados, ya que deben aprender todas las reglas y todas las circunstancias en las que deben aplicar las normas. Dos métodos se utilizan para que los routers sean "entrenados" para estos fines:

Un método utiliza la programación difícil y es similar a la forma en la que un router está programado para el enrutamiento estático. La programación estática elimina la capacidad de redirigir dinámicamente o gestionar el tráfico.

Las redes modernas pueden cambiar de forma dinámica. Para adaptarse a las necesidades de ajuste de estas redes, muchos ingenieros de la red han optado por utilizar el segundo método de programación de conmutadores MPLS: dinámica de la señalización y la distribución de la etiqueta. La distribución de etiquetas dinámicas y de señalización puede usar uno de varios protocolos.

Cada protocolo tiene sus ventajas y desventajas. Debido a que esta es una tecnología emergente, que no hemos visto establecerse. El más dominante es el de etiquetado y protocolos de señalización. Sin embargo, a pesar de la selección de los protocolos y sus ventajas y desventajas, los conceptos básicos de la distribución de etiquetas y de señalización permanecen consistentes a través de los protocolos.

Como mínimo, los routers MPLS deben aprender cómo procesar los paquetes con etiquetas de entrada. Este proceso se logra mediante el uso de una conexión cruzada de mesa.

Comenzamos nuestro análisis con una red simple (Figura 10), con cuatro routers. A cada router se ha designado a los puertos. Para la ilustración, cada puerto se le

ha dado una simple carta (a, b, s, H, A y E). Estas identificaciones son específicas del puerto del router. Los flujos de datos desde la entrada A, de R1 a la entrada de la R4.

Figura 10. Red MPLS básica con cuatro routers *(Fuente propia)*

6.3.2 Control de la distribución de etiquetas

Dos modos son usados para cargar las tablas de conexión cruzadas: el control independiente y el control de mando pedido

6.3.2.1 Control independiente

Cada router puede escuchar las tablas de enrutamiento, hace su propia tabla de conexión cruzada, e informa a los otros con esta información. Estos routers van a operar independientemente. El control independiente es un término dado a la situación en la cual no está designada la etiqueta gerente y cuando cada router tiene la habilidad de escuchar los protocolos de enrutamiento, genera las tablas de conectividad cruzada, y las distribuye equitativamente (figura 11).

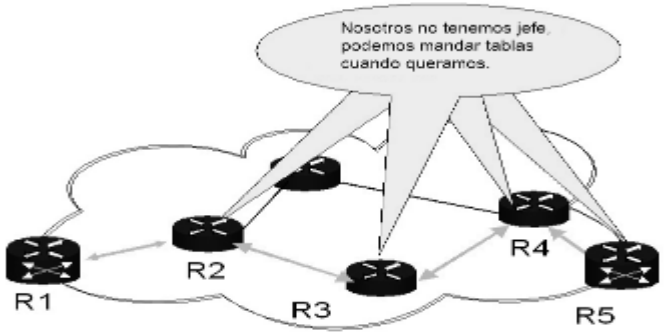


Figura 11.control independiente *(Fuente propia)*

6.3.2.2 Control ordenado

El otro modelo de cargar las tablas es el control ordenado, como se muestra en la figura 12, en el modo de control ordenado, un router (típicamente la salida LER) es el responsable de distribuir las etiquetas

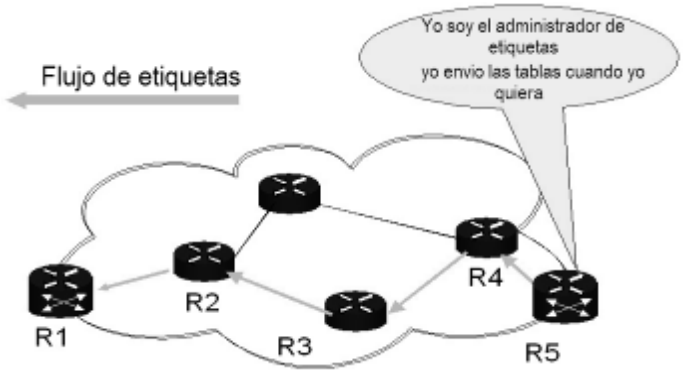


Figura 12. Control ordenado *(Fuente propia)*

Cada uno de los dos modelos tiene sus intercambios. El control independiente provee una convergencia más rápida de red. Cualquier router que escuche un cambio de ruta puede relevar esta información a los otros routers. La desventaja es que no hay un punto simple de control que este generando tráfico, el cual hace que el diseño sea más difícil.

El control ordenado tiene la ventaja de tener un diseño mejor y un control de red de mando, sin embargo, sus desventajas son el tiempo de retraso de convergencia y que el controlador de punto simple puede ser una falla.

6.3.2.3 Activación de la distribución de etiquetas.

Con el control ordenado, dos métodos principales se utilizan para activar la distribución de las etiquetas. Estos son llamados Downstream unsoliciteded ***DOU*** (activación de la distribución de etiquetas con la corriente sin solicitar) y Downstream on demand ***DOD*** (activación de la distribución de etiquetas con la corriente solicitado).

DOU

En la figura 11, hemos visto a las etiquetas ser enviadas a los routers intermedios, Esta campaña se basa en las decisiones del router que ha sido designado como gerente de etiqueta. Cuando las etiquetas no solicitadas son enviadas por el administrador de etiqueta, es conocido como un DOU (Downstream).

Considere estos ejemplos: El gestor de la etiqueta puede utilizar los puntos gatillo (como los intervalos de tiempo) para enviar las etiquetas o en la etiqueta los mensajes de actualización cada 45 segundos. O un gestor de la etiqueta puede utilizar el cambio de tablas de enrutamiento estándar como un gatillo, cuando cambia un router, el gerente de la etiqueta pueden enviar actualizaciones de la etiqueta a todos los routers afectados.

DOD

Cuando las etiquetas se solicitan, son "tirada" hacia abajo, o solicitados, por lo que este método ha sido llamado tirado o posterior en la demanda. Nótese en la figura 13 que las etiquetas se solicitan en el primer paso, y que se envían en el segundo paso.

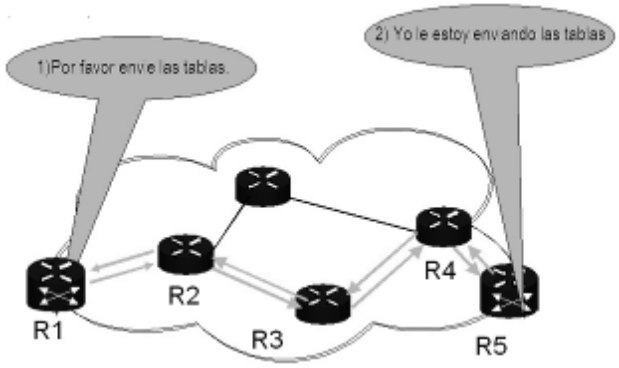


Figura 13. DOD *(Fuente propia)*

Si llegan a través de las etiquetas de control independiente o de control ordenado, a través del DOU, el LSR crea una tabla de conexión cruzada (figura 14).

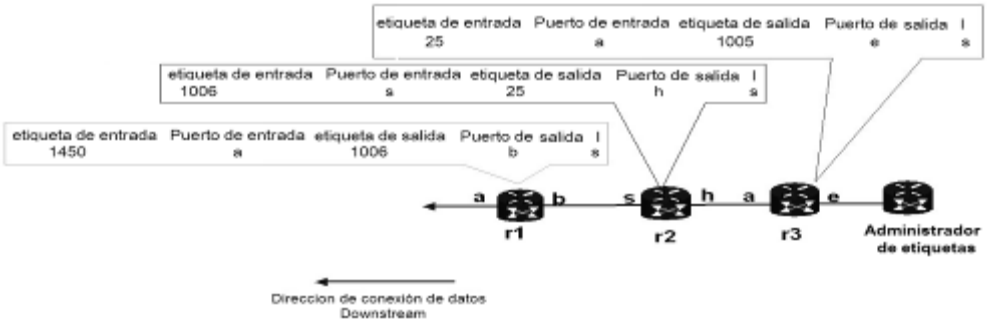


Figura 14. LSR con Tablas de conexión cruzadas copuladas *(Fuente propia)*

En la conexión se tenían tablas de R3 a R1. Los encabezados de lectura de la etiqueta de entrada, puerto de entrada, etiquetan de salida, puerto de salida u la instrucción (I). En este caso, la instrucción de intercambio (S). Es importante señalar que las etiquetas de las tablas de conexión cruzada son específicas en del router.

Después que las tablas de conexión cruzada están cargadas, los datos pueden derivarse de router 4 a router 1, con cada router siguiendo las instrucciones específicas para cambiar las etiquetas. Al estar cargadas las tablas de conexión cruzada los datos pueden seguir un LSP designado y el flujo de router 1 a router 4, como se muestra en la figura 15.

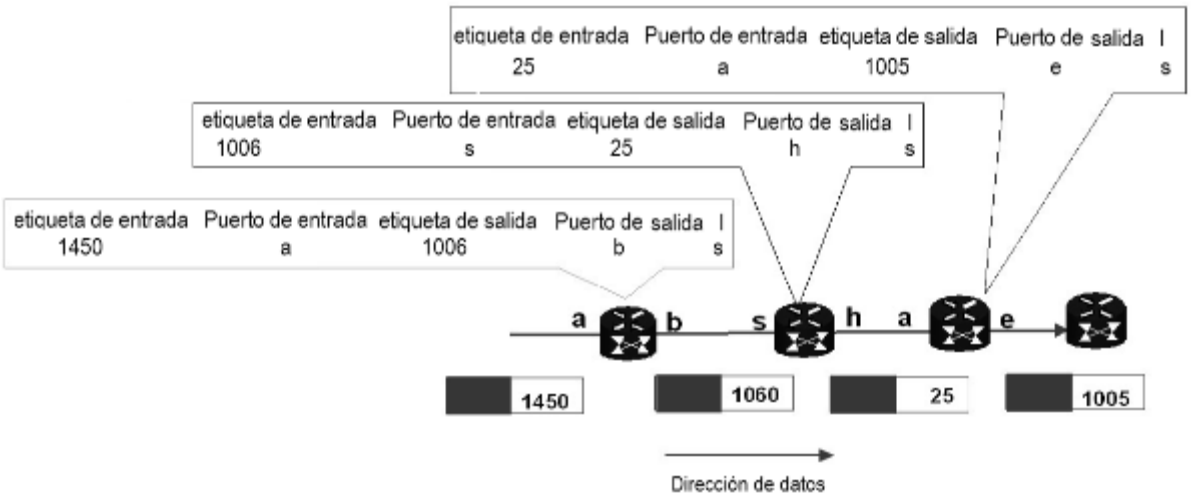


Figura 15. Flujo de datos en LSP *(Fuente propia)*

6.3.2.4 Protocolos

Encontrar un vehículo de transporte con el que construir estas tablas complejas es de suma preocupación para los diseñadores de red. Lo que se necesita es un protocolo que puede llevar a todos los datos necesarios, que sea rápido, que se auto-corrija, y que el mantenimiento de una excelente fiabilidad.

El Protocolo de Distribución Etiqueta, o LDP (label distribution protocol), fue creado por los ingenieros de diseño y el grupo de trabajo de MPLS como medio de atender las necesidades de transporte. Este protocolo funciona como una llamada de teléfono: Cuando las etiquetas están obligadas, éstas seguirán vinculadas hasta que un comando aparece a derribar la llamada. Esta difícil operación de estado provee menos tráfico que un protocolo que exige refrescarse. Los protocolos de enrutamiento LDP pueden proporcionar de forma implícita.

Otros grupos argumentan que no es bueno el uso de un nuevo protocolo de distribución cuando existen protocolos de enrutamiento que pueden ser modificados o adaptados para transportar los enlaces. Así, algunos protocolos de enrutamiento existentes han sido modificados para llevar la información de las etiquetas. Border Gateway Protocol (BGP) y Intermediate System-to-Intermediate System (IS-IS), funcionan bien para la distribución de información de la etiqueta, junto con la información de enrutamiento.

