MPLS SOBRE REDES METROETHERNET

SULAY DEL CARMEN PEREIRA CONTRERAS

ANTONIO SEGUNDO SOTOMAYOR SOLANO

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

PROGRAMA ESPECIALIZACION EN TELECOMUNICACIONES

CARTAGENA DE INDIAS, D.T Y C

2010

MPLS SOBRE REDES METROETHERNET

SULAY PEREIRA CONTRERAS
ANTONIO SEGUNDO SOTOMAYOR SOLANO

MONOGRAFÍA PRESENTADA COMO REGISTRO DE APROBACIÓN DE LA ESPECIALIZACION EN TELECOMUNICACIONES

DIRECTOR
GONZALO LOPEZ
INGENIERO ELECTRÓNICO
ESPECIALISTA EN TELECOMUNICACIONES

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
PROGRAMA ESPECIALIZACION EN TELECOMUNICACIONES
CARTAGENA DE INDIAS, D. T. Y C
2010

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

FIRMA DEL PRESIDENTE DEL JURADO

_____

FIRMA DEL JURADO

_____

FIRMA DEL JURADO

CARTAGENA, ENERO 21 DE 2010

SEÑORES

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

LA CIUDAD

APRECIADOS SEÑORES:

Por medio de la presente me permito informarles que la monografía titulada "**MPLS SOBRE REDES METROETHERNET**" ha sido desarrollada de acuerdo a los objetivos establecidos.

Como autor del proyecto considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

ATENTAMENTE,

_____

SULAY DEL CARMEN PEREIRA CONTRERAS

CARTAGENA, ENERO 21 DE 2010

SEÑORES

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

LA CIUDAD

APRECIADOS SEÑORES:

Por medio de la presente me permito informarles que la monografía titulada "**MPLS SOBRE REDES METROETHERNET**" ha sido desarrollada de acuerdo a los objetivos establecidos.

Como autor del proyecto considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

ATENTAMENTE,

_____

ANTONIO SEGUNDO SOTOMAYOR SOLANO

CARTAGENA, ENERO 21 DE 2010

SEÑORES

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

LA CIUDAD

APRECIADOS SEÑORES:

Por medio de la presente me permito informarles que la monografía titulada "**MPLS SOBRE REDES METROETHERNET**" ha sido desarrollada de acuerdo a los objetivos establecidos.

Como director del proyecto considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

ATENTAMENTE,

_____

GONZALO LOPEZ
INGENIERO ELECTRONICO
ESPECIALISTA EN TELECOMUNICACIONES

AGRADECIMIENTOS

LOS AUTORES EXPRESAN SUS AGRADECIMIENTOS A:

A nuestro director de monografía, GONZALO LOPEZ

Por su constante colaboración y apoyo durante el desarrollo de la monografía.

CONTENIDO

LISTA DE FIGURAS

Pág.

GLOSARIO

Acrónimos

ATM. Asynchronous Transfer Mode. *Modo de Transferencia Asincrona.*

CE. Customer Equipamnet. *Equipo del lado del Cliente.*

CD. Collision Detection. Detección de Colisión.

CSMA. Carrier Sense Multiple Access. *Acceso Múltiple por Detección de Portadora.*

DWDM. Dense Wavelength Division Multiplexing. *Multiplexación por división en longitudes de onda densas.*

EVC. Ethernet Virtual Connection. *Conexión Virtual Ethernet.*

IEEE. Institute of Electrical and Electronics Engineers. *Instituto de Ingenieros Electricos y Electronicos.*

IP. Internet Protocol. *Protocolo de Internet.*

ISO. International Organization of Standardization. Organización Intarnacional para la Estandarización.

LAN. Local Area Network. Red de Área Local.

MAN. Metropolitan Area Network. *Red de Área Metropolitana.*

MEN. Metro Ethernet Network. Red Metro Ethernet.

MPLS Multiprotocol Label Switching. *Multiprotocolo de Conmutación de Etiquetas.*

QoS. Quality of Service. *Calidad de Servicio.*

SDH. Synchronous Digital Hierarchy. *Jerarquia Digital Sincrona.*

SONET. Synchronous Optical Network. *Red Óptica Síncrona.*

TDM. Time Division Multiplexing. *Multiplexación por División de tiempo.*

UNI. User Network Interface. *Interfaz de Red de Usuario.*

VLAN. Virtual Local Area Network. *Red de Área Local Virtual.*

VPN. Virtual Private Network. *Red Privada Virtual.*

WAM. Wide Area Network. *Red de Área Extensa.*

INTRODUCCIÓN

En el mundo tecnológico los crecimientos en las tecnologías de han dado a pasos muy agigantados como en la trasmisión de datos o Internet la cual ha cambiado significativamente el mundo de las personas que la manejan. Hoy por hoy es posible contar con servicios estables, rápidos eficientes y multificuncionales como la integración de voz, dato y video todo al alcance del usuario a un precio muy cómodo creando una expansión cada día mas notable.

Cuando en el año de 1973 se invento un sistema de red para la primera impresora láser del mundo estaban lejos de creer que el protocolo que se estaba creando conocido luego como Ethernet, llegaría a ser el protocolo dominante del siglo XXI de las redes de Área Local (*LAN*). Pero tal vez más lejos aún se estaba de pensar que este protocolo podía llegar a tener éxito como el nuevo paradigma de las Redes de Área Metropolitana (*MAN*).

Sin embargo se empezaron a trabajar las Redes de Área metropolitana Basadas en Ethernet (*MEN*) los requerimientos para la transmisión de voz, datos y video se han ajustado de una manera transparente y rápida a las necesidades de los usuarios. La posibilidad de que un hogar o empresa pueda tener Internet 24x7, telefonía y TV todo a través de un mismo servicio actualmente ya es posible gracias a las redes Metropolitanas Ethernet.

Es posible que las tecnologías como Metro Ethernet, vayan a cambiar la cara al servicio de las Telecomunicaciones. Muy pronto será posible tener en cada uno de nuestros hogares un servicio unificado de telefonía, Internet a alta velocidad y TV por IP, todo a través de un simple dispositivo.

La era de la integración de las aplicaciones no es el futuro sino el presente. Actualmente, el crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y más sofisticados servicios, supone cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas a mitad de los años 90. Nuevas tecnologías de transmisión sobre fibra óptica, tales como Dense Wavelength Division Multiplexing (*DWDM*), proporcionan una eficaz alternativa al ATM para multiplexar varios servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de routers con funciones especializadas en el transporte de paquetes en el núcleo de las redes.

Esta situación se complementa con una nueva arquitectura de red de reciente aparición, conocida como Multi Prototocol Label Switching (*MPLS*). MPLS se considera fundamental en la construcción de los nuevos cimientos para la Internet del presente siglo. El IETF (*Internet Engineering Task Force*) establece el grupo de trabajo **MPLS (*MultiProtocol Label Switching*)** para producir un estándar que unificase las soluciones propietarias de conmutación de nivel 2.

El resultado fue la definición del estándar conocido por MPLS, recogido en la RFC 3031. MPLS proporciona los beneficios de la ingeniería de tráfico del modelo de IP sobre ATM, pero además, otras ventajas; como una operación y diseño de red más sencillo y una mayor escalabilidad. Por otro lado, está diseñado para operar sobre cualquier tecnología en el nivel de enlace, no únicamente ATM, facilitando así la migración a las redes ópticas de próxima generación, basadas en infraestructuras SDH/SONET y DWDM.

La diferencia fundamental entre la arquitectura MPLS y las tecnologías WAN (*Wide Área Network*) es la manera de asignación de las etiquetas y la capacidad de transportar las etiquetas, abriendo la posibilidad para aplicaciones de Ingeniería de Tráfico y un enrutamiento más rápido en caso de presentarse fallas en los nodos.

MPLS busca agrupar las diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes. Según el énfasis o interés que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como:

- Un suplente de la conocida arquitectura IP sobre ATM.
- Un protocolo para hacer túneles.
- Técnica para acelerar el encaminamiento de los paquetes.

MPLS integra las características claves de la capa 2 y capa 3 del modelo ISO/OSI, además no está limitado a ningún protocolo de la capa 2 o 3. En el

enrutamiento tradicional, un paquete se direcciona salto a salto. Es decir, cada vez que ese paquete llega a un enrutador tiene que revisar rutas basadas en la dirección de destino de la capa 3 incluida en el encabezado del IP (Internet Protocol). Esto es necesario cada vez para determinar el siguiente salto en su trayecto hasta llegar a su destino final.

MPLS esta destinado a solucionar los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes. Pero ante todo esto, debemos considerar MPLS como un avance más reciente en la evolución de las tecnologías de enrutamiento y forwading en redes IP, lo que implica una nueva manera de pensar a la hora de construir y gestionar estas redes.

CAPITULO 1

Problema de Investigacion

1.1 PLANTEAMIENTO DEL PROBLEMA

1.2 OBJETIVOS

1.3 JUSTIFICACION

1.1 PLANTEAMIENTO DEL PROBLEMA

Ante la nueva y creciente presencia de aplicaciones y servicios de nueva generación cada vez es mas resultante el acercamiento de la banda ancha a los clientes, conviene por lo tanto emigrar las tecnologías Ethernet de las redes LAN y las redes MAN y mejorar las redes IP con la implementación de (Multi-Protocol Label Switching) MPLS. Esta es una solución clásica y estándar para el transporte de información en las redes metropolitanas, tratando de realizar una convergencia de redes que sea aceptada en la comunidad de la Internet y dando una solución aceptable para el envió de información, con ciertas garantías.

