VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

NUEVA GENERACION DE REDES DE ACCESO CON MPLS

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A :

ROCIO GUERRERO AVILA

DIRECTOR DE TESIS: JOSE ARTURO LANDEROS AYALA

CD. UNIVERSITARIA MEXICO, D. F. NOVIEMBRE 2004

Agradecimientos

Cuando una meta se ha cumplido, es importante detener el paso, y dar gracias a aquellos que la hicieron posible. Por tal motivo no puedo dejar de dar gracias a Dios, por darme la fortaleza para vencer mis miedos y debilidades, por hacerme levantar la cabeza cuando miraba hacia abajo y por darme lo que necesitaba aunque yo no mediera cuenta.

A mis padres ***José y Elsa*** *que con su ejemplo me han inspirado a salir adelante y motivado para luchar por todos mis sueños, por dar todos sus esfuerzos, amor y paciencia para que yo llegara hasta este punto. Gracias, los quiero mucho.*

A mis tíos ***Rigoberto y Andrés*** *les doy gracias por preocuparse en darme siempre un buen consejo. Han sido un gran ejemplo para que yo estuviera aquí, los admiro mucho, gracias.*

A mi abuelita ***Ofelia Mendoza,*** *por todo su cariño que me ha dado desde niña, por preocuparse siempre por mi y por mostrarme una vida digna, gracias, te quiero mucho abuelita.*

A mis hermanos ***Gaby , Lupe y César,*** *por hacerme ver la vida diferente, por despertar en mi el niño que llevo dentro, por hacerme reír aun en los peores momentos y por todo su cariño gracias. Ustedes saben cuanto los quiero.*

A ***Ana Laura, Cinthya, Lorena, Lizette, Oralia, Marlene, Claudia y Pablo****, les doy gracias por ser cómplices de muchas aventuras, por fortalecer mi espíritu con su amistad, y por enseñarme lo que es ser un buen amigo en los tiempos difíciles y buenos, gracias.*

A ***Gustavo Serrano Diez****, por llegar y darle un cambio a mi vida, por ayudarme a encontrar el verdadero camino cuando estaba perdida , por involucrarse en mis problemas y por darme la confianza y la fe de terminar esta carrera, gracias.*

A ***Guillermina Martínez****, por todo el apoyo que me ha dado en estos últimos días. Es un honor contar con tu amistad gracias.*

A mis ***profesores*** *que con sus enseñanzas me han enseñado a buscar el camino de la superación*

Al ***Ing. José Arturo Landeros Ayala****, quien me brindo su tiempo, paciencia y apoyo para la realización de este trabajo.*

ÍNDICE

CAPÍTULO 4

4. MPLS EN LOS PROTOCOLOS DE ENLACE DE IP

CAPÍTULO 5

ARQUITECTURA Y FUNCIONAMIENTO DE MPLS

CAPÍTULO 6

APLICACIONES DE MPLS

CAPÍTULO 7

TENDENCIAS EN EL MERCADO DE MPLS

CAPÍTULO 1

1. INTRODUCCIÓN

1.1. Delimitación del tema

1.1.1.Origen y Razón de MPLS

La red IP se ha convertido en una extensa red en la que las posibilidades de negocio y los mercados de consumo inducen al desarrollo de nuevas aplicaciones, tales como voz, video, multimedia etc, por lo que se requiere un mayor ancho de banda, así como también clases diferenciadas de servicios a los distintos usuarios que utilizan la red. Pero una red sin conexión no puede proporcionar una alta calidad de servicio. IP al no ser orientada a conexión se imposibilita para seleccionar diferentes niveles de servicio para distintos tipos de aplicaciones de usuario. Una red IP se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como de "best-effort", por lo que los paquetes se entregan de la mejor forma posible.

Avanzamos hacia una convergencia entre voz y datos en la red IP y su infraestructura y protocolos han sido optimizados sólo para datos. IGPs (*Interior Gateway Protocol*), RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*), EGPs (*Exterior Gateway Protocol*) y BGP4 (*Border Gateway Protocol v4*), no son la solución óptima. Muchos de estos protocolos de enrutamiento están basados en algoritmos para obtener el camino más corto (como RIP y BGP4, basados en el vector distancia) sin tener en cuenta métricas adicionales como retardo, *jitter* y congestión del tráfico.

Todo esto se traduce en una sobrecarga en el enrutador IP, problemas de propagación de las rutas y la obligación de integrar redes IP con ATM, para así darles a las redes IP un comportamiento orientado a conexión y solucionar varios de estos problemas, sin embargo la idea de superponer IP sobre ATM trae varias discontinuidades, ya que se trata de integrar dos niveles diferentes: nivel 2 (transporte) y nivel 3 (red), tal como se verá a continuación. MPLS logra esa integración de niveles sin discontinuidades, combinando eficazmente las funciones de control del enrutamiento con la simplicidad y rapidez de la conmutación de nivel 2.

Veamos a continuación a mas a detalle cómo surge MPLS.

El aumento en número de usuarios llevo a una creciente demanda de ancho de banda, por lo que había que idear otras alternativas de ingeniería de tráfico. Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los enrutadores tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los enrutadores IP. Las redes ATM ofrecían entonces (1995-1997) mayores velocidades (155 Mpbs) debido a que las características de respuesta determinísticas de los circuitos virtuales ATM, hacían posible la implementación de soluciones de ingeniería de tráfico. Por lo que el modelo de red "IP sobre ATM" (*IP/ATM*), facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de enrutadores IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los enrutadores de la periferia. Cada enrutador se comunica con el resto mediante los PVCs (*Permanent Virtual Circuit)* que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los enrutadores de la periferia. Estos sin embargo desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los enrutadores ven los PVCs como enlaces punto a punto entre cada par [1].

En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas. Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte de datos que proporcionan los conmutadores. La ingeniería de tráfico se hace a base de proporcionar a los enrutadores los PVCs necesarios, con una topología lógica entre enrutadores totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los subinterfaces en los enrutadores con los PVCs, a través de los cuales se intercambian los enrutadores la información de enrutamiento correspondiente al protocolo interno IGP. Lo habitual es que, entre cada par de enrutadores, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal [2].

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes. Existe, además, lo que se llama la "tasa

impuesta por la celda", un overhead aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada. Piénsese por ejemplo en una red con 5 enrutadores externos con una topología virtual totalmente mallada sobre una red ATM. Son necesarios 5 x 4 =20 PVCs, uno en cada sentido de transmisión. Si se añade un sexto enrutador se necesitan 10 PVCs más para mantener la misma estructura (6 x 5=30). Una paga adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP.[2]

Como conclusión, podemos decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas. El MPLS, tal como se verá a continuación, logra esa integración de niveles sin discontinuidades.

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señalas anteriormente. Esas técnicas se conocieron como "conmutación IP" (*IP switching*) o "conmutación multinivel" (*multilayer switching*). Una serie de tecnologías privadas -entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Enrutador (CSR) de Toshiba condujeron finalmente a la adopción del actual estándar MPLS (*Multiprotocol Label Switching: conmutación de etiquetas multiprotocolo*) es un estándar del IETF (*Internet Engineering Task Force*) que surgió para unificar las diferentes soluciones que los distintos fabricantes estaban proponiendo. De tal manera que MPLS logra integrar sin discontinuidades los niveles 2 (transporte) y 3 (red). Por lo que se dice que MPLS se puede presentar como un sustituto de la conocida arquitectura IP/ATM ó como una tecnología que le adiciona orientación a conexión a las redes IP.

1.1.2. Ventajas de utilizar MPLS

La naturaleza de orientación a conexión de MPLS se logra con la adición de una pequeña etiqueta de longitud fija al principio de los paquetes IP. En lugar de que el enrutador IP tome una decisión de envío basada en una larga operación de búsqueda y comparación del prefijo de la dirección IP del destino, los paquetes son enviados con base en la operación de busqueda exacta de la etiqueta de MPLS. Es de esta manera como MPLS soluciona varios de los problemas que presenta una red IP, otorgando así las siguientes ventajas:

Ingeniaría de Tráfico

La ingeniaría de tráfico permite forzar a determinados paquetes a seguir una ruta particular, para encontrar el mejor camino para un determinado tipo de tráfico, puede seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). También permite a la red re-enrutar el tráfico rápido y automáticamente cuando se detectan condiciones de falla o congestión.

Diferenciación de niveles de servicio mediante CoS.

CoS *(Class of Service)* provee diferentes categorías especificas de servicio. Los paquetes pertenecientes a una misma Clase de Servicio tienen en común los mismos requerimientos de tratamiento en cuanto a ancho de banda necesario, retardo, variación del retardo (*jitter*) y pérdida de paquetes, es decir, de QoS (*Quality Service*). Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades.

Servicio de VPN

Una red VPN (*Virtual Private Network)* se puede definir como una red en la que la conectividad entre múltiples lugares se realiza a través de una infraestructura compartida con las mismas políticas de acceso y seguridad que en una red privada, por lo que le permite a los usuarios seguridad y privacidad.

Precio-Rendimiento

MPLS permite conseguir la simplicidad del reenvío de las tecnologías de conmutación de la capa 2 (enlace de datos) manteniendo la flexibilidad y escalabilidad del enrutamiento de la capa 3 (capa de red). En general un enrutador es un dispositivo de nivel 3, reenvía paquetes IP, mientras que un conmutador es un dispositivo de nivel 2, reenvía paquetes de nivel 2. Un conmutador es más simple que un enrutador y soporta un número más limitado de protocolos y características. El algoritmo de reenvío de un conmutador es mucho más simple que el de enrutador. El precio de un enrutador es mayor que el de un conmutador, pero éste suele ser más rápido que aquel. Esto es debido a que básicamente lo único que hace un conmutador es reenviar paquetes. Gracias a la conmutación de etiquetas se tienen dispositivos con características de precio/rendimiento de un conmutador, pero con la funcionalidad de un enrutador [3].

Figura 1.1.2.1. Dispositivo con las características de un conmutador, pero con la funcionalidad de un enrutador.

MPLS es independiente de la tecnología de transporte

MPLS dispone de los medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes (Ethernet, DWDM, ATM y Frame Relay, etc) , es decir, las conexiones MPLS pueden existir desde una capa de una red, hasta y a través de otra, incluso si esas redes están compuestas de múltiples tecnologías de transporte. Además, los nuevos estándares permitirán a IP/MPLS convertirse en el plano de control común para otras tecnologías de transporte como DWDM y conmutadores ópticos. En este caso, las lambdas también serían tratadas como parte de una conexión MPLS, de tal modo también controlados por IP.

Escalabilidad

Otro de los problemas del *modelo superpuesto* consiste en que tenemos una red completamente mallada: todos los enrutadores están conectados entre sí. Cada conmutador tendrá n x (n-1) vecinos (siendo n el número total de conmutadores). El hecho de que haya conmutadores entre los enrutadores no hace que no sigan apareciendo directamente conectados en el nivel de red.[4]

Si hubiera un cambio en la topología del núcleo de la red, la cantidad de información de actualización de rutas que se deberían transmitir entre sí los enrutadores, sería muy elevada. Aumentando el número de enrutadores, llegará un momento en que la cantidad de información transmitida será tal que el rendimiento caerá exponencialmente.

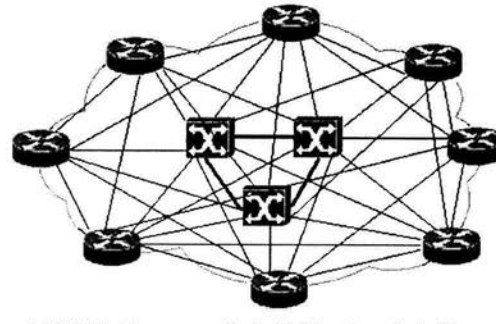


Figura 1.1.2.2. Modelo superpuesto. Red totalmente mallada. Sin usar MPLS

De nuevo, la solución al problema anterior la encontramos en la conmutación de etiquetas. Como vimos antes, los enrutadores están acoplados a los conmutadores por lo que tendremos menos vecinos y por tanto una alta escalabilidad.

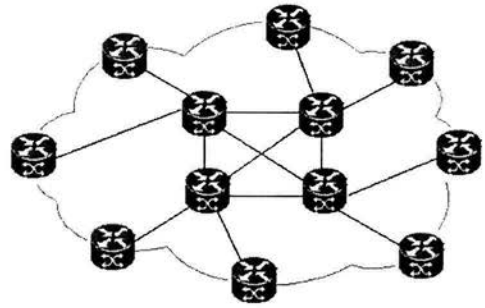


Figura 1.1.2.3. Modelo acoplado. Red de alta estabilidad, usando MPLS

Velocidad y retardo

El reenvío tradicional basado en software es demasiado lento para manejar las grandes cantidades de tráfico de Internet o de las redes interconectadas. El tiempo de la búsqueda en las tablas de enrutamiento es demasiado elevado aún teniendo en cuenta métodos de aceleración de la búsqueda. Esto se traduce en pérdida de paquetes y conexiones, y por tanto en un bajo rendimiento.

La conmutación de etiquetas es más rápida. El motivo es simple, el valor de la etiqueta que se pone en la cabecera de los paquetes es el que se usa para acceder a la tabla de enrutamiento del enrutador, es el índice para acceder a la tabla. Esto requiere un solo acceso a la tabla, cómo tenemos el índice, accedemos directamente. Por tanto, el tiempo para transmitir un paquete es menor que con el enrutamiento tradicional IP, el cual revisa un tabla de enrutamiento para analizar la dirección IP destino [5].

De los argumentos anteriores podemos decir que el protocolo MPLS añade a las redes basadas en IP funciones que mejoran el desempeño de la interconexión de redes, por lo cual los servicios de telecomunicaciones son mejorados, sin embargo en México, el uso de este protocolo apenas inicia y prácticamente no existen ingenieros familiarizados con dicho protocolo, lo cual implica una falta de recursos humanos para la implantación de éste en nuestro país. Es por eso que surge la idea de realizar un trabajo en el cual se analicen las principales características del protocolo MPLS, sus ventajas sobre IP y aplicaciones.

1.2. Objetivos de la tesis

El objetivo general de este trabajo es analizar de qué manera influirá el protocolo MPLS sobre las nuevas tecnologías basadas en IP para soportar servicios integrados de voz y datos de banda ancha sobre un solo enlace y como impactará en los mercados de las telecomunicaciones.

Los objetivos específicos de este trabajo se plantearon de la siguiente manera:

- Explicar y conocer los motivos que llevaron a los desarrolladores e investigadores de redes, a crear MPLS. Esto implica revisar protocolos anteriores, problemáticas generadas por sus limitaciones y soluciones formuladas antes de MPLS.

- Conocer las ventajas que añade MPLS a el protocolo IP.

- Conocer las características de MPLS, su arquitectura y funcionamiento.

- Analizar el futuro de MPLS en el mercado de las telecomunicaciones.

REFERENCIAS

[1] MPLS: Una arquitectura de backbone para la Internet del siglo XXI, José Barberá
www.rediris.es/rediris/boletin/53/enfoque1.1.gif

[2] Curso de Teleducación sobre MPLS, Fernando Alcober Bayo, Mayo 2001
http://www.fi.upm.es/~jgarcia/Curso_MPLS/capitulo1.html

[3] Marconi presenta los logros del MPLS en la demostración de interoperabilidad
www.quetzal.uis.edu.co/ciee-html/seminario_convergencia/

[4] Advanced MPLS Design and Implementation, Vivek Alwayn, Cisco Press, pag 35

[5] Li-T. MPLS and the evolving Internet architecture. IEEE Communications Magazine. Diciembre 1999. Volumen 37. Número 12

CAPÍTULO 2

2. EVOLUCIÓN DE LAS REDES

Las redes han evolucionado desde su creación y seguirán evolucionando a medida que la tecnología de conectividad que las soporte, se siga desarrollando.

Esta evolución se ha llevado a cabo en los últimos diez años y corresponde en mucho, al desarrollo de nuevas corrientes en la gestión de los Servicios Informáticos, el surgimiento de nuevos productos y tecnologías y a las nuevas utilidades que la computación y las redes presentan a la comunidad, las empresas y las instituciones en general.

Las redes de comunicación surgieron a partir de la necesidad que tenían los usuarios de compartir un conjunto diverso de recursos distribuidos, dichas redes se convirtieron en el vehículo que permitió el intercambio de información. En el caso de las redes LAN (*Local Área Networks*) prevalecieron las llamadas redes de difusión. Una red de difusión es aquella en la cual todas las estaciones comparten el canal de comunicaciones y cuando una de ellas transmite, todas las demás la escuchan.

Dos formas básicas de interconexión y de acceso al canal de comunicaciones pugnaron por obtener la supremacía; de un lado estaban las redes con topología en bus, y por otro las redes que tenían topología en anillo. En las redes con topología en bus el acceso al canal se resolvía por contienda, ello daba lugar a frecuentes colisiones entre las estaciones que deseaban transmitir. En las redes que tenían topología en anillo un "testigo" (token) mediaba el acceso al canal, sólo aquella estación que tenía en su poder el testigo podía enviar información a través del canal. Razones de orden económico hicieron que las redes con topología en bus y con protocolo de acceso al canal basado en contienda prevalecieran. Las redes del tipo Ethernet, como fueron conocidas, reinan desde entonces en el ambiente de las redes locales, el hecho de pugnar por el canal, de generar colisiones, tiene un efecto directo sobre el desempeño de la red ya que resulta imposible predecir con exactitud el momento en el cual una estación de la red pueda transmitir. En esta evolución histórica, las redes Ethernet de medio compartido se constituyen en el punto de partida [1].

Cabe una pregunta: ¿Cómo se implementaron las redes Ethernet de medio compartido? Este tipo de redes utilizaban generalmente cable coaxial delgado, del tipo RG-58, y conectores del tipo BNC. La topología física de la red era en bus y se instalaba en cada estación una tarjeta de red que tenía una interfaz física que la conectaba al canal. No existía ningún tipo de jerarquía, la red era completamente plana y la topología física (la forma como se interconectaban las estaciones) coincidía con la topología lógica (la forma como las estaciones pugnaban por el uso del canal).

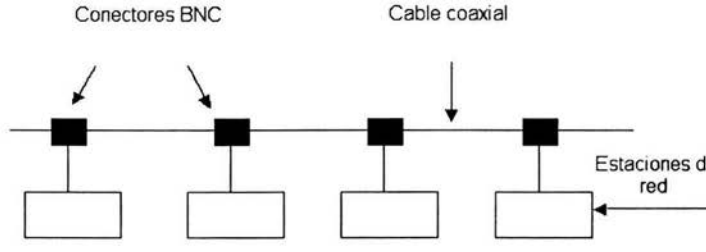


Figura 2.1 Red Ethernet de medio compartido basado en cable coaxial

Las estaciones de red interconectadas con topología en bus dieron lugar al concepto de dominio de colisión. Un dominio de colisión es el conjunto de todas aquellas estaciones que en un momento dado pugnan o compiten por el uso del canal. En la medida que el dominio de colisión sea más grande, mayor será el número potencial de colisiones, y por consiguiente, menor el desempeño de la red. Como se verá un poco más adelante, el incremento en el número de usuarios que hacen parte de una red corporativa tendrá efectos devastadores sobre este tipo de redes.

Las redes Ethernet de medio compartido fueron muy populares en las organizaciones, sin embargo, muy pronto las dificultades empezaron a surgir; la administración y la solución de problemas se volvieron prácticamente inmanejables. Los conectores del tipo BNC obligaban a cortar físicamente el cable coaxial y cuando, por alguna razón, se desconectaba el segmento físico de cable del conector, la conexión en bus desaparecía y la comunicación no era posible, existían entonces N puntos de falla en la red, tantos como estaciones hubiera [2].

El siguiente paso en la evolución tuvo lugar con la aparición de los sistemas de cableado estructurado. La gran mayoría de las dificultades asociadas con la administración en las redes Ethernet de medio compartido basadas en cable coaxial se encontraban en el nivel físico; el cableado estructurado resolvió muchas de estas dificultades.

El cable coaxial fue cambiado por cable UTP (*Unshielded Twisted Pair*), lo cual significó un retroceso en términos del canal, dado que las características de transmisión del cable coaxial son superiores a las ofrecidas por el cable UTP. Sin embargo, la diferencia fundamental radicó en la utilización de un concentrador (hub), el cual se constituyó en el núcleo de una topología física en estrella que permitió centralizar muchas de las tareas de administración. Ahora, en lugar de ir de estación en estación tratando de localizar una falla, se visitaba el cuarto de cableado y se revisaba el estado de cada uno de los puertos del concentrador para encontrar la fuente de las dificultades.

El cableado estructurado produjo un cambio significativo en la estructura de la red. A partir de este momento las redes tienen una topología punto a punto, son redes que físicamente tienen una topología en estrella, sin embargo; y gracias al comportamiento del concentrador, la topología lógica de la red seguía siendo en bus, cuando una estación "habla" (transmite sobre el canal), el concentrador se encarga de repetir aquello que "escuchó" a cada uno de los puertos restantes, es decir, "cuando alguien habla, todos escuchan" (el principio operativo de las redes de difusión en bus). En conclusión, el gran aporte del cableado estructurado fue el permitir tener una topología física diferente a la topología lógica, las redes se configuraban en estrella pero seguían siendo redes de medio compartido, estaban basadas en cable UTP y no existía ninguna relación jerárquica, la red era completamente plana (Ver Figura 2.2).

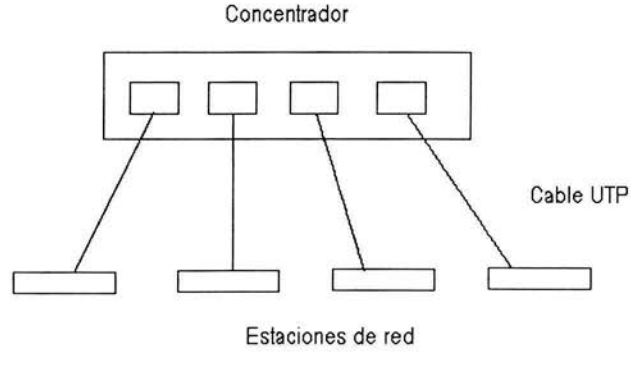


Figura 2.2 Cableado estructurado. Red Ethernet de medio compartido, basada en cable UTP.

Hasta ahora los fenómenos que hemos analizado son de carácter eminentemente tecnológico, específicamente en el área del hardware. Sin embargo, es tiempo de echar un vistazo a lo que está ocurriendo en ese mismo instante en el software y en la organización.

En las empresas, el número de usuarios conectados a la red crece día a día. Hasta entonces, la tarjeta de red era un periférico que se cotizaba de forma independiente y opcional por parte del proveedor; a partir de este instante, los equipos de procesamiento de datos tienen incorporada la tarjeta de red en su configuración estándar porque se supone que serán utilizados como estaciones de red. En el software, se incrementa significativamente el número de aplicaciones que operan en ambiente de red; por otra parte, el tamaño de los bloques de información que son transmitidos a través de la red también se amplía.

Estamos entonces ante una situación en la cual se aumenta el número de usuarios de red, el de aplicaciones de red y el tamaño de los bloques de información que transitan a través de ella. El resultado: un incremento exponencial en el tráfico que la red debe administrar y es aquí donde debemos pagar el precio de haber optado por una tecnología de contienda en el uso del canal. El crecimiento desmesurado en el volumen de tráfico generado en el dominio de colisión produjo un colapso en las redes, a este colapso se lo denominó la "crisis del ancho de banda": la demanda de ancho de banda de los usuarios y sus aplicaciones empezaba a superar la oferta que era capaz de presentar la red.

Para enfrentar este desafío se presentaron dos posibles soluciones: la utilización de tecnologías de alta velocidad y la segmentación. La primera implicaba desarrollar o actualizar mecanismos que permitieran enviar una mayor tasa de bits por segundo en el canal, aquí también se presentaron dos posibles soluciones: la primera, romper de una vez por todas con las redes Ethernet y repensar el mecanismo de acceso al medio surgiendo alternativas como FDDI (*Fiber Distributed Data Interface*), una propuesta de ANSI (*American National Standards Institute*) para contar con un anillo en fibra óptica a 100 Mbps; la otra tecnología representante de esta variante fue 100 *VGAnyLAN* en la que también se replanteaba el mecanismo de acceso al medio. El optar por este camino hubiera significado, en todos los casos, haber cambiado todas las tarjetas de comunicación tanto de las estaciones de red como de los equipos de interconectividad, aspecto que desde el punto de vista económico y práctico resultaba inmanejable. La segunda de las soluciones proponía incrementar la tasa de transmisión de la Ethernet convencional; en lugar de contar con un canal de capacidad nominal de 10 Mbps, se dispondría de un canal de 100 Mbps, esta alternativa fue la que finalmente se impuso y parecía que iba a ser la solución definitiva a la "crisis del ancho de banda" a no ser por un aspecto de trascendental importancia: este enfoque de solución se concentraba en atacar los síntomas del problema pero no en resolver las causas del mismo, si bien resultaba posible contar con un canal de mayor capacidad no se hacía nada respecto del tamaño del dominio de colisión, la fuente del problema. De hecho, la misma realidad se ha encargado de mostrarnos que este enfoque no se ha constituido en solución, los desarrollos de GigabitEthernet y de 10GigabitEthernet así lo demuestran. La otra posible ruta de solución al problema de la crisis del ancho de banda estaba en la segmentación. Segmentar una red implica descomponer un dominio de colisión en dos o más, de tal

manera que se disminuya el número de estaciones de red que pugnan por el uso del canal. Este enfoque de solución realmente enfrenta las causas del problema y provocó un replanteamiento en el diseño y en la estructura de la red (Ver Figuras 2.3 y 2.4)

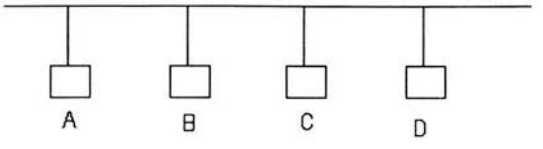


Figura 2.3 Un solo dominio de colisión

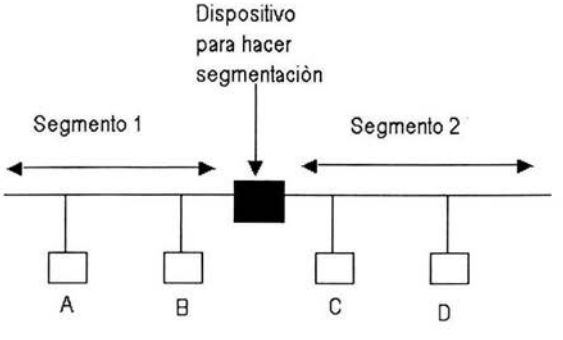


Figura 2.4. Dominios de colisión

Surge una pregunta: ¿Cómo se puede efectuar una segmentación de la red? Inicialmente, la segmentación fue realizada utilizando puentes (*bridges*) o enrutadores (*routers*). Sin embargo, aunque la orientación de la solución era la adecuada, su implementación no lo era. Los puentes y los enrutadores son dispositivos de interconectividad, por principio filosófico de operación, su tarea fundamental es la de conectar redes, entonces, ¿cómo podrían ser empleados para producir el efecto contrario?.

En estos dispositivos se aprovechaba el proceso de filtrado, uno de los procesos básicos que gobiernan su operación para efectuar la segmentación. Detallemos un poco más en qué consiste el proceso de filtrado: cuando la estación A desea enviar información a la estación B, resulta claro que tanto la estación origen como la estación destino se encuentran en el mismo segmento de red, por lo tanto, el dispositivo de interconectividad (el enrutador o el puente). No retransmiten la información hacia el otro segmento. Ello permite que C pueda estar simultáneamente hablándole a D, de esta manera, el tamaño de los dominios de colisión se hace más pequeño y en promedio cada estación tendrá la posibilidad de transmitir una mayor cantidad de información.

Surgió entonces la necesidad de contar con un dispositivo que permitiera realizar la segmentación de las redes: El conmutador, un dispositivo especializado en realizar conmutación de tramas. En esencia, un conmutador no es otra cosa que un bridge multipuerto con hardware especializado en conmutación. Cada uno de sus puertos da lugar a un dominio de colisión independiente permitiendo, en el mejor de los casos, que toda la capacidad de canal se asigne a una estación de red. El conmutador cambió sustancialmente el diseño de la red, permitiendo la evolución desde una red de medio compartido hasta una red de medio dedicado. (Ver Figura 2.5) La presencia del conmutador da lugar a dos segmentos. En el primero, las estaciones A y B constituyen el primer dominio de colisión, y en el segundo, la estación C constituye el segundo dominio de colisión. En este caso, la estación C no pugna con ninguna otra por el acceso al canal [3].

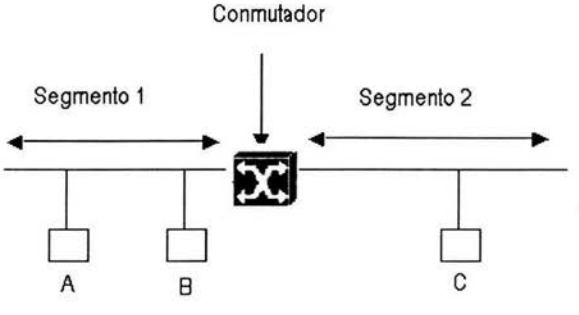


Figura 2.5 Segmentación utilizando conmutador. Red de medio dedicado

A esta forma de segmentación en la cual no existe pugna por el canal se la denominó microsegmentación. Con el advenimiento de la microsegmentación, la contienda por el uso del canal resulta inútil, se hace necesario efectuar una modificación sobre el mecanismo de acceso al canal.

Hasta ahora, las redes tenían una estructura plana, no existía una jerarquía. El siguiente paso en la evolución estuvo determinado por el establecimiento de una jerarquía en los conmutadores de la red (Ver Figura 2.6).

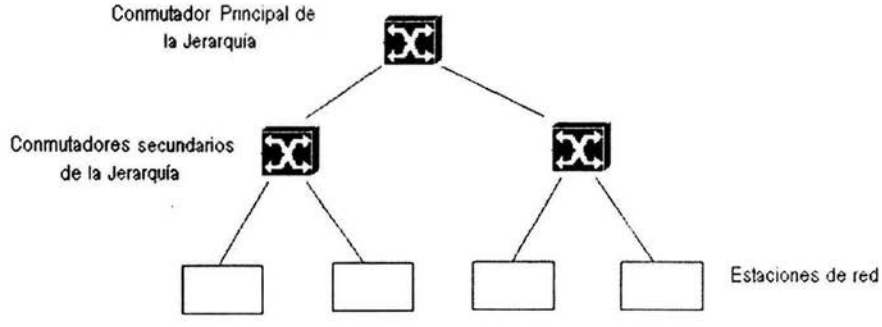


Figura 2.6 Estructura jerárquica de una red

La estructura mostrada en la Figura 2.6 ha sido denominada de "backbone colapsado", en ella, vale la pena anotar lo siguiente: los enlaces entre los conmutadores (principal y secundarios) son generalmente enlaces en fibra óptica, los enlaces entre los conmutadores secundarios y las estaciones de red son generalmente enlaces en cable UTP. Vemos entonces cómo en la red se produce una mixtura de medios físicos; por otra parte, se dice que el backbone colapsó porque el backbone de la red se encuentra ahora distribuido entre los conmutadores y los enlaces de fibra que los comunican. Igualmente, la capacidad de los enlaces no es uniforme como lo era en la etapa evolutiva previa, ahora resulta posible tener enlaces de capacidad entre los conmutadores, o entre los conmutadores y los servidores (Ethernet a 100 Mbps o Fast Ethernet) y enlaces convencionales (Ethernet a 10 Mbps) entre los conmutadores y las estaciones de red que hacen las veces de clientes [4].

Tenemos entonces ahora una red jerárquica, de medio dedicado, con enlaces de alta capacidad en el backbone. En este punto del proceso evolutivo, parece ser que todas las posibles mejoras que se podían realizar en el nivel de enlace de datos han sido efectuadas. Para entender el próximo paso en la evolución de la red necesitamos entender el concepto de dominio de broadcast. Un dominio debroadcast es el conjunto de aquellas estaciones que "escuchan" un mensaje de broadcast (un mensaje generado por una estación en particular para todas las estaciones que componen la red). El conmutador, como dispositivo de nivel dos, es incapaz de contener el tráfico de broadcast, este tipo de tráfico sólo puede ser limitado por un enrutador, precisamente un dispositivo de nivel tres. El broadcast

excesivo tiene un efecto indeseado sobre el desempeño de la red, en primer lugar porque la congestiona (es tráfico que efectivamente viaja a través de los diferentes enlaces) y en segundo lugar porque al estar dirigido hacia todas las estaciones debe ser procesado por ellas, lo que implica un consumo de recursos de cómputo en cada estación. Muchos protocolos y servicios de red utilizan el broadcast como estrategia de notificación a las demás estaciones de la red, por esta razón un diseñador de red debería tratar de evitar su excesiva proliferación.

De la misma manera que en un momento dado se hizo necesario hacer más pequeños los dominios de colisión, en este punto del proceso evolutivo necesitamos limitar el alcance del dominio de broadcast. Sin embargo, como lo dijimos anteriormente, el conmutador es incapaz de contener el tráfico de broadcast, se hace necesario entonces ascender un nivel e ir desde el nivel 2 (nivel de enlace de datos) hasta el nivel 3 (nivel de red) para resolver el problema.

Para contener o limitar el tráfico de broadcast se han propuesto dos opciones: Una, la utilización de VLANs (*Virtual LAN*) , y la otra, extender el concepto de conmutación al nivel tres y utilizar conmutadores de nivel tres. Una red virtual, como su nombre lo sugiere, es un agrupamiento virtual de nodos en un dominio de broadcast, el administrador de la red, utilizando alguna herramienta de software, realiza dicho agrupamiento. La gran ventaja derivada de la utilización de las VLANs es que permiten contener el tráfico de broadcast y efectuar una separación de los flujos de tráfico. Para permitir la comunicación entre usuarios que pertenecen a diferentes redes virtuales es necesario utilizar una función de nivel tres, a través de un enrutador o de un conmutador de nivel tres [5].

Ya habíamos hecho referencia a las dificultades, en cuanto a costo y desempeño, que ofrece un enrutador como alternativa de segmentación. Sin embargo, para salvar estas dificultades se propuso una solución: utilizar en el ambiente LAN un dispositivo especializado en conmutación, implementado completamente en hardware y especializado en el manejo del protocolo IP, a este dispositivo se lo conoce como conmutador de nivel tres. El desarrollo del conmutador de nivel tres permite contar en la red de área local con un dispositivo de alto desempeño capaz de realizar las tareas de un enrutador. Surge una pregunta: ¿Cuáles son las consecuencias que se derivan de estos nuevos desarrollos? Para responder tendríamos que decir que la estructura de las redes evoluciona hacia una estructura jerárquica en varios niveles y que esta red utiliza diferentes niveles de conmutación (conmutación de nivel dos y conmutación de nivel tres) con diferentes velocidades de acceso al medio (10 Mbps, 100 Mbps y 1000 Mbps).