El PLD, BGP, IS-IS y protocolos de establecer la ruta de acceso del Switch de etiqueta (LSP pero hacen poco al servicio de la ingeniería de tráfico, ya que enruta el tráfico que potencialmente puede ser redirigido con alta prioridad LSP, lo que causa congestión.

Para superar este problema, se establecieron protocolos de señalización para crear los túneles de tráfico (rutas explícitas) y permitir la mejor ingeniería de tráfico. Estos protocolos son la restricción del protocolo de distribución de Ruta

(CR-LDP) y el Protocolo de configuración de reserva de recursos (RSVP-TE). Además, el *Open Shortest Path First* (OSPF) protocolo de enrutamiento ha sufrido modificaciones para manejar la ingeniería de tráfico (OSPF-TE). Véase tabla 3.

Tabla 3: Protocolos de señalización

Protocolo	Enrutado	Ingenieria de trafico
LDP	Implicit	No
BGP	Implicit	No
IS-IS	Implicit	No
CR-LDP	Explicit	Yes
RSVP-TE	Explicit	Yes
OSPF-TE	Explicit	Yes

6.4 SEÑALIZACIÓN DE MPLS

6.4.1 Control del tráfico en las redes MPLS

MPLS es tráfico directo que lleva cuatro bytes adicionales de carga útil. Por tomar el esfuerzo para llevar estos datos extra, consigue viajar en “las vías rápidas.” Pero, la vía rápida está sujeta a la presencia de el tráfico re-enrutado rutinario, trayéndole congestión y retrasos en los cuales se han trabajado para evitar.

MPLS es un protocolo de la cubierta que aplica trafico MPLS a una red de IP rutinaria. Las propiedades auto-corrección de IP pueden causar la congestión en sus vías rápidas. No hay respuesta alguna para re-enrutar el tráfico rutinario hacia las vías rápidas cuando ocurre un accidente de tráfico imprevisto.
La Internet es auto-curativa, con las capacidades del los recursos, pero debemos cuestionarnos en cómo los usuarios aseguran que los anchos de banda reservados para sus paquetes no sean invadidos por el tráfico de re-enrutamiento?

En Figura 16, se puede observar una red MPLS normal de computadoras con tres caminos diferentes por el área de banda ancha conectada una red de computadoras (WAN). El Camino A se diseña al 90% de ancho de banda de hora ocupada máxima; El Camino B se diseña al 100% del porcentaje de hora máxima ocupada; finalmente, el Camino C se diseña al 120% de la hora máxima ocupada. En la teoría, el Camino A nunca tiene que enfrentarse con la congestión. En otros términos, el camino se diseña para tomar más tráfico que el que recibirá durante hora máxima. La red C, sin embargo, experimentará los atascos durante hora máxima, porque se diseña para no enfrentarse a estas condiciones de tráfico.

Figura 16. MPLS con tres caminos (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

El QoS en el camino C va a tener algún nivel de imprevisibilidad en relación con los otros dos caminos y va a tener pérdidas de paquetes, mientras que el tráfico en un camino normal debe tener mediciones de la calidad de servicio

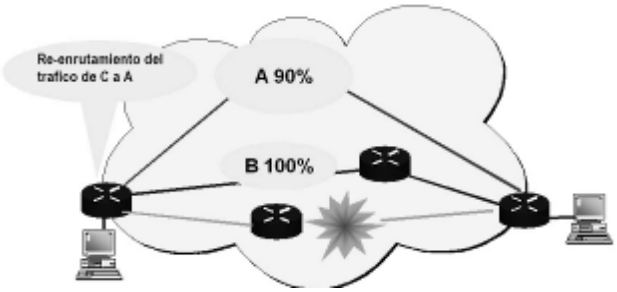


Figura 17. MPLS con el fallo del camino C (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

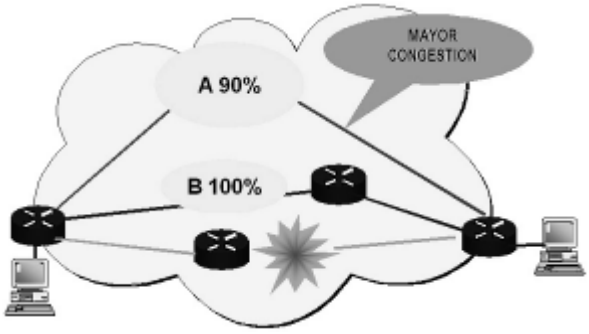


Figura 17a. MPLS con congestión debido al re-enrutamiento (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

Para ayudar a superar los problemas de desvío de la congestión, *la Internet Engineering Task Force* (IETF) y los grupos de trabajo relacionados han estudiado varias posibles soluciones. Este problema ha de abordarse tanto en los protocolos como en los sistemas de software integrado de los routers.

Para tener un completo servicio de calidad QoS, El sistema debe ser capaz de marcar, clasificar y hacer la función de policía. Se sabe como MPLS puede clasificar y marcar los paquetes con etiquetas, pero la función de policía se ha estado perdiendo. Enrutamiento y la distribución de etiquetas pueden establecer el LSP, pero todavía no la función de policía de tráfico y control de los factores de carga en cada enlace.

Nuevos motores de software (ver Figura 18), que se suman a los módulos de gestión entre las funciones de enrutamiento y el selector de ruta, permiten la vigilancia y gestión de ancho de banda. Estas funciones, junto con la adición de dos protocolos, pueden permitir el control de tráfico.

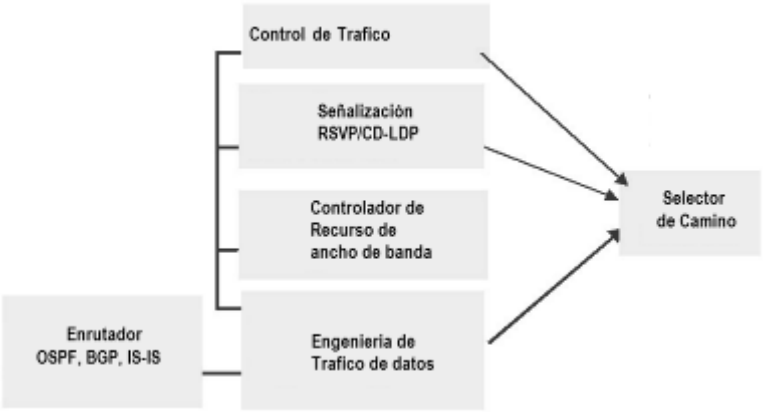


Figura 18. Estado de las maquinas del enrutador MPLS (fuente Multiprotocol Label Switching Architecture. Network Working Group)

Los dos protocolos que dan MPLS la capacidad de la policía de tráfico y las cargas de control son RSVP-TE y CR-LDP.

6.4.1.1 **RSVP-TE**

Usa el concepto de un proceso de establecimiento de llamada, en donde los recursos están reservados antes de que las llamadas estén establecidas, se remonta a los días de la teoría de la señalización de telefonía. Este concepto fue adaptado a las redes de datos cuando QoS (calidad de servicio) se convirtió en un problema.

En 1997, el IETF diseñó un método temprano, llamado Protocolo de reserva de recursos (RSVP), para esa función. El protocolo fue diseñado a solicitud de ancho de banda necesario y las condiciones de tráfico en una ruta de acceso definido. Si se dispone de ancho de banda en las condiciones establecidas, la relación se establecería.

El vínculo se estableció con tres tipos de tráfico que eran similares a los de primera clase, segunda clase, y el transporte aéreo de espera y los patrones se denominan, respectivamente, carga garantizada, de carga controlada, de carga y de mejor esfuerzo.

En las figuras 19 y 20, vemos cómo una llamada o una ruta se arregla entre dos extremos. El cliente solicita a la estación una ruta específica, con las condiciones de tráfico detallados y los parámetros de tratamiento incluidos en el mensaje de solicitud de ruta. Este mensaje es recibido en el servidor de aplicaciones. El servidor de aplicaciones envía una reserva para el cliente, la reserva de ancho de banda de la red. Después de que el mensaje de la primera reserva se recibe en el cliente, los datos pueden comenzar a fluir en rutas de acceso explícitas de extremo a extremo.

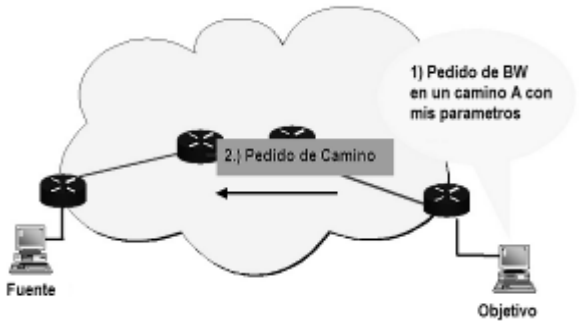


Figura 19. Petición de camino de RSVP-TE *(Fuente propia)*

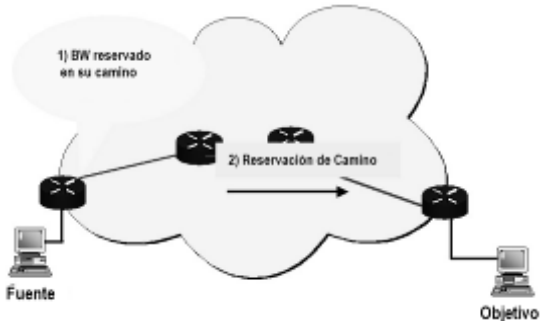


Figura 20. Reservación RSVP-TE *(Fuente propia)*

El proceso de establecimiento de llamada (o "señalización") se denomina estado blando porque la llamada será demolida si no se actualiza de acuerdo con los temporizadores de refresco. En la figura 21, vemos que la ruta de acceso y los mensajes de solicitud de reserva durante tanto tiempo como los datos que fluyen.

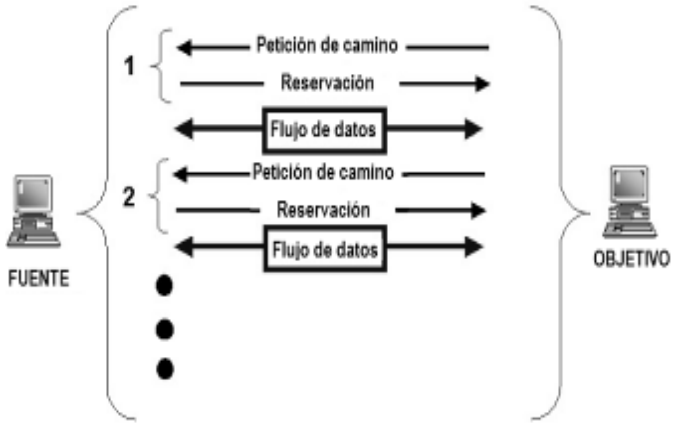


Figura 21. RSVP-TE ruta de instalación (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

Algunos argumentos en contra de principios RSVP incluido el problema de la escalabilidad: Más rutas establecidas, más mensajes de actualización de los que se crearían, y la red pronto se sobrecargaría con los mensajes de actualización. Métodos de abordar este problema incluyen la prevención de los enlaces de tráfico y rutas de acceso.

Los detalles de una solicitud de camino RSVP-TE y reservas se pueden ver en el sitio Web de Ethereal.com. En la Figura 22, captura MPLS, MPLS TE archivos. En la captura, podemos ver las especificaciones de tráfico (tspec) para la carga controlada.