Un gran número de operadores de tecnología ya están familiarizados con estas, sin embargo lo interesante es combinarlas para llevar Ethernet a cualquier ubicación y quien más que MPLS. Con este acoplamiento se puede dar el aumentando de los numerosos beneficios de Ethernet, con las múltiples capacidades de fácil aprovisionamiento de las, SLTs (Servicios LAN transparentes) y QoS (Calidad de Servicio) garantizadas de extremo a extremo.

MPLS es una tecnología que permite enrutar y conmutar tráfico heterogéneo en redes de gran complejidad muy eficientemente. Reduce el Overhead IP y resuelve los problemas de manejo de rutas de las grandes redes además ofrece la potencia y escalabilidad de los túneles IP y permite aprovisionar de

manera dinámica los túneles MPLS, conocidos como LSPs (Label Switched Paths). Los LSPs pueden ser empleados para proporcionar QoS y establecer grupos de usuarios privados, además de garantizar los SLAs comprometidos. Debido a que la información de forwarding de MPLS está separada del contenido de la cabecera IP, puede trabajar junto con otros mecanismos de routing y mejorar así sus prestaciones y los de la red.

La unión de Ethernet con MPLS se podría definir casi como el matrimonio perfecto. MPLS mejora las funciones de Ethernet sin afectar a todo lo bueno de éste. EoMPLS (Ethernet over MPLS) implica dotar a una tecnología de Nivel 2 de capacidades de Nivel 3. MPLS aporta las capacidades orientadas a conexión que necesita Ethernet, centrada en el transporte, creando así servicios complejos con posibilidades de SLAs. Cuando se utiliza EoMPLS para dar SLTs, cada VLAN es mapeada a un LSP que se extiende a lo largo de la red. Cada LSP puede ofrecer ancho de banda reservado, y todos los mecanismos de seguridad, ingeniería de tráfico y QoS disponibles.

Una red con MPLS es capaz de dar la baja latencia y los caminos de tráfico garantizados para que el tráfico multiservicio reciba el tratamiento especial que requiere por sus características únicas de transmisión. Para que una red IP sea considerada multiservicio debe ser capaz de acomodar al menos el tráfico de voz y vídeo. Estas aplicaciones no pueden sufrir grandes retrasos y sus paquetes no pueden ser ordenados. Combinando estas tecnologías los operadores pueden ofrecer una cantidad de ancho de banda garantizada de

extremo a extremo, y además si es necesario añadir ancho de banda cuando esté disponible. Esto les permite sobrescribir con seguridad, obteniendo mejores beneficios sin poner en peligro los SLAs acordados. Además, se puede ofrecer balanceo de carga entre distintos LSPs y backup del LSP primario con las condiciones deseadas. De esta manera al cliente se le asegura la elasticidad y recuperación del servicio que desea y está dispuesto a pagar.

En definitiva, posiblemente esta tecnología facilite el despliegue de las redes de banda ancha a corto y medio plazo.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

El objetivo del proyecto es una investigación de convergencia de dos tipos de tecnología multi-Protocol Label Switching (MPLS) sobre las redes Metro Ehternet.

1.2.2 OBJETIVOS ESPECÍFICOS

- Analizar las redes Metro Ethernet y mirar su convergencia con la tecnología MPLS.

- Describir los componentes fundamentales y arquitectura de MPLS.

- Describir los Servicios y Aplicaciones de las redes MPLS y Metro Ethernet

1.3 JUSTIFICACION

Ethernet es el tipo de red más usado en el mundo, gracias a su simplicidad y gran capacidad de ancho de banda unido esto a el alto rendimiento en conmutación y enrutamiento, más los mecanismos avanzados de QoS para soportar tráfico en tiempo real de voz y vídeo, la sitúa en una posición privilegiada para dar el salto a las redes MAN es por esto que este tipo de convergencia busca ofrecer a los clientes servicios de datos nativos a través de Ethernet en lugar de líneas arrendadas, además los clientes se sienten atraídos por estos servicios por parte de la flexibilidad que se ofrece a un bajo costo del ancho de banda, y el hecho de que estos servicios pueden ser rápidamente abastecido con facilidad.

A esto se le incluye la integración del multi-Protocol Label Switching (MPLS). El cual se está abriendo paso a una tecnología de red central unificada además de esta red MPLS, le da un valor añadido tales como ingeniería de tráfico, protección de redes, ancho de banda y QoS entre otros que pueden convertirse en una red de alto rendimiento y de alta demanda.

Una de las principales ventajas de la Multi-Protocol Label Switching (MPLS) es que permite a los proveedores de servicio de metro (PE) ofrecer nuevos servicios que no podían ofrecer antes tan fácilmente con el apoyo de las técnicas convencionales de enrutamiento IP.

Con MPLS el enrutamiento IP tradicional se apoya mas en la destinacion del reenvió basándose en la separación de los componentes de control del componente de reenvió. MPLS es diseñado con la capacidad de evolucionar sin tener que cambiar su funcionalidad de control del mecanismo de reenvió. Con esta flexibilidad recién adquirida por MPLS, se posiciona para apoyar el despliegue de un mayor control y capacidad de transmisión que se requiere en el valor añadido y de servicio de metro altamente rentables, tales como la ingeniera de trafico (TE), las clases de servicio (CoS), redes privadas virtuales (VPN), las líneas virtuales (VLLs), y los servicios de LAN privadas (VPLS). MPLS proporciona un conjunto de construcciones de gran alcance que permiten a los SP de metro de conquistar todos los retos que se propongan.

CAPITULO 2

Redes Metroethernet

2.1. CARACTERÍSTICAS DE UNA RED METRO ETHERNET

2.2. DESCRIPCIÓN DEL SERVICIO METROPOLITANO ETHERNET

2.3 TIPOS DE SERVICIO Y SU DEFINICIÓN EN UNA RED METRO ETHERNET

2.3.1 Conexión Virtual Ethernet EVC (Ethernet Virtual Connection)

2.3.2 Servicio Punto a Punto (E-Line)

2.4 CLASES DE SERVICIOS (COS)

2.5 SERVICIO DE MULTIPLEXACIÓN

2.1. CARACTERÍSTICAS DE UNA RED METRO ETHERNET

En el año de 1.974 los ingenieros Robert M. Metcalfe y David R. Boggs diseñaron en el Centro de Investigaciones de XEROX Corporation en Palo Alto (California, Estados Unidos) una red basada en el protocolo CSMA/CD, la cual operaba a una velocidad de transferencia de 2.94 Mbit/s, permitía conectar hasta 100 computadores a lo largo de un bus de 1 Kilometro de longitud, los cuales compartían archivos e impresoras. Después de un tiempo las compañías DIGITAL (DEC), INTEL y XEROX conforman la alianza DIX, con la cual proponen el estándar de conectividad local llamado ETHERNET, operando a una velocidad de transferencia de 10 Mbit/s.

Ethernet fue adoptada por **el Instituto de Ingenieros Eléctricos y Electrónicos** y estandarizada como IEEE 802.3. Este estándar fue publicado por primera vez en el año de 1985.

Ethernet ha dominado las redes de área local “LAN” debido a características tales como:

- Bajos costos en la implementación de la infraestructura, mantenimiento e incluso en la configuración debido a solamente es necesario conectar los equipos a la red sin la necesidad de realizar configuraciones avanzadas.

- Flexibilidad al momento de ampliaciones en la red.
- Gran variedad de velocidades de transmisión en el rango comprendido entre 10Mbps y 10Gbps.
- Facilidad de interconexión con otras redes debido a que la mayoría de las redes LAN están implementadas en Ethernet, por lo cual no es necesario realizar conversión de protocolos entre LAN y MAN, facilitando la integración entre las dos redes.

Pero debido a sus limitaciones técnicas en comparación con tecnologías tales como ATM y FRAME RELAY, Ethernet se quedo confinada en el entorno de las redes LAN; sus principales desventajas ante estas tecnologías fueron:

- La distancia cubierta por la red Ethernet utilizando cable de cobre solo alcanza los 100 metros antes de comenzar a degradarse la transmisión.
- Los mecanismos utilizados por la redes Ethernet para garantizar la fiabilidad y redundancia eran lentos e ineficientes.
- La capacidad de crecimiento era considera como limitada debido los broadcast, la necesidad del aprendizaje de las direcciones MAC de todos los equipos conectados a este tipo de redes.
- La seguridad era muy deficiente debido a que es una tecnología considerada de medio compartido, por tal razón los usuarios podían acceder al tráfico de otros.

Sin embargo debido a las ventajas ofrecidas por Ethernet los organismos de estandarización y los fabricantes realizaron investigaciones cuyo resultado hoy en día proporciona a Ethernet las herramientas tecnológicas necesarias para superar las limitaciones tecnológicas mencionadas anteriormente. Permitiéndole recorrer cientos de kilómetros sin que se degrade la transmisión debido a las tecnologías ópticas, excelentes soluciones de fiabilidad y redundancia, crecimiento de las redes Ethernet en varios órdenes de magnitud, además, seguridad y separación entre usuarios fue reforzada a través de tecnologías de tunelización.

Adicionalmente fue creado el organismo MEF, el cual se encarga de definir a Ethernet como un servicio metropolitano.

2.2. DESCRIPCIÓN DEL SERVICIO METROPOLITANO ETHERNET

El modelo básico de un servicio metropolitano Ethernet consta de tres partes:

- El dispositivo instalado del lado del usuario
- La interfaz de conexión del usuario a la red.
- La Red Metropolitana conocida como Metro Ethernet Network (*MEN*).