Cisco propone una estructura para la red constituida por tres niveles: El nivel de acceso, el nivel de distribución y el nivel núcleo (o "core" de la red). Las responsabilidades de cada nivel son complementarias, el establecer una jerarquía para la red permite realizar un diseño modular y

funcionalmente especializado. El nivel de acceso es el punto de entrada a la red; en este nivel de la jerarquía se conectan las estaciones del usuario, generalmente el acceso se realiza utilizando un hub o un conmutador de nivel dos. Este nivel corresponde con un área funcional de la organización y permite la transferencia de información entre las personas que hacen parte del grupo de trabajo (*workgroup*). El siguiente nivel dentro de la jerarquía corresponde con el nivel de distribución; este nivel se constituye en el punto de acceso a los diferentes grupos de trabajo. Por la naturaleza de su ubicación, es el sitio en donde se imponen las más fuertes restricciones de acceso y de seguridad, en este nivel encontramos funciones típicas de nivel tres. Finalmente, se encuentra el nivel de núcleo ("*core*") que corresponde con el backbone de la red; este nivel se encarga de transportar grandes volúmenes de datos a gran velocidad. Para poder cumplir con su objetivo es necesario que no se impongan grandes restricciones ni verificaciones al tráfico que circula a través de este nivel de la jerarquía (Ver Figura 2.7).

Cabe aquí un nuevo concepto: *"Multilayer Conmutadoring"* como resultado de la evolución de las tecnologías LAN y de interconectividad. Los dispositivos multinivel combinan características del nivel dos (nivel de enlace de datos) y del nivel tres (nivel de red) en conmutadores híbridos que pueden enrutar paquetes a velocidades de hardware. Un conmutador básico es un puente multipuertos, como ya se mencionó estos conmutadores fueron desarrollados para permitir la microsegmentación en redes locales. A medida que la tecnología evolucionó se le adicionaron funciones de enrutamiento en hardware y la posibilidad de analizar aquella información contenida en los paquetes que pudiera colaborar en el proceso de envío; de esta forma, los conmutadores multinivel son dispositivos que examinan la información relacionada con los niveles 2 hasta el 7 del modelo OSI [6] .

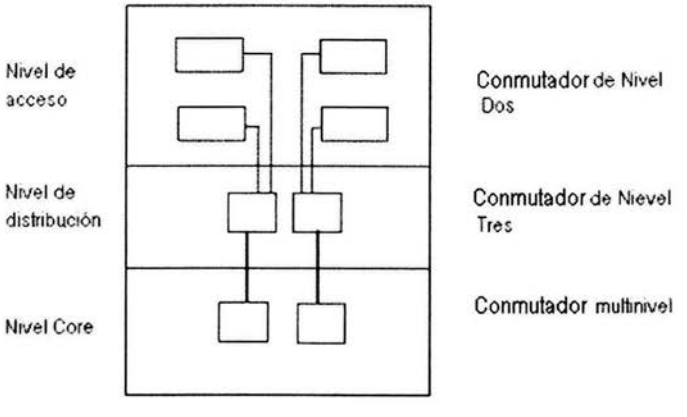


Figura 2.7 Dispositivos de interconectividad en los diferentes niveles de la estructura jerárquica de la red

Estamos entonces en un estado evolutivo en el cual la estructura de la red es jerárquica, el dispositivo de interconectividad que reina es el conmutador. Teniendo en cuenta la convergencia (un componente que le agrega complejidad al diseño), las redes de hoy, más que redes de datos, son redes de información: flujos de información de datos, de voz y de video surcan las redes modernas, los dispositivos de interconectividad deben estar en capacidad de reconocerlos y darles un tratamiento diferenciado, aspecto este al que llamaremos "calidad de servicio". La red debe estar en capacidad de comprometerse a ofrecer servicios de diferente tipo, dependiendo del tipo de información que se quiera transferir a través de ella, los requerimientos de retraso en la transferencia, de variación del mismo (varianza) y de capacidad de transmisión deben ser reconocidos y entendidos por los diferentes dispositivos que conforman la arquitectura de una red [6].

Toda esta reflexión nos conduce a pensar en la necesidad de contar con una metodología que permita abordar con éxito el proceso de diseño de una red. Existen razones de orden económico y tecnológico que lo justifican; por una parte, la red se ha convertido en un recurso estratégico para la organización, muchos de sus procesos y aplicaciones corren sobre ella; por lo tanto, se imponen requerimientos de alto desempeño y de alta disponibilidad. Por otra parte, según lo hemos venido mostrando en este capitulo, la estructura de la red se ha vuelto jerárquica, funcionalmente modular, con tecnologías de conmutación (*conmutadoring*) de diferente nivel y capacidad de transmisión variable en cada uno de sus niveles. La red corporativa ha adquirido el compromiso de ofrecer servicios diferenciados a aplicaciones y usuarios que necesitan transferir información de carácter multimedia a través de ella. Y es MPLS el capaz de llevar al éxito esta conmutación multinivel, gracias a la conmutación de etiquetas. Por lo que MPLS permitirá que sea posible la evolución de las redes, logrando avanzar hacia mejores estructuras, y logrando cumplir con los requerimientos que los proveedores de servicio requieran.

REFERENCIAS

[1] Evolución de las Redes, Econ. Félix Murillo Alfaro Jefe del INEI
www.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5009/cap0105.htm

[2] Redes de próxima generación
http://iio.ens.uabc.mx/~jmilanez/escolar/redes/01040000.html

[3] Redes de comunicaciones y aplicaciones distribuidas, pasado, presente y futuro
http://eia.udg.es/~atm/grup_docencia/xdsi/xdsi_tema1/sld003.htm

[4] Visión del mercado de redes, Ingeniero humberto de la cota
www.internet.uson.mx/webpers/hcota/evolucion

[5] Evolución de la arquitectura de las redes, Ing. Alvaro Pachón D.
www.icesi.edu.co/es/publicaciones/publicaciones/contenidos/sistemas_telematica/1/apachon_evoluc-redes.pdf

[6] Evolución de las redes de datos. Revista de telecomunicaciones de Alcatel.-tercer trimestre 2002.-
G. Hoebeke, P. Meyeres , T. Nguyen

CAPÍTULO 3

3. PROTOCOLO IP

3.1. Introducción

La Internet es una red de redes, miles de redes basadas en tecnologías heterogéneas se enlazan en la Internet ofreciendo un conjunto homogéneo de servicios. Mas aun en la Internet se encuentran ordenadores muy diversos con sistemas operativos diferentes, desde ordenadores de sobremesa PC o Macintosh hasta grandes sistemas IBM o digital.

En general una red de comunicaciones se compone de diferentes medios, los cuales deben garantizar la comunicación entre sí de todos los equipos conectados a la red. El nivel de red (del modelo de referencia OSI) oculta los detalles del medio, ofreciendo al usuario la imagen de una única red, aunque dicha red esté formada por varias redes distintas en medios físicos diferentes, y es ahí en la capa de red donde opera el protocolo IP como el principal elemento que permite integrar las distintas redes entre si. El protocolo IP (*Internet Protocol*) enlaza las diferentes piezas (distintas redes: FDDI, RDSI, X.25, líneas dedicadas, token ring, Ethernet, líneas telefónicas,...) de la Internet, por lo que es encargado de identificar cada uno de los paquetes que pasan por la capa y de seleccionar la mejor ruta posible entre los host que desean comunicarse.

Funciones Principales de IP

- Aceptar y transportar los datos provenientes de TCP o UDP.
- Crear un datagrama de IP, enrutarlo por la red y entregarlo a una aplicación destino.
- Adaptarse a las características del medio.

3.2. Características del protocolo IP

1. Transmisión de datos en datagramas (paquetes IP).
2. No está orientado a la conexión, por lo que los paquetes que circulan entre los host son tratados de forma independiente, lo que origina que cada uno pueda seguir una trayectoria diferente en su viaje hasta el host destino., es decir, cada datagrama puede seguir una ruta cualquiera del origen al destino, por lo que pueden llegar en desorden o duplicados. Es imposible manejar aplicaciones de voz y miltimedia en tiempo real.
3. No es confiable. Realiza el "mejor esfuerzo" para el transporte de paquetes y no garantiza su entrega. No implementando mecanismos de verificación de entrega de los paquetes, por lo que no garantiza la entrega de los mismos, ni la entrega en secuencia, ni la entrega única. IP no garantiza la entrega fiable de los datagramas al host destino, los datagramas se pueden destruir porque los paquetes pueden perderse, dañarse o llegar retrasados debido a:

    - Errores en los bits durante la transmisión por el medio.
    - Que un enrutador congestionado descarto el datagrama debido a la falta de espacio en el bufer.
    - Temporalmente, no había camino hasta el destino.

4. Todas las funciones que aseguran la fiabilidad del envío y entrega de datos se ha concentrado en la capa de TCP como vimos con anterioridad. IP sólo hace lo mejor por entregar estos datagramas de un extremo a otro. Esto queda en manos del protocolo TCP de la capa superior.
5. No implementa corrección de errores ni control de congestión.
6. Puede fragmentar los paquetes, si es necesario. IP utiliza también, técnicas de fragmentación y reensamblado más temporizadores de datagramas que permiten enrutar los datagramas a través de enrutadores congestionados o pasar de redes con grandes prestaciones a redes pequeñas y de baja calidad de tráfico. Esto hace posible que un datagrama de IP atraviese el continente pasando por una gran variedad de tecnologías de comunicación que van desde las redes de telefonía básica hasta los enlaces dedicados por satélite o fibra óptica y viceversa.
7. Direcciona los paquetes mediante direcciones lógicas IP de 32 bits (IP v4). Cada máquina de la red Internet tiene una dirección IP única. Una dirección IP es un número de 32 bits que normalmente se escribe como cuatro enteros entre 0 y 255 separados por puntos (192.112.36.5), la dirección IP permite el enrutamiento de la información a través de la Internet.
8. Sólo verifica la integridad del paquete en sí, no los datos que contiene.

9. Asigna tiempos de vida (TDV oTTL) a los datagramas de IP. Cada datagrama de IP tiene un Tiempo de Vida que expira según se configure el temporizador por TCP, ésto provoca la retransmisión del datagrama por parte de TCP.

Sus misiones más importantes son pues definir la unidad básica para la transferencia de datos en una red interna, especificando el formato exacto de un datagrama IP, realizar las funciones de enrutamiento (direccionamiento de los paquetes), definir las reglas para que los host y enrutadores procesen paquetes, los descarten o generen mensajes de error. Para el direccionamiento de los paquetes, el protocolo IP examina la topología de la red para determinar la mejor ruta de envío. A pesar de estas características, que parecen dar a entender que es un protocolo poco fiable, IP es fundamental para poder intercomunicar diferentes redes, hasta tal punto que constituye el pilar sobre el que se ha construido Internet. Para dar confiabilidad al sistema se usan tanto los protocolos de las capas superiores como los de la Capa de Enlace de Datos, encargándose IP tan sólo del enrutamiento de paquetes entre los host que se comunican.

IP se encuentra actualmente en su versión 4, usando longitudes de dirección de 32 bits. Aunque el número de direcciones posibles parece suficiente (2^{32}=4.294.967.296), las direcciones IP v4 han sido agotadas prácticamente en la actualidad. Para suplir esta carencia, así como para solventar otros problemas inherentes a su propia naturaleza, se están realizando estudios para ampliar y mejorar el protocolo. Inicialmente se quiso implementar la versión 5 del mismo, pero la arquitectura en que se basó la hizo inservible, por lo que actualmente los estudios van dirigidos a IP v6, que parece será suficiente para dar al protocolo IP las funcionalidades necesarias. Pero mas adelanté veremos como MPLS da solución a este problema y a muchos mas de IP.

3.3. El datagrama IP

El esquema de envío de IP es similar al que se emplea en la capa de acceso. En esta última se envían tramas formadas por un encabezado y los datos. En el encabezado se incluye la dirección física del origen y del destino.

El datagrama IP es la unidad básica de transferencia entre el origen y el destino. Este datagrama viaja en el campo de datos de las tramas físicas de las distintas redes que va atravesando. El propio datagrama IP tiene también un campo de datos: será aquí donde viajen los paquetes de las capas superiores, estos también incluyen un encabezado, pero las direcciones empleadas son direcciones IP[1].

Encabezado	Datos

Figura 3.3.1. Datagrama IP

Formato del datagrama IP

Los protocolos IP de dos host que se comunican intercambian entre sí unas unidades de protocolo denominadas datagramas o paquetes IP, cuya longitud máxima es de 65.635 bytes.

IP recoge los segmentos elaborados por la Capa de Transporte, introduciéndolos en el campo de datos del datagrama, añadiéndole otros diferentes campos de encabezado. Un datagrama IP consiste en una parte de cabecera y en una parte de texto. La cabecera tiene una parte fija de 20 bytes y una opcional de longitud variable. El formato de la cabecera se muestra en la figura:

Version	Hlen	TOS	Longitud Total	
Identificación			Flags	Desplazamiento De Fragmento
TTL		Protocolo	Header Checksum	
Dirección IP de la Fuente				
Dirección IP del Destino				
Opciones IP (Opcional)				Relleno
Datos				

Figura 3.3.2. Formato de la cabecera de IP

- ***Version*** (4 bits).- Indica la versión del protocolo IP que se utilizó para crear el datagrama. La inclusión de este campo hace posible la transición entre diferentes versiones del protocolo IP, ejecutando cada máquina la mayor versión que soporte.

- **Hlen** (4 bits).- Longitud del encabezado IP en palabras de 32 bits, necesario ya que la cabecera de un datagrama no es constante. El valor mínimo de este campo es 5, y el valor máximo 15, lo que limita la cabecera a 600 bytes.

- **Tipo de servicio** (Type Of Service).-Los 8 bits de este campo se dividen a su vez de acuerdo a la "prioridad".

- **Prioridad** (3 bits).-Un valor de 0 indica baja prioridad y un valor de 7 indica prioridad máxima. Los siguientes tres bits indican cómo se prefiere que se transmita el mensaje, es decir, son sugerencias a los enrutadores que se encuentren a su paso los cuales pueden tenerlas en cuenta o no.

    - Bit D *(Delay)*. Solicita retardos cortos (enviar rápido).
    - Bit T *(Throughput)*. Solicita un alto rendimiento (enviar mucho en el menor tiempo posible).
    - Bit R *(Reliability)*. Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien).

- **Total length** (16 bits).- Indica la longitud total del datagrama expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un datagrama será de 65535 bytes. Permite calcular el tamaño del campo de datos: Datos = Longitud Total – 4 * Hlen.

- **Time to live TTL** (8 bits).- Especifica el número de segundos que se permite al datagrama circular por la red antes de ser descartado. Generalmente se implementa mediante la métrica de contador de saltos, por la cual indica el número máximo de enrutadores que puede atravesar el datagrama antes de su destrucción. En cada enrutador se resta 1 a este número. Cuando llegue a cero, el datagrama se descarta (tiempo de vida excedido), por lo que es el tiempo de espera que puede estar un datagrama en la red antes de su destrucción y es la acción necesaria para que un datagrama no entregado no vague indefinidamente por la red.

- **Protocolo** (8 bits).- Especifica qué protocolo de alto nivel se empleó para construir el mensaje transportado en el campo datos de datagrama IP: 1 para ICMP, 2 para IGMP, 6 para TCP y 17 para UDP.

- **Header checksum** (CCR) (16 bits).- Contiene la suma de comprobación de errores sólo para la cabecera del datagrama. La verificación de errores de los datos corresponde a las capas superiores. Es útil para detectar errores generados por palabras de memoria erróneas en uno de los enrutadors que atraviesa en datagrama. Se calcula haciendo el complemento a uno de

cada palabra de 16 bits del encabezado, sumándolas y haciendo su complemento a uno. Esta suma hay que recalcularla en cada nodo intermedio debido a cambios en el TTL o por fragmentación.

- **Dirección IP de la fuente** (32 bits).-Contiene la dirección IP del origen.

- **Dirección IP destino** (32 bits).-Contiene la dirección IP del destino.

- **Opciones IP.**-Este campo no es obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red y depuración).

- **Relleno.** Bits necesarios para asegurar que la longitud del datagrama séa múltiplo de 32 bits

- **Datos.** Segmento TCP/UDP de la Capa de Transporte

Fragmentación

El tamaño para un datagrama debe ser tal que permita la encapsulación, esto es, enviar un datagrama completo en una trama física. El problema está en que el datagrama debe transitar por diferentes redes físicas, con diferentes tecnologías y diferentes capacidades de transferencia. A la capacidad máxima de transferencia de datos de una red física se le llama *MTU* (el MTU de ethernet es 1500 bytes por trama, la de FDDI es 4497 bytes por trama). Cuando un datagrama pasa de una red a otra con un MTU menor a su tamaño es necesaria la *fragmentación*. A las diferentes partes de un datagrama se les llama *fragmento*. Al proceso de reconstrucción del datagrama a partir de sus fragmentos se le llama *Reensamblado de fragmentos* [11].

El control de la fragmentación de un datagrama IP se realiza con los campos de la segunda palabra de su cabecera:

- Identificación. Número de 16 bits que identifica al datagrama, que permite implementar números de secuencias y que permite reconocer los diferentes fragmentos de un mismo datagrama, pues todos ellos comparten este número.
- Banderas. Un campo de tres bits donde el primero está reservado. El segundo, llamado bit de No - Fragmentación significa: 0 = Puede fragmentarse el datagrama o 1 = No puede

fragmentarse el datagrama. El tercer bit es llamado Más – Fragmentos y significa: 0 = único fragmento o ultimo fragmento, 1 = aun hay más fragmentos. Cuando hay un 0 en más – fragmentos, debe evaluarse el campo desp. De Fragmento: si este es cero, el datagrama no esta fragmentado, si es diferente de cero, el datagrama es un ultimo fragmento.

- Desplazamiento de Fragmento (*Fragment offset*) (13 bits). Indica el lugar en el cual se insertará el fragmento actual dentro del datagrama completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor cero.

Para finalizar con el tema de fragmentación, hay que mencionar el *Plazo de Reensamblado*, que es un time out que el host destino establece como máximo para esperar por todos los fragmentos de un datagrama. Si se vence y aun no llegan todos, entonces se descartan los que ya han llegado y se solicita el reenvío del datagrama completo.

3.4. Direcciones IP

La dirección IP identifica la localización de un sistema en la red. Cada dirección IP tiene dos partes. Una de ellas, identifica a la red y la otra identifica a la máquina dentro de esa red. Todas las máquinas que pertenecen a la misma red requieren el mismo número de red el cual debe ser además único en Internet [2].

El número de máquina, identifica a una *workstation*, servidor, *enrutador* o cualquier otra máquina TCP/IP dentro de la red. El número de máquina (número de *host)* debe ser único para esa red. Cada *host* TCP/IP, por tanto, queda identificado por una dirección IP que debe ser única

Se trata de una dirección única a nivel mundial y la concede INTERNIC, Centro de Información de la Red Internet.

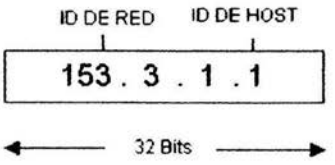


Figura 3.4.1. Formato de una dirección IP

Hay dos formatos para referirnos a una dirección IP, formato binario y formato decimal con puntos. Los 32 bits de una dirección IP contienen tanto la Identificación de red como la Identificación de *Hosts* dentro de la red. Si nos referimos al formato decimal es esta compuesto de cuatro grupos de tres dígitos separados por puntos, tal como 167.216.245.249 y cada número estará entre cero y 255.

Mientras que si hablamos de un formato binario cada número entre los puntos en una dirección IP se compone de 8 dígitos binarios (00000000 a 11111111); pero normalmente se escribe una dirección IP en la forma decimal para hacerlos más comprensibles, pero hay que tener bien claro que la red entiende sólo direcciones binarias. Para identificar que parte de los 32 bits pertenecen al identificador de red y que parte al identificador de host, es necesario saber a que clase de red pertenecen, las cuales son asignadas dependiendo el tamaño y las necesidades de la red

3.4.1. Clases de redes según las direcciones IP

La comunidad Internet ha definido 5 clases de direcciones para poder acomodar redes de diferentes tamaños. El TCP/IP de Microsoft soporta las clases A, B y C. Estas clases, definen que bits son usados para la red y cuales son usados para identificar el número de *host* dentro de la red.

Se puede identificar la clase de dirección por el número del primer octeto

1) Redes de clase A

Son aquellas redes que precisan un gran número de direcciones IP, debido al número de host que comprenden. A este tipo de redes se les asigna un rango de direcciones IP identificado por el primer grupo de 3 dígitos (primer octeto de la IP), de tal forma que disponen de los otros 3 grupos siguientes para asignar direcciones a sus host. Los 3 últimos octetos o 24 bits representan el número de host. Esto permite en total 126 redes y aproximadamente 17 millones de host por cada red.

Si expresamos una dirección IP de este tipo en formato binario, su primer bit es siempre un 0, por lo que tendremos para estas redes:

desde 00000000.xxxxxxxx.xxxxxxxx.xxxxxxxx (0.aaa.aaa.aaa)
hasta 01111111.xxxxxxxx.xxxxxxxx.xxxxxxxx (127.aaa.aaa.aaa)

Por esta causa, su primer byte tiene un valor comprendido entre 1 y 126, ambos inclusive . Las direciones 127.aaa.aaa.aaa están reservadas para tareas de diagnóstico - loopback - y no se usan.

El número de direcciones resultante es muy elevado, más de 16 millones, por lo que las redes de clase A corresponden fundamentalmente a organismos gubernamentales, grandes universidades, etc.

2) Redes de clase B

Son redes que precisan un número de direcciones IP intermedio para conectar todos sus host con Internet. A este tipo de redes se les asigna un rango de direcciones IP identificado por los dos primeros grupos de 3 dígitos (primer y segundo octetos de la IP), de tal forma que disponen de los otros 2 grupos siguientes para asignar direcciones a sus host.

Si expresamos una dirección IP de este tipo en formato binario, su dos primeros bits son siempre un 10, por lo que tendremos para estas redes:

desde 10000000.xxxxxxxx.xxxxxxxx.xxxxxxxx (128.aaa.aaa.aaa)
hasta 10111111.xxxxxxxx.xxxxxxxx.xxxxxxxx (191.aaa.aaa.aaa)

Por esto, sus dos primeros bytes deben estar entre 128.1 y 191.254. Las direcciones 128.0.aaa.aaa y 191.255.aaa.aaa están reservadas, y no se pueden usar), por lo que el número de direcciones

resultante es de 64.516. Las redes de clase B corresponden fundamentalmente a grandes empresas, organizaciones gubernamentales o universidades de tipo medio, etc.

3) **Redes de clase C**

Son redes que precisan un número de direcciones IP pequeño para conectar sus host con Internet. A este tipo de redes se les asigna un rango de direcciones IP identificado por los tres primeros grupos de 3 dígitos (primero, segundo y tercer octetos de la IP), de tal forma que disponen de un sólo grupo para asignar direcciones a sus host.

Si expresamos una dirección IP de este tipo en formato binario, su tres primeros bits son siempre un 110, por lo que tendremos para estas redes:

desde 11000000.xxxxxxxx.xxxxxxxx.xxxxxxxx (192.aaa.aaa.aaa)
hasta 11011111.xxxxxxxx.xxxxxxxx.xxxxxxxx (223.aaa.aaa.aaa)

Por lo que sus 3 primeros bytes deben estar comprendidos entre 192.1.1 y 223.254.254 (las direcciones desde 192.0.0.aaa hasta 192.1.0.aaa y desde 223.254.255.aaa hasta 223.255.255.aaa están reservadas, y no se pueden usar). El número de direcciones resultante es de 256 para cada una de las redes, por lo que éstas corresponden fundamentalmente a pequeñas empresas, organismos locales, etc.

En la siguiente tabla aparece un resumen de los tipos posibles de redes.

Clase	Primeros binarios	Primer byte decimal	Identificación de red	Identificación de host	Número de redes	Número de host
A	0	1 - 126	1 byte	3 bytes	126	16.387.064
B	10	128 - 191	2 bytes	2 bytes	16.256	64.516
C	110	192 - 223	3 bytes	1 byte	2.064.512	254

Tabla 3.4.1.1. Clases de redes

Si observas la tabla anterior verás que hay ciertos números de red que no se usan. Esto es así porque están reservados para ciertos usos concretos. De esta forma, las redes cuyo primer byte es superior a 223 corresponden a otras clases especiales.

4) Redes de clase D

Las direcciones de clase D son usadas para uso de grupos multicast. Un grupo multicast puede estar formado por uno o más hosts o por ninguno de ellos. Los 4 bits de mayor orden en el primer octeto en una clase D son siempre 1 1 1 0. El resto de bits designan el grupo especifico en el cual participa el cliente. No hay redes o Identificaciones de hosts del las operaciones de multicast. Los paquetes son pasados a una colección de hosts en una red. Solo los hosts registrados con una dirección multicasr van a recibir esos paquetes. Microsoft soporta las direcciones de clase D para las aplicaciones de datos en multicasting (radiodifusión) a los hosts en un segmento de trabajo Internet. Esto incluye WINS, Microsoft, NetShow , videoconferencias etc [3].

5) Redes de clase E

La clase E son direcciones experimentales que no están disponibles para uso general y que se reservan para uso futuro. Los 4 bits del byte de mayor orden en una clase E están siempre colocados a 1 1 1 1.

Mientras que las que empiezan con el byte 127 (nota que falta en la tabla) se usan para propósito especiales.

También hay que destacar que los valores extremos en cualquiera de los bytes, 0 y 255, no se pueden asignar a ningún host ni red, siempre que nos estemos refiriendo a una dirección pura, es decir, 63.1.0.0 es perfectamente asignable a un host por ser de clase A, pero no lo serían ni la 63.0.0.0 ni la 63.255.255.255. El número 0 se denomina dirección de red, está reservado como dirección de la propia red, y el 255 se reserva para la función broadcast en las redes Ethernet, mediante la cual, un mensaje es enviado a todas las máquinas de la red, no saliendo fuera de la misma. La dirección de broadcast hace referencia a todos los host de la misma red.

Por lo tanto, dada una red cualquiera, por ejemplo la red de clase C 220.40.12.x (donde x puede varias entre 0 y 255), tendríamos las siguientes direcciones IP:

220.40.12.0.....dirección de red
220.40.12.1 a 220.40.12.224.....direcciones disponibles para host
220.40.12.255.....dirección de broadcast

No todas las direcciones IP posibles son aptas para su uso común. En primer lugar, existen una serie de direcciones reservadas para su uso en redes privadas (aquellas cuyos host no van a ser visibles desde Internet), que sirven para implementar la pila de protocolos TCP/IP a las mismas. Existe un rango de direcciones reservadas según la clase de red:

Clase	Rango de direcciones reservadas
A	10.x.x.x
B	172.16.x.x - 172.31.x.x
C	192.168.0.x - 192.168.255

Tabla 3.4.1.2. Direcciones reservadas.

A la hora de configurar una red privada el administrador de red es el encargado de fijar qué clase de red va a usar, según el número de direcciones IP que necesite, y asignar luego una IP adecuada a cada uno de los host, de forma que el esquema final de la red sea lógico y funcional.

Estas IPs privadas no se pueden asignar a ningún host que tenga acceso directo a Internet, son para uso exclusivo interno. De esta forma nos aseguramos de que no si conectamos luego alguno de los host de la red privada a Internet no nos encontraremos con IPs repetidas, que haría que los host que las tuvieran fueses inaccesibles (las direcciones IP son únicas para cada host conectado a Internet) [4].

De la misma forma, si usamos direcciones IP privadas para configurar una serie de redes o subredes internas, nunca se puede asignar una misma IP a dos host diferentes.

De esta forma, si queremos mandar un mensaje broadcast a la red de clase B 140.26.5.95 tendríamos que hacerlo mediante la IP 140.26.255.255, con lo que el mensaje llegaría a todos los host de esa red.

La dirección de loopback (generalmente la 127.0.0.1) corresponde a nuestro propio host, y se utiliza para acceder a los servicios TCP/IP del mismo. Por lo tanto, si tenemos un servidor web local y queremos acceder a las páginas del mismo vía HTTP, tendremos que introducir en la barra de direcciones del navegador la dirección 127.0.0.1, si el puerto en el que está escuchando el servidor es el 80 (el que se usa por defecto). Si hubiésemos configurado el servidor web para que escuchara en el puerto 9025, por ejemplo, la dirección de acceso sería la 127.0.0.1:9025, Otra forma de acceder al loopback de nuestra máquina es usando el nombre reservado local host, que produce el mismo resultado.

3.4.2. Máscara de red

Cuando dos o más redes diferentes se encuentran conectadas entre si por medio de un enrutador, éste debe disponer de algún medio para diferenciar los paquetes que van dirigidos a los host de cada una de las redes. Es aquí donde entra en juego el concepto de máscara de red, que es una especie de dirección IP especial que permite efectuar este enrutamiento interno de paquetes [5].

Dada una dirección IP de red cualquiera, la máscara de red asociada es aquella que en binario tiene todos los bits que definen la red puestos a 1 (255 en decimal), y los bits correspondientes a los host puestos a 0 (0 en decimal), siempre que trabajemos con redes completas, no con subredes, mientras que cuando nos referimos a la *longitud del prefijo de red extendido* nos referimos a la máscara de subred, aunque indican lo mismo. La longitud del prefijo es igual al número de bits a 1 contiguos en la máscara de subred. De este modo, la dirección 135.146.91.26 con una máscara de subred 255.255.255.0 podrá expresarse también de la forma 135.146.91.26/24, lo que resulta más compacto y fácil de entender. Así, las máscaras de red de los diferentes tipos de redes principales son:

Red de Clase	Mascara de red o subred (decimal)	Mascara de red o subred (Binario)	Longitud del prefijo de red extendido
A	255.0.0.0	11111111. 00000000. 00000000. 000000	8
B	255.255.0.0	11111111. 11111111. 00000000. 000000	16
C	255.255.255.0	11111111. 11111111. 11111111. 000000	24

Tabla 3.4.2.1. Longitud de prefijo extendido

La máscara de red posee la importante propiedad de que cuando se combina con la dirección IP de un host se obtiene la dirección propia de la red en la que se encuentra el mismo. Cuando al enrutador que conecta varias redes le llega un paquete saca de él la dirección IP del host destino y realiza una operación AND lógica entre ésta IP y las diferentes máscaras de red de las redes que une, comprobando si el resultado coincide con alguna de las direcciones propias de red. Este proceso de identificación de la red destino de un paquete y del host al que va dirigido el paquete se denomina enrutamiento, el cual veremos con mas detalle mas adelante.

Para conocer a la red que pertenece una IP se le aplica la técnica del "AND" con la álgebra booleana :

1 and 1 = 1
1 and 0 = 0
0 and 1 = 0
0 and 0 = 0

Vamos a hacer una ejemplo : Tenemos la ip "206.175.162.21" sabemos que es una clase C y en binario seria :

11001110.10101111.10100010.00010101

Decimal : 206 . 175 . 162 . 21
Binario : 11001110.10101111.10100010.00010101

También sabemos que la mascara por defecto de una clase C es 255.255.255.0 que en binario seria : 11111111.11111111.11111111.00000000

Si le aplicamos el "AND" resultaría en :

```
   11001110.10101111.10100010.00010101
AND 11111111.11111111.11111111.00000000
    ----------------------------------------
    11001110.10101111.10100010.00000000
```

Recordemos que solamente dará "1" cuando los dos bits sean "1".

El resultado es : 11001110.10101111.10100010.00000000 que en decimal seria 206.175.162.0 la red a la que pertenece.

3.5. Subredes

Cuando se trabaja con una red pequeña, con pocos host conectados, el administrador de red puede fácilmente configurar el rango de direcciones IP usado para conseguir un funcionamiento óptimo del sistema. Pero conforme la red va creciendo se hace necesaria una división en partes de la misma [6].

En primer lugar, porque conforme se va extendiendo la red va aumentando de forma pareja el dominio de colisión, llegando un momento en el que el rendimiento de la red se ve afectado seriamente. Esto se puede mitigar segmentando la red, dividiendo la misma en una serie de segmentos significativos, de tal forma que mediante conmutadores podremos limitar estos dominios de colisión, enviando las tramas tan sólo al segmento en el que se encuentra el host destino.

En segundo lugar, y aunque segmentemos la red, conforme aumenta el número de host aumenta también el número de transmisiones de broadcast (cuando un equipo origen envía datos a todos los dispositivos de la red), llegando un momento en que dicho tráfico puede congestionar toda la red de forma inaceptable, al consumir un ancho de banda excesivo. Esto es así porque todos los host están enviando de forma constante peticiones de este tipo: peticiones ARP, envíos RIP, peticiones DNS, etc.

Para solventar este hecho es preciso dividir la red primaria en una serie de subredes de tal forma que cada una de ellas va a funcionar luego, a nivel de envío y recepción de paquetes, como una red individual, aunque todas pertenezcan a la misma red principal (y por lo tanto, al mismo dominio). De esta forma, aunque la red en su conjunto tendrá una dirección IP única, administrativamente, a nivel administrativo podremos considerar subredes bien diferenciadas, consiguiendo con ello un control del tráfico de la red así como también facilitar el diagnostico de problemas en la red y una limitación de las peticiones de broadcast que la atraviesan.

Para crear subredes a partir de una dirección IP de red padre, la idea es "robar" bits a los host, pasándolos a los de identificación de red. ¿Cuántos?. Dependiendo de las subredes que se quiera obtener, teniendo en cuenta que cuántos más bits sean "robados" más subredes se obtendrán, pero con menos host cada una. Por lo tanto, el número de bits a robar depende de las necesidades de funcionamiento de la red final. Pero para hacer esto posible fue necesario añadir otro nivel de jerarquía, creándose una jerarquía a tres niveles en la estructura del direccionamiento IP. Como se muestra en la figura siguiente. La idea consistió en dividir la parte dedicada al número de host en dos partes: el número de subred y el número de host en esa subred [7]:

Prefijo de Red	Número de Host
135.146	91.26

Tabla 3.5.1. Jerarquía a dos Niveles

Prefijo de Red	Número de Subred	Número de Host
135.146	91	26

***Tabla 3.5.2.** Jerarquía a tres Niveles*

Este sistema aborda el problema del crecimiento de las tablas de enrutamiento, asegurando que la división de una red en subredes nunca es visible fuera de la red privada de una organización. Los enrutadores dentro de la organización privada necesitan diferenciar entre las subredes individuales, pero en lo que se refiere a los enrutadores de Internet, todas las subredes de una organización están agrupadas en una sola entrada de la tabla de rutas. Esto permite al administrador local introducir la complejidad que desee en la red privada, sin afectar al tamaño de las tablas de rutas de Internet [8].

Por otra parte, sólo hará falta asignar a la organización un único número de red (de las clases A,B o C). La propia organización se encargará entonces de asignar distintos números de subred para cada una de sus redes internas. Esto evita en la medida de lo posible el agotamiento de los números IP disponibles.