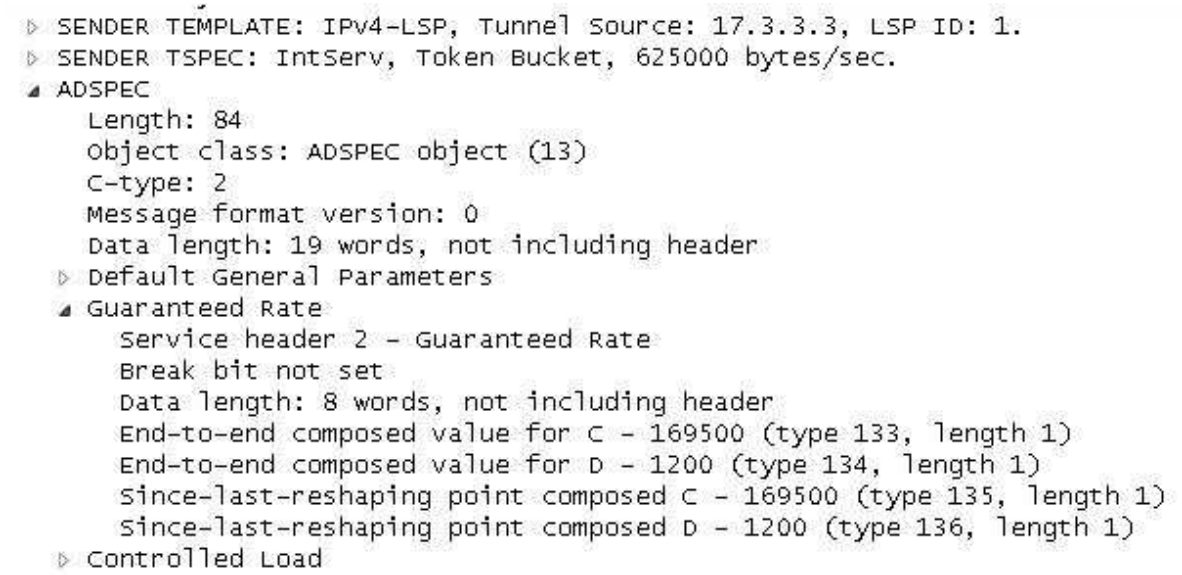


Figura 22. Detalles RSVP-TE (www.wireshark.org)

CR-LDP

Con la restricción basada en enrutamiento por encima del Protocolo de distribución de etiquetas (CR-LDP), se realizaron modificaciones en el protocolo LDP para permitir a las especificaciones de tráfico. El impulso para este diseño fue la necesidad de utilizar un protocolo existente (PLD) y le dan la capacidad de

ingeniería de tráfico. Nortel Networks hecho un gran esfuerzo para poner en marcha el protocolo CR-LDP.

El CR-LDP protocolo añade campos con el protocolo LDP a estos se les denominan, rata de datos pico, tamaño de ruptura pico, tasa de datos comprometidos, tamaño de ruptura comprometida, y el exceso de datos (tamaño de exceso de ruptura) son muy similares a los utilizados en las redes ATM. El formato del cuadro se muestra en la figura 23.

Figura 23. Formato de Estructura de CD-LDP (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

El procedimiento de establecimiento de llamada de CR-LDP es sumamente simple de dos pasos, la de petición y un mapa (como se muestra en la Figura 24). La razón de la configuración simple, es que CR-LDP es un Protocolo duro del Estado-bajo que significa que, una vez establecida la llamada, enlace, o la ruta no serán distribuidos hasta la terminación que se solicita.

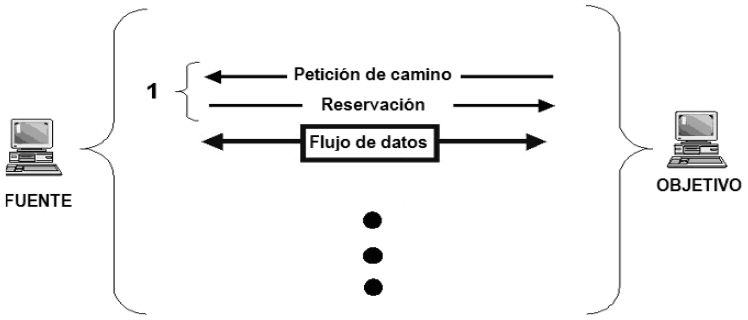


Figura 24. Configuración de llamada CR-LDP (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

La principal ventaja de un protocolo duro de estado es que puede y debe ser más escalable, y de menos tráfico es necesaria para mantener el enlace activo.

Comparando CR-LDP VS RSVP-TE

Las comparaciones técnicas de la CR-LDP y RSVP-TE protocolos aparecen en la Tabla 4. Vemos que CR-LDP utiliza el protocolo del PLD como su portador, mientras que RSVP-TE utiliza el protocolo RSVP. RSVP es típicamente emparejado con la detección de IntServ de calidad de servicio, mientras que el protocolo CR-LDP, ATM utiliza términos de ingeniería de tráfico para asignar QoS

Tabla4: CR'LDP vs RSVP-TE

Comparación	CR-LDP	RSVP-TE
vendedores	Nortel	Cisco, Juniper, Foundry
Estado	Estado duro	Estado suave
tipo de QoS	ATM	IntServ
tiempo de recuperación	Un poco lento	Rapido
charla sobre la cabeza	Bajo	Alto
trasportado en	LDP encima TCP	RSVP en IP
Modificaciones en el camino	lo hace antes de la pausa	lo hace despues de la pausa

6.5 RED MPLS DEPENDENCIA Y LA RECUPERACIÓN

El sueño de todos los proveedores y de cada cliente es tener una red libre de fallas. Ese ideal no es fácil de traducir a la realidad, y algunas consideraciones de cuidado de la eficacia frente a la asequibilidad deben ser realizados. Además, el grado en que una red está equipada para manejar y recuperarse de los fracasos

es tan importante como la salvaguardia de una red de los fracasos en el primer lugar. Se debe mostrar maneras de proteger las redes, los medios de asegurar la recuperación rápida, y la necesidad de confiabilidad.

6.5.1 Protección de la red

MPLS se ha aplicado principalmente en el núcleo de una red IP. A menudo, MPLS compite cabeza a cabeza con redes ATM, por lo que se espera que se comporte como un switch ATM, en el caso de fallo de red. Con un fallo en una ruta de red, la recuperación puede tomar desde unas pocas décimas de segundo hasta varios minutos. De MPLS, sin embargo, debe recuperarse de un error en cuestión de milisegundos, el estándar más común es de 60 milisegundos. Para complicar aún más el proceso de recuperación, una recuperación MPLS debe garantizar que el tráfico pueda continuar fluyendo con la misma calidad que lo hizo antes del fallo. Así, el desafío para las redes MPLS es detectar un problema y cambiar a una ruta de acceso de la calidad de igualdad dentro de 60ms.

6.5.2 Detección de fallas y soluciones

Hay dos métodos principales se utilizan para detectar fallos de red: la detección de latidos del corazón (heartbeat) y mensajes de error. El método de ritmo cardíaco (se usa en conmutación rápida) detecta y se recupera de los errores más rápidamente, pero utiliza más recursos de red. El método de mensaje de error requiere mucho menos recursos de la red, pero es un método más lento. En la figura 25 los intercambios entre los latidos del corazón y los métodos de mensaje de error de detección de fallos

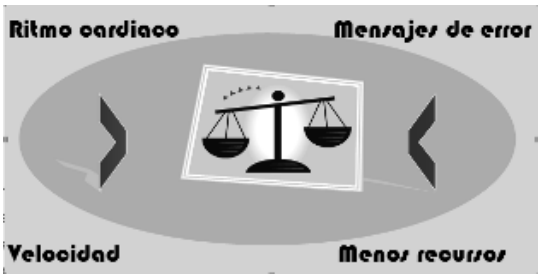


Figura 25 ritmo cardiaco Vs Mensaje de error *(Fuente propia)*

El método de ritmo cardíaco (Figura 26) utiliza una solución simple para detectar fallas. Cada dispositivo anuncia que está activo a un gestor de la red en un intervalo de tiempo determinado, de ahí el ritmo cardiaco a largo plazo. Si se pierde un mensaje que indique q la ruta la ruta de acceso esta activa, el enlace o nodo se declara como inactivó y una a continuación conversión se realiza.

El método de ritmo cardiaco requiere considerables funciones generales la más frecuente es la sobrecarga. Por ejemplo, con el fin de lograr una conversión de 50 ms cada mensaje que indica q una ruta esta activo, debe ocurrir aproximadamente cada 10 ms.

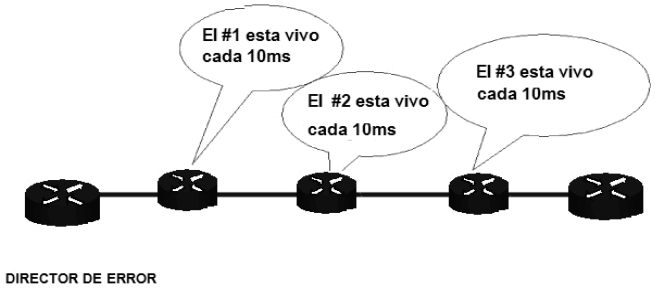


Figura 26. Método de ritmo cardiaco *(Fuente propia)*

El segundo método de detección de fallos del sistema es el es el que se basa en un mensaje de mensaje de error de detección (ver figura 27), cuando un dispositivo en la red detecta un error, envía un mensaje a sus vecinos, que les ordena a redirigir el tráfico a una ruta de acceso o enrutador que está trabajando.

La mayoría de los protocolos de enrutamiento utilizan adaptaciones de este método. La ventaja del mensaje de error es que la sobrecarga de la red es baja. La desventaja es que se necesita tiempo para enviar el error y el mensaje de redirigir a los componentes de la red. Otra desventaja es que los mensajes de error que nunca podría llegar a los routers intermedios.

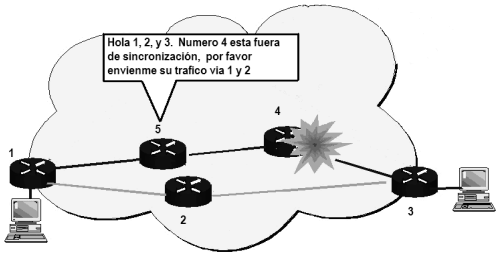


Figura 27. Mensaje de error *(Fuente propia)*

Si el tiempo de conversión no es crítico (como lo ha sido históricamente en redes de datos), el método mensaje de error funciona bien, pero en un tiempo de transición crítica, el método de ritmo cardíaco es a menudo la mejor opción para la recuperación de errores óptimos.

Figura 28. Enrutamiento estándar *(Fuente propia)*

6.5.3 Caminos alternativos

Si un enlace o router falla, una vía alternativa es finalmente encontrada. Si los paquetes se eliminan en el proceso, un protocolo de capa 4 (como TCP) va a retransmitir los datos que faltan.

Este método funciona bien para la transmisión de los datos fuera de tiempo real, pero cuando se trata de enviar los paquetes de tiempo real (como voz y vídeo), los retrasos y pérdida de paquetes no son tolerables.

6.5.4 IGP de convergencia rápida

Para hacer frente a los problemas de enrutamiento de convergencia, OSPF IGP y grupos de trabajo han desarrollado IGP de convergencia rápida, lo que reduce el tiempo de convergencia de una ruta de red en aproximadamente 1 segundo.

Los beneficios de usar IGP de convergencia rápida incluyen tanto las funciones generales y de mayor tráfico en la red, sin embargo, sólo aborda la mitad del problema planteado por MPLS. El desafío de mantener los túneles de los parámetros QoS no es abordado por esta solución.

6.5.5 Protección de Red

En una red, hay varios puntos potenciales de fallas. Dos tipos principales de los fracasos son el fallo de enlace y el fallo de nodo (Figura 29). Fallas menores podría implicar cambiar el hardware, el software de conmutación, bases de datos de conmutación, y la degradación del vínculo.

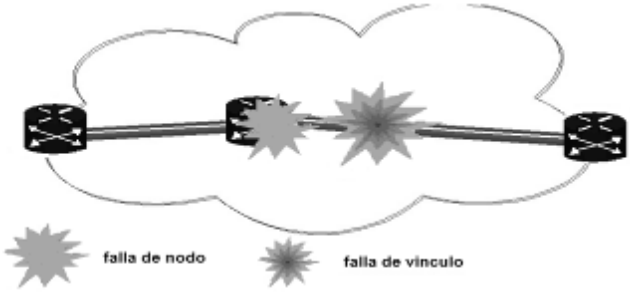


Figura 29. Fallas de red (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

La industria de telecomunicaciones a tenido históricas fallas en los links de dirección, con dos tipos de redes para la tolerancia de error: la redundancia uno a uno y la redundancia uno a muchos. Otra táctica de protección usada comúnmente emplea un hardware para la tolerancia de errores.