Es posible tener múltiples UNIs conectadas a la MEN de una simple localización. Los servicios pueden soportar una variedad de tecnologías y protocolos de transporte en la MEN tales como SONET, DWDM, MPLS, etc.

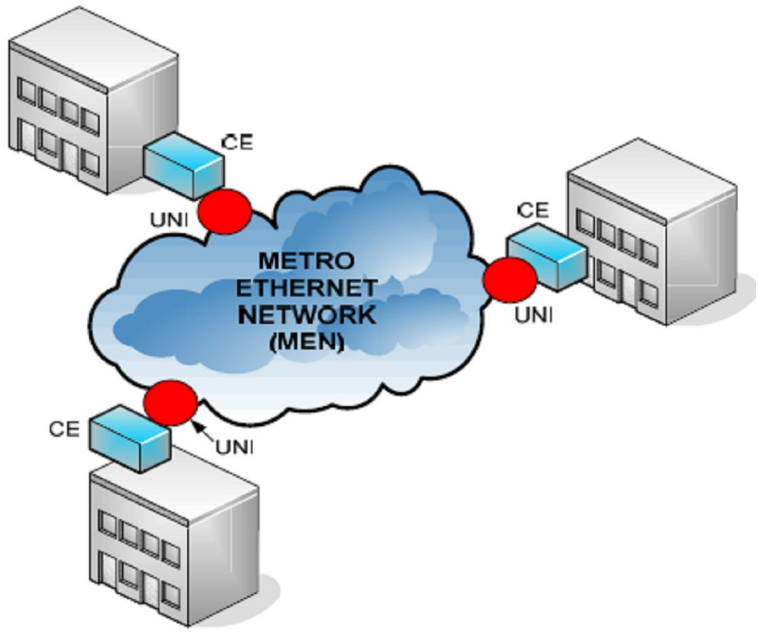


Figura 1. Ubicación del CE, UNI en una Metro Ethernet Network (MEN)

La primera diferencia notable con las típicas conexiones de una empresa hacia una nube metropolitana no basada en Ethernet es el UNI. Atrás quedaron los tiempos en que para conectarse entre las sucursales de una empresa o para conectarse a Internet era necesario utilizar conexiones sincrónicas mediante modems o codecs (*usando últimas millas de cobre o radio microondas*). El UNI definido por Metro Ethernet es el conocido puerto Ethernet RJ45 (*o también un puerto de fibra óptica*) usado por la mayoría de redes de área local hoy en día.

Es decir que un proveedor de red Metro Ethernet llega hacia sus usuarios con un cable de red, tal como si fuese a conectar otro PC más en su LAN.

La segunda diferencia con respecto a otras redes de área metropolitana es la diversidad del tipo de CE que puede conectarse a la red. Se puede usar los conocidos ruteadores para conectar las redes LAN entre la casa matriz y las sucursales o se puede simplemente interconectar los switches de las respectivas LAN (*ubicadas geográficamente en sitios distantes*). El proveedor de la red Metro Ethernet debe garantizar en cualquiera de los dos casos que los datos viajen de manera segura e independiente del resto del tráfico de usuarios dentro de la red Metro Ethernet.

2.3 TIPOS DE SERVICIO Y SU DEFINICIÓN EN UNA RED METRO ETHERNET

En la Red Metro Ethernet se pueden dar dos tipos de servicios diferentes:

- E-lines.
- E-LANs.

Las E-lines son conexiones punto-a-punto, mientras que las E-LANs son conexiones multipunto-a-multipunto (*any-to-any*). Adicionalmente se ha creado un tercer concepto llamado Ethernet Virtual Connection (*EVC*) que es definido como la instancia de asociación entre dos o más puntos de la red Metro Ethernet. Los EVC son análogos a las definiciones de Circuitos virtuales Privados (*PVC*) en Frame Relay o Virtual Channels (*VC*) en ATM.

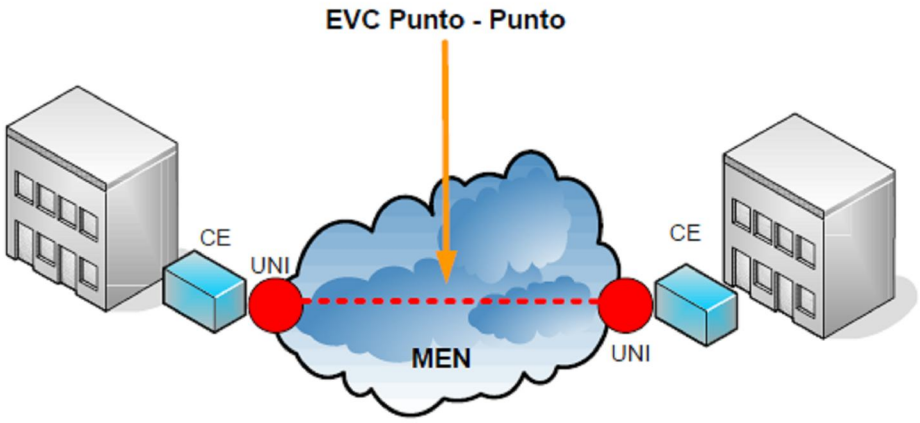


Figura. 2. Servicio E-line punto – punto

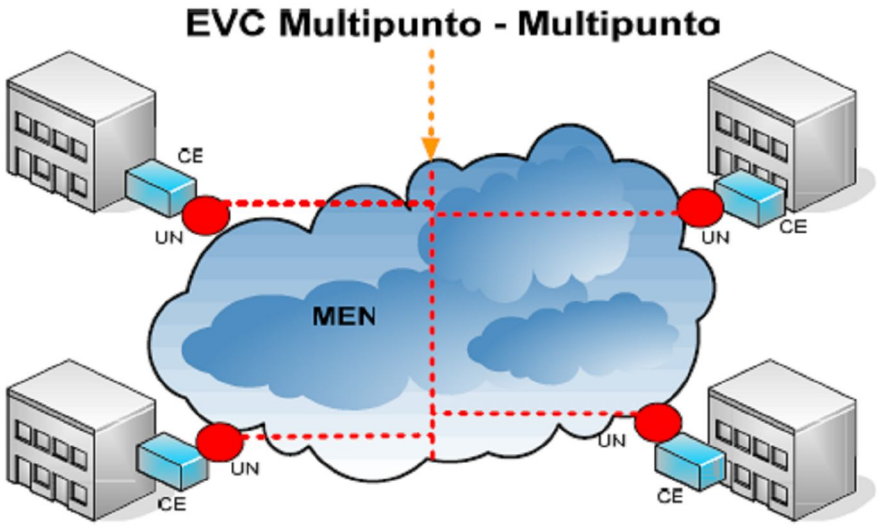


Figura 3. Servicio E-LAN multipunto – multipunto

2.3.1 Conexión Virtual Ethernet EVC (Ethernet Virtual Connection)

Un EVC es la asociación entre dos o más interfaces UNIs (*User Network Interface – Interfaz Usuario-Red*), donde el UNI es la interfaz estándar Ethernet y el punto de demarcación entre el equipo cliente y el proveedor de servicio MEN, pudiéndolo definir también como un camino virtual que proporciona al usuario servicios extremo a extremo atravesando múltiples redes MEN (*Metro Ethernet Network*).

Un EVC tiene dos funciones:

- Conectar dos o más sitios (*UNIs*) habilitando la transferencia de tramas entre ellos.
- Impedir la transferencia de datos entre usuarios que no son parte del mismo EVC, permitiendo privacidad y seguridad.

Un EVC puede ser usado para construir VPNs (*Virtual Private Network*).

2.3.2 Servicio Punto a Punto (E-Line)

El servicio E-Line proporciona un EVC punto a punto entre dos interfaces UNI, es decir, que se utiliza para proporcionar una conexión punto a punto. Un E-Line Service provee ancho de banda simétrico para el envío de datos en ambas

direcciones, sin asegurar desempeño. Al igual que con los PVCs de Frame Relay o ATM, se pueden multiplexar varios EVCs punto a punto en el mismo puerto físico (*UNI*).

E-Line se puede utilizar para crear los mismos servicios que puede ofrecer una red Frame Relay (*a través de PVCs*) o una línea alquilada punto a punto. Pero, como valor añadido, el rango de ancho de banda que puede proporcionar es mucho mayor.

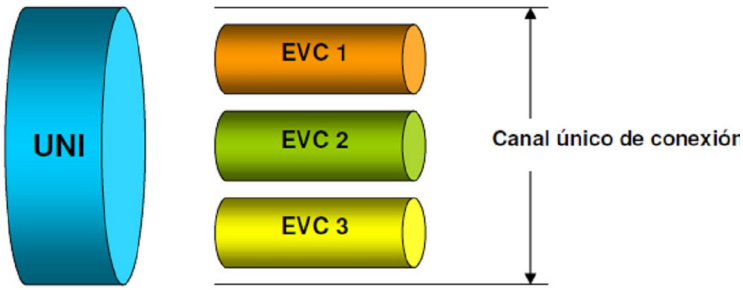


Figura 4. EVCs son las conexiones lógicas que se establecen entre cada par de CEs.

2.4 CLASES DE SERVICIOS (COS)

Metro Ethernet ofrece diferentes clases de servicio, tales como:

- Puerto físico
- CE-VLAN CoS (*802.1p*)
- DiffServ/IP TOS

Cuando el objetivo es proporcionar diferentes parámetros de tráfico, cada clase de servicio puede ofrecer diferentes niveles de desempeño, como retardos, jitter y tramas perdidas, de ahí que los parámetros de desempeño deben ser los especificados para cada clase. A continuación se muestran las características de las clases de servicio.