Otro elemento que deberemos calcular para cada una de las subredes es su máscara de subred o mejor conocido como prefijo de red extendido ya que va a ser la herramienta que utilicen luego los enrutadores para dirigir correctamente los paquetes que circulen entre las diferentes subredes. Los enrutadores de Internet usan solamente el prefijo de red de la dirección de destino para enrutar el tráfico hacia un entorno con subredes. Los enrutadores dentro del entorno con subredes usan el prefijo de red extendido para enrutar el tráfico entre las subredes. Por lo que ahora en el caso de tener subredes, el prefijo de red extendido estará compuesto por el prefijo de red y el número de subred:

Prefijo de Red Extendido		
Prefijo de Red	Número de Subred	Número de Host

Tabla 3.5.3. Prefijo de Red Extendido para subredes.

El prefijo de red extendido se identifica a través de la *máscara de subred*. Por ejemplo, si consideramos la red clase B 135.146.0.0 y queremos usar el tercer octeto completo para representar el número de subred, deberemos especificar la máscara de subred 255.255.255.0

Entre los bits en la máscara de subred y la dirección de Internet existe una correspondencia uno a uno. Los bits de la máscara de subred están a 1 si el sistema que examina la dirección debe tratar los bits correspondientes en la dirección IP como parte del prefijo de red extendido. Los bits de la máscara están a 0 si el sistema debe considerar los bits como parte del número de host. Esto se ilustra en la siguiente figura:

		prefijo de red		nº subred	nº host
Dirección IP	135.146.91.26	10000111	10010010	01011011	00011010
Máscara de Subred	255.255.255.0	11111111	11111111	11111111	00000000
		prefijo de red extendido			

Tabla 3.5.4. Ejemplo del prefijo extendido en suredes

Creación de subredes

Vamos a tomar como ejemplo una red de clase C, teniendo claro que lo explicado a continuación va a ser útil para cualquier tipo de red, séa de clase A, B o C. Entonces, la red será , con dirección IP **210.25.2.0**, por lo que tenemos para asignar a los host de la misma todas las direcciones IP del rango 210.25.2.1 al 210.25.2.254, ya que la dirección 210.25.2.0 será la de la propia red y la 210.25.2.255 será la dirección de broadcast general.

Si expresamos nuestra dirección de red en binario tendremos:

210.25.2.0 = 11010010.00011001.00000010.00000000

Con lo que tenemos 24 bits para identificar la red y 8 bits para identificar los host.

La máscara de red será:

11111111.11111111.11111111.00000000 = 255.255.255.0

Vamos a partir pués de nuestra dirección IP de la red padre y vamos a ir quitando bist sucesivos a la porción de host, calculando en cada caso las subredes obtenidas, sus direcciones IP, sus máscaras de subred y el rendimiento de la partición obtenida.

Para ello, pasamos la dirección IP a binario y cogemos los bits robados a la porción de host.

Veamos para el caso de el "robo" de un bit y dos bits cuantas subredes se crean.

Caso (1) Robo de 1 bit:

Primer paso . Definir la mascara de subred

Para este paso es necesario primero pasar la dirección IP a binario y "robar" los bits de la porción de host y así después calcular la mascara de subred

	prefijo de red			bits nº subr	bits nº host
210.25.2.0/24	11010010	00001100	10000001	000	00000
	prefijo de red extendido				
255.255.255.128	11111111	11111111	11111111	100	00000
	25 bits				

Tabla 3.5.5. Definiendo la mascara de subred

Segundo paso . Definir los números de subred.

Permutando los bits de host robados para obtener las subredes obtenidas: $2^1=2$

Es decir, 2 subredes (11010010.00011001.00000010.0 y 11010010.00011001.00000010.1). Pero resulta que no podemos disponer de la subred que toma el 0, ya que entonces contendría la IP de la red padre, ni de la que toma el 1, ya que contendría la dirección de broadcast de la red padre. Es decir, robando 1 sólo bit no podemos crear subredes.

Como regla general, el número de subredes obtenidas al quitar n bits a la porción de host será 2^2-2, y el número de host disponible en cada subred será $2^{(8-n)}$-2, ya que toda subred debe tener su propia dirección de red y su propia dirección de broadcast.

Caso (2) Robo de 2 bits.

Primer paso . Definir la mascara de subred

	prefijo de red			bits nº subr	bits nº host
210.25.2.0/24	11010010	00001	0000	000	00000
	prefijo de red extendido				
255.255.255.192	11111111	11111	1111	110	00000
	26 bits				

Tabla 3.5.6. Definiendo la mascara de subred para el caso (2)

Segundo paso .-Definir los números de subred

Si en este caso quitamos dos bits a la porción del host, entonces n= 2, por lo que sustituyendo este valor en la formula mencionada anteriormente tenderemos:

No. de subredes = $2^n - 2$

$2^2 - 2 = 2$ subredes validas

Las subredes se numerarán de 0 a 2. Lo único que tenemos que hacer es colocar la representación binaria de dichos números en el campo *bits nº subred* de la primera fila de la figura anterior, y luego traducir las direcciones binarias a decimal. Quedaría lo siguiente:

Red Base: 11010010.00011001.00000010.00000000 = 210.25.2.0/26
Subred 0: 11010010.00011001.00000010.01000000 = 210.25.2.64/26
Subred 1: : 11010010.00011001.00000010.10000000 = 210.25.2.198/26
Subred 2: : 11010010.00011001.00000010.11000000 = 210.25.2.192/26

Tercer paso .-Definir los números de host.

En nuestro ejemplo, disponemos de 6 bits en el campo *bits nº host* de cada dirección de subred, por lo que tendríamos :

Número de host válidos por subred: 2^6-2=62. Obsérvese que se resta 2 pues las direcciones de host todos 0 (esta subred) o todos 1 (broadcast) no pueden usarse. Los host de cada subred se numeran del 0 al 62. Para definir la dirección asignada al host n de una subred dada, colocaremos la representación binaria de n en el campo *bits nº host* y luego traduciremos la dirección completa a notación decimal. Por ejemplo, para la subred 0 quedaría:

Subred 0: 11010010.00011001.00000010.01000000 = 210.25.2.64/24
Host 1: 11010010.00011001.00000010.01000001 = 210.25.2.65/26

Host 2: 11010010.00011001.00000010.01000010 = 210.25.2.66/26

Host 3: 11010010.00011001.00000010.01000011 = 210.25.2.67/26

.

.

.

Host 62: 11010010.00011001.00000010.01111111= 210.25.2.127/26

Subred válida, con dirección de red=210.25.2.64, broadcast=210.25.2.127 y 62 direcciones IP para host, que son las comprendidas entre las dos anteriores (de la 210.25.2.65 a la 210.25.2.126).

Como se puede ver la máscara de subred es la misma para todas las subredes obtenidas robando 2 bits a la porción de host, y lo mismo ocurre para el robo de otro número de bits.

3.6. Enrutamiento IP

La principal responsabilidad del protocolo IP es determinar qué camino deben tomar los paquetes para llegar al punto de destino. La tarea de determinar ese camino es lo que se conoce como *enrutamiento* [9]

IP asume que la computadora está directamente conectada a una *red local* (por ejemplo, una LAN Ethernet) y que puede enviar paquetes directamente a cualquier otra computadora sobre esa misma red. Si la dirección de destino es en la red local, IP simplemente accede al medio físico de transmisión y envía el paquete

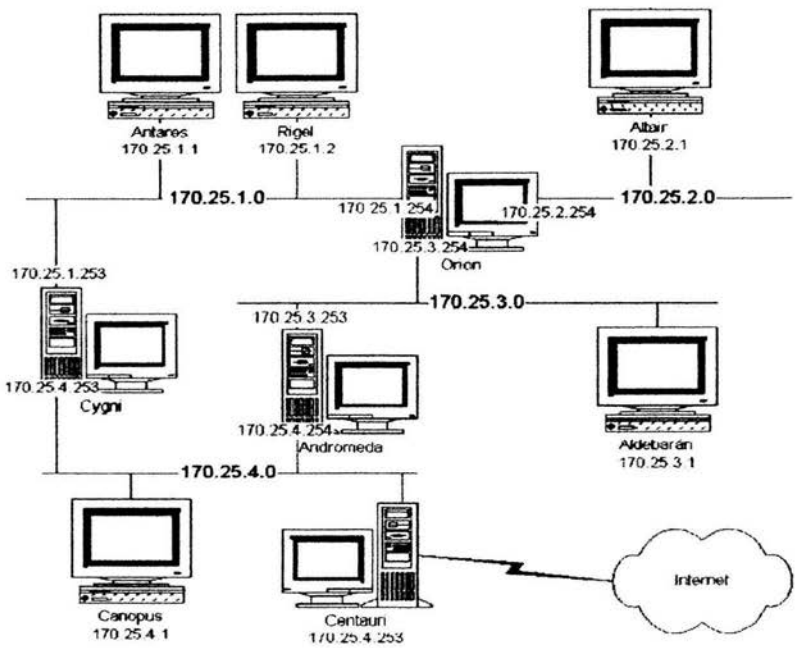


Figura. 3.6.1 Antares y Rigel están sobre la misma red, por lo que pueden comunicarse directamente

El problema aparece cuando la dirección de destino queda en otra red, en cuyo caso IP recurrirá a un enrutador (antes llamados *gateways)* para enviar indirectamente los paquetes. Como se recordará, se denomina enrutador a un dispositivo (ya sea otra computadora o un dispositivo especificamente diseñado a tal efecto) que está conectado a más de una red y tiene la capacidad para redirigir paquetes entre esas redes. Es necesario el uso de mascaras de subred para saber si el host destino de un datagrama esta o no dentro de la misma red física. En la figura anterior, *Orión*, *Andrómeda*, *Cygni* y *Centauri* son los gateways de la red.

Para determinar a qué enrutador deberán enviarse los paquetes, IP extrae la dirección de red del nodo de destino y consulta una tabla, denominada *tabla de enrutamiento*, la cual no puede tener información sobre cada posible destino, de hecho, esto no es deseable. En ves de ello se aprovecha del esquema de direccionamiento IP para ocultar detalles acerca de los host individuales, además, la tabla no contiene las rutas completas, sino solo la dirección del siguiente paso en esa ruta. En general una tabla de enrutamiento IP tiene pares (destino, enrutador), donde destino es la dirección IP de un destino particular y enrutador o gatway la dirección del siguiente enrutador en el camino hacia destino. Nótese

que enrutador debe ser accesible directamente desde la máquina actual. Por ejemplo, la tabla de enrutamiento de *Aldebarán* contiene la siguiente información:

Red	Gateway
170.25.1.0	170.25.3.254
170.25.2.0	170.25.3.254
170.25.3.0	*
170.25.4.0	170.25.3.253

Tabla 3.6.1. Tabla de enrutamiento de Aldebaran

en donde el asterisco indica que no es necesario ningún gateway para llegar a la red en cuestión dado que la máquina tiene conexión directa a la misma. Obsérvese en primer lugar que el enrutamiento hacia redes remotas se realiza en base a direcciones de red (esto es, la parte de host de la dirección IP se ignora); además, la tabla de enrutamiento especifica tanto la red local como las remotas, y que para el caso de éstas últimas, indica la dirección IP de alguna máquina en la red local que puede ser utilizada para alcanzarla.

Supongamos, por ejemplo, que *Altair* requiere enviar datos a *Canopus*. El módulo IP de *Altair* determina que la computadora de destino no pertenece a su misma red; consultando su tabla de enrutamiento, determina que puede llegarse a la red de *Canopus* a través de *Orión*, por lo que le envía los paquetes a dicha computadora. El módulo IP residente en *Orión*, por su parte, sabe que para llegar a *Canopus* hay dos vías posibles: pasando por *Andrómeda* o por *Cygni*. Aplicando algún criterio para evaluar ambas rutas y seleccionar la mejor de ellas, *Orión* envía cada paquete a, por ejemplo, *Andrómeda*. Esta última determina que la dirección de destino está en una de las redes a las que se encuentra directamente conectada, por lo que los envía diretamente a *Canopus*.

Es importante observar que la ruta que seguirán los paquetes desde el origen hasta su destino se va decidiendo a medida que los mismos viajan por la red. Cada nodo es responsable de determinar cual es el próximo "*salto*" en dirección al nodo final, en función del contenido de su tabla de enrutamiento. Este modelo de enrutamiento asume que si el nodo de destino no pertenece a la red local, deberá haber una entrada en la tabla de enrutamiento que especifique el gateway a utilizar. En otras palabras, asume que todos los nodos están al tanto de la estructura de la red.

En consecuencia, cada vez que la estructura de la red cambia (por ejemplo, cuando se agrega o elimina una subred), el administrador debería actualizar las tablas de enrutamiento en todos los nodos. Igualmente, si la red se interconectara a otra red, una nueva entrada debería agregarse en las tablas de enrutamiento de cada máquina.

Siguiendo con este razonamiento, a medida que la red crece y se interconecta a otras redes las tablas de enrutamiento se hacen mas largas y complejas; inclusive sería posible que fueran virtualmente imposibles de construir o mantener, en especial si la red se conecta a Internet (formada por miles de redes independientes).

Por supuesto, existen previsiones para enfrentar estos problemas y esto es mediante diferentes tipos de algoritmos de enrutamiento

La función principal del Nivel de Red es el diseño de algoritmos para seleccionar rutas junto con sus estructuras de datos. Un algoritmo de enrutamiento es aquel componente software del Nivel de Red responsable de decidir sobre qué línea de salida se deberá transmitir un paquete que llega.

Utilizando algoritmos de enrutamiento se intercambian mensajes de control, a partir de los cuales cada enrutador puede generar la tabla de enrutamiento.

Después, cuando llegue un paquete a enrutar, cada enrutador toma decisiones locales mirando en su tabla, pero que dependen de la topología global.

Objetivos de un algoritmo de enrutamiento:

- Minimizar el espacio de la tabla de enrutamiento para poder buscar rápidamente y para tener menos información a intercambiar con otros enrutadores.
- Minimizar el número y frecuencia de mensajes de control.
- Robustez: evitar agujeros negros, evitar bucles, evitar oscilaciones en las rutas
- Generar caminos óptimos: menor retardo de tránsito.
- Camino más corto (en función de una cierta métrica en función de retardo, costo de los enlaces, máxima utilización de la capacidad de la red .

A continuación clasificaremos los diferentes tipos de algoritmos de enrutamiento:

3.6.1. Algoritmos de enrutamiento

Enrutamiento estático.

Las tablas de enrutamiento no varían con el tiempo. Para redes en las que el tráfico y la topología no varía.

Al implementar las rutas estáticas se crea una matriz de enrutamiento central, almacenada, por ejemplo, en un centro de control de red. Esta matriz especifica, para cada par de nodos origen-destino, la identidad del siguiente nodo en la ruta.

Las tablas de enrutamiento se establecen y almacenan en cada nodo, almacenando cada uno de ellos solamente una columna del directorio de enrutamiento. El directorio de cada nodo especifica el siguiente nodo para cada destino. Con el enrutamiento estático no existen diferencias entre el enrutamiento de datagramas y de circuitos virtuales. Existen dos tipos:

- Centralizados: Las tablas se calculan en un sólo nodo de la red.
- Distribuidos: Las tablas se calculan por cooperación entre todos lo nodos.

Desventajas:

- El costo de procesamiento en cada nodo aumenta.
- Al intercambiar información de nodo en nodo, aumenta el tráfico.
- Es una técnica muy inestable.
- Falta de flexibilidad, no reacciona ante fallos ni congestión en la red

Ventajas:

- El usuario cree que aumentan las prestaciones.
- Se puede ayudar en el control de la congestión.

Interesa saber cual es el mejor camino entre emisor y receptor. Para decidir cuál es se utilizan técnicas basadas en gráficos:

- Vector de distancia.- Un equipo sólo tiene en cuenta la información que le pasan los equipos vecinos, que le dicen a qué distancia está el destino. No tiene en cuenta la topología.
- Jerárquico (estado del enlace).- Construye una topología y envía el paquete por inundación.

Consiste en los siguientes pasos:

- Descubrir a sus vecinos y aprender sus direcciones de red.
- Medir el retardo o coste a cada vecino.
- Construir paquetes para comunicar a todos lo que ha aprendido.
- Distribuir los paquetes a otros *enrutadors*.
- Calcular el camino más corto a los demás *enrutadors*.

Enrutamiento Dinámicos o Adaptativos.

Las tablas de enrutamiento se ajustan a cambios en las condiciones de la red (tráfico o topología). Para que el enrutamiento dinámico sea posible es necesario que los nodos intercambien información acerca del estado de la red. Cuanta más información se intercambie y mayor sea la frecuencia del intercambio, mejor será la decisión de enrutamiento que cada nodo realiza. Por lo que cada host ejecuta un programa que actualice automática y periódicamente la tabla de enrutamiento. Dichos programas se basan en el hecho de que una computadora siempre tiene acceso a otras computadoras conectadas a la red local; esto se traduce en que las tablas de enrutamiento contienen inicialmente al menos las direcciones de las redes locales. Si tomamos por caso a *Orión*, su tabla de enrutamiento inicialmente contendría la siguiente información:

Red	Gateway
170.25.1.0	*
170.25.2.0	*
170.25.3.0	*

Tabla 6.1.1.1 Tabla de enrutamiento de Orion

De manera similar, la tabla de *Andrómeda* contendrá lo siguiente:

Red	Gateway
170.25.3.0	*

170.25.4.0	*

Tabla 6.1.1.2 Tabla de enrutamiento de Andrómeda sin intercambiar información

Si *Orión* y *Andrómeda* intercambiaran sus tablas de enrutamiento, cada una podría "*aprender*" de la otra qué redes son alcanzables por esa vía. Así, *Andrómeda* podría concluir lo siguiente:

Red	Gateway
170.25.1.0	170.25.3.254
170.25.2.0	170.25.3.254
170.25.3.0	*
170.25.4.0	*

Tabla 6.1.1.3 Tabla de enrutamiento de Andrómeda al intercambiar información con Orion

Así, si todos los nodos de la red ejecutan un programa de estas características (llamado *demonio de enrutamiento*) al cabo de cierto tiempo habrán "*descubierto*" por sí mismas la estructura de la red y construido sus tablas automáticamente. Mas aún, si se produjera algún cambio en la estructura de la red, bastaría con que alguna de las computadoras lo detectara para que en pocos segundos esa nueva información se propagará por toda la red.

Esta estrategia se denomina *enrutamiento dinámico* o *adaptativo* y tiene la ventaja de que, al ser automático, permite eliminar las tareas administrativas relacionadas con el mantenimiento de las tablas de enrutamiento, así como también la necesidad de modificar las tablas de enrutamiento cuando la red cambia. Sin embargo, no resuelve el problema de las abultadas tablas de enrutamiento resultantes de conectar una red a muchas otras.

Consideremos la tabla de enrutamiento que construiría una máquina como *Altair*:

Red	Gateway
170.25.1.0	170.25.2.254
170.25.2.0	*
170.25.3.0	170.25.2.254
170.25.4.0	170.25.2.254

Tabla 6.1.1.4. Tabla de enrutamiento de Altair

Como puede verse, *Altair* ha aprendido las rutas a todas las subredes de la red, pero el único gateway que puede utilizar es *Orión*. De manera similar, si fuera posible que todas las computadoras de la red del ejemplo aprendieran las direcciones de todas las redes que forman la Internet, *Altair* eventualmente construiría una tabla de enrutamiento con miles de entradas, en donde todas tendrían a *Orión* como gateway. En ambos casos, el resultado es una tabla de enrutamiento con información altamente redundante.

Para eliminar este problema, es que puede instalarse en la tabla de enrutamiento una *ruta por defecto* (conocida también como *default gateway*). IP utiliza la ruta por defecto (que se indica con el número 0.0.0.0) cada vez que no se encuentra en la tabla de enrutamiento una ruta hacia una red específica. Aplicando éste criterio, la tabla de *Altair* se reduciría a lo siguiente:

Red	Gateway
170.25.2.0	*
0.0.0.0	170.25.2.254

Tabla 6.1.1.5. Tabla de enrutamiento de Altair, utilizando la ruta por defecto

que sencillamente indica que si la dirección de destino está en la red local, es accesible directamente, y que en caso contrario (independientemente de cual sea el destino), los paquetes deberán enviarse a 170.25.2.254 (es decir, *Orión*).

Tipos de algoritmos dinámicos:

- Aislados: Cada nodo toma decisiones independientemente del resto.
- Centralizados: Un nodo acumula toda la información de la red.
- Distribuidos: Los nodos cooperan para adaptarse a las condiciones de la red.
- Mixtos: Un nodo central mantiene información del estado de la red, y aconseja a los otros nodos, que pueden tomar decisiones por su cuenta.

Desventajas:

- Decisión de enrutamiento más compleja, por lo que el coste de procesamiento en los nodos aumenta.
- En la mayor parte de los casos, las estrategias dinámicas dependen de la información de estado obtenida en una parte de la red.Una estrategia adaptable puede reaccionar muy

rápidamente, produciendo oscilaciones y causando congestión, o muy lentamente, en cuyo caso no es válida.

Ventajas:

- El usuario de la red percibe que las prestaciones aumentan con el uso de estas técnicas.

Puede ayudar en el control de congestión.

Inundaciones.

Consiste en que cada nodo envía una copia del paquete a todos sus vecinos y éstos lo reenvía a todos sus vecinos excepto al nodo del cuál lo habían recibido. De esta forma se asegura que el paquete llegará a su destino en el mínimo tiempo posible. Para evitar que a un nodo llegue un paquete repetido, el nodo debe guardar una información que le haga descartar un paquete ya recibido. Esta técnica, al ser muy robusta y de coste mínimo, se puede usar para mensajes de alta prioridad o muy importante. El problema es la gran cantidad de tráfico que se genera en la red. Esta técnica libera de los grandes cálculos para seleccionar un enrutamiento

Enrutamiento aleatorio.

Consiste en que en cada nodo elegirá aleatoriamente el nodo al cuál se va a reenviar el paquete. De esta forma, se puede asegurar que el paquete llegará al destino pero en un mayor tiempo que en el de inundaciones. Pero el tránsito en la red es mucho menor. Esta técnica también libera de cálculos para seleccionar el enrutamiento [10].

3.6. Protocolo IP v6

El protocolo IP en su versión 6 (IPv6, a partir de ahora), surge como un sucesor de la versión 4, que pronto se quedará corta de espacio de direcciones de host, debido al crecimiento exponencial de Internet. Al ver en el horizonte estos problemas, el IETF comenzó a trabajar en 1990 en una versión nueva de IP, que sería más eficiente y con un rango de direcciones virtualmente inagotable, siendo además más flexible, eficiente y segura [11].

En 1991 se convocó un concurso de ideas para tratar de encontrar ese algoritmo, y en diciembre de 1992 había varias propuestas serias. Al final se tomó en consideración una forma que proporciona un rango de direcciones de 16 bytes, una cabecera más simple, que mejora la eficiencia en su transmisión y verificaciones de autenticidad y confidencialidad. Además, se requiere una mayor atención al tipo de servicio, para poder atender adecuadamente al tráfico multimedia que se avecina. Los cambios de IPv6 respecto de IPv4 son, de forma resumida:

- Expansión de las capacidades de direccionamiento. IPv6 incrementa el tamaño de las direcciones de 32 bits (IPv4) a 128 bits, para soportar más niveles en la jerarquía de direccionamiento, un número mayor de nodos direccionables, y un sistema de autoconfiguración de direcciones.

- Simplificación de la cabecera. Algunos campos de la cabecera del IPv4 son eliminados o pasan a ser opcionales, tanto para reducir el coste de procesamiento como el tamaño de la cabecera.

- Mayor flexibilidad para extensiones y nuevas opciones. En IPv6 no existe un campo opciones, como tal. La gestión de opciones se realiza por un campo siguiente cabecera (next header). Eliminando así las limitaciones de tamaño en la cabecera, e introduciendo una gran flexibilidad en el desarrollo de nuevas opciones.

- Capacidades de control de flujo. Se añaden capacidades que permiten marcar los paquetes que pertenezcan a un determinado tipo de tráfico, para el cual el remitente demanda una calidad mayor a la especificada por defecto o servicios en tiempo real.

Con un octeto se pueden representar los números de 0 a 255. Por tanto las direcciones IPv4 se componen de cuatro octetos, o 32 bits, lo cual genera los cuatro millones y pico de direcciones antes mencionadas. En IPv6 las direcciones se componen de 16 octetos, es decir 128 bits. Esto daría lugar a 2_{128} direcciones, más o menos 340 sextillones. No obstante, esta cifra no se alcanza, ya que parte de los dígitos identifican el tipo de dirección, con lo que se quedan en 3800 millones. En cualquier caso se garantiza que no se acabarán en un plazo razonable [12].

Hay tres tipos de direcciones: *unicast*, *anycast* y *multicast*. Las direcciones *unicast* identifican un solo destino. Un paquete que se envía a una dirección *unicast* llega sólo al ordenador al que corresponda. En el caso de las direcciones *anycast* se trata de un conjunto de ordenadores o dispositivos, que pueden pertenecer a nodos diferentes. Si se envía un paquete a una de estas direcciones lo recibirá el ordenador más cercano de entre las rutas posibles. Las direcciones

multicast definen un conjunto de direcciones pertenecientes también a nodos diferentes, pero ahora los paquetes llegan a todas las máquinas identificadas por esa dirección.

Ejemplo de conversión formato IPv4 – IPv6 :

Esta es una dirección de 32 bits: 192.9.32.12
Esta es una dirección de 128 bits: BAF7:7432:FFFF:FFFF:7433:73F9:FFAA

3.8. Enrutamiento IP vs conmutación de etiquetas

A continuación presentaremos las desventajas del enrutamiento IP ante la conmutación de etiquetas.

Plataforma de enrutamiento basada en software.

Es decir el enrutamiento IP se basa en el análisis de la cabecera del paquete y del resultado de ejecutar un algoritmo de enrutamiento, del que ya mencionamos las desventajas que trae, mientras que MPLS es todo por hardware.

Presenta retardo

El reenvío (*forwarding*) tradicional basado en software es demasiado lento para manejar las grandes cantidades de tráfico de Internet o de las redes interconectadas. El tiempo de la búsqueda en las tablas de enrutamiento es demasiado elevado. Esto se traduce en pérdida de paquetes y conexiones, y por tanto en un bajo rendimiento.

La conmutación de etiquetas es más rápida. El motivo es simple, el valor de la etiqueta que se pone en la cabecera de los paquetes es el que se usa para acceder a la tabla de enrutamiento del enrutador , es el índice para acceder a la tabla directamente. Por tanto, el tiempo para transmitir un paquete es menor que con el enrutamiento tradicional IP, el cual revisa un tabla de enrutamiento para analizar la dirección IP destino .

No implementa corrección de errores ni control de congestión

Mientras que la conmutación de etiquetas, puede implementar ingeniería de tráfico puede re-enrutar el tráfico rápido y automáticamente cuando se detectan condiciones de falla o congestión.

Utiliza la técnica del mejor salto posible.

En la red IP y su infraestructura y protocolos han sido optimizados sólo para datos, así que IGPs (*Interior Gateway Protocol*) como RIP (*Routing Information Protocol*) y OSPF (*Open Shortest Path First*) y EGPs (*Exterior Gateway Protocol*) como BGP4 (*Border Gateway Protocol v4*), no son la solución óptima. Muchos de estos protocolos de enrutamiento están basados en algoritmos para obtener el camino más corto (como RIP y BGP4, basados en el vector distancia) mientras que MPLS utiliza el camino mas optimo, aunque este sea mas largo, ya MPLS implementa ingeniería de tráfico , lo cual permite seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). y encontrar el mejor camino para un tipo de tráfico.

IP esta imposibilitado a ofrecer diferentes niveles de servicios para las diferentes aplicaciones, mientras que MPLS es capaz de ofrecer este tipo de aplicación.

El enrutamiento IP , re-examina en cada nodo la cabecera IP del paquete para asignar a un FEC.

En MPLS, solo al ingresar un paquete a la red se le asigna un FEC. Luego ningún enrutador lo hace, lo cual hace mas fácil el proceso de llevar un paquete a su destino.

Hay que resaltar que la conmutación de etiquetas no pretende sustituir al enrutamiento IP.

REFERENCIAS

[1] La Capa de Internet (II), Luciano Moreno
www.htmlweb.net/redes/tcp_ip/capa_3/red_2.htm

[2] Li-T. MPLS and the evolving Internet architecture. IEEE Communications Magazine. Dicciembre 1999. Volumen 37. Número 12.

[3] Protocolo Internet (IP)
www.uam.es/departamentos/medicina/anesnet/redeshtml/protocip.htm

[4] Protocolo de Enrutamiento o Protocolo de Internet (IP)
www.solont.com/z-net/tcp-04/tcp_04.htm

[5] Mascara de red
www.zator.com/Internet/X_Ap_A.

[6] IP Subnetting Tutorial
www.ralphb.net/IPSubnet

[7] TCP/IP Addressing & Subnetting Notes
www.wilsonmar.com/1tcpaddr.htm

[8] IP Addresses, Subnet Masks, & Subnetting
www.compnetworking.about.com/library/weekly/aa043000a.htm

[9] Routing IP
www.cisco.com/univercd/cc/td/doc/product/software/ssr83/rpc_r/48383.htm

[10] Internet Protocols (IP)
www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm

[11] Microsoft Internet Protocol Version 6 (IPv6) -
www.microsoft.com/windowsserver2003/ technologies/ipv6/default.mspx

[12] Jesus García Tomás. Alta velocidad y calidad de servicio en redes IP Ra-Ma. 1997.

CAPÍTULO 4

4. MPLS EN LOS PROTOCOLOS DE ENLACE DE IP

MPLS proporciona la posibilidad de converger múltiples tecnologías de transporte como Ethernet, ATM o Frame Relay, en nuestra red medular. Implementa una eficiente conmutación de paquetes sin importar el protocolo de capa 2 que se este usando, permitiendo el aprovechamiento de las ventajas de protocolos no orientados a conexión como IP y de los orientados a conexión como ATM, FR, etc, facilitando así un mayor rendimiento al manejar conmutación en vez de enrutamiento en cada punto intermedio y dándole Calidad de Servicio (QoS), Ingeniería de Tráfico, entre otras ventajas. También le permite a protocolos orientados a conexión acceder a características que por el modelo del protocolo capa 2 son difíciles de implementar como el enrutamiento dinámico y paquetes de tamaño variable.

Por lo que se dice que MPLS es un estándar diseñado para el futuro que permite a las empresas simplificar sus redes al llevar sus servicios a una sola plataforma. Combina la fiabilidad de los protocolos orientados a conexión y sin conexión en una misma infraestructura, permitiendo así la Ingeniería de Tráfico. Las actualizaciones al protocolo y la adición de nuevas funciones pueden hacerse fácilmente sin afectar el modo en que opera este protocolo. A continuación se dará una breve descripción de algunas tecnologías de transporte de una red MPLS.

4.1. ATM.

4.1.1. Introducción

ATM (*Asynchronous Transfer Mode*) es una tecnología de conmutación que usa pequeñas celdas de tamaño fijo. En 1988, el CCITT designó a ATM como el mecanismo de transporte planeado para el uso de futuros servicios de banda ancha. De este modo la tecnología llamada ATM es el corazón de los servicios digitales integrados que ofrecen las nuevas redes digitales de servicios integrados de Banda Ancha (*B-ISDN*).

ATM es una tecnología orientada a conexión, lo que significa que una conexión necesita ser establecida entre dos puntos con un protocolo de señalización antes de cualquier transferencia de datos. Una vez

que la conexión está establecida, las celdas ATM se auto-rutean porque cada celda contiene campos que identifican la conexión de la celda a la cual pertenecen.

ATM es el complemento de STM (*Synchronous Transfer Mode*). El STM es usado en las redes de telecomunicaciones para transmitir paquetes de datos y voz a lo largo de grandes distancias. La red se basa en la tecnología de conmutadores donde una conexión se establece entre dos puntos antes de que empiece la transmisión de datos. De esta forma, los puntos finales localizan y reservan un ancho de banda para toda la conexión. [1]

Transmisiones de diferentes tipos, incluyendo video, voz y datos pueden ser mezcladas en una transmisión ATM que puede tener rangos de 155 Mbps a 2.5 Gbps. Esta velocidad puede ser dirigida a un usuario, grupo de trabajo o una red entera, porque ATM no reserva posiciones específicas en una celda para tipos específicos de información. Además de esto ATM pretende resolver dos problemas: mayor ancho de banda y rápida conmutación que permita tomar bits de un enlace y llevarlos rápidamente a otro enlace de la misma red.

ATM se basa en SONET, constituyendo una familia de implementaciones de hardware, software y protocolos interoperables y estándares, que pueden proporcionar mayor ancho de banda cuando se requiera. Al basarse en las tecnologías de multiplexado y conmutación se logran redes con unos retrasos insignificantes extremo a extremo. Esta combinación de ATM y SONET proporciona ventajas de gran ancho de banda y la velocidad de los nodos de la red, que depende solo de la capacidad de los propios sistemas; por lo tanto la filosofía de ATM es muy simple: una vez establecida la forma mas eficiente de enviar bits de un punto a otro de la red, no existe sistema o aplicación que requiera mayor ancho de banda o menos retrasos.[1]

Una ventaja de ATM es que es escalable. Varios conmutadores pueden ser conectados en cascada para formar redes más grandes. Como se mencionaba ATM es una red orientada a conexión, un enlace entre dos puntos empieza cuando uno transmite una solicitud a través de la UNI a la red. Un dispositivo responsable de señalización pasa la señal a través de la red a su destino. Si el sistema indica que se acepta la conexión, un circuito virtual es establecido a través de la red ATM entre los dos puntos. Ambas UNIs contienen mapas para que las celdas puedan ser ruteadas correctamente.

El uso de celdas para transmitir datos no significa que los protocolos de hoy no sean usados. ATM es totalmente transparente a protocolo. La carga de cada celda es pasada por el conmutador sin ser "leída" a nivel binario. ATM usa el concepto de control de error y flujo de fin -a -fin en contraste a la red convencional de paquete conmutado que usa un control de error y flujo interno. Esto es que la red en si no checa la carga de datos para errores y lo deja al dispositivo terminal final(De hecho, el único chequeo de error en las celdas es en el *header* , así la integridad de los VCI/VPI esta asegurada).

4.1.2. Funcionamiento

Como mencionamos antes, una conexión ATM consiste de "celdas" de información contenida en un VC (*Virtual Circuit*). Cada celda está compuesta por 53 bytes, de los cuales 48 (opcionalmente 44) son para trasiego de información y los restantes para uso de campos de control (encabezado) con información de "quién soy" y "donde voy"; es identificada por un VCI (*Virtual Circuit Identifier*) y un VPI (*Virtual Path Identifier*), dentro de esos campos de control, que incluyen tanto el enrutamiento de celdas como el tipo de conexión.

La organización del encabezado (*header*) variará levemente dependiendo de si la información relacionada es para interfaces de red a red o de usuario a red. Las celdas son enrutadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local, ya que pueden ser cambiados de interface a interface.[2]

Las conexiones ATM denominadas circuitos virtuales, pueden ser permanentes PVC (*Permanent Virtual Circuit*) que operan como una línea física dedicada creando una conexión permanente entre dos puntos de la red; o pueden ser conmutados SVC (*Switched Virtual Circuit*) equivalentes a los de la red telefónica, donde las conexiones entre dos puntos de la red se establecen dinámicamente par a cada transmisión.