Para proteger una red MPLS se debe prever un camino de repuesto con QoS y las características de procesamiento de tráfico exacto. Este camino seria espacialmente diverso, continuamente usado y probado para operaciones. Sin embargo, este no se pondrá en línea a menos que ocurra un fracaso en el camino protegido primario. Este método conocido como protección de redundancia uno a uno tiene un rendimiento en la protección y la fiabilidad de la red, pero el costo de su aplicación puede a ser muy alto. (Véase figura 30)

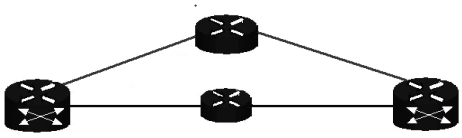


Figura 30. Redundancia uno a uno (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

Un segundo esquema es la protección de redundancia uno a muchos. Usando este método el camino de apoyo entra a funcionar cuando un camino falla. La red mostrada en la figura 21 puede aguantar el fallo de un camino pero no el fallo de dos.

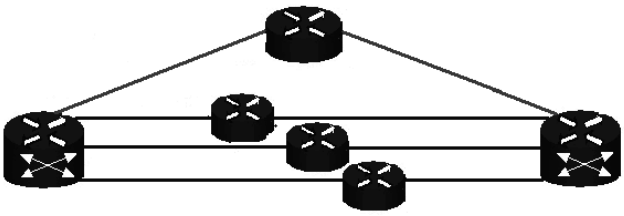


Figura 31. Redundancia uno a muchos (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

Un tercer método de protección es el uso de routers tolerantes de falta (figura 32). En este diseño las características de cada router ofrece las funciones redundantes incorporadas a las tarjetas de red. En la figura 32 se muestra las tarjetas de redundancia de red con un control de apoyo. Nótese que un ítem en común y no redundante es la tabla de conexión cruzada. Si el dato del router se corrompe, el hardware tolerante de falla no puede dirigirse al problema.

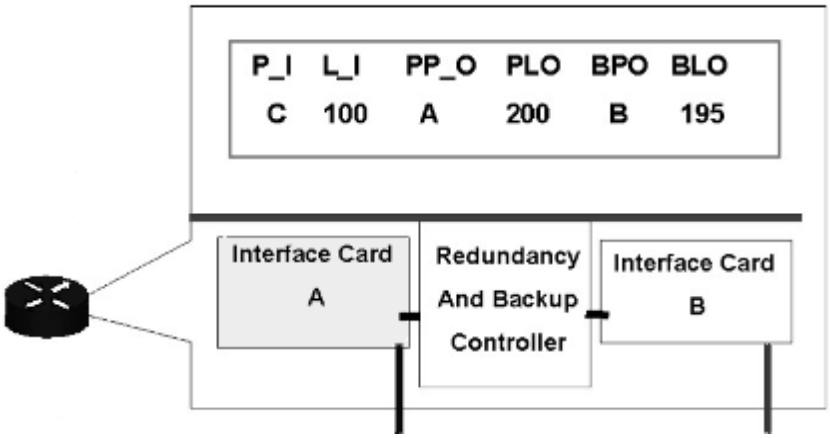


Figura 32. Equipo de falta tolerante (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

6.5.6 Detección de errores en MPLS

LDP y CR-LDP son protocolos que contienen un mensaje de error del tipo longitud-valor (TLV) para informar de los errores de vínculos y nodos. Sin embargo hay dos desventajas en este método; primero, toma tiempo para enviar

el mensaje de error. Segundo, desde que LDP es un mensaje orientado-conexión, el mensaje de la notificación podría nunca llegar si el vinculo esta caído.

Un acercamiento alternativo al descubrimiento de este error es usar el método de latido de corazón, el cual está basado en la fundación del protocolo RSVP-TE. Rsvp tiene rasgos que le hacen una buena alternativa para un modelo de mensaje de error, además es un protocolo de estado-suave el cual requiere estar refrescándose siempre, si el eslabón no ser refresca ese vinculo se torna abajo. Ningún mensaje de error se requiere, y la recuperación rápida (re-enrutamiento rápido) es posible si hay un camino pre-provisionado. Si RSVP-TE ya se usa como protocolo de señalización, es requerido un encabezado adicional para la recuperación rápida.

RRR

Re-enrutamiento Rápido (RRR por su siglas en ingles *rapid reroute*) es un proceso en el que un fracaso del vínculo pude descubrirse sin la necesidad de señalización. Como RSVP-TE ofrece la señalización del estado-suave, puede coparse de un re-enrutamiento rápido.

Protección RSVP-TE

En RSVP-TE, se usan dos métodos para proteger la red: protección de vínculo y protección de nodo.

En la protección de vinculo, un solo vinculo es protegido con un vinculo de apoyo pre-provisionado. Si hay un fracaso en el vinculo, los switches abrirán el camino hacia el pre-provisionado, como lo muestra la figura 33

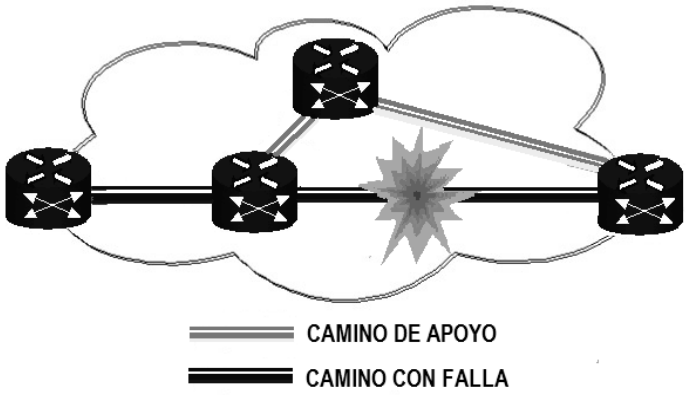


Figura 33. RSVP-TE, con protección de vínculo (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

En una falla de nodo, todo un nodo o un switch puede fallar, entonces todos los vínculos adjuntados a ese nodo pueden fallar. Con la protección de nodo, se utiliza un túnel pre-provisionado alrededor del nodo como lo muestra la figura 34

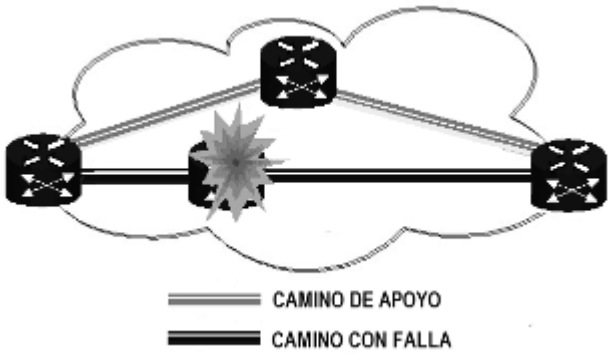


Figura 34. RSVP-TE, con protección de nodo (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

6.6 APLICACIÓN DE MPLS

6.6.1 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 supra utilizados, 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 35 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

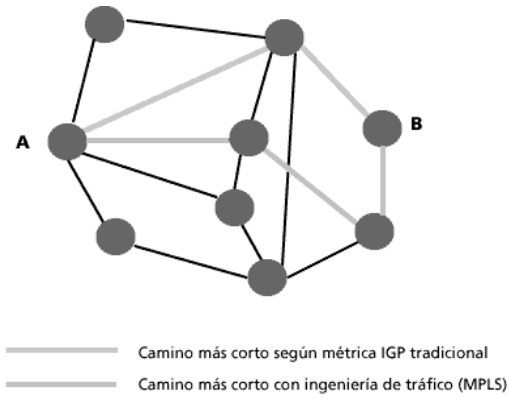


Figura 35. Comparación de dos tipos de rutas entre dos nodos

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 hagan 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.

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.

6.6.2 Aspectos de la ingeniería de tráfico

En las redes de datos y de voz, la función de la ingeniería de tráfico es dirigir el tráfico a los recursos disponibles. Si lograr una red fluida fuera un proceso simple, las redes nunca experimentarían retrasos o caídas en horas de alto tráfico.
En Internet deben emprenderse cuatro pasos para lograr la ingeniería de tráfico: midiendo, caracterizando, planeando y mudando el tráfico a la ubicación deseada.

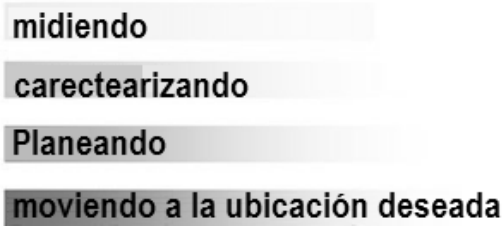


Figura 36. Cuatro pasos para lograr la ingeniería de tráfico (fuente Multiprotocol Label Switching Architecture. Network Working Group)

- **Medida de tráfico**: es un proceso de métrica de la red colectivo, como el número de paquetes, el tamaño de paquetes, paquetes que viajan durante la hora ocupada máxima, las tendencias de tráfico, aplicaciones que la mayoría usó, y datos de la actuación (es decir, transmitiendo y procesando las velocidades).

- **Caracterizando el tráfico**: es un proceso que irrumpe los datos crudos en las categorías diferentes para que pueda planearse estadísticamente. Aquí, los datos que se recogen en la fase de la medida se ordenan y se categorizan.

- **Modelado o planeación del tráfico**: es el proceso de usar todas las características de tráfico y el tráfico estadísticamente analizado para derivar fórmulas y algoritmos de los datos. Cuándo el tráfico se ha planeado matemáticamente, pueden correrse los guiones diferentes contra el modelo de tráfico para el caso.

- **Poniendo el Tráfico dónde usted lo quiere:** La componente de reenvío de paquetes es una componente esencial de ingeniería de tráfico. Es la responsable de 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. Esta es una inmensa tarea que requeriría lejos muchos recursos a nuestra disposición. Antes de que MPLS fuera desarrollado, los ingenieros tenían que entender las características y planear el tráfico de toda la Internet para realizar la ingeniería de tráfico.

Para determinar los datos que pasan a través de cualquier fase dada de transmisión, usted puede medir los datos que viajan a través de una red con exactitud relativa usando las herramientas de medida de gestión de redes. Usando el método de medida alternada, se puede calcular el ancho de banda necesario calculando la carga útil total de la rata de bit por segundo (bps) y agregando la rata de los encabezados en bps;

Cuando se habla de sobre-pro visionado es el proceso de ingeniería en el cual se toman los recursos de ancho de banda los cuales son mayores que la demanda de la red y se utilizan: bajo-pro visionado es el proceso de ingeniería en la cual hay una demanda mayor a los recursos disponibles a la red.

El OC-12 el cual se diseña para manejar 622 MB/s, es pro visionado totalmente y el trafico puesto en el circuito es menor de 622 Mb/s, se dice que esta sobre-pro visionado, y así el verdadero QoS tiene una oportunidad de volverse realidad; sin embargo, el costo es significativamente mas alto

Pero si el tráfico que se pone en el OC-12 es mayor que 622 Mb/s, se dice que es bajo-pro visionado y si esto pasa en un camino en una red hay la probabilidad que

allí se genere demasiado tráfico. La ventaja de bajo-pro visionado es un ahorro significante en el costo, pero se pierde QoS y menos fiabilidad.

En la figura 37 se puede tomar por encima o por debajo de provisión un circuito en porcentajes relativos para el ancho de banda designado.

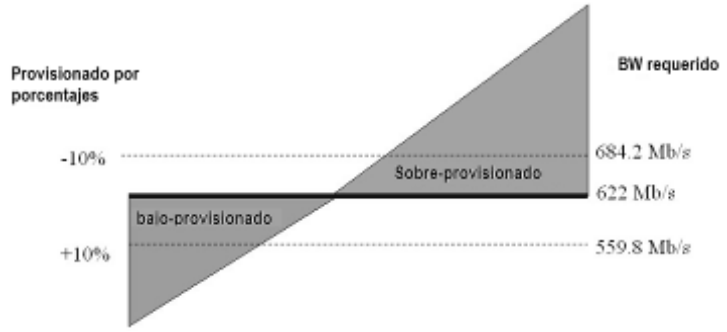


Figura 37. Sobre- provisionado vs bajo-provisionado (Fuente , MPLS: Convergencia entre el Nivel de Transmisión y el Nivel de Enrutamiento)

En la figura 38 se observa que cuando se sobre-provisiona el QoS incrementa pero el costo también, y pasa lo inverso cuando se bajo-provisiona.