- **Puerto Físico**: en este caso, una simple clase de servicio es provista por un puerto físico. Todo el tráfico que ingresa o sale del puerto recibe la misma clase de servicio. Si el usuario requiere múltiples clases de servicio para sus tráficos, se separan tantos puertos físicos como sean requeridos, cada uno con su clase de servicio.

CE-VLAN CoS (802.1p): el MEF (*Metro Ethernet Forum*) ha definido CE-VLAN CoS como la clase de servicio que utiliza 802.1q para etiquetar las tramas, cuando se utiliza, se pueden indicar hasta 8 clases de servicio. El proveedor de servicio especifica el ancho de banda y los parámetros de desempeño.

DiffServ/IP TOS Values: pueden ser usados para determinar la clase de servicio IP TOS, en general, se usa para proveer 8 clases de servicio conocidas como prioridad IP. Prioridad IP es muy similar a la definición en 802.1p en IEEE 802.1q cuando la CoS se basa en prioridad de envío. DiffServ se define como PHS (*Perhop behaviors*), con una calidad de servicio más robusta cuando se compara con IP TOS y 802.1p. DiffServ provee 64

diferentes valores para determinar las clases de servicio. Casi todos los routers y switches soportan estas clases de servicio.

2.5 SERVICIO DE MULTIPLEXACIÓN

Este servicio se usa para soportar varios canales virtuales (*EVC*) de diferentes velocidades simultáneamente en un solo enlace de conexión (UNI), usando multiplexación se elimina la necesidad de tener diferentes interfaces físicas para tener enlaces a diferentes velocidades.

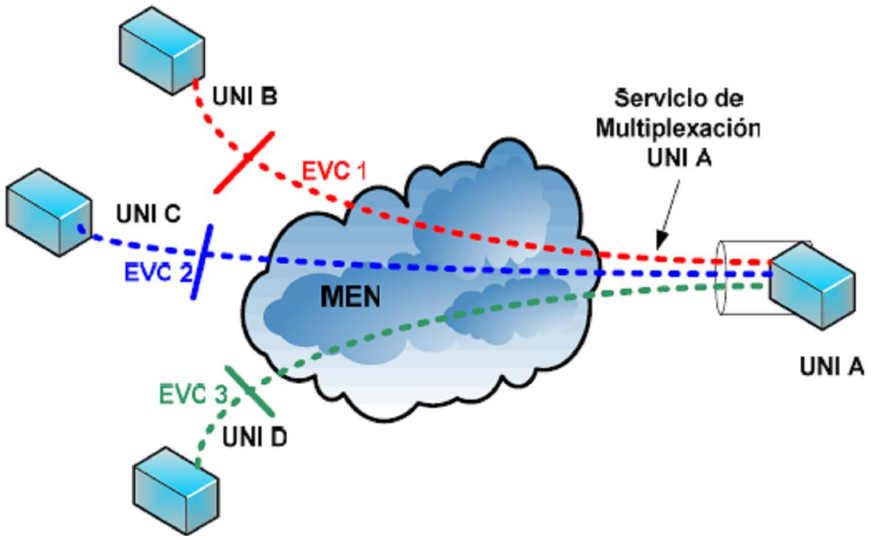


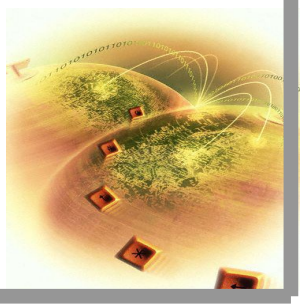
Figura. 5. Servicio de Multiplexación

El servicio permite a un UNI soportar múltiples EVCs, comparado con la alternativa de separar las interfaces físicas para cada EVC, se presentan varios beneficios:

- Costo bajo de los equipos, ya que se minimiza el número de routers y switches y maximiza la densidad de utilización puerto/slot.
- Minimiza espacio, potencia y cableado.
- Simplifica la activación de nuevos servicios.

CAPITULO 3

DESCRIPCIÓN FUNCIONAL DE MPLS



3.1 DESCRIPCIÓN FUNCIONAL DE MPLS (MULTIPROTOCOL LABEL SWITCHING)

MPLS es hoy día una solución clásica y estándar al transporte de información en las redes. Aceptado por toda la comunidad de Internet, ha sido hasta hoy una solución aceptable para el envío de información, utilizando enrutamiento de paquetes con ciertas garantías de entrega (*QoS*).

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.

De aquí derivan los siguientes problemas: el paradigma del enrutamiento está muy extendido en todos los entornos, tanto empresariales como académicos, etc.

El rediseño total del software existente hacia la Conmutación supondría un enorme gasto de tiempo y dinero. Igualmente sucede con el hardware que está funcionando hoy día.

3.2 IDEAS PRECONCEBIDAS SOBRE MPLS

Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas falsas o inexactas sobre el alcance y objetivos de MPLS. Hay quien piensa que MPLS se ha desarrollado para ofrecer un estándar a los vendedores que les permitiese evolucionar los conmutadores ATM a routers de backbone de altas prestaciones. Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel, los recientes avances en tecnologías de silicio ASIC permiten a los routers funcionar con una rapidez similar para la consulta de tablas a las de los conmutadores ATM. Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de envío de paquetes, éste no era el principal objetivo del grupo del IETF. Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM
- MPLS debía soportar el envío de paquetes tanto unicast como multicast.
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP (*Resource Reservation Protocol*).
- MPLS debía permitir el crecimiento constante de la Internet
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

También ha habido quien pensó que el MPLS perseguía eliminar totalmente el encaminamiento convencional por prefijos de red. Esta es otra idea falsa y nunca se planteó como objetivo del grupo, ya que el encaminamiento tradicional de nivel 3 siempre sería un requisito en la Internet por los siguientes motivos:

- El filtrado de paquetes en los cortafuegos (*FW*) de acceso a las LAN corporativas y en los límites de las redes de los NSPs es un requisito fundamental para poder gestionar la red y los servicios con las necesarias garantías de seguridad. Para ello se requiere examinar la información de la cabecera de los paquetes, lo que impide prescindir del uso del nivel 3 en ese tipo de aplicaciones.
- No es probable que los sistemas finales (*hosts*) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (*nivel 3*) que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En este primer salto se puede decidir enviarlo por routing convencional o asignar una etiqueta y enviarlo por un LSP.
- Las etiquetas MPLS tienen solamente significado local (*es imposible mantener vínculos globales entre etiquetas y hosts en toda la Internet*). Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: Por routing convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.

- Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad de MPLS.

3.2 FUNCIONALIDADES DE MPLS

3.2.1 Arquitectura

La arquitectura definida en MPLS utiliza asignación de etiquetas en sentido *downstream* para tráfico IP Unicast. Además soporta asignación de etiquetas bajo demanda en sentido *downstream* y asignación no solicitada. Esto permite que las etiquetas sean globalmente únicas por nodo o por interfaz. Las etiquetas poseen una gran granularidad, lo cual puede traer problemas cuando se producen diferencias de granularidad entre *LSRs*, *Label Switching Routers*, adyacentes.

Para soportar una estructura jerárquica de asignación de etiquetas emplea el mecanismo *LIFO*, *last-in-first-out*. De esta manera, la decisión de *forwarding* se realiza sobre la primera de las etiquetas de la pila.

Para la selección de camino, o *path*, se proponen dos mecanismos:

- Hop by Hop.
- Explicit Routing.

En el primer caso, el siguiente salto (*next hop*) se designa utilizando los resultados obtenidos de los protocolos de ruteo convencionales. En el segundo caso, una ruta explícita (*explicit route*) se especifica completamente por la fuente.

Todos los *LSRs* son capaces de enviar paquetes utilizando este mecanismo, pero no tienen la capacidad de originarlos.

La arquitectura de MPLS no requiere la utilización del mecanismo *Control-Driven* para la asignación de etiquetas, aun cuando este método es el más utilizado en estas redes.

No se define un mecanismo de encapsulación para datos etiquetados, pero se permiten dos opciones:

- Utilizar una encapsulación específicamente desarrollada para MPLS.
- Utilizar “espacios disponibles” en los *Headers* de la capa de datos o de red.

Para realizar el *forwarding* de un paquete IP, se tienen en cuenta dos fuentes de información:

- La tabla de ruteo almacenada en los *router*s.
- La información transportada en el propio paquete IP.

Luego, además de la componente de *forwarding* se tiene la componente de Control, la cual se encarga de la construcción y mantenimiento de la tabla de ruteo, o tabla de *forwarding*. Cada uno de los *router*s de la red implementa ambas funciones, Control y *Forwarding.* La componente de control consiste en uno o más protocolos de ruteo que proveen intercambio de información de ruteo entre los routers de la red, además de los algoritmos que los routers utilizan para convertir esta información en la tabla de *forwarding*. OSPF, BGP y PIM (*Protocol Independent Multicast*) son ejemplos de este tipo de protocolos.

La componente de *Forwarding* consiste en un conjunto de algoritmos que los routers utilizan para tomar la decisión de *forwarding* de un paquete IP.

3.2.2 Clase equivalente de envío FEC (Forwarding Equivalence Class

La clase equivalente de envío (*FEC*) es el conjunto de paquetes de capa 3 que comparten unas mismas características para su transporte, conmutados sobre un mismo camino, así todos recibirán el mismo tratamiento en su camino hacia

el destino. La asignación de un paquete a un determinado FEC se produce una vez el paquete entra en la red. Cada FEC puede representar unos requerimientos de servicio para un conjunto de paquetes o para una dirección fija.