Diferentes categorías de tráfico son convertidas en celdas ATM vía la capa de adaptación de ATM AAL (*ATM Adaptation Layer*), de acuerdo con el protocolo usado. (Más adelante se explica esta capa).

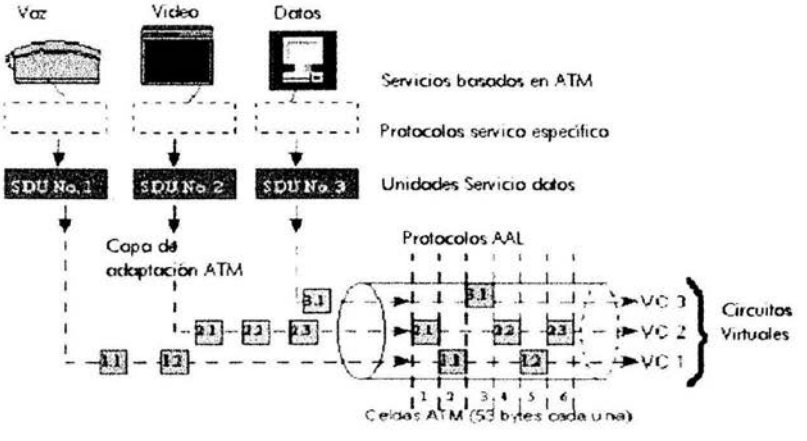


Figura 4.1.2.1. Formato básico y jerarquía de ATM

La tecnología ATM ha sido definida, como la tecnología de transporte para la B-ISDN (*Broad Band Integrated Services Digital Network*), la RDSI de banda ancha. En este contexto "transporte" se refiere al uso de técnicas de conmutación y multiplexación en la capa de enlace (Capa 2 del modelo OSI) para el trasiego del tráfico del usuario final de la fuente al destino, dentro de una red. [2]

El protocolo ATM consiste de tres niveles o capas básicas:

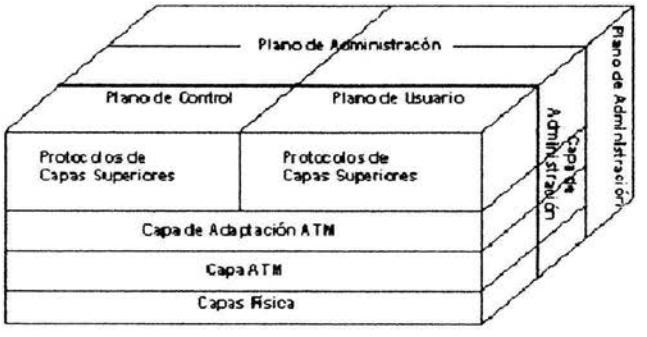


Figura 4.1.2.2 Formato de Protocolo para ATM

Capa física

La primera capa llamada capa física (*Physical Layer*), define los interfaces físicos con los medios de transmisión y el protocolo de trama para la red ATM es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado. A diferencia de muchas tecnologías LAN como Ethernet, que especifica ciertos medios de transmisión, (10 base T, 10 base 5, etc.) ATM es independiente del transporte físico. Las celdas ATM pueden ser transportadas en redes SONET (*Synchronous Optical Network*), SDH (*Synchronous Digital Hierarchy*), T3/E3, TI/EI o aún en modems de 9600 bps. Hay dos subcapas en la capa física que separan el medio físico de transmisión y la extracción de los datos. [2]

La subcapa PMD (*Physical Medium Depedent*) tiene que ver con los detalles que se especifican para velocidades de transmisión, tipos de conectores físicos, extracción de reloj, etc. La subcapa TC (*Transmission Convergence*) tiene que ver con la extracción de información contenida desde la misma capa física; esto incluye la generación y el chequeo del *Header*, Error Corrección (HEC), y el reconocimiento del límite de la celda. Otra función importante es intercambiar información de operación y mantenimiento con el plano de administración.

Capa ATM

La segunda capa es la capa ATM. Ello define la estructura de la celda y cómo las celdas fluyen sobre las conexiones lógicas en una red ATM, esta capa es independiente del servicio. En los extremos de la red, la capa ATM genera e interpreta las cabeceras de las celdas y solo el *payload* es pasado a las capas superiores. El formato de una celda ATM es muy simple. Consiste de 5 bytes de cabecera y 48 bytes para información.

Las celdas son transmitidas serialmente y se propagan en estricta secuencia numérica a través de la red. El tamaño de la celda ha sido escogido como un compromiso entre una larga celda, que es muy eficiente para transmitir largas tramas de datos y longitudes de celdas cortas que minimizan el retardo de procesamiento de extremo a extremo, que son buenas para voz, video y protocolos sensibles al retardo.

Los comités de estándares han definido dos tipos de cabeceras ATM: UNI (*User-to-Network Interface*) y la NNI *(Network to Network Interface*). La UNI es un modo nativo de interfaz ATM que define la interfaz entre el equipo del cliente CPE (*Customer Premises Equipment*), tal como *hubs* o *enrutadores* ATM y la red de área ancha ATM (*ATM WAN*). La NNI define la interface entre los nodos de la redes (los conmutadores o conmutadores) o entre redes. La NNI puede usarse como una interface entre una red ATM de un usuario privado y la red ATM de un proveedor público (*carrier*). Específicamente, la función principal de ambos tipos de cabeceras de UNI y la NNI, es identificar las VPIS (*Virtual Paths Identifiers*) y los VCIS (*Virtual circuits* o *Virtual channels*) como identificadores para el enrutamiento y la conmutación de las celdas ATM. [3]

Capa de adaptación de ATM

La tercera capa es la AAL (*ATM Adaptation Layer*). La AAL juega un rol clave en el manejo de múltiples tipos de tráfico para usar la red ATM, y es dependiente del servicio. Específicamente, su trabajo es adaptar los servicios dados por la capa ATM a aquellos servicios que son requeridos por las capas más altas, tales como emulación de circuitos, (*circuit emulation*), vídeo, audio, *Frame Relay*, etc. La AAL recibe los datos de varias fuentes o aplicaciones y las convierte en los segmentos de 48 bytes.

La clasificación de los servicios AAL son los siguientes: (Figura *4.1.2.3.*)

- Clase A . *Constant bit rate* (CBR), orientado a conexión, tráfico síncrono (Ej. voz o video sin compresión)
- Clase B. *Variable bit traffic* (VBR), orientado a conexión, tráfico síncrono (voz y video comprimidos).
- Clase C. *Variable bit rate*, orientado a conexión, tráfico asíncrono(X.25, *Frame Relay*, etc).
- Clase D. Información de paquete sin conexión(tráfico LAN, SMDS, etc).

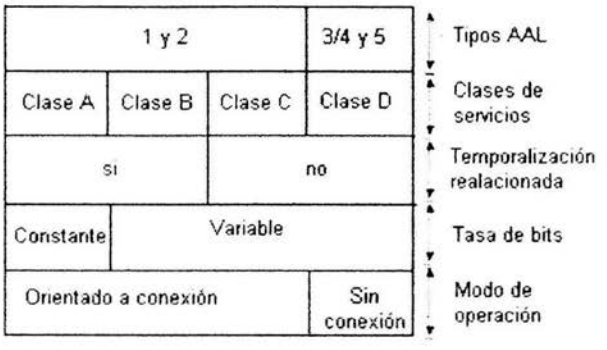


Figura 4.1.2.3. Tipos de tráfico y la capa usada para manejarlos

La capa de Adaptación de ATM yace entre la capa ATM y las capas más altas que usan el servicio ATM. Su propósito principal es resolver cualquier disparidad entre un servicio requerido por el usuario y atender los servicios disponibles de la capa ATM. La capa de adaptación introduce la información en paquetes ATM y controla los errores de la transmisión. La información transportada por la capa de adaptación se divide en cuatro clases según las propiedades siguientes:

1. Temporalización relacionada. Que la información que esta siendo transportada dependa o no del tiempo.
2. Tasa de bit constante/variable.
3. Modo de operación

La capa de adaptación se divide en dos subcapas:

1.- Capa de convergencia (*Convergence Sublayer* (CS))

En esta capa se calculan los valores que debe llevar el encabezado y los *payloads* del mensaje. La información en el encabezado y en el *payload* depende de la clase de información que va a ser transportada.

2.- Capa de Segmentación y reensamblaje (*Segmentation and Reassembly* (SAR)).

Esta capa recibe los datos de la capa de convergencia y los divide en trozos formando los paquetes de ATM. Agrega el encabezado que llevara la información necesaria para el reensamblaje en el destino.

Tipos de AAL

1) AAL-1

AAL-1 se usa para transferir tasas de bits constantes que dependen del tiempo. Debe enviar por lo tanto información que regule el tiempo con los datos. AAL-1 provee recuperación de errores e indica la información con errores que no podrá ser recuperada.

Las funciones provistas a esta capa difieren dependiendo del servicio que se proveyó. Provee la corrección de errores.

En esta capa los datos son segmentados y se les añade un encabezado. El encabezado contiene 3 campos:

1. Número de secuencia usado para detectar una inserción o perdida de un paquete.
2. Número de secuencia para la protección usado para corregir errores que ocurren en el número de secuencia.
3. Indicador de capa de convergencia usado para indicar la presencia de la función de la capa de convergencia.

2) ALL-2

AAL-2 se usa para transferir datos con tasa de bits variable que dependen del tiempo. Envía la información del tiempo conjuntamente con los datos para que esta puede recuperarse en el destino. AAL-2 provee recuperación de errores e indica la información que no puede recuperarse.

Esta capa provee para la corrección de errores y transporta la información del tiempo desde el origen al destino.

El mensaje es segmentado y se le añade un encabezado a cada paquete. El encabezado contiene dos campos.

1. Número de secuencia que se usa para detectar paquetes introducidas o perdidas.
2. El *payload* que contiene dos campos: indicador de longitud y el CRC que es para hacer el control de errores.

3) AAL-3

AAL-3 se diseña para transferir los datos con tasa de bits variable que son independientes del tiempo. AAL-3 puede ser dividido en dos modos de operación:

1. Fiable: En caso de perdida o mala recepción de datos estos vuelven a ser enviados. El control de flujo es soportado.
2. No fiable: La recuperación del error es dejado para capas mas altas y el control de flujo es opcional.

Añade un encabezado y un payload a la parte común.

El encabezado contiene 3 campos:

1. Indicador de la parte común que dice que el payload forma parte de la parte común.
2. Etiqueta de comienzo que indica el comienzo de la parte común de la capa de convergencia.
3. Tamaño del buffer que dice al receptor el espacio necesario para acomodar el mensaje.

El payload también contiene 3 campos:

1. Alineación es un byte de relleno usado para hacer que el encabezado y el *payload* tengan la misma longitud.
2. Fin de etiqueta que indica el fin de la parte común de la CS(capa de convergencia).
3. El campo de longitud tiene la longitud de la parte común de la CS.

Parte especifica del servicio. Las funciones proveídas en esta que capa dependen de los servicios pedidos. Generalmente se incluyen funciones para la recuperación y detección de errores y puede incluir también funciones especiales.

4) AAL-4

AAL-4 se diseña para transportar datos con tasa de bits variable independientes del tiempo. Es similar al AAL3 y también puede operar en transmisión fiable y o fiable. AAL-4 provee la capacidad de transferir datos fuera de una conexión explícita. También proporciona servicios para comunicación de datos, tanto orientados a conexiones como sin ellas, de tráfico asíncrono.

AAL 2, AAL 3/4 y AAL 5 manejan varios tipos de servicios de datos sobre la base de tasas de bits variables tales como SMDS (*Conmutadored Multimegabit Data Service*), Frame Relay o tráfico de redes de área local (LAN). AAL 2 y AAL 3 soportan paquetes orientados a conexión.

4.1.3. Ventajas

- *Ancho de banda bajo demanda*: el acceso está garantizado mediante un ancho de banda predefinido y dedicado segundo sea necesario; el ancho de banda puede incrementarse según la demanda. La asignación del ancho de banda se realiza en función de la demanda de envío de tráfico. La multiplexación estadística del sistema ATM (también conocida como asignación bajo demanda) permite aprovechar todos los recursos disponibles; es decir si un usuario/a no tiene nada que transmitir en un momento determinado su canal queda desaprovechado y pasa a ser utilizado por otro usuario/a que tiene que transmitir mucha información.

- *Operación por conmutación de paquetes*: al utilizar paquetes de longitud fija se permite el uso de nodos de conmutación a velocidades muy altas.

- *Velocidad*: Capacidades escalables de 34, 45, 100, 155, 622, 2488 Mbps

- *Despliegue Universal*: Adaptable para LAN (*Redes de área Local*) y WAN (*Redes de área extensa*)

- *Diseñado para todo tipo de tráfico*: voz, datos, imagen, video, gráficos y multimedia.

- *Compatibilidad*: ATM no está basado en un tipo específico de transporte físico. Es compatible con las actuales redes físicas. ATM puede ser implementado sobre par trenzado, cable coaxial y fibra óptica.

- *Escalabilidad*: Permite incrementar el ancho de banda y la densidad de los puertos dentro de las arquitecturas existentes. Esto simplifica el diseño y la administración de las redes, permitiendo a su vez la integración con las redes existentes.

- *Largo periodo de vida de la arquitectura*: los sistemas de información y las industrias de telecomunicaciones se están centrando y están estandarizando el ATM. ATM ha sido diseñado desde un principio para ser flexible en: distancias geográficas, número de usuarios/as, acceso y ancho de banda .Hasta ahora las velocidades de transmisión varía de Megas a Gigas.

4.1.5. Desventajas

En el pasado los protocolos de comunicaciones de datos evolucionaron en respuesta a circuitos poco confiables. Los protocolos en general detectan errores en bits y tramas perdidas, luego retransmiten los datos. Los usuarios puede que jamás vean estos errores reportados, la degradación de respuesta o de caudal serían los únicos síntomas.

Si el control del flujo se hiciese como una realimentación del lazo extremo a extremo, en el momento en que el mensaje de control de flujo llegase a la fuente, ésta habría transmitido ya algunos Mbytes de datos en el sistema, exacerbando la congestión. Y en el momento en que la fuente reaccionase al mensaje de control, la condición de congestión hubiese podido desaparecer apagando innecesariamente la fuente. La constante de tiempo de la realimentación extremo a extremo en las redes ATM (retardo de realimentación por producto lazo - ancho de banda) debe ser lo suficientemente alta como para cumplir con las necesidades del usuario sin que la dinámica de la red se vuelva impráctica.

Las condiciones de congestión en las redes ATM están previstas para que sean extremadamente dinámicas requiriendo de mecanismos de hardware lo suficientemente rápidos para llevar a la red al estado estacionario, necesitando que la red en sí, éste activamente involucrada en el rápido establecimiento de este estado estacionario. Sin embargo, esta aproximación simplista de control reactivo de lazo cerrado extremo a extremo en condiciones de congestión no se considera suficiente para las redes ATM.

La recomendación UIT - T I. 371 especifica un contrato de tráfico que define como el tráfico del usuario sería administrado. El contrato que existe para cada conexión virtual (*virtual path o virtual channel*), es básicamente un acuerdo entre el usuario y la red con respecto a la QoS (*Quality of Service*) y los

parámetros que regulan el flujo de celdas. Estos descriptores de tráfico dependen de una particular clase de servicio y pueden incluir bajo la especificación del ATM Forum UNI / a cinco QoS referenciados en los AALS. El objetivo de estas subclases de servicio es agrupar características de servicio como requerimiento de ancho de banda similares, sensibilidad a la perdida de datos y retardos para un correcto manejo de los datos en los puertos de acceso ATM, etc. Estos parámetros pueden incluir el SCR (*Sustained Cell Rate*), el MCR (*Mínimum Cell Rate (MCR), el Peak Cell Rate*) y/o el BT (Burst Tolerance). Para soportar todas las diferentes clases de servicios definidos por los estándares el conmutador ATM debe ser capaz de definir éstos parámetros en base a cada VC o cada VP y debe proveer amortiguadores (*buffers*) para absorber las ráfagas de tráfico. [4]

4.1.6. ATM sobre MPLS

De la misma manera que ATM ha sido usado para transportar tráfico multiservicio sobre una red de área amplia, ahora existe la oportunidad de utilizar MPLS para transportar tráfico ATM a través de un núcleo IP/MPLS. Cuando el tráfico ATM es mediado sobre una red IP/MPLS, las conexiones ATM se transportan transparentemente sobre túneles LSP establecidos entre puntos del borde del núcleo. En la red convergente ATM/MPLS, hay túneles LSP entre las pasarelas de mediación ATM/MPLS que rodean el borde de la red MPLS. Estos LSP sirven como túneles de transporte a través de la red MPLS. La red ATM ve a los nodos de mediación ATM/MPLS como conmutadores ATM, y a los túneles LSP como simples enlaces virtuales ATM punto a punto que conectan los nodos ATM.

El desafío de la mediación es construir los túneles LSP (*Label Switch Path*) a través del núcleo MPLS de tal forma que proporcione el mismo o mejor nivel de servicio que el enlace físico ATM. En la pasarela de mediación ATM/MPLS, las conexiones que atraviesan desde la red ATM a la red MPLS se admiten en el túnel LSP de la misma manera que lo serían en un enlace físico ATM. Una función de control de admisión de las conexiones en la pasarela de mediación ATM/MPLS garantiza que el túnel LSP tiene suficientes recursos para acomodar los requerimientos de servicio de las conexiones ATM. Los mecanismos de colas y planificación usados para lanzar las tramas MPLS conteniendo tráfico ATM en los túneles LSP serán funcionalmente equivalentes a los usados para lanzar células ATM en enlaces físicos ATM.

Un punto fuerte de ATM es que puede proporcionar diferentes niveles de calidad de servicio a diferentes clientes. Esta habilidad se mantiene y se mejora en la red convergente ATM/MPLS. Entre un par dado de pasarelas de mediación ATM/MPLS, se pueden transportar varias conexiones ATM con diferentes

calidades de servicio dentro del mismo túnel LSP. Dentro de la red MPLS, un conmutador MPLS puede simplemente conmutar las tramas de un túnel LSP particular entre el punto de entrada y el de salida manteniendo un orden estricto de lo primero que entra es lo primero que sale. Esto significa que el enlace ATM virtual representado por el túnel LSP imitará perfectamente el comportamiento de un enlace físico ATM.

Alternativamente, cada trama MPLS puede transportar en su cabecera, específicamente en los bits experimentales (EXP), una indicación de la clase de servicio que corresponde a la trama. De esta forma, las tramas MPLS que transportan el tráfico de una conexión ATM sobre un túnel particular LSP pueden ser marcadas para recibir diferente tratamiento que el tráfico de otra conexión ATM del mismo túnel LSP. La red MPLS asume un papel activo en la diferenciación de los servicios. A diferencia de los enlaces físicos ATM, los enlaces virtuales ATM proporcionados por los túneles LSP pueden ser elásticos. Los servicios ATM de tiempo real pueden ser ajustados para encajar en los recursos reservados dentro del túnel LSP, y los servicios ATM sin calidad garantizada *("Best Effort")* pueden estar autorizados a expandirse más allá de estos límites para aprovechar de la capacidad no utilizada dentro de la red MPLS.

El despliegue de redes multiservicio ATM ha permitido a los proveedores de servicio consolidar varias redes dispares en una infraestructura común con una gran reducción de costes. Como resultado los proveedores de servicio ahora buscan que los servicios de datos sean una de sus operaciones más rentables.

Para permanecer competitivos, los proveedores de servicios deben ajustar sus operaciones usando elementos que puedan transportar y gestionar tráfico de múltiples tipos de servicio. Las redes superpuestas actuales deben sufrir un proceso continuo de consolidación y optimización de red: La voz se convertirá en un tipo de datos más dentro del núcleo de paquetes. IP y ATM coexistirán en un núcleo multiprotocolo con MPLS como la tecnología unificadora que une los beneficios de ambos mundos. Se desarrollará una capa subyacente de transporte óptico inteligente.

La consolidación reducirá la complejidad y el coste de construir, configurar y operar redes separadas, y proporcionará la infraestructura necesaria para soportar nuevos servicios.

Para las redes ATM existentes, donde se usan líneas alquiladas para transportar el tráfico troncal y existe una significativa infraestructura en el núcleo de paquetes, es posible obtener un gran ahorro consolidando este tráfico troncal en el núcleo de la red IP/MPLS.

4.2. Frame Relay

4.2.1. Introducción

Frame Relay es un protocolo de WAN de alto desempeño que opera en las capa física y de enlace de datos del modelo de referencia OSI. Originalmente, la tecnología Frame Relay fue diseñada para ser utilizada a través de las ISDN (*Interfases de la Red Digital de Servicios Integrados*). Hoy en día, se utiliza también a través de una gran variedad de interfases de otras redes. [5]

Frame Relay es una tecnología de conmutación de paquetes. En las redes que utilizan esta tecnología, las estaciones terminales comparten el medio de transmisión de la red de manera dinámica, así como el ancho de banda disponible. Los paquetes de longitud variable se utilizan en transferencias más eficientes y flexibles. Posteriormente, estos paquetes se conmutan entre los diferentes segmentos de la red hasta que llegan a su destino. Las técnicas de multiplexaje estadístico controlan el acceso a la red en una red de conmutación de paquetes. La ventaja de esta técnica es que permite un uso más flexible y eficiente de ancho de banda, las velocidades de acceso de Frame Relay van desde los 56 kbps, 64 kbps a los 34 Mbps.

A veces se describe a Frame Relay como una versión compacta de X.25 con menos características en cuanto a robustez, como el ventaneo y la retransmisión de los datos más recientes, que se ofrecen en X.25. Esto se debe a que Frame Relay normalmente opera a través de instalaciones WAN que ofrecen servicios de conexión más confiables y un mayor grado de confiabilidad que las disponibles a finales de los años 70 e inicio de los 80, las cuales servían como plataformas habituales para las WANs X.25. Frame Relay es estrictamente una arquitectura de la Capa 2. [6]

Frame Relay es un servicio de vanguardia tecnológica para la transmisión de datos a altas velocidades, que ofrece banda sobre demanda que permite la interconexión de múltiples localidades distribuidas en cualquier parte de México, para el intercambio de información entre ellas, además mediante las distintas alianzas estratégicas, es posible proporcionar el servicio alrededor del mundo con los más altos estándares de calidad.

El servicio está diseñado para aplicaciones que generan tráfico cuyo comportamiento es en forma de ráfagas (burst traffic) de altos volúmenes de datos y de transmisión frecuente; para lo cual se establece

una conexión virtual permanente entre el origen y el destino, de esta manera es posible transmitir información a la velocidad contratada por el cliente.

Aunque bajo ciertas condiciones Frame Relay es capaz de transportar voz, al igual que Internet, es una tecnología pensada en el transporte de datos.

4.2.2. Dispositivos de Frame Relay

Los dispositivos conectados a una WAN Frame Relay caen dentro de una de dos categorías generales.

Equipo Terminal de Datos. Los DTEs (*Data Terminal Equipment*), en general, se consideran equipo de terminal para una red específica y, por lo general, se localizan en las instalaciones de un cliente. De hecho, pueden ser propiedad del cliente. Algunos ejemplos de los dispositivos DTE son las terminales, computadoras personales, enrutadores y puentes (*bridges*).

Equipo de Circuito Terminal de Datos. Los DCEs (*Data Circuit terminationEquipment*), son dispositivos de interconexión del propietario de la compañía de larga distancia. El propósito del equipo DCE es proporcionar los servicios de temporización y conmutación en una red, que son en realidad los dispositivos que transmiten datos a través de la WAN. En la mayoría de los casos, éstos son conmutadores y enrutadores. [7]

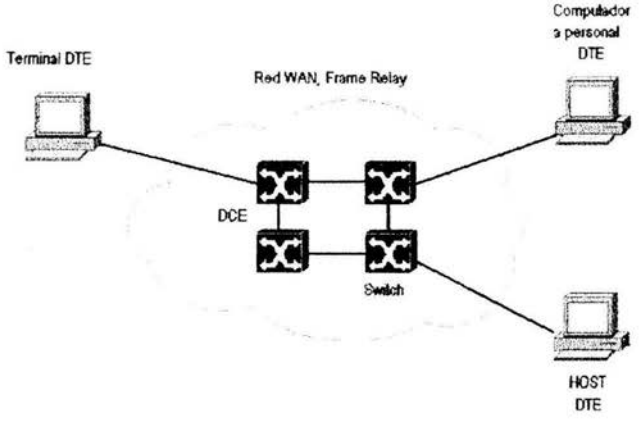


Figura 4.2.2.1. Dispositivos de Frame Relay

La conexión entre un dispositivo DTE y un dispositivo DCE consta de un componente de la capa física y otro de la capa de enlace de datos, El componente físico define las especificaciones mecánicas, eléctricas funcionales y de procedimiento para la conexión entre dispositivos. La componente de capa de enlace definen al protocolo que establece la conexión ente el dispositivo DTE, que puede ser un enrutador, y el dispositivo DCE que puede ser un conmutador.

Circuitos Virtuales Frame Relay

Frame Relay ofrece comunicación de la capa de enlaces de datos orientada a la conexión esto significa que hay una comunicación definida entre cada par de dispositivos y que estas conexiones están asociadas con el identificador de conexión. Este servicio se implementa por medio de un circuito virtual Frame Relay, que es una conexión lógica creada entre dos DTE (*Equipos Terminales de Datos*) a través de una PSN (*Red de Comunicación de Paquetes*) de Frame Relay.

Los circuitos virtuales ofrecen una trayectoria de comunicación bidireccional de un dispositivo DTE a otro y se identifica de manera única por medio del DLCI (*Identificador de Conexiones de Enlace de Datos*). Se puede multiplexar una gran cantidad de circuitos virtuales en un solo circuito físico para transmitirlos a través de la red. Con frecuencia esta característica permite conectar múltiples dispositivos DTE con menos equipo y una red compleja.

Un circuito virtual puede pasar por cualquier cantidad de dispositivos intermedios DCE (Conmutadores) ubicados en la red Frame Relay PSN.

Los circuitos virtuales Frame Relay caen dentro de dos categorías al igual que ATM: SVCs (*Circuitos Virtuales Conmutados*) y PVCs (*Circuitos Virtuales Permanentes*).

Los circuitos virtuales de Frame Relay se identifican a través de los DLCIs (*Identificadores de Conexión del Enlace de Datos*). Normalmente los valores de DLCI son asignados por el proveedor de los servicios de Frame Relay (en su caso, la compañía telefónica).

Los DLCIs Frame Relay tiene un significado local, lo que significa que los valores en sí mismo no son únicos en la WAN Frame Relay; por ejemplo, dos dispositivos DTE conectados a través de un circuito virtual, pueden usar un valor diferente de DLCI para hacer referencia a la misma conexión.[8]

La siguiente figura nos ilustra como dos diferentes dispositivos DTE pueden asignar a un circuito virtual un valor DLCI diferente en cada extremo de la conexión.

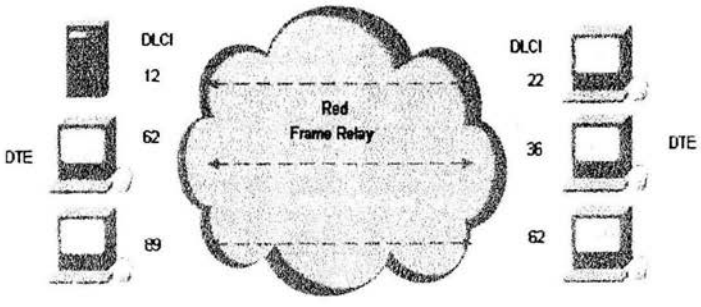


Figura 4.2.2.1. Asignación de un DLCI diferente a cada extremo de la conexión de un circuito virtual

4.2.3. Mecanismos de control de saturación

Frame Relay reduce el gasto indirecto de la red, al implementar mecanismos simples de notificación de la saturación, mas que un control de flujo explícito por cada circuito virtual. En general Frame Relay se implementa sobre medios de transmisión de red confiables para no sacrificar la integridad de los datos, ya que el control de flujo se puede realizar por medio de los protocolos de las capas superiores La tecnología Frame Relay implementa dos mecanismos de notificación de saturación:

- FECN (*Notificación de la Saturación Explícita Hacia Adelante*)
- BECN (*Notificación de la Saturación explícita Hacia atrás*)

Tanto FECN como BECN son controlados por un solo bit incluido en el encabezado de la trama Frame Relay. Este también contiene un bit DE (*Elegibilidad para descarte*), que se utiliza para identificar el tráfico menos importante que se puede eliminar durante periodos de saturación.

Bit FECN

El bit FECN es parte del campo direcciones en el encabezado de la trama Frame Relay. El mecanismo FECN inicia en el momento en que un dispositivo DTE envía tramas Frame Relay a la red. Si la red esta saturada, los dispositivos DEC (conmutadores) fijan el valor de los bits FECN de las tramas en 1.

Cuando las tramas llegan al dispositivo DTE de destino, el campo de direcciones (con el bit FECN en 1) indica que la trama se saturó en su trayectoria del origen al destino. El dispositivo DTE puede enviar esta información a un protocolo de las capas superiores para su procesamiento.
Dependiendo de la implementación, el control de flujo puede iniciarse o bien la indicación se puede ignorar.

Bit BECN

El bit BECN es parte del campo Direcciones del encabezado de la trama Frame Relay. Los dispositivos del DCE fijan el valor del bit BECN en 1 en las que viajan en sentido opuesto alas tramas con bit FECN igual a 1. Esto permite al dispositivo DTE receptor saber que una trayectoria específica en la red está saturada.

Posteriormente el dispositivo DTE envía información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien se puede ignorar la indicación.

Bit DE

El bit DE (Elegibilidad para Descarte) de utiliza para indicar que una trama tiene una importancia menor que otras. El bit DE es parte del campo Direcciones en el Encabezado de la trama Frame Relay.

Los dispositivos DTE pueden fijar el valor del bit DE de una trama en 1 para indicar que esta tiene una importancia menor respecto a las demás tramas. Al saturarse la red los dispositivos DCE descartaran las tramas con el bit DE fijado en 1 antes de descartar aquellas que no la tienen. Por lo anterior disminuye la probabilidad de que los dispositivos DCE de Frame Relay eliminen datos críticos durante el blindaje de saturación.

4.2.4. Mecanismo de verificación de errores

Frame Relay utiliza un mecanismo para la verificación de errores conocido como CRC (*Verificación de Redundancia cíclica*). El CRC compara dos valores calculados para determinar si se ha presentado errores durante la transmisión del origen al destino. Frame Relay disminuye el gasto indirecto al implementarse la verificación de errores mas que su corrección. Frame Relay por lo general se implementa en medios confiables de transmisión de red, por lo que la integridad de los datos no se sacrifica si la corrección de un error se deja a los protocolos de las capas superiores que operan en la parte más alta de Frame Relay. [9]

4.2.5. Ventajas

- El servicio se basa en una tecnología madura y probada.
- Posibilidad de conexión a bajas y altas velocidades según se requiera.
- Redundancia y diversidad de conexiones dentro de la red, con la garantía de una total seguridad en el transporte de la información.
- Administración de la plataforma de comunicaciones por una empresa especializada.
- Eliminación del Encabezado. Frame Relay elimina el encabezado asociado con X.25, el cual realiza las corrección de errores y la retransmisión de datos, lo cual obliga a los dispositivos inteligentes del usuario realizar la corrección de errores.
- Multiplexación Estadística. Comparado con las líneas privadas, Frame Relay simplifica las configuraciones ya que cada sitio necesita una sola línea física de acceso a la red de *MultiData* para comunicarse con múltiples sitios. Sobre esta misma línea de acceso, se llevan a cabo "múltiples conversiones" sobre un Circuito Virtual Permanente (PVC) predefinido. Un PVC interconecta dos sitios, tal como lo hace una línea privada, pero en este caso el ancho de banda es compartido, a diferencia de las líneas privadas en las que el ancho de banda es dedicado para el uso de un solo enlace.

- Al soportar enlace lógicos múltiples sobre una misma línea física, se reduce la cantidad de equipo terminal del cliente, costos de los puertos y líneas físicas requeridas para interconectar usuarios. Ya que los PVC's están predefinidos para cada par de dispositivos finales, siempre esta disponible una ruta para la aplicación. Esto se traduce en accesos mas rápidos a la red para las aplicaciones del usuario final.

- Confiabilidad. La conmutación de paquetes permite que las llamadas sean re-enrutadas dentro de la red en caso de fallas, también permite conectividad diversa utilizando un esquema de direccionamiento para dicho propósito.

- El re-enrutamiento protege a la red de fallas en el equipo y en la línea, asegurando el transporte de datos aun en condiciones críticas.

- Transparencia al Protocolo. Frame Relay provee de servicio de transporte transparente al protocolo, para protocolos de capas superiores. Al encapsular protocolos de capas superiores, Frame Relay elimina la necesidad de conversión de protocolo.

- Asignación Dinámica de Ancho de Banda. Frame Relay provee de un servicio de ancho de banda sobre demanda permitiendo al usuario incrementar potencialmente su ancho de banda de una manera dinámica en función de las disponibilidad del mismo en ese momento.

4.2.6. Desventajas

Una característica existente en la conmutación de paquetes es una técnica que es actualmente muy considera por los usuarios, el proceso de garantizar el envío de datos.

Frame Relay no ofrece esto, no se establece ninguna orden acerca como las tramas deben pasar a través de la red. La única recomendación de Frame Relay es que las tramas deben llegar en el mismo orden en que fueron mandadas. Para garantizar la correcta secuenciación de la tramas.

Este mecanismo de secuenciación no debe confundirse con el proceso de garantizar la integridad de los datos. Las redes de conmutación de paquetes, generalmente garantizan que los datos que son mandados en la red son recibidos por el usuario en el misma secuencia y sin errores. Mediante un número de comprobación secuencia de paquetes y su validación, una comprobación de error en los paquetes y de las capacidades de buffering.

En cambio Frame Relay no garantiza la entrega de los datos. Los requisitos para que los datos sean entregados en la misma secuencia en que fueron recibidos esta relacionado únicamente con que los datos no sean perdidos dentro de la red.

La intención del protocolo de Frame Relay es operar a altas velocidades, en circuitos digitales de excepcionalmente buena calidad, donde los errores en los bits son extremadamente raros. Sin embargo, mientras que el número de errores introducido por el uso de esa infraestructura es pequeño, la red podría perder muchas tramas simplemente por que es incapaz de entregarlas a causa de la congestión.

4.2.7. Frame Relay sobre MPLS

El tráfico Frame Relay de los clientes puede ser encapsulado en paquetes MPLS y reenviados sobre un *backbone* MPLS a otro destinatario Frame Relay requerido por el cliente. Por lo cual los proveedores pueden añadir nuevos sitios con menos esfuerzo que típicamente Frame Realy proporciona y con una mayor seguridad de su información.

Con MPLS los paquetes son colocados en orden en una ruta previamente establecida y se mantienen en orden al menos que la ruta sea cambiada pero esto no sucede con frecuencia debido a que la ruta se establece antes de colocarlos.

Frame Relay puede ser directamente integrado en MPLS . Los conmutadores de Frame Relay han sido actualizados para realizar distribución de etiquetas y enrutamiento. El DLCI es usado como la etiqueta.