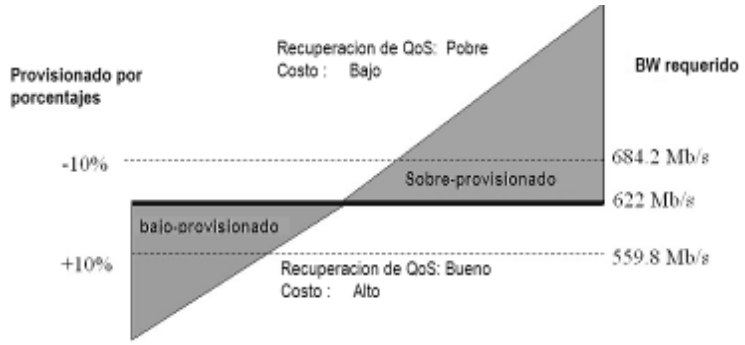


Figura 38. Comparación entre sobre-provisionado y bajo-provisionado (Fuente , MPLS: Convergencia entre el Nivel de Transmisión y el Nivel de Enrutamiento)

6.6.3 Diferenciación de niveles de servicio mediante clases QoS

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el *WWW*, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de vídeo y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De es te modo, una red MPLS puede transportar distintas clases de tráfico, ya que el tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP; También porque entre cada par de LSR exteriores se pueden aprovisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, primero, preferente y turista, que, lógicamente, tendrán distintos precios.

6.6.4 Servicio de redes privadas virtuales VPN

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. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

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

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los 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. No es el objetivo de esta sección una exposición completa de IP VPNs sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones. Se puede obtener más información sobre IP VPN con túneles en las referencias correspondientes a VPNs con MPLS.

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

1. En el nivel 3, mediante el protocolo IPSec del IETF.
2. 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 data-gramas 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.

6.6.5 Modelos VPN: Modelo de cubierta

El modelo de cubierta es llamado también modelo cliente-equipo-a-cliente-equipo (CE a CE). El trafico IP de una red VPN es dirigido hacia los túneles extremo a extremo. Los servicios de Frame Relay (FR) y ATM son ejemplos del modelo de cubierta. El protocolo IP es flanquea de CE a CE encima de la capa 2 donde estos portadores mantienen los backbones desde las VPNs. En la figura 39 se observa como los sitios de consumidores 1, 2, 3 y 4 están conectados vía túneles. Los datos están encapsulados para que los datos IP no estén expuestos a través de las redes.

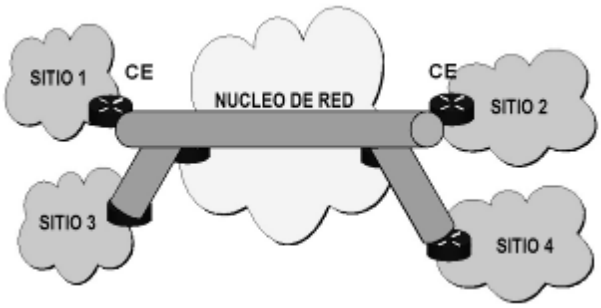


Figura 39. Modelo VPN de cubierta (fuente Multiprotocol Label Switching Architecture. Network Working Group)

En la figura 40 se observa que si se agrega un consumidor adicional un nivel de complejidad es agregado. Los ingenieros de configuración y los directores de red deben mantener el tráfico de los consumidores azules separado del tráfico del consumidor en rojo y viceversa

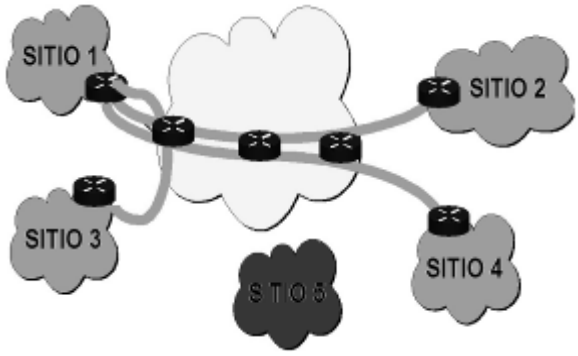


Figura 40. La Configuración del hub and spoke con 4 Sitios (la Configuración Original) (fuente Multiprotocol Label Switching Architecture. Network Working Group)

El modelo de cubierta puede ofrecer lo último en seguridad, pero con sus desafíos:

- Una compañía tiene dos opciones al usar esta opción: manejar y mantener sus propios túneles o permitir que su proveedor de servicio maneje sus túneles por ellos. En cualquier caso hay un costo por mantener los túneles y llaves del encriptación.

- Como el número de sitios crece dentro de la red crece, la complejidad de hardware y software aumenta y a su vez los aumentos en el costo de mantenimiento y configuración también.

- El hardware y gastos del capital también son un problema. Para cliente con n-sitios, el número de routers requeridos son n-1. Cuando agrega, mueve y cambia la configuración de cada sitio es requerida.

Se observa dos ejemplos de cómo el Sitio 5 puede agregarse. Para un diseño hub and spoke se cambia el Sitio 1 y el Sitio 5. Usando el ejemplo en Figuras 41 y 42, se va a agregar el Sitio 5 a la configuración. Actualmente lal tabla de configuración es la siguiente:

El sitio 1 habla con los Sitios 2, 3, 4

El sitio 2 habla con el Sitio 1

El sitio 3 habla con el Sitio 1

El sitio 4 habla con el Sitio 1

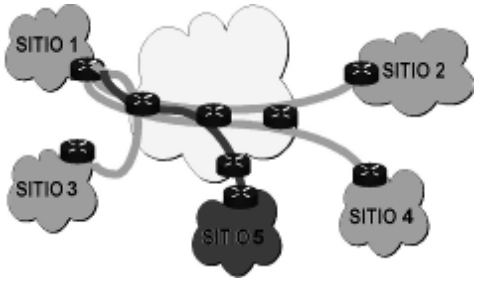


Figura 41 agregando el sito 5 al diseño hub and Spike (fuente Multiprotocol Label Switching Architecture. Network Working Group)

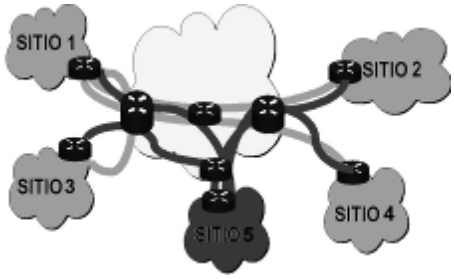


Figura 42. agregando el sito a una red total mente enredada (fuente Multiprotocol Label Switching Architecture. Network Working Group)

Lo siguiente ilustra las modificaciones que se requieren por agregar el Sitio 5:

Agregue Sitio 5

El sitio 1 habla a los Sitios 2, 3, 4, 5

El sitio 5 habla al Sitio 1

Note eso con una configuración de la matriz llena que la complejidad crece.

La siguiente es la configuración antes de que el Sitio 5 es agregado.

El sitio 1 habla a los Sitios 2, 3, 4
El sitio 2 habla a los Sitios 1, 3, 4
El sitio 3 habla a los Sitios 1, 2, 4
El sitio 4 habla a los Sitios 1, 2, 3

Toda la configuración siguiente configuración debe modificarse para comunicar a todos los sitios con el nuevo Sitio 5.

Agregando el Sitio 5

El sitio 1 habla a los Sitios 2, 3, 4, 5
El sitio 2 habla a los Sitios 1, 3, 4, 5
El sitio 3 habla a los Sitios 1, 2, 4, 5
El sitio 4 habla a los Sitios 1, 2, 3, 5
El sitio 5 habla a los Sitios 1, 2, 3, 4

6.6.6 Modelo Peer VPN (MPLS)

Debido al costo de propiedad y complejidad de aplicación, muchas empresas escogen confiar en su portador para mantener la integridad de los datos. Estas redes se han dado a conocer como ' VPNs confiables; 'las redes con encriptación son conocidas como 'VPNs seguras.' En VPNs confiables, los sitios se unen al equipo Edge del proveedor (PE) vía los vínculos dedicados o en arriendo se construyen líneas y túneles de PE a PE (vea Figura 43). El modelo peer también se le denomina como router adyacente.

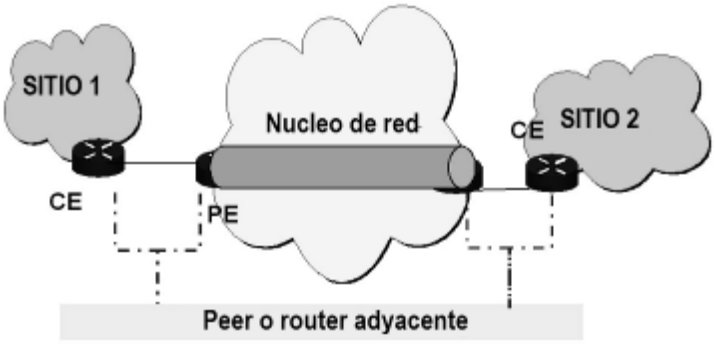


Figura 43. Modelo Peer (fuente Multiprotocol Label Switching Architecture. Network Working Group)

En el mercado de datacom, el tráfico de IP es el transporte de la red primario. Portadores que desean proporcionar IP VPNs ofrecieron la Frame Relay (FR) y ATM. Estas soluciones son buenas, pero a menudo no es escalable o el costo eficaz sea bastante para mantener las soluciones viables para muchOS negocios.

6.6.7 Topologías Mpls VPN

MPLS VPNs puede proveer una solución VPN flexible a los proveedores de servicio (ISP). En orden de conocer estas necesidades se desarrollo el etiquetado de capa 3.

La topología y el diseño de MPLS VPN ha sido desarrollado rápidamente. A través de los años, MPLS VPNs ha crecido desde VPNS de capa 3 en una variedad de opciones incluyendo protocolos cualquiera- a –cualquiera, como lo es Ciscos AToM (Cualquiera trasporta sobre MPLS).

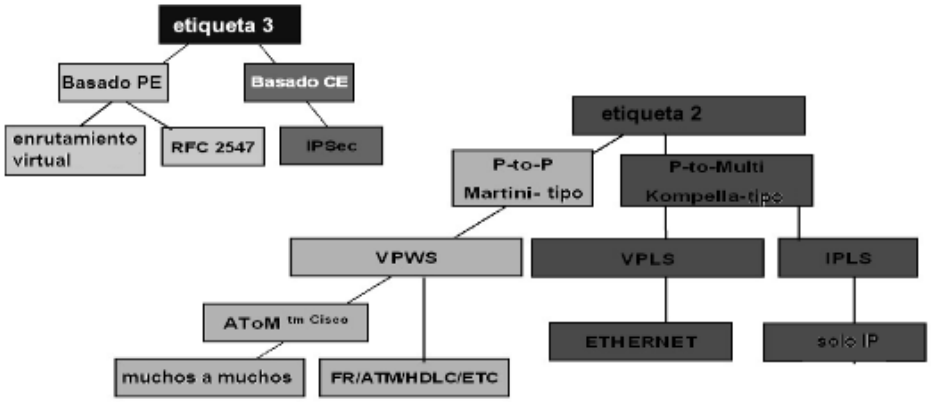


Figura 44 las etiquetas de VPNs (árbol VPN) ***(fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)***

6.6.8 VPNS MPLS

El modelo Peer, el PE y el CE cambian la información de ruta IP en una relación peer-to peer. Los túneles VPN están establecidos en el núcleo de una red MPLS.

Refiriéndose al árbol de MPLS VPN (figura 44) se observa la etiqueta de capa 3 MPLS VPNs en la izquierda de la imagen con dos modos abajo; el RFC 2547 y el enrutamiento virtual.