Desde el punto de vista del *forwarding*, los paquetes IP dentro de cada conjunto son tratados por los routers de la misma manera, aun cuando los paquetes dentro de un conjunto difieran el uno del otro con respecto a la información del encabezado de la capa de red. Cada uno de estos conjuntos se define como *Forwarding Equivalence Classes, FECs*. Un conjunto de paquetes IP Multicast con la misma dirección de red de fuente y destino es un ejemplo de *FEC*.

Una característica importante de los *FECs* es su granularidad de *forwarding*, un *FEC* puede incluir todos los paquetes cuya dirección de red de destino coincide con un determinado prefijo. Además, un *FEC* podría incluir sólo los paquetes pertenecientes a una aplicación particular siendo ejecutada entre dos computadoras, incluyendo así sólo los paquetes IP con el mismo par de direcciones fuente y destino y los puertos TCP/UDP utilizados.

La arquitectura MPLS presenta dos tipos de routers:

- Label Edge Router LER
- Label Switched Router LSR

3.2.2.1 LER (Label Edge Router)

Se conoce también como ELSR (*Edge Label Switched Router*), es el Router en la frontera de la red al que se pueden conectar diversas redes (Frame Relay, ATM, Ethernet). Envía el tráfico entrante a la red MPLS utilizando un protocolo de señalización de etiquetas y distribuye el tráfico saliente entre las distintas redes.

Los LERs utilizan diferentes métodos para etiquetar el tráfico. Bajo el esquema más simple, los paquetes IP están ligados a una etiqueta y a un FEC utilizando tablas preprogramadas.

3.2.2.2 LSR (Label Switched Router)

Los LSR o router de conmutación de etiquetas son equipos de conmutación de gran velocidad en el núcleo de una red MPLS, estos funcionan a base de intercambiar etiquetas según una tabla de envío.

Sus funciones son las siguientes:

- Participar en el establecimiento de los LSPs usando un protocolo de señalización apropiado.

- Conmutar rápidamente el tráfico de datos entre los caminos establecidos.

Para que los LSPs se puedan usar, las tablas de envío de cada LSR deben contener:

1. (Interfaz de entrada, etiqueta asociada)
2. (Interfaz de salida, etiqueta asociada)

Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la figura 5 se ilustra un ejemplo del funcionamiento de un LRS del núcleo MPLS. A un paquete que llega al LSR por la interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

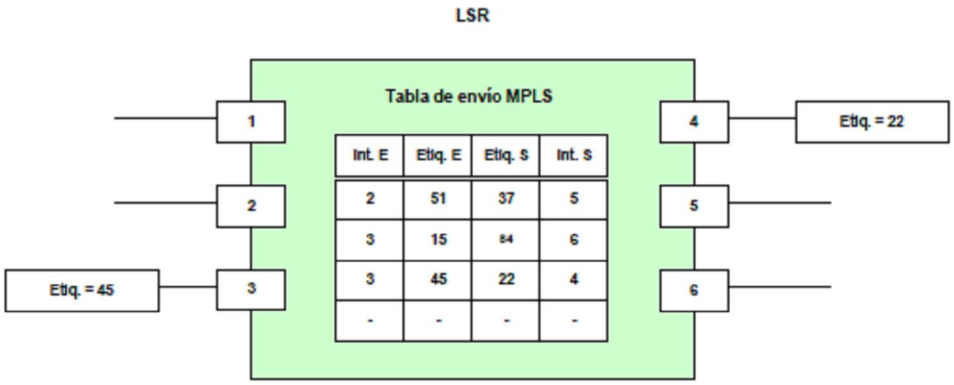


Figura 6. Detalle de la tabla de envío de un LSR.

3.2.3 Etiquetas

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

Pasos para la asignación de etiquetas:

- Cada paquete se clasifica como un nuevo FEC o se le asigna un FEC ya existente.
- Se asigna una etiqueta a cada paquete. Éstas se derivan de la capa de enlace, es decir, para redes Frame Relay, ATM o redes ópticas, los

identificadores de la capa 2 (DLCIs (*Data Link Connection Identifier*), VPIs/VCIs y longitud de onda DWDM, respectivamente) pueden servir como etiquetas. Para redes como Ethernet y PPP (*Point to Point Protocol*), a la etiqueta se le añade una cabecera intermedia entre las cabeceras de la capa de enlace y la capa de red, que contendrá el campo TTL (*Time To Live*).

Las decisiones de asignación de etiquetas pueden estar basadas en criterios de envío como encaminamiento unicast, multicast, ingeniería de tráfico, VPN (*Virtual Private Network*) y QoS (*Quality of Service*).

La encapsulación de la etiqueta presenta dos alternativas, dependiendo de la tecnología utilizada:

- *Shim Header*, este mecanismo se adopta para todas aquellas tecnologías que no permiten transportar la información de Etiqueta en el *Header* del paquete de capa física. Es decir, se utiliza esta metodología para todas las tecnologías, excepto para ATM y Frame Relay.
- *Header* del *PDU*, *Paquet Data Unit*, de capa física.

Las etiquetas constan de 32 bits y tienen el siguiente formato:

Figura 7. Formato de una Entrada en la Pila de Etiquetas

Etiqueta (20 bits): contiene la etiqueta asignada.

- *Exp (3 bits):* indica la clase de servicio que requiere el paquete.
- *Pila (1 bit):* permite apilar etiquetas en un paquete para realizar un encaminamiento jerárquico.
- *TTL (8 bits):* tiene el mismo significado que en IP, se denomina cabecera *shim*.

El *TTL* se obtiene a partir del *TTL* definido en el paquete IP, y se decrementa en 1 con cada *LSR* De esta manera, un paquete IP que ingresa en una red MPLS egresará de la misma con el *TTL* decrementado en 1 por cada *LSR* que haya tenido que pasar. Una alternativa a este procedimiento es decrementar el *TTL* en 1 únicamente cuando el paquete IP egrese de la red MPLS. De esta manera un *LSP* se verá, desde el punto de vista de IP, como un sólo salto (*Hop*).

Es posible que los paquetes etiquetados requieran de fragmentación, como en el caso de paquetes IP, ya que es posible que un paquete requiera la asignación de más de una etiqueta, por lo cual puede requerirse la fragmentación del mismo.

Para estos casos, la fragmentación se realiza sobre el datagrama IP, y luego se especifica la misma utilizando el bit de *Stack* y la información de etiqueta.

CAPITULO 4

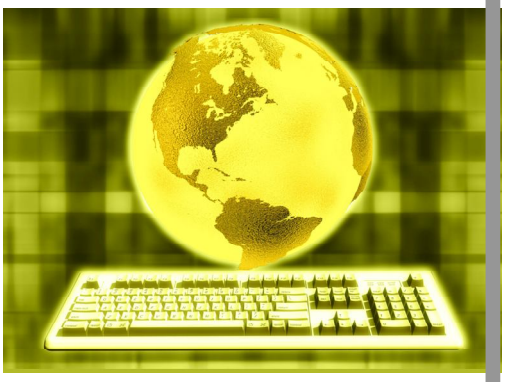
APLICACIONES DE MPLS

4.1 INGENIERÍA DE TRÁFICO

4.2 CLASES DE SERVICIO (COS)

4.3 REDES PRIVADAS VIRTUALES VPNS

4.3.1 Modelo jerárquico de un backbone.



Las principales aplicaciones que hoy en la actualidad tiene MPLS son:

- Ingeniería de tráfico
- Diferenciación de niveles de servicio mediante clases (CoS)
- Servicio de redes privadas virtuales (VPN)

Veamos las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

4.1 INGENIERÍA DE TRÁFICO

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

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados.

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

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

Para calcular estas rutas existen dos métodos:

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

Los dos métodos se pueden combinar si en alguna parte de la ruta la información no está disponible (por ejemplo en un Sistema Autónomo).

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 8 se comparan estos dos tipos de rutas para el mismo par de nodos origen destino.

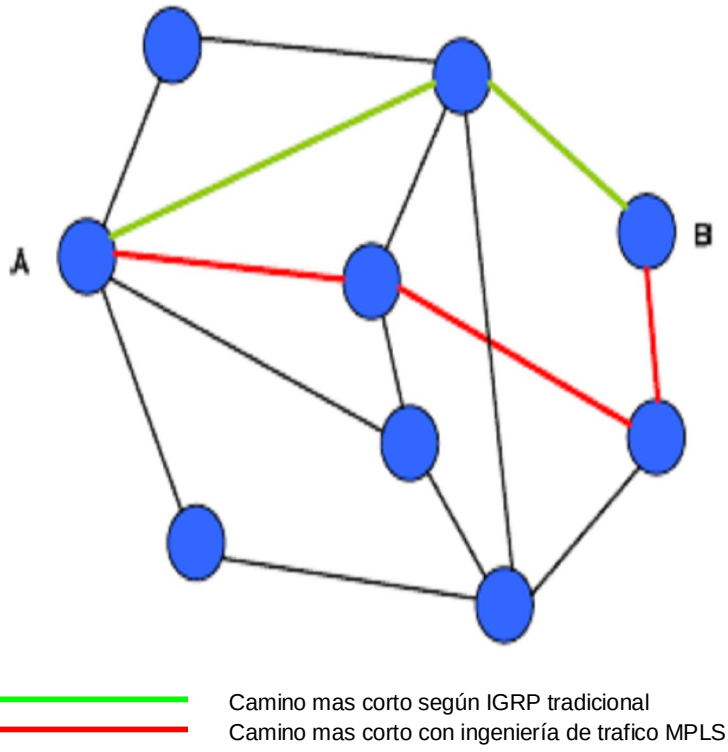


Figura 8. Comparación ente camino más corto IGP con Ingeniería de Tráfico MPLS

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

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

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.