El *header* de Frame Relay es reemplazado por bits de control que contienen el FECN, BECN, y el DE bits

4.3. Ethernet

4.3.1. Introducción

Ethernet es el protocolo por el cual se comunican las computadores en un entorno local de red. El cable que se inserta atrás de la computadora y parece un *"jack"* de teléfono grande es utilizado para enviar información en este protocolo, la computadora utiliza una tarjeta NIC (*Network Interface Card*) para realizar la comunicación. Cada tarjeta NIC contiene una dirección MAC (única), esta dirección MAC corresponde a la dirección física o *"Hardware"* de la computadora, esto sería el equivalente a la capa 2 del modelo OSI.[10]

Ahora bien, Ethernet como protocolo es considerado *CSMA/CD (Carrier Sense Multiple Acces Collision Detect)*, lo cual significa que por su cable solo puede ser transmitida una sola señal a cierto punto en el tiempo, esto es, si a un cable se encuentran conectadas 10 o 20 PC's, sólo una puede transmitir información a la vez, las demás deben esperar a que finalice la transmisión.

Además de esta característica *CSMA/CD*, el protocolo Ethernet también utiliza lo que es denominado *"Broadcast"* o "Transmisión a todas las terminales" , considerando el ejemplo anterior, lo que ocurre cuando una PC envía información es que las otras 9 o 19 recibirán esta misma información, lo que sucede posteriormente es que solo la PC con la dirección MAC especificada acepta la información, las restantes la descartan.

Llega un punto en el uso de una red en que estos *"Broadcasts"* son excesivos, aunado a la característica CSMA/CD que sólo una PC puede transmitir a la vez; la transmisión de información (*"throughput"*) en la red (LAN) empieza a decaer, y la forma mas común de evitar estos problemas es mediante un conmutador, aunque también pudiera ser utilizado un router pero esto dependerá de situaciones específicas. El problema es que el "Hub" transmite estos *"Broadcasts"* a todos los puertos que contenga, esto es, si el "Hub" contiene 8 puertos , todas las computadoras que estén conectadas al Hub recibirán la misma información, y como se mencionó anteriormente, en ocasiones resulta innecesario y excesivo. En cambio en un conmutador empieza a reconocer las direcciones MAC que generalmente son enviadas por cada puerto, en otras palabras, cuando llega información al Conmutador éste tiene mayor conocimiento sobre que puerto de salida es el más apropiado, y por lo tanto ahorra una carga a los demás puertos del conmutador, esta es una de la principales razones por la cuales en redes por donde viaja video, se procura utilizar conmutadores para de esta forma garantizar que el cable no sea

sobrecargado con información que eventualmente sería descartada por las computadoras finales, en el proceso, otorgando el mayor ancho de banda posible a los videos o aplicaciones CAD. [10]

4.3.2. Tipos de Ethernet

4.3.2.1. Cable coaxial

Este tipo de medio fue el primero en utilizarse para Ethernet y puede ser de dos tipos:

- *Thinnet* : Grosor de 1/4" o menor, comúnmente utilizado en diseños 10Base2 para ambientes ARCnet. Distancia Máxima de 185 mts. , el cableado utilizado para *Thinnet* es por lo general tipo RG-58.

- *Thicknet* : Comúnmente utilizado para "*backbones*" su tamaño es de 3/8" (0.375 pulgadas), utilizado en *backbones* de televisión y en diseños 10Base5, su distancia máxima entre centrales es de 500 mts.

A su vez el cableado coaxial puede ser de varios tipos, algunos son:

- *RG-58 /U* : Centro Sólido de Cobre "*Solid Copper core*"

- *RG-58 A/U* : Acordonado de Cobre "*Stranded wire copper*"

- *RG-58 C/U* : Especificación Militar "*Military Specification of RG-58 A/U*"

- *RG-59* : Transmisión Altabanda (cable de televisión) "*Broadband transmission*"

- *RG-62* : Tipo Red ARCnet "*ARCnet Network Specific*"

El cable coaxial a diferencia del cableado Ethernet que comúnmente es utilizado hoy en día, utiliza conectores llamados BNC *(British Naval Conectors)*, que es una "T" con orificios muy similares a los que son utilizados por un TV con cable. [11]

4.3.2.2. Cable empalmado "Twisted Pair"

Este tipo de cableado es el que se encuentra en mayor uso y puede ser de 5 tipos: [5]

- *Categoría 1* : (UTP) Apto únicamente para voz , utilizado para transmisiones comunes de telefonía.
- *Categoría 2* : (UTP) No es muy utilizado, su velocidad máxima de transmisión es 4 Mbps.
- *Categoría 3* : (UTP o STP) Optimo para transmisiones 10BaseT ,velocidad máxima hasta 10 Mbps.
- *Categoría 4* : (UTP o STP) Velocidad máxima 16 Mbps, comúnmente utilizado en un ambiente *Token Ring* de IBM.
- *Categoría 5* : (UTP o STP) Alcanza velocidades de 100 Mbps, utilizado para Fast-Ethernet.
- UTP : Significa que el cable no tiene capa protectora, UTP puede extenderse a una distancia máxima de 100 metros, es utilizado primordialmente para Ethernet.
- STP : Utiliza un capa protectora para cada cable para limitar interferencia, permite una mayor distancia que UTP (aunque limitadas) , comúnmente utilizado en ARCnet o Redes IBM.

El cable "empalmado" consta de 4 pares de alambre empalmado y utiliza conectores tipo RJ-45. Aunque todo "cable empalmado" utiliza conectores RJ-45, el uso de cada alambre dentro del "cable empalmado" depende del medio que se este utilizando, esto dependerá en gran parte de la Tarjeta NIC y Categoría de cable que se utilicen, los distintos medios son: [11]

- *10BaseT* : Conocido como IEEE802.3 permite una velocidad máxima de 10Mbps, su distancia máxima entre nodos es 100mt. El surgimiento de tarjetas NIC más eficientes han suplantado el uso de 10BaseT en favor de 100BaseTX-100BaseT4.

- *100BaseTX :* También conocido como Fast-Ethernet especificación IEEE 802.3u. 100TX solo utiliza 2 de los 4 pares del cableado, su distancia máxima es 100 mts. El cableado de categoría 5 es el mínimo requerido para 100TX, su velocidad máxima es de 100Mbps (si se utiliza full-duplex ésta puede ser 200Mbps).

- *100BaseT4 :* Permite la tecnología de Fast-Ethernet sobre cableado de categoría 3 y 4. Utiliza los 4 pares de alambre y altera el funcionamiento nativo de CSMA/CD en Ethernet; sin embargo el uso de los 4 pares de cable elimina la posibilidad de instalar transmisión full-duplex. Este método es utilizado exclusivamente cuando ya se tiene cableado categoría 3.

- *100FX :* Es la especificación para correr Fast-Ethernet sobre fibra óptica.

- *100BaseVG-AnyLAN :* 100Base(*Voice-Grade*)-Any LAN es la especificación IEEE802.12 que permite la transmisión de 100 Mbps sobre cableado Tipo 3. Es capaz de ejecutar tecnologías Token Ring y Ethernet. Sin embargo como es una implementación que no es estándar y no ofrece ningún beneficio sobre una instalación 100BaseTx, generalmente se opta por 100BaseTx en vez de 100BaseVG. [11]

4.3.3. Ventajas

- Tolerante a fallas
- Fácil ubicación de fallas
- Fácil de trasladar o cambiar

4.3.4. Desventajas

Debido a la naturaleza de Ethernet, siendo un protocolo de transmisión "*Broadcast*" el uso de Hubs en la red local (LAN) puede dar cabida a piratear información, ya que un "Hub" conforme recibe información es enviada a todos los nodos que están conectados al "Hub", y aunque las tarjetas NIC están diseñadas para descartar información que no va dirigida hacia ellas, si se tiene el suficiente conocimiento se puede alterar una tarjeta NIC para que intercepte estos paquetes de información, contraste esta deficiencia en seguridad con el funcionamiento de un "Conmutador" que evita la propagación de paquetes de

información a sólo ciertos puertos, de esta forma evitando que alguna computadora intrusa intercepte esta información. [12]

4.3.5. Ethernet sobre MPLS

Fiabilidad, relativa sencillez de instalación y mantenimiento, adaptabilidad y bajo costo de implementación son algunas de las características que avalan a Ethernet, aunque si hubiera que subrayar alguna en particular, probablemente, su mayor virtud sería la capacidad para evolucionar al ritmo que el desarrollo del mercado.

Así Ethernet ha sido capaz de avanzar en esa carrera desde los 10 Mbps iniciales, hasta llegar a los 1.000 Mbps proporcionados por Gigabit-Ethernet, sin olvidar la etapa intermedia que supuso Fast-Ethernet (100 Mbps). [13]

El 85 por ciento de las conexiones de red instaladas y servidores están basados en Ethernet. Ante la creciente presencia de las aplicaciones y servicios de nueva generación, cada vez resulta más impredecible acercar la banda ancha a los clientes. Conviene migrar la tecnología Ethernet de las redes LAN a las redes MAN y mejorar las redes IP con la implementación de MPLS. La mayoría de los operadores están familiarizados con estas tecnologías, sin embargo lo interesante es combinarlas para llevar Ethernet a cualquier ubicación.

MPLS aumenta los beneficos de Ethernet con las capacidades de fácil aprovisionamiento, SLT's (*Servicios LAN Transparentes*) y QoS . Ethernet es con gran diferencial, el tipo de red más usado en el mundo, gracias a su simplicidad y gran capacidad de ancho de banda (se cree que dentro de dos años se alcanzaran los 100 Gbps) a un precio muy competitivo. Por otro lado, el aumento de su alcance (mas de 70 Kilómetros) unido a las capacidades de alto rendimiento en conmutación y enrutamiento, más los mecanismos avanzados de QoS para soportar tráfico en tiempo real de voz y video, le sitúa en una posición privilegiada para dar el salto a las redes MAN.

Aunque Ethernet puede ser utilizado para ofrecer SLT's con SLA's (*Service Level Agreements*), el resultado no es de todo bueno. El hecho de que Ethernet sea una tecnología de nivel 2 hace que estos servicios presenten ciertas limitaciones, como falta de reserva de ancho de banda, tiempo s de recuperación en caso de caída de la red bastantes altos y problemas de escalabilidad.

La unión de Ethernet con MPLS es perfecta ya que MPLS mejora la 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 SLA's. Cuando se utiliza EoMPLS para dar SLT's 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 multiservico reciba el tratamiento real que requiere por sus características únicas de transmisión.

Para que una red IP sea considerada multiservicio debe ser capaz de acomodar el tráfico de voz y video. Estas aplicaciones no pueden sufrir grandes retrasos y sus paquetes no pueden ser reordenados.

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 SLA's acordados. Además se puede ofrecer balanceo de carga entre distintos LSP's y *backup* del LSP primario con las condiciones deseadas. De esta manera al cliente se le asegura elasticidad y recuperación del servicio que desea y esta dispuesto apagar. En definitiva, posiblemente esta tecnología facilite el despliegue de las redes de banda ancha a corto y medio plazo

Con Eo/MPLS, los operadores pueden ofrecer conectividad con servicios LAN trasparentes garantizados, escalables y seguros. Además con el aprovisionamiento dinámico de MPLS, se mejora la gestión manejabilidad de los túneles, reduciendo los problemas relacionados con su despliegue a gran escala. Eo/MPLS permite, además ofrecer gran ancho de banda a un costo menor, lo que unido a los mecanismos de QoS extremo a extremo garantizan el rendimiento de las nuevas aplicaciones criticas que necesitan y demandan los clientes. Las redes IP multiservicio tienen la capacidad de establecer contenidos personalizados y servicios customizados, y MPLS permite a los operadores explotar estas redes para ofrecer niveles previsibles de QoS, latencia y fiabilidad para todo tipo de aplicaciones[13].

REFERENCIAS

[1] ¿Qué es ATM?. La nueva tecnología.
www.cesga.es/ca/defaultC.html?Teleensino/vconf/atm.html&2

[2] Multiplexación en ATM, Protocolo
http://www.cgrt.com/trabajo/atm/atm.shtl

[3] Asyncronous Transfer Mode Switching, Cisco System Inc; 2002
http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm

[4] ATM y sus orígenes
http://www.comunicaciones.unitronics.es/tecnologia/atm_origenes/atm_origenes.htm

[5] Mecanismos de Control de Saturación. Frame Relay
www.angelfire.com/sc/itiaux/antecede.hmtl

[6] Frame Relay Tutorial
http://consulitel.es/html/tutoriales/articulos/tutorial_fr.html

[7] Frame Relay: Networks for Tomorrow and today
http://new.fr.forum.com/4000/4000index.html

[8] Introducción a Frame Relay, Sunrise Telecom. Incorporated, Nov 1998
http://www.sunrisetelecom.com/espanol/frame_relay.pdf

{9] NNI:The Key to Multi-Carrier Frame Relay
http://new.fr.forum.com/7000/7000index.html

[10] La Ethernet del siglo XXI ya está aquí. Almudena, Jiménez
http://www.femp.es/documentos/rural/documentación/reg%20tec%5ethernet_sigloXXI.pdf

[11] Interworking Technologoes Hadbook. Segunda Edición. Cisco Press Cap 10

[12] Tecnologías de Interconectividad de Redes
http://www.angelfire.com/sc/itiaux/mecanism.html

[13] Eo/MPLS

www.soluziona.es/htdocs/areas/telecomunicaciones/interes/publicaciones/articulo08.shtml+MPLS+en+el+mundo+&hl=es

CAPÍTULO 5

5. ARQUITECTURA Y FUNCIONAMIENTO DE MPLS

5.1. Estructura de las redes MPLS

La estructura de MPLS describe los mecanismos para ejecutar la conmutación de etiquetas, en donde se combinan los beneficios del envío de paquetes basados en capa 2 con los benéficos del enrutamiento en capa de red. Similarmente a las redes de capa 2 (Frame Relay o ATM), MPLS asigna una etiqueta a los paquetes para ser transportados a través de redes basadas en celdas o paquetes. El mecanismo de esta tecnología es la conmutación de etiquetas, en la cual las unidades de datos (paquetes o celdas) son llevadas por etiquetas cortas que le dicen a los nodos de conmutación como procesar y enviar los datos.

Su arquitectura esta dividida en dos componentes funcionales: las componentes de envío (también llamado plano de datos) y la componente de control, las cuales a continuación se dará una breve explicación.

5.1.1. Funciones de control y envío

Todas las soluciones de conmutación multinivel (incluido MPLS) se basan en dos componentes básicos comunes:

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

En la figura 5.1.1 se representa la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos de enrutamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros enrutadores, la construcción y el mantenimiento de las tablas de enrutamiento. Además la componente de control es la encargada de crear las asociaciones entre etiquetas y FEC's y distinguir esta información. Mientras que al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de enrutamiento para cada paquete. En concreto, la componente de envío examina la información de la

cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde el interfaz de entrada al de salida a través del correspondiente hardware de conmutación. Por tanto, la componente de envío consiste en el conjunto de procedimientos que usa el enrutador para tomar la decisión sobre el envío de un paquete. Estos algoritmos definen la información del paquete que utiliza el enrutador para encontrar una entrada en la tabla de enrutamiento, así como los procedimientos exactos que el enrutador utiliza para encontrar la entrada [1].

Cada enrutador de la red implementa ambos componentes. Podríamos ver el enrutamiento del nivel de red como una composición de ambos componentes (control y envío) implementada de una manera distribuida por el conjunto de enrutadores que conforman la red.

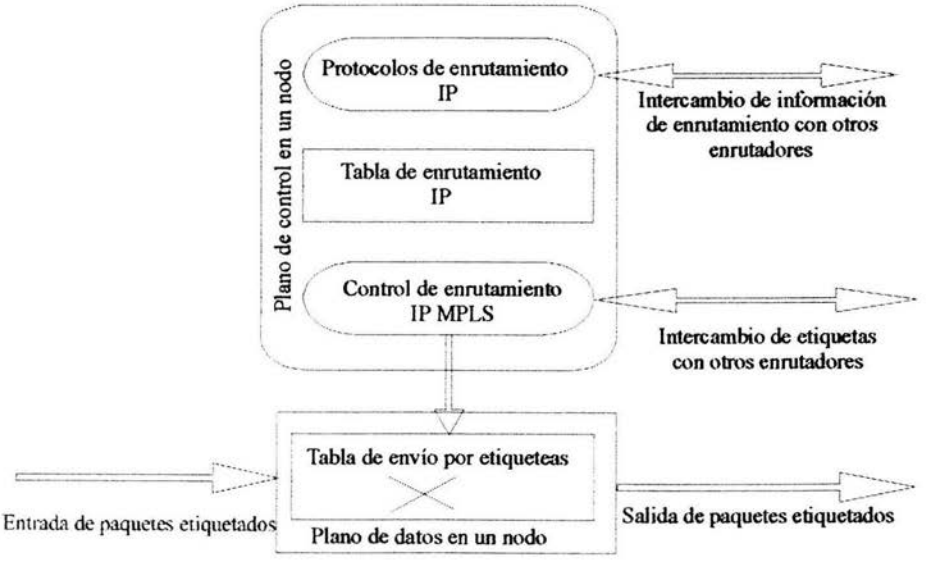


Figura 5.1.1.1 Componente de control y componente de envío

Al separar la componente de control de la componente de envío, cada una de ellas se puede implementar y modificar independientemente. El único requisito es que la componente de control mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para ATM. La diferencia está en que ahora lo que se envía por el interfaz físico de salida son

paquetes "etiquetados". De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de enrutamiento, pero ¿ que es una etiqueta?.

5.1.2. Qué es una etiqueta

En cuanto a la etiqueta que marca cada paquete, no es un solo campo de unos pocos bits, de longitud fija que se añade a la cabecera del mismo, si no que es aquella que identifica una FEC (Forwarding Equivalence Class) especifica. En MPLS, la asignación de un paquete a una FEC particular se hace tan solo una vez, y es cuando el paquete ingresa a la red MPLS. La FEC a la que es asignado dicho paquete es codificada como un valor fijo llamado "etiqueta". Por lo que para establecer la relación entre una FEC y un paquete, MPLS usa la etiqueta.

Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes. Por ejemplo, en el enrutamiento convencional IP una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo.

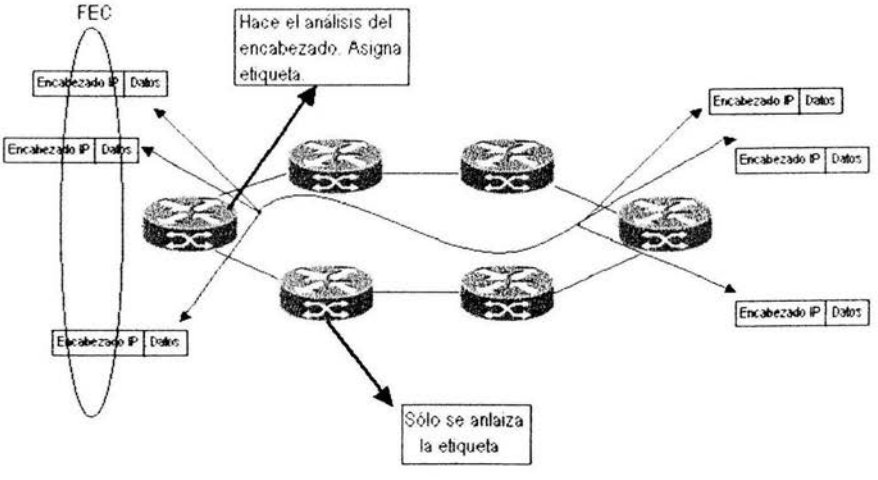


Figura 5.1.2.1. Un conjunto de paquetes se envían por un mismo camino

También se puede asociar el valor de la FEC a una dirección destino y a una clase de tráfico. La clase de tráfico esta asociada habitualmente a un número de puerto destino.

Uno de los motivos por los que MPLS utiliza la FEC es porque permite agrupar paquetes en clases. Gracias a esta agrupación, el valor de la FEC en el paquete se puede utilizar para establecer prioridades, de tal forma que se da más prioridad a unos FECs sobre otros. Se pueden usar las FECs para dar soporte a operaciones eficientes de QOS (Quality Service). Por ejemplo, se pueden asociar FECs de alta prioridad a tráfico de voz en tiempo real, de baja prioridad a correo, etc.

Una parte esencial de la tabla de enrutamiento mantenida por un enrutador es la dirección del siguiente enrutador . Un paquete perteneciente a una FEC asociado a una determinada entrada de la tabla se reenviará al siguiente enrutador según esté especificado en dicha tabla.

Realmente, una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, asignando el tráfico a los correspondientes FEC.

El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (Label-Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay. En el fondo, lo que hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la diferencia básica con el modelo IP/ATM. Al hablar de MPLS con más detalle se entenderán mejor estas peculiaridades [2].

5.1.2.1. Ventajas del reenvío de etiquetas

En MPLS, la asignación de un paquete a una FEC se realiza cuando el paquete entra en la red asignándole a dicho paquete una etiqueta. Cuando un paquete es enviado hacia el próximo hop, su etiqueta es enviada junto con él; o sea que los paquetes han sido etiquetados antes de ser enviados. En los siguientes saltos sólo se usará la etiqueta para determinar la interfaz por donde reenviar el paquete, por lo que no será necesario analizar la cabecera del nivel de red. La etiqueta se usa como índice en la tabla de enrutamiento donde se obtiene el siguiente salto y la nueva etiqueta con la que sustituir la anterior. Hay que recordar que las etiquetas son locales a los enrutadores.

En MPLS los conmutadores pueden realizar el reenvío, pero éstos no tienen necesidad de analizar las cabeceras del nivel de red, todo el reenvío es mediante etiquetas . Esto tiene un numero importante de ventajas:

- El despacho de paquetes en MPLS puede ser hecho por enrutadores con la capacidad de inspeccionar las etiquetas y reemplazarlas, pero sin capacidad de analizar headers de paquete a nivel de red, o al menos sin poder hacerlo a la velocidad adecuada.
- Dado que un paquete se asigna a una FEC cuando entra en la red, el enrutador frontera que le asigna una etiqueta, podrá usar toda la información que tenga sobre el paquete, incluso información que no esté en la cabecera del nivel de red. Por ejemplo podrá usar información del nivel de transporte, como los números de puerto, para asignar paquetes a FECs. Por tanto, gran parte del trabajo se realiza antes de que el tráfico entre en la red. Con el enrutamiento convencional sólo se puede examinar la cabecera del nivel de red
- Es sencillo establecer decisiones de enrutamiento en base al enrutador de ingreso a la red, cosa imposible en enrutamiento convencional, (no se posee la información del enrutador de ingreso). Un paquete que entra en la red por un determinado enrutador puede etiquetarse de distinta forma que si hubiera entrado por otro. Por tanto, se pueden tomar decisiones dependientes del enrutador frontera que encapsula el paquete. Esto no se puede hacer en el enrutamiento convencional porque la identidad del enrutador frontera que introdujo el paquete en la red no viaja con el paquete.
- Las consideraciones que determinan la asignación de un paquete a una FEC pueden ser muy complejas sin impacto en los enrutadores del "core" que solo reciben y despachan los paquetes etiquetados.
- Se podría forzar a un paquete a seguir una ruta elegida explícitamente antes o en el momento que el paquete entre en la red, en vez de elegirse por el algoritmo dinámico de enrutamiento a medida que el paquete fluye por la red. Esto podría hacerse para permitir la ingeniería de tráfico. En el enrutamiento convencional el paquete tendría que llevar la información de la ruta (enrutamiento fuente). En MPLS se puede usar una etiqueta para representar la ruta, de tal forma que el paquete no tiene por qué llevar la información de la ruta.
- Se pueden establecer reglas de precedencia en las FEC, de forma de aplicar Clase de Servicio al tráfico manejado. Esta técnica permite el etiquetado de paquetes de cualquier protocolo de nivel de red, por ello se la denomina "Multiprotocolo".

5.1.2.2. Formato de las etiquetas

Una etiqueta MPLS tiene 32 bits, de los cuales se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS), 1 bit de stack para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (time-to-live), número de nodos (saltos) que puede atravesar el paquete MPLS. Se necesita porque los LSRs intermedios no analizan el campo IP TTL.

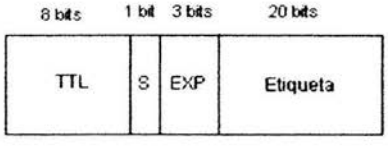


Figura 5.1.2.2.1Estructura de una etiqueta

5.1.2.3. Dónde se insertan las etiquetas

Las etiquetas son insertadas dependiendo del tipo de transporte, MPLS debe funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por lo se separara en dos alternativas para la inserción de las etiqueta, una donde el protocolo de transporte de datos ya contenga un campo para etiquetas, y otro donde no sea este caso.

Alternativa 1

Para los protocolos de transporte de datos que ya contengan un campo para etiquetas como es el caso de ATM y Frame Ralay . ATM puede llevar la etiqueta en el identificador de canal virtual VCI (*Virtual Channel Identifier*) o en el el identificador de trayecto virtual VPI (*Virtual Path Identifier*), mientras que en Frame Relay estará en el campo DLCI (*Data Link Connection Identifier*)

El hecho de llevar la etiqueta en el campo VCI de las células ATM permite que un conmutador ATM funcione como un LSR (*Label Switching Enrutador*) , un enrutador de conmutación de etiquetas, siempre que tenga el software de control apropiado.

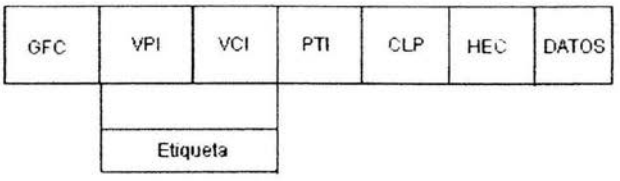
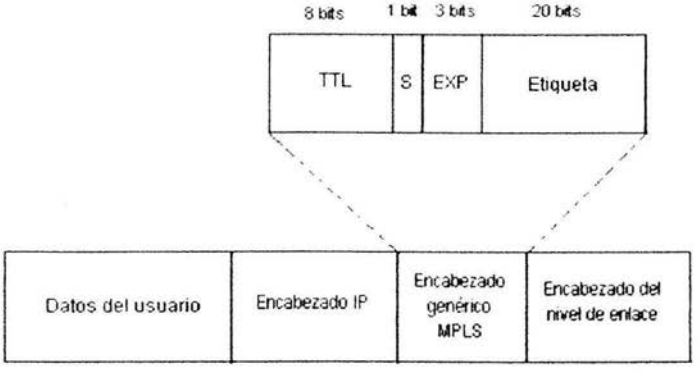


Figura 5.1.2.3.1 Inserción de las etiquetas en ATM

Alternativa 2

Si la tecnología de nivel 2 empleada no soporta un campo para etiquetas, como es el caso de enlaces PPP ethernet, LAN, entonces se emplea un encabezado genérico MPLS de 4 octetos, denominada encabezado shim o de relleno , que contiene un campo específico para la etiqueta y que se inserta entre el encabezado del nivel 2 y nivel 3 del paquete.



En la figura 5.1.2.3.2 Esquema de los campos del encabezado genérico

En DWDM (*Dense Wavelength Division Multiplexing*) la etiqueta puede asociarse con una longitud de onda en la fibra.

De este modo se permite cualquier tecnología o combinación de tecnologías del nivel de enlace. Ej: conmutación de etiquetas en redes Ethernet.

La cabecera shim o genérica está situada en una posición donde la mayoría de los enrutadores pueden procesarla por software, por lo que los enrutadores convencionales pueden convertirse en LSRs siempre que tengan el software apropiado

5.1.3. Tipos de nodos MPLS

Como en cualquier nueva tecnología, muchos términos nuevos son introducidos para describir los dispositivos que conforman a la arquitectura. Estos nuevos términos describen la funcionalidad de cada uno de los dispositivos y sus papeles dentro de la estructura MPLS.

5.1.3.1. LER

Un LER (*Label Edge Router*) es un LSR que opera en los extremos de las redes MPLS, funciona como el punto de interconexión entre ésta y la red de acceso y son los encargados de etiquetar los paquetes que entran en la red o de poderle quitar las etiquetas según sea el caso. Para poder realizar este trabajo estos LERs deben implementar la componente de control y la componente de envío tanto del enrutamiento convencional como de la conmutación de etiquetas.

Estos a su vez se dividen en dos tipos:

- LER de entrada (ingress LSR): recibe tráfico de usuario (por ejemplo datagramas IP) y lo clasifica en su correspondiente FEC. Genera una un encabezado MPLS asignándole una etiqueta y encapsula el paquete junto al encabezado MPLS.
- LER de salida (egress LSR): LSR que realiza la operación inversa al de entrada, es decir, desencapsula el paquete removiendo el encabezado genérico MPLS. Cuando el

paquete va a salir de la red MPLS, el LSR de salida recibe el paquete, le quita la etiqueta y lo reenvía al siguiente salto usando el componente de reenvío del enrutamiento convencional. Dicho LSR sabrá que el paquete quiere abandonar la red simplemente porque el siguiente salto no es un LSR.

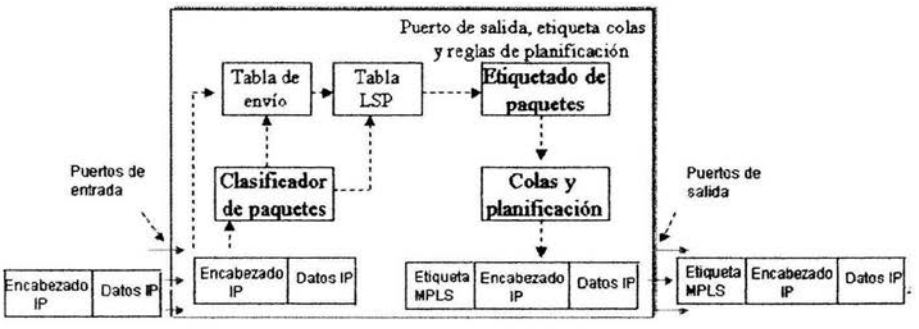


Figura 5.1.3.1.1 Arquitectura del LER

5.1.3.2. LSR intermedios.

Después de que los paquetes han sido etiquetados por el LER, éstos comienzan su viaje a través de la red MPLS, encontrándose en su trayectoria con los enrutadores de conmutación de etiquetas (LSRs) intermedios. Estos son los encargados de dirigir el tráfico en el interior de la red, de acuerdo con las etiquetas asignadas. Cuando un paquete arriba a un LSR intermedio, éste examina su etiqueta y la utiliza como un índice en una tabla propia que especifica el siguiente "salto" y una nueva etiqueta. Esta tabla se construye a partir de la información de enrutamiento que proporciona la componente de control, como se vera mas adelante. La función básica de los procedimientos de distribución de las etiquetas es permitir al LSR distribuir sus etiquetas hacia otros LSR's dentro de la red MPLS. El LSR intercambia entonces esta etiqueta por la que contenía el paquete y lo envía hacia el siguiente enrutador.

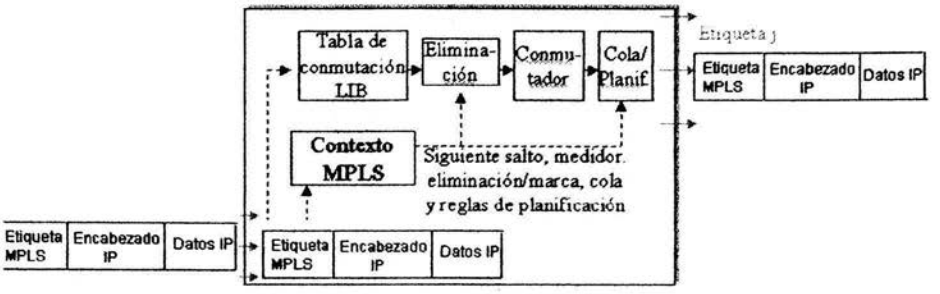


Figura 5.1.3.2 Arquitectura de un LSR

5.1.3.3. LSP

El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (*Label-Switched Paths)* funcionalmente equivalentes a los PVCs de ATM y Frame Relay. Por lo que se podría decir que un LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Swiching Enrutador) a otro, a través del dominio MPLS. Los LSPs simplex son aquellos que se establecen para un sentido del tráfico en cada punto de entrada a la red; el tráfico dúplex requiere dos LSPs, uno en cada sentido.

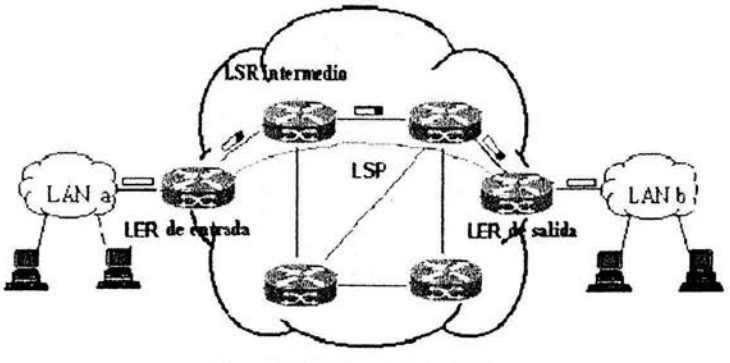


Figura 5.1.3.3.1 Tipos de Nodos MPLS

Enrutamiento salto a salto y explicito.

La selección de una ruta se refiere al método empleado para seleccionar el camino LSP para una determinada clase FEC. La arquitectura propuesta para el protocolo MPLS soporta dos opciones para la selección de ruta:

(1) enrutamiento salto a salto, y (2) enrutamiento explícito.

El enrutamiento salto a salto permite a cada nodo elegir independientemente el próximo salto de cada clase FEC. Este es el modo habitual hoy en dia en las redes IP existentes. Un camino LSP salto a salto es un camino LSP es una ruta seleccionada por el enrutamiento salto a salto.

En un camino LSP con *enrutamiento explícito*, cada enrutador LSR no elige independientemente el próximo salto; más bien, un único enrutador LSR, generalmente el enrutador de entrada o de salida del camino LSP, especifica varios (o todos) los enrutadores LSR del camino LSP. Si un único enrutador LSR especifica todo el camino LSP, el camino LSP es "estrictamente" explicitamente enrutado. Si un único enrutador LSR especifica solamente algunos enrutadores LSR del camino LSP, el camino LSP es explicitamente enrutado" aproximadamente".

La secuencia de los enrutadores LSR seguidos por un enrutamiento esplícito del camino LSP se puede elegir por configuración, o se puede seleccionar dinámicamente por un único nodo (por ejemplo, el nodo de salida puede hacer uso de la información topológica aprendida por una base de datos de estado de enlace con el fin de calcular el camino completo para el árbol que acaba en el nodo de salida

El enrutamiento explícito puede ser útil para algunos fines, tales como la política de enrutamiento o la ingeniería de tráfico. En MPLS, el enrutamiento explícito necesita ser especificado en el momento en que son asignadas las etiquetas, pero no tiene que ser especificado con cada paquete IP. Esto hace que el enrutamiento explícito MPLS sea mucho más eficiente que la alternativa del enrutamiento propio de IP.