El RFC 2457 es un simple flujo de datos como se muestra en la figura 45 y en la figura 46, estos van a través de la capa RFC 2541 VPN. Los datos de la IP nativa son enviados a PE1 agregando las etiquetas VPN al mapeo de la interfase del consumidor. PE1 entonces asigna un LSP y una etiqueta MPLS a ese camino.

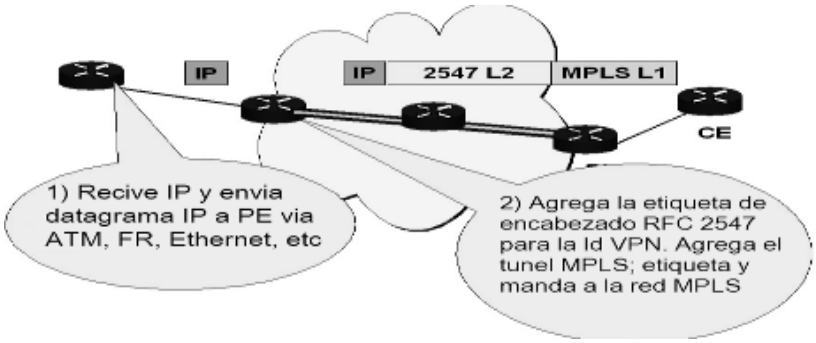


Figura 45. Flujo de datos RFC 2547, paso 1 y 2 (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

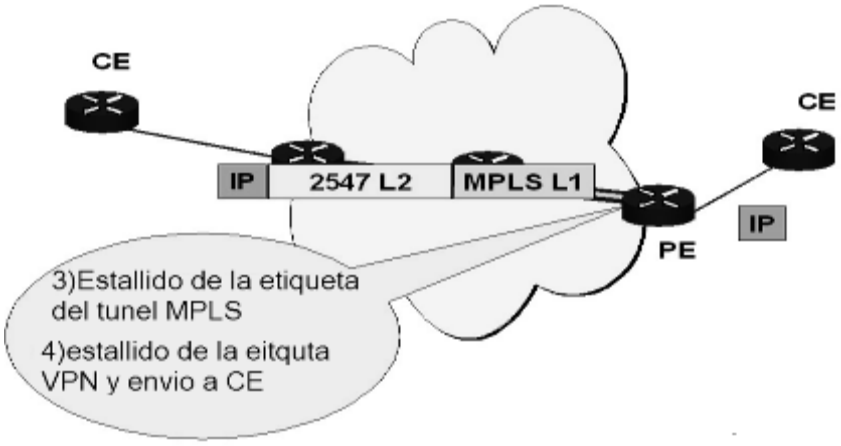


Figura 46. Flujo de datos RFC 2547 pasos 3 y 4(fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

Una red virtual es establecida a través del núcleo de la red usando extensiones del protocolo BGP. Esto permite la simplificación del intercambio de enrutamiento del núcleo y los proveedores del servicio son capaces de usar el protocolo con el cuales están familiarizados.

En la figura 47 y 48 se observa el esquema de trabajo seguido: el CE es conectado a la PE e intercambia las tablas de enrutamiento usando cualquier número del protocolo interno de enrutamiento (IRP), incluyendo Rip, OSPF, IBGP,

EIRGP. Las tablas de rutas son enviadas al más lejano final PEs vía BGP. En el más lejano final, los routers PE envían las tablas reenviadas a los routers CE.

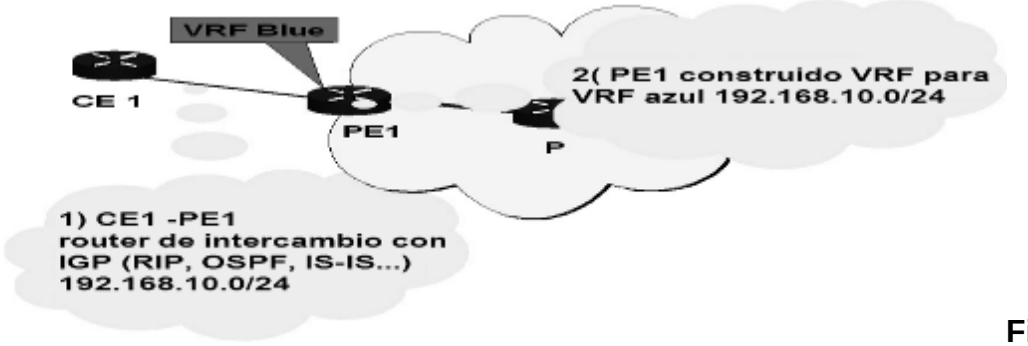


Figura 47 RFC 2547 intercambio de enrutamiento paso 1 y 2 *(fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)*

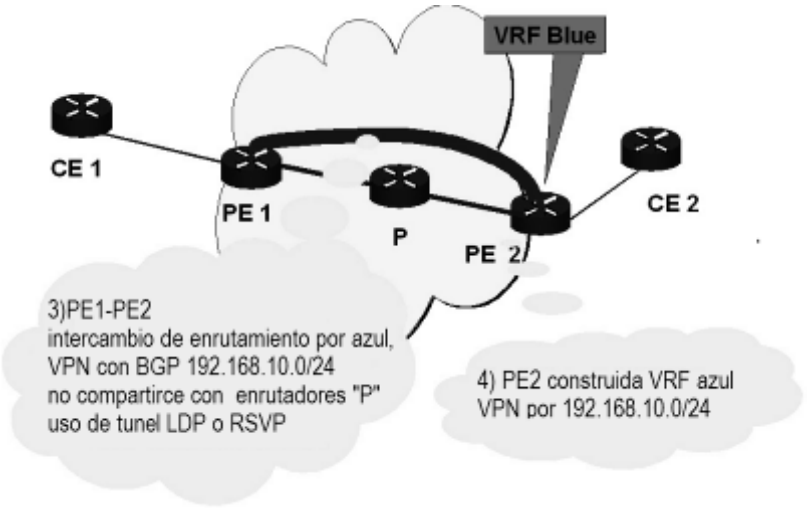


Figura 48. Intercambio de enrutamiento RFC 2547, pasos 3 y 4(fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

Un reto aparece cuando los sitios tienes una dirección IP interna (como lo permite RFC 1918). Para mantener estos separados, los PEs agregan un designador de rutas a la dirección IP como lo muestra la figura 49

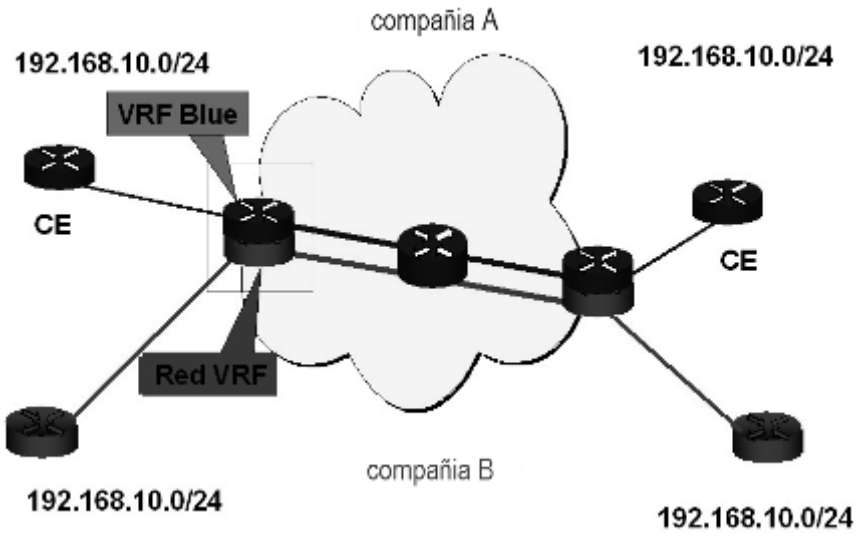


Figura 49. Dirección independiente IP(fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

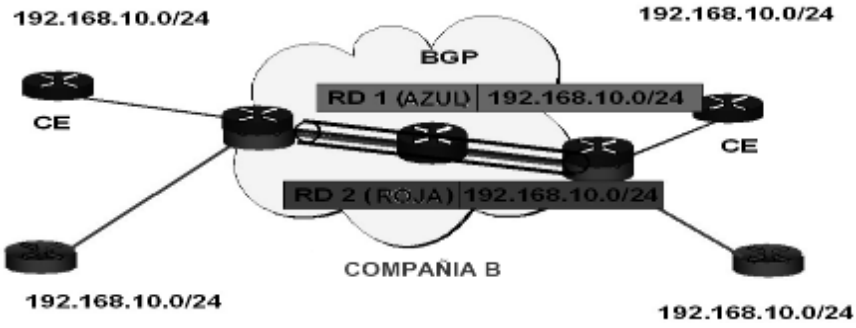


Figura 50. Dirección independiente con un designador de enrutamiento (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

El RFC 2547 ha ganado una aceptación grande en la comunidad. Sin embargo tiene dos grandes fallas,

- Las tablas de enrutamiento del consumidor están expuestas al proveedor de servicio.

- Desde que las conexiones que usan un caso de BGP se anuncian a través del núcleo, una falta de configuración podría producir una exposición de los datos de información.

6.6.9 Enrutamiento virtual

En esta versión de soluciones MPLS VPN, las interfaces Ethernet LANs hacia CE, que proveen un núcleo que actúa como un puente de capa-2. En VPLS, el núcleo MPLS puede conectar sitios bases por medio de punto a multipuntos. La CE en el lado de ingreso simplemente repasa la dirección de capa-2 y re-envía información a la CE en el lado de salida basado en el switche de capa do o las tablas de puente como se observa en la figura 51

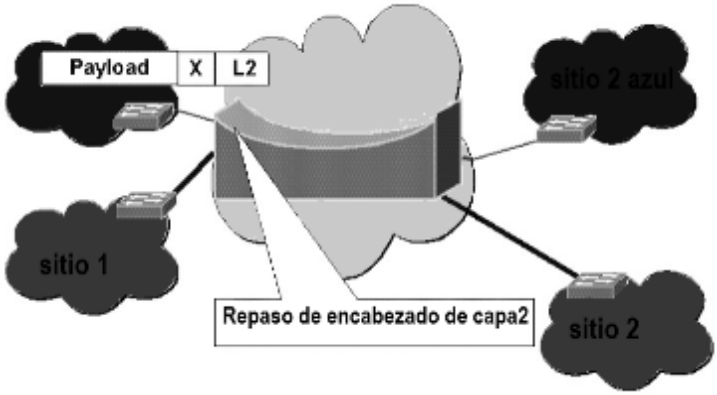


Figura 51. Red VPLS (fuente Multiprotocol Label Switching Architecture. Network Working Group)

Se puede observar que VPLS actúa como un gran puente. En este tipo de diseño de redes, se debe considerar la escalabilidad de los servicios de una LAN extendida y las desventajas de una red plana, sin embargo VPLS ofrece los avances de los ambientes de capo del switch.

6.6.10 VPNS de capa 2

Las empresas en el mercado constataron que la VPN de capa 3 reunió sólo una parte de las necesidades de los usuarios finales. De vuelta a los primeros días de la aplicación de MPLS, los primeros en adoptar la tecnología descubrieron que también existía una demanda del mercado de las VPNs de capa 2.

La VPN de capa 3 funcionó bien durante un número determinado de clientes, sin embargo, hubo un porcentaje significativo del mercado utilizando sistemas heredados y las redes para que una solución con VPN de capa 2 fuera más adecuada. Como no se identificaron estas necesidades, sugirieron diferentes arquitecturas para MPLS VPN de capa 2, Virtual Private incluyendo Wire Service (VPWS) y Virtual Private LAN Services (VPLS).