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

- **TE-RSVP**

  TE-RSVP (*Traffic Engneering – RSVP*) es una extensión del protocolo RSVP. TE-RSVP es un protocolo de señalización de estado suave que utiliza UDPs o datagramas IP para la comunicación entre compañeros LSR (*LSR peers*).

- **CR-LDP.**

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

- Comparación de ambos métodos

TE-RSVP es de estado suave, lo que significa que la información se intercambia cuando se establece el LSP, pero se deben enviar mensajes periódicos para notificar que la conexión todavía se requiere. Por el contrario, CR-LDP es de estado duro, es decir, toda la información se intercambia al

iniciar la conexión y no se produce más información adicional hasta que el LSP se elimine.

El hecho que TE-RSVP sea de estado suave e introduzca una sobrecarga adicional hace que no sea escalable ya que esta sobrecarga crecerá proporcionalmente con el número de sesiones RSVP. Para evitar esto se intenta resumir la información y aprovechar un único mensaje para enviar varios mensajes de refresco.

CR-LDP utiliza conexiones TCP lo que hace que éstas sean más fiables y seguras, mientras que TE-RSVP utiliza UDP o datagramas IP para establecer las comunicaciones, lo que supone mayor vulnerabilidad aunque puede utilizar IPSec o algún otro esquema de encriptación.

Las conexiones TCP de CR-LDP permiten detectar un fallo mediante notificaciones propias de TCP. Esta notificación se procesa rápidamente así que las acciones oportunas se inician. Sin embargo, una conexión fallida en TE-RSVP se detecta cuando no se recibe un determinado mensaje de refresco y, dependiendo de cómo se haya configurado, detectar un fallo tardará segundos o minutos antes de que puedan iniciarse las acciones de recuperación.

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

- TE-RSVP puede crear una nueva ruta a partir de un salto diferente en un LSR, así, en el momento en que se detecte el fallo refresca esta nueva ruta que pasa a ser operativa y, la antigua se eliminará cuando deje de recibir mensajes de refresco.
- Otra alternativa que soportan ambos protocolos es crear una ruta completa alternativa mientras se usa la antigua, en el momento que se produzca un fallo la nueva ruta será operativa y se eliminará la antigua.
- CR-LDP soporta que un LSP de servicio a muchos hosts mediante la designación de FECs, mientras que RSVP sólo reserva ancho de banda a una única dirección IP.
- La elección entre los diferentes protocolos se deberá a factores como la complejidad de la red, si las conexiones van a ser cortas o permanentes, qué grado de tolerancia a fallos se requiere, etc.

4.2 CLASES DE SERVICIO (COS)

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

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.
- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

4.3 REDES PRIVADAS VIRTUALES VPNS

Una red privada virtual (VPN) se construye a base de conexiones que se realizan 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.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías.

Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los 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 specie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP-VPN. Los túneles IP en conexiones dedicadas (no se va a tratar aquí de las conexiones conmutadas de acceso) se pueden establecer de dos maneras:

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

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios

routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

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

A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

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

- Están basadas en conexiones punto a punto (PVCs o túneles).

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

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos.

Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de

etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una Internet privada (intranet) entre los miembros de su VPN. De este modo, se Pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

En las figuras 9 y 10 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, a base de LSPs, y no de extremo a extremo a través de la red.

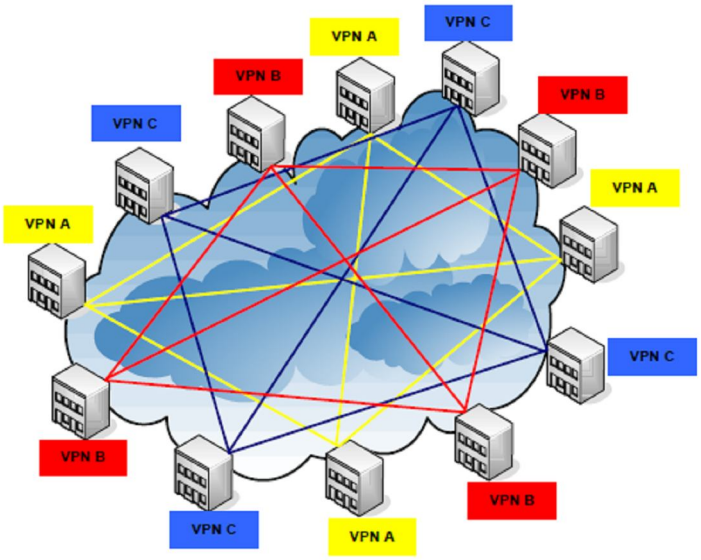


Figura 9. Modelo “Superpuesto” Túneles o PVCs. Topología VPN conectiva

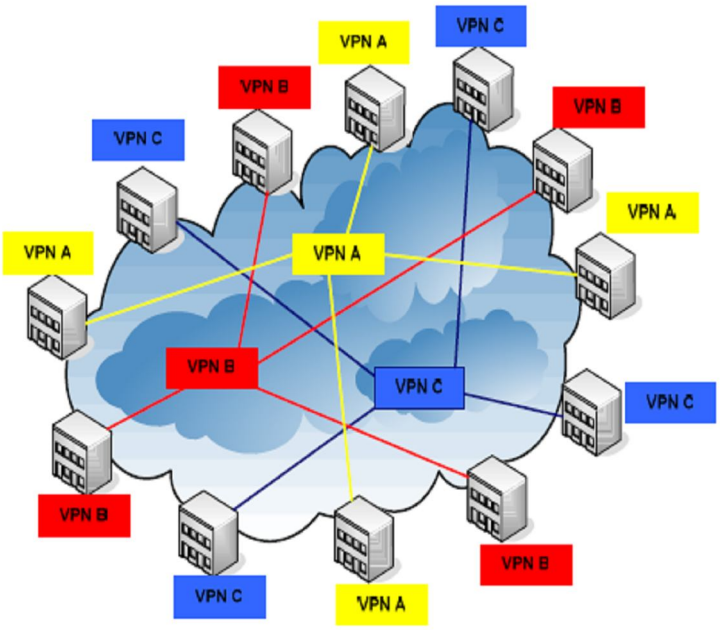


Figura 10. Modelo “acoplado” (MPLS) Topología VPN no-conectiva

Se puede evidenciar que, las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs)
- Evita la complejidad de los túneles y PVCs
- La provisión de servicio es sencilla: una nueva conexión afecta a un solo router.
- Tiene mayores opciones de crecimiento modular.
- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.
- Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación), lo que es necesario para un servicio completo VPN.

4.3.1 Modelo jerárquico de un backbone

El modelo jerárquico para un backbone, o red de comunicaciones, consta de tres capas bien definidas. Este modelo permite tener redes escalables que soportan un crecimiento constante. Se usa principalmente routers, que

dependiendo de la capa en la cual trabajen, tendrán sus propias características.

- **Capa de acceso**

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Ésta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo, capa de escritorio o de usuario. Los usuarios así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales. En la capa de acceso se puede encontrar múltiples grupos de usuarios con sus correspondientes recursos. En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico al Web. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

- **Capa de distribución**

La capa de distribución marca el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN.

En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

- Servir como punto de concentración para acceder a los dispositivos de capa de acceso.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de difusión / multidifusión.
- Proporcionar servicios de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquete pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo. La capa de núcleo podrá entonces transportar la petición al servicio apropiado.

- **Capa de conmutación**

Se la conoce también como capa del núcleo, principal o Core se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados.

Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos. Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia. Cuando un usuario necesita acceder a un servicio

corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado.

El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

CAPITULO 5

ESTRUCTURA DE MPLS

5.1 ESTRUCTURA DE UN NÚCLEO MPLS

5.1.1Paquetes Simples basados en MPLS

5.2 MPLS en las Redes MEN

5.1 ESTRUCTURA DE UN NÚCLEO MPLS

Una estructura típica de una red MPLS se muestra en la figura 11, está constituida principalmente de los LER alrededor del núcleo y los LSR. Los equipos de conexión del lado del usuario CPE, corre normalmente direccionamiento IP y no MPLS, en el supuesto caso que estos equipos trabajen con MPLS es total responsabilidad del usuario y no del proveedor del servicio. Los equipos LER son administrados por el proveedor del servicio y no funcionan como CPE bajo ninguna circunstancia.