Sin embargo puede que la ruta no esté completamente especificada, es decir, puede haber un conjunto de nodos (Nodo Abstracto) que es representado como un único salto en la ruta. También puede contener un identificador de Sistema Autónomo que permite que el LSP sea enrutado a través de un área de la red que está fuera del control administrativo de quien inició el LSP. Dentro de estos dos casos se hará un enrutamiento salto a salto.

Puede clasificarse como estricto (*strict*), aquel camino que incluye todos los nodos, nodos abstractos y Sistemas Autónomos por los que pasa y el orden establecido; o como tolerante (*loose*), aquél que incluye todos los saltos y mantiene el orden, pero puede incluir saltos que sean necesarios para alcanzar algún salto específico [3].

El camino puede que no sea óptimo puesto que deben tenerse en cuenta los parámetros del servicio. Los recursos serán reservados a lo largo del camino para asegurar QoS. Esto facilita la ingeniería de tráfico y el poder tener servicios diferenciados usando políticas de tráfico o métodos de gestión de red.

El establecimiento de un LSP para un FEC es unidireccional. El tráfico de vuelta debe tomar otro LSP.

Cuando se detecte un fallo en la red o la topología cambie se debe de proporcionar un nuevo LSP para re-enrutar el tráfico. En una ruta explícita estricta sólo se puede re-enrutar el tráfico en el LER de entrada que es quien decide la ruta, con lo que debe ser informado del error para proporcionar una ruta alternativa. En una ruta explícita tolerante cualquier LSP puede tomar un camino alternativo si es capaz de detectar el fallo del vecino, si la ruta ya está disponible o si un LSP de mayor prioridad requiere esos recursos reservados [3].

5.2. Descripción funcional del MPLS.

La operación del MPLS se basa en las componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí. Empecemos por la primera.

5.2.1. Funcionamiento del envío de paquetes en MPLS.

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un LSR a otro, a través del dominio MPLS.

En la figura 5.2.1.1 se puede ver la funcionalidad del MPLS. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control y de envío como se vio anteriormente. Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de enrutamiento definidos por el ATM Forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización LDP (*Label Distribution Protocol*), del que se tratará más adelante. Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de enrutamiento en las direcciones y el enrutamiento ATM, esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos a base de celdas..

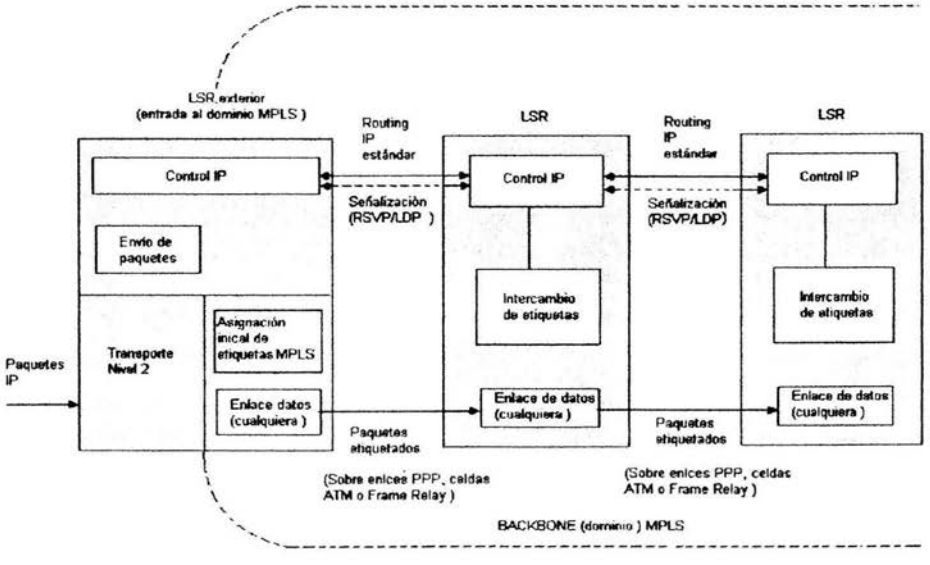


Figura 5.2.1.1. Esquema del funcionamiento del envío de paquetes en MPLS

Como vimos anteriormente el primer LSR que interviene en un LSP se le denomina LER de entrada y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs intermedios del dominio MPLS. La principal función de un LSR intermedio es la distribución de etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de enrutamiento que proporciona la componente de control y esta constituida por múltiples entradas, cada entrada consta de:

- Etiqueta de entrada
- Una o más subentradas:
  - Etiqueta de salida
  - Interfaz de salida
  - Dirección del siguiente salto

Puede haber más de una subentrada, puesto que hay que tratar los paquetes de difusión. De esta forma se puede enviar un paquete por múltiples interfaces de salida. Así como también puede existir una tabla de enrutamiento única o por interfaz, en cuyo caso a la hora de enrutar un paquete habrá que saber la interfaz por donde ha entrado el paquete.

La tabla está indexada por el valor de la etiqueta, de tal forma que la búsqueda en la tabla es inmediata. Necesitaremos un solo acceso a memoria, lo que se traduce en un acceso rápido.

Así mismo, 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 ese interfaz y con la misma etiqueta. En los LSR frontera, sólo hay una etiqueta, de salida o de entrada, según sea el caso. En la siguiente figura se ilustra un ejemplo del funcionamiento de un LSR del núcleo MPLS. A un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla proporcionada por la componente de control [4].

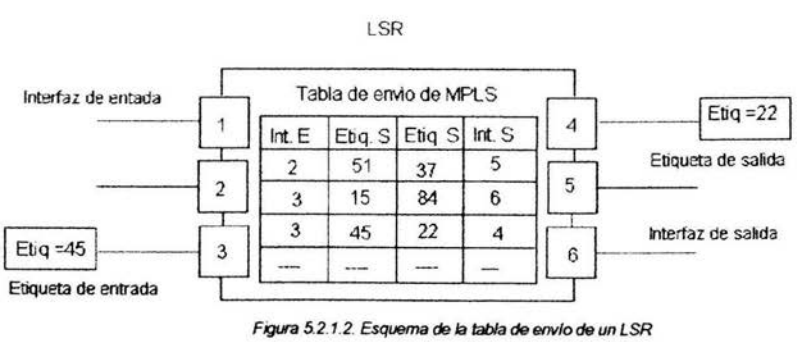


Figura 5.2.1.2. Esquema de la tabla de envío de un LSR

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LER de entrada. En la figura 5.1.1.3. el LER de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LER consulta la tabla de enrutamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LER le asigna una etiqueta con valor 5 y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran el encabezado IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LER de salida, ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por enrutamineto convencional.

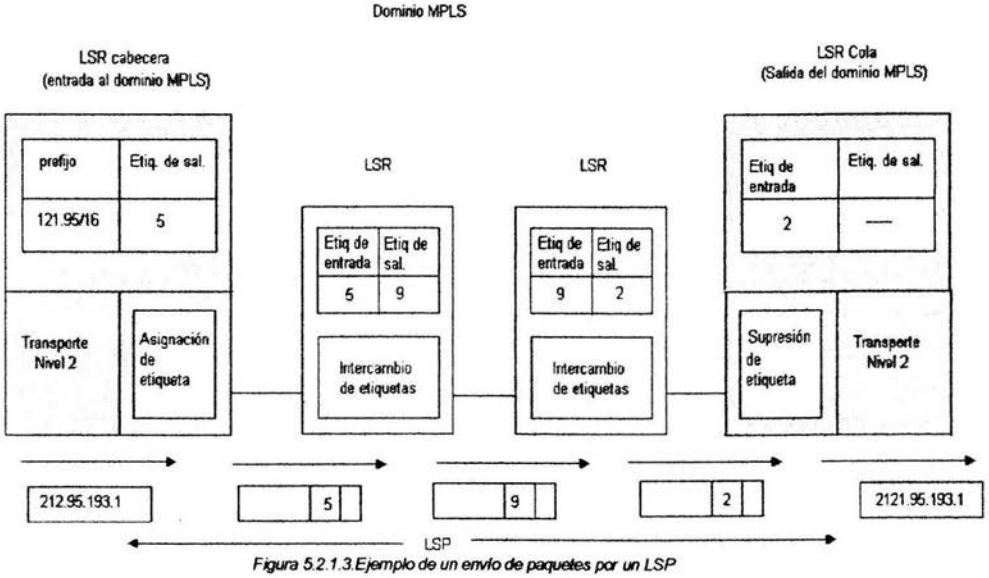


Figura 5.2.1.3.Ejemplo de un envío de paquetes por un LSP

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP.

5.2.2. Control de la información en MPLS

Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSPs mediante el procedimiento de intercambio de etiquetas según las tablas de los LSRs. Pero queda por ver dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSPs
- Cómo se distribuye la información sobre las etiquetas a los LSRs

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de enrutamiento. MPLS necesita esta información de enrutamiento para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información de enrutamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP...) para construir las tablas de enrutamiento (recuérdese que los LSR son enrutadores con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de "señalización" , las comillas se ponen por el impacto que puede suponer este término para los puristas del mundo IP, de naturaleza no conectiva. Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF. Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del LDP (Label Distribution Protocol). En el capítulo 5.3 veremos a mas a detalle estos protocolos.

5.3. Encapsulado de etiquetas y envío de paquetes

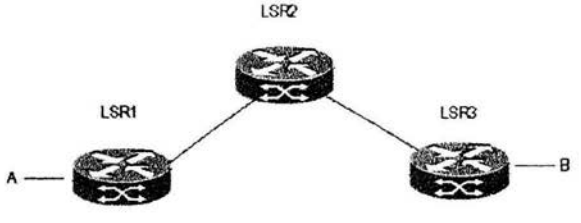
5.3.1. Distribución y asignación de etiquetas

Para la asociación de una etiqueta a una FEC, MPLS se apoya de los enrutadores LSR de tráfico de entrada y de tráfico de salida o mas comúnmente llamados Ru (upstream enrutador) y Rd (downstream enrutador), respectivamente.

5.3.1.1. Enrutadores LSR de tráfico de entrada y de tráfico de salida

Supongamos que los enrutadores Ru y Rd han acordado ligar la etiqueta L a la clase FEC F, para los paquetes enviados desde el enrutador Ru al enrutador Rd. Entonces con respecto a esta ligadura, el enrutador Ru es el enrutador LSR de tráfico de entrada y el enrutador Rd es el enrutador LSR de tráfico de salida.

Decir que un nodo es de entrada y que uno es de salida con respecto a una ligadura dada significa solamente que una determinada etiqueta representa una determinada clase FEC en paquetes que viajan del nodo de entrada al nodo de salida. Esto no significa implicar que actualmente los paquetes de esta clase FEC serían enrutados desde el nodo de entrada al nodo de salida.



Para un enlace entre A y B

LSR1 es el LER frontera de entrada
LSR3 es LER frontera de salida
LSR1 el enrutador Ru para el LSR2
LSR2 es el enrutador Ru para LSR3
LSR3 es el enrutador Rd para LSR2
LSR2 es el enrutador Rd para LSR1

Figura 5.3.1.1.1 Enrutadores LSR de tráfico de entrada y de tráfico de salida

En MPLS, la decisión correspondiente a la asignación de una etiqueta L a una FEC la realiza el LSR de tráfico de salida Rd con respecto a la asociación.

Entonces el enrutador LSR de tráfico de salida informa al enrutador LSR de tráfico de entrada de la ligadura. Por tanto, las etiquetas se asignan o asocian por medio del LSR de tráfico de salida y se distribuyen en el sentido que va del LSR de tráfico de salida al LSR de tráfico de entrada. Y en la tabla de enrutamiento de Ru tendremos como etiquetas de salida las etiquetas que el enrutador de tráfico de salida ha elegido, a lo que se llama asociación remota y como etiquetas de entrada las de la asociación local , es decir las que establezca el enrutador.

Como ejemplo veamos la figura 5.2.1.1.2. Si Ru y Rd son enrutadores LSR, entre ellos pueden acordar que cuando Ru transmita un paquete a Rd, Ru etiquetará cada paquete con un valor de etiqueta L si y solo si el paquete es un miembro de una determinada clase FEC F. Es decir, los enrutadores Ru y Rd pueden acordar una ligadura entre la etiqueta L y la clase FEC F para paquetes que se mueven del enrutador Ru al enrutador Rd.

Como resultado de este acuerdo, L es la etiqueta de salida del enrutador Ru representando a la clase FEC F, y L es la etiqueta de entrada del enrutador Rd , lo cual es llamado como asociación local representando a la clase FEC F.

Notar que L no representa necesariamente la clase FEC F para otros paquetes que están siendo enviados del enrutador Ru al enrutador Rd. L es un valor arbitrario que liga a la clase FEC F y es un valor local para los enrutadores Ru y Rd.

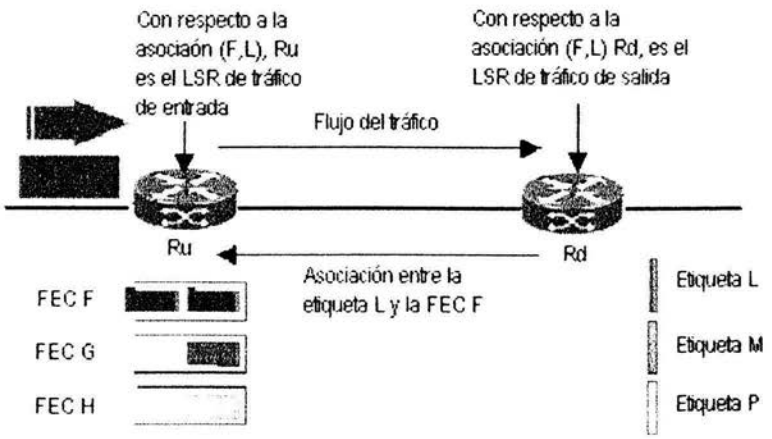


Figura 5.3.1.1.2 Asociación de etiquetas

Cuando hablamos de paquetes que son enviados del enrutador Ru al enrutador Rd, no implicamos que el paquete tenga su origen en el enrutador Ru ni que su destino sea el enrutador Rd. Mas bien queremos decir que son paquetes en tránsito desde un extremo a otro de los dos enrutadores LSR.

A veces es difícil o aún es imposible para el enrutador Rd decir, de un paquete que le llega con la etiqueta L, que la etiqueta L fue colocada en el enrutador Ru o por otro enrutador LSR. Típicamente esto será en el caso cuando los enrutadores Ru y Rd no son vecinos directos. En tales casos, el enrutador Rd debe asegurarse de que la ligadura de la etiqueta a la clase FEC es uno-a-uno, es decir, el enrutador Rd no debe acordar con el enrutador Ru1 ligar L a la clase FEC F1, mientras también esté acordando con algún otro enrutador LSR Ru2 ligar L a un clase FEC distinto F2, amenos que el enrutador Rd pueda siempre decir, cuando recibe un paquete con etiqueta de entrada L, si la etiqueta fué puesta al paquete por el enrutador Ru1 o si fué puesta por el enrutador Ru2.

Es la responsibilidad de cada enrutador LSR asegurarse que puede unicamente interpretar sus etiquetas de entrada.

Una determinada ligadura de la etiqueta L a la clase FEC F, distribuida por el enrutador Rd al enrutador Ru, puede tener asociados "atributos". Si el enrutador Ru, actuando como un enrutador LSR de tráfico de salida, también distribuye una ligadura de una etiqueta a la clase FEC F, entonces bajo determinadas condiciones, también se le puede requerir que distribuya el correspondiente atributo que recibió del enrutador Rd.

5.3.1.2. Alcance y unicidad de las etiquetas

Un enrutador LSR Rd determinado puede ligar la etiqueta L1 a la clase FEC F, y distribuir esta ligadura al puerto de distribución de etiquetas Ru1. El enrutador Rd también puede ligar la etiqueta L2 a la clase FEC F2, y distribuir esta ligadura al puerto de distribución de etiquetas Ru2. Si (y solo si) el enrutador Rd puede decir, cuando recibe un paquete de la parte superior si la etiqueta es l, si la etiqueta fué puesta por el enrutador Ru1 o Ru2, entonces la arquitectura no requiere que F1 == F2. En tales casos, podemos decir que el enrutador Rd está usando un espacio de etiquetas diferente para las etiquetas que distribuye al enrutador Ru1 que para las etiquetas que distribuye al enrutador Ru2.

En general, el enrutador Rd solamente puede decir si fué el enrutador Ru1 o Ru2 que pusieron la etiqueta L en la parte superior de la pila de etiquetas si se cumplian las condiciones siguientes

- si los enrutadores Ru1 y Ru2 son los únicos puertos de distribución a que el enrutador Rd
- distribuyó una ligadura de la etiqueta L, y
- si los enrutadores Ru1 y Ru2 están conectados directamente al enrutador Rd vía una interfase punto a punto.

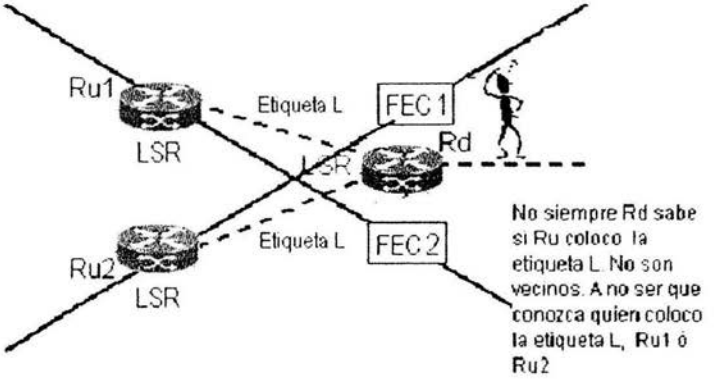


Figura 5.3.1.2.1. Rd no siempre sabe quién coloco la etiqueta

Cuando estas condiciones se cumplen, un enrutador LSR puede usar etiquetas que tienen alcance "por interfase",por ejemplo, que solo haya una por interfase. Podemos decir que el enrutador LSR está usando un "espacio de etiquetas por interfase". Cuando estas condiciones no se cumplen, las etiquetas deben ser únicas en el enrutador LSR que las ha asignado, y podemos decir que el enrutador LSR está usando un "espacio de etiquetas por interfase".

Si un enrutador LSR Rd concreto es adjuntado a un enrutador LSR Ru concreto sobre dos interfases punto a punto, entonces el enrutador Rd puede distribuir al enrutador Ru una ligadura de la etiqueta L a la clase FEC F1, así como una ligadura de la etiqueta L a la clase FEC F2, F1 != F2, si y solo si cada ligadura es válida solo para paquetes que el enrutador Ru envía al enrutador Rd sobre una interfase determinada de las suyas. En todos los demás casos, el enrutador Rd no debe distribuir al enrutador Ru ligaduras de las mismas etiquetas para dos clases FEC diferentes.

Esta prohibición se mantiene si las ligaduras son consideradas como pertenecientes a diferentes "niveles de jerarquía". En MPLS, no hay noción de tener un espacio diferente de etiquetas para niveles diferentes de jerarquía; cuando se interpreta una etiqueta, el nivel de la etiqueta es irrelevante.

La cuestión aparece cuando es posible para un enrutador LSR usar múltiples espacios de etiquetas por plataforma, o usar múltples espacios de etiquetas por interfase en la misma interfase. Esto no está prohibido en esta arquitectura. Sin embargo en estos casos el enrutador LSR debe tener algunos medios, no especificados por la arquitectura, para determinar para una determinada etiqueta de entrada, a que espacio de etiquetas pertenece esta etiqueta. Por ejemplo, para los casos en los que se utilice la encabezado genérico, se especifica que se usen distintos espacios de etiquetas para paquetes "unicast" y paquetes "multicast", y usa un punto de código a nivel de enlace de datos para distinguir los dos espacios de etiquetas [5].

5.3.1.3 Control de etiquetas independiente y ordenado

Un ruteador MPLS debe conocer las "reglas" para poder asignar o intercambiar etiquetas. Aun cuando los enrutadores convencionales suelen ser programados para determinar qué es lo que harán con un determinado paquete, es preferible contar con una **asignación dinámica** de reglas que permita mayor flexibilidad. Existen dos alternativas diferentes para hacer esta distribución. Cuando los enrutadores son capaces de "escuchar" estas reglas, crear una base de datos interna y distribuir esta información a otros enrutadores, sin necesidad de contar con un administrador de etiquetas previamente designado, el control del camino LSP se hace de manera **independiente**. La otra alternativa, preferida en MPLS, es el **control ordenado del camino LSP**. En este método de distribución, el LER de salida es, por lo regular, el encargado de la distribución de etiquetas, siendo este proceso en sentido contrario al direccionamiento de paquetes.

Algunas clases FEC corresponden a prefijos de dirección que son distribuidos vía un algoritmo de enrutamiento dinámico. El arranque de los caminos LSP para estas clase FEC se puede hacer de una de las dos maneras: control independiente del camino LSP o control ordenado del camino LSP.

Control independiente

Cuando un LSR reconoce una FEC realizará una asociación de forma independiente de una etiqueta a esa FEC. Una vez hecho esto informará de dicha asociación a los LSRs vecinos.

Esta es la forma de trabajar en el enrutamiento IP convencional: cada nodo toma una decisión independiente de cómo tratar cada paquete enruta los paquetes de forma independiente, apoyándose en que el algoritmo de enrutamiento converge rápidamente garantizando de esta forma que los datagramas son entregados de forma correcta.

Veamos las siguientes figuras como manera de ejemplo

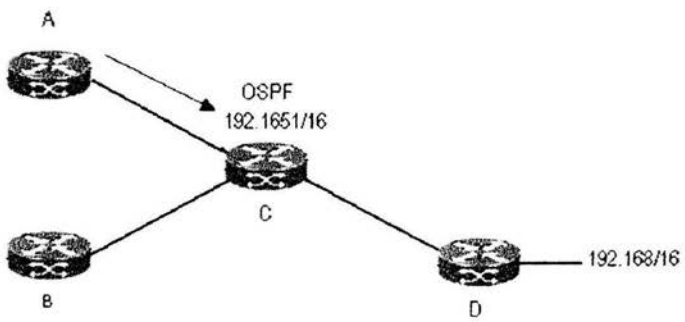


Figura 5.3.1.3.1 el LSR A utiliza OSPF para informarle al LSR C el prefijo de dirección 192.165/16

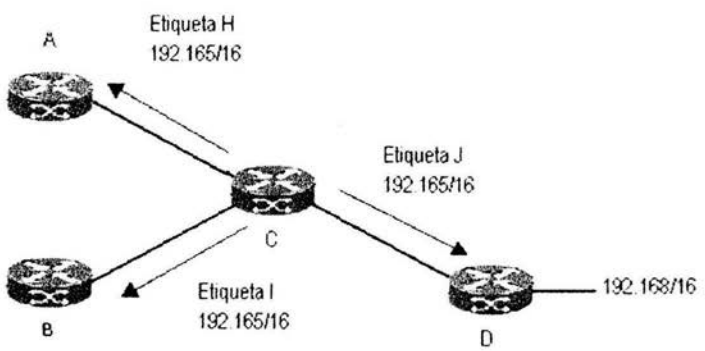


Figura 5.3.1.3.2. Cuando C recibe el prefijo, asigna de forma independiente una etiqueta a esta FEC e informa de dicha asociación a los LSRs vecinos.

Control ordenado

La asignación de etiquetas ocurre de forma ordenada desde un extremo del LSP hacia el otro. El establecimiento del LSP puede iniciarse por el LSR de entrada o por el LSR de salida del LSP.
Ejemplo: supongamos que el establecimiento del LSP lo inicia el LSR de salida, veamos las dos siguientes dos figuras.

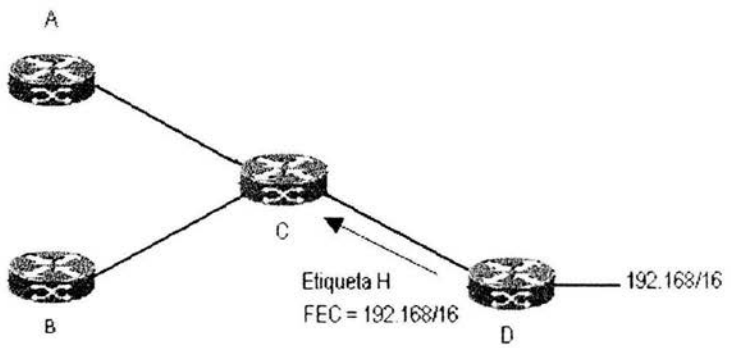


Figura 5.3.1.3.3. El nodo D se da cuenta que es el LSR de salida para el prefijo de dirección 192.168/16. Dicho nodo asigna una etiqueta a esta FEC e informa de dicha asociación a su vecino.

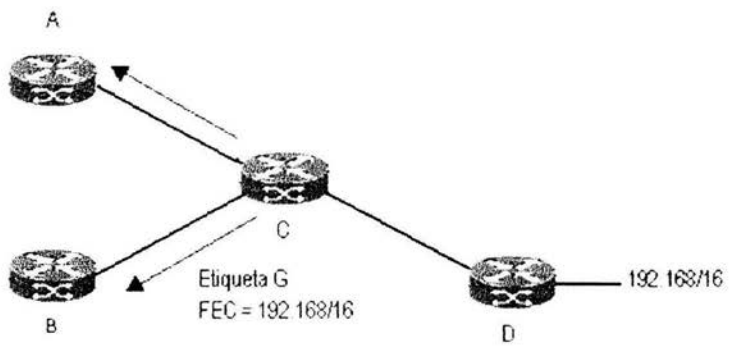


Figura 5.3.1.3.4. Cuando el LSR C recibe dicha información, asigna una etiqueta e informa de dicha asociación a sus LSRs vecinos. De esta forma, el establecimiento del LSP se hace de forma ordenada desde el LSR de salida al LSR de entrada.

Si se pretende garantizar que el tráfico de una FEC particular sigua un camino que tiene una serie de propiedades(p.e., que el tráfico no atraviese ningún nodo dos veces, que una cantidad especificada de recursos esté disponible al tráfico, que el tráfico siga un camino explícitamente especificado, etc.), se debe usar el control ordenado. Con el control independiente, algunos enrutadores LSR pueden empezar a etiquetar conmutando un tráfico de la clase FEC antes de que el camino LSP esté completamente en funcionamiento, y así algún tráfico de la clase FEC puede seguir un camino que no tiene el conjunto especificado de propiedades. El control ordenado también se debe usar si el reconocimiento de la clase FEC es una consecuencia del establecimiento del correspondiente camino LSP.

MPLS permite tanto el control independiente como el control ordenado. Un LSR sólo necesita implementar uno u otro.

Un inconveniente del control independiente ocurre cuando dos vecinos no están de acuerdo en las FECs que van a usar. Cuando esto ocurre algunas FECs no tendrán LSPs asociadas a ellas.

El control ordenado facilita la prevención de bucles. También permite a los administradores de la red controlar cómo se establecen los LSPs. Un inconveniente es que se tarda más tiempo en establecer un LSP que con el control independiente, debido a que las asociaciones deben propagarse a través de una región entera antes de que se establezca el LSP [4].

Si se quiere que el control ordenado sea efectivo, se deberá implementar en todos los LSRs.

5.3.1.4. Tráfico de salida no solicitada y Tráfico de salida por demanda

La distribución con control ordenado puede darse, a su vez, de dos maneras distintas.

Una alternativa consiste en distribuir las etiquetas sin que éstas sean solicitadas por otros enrutadores, desde el LER en el extremo de salida de la red y "empujándolas" hacia la entrada. Este método de distribución, conocido como **tráfico de salida no solicitada** (*downstream unsolicited*), puede hacerse cada determinado tiempo o cada vez que cambie la Base de Información de Etiquetas de un enruteador cualquiera.

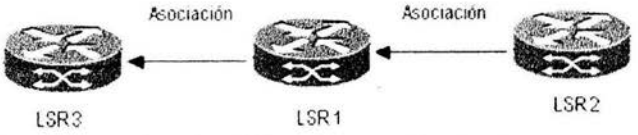


Figura 5.3.1.4.1. La Arquitectura MPLS permite a un LSR distribuir una etiqueta a otro LSR que no lo requiera explícitamente

La segunda opción, denominada **tráfico de salida por demanda** (**"*downstream on-demand*"**), requiere que un enrutador en particular solicite sus tablas, siendo estas posteriormente distribuidas por el LER de salida.

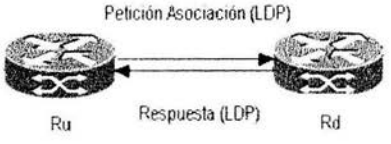


Figura 5.3.1.4.2. La Arquitectura MPLS permite a un LSR que solicite explícitamente a su siguiente salto una asociación de una etiqueta a una FEC

Se espera que algunas implementaciones MPLS solo proveerán distribución de etiquetas de solicitud de tráfico de salida bajo demanda y otras solo proveerán distribución de etiquetas de tráfico de salida sin solicitud y otras proveerán ambas. Estas tipos puede depender de las características de las interfaces que se soportan en una determinada implementación. Sin embargo ambas técnicas de distribución de etiquetas se pueden usar en la misma red y al mismo tiempo. En una distribución de etiquetas adyacente dada, el enrutador LSR posterior y el enrutador LSR anterior deben estar de acuerdo en que técnicas van a usar [5].

5.3.2. La pila de etiquetas

Hasta aquí hemos hablado de como se maneja un paquete etiquetado con una única etiqueta. En MPLS un paquete puede tener más de una etiqueta, organizadas éstas a modo de pila LIFO (Last-In, First-Out).. A esto se le conoce como pila de etiquetas.

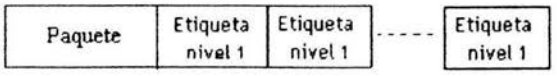


Figura 5.3.2.1 Esquema de una pila de etiquetas

Aunque MPLS soporte una jerarquía gracias a la pila de etiquetas, el procesamiento de un paquete etiquetado es completamente independiente del nivel de la jerarquía. Siempre que se procese una etiqueta, ésta será la de la cima, sin importar cuántas etiquetas pueda haber debajo.

Se puede considerar a un paquete no etiquetado como un paquete con una pila de etiquetas vacía.
Si la profundidad de la pila de etiquetas de un paquete es m, a la etiqueta que está al fondo de la pila se le llama etiqueta de nivel 1, a la que está encima etiqueta de nivel 2, y así sucesivamente [RFC3301].

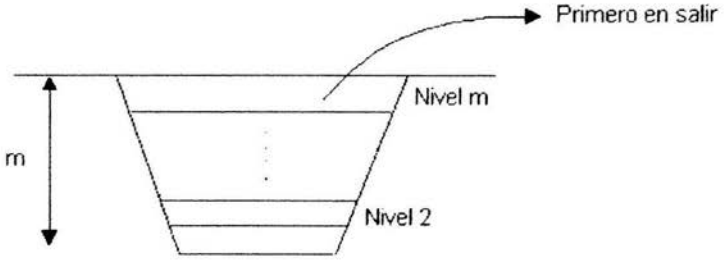


Figura 5.3.2.2. Niveles de una pila de etiquetas

5.3.2.1. Proceso de apilamiento

En la siguiente figura tenemos tres dominios. Supongamos que el dominio 2 es un dominio de tránsito. En dicho dominio no se originan paquetes. Tampoco hay paquetes destinados a él. Para anunciar las direcciones del dominio 3 el LSR F le distribuye la información al LSR E. El LSR E le distribuye la información al LSR B el cual se la distribuye al LSR A. No se distribuye la información a los LSRs C y D porque son LSRs intermedios.

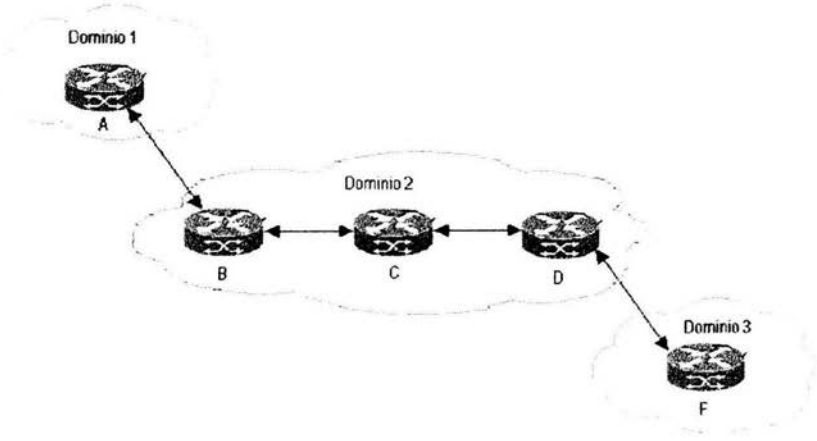


Figura 5.3.2.1.1. Distribución de la información para diferentes dominios MPLS

Se usan dos niveles de etiquetas. Cuando el tráfico entra en el segundo dominio se apila una nueva etiqueta en la cima de la pila, por lo que las etiquetas que hubiera en la pila descienden un nivel.

Veamos como ejemplo la figura 5.2.1.5.4. para entender mejor el proceso de apilamiento

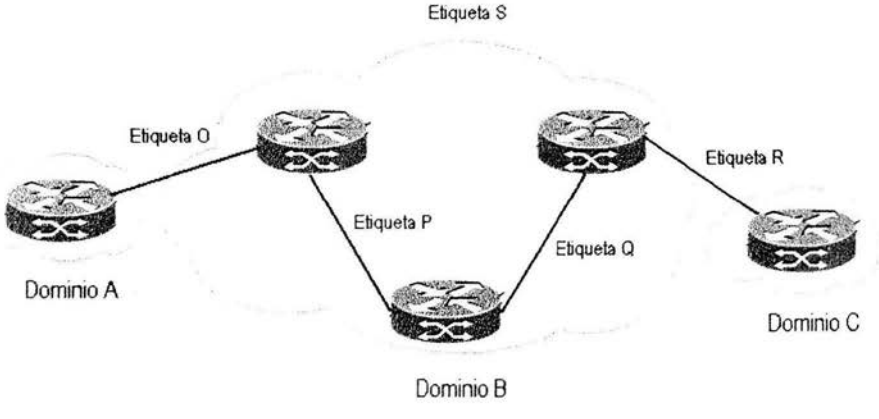


Figura 5.2.2.1.2

Conmutación de etiquetas:

- La secuencia de etiquetas entre dominios es: O, S, R
- La secuencia de etiquetas dentro del dominio B es: P, Q

Las operaciones que se realizarán son:

1. Del dominio A al B el paquete llevará la etiqueta O
2. En el enrutador de entrada al dominio B se intercambiará la etiqueta O por la S, que identifica al nuevo dominio, y apila la etiqueta P que indica el siguiente salto en esa red.
3. En el siguiente enrutador se intercambiará la etiqueta P por la Q.
4. En el enrutador de salida se desapila Q y ve que la etiqueta de entrada que tiene es S, e intercambia ésta con R para llegar al siguiente dominio.