Refiriéndose al Árbol de VPN (Figura 52), podemos ver que hay varios tipos de VPN capa 2. En primer lugar, se ocupará de VPWS, VPLS, y IPL seguido por la tecnología de apoyo en cada categoría

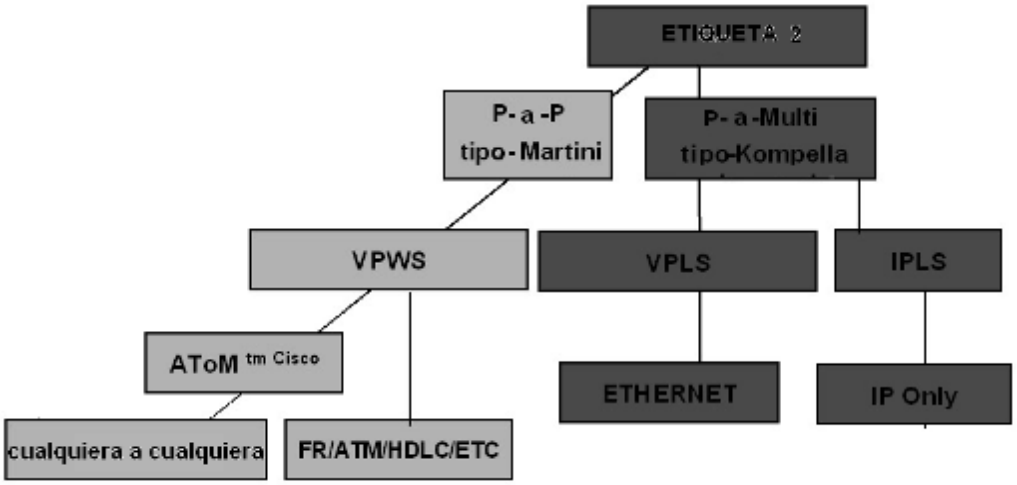


Figura 52.Arbol VPN (fuente Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching)

7 LABORATORIO SOBRE MPLS

El objetivo de la presente práctica es familiarizarse con la tecnología y los conceptos de MPLS (Multiprotocol Label Switching), así como su configuración en escenario de simulación.

Para el desarrollo de esta práctica se utilizó el simulador OpenSimMPLS 1.0[1], desarrollado en la Universidad de Extremadura ESPAÑA que funciona como un simulador de MPLS tradicional y permite comprobar el comportamiento de escenarios basados en tecnología de redes con calidad de servicio, como ATM e IP con la ventaja añadida de la garantía de servicio sobre MPLS mediante técnicas activas.

7.1 OPENSIMMPLS

Open SimMPLS es una aplicación cuya finalidad es la simulación de escenarios completos basados en redes MPLS con soporte para GoS[2] mediante técnicas activas con la que podemos recrear dichos escenarios y comprobar su comportamiento. Al estar escrita en Java, es una herramienta muy portable. Desde la sección de descargas de la web del proyecto se distribuye su código fuente completo, aunque también se distribuye en forma de aplicación standalone en un archivo JAR listo para su uso que se puede ejecutar desde una terminal de comandos dentro de una sesión gráfica:
java -jar openSimMPLS.jar &

El simulador trabaja en tres modos distintos con cada escenario:
Modo diseño: Donde se podrán hacer todas las labores de diseño de topologías y configuración de los elementos de red que se quieren simular.
Modo simulación: Donde se podrá realizar la simulación en tiempo real del funcionamiento de la red diseñada.
Modo análisis: Donde se podrán ver gráficas analíticas sobre lo que ocurre en la simulación.

[1] http://www.manolodominguez.com/projects/opensimmpls/
[2] GoS: Garantía de servicio

7.2 CREANDO UN ESCENARIO

Para crear un nuevo escenario de simulación por primera vez seleccionamos la opción Nuevo de la entrada Escenario, desde el menú principal. Aparece entonces una ventana en el área de trabajo con varias pestañas desde las que configurar y visualizar los diferentes elementos constituyentes de la simulación. Desde la pestaña de Diseño (ver Figura 53), que es la predeterminada al crear un nuevo escenario, editamos el aspecto y la configuración de la red que vamos a simular. Podemos insertar emisores de tráfico, receptores, LERs, LERs activos, LSRs, LSRs activos y enlaces.

Figura 53: Ventana de diseño Open SimMPLS *(Fuente propia)*

Siempre hay que crear un receptor antes de poder insertar un nuevo emisor. Desde la pestaña General podemos especificar el Nombre del Receptor e incluso la posición en que se ubicará el receptor en el escenario de simulación. Tras Aceptar la nueva configuración, podemos proceder a crear el nuevo emisor.

La pantalla de configuración del emisor es similar a la del receptor, excepto por la existencia de un menú desplegable desde el que se ha de seleccionar obligatoriamente el receptor al que va dirigido su tráfico. Desde la pestaña Avanzada de la pantalla de configuración del emisor se pueden definir las peculiaridades del tráfico generado, tales como la Tasa de Tráfico, especificada en una unidad de Megabits por segundo; el Tipo de Tráfico, que puede ser constante, por el cual el emisor genera paquetes de tamaño fijo y

siguiendo un período de tiempo también fijo, o de tipo variable, en cuyo caso el emisor genera paquetes de tamaño variable entre 0 y 65535 octetos siguiendo el modelo estadístico ofrecido por la red Abilene (ver cuadro titulado “Tamaños Medios”); el Tamaño de la carga útil, que sólo se puede configurar en caso de haber elegido un tráfico de tipo constante; Encapsular tráfico sobre MPLS, que si se activa, en vez de generar tráfico IPv4, el emisor genera tráfico MPLS etiquetado; Nivel de GoS, por el que se especifica el nivel de prioridad del tráfico del 1 al 3, siendo el 3 el de mayor prioridad; Crear LSP de respaldo, una casilla de verificación que nos permite especificar si deseamos que se nos procure un LSP alternativo; y por último, Generar estadísticas para este emisor, algo que no se recomienda utilizar a menos que haya que depurar un nodo en particular, ya que su uso genera una enorme carga sobre el simulador.

Un LER es un nodo encargado de tratar los paquetes IPv4 o MPLS para clasificarlos, establecer un camino hacia su destino a través del dominio MPLS, y permitir la entrada de dichos paquetes, una vez etiquetados, en el dominio. Al crear un nuevo LER se nos presenta la correspondiente pantalla de configuración. Desde la pestaña de configuración Avanzada podemos especificar parámetros como la Potencia de conmutación o el Tamaño de buffer de entrada.

Un LERA (Label Edge Router Activo) es similar a un LER, sólo que además de realizar las funciones de un LER regular, analiza además las cabeceras IPv4 de los paquetes para determinar el nivel de GoS de los mismos y codificarlo dentro de la cabecera MPLS. Si un tráfico con requerimientos de GoS accede a través de un LER regular, perderá sus atributos dentro del dominio MPLS. Desde la configuración Avanzada, a los parámetros del LER ordinario se suma el Tamaño de la DMGP, que es directamente proporcional a la probabilidad de que el paquete pueda servir a una petición de retransmisión de un paquete descargado en otro nodo de la red.

El LSR no es más que un conmutador de tráfico MPLS dentro del dominio, y los parámetros de la configuración Avanzada son similares a los del LER.

El LSRA (Label Switch Router Activo) cumple las mismas funciones que el LSR, excepto que además es capaz de almacenar temporalmente y recuperar paquetes activos, así

como de reestructurar caminos en un entorno local. Los parámetros de la configuración Avanzada son similares a los de un LERA.

Para crear un enlace hay que especificar en la configuración General los elementos que se situarán en sendos extremos, siguiendo la lógica de la topología de la red. Por ejemplo, sería absurdo tratar de conectar directamente un Emisor a un Receptor, por el contrario, hay que conectar siempre un Emisor a un LER o un LERA. Otro parámetro configurable de los elementos de tipo enlace es el Retardo, que se puede especificar desde la pestaña de configuración Avanzada del elemento.

7.3 SIMULANDO

Una vez creado el escenario de simulación, vamos a la pestaña Simulación que aparece junto a un icono en forma de reloj en la ventana del nuevo escenario, y pulsamos sobre el único icono que aparece habilitado en un primer momento (con forma de engranaje). Se podrá ver entonces cómo los nodos emisores generan el tráfico, que fluye hacia los nodos receptores correspondientes siguiendo la configuración especificada.

En la web oficial del proyecto se pone a disposición del usuario un paquete comprimido con varios archivos de simulación pre-elaborados, en los que se recrean varias situaciones que podrían darse en una red MPLS real y para las que nos gustaría estar preparados.

Tras descargar y descomprimir los archivos se crea un directorio packdeejemplo1_0, que contiene los archivos de escenario de ejemplo, de extensión .osm.

Para cargar uno de estos escenarios, seleccionamos Abrir desde la opción Escenario del menú principal y elegimos el archivo .osm desde el navegador de archivos que se abre. Si, por ejemplo, seleccionamos el archivo TodosLosTraficos. osm, la aplicación abrirá en el área de simulaciones el correspondiente escenario (ver Figura 54). En él hay definidos inicialmente tres emisores con requerimientos de GoS, con niveles de prioridad que van desde el uno hasta el tres, un emisor sin requerimientos de Gos, tres LERAs que hacen de puntos de entrada para los emisores con requerimientos de GoS, un LER para el

emisor sin requerimientos de GoS, dos LSRs activos, un LSR ordinario, otro LER para conectar el receptor, y una serie de enlaces.

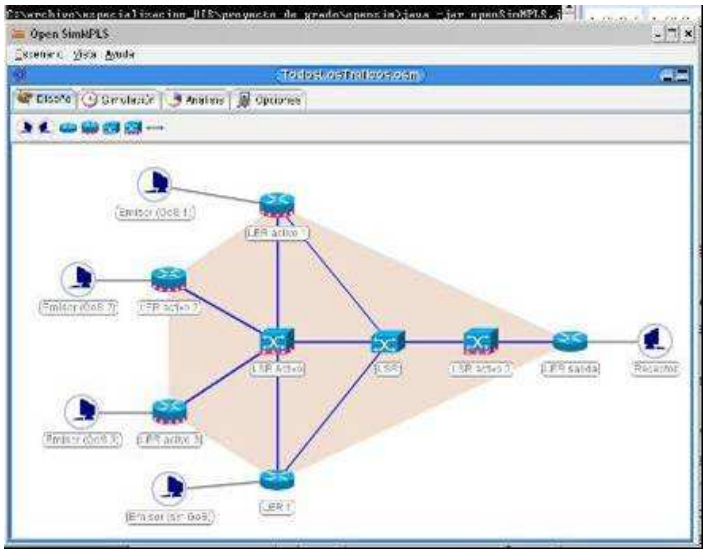


Figura 54: Escenario de ejemplo. TodosLosTraficos.osm *(Fuente propia)*

Al iniciar la simulación se puede ver cómo se organiza el tráfico para llegar en orden de prioridad al receptor (Figura 55). Si pulsamos sobre el enlace que une el primer LSRA al primer LSR ordinario, provocamos la simulación de una eventual caída del enlace y vemos cómo todo el tráfico se reenvía a través del LER de entrada del emisor que no tiene requerimientos de GoS, demostrándose así la eficacia del protocolo y el funcionamiento del soporte de GoS incluso con enlaces caídos y usando caminos alternativos.

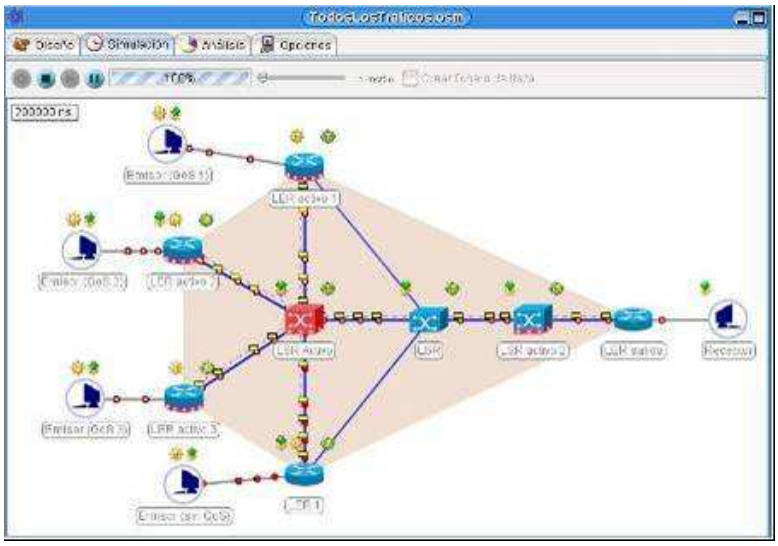


Figura 55: Simulación del escenario TodosLosTraficos.osm *(Fuente propia)*

Como conclusión de la simulación, MPLS puede proporcionar los mecanismos necesarios para la resolución de la mayoría de los problemas de red más apremiantes. El soporte de GoS sobre MPLS es una de garantía de servicio de clientes de ISPs y de grandes redes privadas o corporativas, así como para la transmisión de flujos de datos multimedia o comunicaciones “en tiempo real”. Open SimMPLS ha demostrado también ser una herramienta de simulación muy útil y de fácil uso.