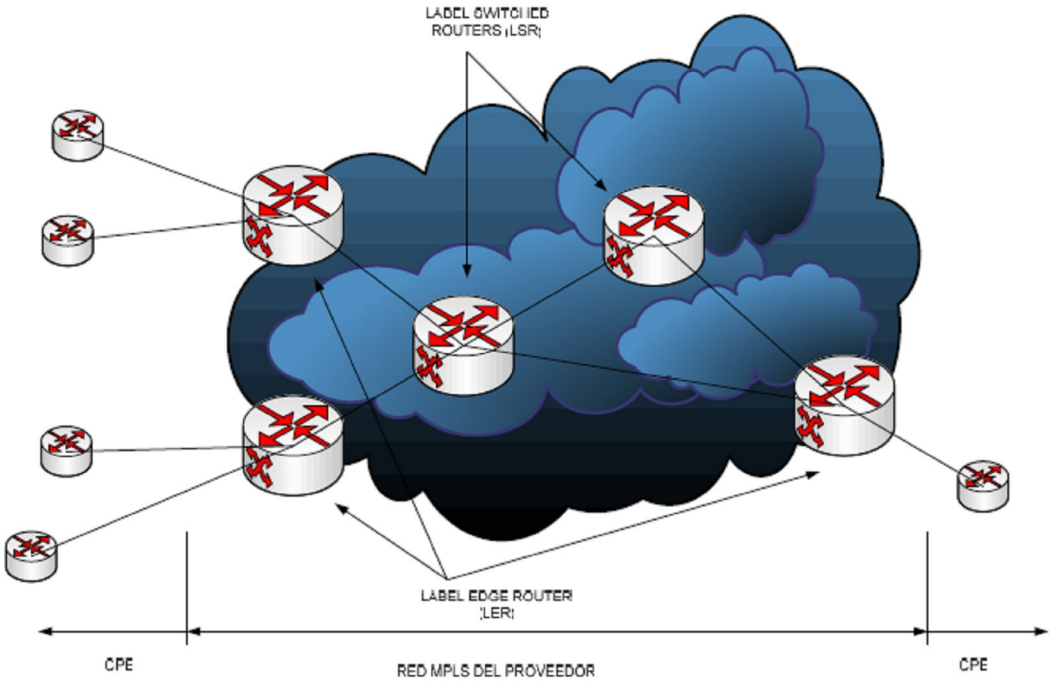


Figura.11. Estructura típica de una red MPLS

5.1.1 Paquetes Simples basados en MPLS

La estructura de red más simple basada en MPLS se muestra en la figura 12. Esta estructura se aplica a la red que puede soportar MPLS para brindar servicios VPN o ingeniería de tráfico IP. En este modelo, los sitios de usuario están conectados directamente al router LER y éste está conectado a un LSR.

Estos routers están conectados entre sí por enlaces como: serial, Ethernet, paquetes sobre SONET y paquetes con cabeceras MPLS.

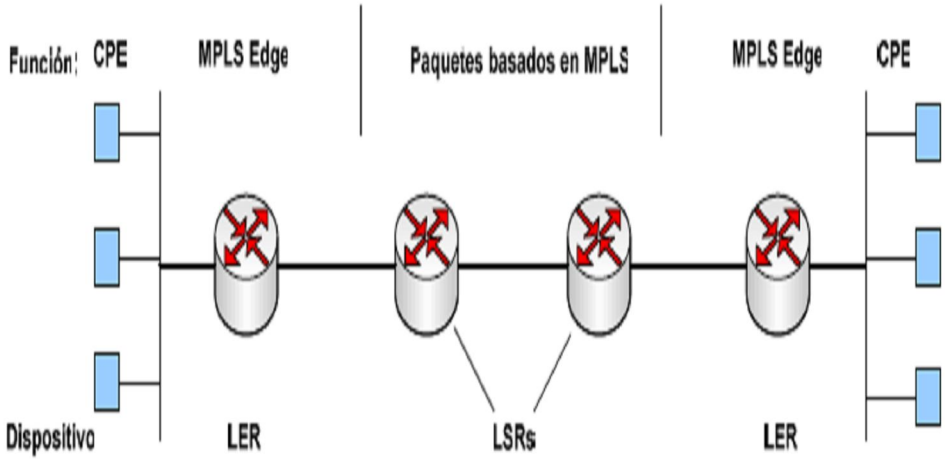


Figura. 12. Paquetes simples basados en MPLS

5.2 MPLS EN LAS REDES MEN

Debido a las limitantes que tiene la familia Metro Ethernet en aspectos como Ingeniería de Trafico, Recuperación a Fallos, Escalabilidad de Servicios,

Convergencia de Servicios con QoS, se realizo una convergencia con MPLS y de esta forma estas limitantes son solucionadas y la su vez se aprovechan sus cualidades.

La utilización de MPLS sobre Redes Metro Ethernet se logran los siguientes resultados:

Ingeniería de tráfico (TE). Ethernet como tal no tiene la capacidad de asegurar que bajo cierto ancho de banda éste sea compartido justamente. Esta situación se convierte en un punto crítico cuando deseamos contar con una red multiservicios convergentes.

Recuperación a fallos (Network Resiliency). Los protocolos de Ethernet como los 802.1d y 802.1w, encargados de prevenir ciclos y realizar recuperación en caso de fallas en sus enlaces, sin embargo, el tiempo que requiere para complementar esta actividad va desde los 30 segundos hasta varios minutos. Por lo cual la disponibilidad de acceso a la red no le permitiría garantizar la distribución equitativa de ancho de banda requerido por las aplicaciones convergentes. MPLS permite contar con LSP de respaldo con un grado de recuperación, de tal manera que una falla en los enlaces de nuestra red metropolitana Ethernet podría restablecerse en no más de 50 milisegundos.

Con ésta velocidad de recuperación, se puede mantener transparente la disponibilidad de la red para el usuario final, incluso con miles de servicios ejecutándose de manera simultánea en el momento de la falla del enlace.

***Escalabilidad de Servicios*.** Con el fin de disminuir los gastos de instalación y operación, se necesita de una arquitectura de red que crezca de manera proporcional al número de usuarios. Para ello es fundamental hacer la distinción de los tráficos de todos los usuarios sin importar el número de redes de acceso o cantidad de nodos conectados simultáneamente. La forma tradicional de Ethernet para afrontar esta problemática es utilizar redes locales virtuales (VLAN). Las VLAN o IEEE 802.1q, tienen la desventaja de sólo direccionar hasta 4,094 etiquetas, las cuales deben ser una por conexión, impidiendo un crecimiento a futuro en la red metropolitana.

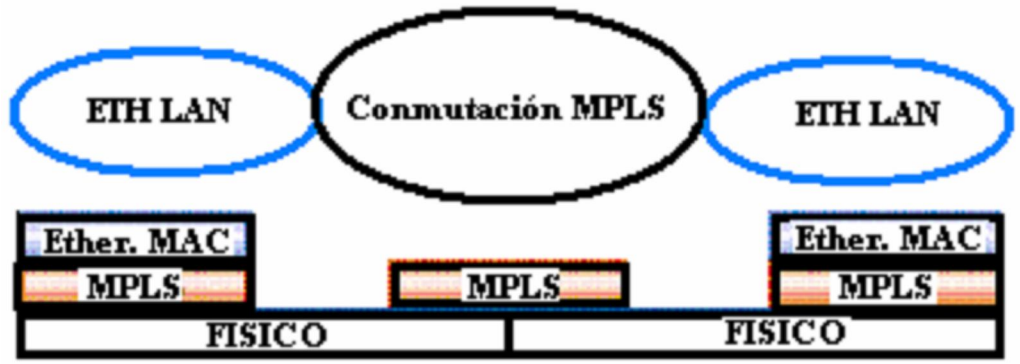


Figura 13. Encapsulado MPLS y Conmutación en la MAN

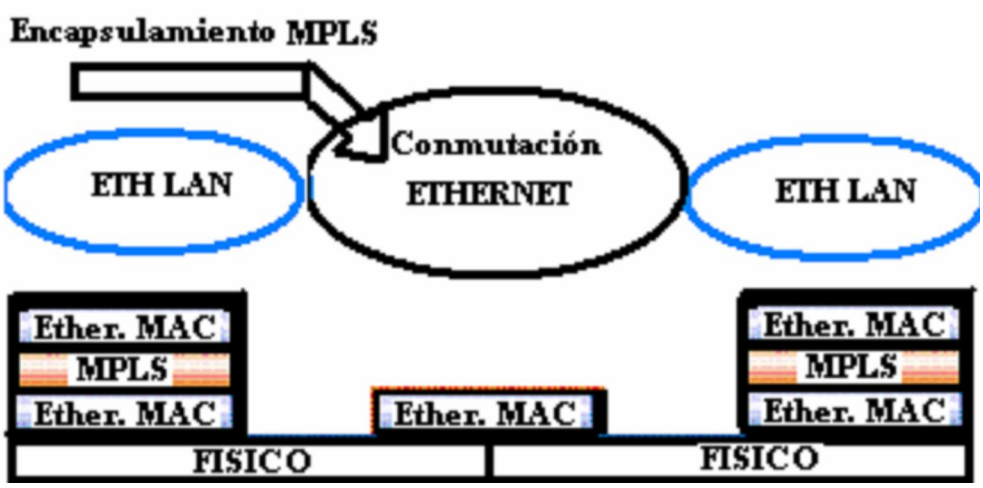


Figura 14. Encapsulado MPLS y Conmutación Ethernet en la MAN

Por el contrario, las redes metropolitanas basadas en MPLS encapsulan las etiquetas del 802.1q, de tal forma que sólo tienen significado local debido a que mapean cada etiqueta con un respectivo LSP permitiendo la diferenciación de tráficos de manera eficiente. Con el uso de MPLS no existe una limitante geográfica para el envió de paquetes pertenecientes a una VLAN, lo cual permite al operador de la red metropolitana incrementar sus servicios para cubrir las demandas de los usuarios sin importar su localización o topología de red a la cual pertenece.

***Convergencia de Servicios con QoS*.** Con el binomio IP/MPLS en el corazón de la red metropolitana se tiene mucho que ganar si consideramos la red de acceso metropolitano Ethernet como parte indispensable de una red extremo a extremo. El uso de MPLS facilita la entrega de servicios al proveer la misma conectividad y niveles de seguridad de la red extremo a extremo al interoperar con otros protocolos de capa dos como Frame Relay, ATM, SONET, RPR y

DWDM. Empleando MPLS en la red metropolitana, permite crear nuevos puntos de servicio Ethernet sin tener la necesidad de migrar los servicios e infraestructuras de red existentes y continuar disfrutando de VPN o VLAN como si todos los usuarios se encontraran en la misma red local.