Camino de conmutación de etiquetas (LSP): reglas de apilamiento

Un LSP de nivel m para un paquete P es una secuencia de enrutadores <R1,...,Rn> con las siguientes propiedades [RFC3301]:

- R1, el LSR de entrada, es un LSR que apila una etiqueta en la pila de etiquetas de P, resultando una pila de etiquetas de profundidad m.
- Para todo i, 1<i<n , P tendrá una pila de etiquetas de profundidad m cuando lo reciba el LSR Ri. Mientras P se encuentre entre R1 y Rn-1 su pila de etiquetas nunca tendrá una profundidad menor que m.
- Para todo i, 1<i<n: P es transmitido desde Ri hasta Ri+1 por medio de MPLS, por ejemplo usando la etiqueta de la cima de la pila como índice de una ILM (*Incoming Label Map*).
- Para todo i, 1<i<n: si un sistema S recibe y reenvía P después de que P sea transmitido por Ri pero antes de que P sea recibido por Ri+1 (por ejemplo, Ri y Ri+1 pueden estar conectados vía una subred conmutada de enlace de datos, y S puede ser un conmutador de enlace de datos), entonces la decisión del reenvío de S no está basado en la etiqueta de nivel m, o en la cabecera del nivel de red. Esto puede ser debido a que:

a. La decisión no se basa en absoluto en la pila de etiquetas o en la cabecera del nivel de red.
b. La decisión se basa en una pila de etiquetas en la que se han apilado etiquetas adicionales (ejemplo: en un nivel de etiquetas m+k con k>0).

Una consecuencia (o quizás una presuposición) de esto es que cuando un enrutador LSR pone una etiqueta en un paquete que ya está etiquetado, necesita asegurarse de que la nueva etiqueta corresponde a la clase FEC de cuyo enrutador de salida del camino LSP es el enrutador LSR que asignó la etiqueta que es ahora segunda en la pila.

Diremos que una secuencia de enrutadores LSR es un camino LSP para una determinada clase FEC F si es un camino LSP de nivel m para un determinado paquete P cuando la etiqueta de nivel m del paquete P es una etiqueta que corresponde a la clase FEC F.

Consideremos el conjunto de nodos que pueden ser nodos enrutadores de entrada de un camino LSP para la clase FEC F. Entonces hay un camino LSP para la clase FEC F que empieza con cada uno de estos nodos. Si varios de estos caminos LSP tiene el mismo enrutador de salida del camino LSP, entonces se puede considerar que el conjunto de estos caminos LSP es un árbol, cuya raíz es el enrutador de salida del camino LSP. (ya que los datos viajan a lo largo de este árbol hacia la raíz, se puede decir que es un árbol multipunto-a-punto.) Así podemos hablar del "árbol LSP" para una deterinada clase FEC F.

Extracción en el penúltimo salto

Si <R1,...,Rn> es un LSP de nivel m para el paquete P, P puede ser transmitido desde Rn-1 a Rn con una pila de etiquetas de profundidad m-1. Se puede extraer de la pila de etiquetas en el penúltimo LSR del LSP, en vez de en el LSP de salida [RFC3301].
Desde una perspectiva arquitectónica, esto es apropiado. El propósito de la etiqueta de nivel m es hacer llegar el paquete a Rn. Una vez que Rn-1 ha decidido mandar el paquete a Rn, la etiqueta ya no tiene ninguna funcionalidad y por tanto no es necesario transportarla.

La extracción en el penúltimo salto tiene una ventaja: si no se hace, cuando el LSP de salida reciba el paquete, éste mirará la etiqueta de la cima de la pila y determinará que es el LSP de salida. Entonces

deberá hacer una extracción de la pila y examinar lo que quede del paquete. Si hubiera otra etiqueta en la pila, el LSP de salida miraría esta etiqueta y reenviaría el paquete basándose en la información que ha obtenido. En este caso, el LSP de salida para el paquete del LSP de nivel m es también un nodo intermedio para un LSP de nivel m-1. Si no hubiera etiquetas en la pila, entonces se reenviaría el paquete utilizando la dirección de destino del nivel de red. Esto obliga a que el LSR de salida haga dos consultas: bien dos consultas de etiquetas o una consulta de etiqueta seguido de una consulta de dirección [6].

Con esta técnica, el LSR de salida sólo tiene que hacer una consulta y requiere que el penúltimo nodo haga una consulta.

La creación del "camino rápido" del reenvío en un producto de conmutación de etiquetas puede ser muy favorecedor si se sabe que sólo requerirá una consulta:

- Se puede simplificar el código si se asume que sólo se necesitará una consulta.
- Se puede basar el código en un "presupuesto de tiempo" que asuma que sólo se necesitará una consulta.

De hecho, cuando se usa la extracción en el penúltimo salto, el LSP de salida puede incluso no ser un LSR.

No obstante, algunos motores hardware de conmutación pueden no ser capaces de extraer de la pila de etiquetas, por lo que esto no puede ser requerido universalmente.

También pueden haber situaciones en las que no es deseable la extracción en el penúltimo salto. Por tanto, el penúltimo nodo extraerá la etiqueta de la pila de etiquetas si el LSR de salida se lo pide explícitamente, o si el siguiente nodo en el LSP no soporta MPLS. Si el siguiente nodo en el LSP no soporta MPLS, y no hace tal petición, el penúltimo nodo no tendrá manera de saber que es el penúltimo nodo.

Un LSR que es capaz de extraer de la pila de etiquetas deberá realizar la extracción en el penúltimo salto cuando se lo pida el LSR del mismo nivel (su "igual" o peer) que está en de tráfico de salida (dowstream)

Las negociaciones iniciales del protocolo de distribución de etiquetas deben permitir a cada LSR determinar si sus LSRs vecinos son capaces de extraer de la pila de etiquetas. Un LSR no le debe pedir

a su "igual" de distribución de etiquetas que extraiga de la pila de etiquetas a no ser que sea capaz de hacerlo.

Un nodo de salida siempre podrá interpretar la etiqueta de la cima de un paquete recibido cuando se utiliza la extracción en el penúltimo salto si se cumplen las reglas de alcance y unicidad expuestas en el apartado anterior.

En el gráfico de la figura se puede apreciar que el LSR F realiza una doble consulta, lo que repercute en el rendimiento de dicho nodo. Para mejorar el rendimiento se usa la extracción en el penúltimo salto.

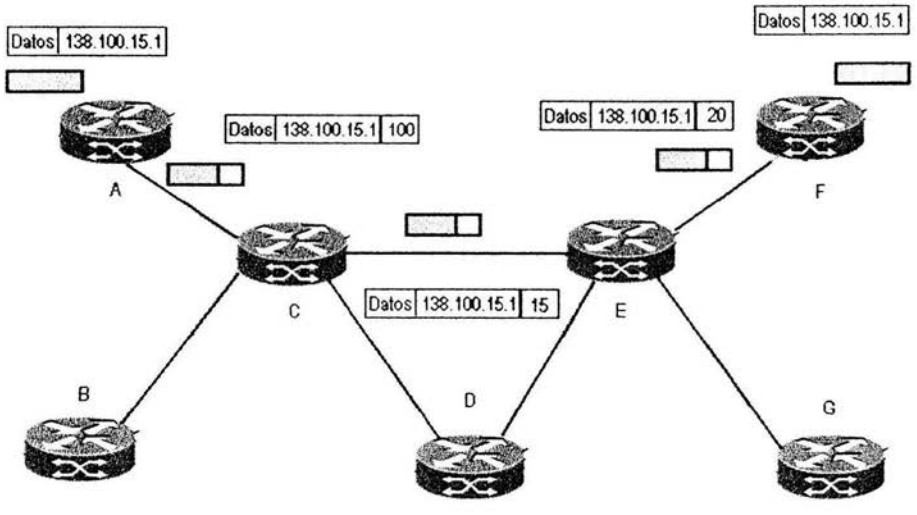


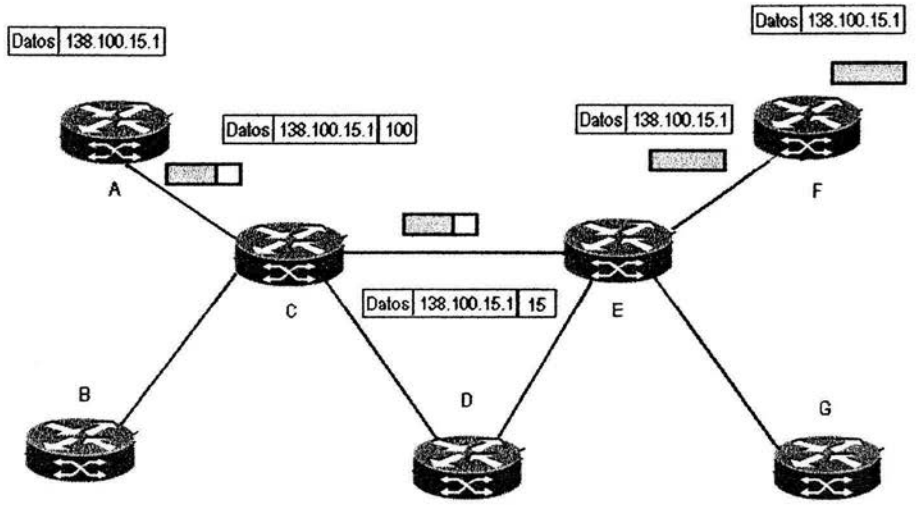
Figura 5.3.2.1.3. Ejemplo: doble consulta en el LSR F

Pasos:

- Primero: llega un paquete IP al LSR A (LER de entrada).
- Segundo: el LSR A etiqueta el paquete y se lo reenvía al LSR C (LSR intermedio).
- Tercero: el LSR C realiza una búsqueda en la tabla, intercambia la etiqueta y reenvía el paquete al LSR E (LSR intermedio).
- Cuarto: el LSR E realiza una búsqueda en la tabla, intercambia la etiqueta y reenvía el paquete la LSR F.

- Quinto: el LSR F realiza una búsqueda en la tabla, extrae la etiqueta, realiza una búsqueda de nivel 3 y reenvía el paquete hacia un enrutador externo.

En la siguiente figura podemos apreciar que el LSR F realiza una consulta menos que en el caso anterior.



5.3.2.1.4.Figura Ejemplo: extracción en el penúltimo salto

Pasos

- Primero: llega un paquete IP al LSR A (LER de entrada).
- Segundo: el LSR A etiqueta el paquete y se lo reenvía al LSR C (LSR intermedio).
- Tercero: el LSR C realiza una búsqueda en la tabla, intercambia la etiqueta y reenvía el paquete al LSR E (LSR intermedio).
- Cuarto: el LSR E realiza una búsqueda en la tabla, extrae la etiqueta y reenvía un paquete IP puro al LSR F.
- Quinto: El LSR F realiza únicamente una búsqueda de nivel 3 y reenvía el paquete hacia un enrutador externo.

5.3.3. Formación de túneles

A veces un enrutador Ru toma una acción explícita para hacer que un determinado paquete sea entregado a otro enrutador Rd, aunque Ru y Rd no sean enrutadores consecutivos en el camino salto a salto para este paquete, y el enrutador Rd no sea el último destino del paquete. Por ejemplo, esto se puede hacer por encapsulación del paquete dentro de un paquete de nivel de red cuya dirección destino es la dirección del enrutador Rd. Esto crea un túnel del enrutador Ru al enrutador Rd.

Cualquier paquete manejado de esta forma diremos que es un paquete tunelado.

En cada enrutador se realiza la siguiente operación

Interfaz de entrada	Etiqueta	Interfaz de salida	Etiqueta
i 1	200	04	18

Tabla 5.3.3.1. Operaciones que realiza cada LSR

De esta forma se construye para cada FEC un túnel llamado LSP (*Label switched Path*)

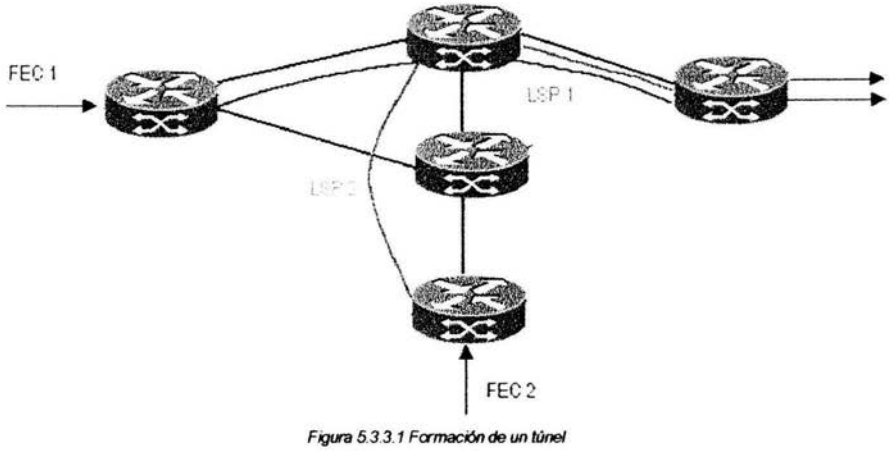


Figura 5.3.3.1 Formación de un túnel

Túnel Enrutado Salto a Salto

Si un paquete tunelado sigue el camino salto a salto del enrutador Ru al enrutador Rd, diremos que es un "Túnel Enrutado Salto a Salto" cuyo extremo de transmisión es el enrutador Ru y cuyo extremo de recepción es el enrutador Rd.

Túnel Enrutado Explícito

Si un paquete tunelado viaja del enrutador Ru al enrutador Rd por un camino diferente del camino salto a salto, diremos que es un "Túnel Enrutado Explícito" cuyo extremo de transmisión es el enrutador Ru y cuyo extremo de recepción es el enrutador Rd. Por ejemplo, podemos enviar un paquete a través de un Túnel Enrutado Explícito encapsulándolo en un paquete que es enrutado en origen.

5.3.3.1 Jerarquía: Túneles LSP dentro de caminos LSP

Ocurre cuando se crea un nuevo LSP dentro de un túnel de un LSP de orden superior ya existente. En el siguiente ejemplo se muestra cómo los LSPs de orden inferior disparan la formación de un LSP de orden superior. Los nodos en el borde de dos regiones con respecto a las características de multiplexado, son los responsables de la agregación de los LSPs.

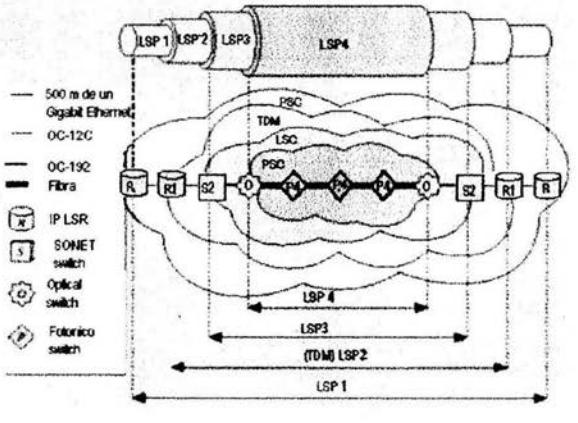


Figura 5.3.3.1.1. Túneles LSP dentro de caminos LSP

- R0, R1, R9 y R10 manejan paquetes.
- S0 y S8 son conmutadores SONET/SDH.
- O3 y O7 son conmutadores electro-ópticos.
- P4, P5 y P6 son conmutadores ópticos.
- Entre R0-R1 y R9-R10 hay enlaces de 500 Mbps.
- Entre R1-S2 y S8-R9 hay un enlace de OC-12 (mayor capacidad que el anterior).
- Entre S2-O3 y O7-S8 hay un enlace de OC-192 (mayor capacidad que el anterior).
- Entre O3-O7 hay un enlace de fibra.
- LSP1 está configurado de R0 a R10 con ancho de banda de 500 Mbps.
- LSP1 está anidado dentro de LSP2,3,4 que son LSPs de orden superior.

Los nodos en el borde de dos regiones con respecto a las características de multiplexado, son responsables de la formación de LSPs de orden superior o de agregar los LSPs de nivel inferior

La siguiente figura muestra el proceso de formación del LSP.

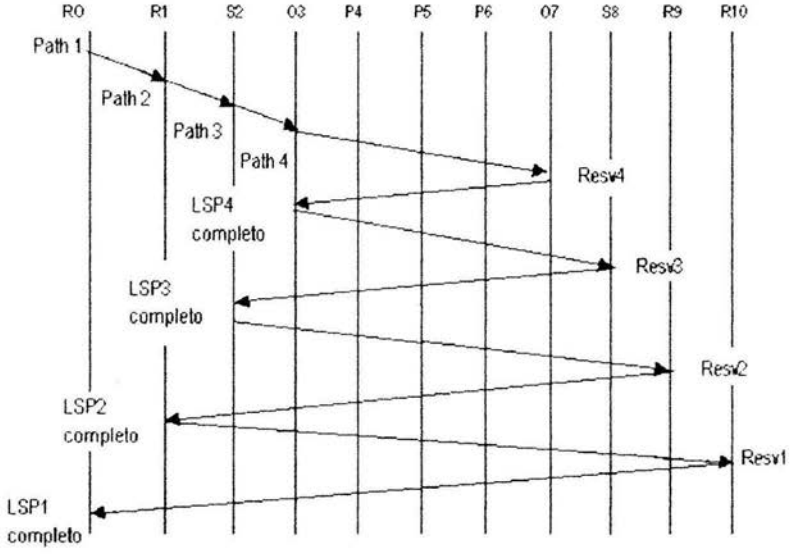


Figura 5.3.3.1.2 Formación de LSP s

La formación del LSP1 dispara la formación de los LSPs 2, 3 y 4. R0 manda una petición de camino (Path) a R1. La llegada de dicha petición a R1 dispara la formación del LSP1 de R1 a R9 y así sucesivamente hasta que se dispare la formación del LSP4 en O3. Una vez establecido el LSP4, el mensaje tercero de Path se manda a través del LSP4 (o sea, por el túnel) . Este proceso continua hasta que se cree el primer LSP y se forme la jerarquía [7].

Ahora veamos otro ejemplo para entender mas afondo la jerarquía de los túneles en MPLS

Consideremos un camino LSP formado por los enrutadores <R1, R2, R3 >. Supongamos que el enrutador R1 recibe un paquete P sin etiqueta, y pone en la pila de etiquetas la etiqueta necesaria para que siga este camino, y que de hecho es un camino salto a salto. Sin embargo supongamos además que los enrutadores R2 y R3 no están directamente conectados, pero que son "vecinos" dado que son extremos de un túnel LSP. Así la secuencia actual de enrutadores LSR atravesados por el paquete P es <LSR1 LSRa LSRb LSRc LSR2 LSR3 >

Cuando el paquete P viaja del enrutador R1 al enrutador R2, tendrá una pila de etiquetas de profundidad 2. El enrutador R1, conmutando con esta etiqueta, determina que el paquete P debe entrar en el túnel. Primero el enrutador R1 reemplaza la etiqueta de entrada con una etiqueta que sea entendida por el enrutador R2. Entonces pone una nueva etiqueta. Esta

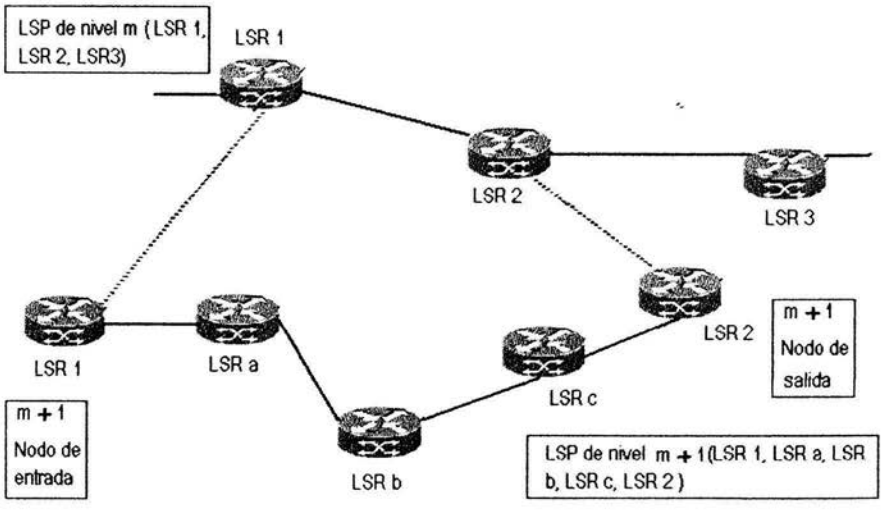


Figura 5.3.3.1.3 Jerarquía MPLS

etiqueta de nivel 2 tiene un valor que es significativo para el enrutador Ra. Se ha hecho conmutación en la etiqueta de nivel 2 por los enrutadores Ra, Rb, Rc., que es el penúltimo salto en el túnel R1-R2, poniendo la pila de etiquetas como antes de enviar el paquete P al enrutador R2. Cuando el enrutador R2 ve el paquete P, éste tiene solamente una etiqueta de nivel 1, habiendo salido ahora del túnel. Dado que el enrutador R2 es el penúltimo salto en el nivel 1 del camino LSP del paquete P, pone la pila de etiquetas, y el enrutador R3 recibe un paquete P sin etiquetas.

El mecanismo de pila de etiquetas permite que el túnel LSP las anide a cualquier profundidad.

5.3.4. Conmutadores ATM como LSRs

Como se mencionó en el capítulo introductorio, se pueden utilizar conmutadores ATM como LSRs si se les dota del software adecuado. Los conmutadores ATM utilizan el puerto de entrada y el valor del campo VPI/VCI como índice de la tabla de donde obtienen el puerto de salida y el valor de salida del campo VPI/VCI. Por tanto, si se codifica el valor de la etiqueta en estos campos se podrán utilizar estos conmutadores como LSRs. Nos referiremos a estos dispositivos como "ATM-LSRs". Por lo que trasmite paquetes etiquetados como celdas ATM, como se muestra en la figura siguiente.

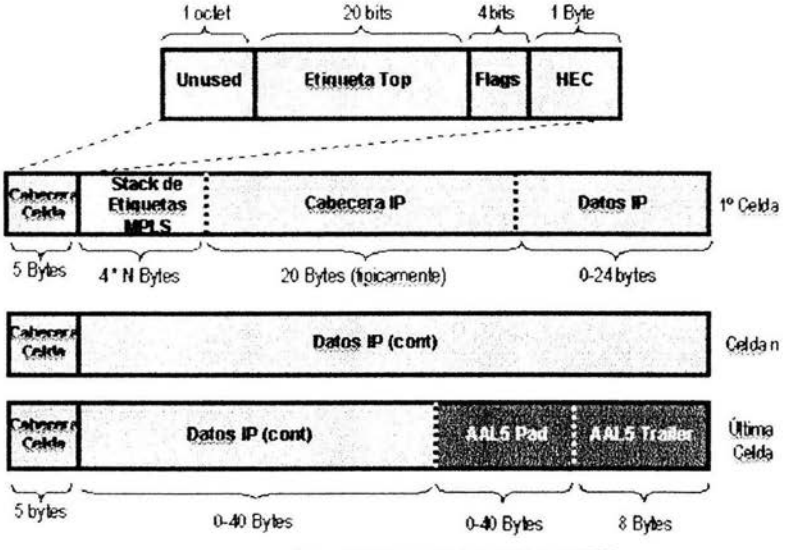


Figura 5.3.4.1 Conmutadores ATM como LSR

5.3.4.1. Codificación de Etiquetas

Con el fin de transmitir una pila de etiquetas junto con el paquete, es necesario definir una codificación concreta de la pila de etiquetas. La arquitectura soporta distintas técnicas de codificación; la elección de la técnica de codificación depende de la clase particular de dispositivo que se use para enviar los paquetes etiquetados.

Hay tres maneras obvias de codificar las etiquetas en la cabecera de una celda ATM (presuponiendo el uso de AAL5):

1. **Codificación SVC**

Usar el campo VPI/VCI para codificar la etiqueta que está en la parte superior de la pila de etiquetas. Esta técnica se puede usar en cualquier red. Con esta técnica de codificación, cada camino LSP funciona como un SVC de ATM, y el protocolo de distribución de etiquetas es el protocolo de "señalización" de ATM. Con esta técnica de codificación, el enrutador ATM-LSR no puede realizar operaciones de poner ni sacar etiquetas de la pila de etiquetas.

2. **Codificación SVP**

Usar el campo VPI para codificar la etiqueta que está en la parte superior de la pila de etiquetas, y el campo VCI para codificar la segunda etiqueta de la pila, si existe. Esta técnica tiene algunas ventajas sobre la anterior, en que permite el uso de ATM con conmutación VP. Eso es, los caminos LSP funcionan como SVPs de ATM, con el protocolo de distribución de etiquetas funcionando como el protocolo de señalización ATM.

Sin embargo esta técnica no se puede usar siempre. Si la red incluye un "Virtual Path" de ATM a través de una red ATM sin MPLS, entonces el campo VPI no es necesariamente útil para usarlo por MPLS.

Cuando se usa esta técnica de codificación, el enrutador ATM-LSR a la salida del VP efectivamente hace una operación de sacar la etiqueta.

3. Codificación Multipunto SVP

Usar el campo VPI para codificar la etiqueta que está en la parte superior de la pila de etiquetas, usar parte del campo VCI para codificar la segunda etiqueta de la pila, si existe, y usar el resto del campo VCI para identificar el enrutador de entrada del camino LSP. Si se usa esta técnica, las capacidades convencionales de la conmutación VP ATM se pueden usar para suministrar VPs multipunto-a-punto. Entonces las celdas de diferentes paquetes transportarán diferentes valores VCI.

Como veremos en el capítulo 5.3.9. , esto nos permite hacer fusión de etiquetas, sin correr en problemas de superposición de celdas, en los conmutadores ATM que pueden suministrar VPs multipunto-a-punto, pero que no tienen capacidad de fusión de VCs.

Esta técnica depende de la existencia de una capacidad para asignar los valores VCI de 16-bit a cada conmutador ATM de forma que solo se asigne un valor único VCI a dos conmutadores diferentes. Si un número adecuado de tales valores se puede asignar a cada conmutador, sería posible también tratar el valor VCI como la segunda etiqueta de la pila.

Si hay más etiquetas en la pila que pueden ser codificadas en la cabecera ATM, las codificaciones ATM deben ser combinadas con el encabezado genérico.

Interoperabilidad entre Técnicas de Codificación

Si el camino de enrutadores <R1, R2, R3> es un camino LSP, es posible que el enrutador R1 usará una codificación de la pila de etiquetas cuando transmita el paquete P al enrutador R2, pero que el enrutador R2 usará una codificación distinta cuando transmita un paquete P al enrutador R3.

En general, la arquitectura MPLS soporta caminos LSP con diferentes codificaciones de la pila de etiquetas usadas en diferentes saltos. Por tanto cuando discutimos los procedimientos para procesar un paquete etiquetado, hablamos en términos abstractos de operar en la pila de etiquetas del paquete.

Cuando se recibe un paquete etiquetado, el enrutador LSR debe decodificarlo para determinar el valor actual de la pila de etiquetas, entonces debe operar en la pila de etiquetas para determinar el nuevo valor de la pila, y entonces codificar el nuevo valor apropiadamente antes de transmitir el paquete etiquetado al salto siguiente.

Desafortunadamente, los conmutadores ATM no tiene capacidad para traducir de una técnica de codificación a otra. La arquitectura MPLS por tanto requiere que a ser posible, para dos conmutadores

ATM que estén en sucesivos enrutadores LSR a lo largo de un nivel m de un camino LSP para el mismo paquete, que se use la misma técnica de codificación en los conmutadores ATM.

Naturalmente habrá redes MPLS que contienen una combinación de conmutadores ATM operando como enrutadores LSR, y otros enrutadores LSR que operan usándole encabezado genérico MPLS.

Cuando exista una combinación de LSRs ATM y LSRs que utilicen el encabezado genérico MPLS, deberán existir LSRs con interfaces ATM e interfaces genérico MPLS. De esa forma el LSR podrá hacer una traducción de un tipo de codificación a otro.

Valores reservados de etiquetas

- 0: representa la "etiqueta explícita nula (NULL) IPv4". Esta etiqueta se podrá encontrar en el caso de que sea la única entrada en la pila de etiquetas e indica que debe ser extraída de la pila de etiquetas y reenviado el paquete basándose en la cabecera del paquete IPv4.
- 1: representa la "etiqueta de alerta del enrutador". Esta etiqueta no puede estar en el último lugar de la pila.
- 2: representa la "etiqueta explícita nula IPv6". Es igual que el primer paso excepto que se reenvía el paquete basándose en la cabecera IPv6.
- 3: representa la "etiqueta implícita nula" [9].

5.3.5. Componentes de un LSR

5.3.5.1. FIB

Los LERs utilizan diferentes métodos para etiquetar el tráfico. Bajo el esquema más simple, los paquetes IP son ligados a una etiqueta y a un FEC utilizando tablas preprogramadas. Cuando los paquetes abandonan el LER e ingresan al LSR correspondiente, la etiqueta MPLS es examinada y comparada contra una tabla de conectividad conocida como LIB (*Forwarding Information Base*), *Base de información del reenvío*, para determinar la acción a seguir. El intercambio de instrucciones se llevará a

cabo dependiendo de las instrucciones del LIB. Debe señalarse que las etiquetas poseen únicamente un significado local dentro del enrutador correspondiente [10].

La FIB se compone de :

NHLFE(*Next Hop Label Forwarding Entry*)

5.3.5.2. NHLFE

El NHLFE (*Next Hop Label Forwarding Entry*) es la entrada de la etiqueta a usar para el próximo salto. Se usa cuando se envía un paquete etiquetado. Contiene la información siguiente:

1. El próximo salto del paquete

2. La operación a realizar en la pila de etiquetas del paquete; este es una de las operaciones siguientes:

a) Sustituir la etiqueta en la parte superior de la pila con una etiqueta nueva específica
b) Sacar una etiqueta de la pila
c) Sustituir la etiqueta de la parte superior de la pila con una etiqueta nueva específica, y entonces poner una o más etiquetas nuevas específicas en la pila de etiquetas.

También puede contener:

d) La encapsulación del enlace de datos a usar cuando se transmite el paquete
e) La forma de codificar la pila de etiquetas cuando se transmite el paquete
f) Cualquier otra información necesaria con el fin de disponer de forma adecuada el paquete.

Notar que en un enrutador LSR dado, el próximo salto del paquete puede ser el mismo enrutador LSR. En este caso, el enrutador LSR necesitaría sacar la etiqueta de más arriba, y entonces enviarse a él mismo el paquete resultante. Entonces tomaría otra decisión de envío, basada en lo que resta después de que la etiqueta guardada sea sacada. El resultado o puede ser un paquete etiquetado si había más de una etiqueta en la pila, o puede ser el paquete IP nativo sin etiqueta si solo había una.

Esto implica que en algunos casos el enrutador LSR puede necesitar operar en la cabecera IP con el fin de enviar el paquete.

Si el próximo salto del paquete es el enrutador LSR actual, entonces la operación de la pila de etiquetas debe ser sacar de la pila[11].

5.3.5.3. ILM

El ILM (*Incoming Label Map*) mapea o correlaciona cada etiqueta de entrada a un conjunto de NHLFEs.

Se utiliza cuando se reenvían paquetes que llegan como paquetes etiquetados. Si la ILM correlaciona una etiqueta particular con un conjunto de NHLFEs que contienen más de un elemento, se deberá elegir exactamente un elemento del conjunto antes de reenviar el paquete. La etiqueta de la cima de la pila se utiliza como índice de la ILM. Puede ser útil hacer que la ILM correlacione una etiqueta con un conjunto que contenga más de una NHLFE por si, por ejemplo, se desea hacer un balance de la carga de tráfico a través de múltiples enlaces.

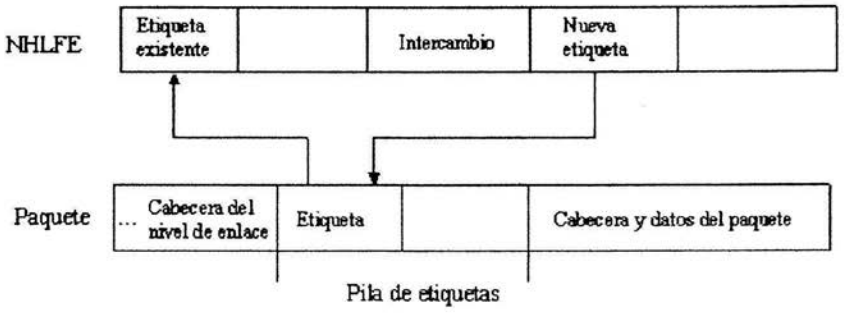


Figura 5.3.5.3.1. ILM para el reenvío a otro usuario de paquetes que llegan etiquetados

5.3.5.4. FTN

El FTN (*FEC-to-NHLFE*) mapea o mejor dicho correlaciona cada clase FEC a un conjunto de NHLFEs. Se usa cuando los paquetes enviados que llegan no tienen etiqueta, pero que son etiquetados antes de ser enviados [12].

Si el mapeo FTN mapea una etiqueta concreta a un conjunto de NHLFEs que contiene más de un elemento, exactamente un elemento de este conjunto debe ser elegido antes de enviar el paquete.

Teniendo el mapeo FTN que correlaciona una etiqueta al conjunto que contiene más de un NHLFE, puede ser útil si, p.e., se desea hacer balanceo de cargas sobre múltiples caminos de igual coste.

Módulo de determinación de la ruta

En el capítulo 5.1.1. a este módulo lo llamamos componente de control.

Este módulo construye las entradas de la FIB en una operación MPLS. Con la información de los protocolos de enrutamiento se determinan las FECs para las que se quieren crear NHLFEs. También se obtiene la información del siguiente salto que se necesita para crear la NHLFE.
Dado que en MPLS sólo se permite la asociación de etiquetas por el LSR de tráfico de salida (Rd) , una NHLFE no tendrá información de la etiqueta de salida hasta que Rd del mismo nivel le asigne una etiqueta.
Un LSR puede construir las NHLFEs de dos formas [RFC3301]:

1. Asignando una o más etiquetas para usar como la etiqueta de entrada, creando ILMs para cada una, asociando cada ILM a un conjunto de NHLFEs y distribuyendo las etiquetas asociadas a los LSRs de tráfico de entrada (Ru).
2. Creando FTNs para las FECs asociadas con entradas específicas de enrutamiento y asociando cada una a un conjunto de NHLFEs con la información del siguiente salto.

La función de determinación de la ruta se usa también para borrar o actualizar las entradas de la FIB cuando las rutas asociadas a una FEC son removidas o cuando cambia la información del siguiente salto.

Módulo de reenvío

La función de reenvío se basa en la comparación exacta entre una etiqueta y la ILM, que a su vez se correlaciona con una NHLFE. El LSR seguirá las instrucciones de manipulación de la etiqueta que indique la NHLFE y enviará el paquete por la interfaz especificada en la información del siguiente salto. Puede ser que el LSR necesite usar la información de encapsulación de nivel de enlace especificada en la NHLFE para encapsular el paquete antes de enviarlo al siguiente salto. Ejemplo de esto último sería un enlace Ethernet, en donde la dirección MAC (*Media Access Control*) de la interfaz de salida y el siguiente salto se tienen que incluir en la encapsulación Ethernet para poder entregar el paquete al siguiente salto.