El proceso de simulación a través OpenSimMPLS refuerza el aprendizaje de los autores gracias a ejemplos prácticos, ya que el simulador ofrece resultados sobre el comportamiento de la red cuando se introducen servicios particulares; por ejemplo, tráfico multimedia. También permite contrastar resultados gracias al sistema de reconfiguración de los elementos del dominio. De esta forma el alumno puede realizar propuestas para la mejora de supuestos de redes MPLS y detectar los posibles efectos perniciosos o beneficiosos sobre el tráfico.

OpenSimMPLS ofrece un sistema de aprendizaje por descubrimiento en el que se introduce al alumno a resolver problemas y situaciones, aprender procedimientos de la tecnología, llegando a entender las diferentes características de los eventos

y decidiendo cómo controlarlos y qué acciones realizar en situaciones particulares, gracias a la interactividad que admite la herramienta durante la simulación. Se puede emplear OpenSimMPLS de forma que el alumno se trace hipótesis basadas en su experiencia y conocimientos teóricos acumulados, a modo de síntesis o repaso de lo que ya ha estudiado. Tiene la posibilidad de poner en práctica sus ideas.

En resumen, el uso del simulador da lugar a un proceso de doble feedback: Por un lado la interacción con la simulación en ejecución permite al estudiante analizar el comportamiento del escenario MPLS, obteniendo conclusiones basadas en sus conocimientos teóricos previos y detectando así posibles problemas de la fase de diseño del escenario. Por otro lado, tras el análisis de los resultados estadísticos el alumno también puede obtener conclusiones que redundarán en nuevos cambios de configuración. Este proceso experimental y analítico de refinamientos sucesivos motiva al alumno a desarrollar sus propias estrategias de pensamiento acerca del funcionamiento de la tecnología MPLS.

8 ANÁLISIS DE TRÁFICO SOBRE LA RED DE COPETRAN LTDA

Actualmente la red de área extendida de COPETRAN cubre gran parte del territorio Nacional con 260 sucursales, de los cuales 7 son enlaces MPLS.

Con la actualización del software de cada una de las áreas de negocio de la empresa (Giros de Dinero, Carga y Pasajes), la implementación de sistemas de voz IP y el cambio en los modelos de capacitación pasando de modelos presenciales a modelos virtuales a través de videoconferencia, la empresa empezó a experimentar problemas en el enrutamiento del tráfico y de frente al usuario se empezó a experimentar demora en el acceso a los aplicativos misionales que funcionan bajo ambiente Web.

En vista de lo anterior se revisó con cada uno de los proveedores de acceso la forma de realizar priorización de tráfico evitando la latencia en el acceso a las aplicaciones; se obtuvo por parte de la empresa ETB la implementación de MPLS como alternativa de solución a esta problemática.

Para el análisis de tráfico el proveedor de servicios le suministra a la empresa la herramienta MRTG (Multi Routing Traffic Grapher) que proporciona información de la monitorización del tráfico sobre enlaces de red con ayuda del protocolo snmp. Esta aplicación realiza recolección de muestras cada x minutos y genera reportes de tráfico entrante/saliente pico, promedio y mínimo.

En la salida del nodo principal de COPETRAN LTDA, no existen redundancias y se tenía una sobreoferta de la capacidad real de la red. Por este motivo, cuando uno de los clientes[1] generaba un tráfico excesivo se requería reenrutar al resto para que no presenten en sus enlaces tiempos promedios elevados y degradación del canal. Al implementar MPLS en la red de datos e incrementar el Ancho de

[1] Hace referencia a un PC conectado a la red MPLS de la empresa COPETRAN.

banda de la salida principal se consiguió una mejora considerable en los tiempos de respuesta de las aplicaciones. Actualmente, con el diseño de red implementado sobre MPLS, el canal de datos no registra saturación como se observa en las siguientes gráficas.

Figura 56: Gráfico diario MRTG canal principal COPETRAN.

Fuente: COPETRAN LTDA

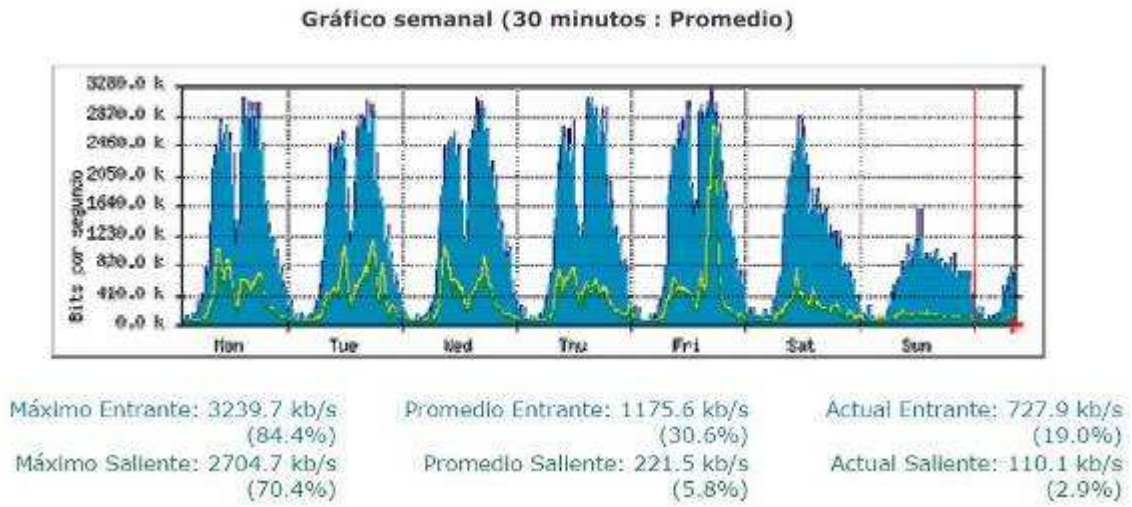


Figura 57: Gráfico semanal MRTG canal principal COPETRAN. Fuente: COPETRAN LTDA

Figura 58: Gráfico anual MRTG canal principal COPETRAN. Fuente: COPETRAN LTDA

Como se puede ver en la red implementada en la actualidad con MPLS, el tráfico ni siquiera alcanza el ancho de banda contratado con el proveedor, así como

tampoco se observa saturación en el canal de principal. Esto deja ver que a pesar que la cantidad de tráfico se mantiene, la tecnología MPLS brinda la posibilidad de unificar múltiples plataformas y mantener requerimientos de diversos clientes para prestación de multiservicios.

MPLS es una herramienta efectiva para esta aplicación en un backbone, ya que permite al administrador establecer rutas explícitas, obtener datos estadísticos de uso LSP usadas para planificación de la red y análisis de cuellos de botella y carga de enlaces, y por último, hacer enrutamiento restringido, de modo que el administrador puede determinar rutas para servicios especiales. Se utiliza el protocolo IT-RSVP que permite reservar ancho de banda.

Finalmente, si COPETRAN comienzan un proceso de convergencia de tecnologías y unificación de sus respectivas redes a nivel nacional, ya que en la mayoría de puntos existen dependencias de todas las filiales, con el fin de unir recursos técnicos y humanos para extender puntos de cobertura; el diseño MPLS propuesto por el proveedor mantendría la independencia de tráfico, satisfaciendo los niveles de calidad de servicio requeridos por sus aplicativos.

En el anexo 1 se presenta los gráficos de las mediciones del uso de los enlaces para las principales sucursales de COPETRAN LTDA

En el anexo 2 se describe la infraestructura de red actual de COPETRAN LTDA

9 CONCLUSIONES

- El presente trabajo es una actualización en las soluciones de última milla como herramienta de estudio para los estudiantes de la Especialización en Telecomunicaciones de la Universidad Industrial de Santander, dando una base no solo teórica si no también mostrando una aplicación real en la empresa COPETRAN LTDA, en la cual se observan los beneficios reales en esta red y generando un proceso de aprendizaje al lector desde la parte teórica a la parte aplicativa.

- La adopción de MPLS por parte de la empresa COPETRAN a través de sus proveedores de telecomunicaciones le ha permitido mejorar el servicio a sus clientes internos ofreciendo calidad de servicio, priorización de tráfico, seguridad y eficiencia.

- MPLS puede proporcionar los mecanismos necesarios para la resolución de la mayoría de los problemas de red más apremiantes. El soporte de QoS sobre MPLS mediante técnicas activas es una de las posibles soluciones a los requerimientos de garantía de servicio de clientes de ISPs y de grandes redes privadas o corporativas, así como para la transmisión de flujos de datos multimedia o comunicaciones “en tiempo real”. Open SimMPLS ha demostrado también ser una herramienta de simulación muy útil y de fácil uso.

- Existen muchas tecnologías que soportan calidad de servicio, para poder proporcionar anchos de banda distintos, dar privilegios, calidad de servicio, pero en realidad MPLS es una solución que satisface todas las necesidades implicadas en el mundo de las telecomunicaciones hoy en día.

- El monitoreo eficiente y continuo de la infraestructura tecnológica de una empresa permite además de llevar un control adecuado de aplicativos, servicios, servidores y equipos de interconectividad, el tomar medidas

correctivas con el fin de mantener constante el rendimiento de la misma, adecuarse de manera rápida a las nuevas necesidades y cambios de la empresa, así como también contribuye a tener el Costo total de propiedad lo más bajo posible.

- MPLS es un esquema de reenvió independiente de la tecnología de Capa 3 y de la Capa 2 del modelo de referencia OSI, lo cual facilita que se pueda usar las tecnologías existentes mientras se migra a otras; Gracias a su estructura de pila de etiquetas es fácil construir jerarquías de dominios globales. Además de lo anterior presenta las siguientes ventajas:

  - Permite aplicar tendencia de ingeniería de trafico con lo cual la red deja de ser un elemento de trasporte y se vuele más versátil.
  - Permite usar cualquier protocolo de distribución de etiquetas Tradicional.
  - El modelo de puertos es un gran avance tecnológico que pone a MPLS-VPN en una categoría diferente a sus predecesores
  - Ofrece caminos virtuales con QoS y ancho asegurado.
  - Proporciona una conmutación en base a etiquetas rápida y eficiente, no encapsula las tramas de red, y esta etiqueta no afecta sus propiedades.
  - Proporciona Mecanismos eficientes para el establecimiento de túneles.

10 REFERENCIAS BIBLIOGRÁFICAS

- MPLS "Multiprotocol Label Switching": Una Arquitectura de Backbone para la Internet del Siglo XXI. María Sol Canalis. Departamento de Informática. Universidad Nacional del Nordeste. Corrientes. Argentina

- MPLS: Convergencia entre el Nivel de Transmisión y el Nivel de Enrutamiento. Ana González. Publicado en la Revista Antena de Telecomunicación, Diciembre 2002.

- CCNA Cisco Certified Network Associate Study Guide, 4th Edition (640-801) by Todd Lammle, Sybex.

- Rick Gallaher's MPLS Training Guide—Building Multi Protocol Label Switching Networks, ISBN:1932266003, Syngress Publishing © 2003 (301 pages).

- Guia de estudio del curso para la certificación CCNP de CISCO, CISCO MULTIPROTOCOL LABEL SWITCHING (MPLS)

ANEXO 1

Ver archivo que contiene el anexo 1: graficas MRTG Copetran.pdf

ANEXO 2

Ver archivo que contiene el anexo 2: anexo 2 red copetran.pdf