La contribución de MPLS a QoS en las redes metropolitanas Ethernet se basa primordialmente en el manejo de sus etiquetas. La conmutación de etiquetas MPLS es una excelente herramienta para combatir la latencia y el jitter debido a la rapidez con la cual se logra analizar el destino en los paquetes procesados.

Con esta simple operación se logra desminuir la latencia en la red, lo cual mejora en mucho el jitter final, no obstante ello, la conmutación de etiquetas no representa la solución real para aquellas aplicaciones sensibles al retardo. Si tenemos una conexión de bajo ancho de banda, MPLS no provee más ancho de banda, pero mejora de manera significante los problemas de retardo inherente en las redes actuales. Si reunimos las características más importantes que brinda MPLS metropolitano, se podrían resumir en las siguientes:

- Ingeniería de tráfico.
- VPN .
- Eficiente transporte de capa dos.
- Eliminación de múltiples capas.

- Transforma direcciones IP a etiquetas.
- Soporte para RSVP y protocolos de ruteo.
- Incrementa la escalabilidad de redes y servicio

CONCLUSION

En la actualidad la tecnología nos proporciona las herramientas necesarias para superar ciertas limitaciones, es por esto que podemos decir que la distancia ya no es una limitación. Las tecnologías ópticas nos permiten transportar Ethernet a decenas e incluso centenares de Kms, la fiabilidad y la redundancia han dejado de ser un problema y hoy en día los fabricantes de equipamiento Ethernet aportan soluciones tan fiables como las de telefonía tradicional TDM, con tiempos de protección similares además la capacidad de crecimiento de las redes Ethernet se ha incrementado en varios órdenes de magnitud, gracias a modificaciones de la tecnología, la seguridad y la separación entre usuarios se ha reforzado gracias a tecnologías de tunelización.

Cuando se introdujeron FDDI, el canal de fibra y ATM, eran más rápidos que Ethernet, pero también incompatibles con éste, mucho más complejos y difíciles de manejar. Con el tiempo, Ethernet los igualó en cuanto a velocidad, por lo que ya no tenían ventajas y poco a poco están dejando de utilizarse, excepto ATM, el cual se utiliza en el núcleo del sistema telefónico.

Por éste y otros motivos apuntados, los mayores operadores de telecomunicaciones están ofreciendo ya servicios Ethernet como alternativa a otras tecnologías de comunicación de datos de larga distancia. Agregándole a esto la implementación de MPLS como una solución IP sobre Ethernet, Fast Ethernet o Gigabit Ethernet, es la conocida como IP pura. Puesto que IPv4 es un protocolo diseñado mucho antes que MPLS, el funcionamiento de IPv4 ha sido totalmente satisfactorio, no obstante, el sorprendente crecimiento de Internet evidenció importantes carencias, como: la escasez de direcciones IP, la imposibilidad de transmitir aplicaciones en tiempo real y los escasos mecanismos de seguridad.

La implementación de MPLS como una solución IP sobre ATM está muy extendida. Primeramente indicar, que MPLS no fue desarrollado para reemplazar ATM, sino para complementarlo. De hecho, la aparición de switches ATM e IP con soporte de MPLS, ha integrado las ventajas de los routers IP y los switches ATM y ha supuesto una mejora de la relación precio/rendimiento de estos dispositivos. La diferencia principal entre MPLS y otras soluciones de IP sobre ATM, es que las conexiones MPLS se establecen utilizando LDP, y no por los protocolos de señalización ATM tradicionales, tales como PNNI (*Private Network to Network Interface*). Por otro lado, MPLS elimina la complejidad de hacer corresponder el direccionamiento IP y la información de encaminamiento directamente en las tablas de conmutación de ATM.

La migración a IP está provocando profundos cambios en el sector de las telecomunicaciones y configura uno de los retos más importantes para los ISP, inmersos actualmente en un proceso de transformación de sus infraestructuras de cara a incorporar los beneficios de esta tecnología.

MPLS nació con el fin de incorporar la velocidad de conmutación; pero actualmente esta ventaja no es percibida como el principal beneficio, ya que los gigarouters son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces.

Mediante MPLS, los ISP pueden soportar servicios diferenciados o DiffServ, como viene recogido en la RFC 3270. El modelo DiffServ define varios mecanismos para clasificar el tráfico en un pequeño número de CoS. Los usuarios de Internet demandan continuamente nuevas aplicaciones, teniendo los servicios actualmente soportados unos requerimientos de ancho de banda y de tolerancia a retrasos en la transmisión muy distintos y para satisfacer estas necesidades óptimamente, los ISP necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de clasificación de dicho tráfico.

De nuevo, MPLS ofrece a los ISP una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes.

Finalmente, MPLS ofrece también un mecanismo sencillo y flexible para crear VPN. Una VPN simula la operación de una WAN (*Wide Area Network*) privada

sobre la Internet pública. Para ofrecer un servicio de VPN viable a sus clientes, un ISP debe solventar los problemas de seguridad de los datos y soportar el uso de direcciones IP privadas no únicas dentro de la VPN. Puesto que MPLS permite la creación de circuitos virtuales o túneles a lo largo de una red IP, es lógico que los ISP utilicen MPLS como una forma de aislar el tráfico.

BIBLIOGRAFÍA

WALLEY, Mark, “Metro Ethernet Networks”, Agosto 2003. www.metroethernetforum.org/metro-ethernet-networks.pdf

SANTITORO, Ralph, “Metro Ethernet Services”, Octubre 2003 www.metroethernetforum.org/metro-ethernet-services.pdf

PASTOR J., RABADAN J., TOMILLO A., “Redes Metro Ethernet” http://www.coit.es/publicaciones/bit/bit149/64-66.pdf

SIERRA, Emilio, “Proyecto Metro Ethernet en Medellín-Antioquía”. http://www.monografias.com/trabajos17/metro-ethernet/metro-ethernet.shtml

CARREON, Roberto, “Redes Privadas Virtuales” http://www.monografias.com/trabajos11/repri/repri.shtml

ESPINEL, Esteban, “Estudio para la migración de una red de datos perteneciente a una empresa potadora de servicios de telecomunicaciones a la tecnología ATMMPLS”, Biblioteca Facultad Ingeniería Eléctrica, Julio 2004.

CISCO SYSTEMS, “Deploying Large Scale VPN with MPLS”, Sesión RTS-230

PEPELNJAK Ivan, GUICHARD Jim, “MPLS and VPN Arquitecture”, Quinta Edición, Editorial Prentice Hall PTR.

DAVIE Bruce, REKHTER Yahov, “MPLS: Technology and Applications”.

REQUEST FOR COMMENT RFC 3031, “Multiprotocol Label Switching Architectures”. http://www.rfc-es.org/rfc/rfc3031-es.txt

FERRER, María, “Multiprotocol Label Switching”
http://www.uv.es/~montanan/redes/trabajos/MPLS.doc

PÉREZ, David, “Análisis de Requerimientos de QoS sobre Redes IP Multicast”
http://www.uv.es/~montanan/redes/trabajos/MPLS.doc

BARBERÄ, José ”MPLS: Una arquitectura de backbone para la Internet del siglo XXI” http://www.rediris.es/rediris/boletin/53/enfoque1.html

CISCO SYTEMS, “Cisco IOS XR MPLS Configuration Guide”
http://www.cisco.com/application/pdf/en/us/guest/products/ps5845/c2001/ccmigration_09186a00806f9b23.pdf

CISCO SYSTEMS, “Cisco MPLS Controller Software Configuration Guide- Quality of Service MPLS Networks”
http://www.cisco.com/univercd/cc/td/doc/product/wambu/bpx8600/mpls/9_3_1/mpls03.pdf

CISCO SYSTEMS, “Cisco MPLS Controller Software Configuration Guide- Designing MPLS for ATM”
http://www.cisco.com/univercd/cc/td/doc/product/wanbu/bpx8600/mpls/9_3_1/mpls04.pdf

CISCO SYSTEMS, “Cisco Academy Network”, Módulo 4.

MC MCSE Certification Resources, “Modelo Jerárquico de una red de datos” http://www.mcmcse.com/cisco/guides/hierarchical_model.shtml#

ALCATEL, “Mediación ATM – MPLS ”
http://wap.alcatel.es/tecno/tribuna/intmov/pdf/im_mpls.pdf

DYSTAR, “Caso de estudio para la migración de una red antigua Frame Relay a una MPLS ”
http://www.btglobalservices.com/business/es/es/docs/case_studies/bt_dystar_casestudy_ES.pdf

EASYNET, “Tendencias emergentes en servicios Panaeuropeos de IP VPN ”
http://www.idg.es/comunicaciones/conocimiento/pdfs/ip%20vpn%20white%20paperSP.pdf
EASYNET, “Redes MPLS - ¿Hasta que punto son seguras?
http://www.easynet.com/pdf/whitepaper/wp_redesmplsseguridad_es.pdf

CISCO SYSTEMS, “Cisco MPLS Controller Software Configuration Guide-Designing MPLS for ATM”
http://www.cisco.com/univercd/cc/td/doc/product/wanbu/bpx8600/mpls/9_3_1/mpls04.pdf

CIENTEC, “Análisis de MPLS ”http://www.cientec.com/analisis/mpls.asp

TEXTOS CIENTÍFICOS, “Frame Relay”
http://www.textoscientificos.com/redes/area-amplia/frame-relay

NEILA, Rafael, “Introduction to corporate security in communications ”
http://www.fistconference.org/data/presentaciones/seguridaddecomunicacionescorporativas.pdf