5.3.6. Intercambio de etiquetas

El intercambio de etiquetas es el uso de los procedimientos siguientes para enviar un paquete.
Con el fin de enviar un paquete etiquetado, un enrutador LSR examina la etiqueta de la parte superior de la pila de etiquetas. Usa el mapeo ILM para mapear esta etiqueta a un NHLFE. Usando la información del NHLFE, determina a donde enviar el paquete, y realiza una operación en la pila de etiquetas del paquete. Entonces codifica la nueva pila de etiquetas en el paquete, y envía el resultado.

Con el fin de enviar un paquete sin etiquetar, un enrutador LSR analiza la cabecera de nivel de red para determinar la clase FEC del paquete. Entonces usa el mapeo FTN para mapear ésta a un NHLFE. Usando la información del NHLFE, determina a donde enviar el paquete, y realiza una operación en la pila de etiquetas del paquete. Por supuesto sacando de la pila de etiquetas sería ilegal en este caso. Entonces codifica la nueva pila de etiquetas en el paquete, y envía el resultado.

Es importante notar que cuando hay un intercambio de etiquetas, el salto siguiente siempre es tomado del NHLFE.; en algunos casos esto puede ser diferente de lo que el salto siguiente sería si no se usara el MPLS.

Por lo que el intercambio de etiquetas se considera para dos casos [RFC3301]:

- Si se quiere reenviar un paquete etiquetado, el LSR examinará la etiqueta de la cima de la pila de etiquetas. Con dicha etiqueta, escogerá una ILM y obtendrá la NHLFE. Con la NHLFE obtendrá la nueva etiqueta y la información necesaria para reenviar el paquete.
- Si se quiere reenviar un paquete no etiquetado, el LSR examinará la dirección del nivel de red para determinar la FEC a la que pertenece el paquete. Una vez hecho esto, usará la FTN para correlacionar la FEC con una NHLFE. Con la NHLFE sabrá dónde reenviar el paquete y realizará una operación en la pila de etiquetas del paquete.

En ambos casos, el LSR codificará la nueva pila de etiquetas en el paquete y lo reenviará a otro salto [13]

.

Salto Siguiente del camino LSP

El Salto Siguiente del camino LSP para un determinado paquete etiquetado en un determinado enrutador LSR es el enrutador LSR que es el salto siguiente, como seleccionado por la entrada NHLFE usada para enviar este paquete.

El Salto Siguiente del camino LSP para una determinada clase FEC es el salto siguiente seleccionado por la entrada NHLFE indexada por una etiqueta que corresponde a esta clase FEC.

Notemos que el Salto Siguiente del camino LSP puede diferir del salto siguiente que elegiría el algoritmo de enrutamiento del nivel de red.

5.3.7. Etiquetas de entrada inválidas: formación de un bucle

¿ Qué haría un enrutador LSR si recibe un paquete etiquetado con una determinada etiqueta de entrada, y no tiene ligadura para esta etiqueta? Pensará que las etiquetas han sido removidas, y el paquete se enviará como paquete IP sin etiqueta. Sin embargo, en algunos casos, haciendo esto causaría un bucle. Si el enrutador Ru piensa que la etiqueta está ligada a una ruta explícita, y el enrutador Rd no piensa que la etiqueta está ligada a algo, y si el enrutamiento salto a salto de un paquete IP no etiquetado devuelve el paquete al enrutador Ru , ya tenemos el bucle.

También es posible que la etiqueta estaba deseando representar una ruta que no puede ser deducida de la cabecera IP.

Por lo tanto, cuando un paquete etiquetado es recibido con una etiqueta inválida de entrada, debe ser descartada, a menos que se determine de alguna forma que enviarlo sin etiquetar no puede causar ningún daño.

Carencia de Etiqueta de Salida

Cuando un paquete etiquetado está viajando a lo largo de un camino LSP, puede suceder ocasionalmente que alcance un enrutador LSR en el que el mapeo ILM no mapee la etiqueta de entrada del paquete en un NHLFE, aunque la etiqueta de entrada sea válida por si. Esto puede suceder debido a las condiciones transitorias, o debido a un error en el enrutador LSR que sería el próximo salto del paquete.

En tales casos se está induciendo a vaciar la pila de etiquetas e intentar enviar el paquete más bien vía el envío convencional, basado en la cabecera del nivel de red. Sin embargo en general esto no es un procedimiento seguro:

- Si el paquete ha estado siguiendo un camino LSP enrutado explícitamente, puede resultar un bucle.

- La cabecera de red del paquete puede no contener suficiente información para que determinado enrutador LSR pueda enviarlo correctamente.

A menos que pueda ser determinado, que ninguna de estas situaciones ocurre, el único procedimiento seguro es descartar el paquete.

5.3.7.1. Tiempo de Vida (TTL)

En el envío convencional IP, cada paquete transporta un "Tiempo de Vida" (TTL) en su cabecera.

Cada vez que un paquete pasa a través de un enrutador, su TTL se decrementa en 1; si el TTL llega a valer 0 antes de que el paquete haya llegado al destino, el paquete es descartado.

Esto suministra un nivel de protección contra los bucles de envío que puedan existir debido a malas configuraciones, o debido a un fallo o a una convergencia lenta del algoritmo de enrutamiento. Esto implica que hay dos asuntos relacionados con el TTL que el MPLS necesita negociar con: (i) el TTL es una forma de suprimir los bucles; (ii) el TTL es una forma de conseguir otras funciones, tales como limitar el objetivo de un paquete.

Cuando un paquete viaja a lo largo de un camino LSP, debería emerger con el mismo valor de TTL que habría tenido si hubiese atravesado la misma secuencia de enrutadores sin haber habido conmutación de etiquetas. Si el paquete viaja a lo largo de una jerarquía de caminos LSP, el número total de saltos de enrutadores LSR atravesados se debería reflejar en su valor del TTL cuando emerge de la jerarquía de caminos LSP.

La forma en que el TTL es manejado puede variar dependiendo de si los valores de la etiqueta MPLS son transportados en un encabezado genérico específica de MPLS [MPLS-SHIM], o si las etiquetas MPLS son transportadas en una cabecera de nivel 2, tales como una cabecera ATM o una cabecera Frame Relay.

Si los valores de la etiqueta están codificados en un encabezado genérico que está entre las cabeceras del nivel de enlace y el nivel de red, entonces este encabezado genérico debe tener un campo TTL que inicialmente se debería cargar con el valor del campo TTL de la cabecera de nivel de red, se debería decrementar en cada salto de enrutador LSR, y se debería copiar en el campo TTL de la cabecera del nivel de red cuando el paquete emerge de su camino LSP.

Si los valores de la etiqueta son codificados en una cabecera de nivel de enlace (p.e. el campo VPI/VCI de una cabecera AAL5 de ATM), y los paquetes etiquetados son enviados por un conmutador de nivel 2 (p.e., un conmutador ATM), y el nivel de enlace (como ATM) no tiene el campo TTL, entonces no será posible decrementar el TTL del paquete en cada salto de enrutador LSR. Un camino LSP que consiste de una secuencia de enrutadores LSR que no puede decrementar el TTL de un paquete se denominará "camino LSP sin TTL".

Cuando un paquete emerge de un camino LSP sin TTL, sin embargo se le DEBERÍA dar un TTL que reflejara el número de saltos de enrutadores LSR que atraviesa. En el caso "unicast", esto se puede conseguir propagando una significativa longitud del camino LSP a los nodos de entrada, permitiendo a su entrada decrementar el TTL antes de enviar los paquetes a un camino LSP sin TTL.

Algunas veces se puede determinar, después del ingreso en un camino LSP sin TTL, que un determinado TTL de un paquete expirará antes de que el paquete alcance la salida del camino LSP sin TTL. En este caso, el enrutador LSR de entrada del camino LSP sin TTL no debe conmutar la etiqueta del paquete. Esto significa que se deben desarrollar procedimientos especiales para soportar la funcionalidad del "traceroute", por ejemplo, los paquetes "traceroute" se pueden enviar mediante el envío convencional de enrutamiento salto a salto.

Control de Bucle

En un camino LSP sin TTL, por definición, el TTL no se puede usar para proteger al paquete de posibles bucles. La importancia del control del bucle puede depender del hardware que se usa para el suministro de las funciones del enrutador LSR a lo largo del camino LSP sin TTL.

Supongamos, por ejemplo, que el hardware de un conmutador ATM que se está usando para suministrar las funciones de conmutación MPLS, con la etiqueta transportada en el campo VPI/VCI.

Dado que el hardware de conmutación ATM no puede decrementar el TTL, no hay protección contra bucles. Si el hardware ATM es capaz de suministrar un buen acceso al buffer de las celdas que llegan transportando diferentes valores VPI/VCI, la posibilidad de bucles no puede tener ningún efecto nocivo en el tráfico. Sin embargo si el hardware ATM no puede suministrar un buen acceso al buffer de este tipo, entonces incluso los bucles de tránsito pueden causar una severa degradación de la rentabilidad total del enrutador LSR.

Aún si se puede suministrar un buen acceso al buffer, merece la pena tener alguna forma de detectar los bucles que duran demasiado. Además, aunque donde el TTL y/o las colas por VC proveen una forma para los bucles supervivientes, aún puede ser deseable donde prácticamente evitar establecer los caminos LSP con bucle. Por tanto todos los enrutadores LSR que pueden estar conectados a un camino LSP sin TTL serán requeridos para soportar una técnica común para la detección de bucles; sin embargo, el uso de una técnica de detección de bucles es opcional

5.3.8. Agregación

Una forma de particionar el tráfico en FECs es crear una FEC por cada prefijo de dirección que aparece en la tabla de enrutamiento. Gráficamente:

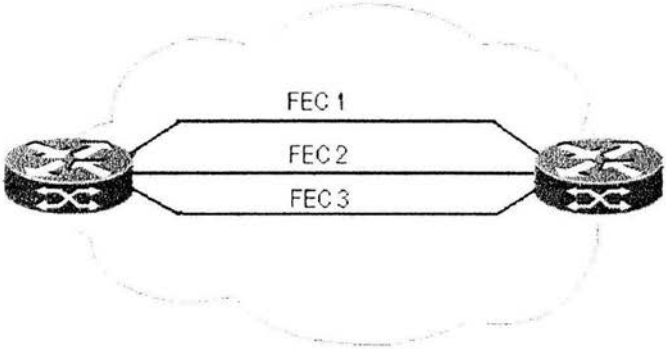


Figura 5.3.8.1. Agregación

Puede ocurrir que el tráfico del conjunto de FECs siga la misma ruta hacia el LSR de salida y que el intercambio de etiquetas sólo se utilice para hacer que el tráfico llegue a dicho LSR. En este caso, en el dominio MPLS, la unión de las FECs es a su vez una FEC. Por tanto habrá que elegir entre [RFC3301]:

- Asociar una etiqueta distinta a cada FEC
- Asociar una etiqueta a la unión y aplicar dicha etiqueta a todo el tráfico de la unión.

La arquitectura MPLS define la agregación como el procedimiento mediante el que se asocia una única etiqueta a una unión de FECs, que será a su vez una FEC (en algún dominio) y que aplica dicha etiqueta a todo el tráfico de la unión.

La agregación puede reducir la cantidad de etiquetas que se necesitan para manejar un conjunto particular de paquetes, y también puede reducir la cantidad necesaria de tráfico de control de distribución de etiquetas.

Dado un conjunto de FECs que pueden ser agregadas en una única FEC, se podrá:

- Agregarlas en una única FEC.

- Agregarlas en un conjunto de FECs.
- No agregarlas.

Por tanto se podrá hablar de grado de granulado de la agregación. La agregación más gruesa se corresponderá con el primer punto y la agregación más fina con el tercero.

Cuando se utiliza el control ordenado, cada LSR deberá tener, para un conjunto de FECs, el mismo grado de granulado para dichas FECs que el siguiente salto.

Cuando se utilice el control independiente se podrá dar el caso en el que dos LSRs adyacentes agreguen un conjunto de FECs de distinta forma.

Sea Ru el LSR de tráfico de entada y Rd el LSR de tráfico de salida. Si el grado de granulado de Ru es menor que el de Rd, Ru distribuirá más etiquetas para el conjunto de FECs que Rd. Por tanto, Ru deberá transformar n etiquetas en m etiquetas, con n>m. Otra opción sería que Ru retirara las n etiquetas y distribuyera un conjunto de m etiquetas que se corresponderían con el grado de granulado de Rd.

Si la granularidad de Ru es mayor que la de Rd, tendrá dos opciones:

- Adoptar el grado de granulado de Rd.
- Correlacionar sus m etiquetas con un subconjunto de las n etiquetas de Rd, siempre y cuando sepa que el enrutamiento será el mismo.

En todo momento cada LSR tendrá que saber qué grado de granulado aplicar a las etiquetas que asigna.

5.3.9. Fusión de etiquetas

Un LSR que soporta la fusión de etiquetas, al recibir dos paquetes por dos interfaces de entrada distintas, y/o con etiquetas distintas, puede reenviar ambos paquetes por la misma interfaz de salida y con la misma etiqueta. Gráficamente:

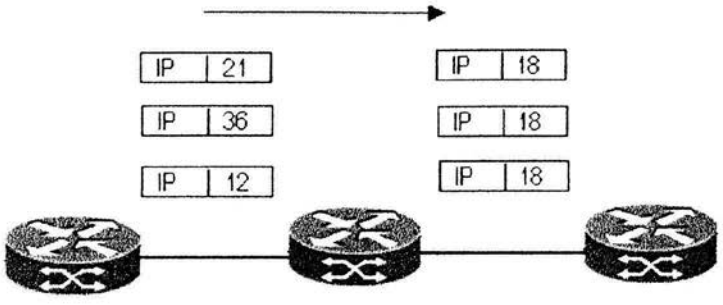


Figura 5.3.9.1 Reenvío de paquetes distintos por la misma interfaz de salida

Un LSR que no soporta la fusión de etiquetas, al recibir algún par de paquetes por interfaces distintas o con etiquetas distintas, reenviará dichos paquetes por interfaces distintas o con etiquetas distintas. Los LSRs ATM que usen codificaciones SVC o SVP no soportarán la fusión de etiquetas.

Con la fusión de etiquetas sólo se necesita una etiqueta de salida por FEC, mientras que sin fusión de etiquetas el número de etiquetas de salida por FEC podría ser tan grande como el número de nodos de la red.

MPLS soporta tanto LSRs con fusión de etiquetas como LSRs sin fusión de etiquetas. Por tanto, se han definido procedimientos que permiten el uso de LSRs que no soportan la fusión de etiquetas, así como procedimientos para permitir que ciertos conmutadores ATM puedan realizar la fusión de etiquetas.

LSRs que no pueden fusionar etiquetas

Un LSR que soporte la fusión de etiquetas y que sea Ru sólo necesitará que le manden una etiqueta por FEC. Si no soportase la fusión de etiquetas necesitaría que le mandasen múltiples etiquetas por FEC.

La arquitectura especifica que a un vecino que sea Ru y que no soporte la fusión de etiquetas, no se le mandarán etiquetas para ninguna FEC, a no ser que lo solicite explícitamente. Dicho vecino podrá realizar múltiples peticiones recibiendo cada vez una nueva etiqueta. Podría ocurrir que el vecino sea Rd y que está recibiendo dichas peticiones no soporte tampoco la fusión de etiquetas, en cuyo caso le pasará la petición al vecino Rd.

Procedimientos para que los conmutadores ATM realicen la fusión de etiquetas

En principio, los conmutadores ATM no soportan la fusión de etiquetas debido a que si se intenta realizar, se podría acabar teniendo células intercaladas de diferentes paquetes. Si esto ocurre será imposible reensamblar los paquetes.

Existen métodos para eliminar este problema y poder utilizar conmutadores ATM que exploten la fusión de etiquetas:

Fusión VC

Nombre aplicado a cualquier técnica que le permita a un conmutador ATM realizar la fusión de etiquetas. Esta técnica requiere encolar las células asociadas a las tramas AAL (*ATM Adaptation Layer*) hasta que se reciba la última célula. Una vez obtenida la última, se transmiten las células en el mismo orden en el que se recibieron, teniendo sumo cuidado de no intercalarlas con células de otra trama AAL que se esté transmitiendo por el mismo VC. El intercalado de células con distinto VCI está permitido, no siendo así en el caso de células asociadas al mismo VCI, las cuales deberán ser transmitidas, por el mismo VCI, sin ser intercaladas con células recibidas por otras interfaces de entrada (o por la misma interfaz pero con diferente VCI).

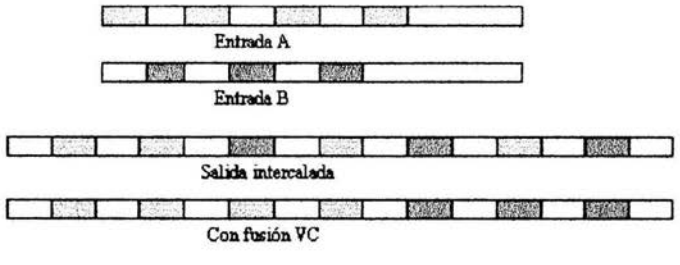


Figura 5.3.9.2 Técnica VC para que cualquier conmutador ATM realice la fusión de etiquetas

El intercalado de células de diferentes VPI/VCIs de entrada en el mismo VPI/VCI de salida hace que el receptor sea incapaz de determinar los límites de la trama a la hora de reensamblar la trama. Los marcadores de fin de trama de múltiples tramas se intercalaran también, lo que provocará que se

ensamblen células de una trama con células de otra, produciendo una trama inservible. Para poder fusionar el tráfico en el nivel VPI/VCI, la primera célula de una entrada VPI/VCI no se deberá mandar a una salida VPI/VCI hasta que la última célula de otra entrada VPI/VCI no se haya mandado por la salida VPI/VCI comentada anteriormente.

Por tanto, la fusión VC requiere encolar las células que se vayan a fusionar de cada entrada VPI/VCI hasta que la última célula de otra entrada VPI/VCI se haya mandado por esa misma salida VPI/VCI.

Fusión VP con codificación multipunto SVP

Nombre aplicado a cualquier técnica que correlacione números VCI distintos en distintos caminos virtuales (VPs) en interfaces de entrada, al mismo VP en una interfaz de salida. Puesto que se usan VCIs distintos al transmitir las células por la interfaz de salida, no será posible intercalar las células de distintos flujos de entrada en la interfaz de salida.

5.3.10. Modos de retención de etiquetas

Un LSR puede recibir información de asociaciones de etiquetas a FECs que no use. Por tanto, un LSR podrá guardar dicha información o descartarla. Los modos de retención de etiquetas especifican el comportamiento ante tal situación.

Sea Ru un LSR que está recibiendo asociaciones de etiquetas para FECs de un LSR Rd que no es su siguiente salto para dicha FEC. Si Ru guarda dicha información y por algún motivo Rd pasa a ser su siguiente salto, entonces Ru podrá usar la información de las asociaciones que le había enviado Rd previamente [RFC3301].

Modo liberal de retención de etiquetas

Si un LSR soporta el modo liberal de retención de etiquetas, mantendrá las asociaciones entre etiquetas y FECs recibidas de LSRs que no son su siguiente salto para dicha FEC.

La ventaja de este modo es que en el caso de que ocurra un cambio en la topología, las etiquetas de la nueva topología estarán ya en el LSR. El inconveniente de este modo es que requiere bastante memoria [2].

Modo conservador de retención de etiquetas

Si un LSR soporta el modo conservador de retención de etiquetas, descartará las asociaciones entre etiquetas y FECs recibidas de LSRs que no son su siguiente salto para dicha FEC.

La ventaja de este modo es que requiere menos memoria que el modo anterior. El inconveniente de este modo es el coste en tiempo en la obtención de nuevas etiquetas ante un cambio en la topología.

5.3.11. Espacio de etiquetas (uninacidad o peer)

El espacio de etiquetas se refiere al alcance de una etiqueta en un LSR y cómo este alcance se relaciona con su par adyacente. Se hablará de alcance por interfaz y alcance por plataforma.

Se hablará de espacio de etiquetas por interfaz cuando se pueda interpretar una misma etiqueta de forma distinta dependiendo de su interfaz de entrada [3].

Se hablará de espacio de etiquetas por plataforma cuando se interprete una etiqueta de la misma forma independientemente de su interfaz de entrada, siempre y cuando estas interfaces sean comunes con su par LSR. Un LSR puede tener múltiples espacios de etiquetas por plataforma, siempre y cuando pueda distinguir a los pares LSR. Por tanto, un LSR no podrá tener múltiples espacios de etiquetas por plataforma si no puede determinar qué interfaces tiene en común con sus pares LSRs.

En general, Rd sólo podrá saber si la etiqueta L de la cima de la pila la puso Ru1 o Ru2 si se cumplen las dos condiciones siguientes:

- Ru1 y Ru2 son los únicos pares de distribución de etiquetas a los que Rd les distribuyó la asociación de la etiqueta L.
- Ru1 y Ru2 están conectados cada uno directamente a Rd mediante un interfaz punto a punto.

5.3.12. MPLS y Multicast

Las nuevas aplicaciones que están surgiendo en Internet han producido un aumento de la necesidad de transmitir información desde un origen a múltiples destinos (multidifusión o multicast) y que esta transmisión garantice ciertos parámetros de Calidad de Servicio (QoS), por ejemplo, el retardo máximo y el número de paquetes que pueden ser descartados sin afectar a la calidad de la transmisión de la información. Esta QoS no puede ser asegurada por los protocolos TCP/IP, por lo que se han desarrollado diferentes tecnologías para superar este inconveniente, entre ellas MPLS[14].

MPLS se le ha especificado el funcionamiento de los protocolos de señalización CR-LDP (*Constraint-Route Label Distribution Protocol*) y RSVP-TE (*Resource Reservation Protocol – Traffic Engineering*) para asegurar parámetros de QoS, como por ejemplo, la reserva de recursos y el retardo máximo para un flujo de información. Todas estas herramientas hacen de MPLS un protocolo eficaz para resolver problemas de ingeniería del tráfico. Véase capitulo 5.4.

La multidifusión IP sobre MPLS asegura para aplicaciones en las que es necesario un retardo máximo y una cantidad máxima de paquetes descartados en la transmisión desde el origen hasta los múltiples destinos del grupo (por ejemplo video stream o videoconferencia). Esto se logra extendiendo los protocolos de señalización para la transmisión de paquetes IP sobre MPLS. En el caso de la transmisión sin QoS, para establecer los LSPs, se puede utilizar cualquiera de los protocolos de enrutamiento multidifusión IP más una señalización sin garantías de QoS, como RSVP (Resource *Reservation Protocol*) o LDP (*Label Distribution Protocol*). Para la transmisión con QoS, CR-LDP y RSVP-TE son usados como protocolos de señalización.

El enrutamiento Multicast procede por construcción de los árboles "multicast". El árbol a través del que un determinado paquete "multicast" se debe enviar depende en general de la dirección origen del paquete y su dirección destino. Cuando un determinado enrutador LSR es un nodo en un determinado árbol "multicast", liga una etiqueta a este árbol. Entonces distribuye esta ligadura a su padre en el árbol "multicast". Si el nodo en cuestión está en una LAN, y tiene hermanos en esta LAN, también debe distribuir la ligadura a sus hermanos. Esto permite al padre usar un único valor de etiqueta cuando multicasting a todos los hijos de la LAN.

Cuando llega un paquete "multicast" etiquetado, el NHLFE correspondiente a la etiqueta indica el conjunto de interfaces de salida para este paquete, así como la etiqueta de salida. Si la misma técnica de codificación de etiquetas se usa en todas las interfaces de salida, el mismo paquete se puede enviar a todos los hijos[15].

5.4. Protocolos de enrutamiento y señalización en MPLS

En el capitulo 5.2. , se introdujo sobre el funcionamiento de MPLS, el cual esta compuesto por dos componetes, la componente de envío y la componente de control. La componente de control se encarga de dos aspectos fundamentales: a) Cómo se generan las tablas de envío que establecen los LSPs y b) Cómo se distribuye la información sobre las etiquetas a los LSRs.

Para ser esto posible MPLS se vale de protocolos de enrutamiento y protocolos de señalización mejorados, para asi ofrecer QoS (Calidad de Servicio), TE (Ingeniería de Tráfico), TM (Gestión de Tráfico), y CR (reconocimiento de la congestión) . Veamos a continuación cada uno de ellos.

5.4.1. Protocolos de enrutamiento mejorados

Los protocolos de enrutamiento IP mejorados son aquellos que distribuyen información con base en la topología de la red y en las limitaciones de la misma, para construcción y mantenimiento de las tablas de enrutamiento. La tabla de enrutamiento contiene toda la información necesaria para el envío de datos IP tradicionales de salto en salto, así como también la información necesaria para realizar los cálculos

de los caminos con base en las limitaciones para MPLS LSPs. Como tal, los protocolos de enrutamiento internos (IGP) de IP, OSPF y IS-IS se han ampliado para soportar el anuncio de las limitaciones de la red. Son estas extensiones a los protocolos de enrutamiento IP basadas en las limitaciones las que permiten que la ingeniería de tráfico ocurra dinámicamente. Después de que el IGP ha convergido, los enrutadores dentro del sistema autónomo entienden la topología de la red, así como también los prefijos anunciados por cada enrutador. Desde que las extensiones de TE al OSPF o IS-IS son utilizadas para anunciar parámetros del enlace tales como ancho de banda y color administrativo dentro de la porción MPLS de la red, los enrutadores también saben qué ancho de banda está disponible en la red.

El enrutamiento basado en las limitaciones de la red y reconocimiento de congestión es un término usado para describir las redes que se dan cuenta completamente de su utilización actual, capacidad existente, y servicios aprovisionados a todo momento. Muchos lectores están familiarizados con las métricas comúnmente utilizadas para el enrutamiento IP y las decisiones de envío de los datos, incluyendo el salto siguiente, cuenta de saltos y costo. Mientras que estas métricas son útiles para predecir el "camino más corto" a través de la red, no pueden ser asumidas como confiables siempre, o ser las mejores para un flujo dado. Las modificaciones a los protocolos de enrutamiento IP están siendo definidas dentro del IETF de modo que se puedan intercambiar métricas adicionales y poder reconocer la congestión. El reconocimiento de la congestión es importante porque una vez que se hayan configurado las conexiones (ya sea por señalización dinámica o por aprovisionamiento estático), la capa 2 y la capa 3 de la red se dan cuenta de la cantidad de ancho de banda que está siendo utilizado, así como también las partes de la red que son utilizadas para enrutar las conexiones. Ejemplos de estas nuevas métricas incluyen: ancho de banda máximo del enlace, multiplicador máximo de la asignación (un porcentaje se puede utilizar para la sobre-suscripción), reservación del ancho de banda actual, clase del recurso (color, grupo administrativo), relación de la pérdida de paquetes, y retardo de propagación del enlace. Esta información se puede entonces propagar con los protocolos de enrutamiento IP que son intercambiados por todas los enrutadores IP, creando una visión verdadera de la congestión de la red y de su topología actual. Entonces, todas las peticiones futuras de la red se pueden dirigir a su destino por no solamente el "camino más corto primero " (según lo definido por OSPF), sino por un camino que garantice los requisitos del ancho de banda de las aplicaciones o servicios IP[16].

5.4.1.1. Extensiones en OSPF y IS-IS

El protocolo OSPF (*Open Shortest Path Firsht*) propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red y mantenimiento de bases de datos con información sobre sistemas locales y vecinos, de esta manera es capaz de calcular la métrica para cada ruta,

entonces se eligen las rutas de enrutamiento más cortas. En este proceso se calculan tanto las métricas de estado del enlace como de distancia, en el caso de RIP (*Routing Information Protocol*) se calcula sólo la distancia y no el tráfico del enlace, por esta causa OSPF es un protocolo de enrutamiento diseñado para redes con crecimiento constante y capaz de manejar una tabla de enrutamiento distribuida y de rápida propagación, entre las características más resaltantes de OSPF están:

- Detección de cambios en la topología y restablecimiento muy rápido de rutas sin bucles
- Poca sobrecarga, usa actualizaciones que informan de los cambios de rutas.
- División de tráfico por varias rutas equivalentes
- Enrutamiento según el tipo de servicio
- Uso de multienvío en las redes de área local.
- Mascaras de subred y superred.
- Autentificación

Enrutamiento por medio de OSPF

El enrutamiento dentro de un área se basa en un mapa completo de estado de enlace del área. OSPF se diseñó para que admitiera el crecimiento de la red porque un enrutador necesita conocer la topología detallada e información de métricas *sólo* de un área a la que pertenece.

Todos los enrutadores con OSPF implementado, en un área mantienen una base de datos de enrutamiento idéntica que describe la topología y estado de todos los nodos de esa área. La base de datos se usa para construir el mapa de esa área. Esta base de datos incluye el estado de todos los enrutadores, interfaces útiles de los enrutadores, las redes conectadas y sus enrutadores adyacentes. Siempre que ocurre un cambio, la información se propaga por toda el área. De esta forma siempre los enrutadores estarán en un estado óptimo para cualquier petición. De esta manera si tenemos un área bastante densa y se cae un enlace con un enrutador, en ese momento el enrutador vecino de ese enlace perdido informará a todos los demás que esa ruta será inaccesible, en cuanto se recupere el enlace informará de nuevo que se recuperó la comunicación con ese enrutador.

Un enrutador que esté arrancando obtendrá una copia de la base de datos actual de enrutamiento de su vecino más cercano (vecino se denomina a cualquier enrutador que esté en su área), tras esto, *solo* se comunicaran los cambios (esto hace más óptimo a OSPF, ya que no replica toda la base de datos de

nuevo). Los cambios se difunden rápidamente, ya que OSPF utiliza un algoritmo de distribución eficiente para extender la información de actualización por un área.

Un enrutador usa su base de datos para construir un árbol de caminos más cortos poniéndose a sí mismo en la raíz. Este árbol se usa para construir la tabla de enrutamiento. Si se dispone de enrutamiento por tipo de servicio en el área, se construye un árbol separado y un conjunto de rutas para cada tipo de servicio.

Tipos de mensajes OSPF

Los cinco tipos de mensajes del protocolo OSPF que se han descrito son:

Saludo Se usa para identificar a los vecinos, es decir, enrutadores adyacentes en un área para elegir un enrutador designado para una red multienvio, para encontrar un enrutador designado existente y para enviar señales de "*Estoy aquí*".

Descripción de la base de datos Durante la inicialización, se usa para intercambiar información de manera que un enrutador puede descubrir los datos que le faltan en la base de datos.

Petición del estado del enlace Se usa para pedir datos que un enrutador se ha dado cuenta que le faltan en su base de datos o que están obsoletos.

Actualización del estado del enlace Se usa como respuesta a los mensajes de Petición del estado del enlace y también para informar dinámicamente de los cambios en la topología de la red.

ACK de estado del enlace Se usa para confirmar la recepción de una Actualización del estado del enlace. El emisor retransmitirá hasta que se confirme.

Mediante el empleo de protocolos de enrutamiento (OSPF, IS-IS) cada miembro del dominio MPLS difunde un mensaje donde describe su entorno topológico junto con su estado de carga y recursos disponibles. Para este fin es necesario habilitar extensiones en los protocolos anteriores con el fin de incluir información de relativa a Ingeniería de Tráfico.

OSPF difundirá de manera transparente esta información mediante un LSA (*Link State Advertisement*), El cual contiene paquetes OSPF que contienen información del estado, métrica y otros de las interfaces del enrutador.

En Sistema Intermedio a Sistema intermedio IS-IS (*intermediate System - Intermediate System*), trabaja de manera similar que OSPF y se le han añadido dos nuevos TLV (*Type, Length and Value Objects*), TLV 22 describe el enlace y TLV 135 indica las redes IP alcanzables

Tras el intercambio masivo de información, cada LER y LSR establece y mantiene una base de datos llamada TED. A partir de la TED cada LER calcula los LSP posibles hacia los restantes LER, para este calculo se emplea el algoritmo CSPF (*Constrained Shortest Path First*)

CSPF es un algoritmo de "ruta-más-corta" modificado para tomar en cuenta las posibles restricciones en el calculo de un LSP a través del dominio MPLS. CSPF considera los siguientes factores:

- Información topológica generada por OSPF y IS-IS
- Atributos asociados con el estado de la red, ancho de banda total, ancho de banda reservado y disponible en cada enlace.
- Información facilitada por las extensiones TE.
- Detalles administrativos introducidos por el usuario, donde se detallan el número máximo de saltos, requerimientos de ancho de banda para ciertos LSP. Con la información anterior CSPF evalúa la participación de cada enlace y LSR en un futuro LSP

El resultado de los cálculos de CSPF para una determinada ruta son una secuencia de direcciones de LSR y enlaces, éstos proporcionaran la ruta más corta y optima para un futuro LSP Esta información reside en TED y será empleada por el módulo de señalización en su solicitud y asignación de etiquetas para un nuevo LSP [17].

5.4.2. Protocolos de distribución de etiquetas

Así como diferentes protocolos de enrutamiento IP tienen maneras únicas de mantener y actualizar las tablas de enrutamiento IP, MPLS soporta múltiples Protocolos de Distribución de Etiqueta (*Label Distribution Protocols - LDPs*), los cuales son protocolos de señalización para asignar y distribuir la información de etiquetado entre LSRs. A medida que se crean y destruyen asociaciones de etiquetas, los LSRs deberán notificarlo a sus vecinos. Para este propósito se utilizan los protocolos de distribución de etiquetas.

La arquitectura MPLS [RFC3301] define el protocolo de distribución de etiquetas como el conjunto de los procedimientos gracias a los cuales un LSR le informa a otro del significado de las etiquetas usadas para reenviar el tráfico a través de ellos. Por último, las tablas de envío creadas por el LDP (desde la dirección del protocolo de enrutamiento IP) permiten al LSRs establecer una conexión a través de la red MPLS. Actualmente, tres protocolos de señalización están bajo consideración de los organismos de estandarización de MPLS:

- El Protocolo de Distribución de Etiqueta LDP (*Label Distribution Protocol*)
- El protocolo de reserva de recursos con extensiones de Ingeniería de Tráfico RSVP-TE (*Resource reSerVation Protocol with Traffic Engineering Extensions*), el cual es basado en los protocolos RSVP existentes
- El protocolo de distribución de etiqueta de enrutamiento basado en limitaciones CR-LDP (*Constraint based Routed Label Distribution Protocol*), el cual es una extensión basada en limitaciones del LDP genérico

Actualmente existe una amplia variedad de protocolos utilizados para la distribución de etiquetas. La arquitectura MPLS no especifica uno de estos en particular, sino que, más bien, recomienda su elección dependiendo de los requerimientos específicos de la red, de las características hardware del LSR y de la estrategia del producto de cada fabricante. Los protocolos utilizados pueden agruparse en dos grupos: protocolos de **enrutamiento explícito** y protocolos de **enrutamiento implícito**. El enrutamiento explícito es idóneo para ofrecer ingeniería de tráfico y permite la creación de túneles. El enrutamiento implícito, por el contrario, permite el establecimiento de LSPs pero no ofrece características de ingeniería de tráfico .

El Protocolo de Distribución de Etiquetas (LDP) es uno de los protocolos de enrutamiento implícito que se utilizan con frecuencia. LDP define el conjunto de procedimientos y mensajes a través de los cuales los LSRs establecen LSPs en una red MPLS.

Por otro lado, entre los protocolos de enrutamiento explícito más comunes encontramos al protocolo LDP de Ruta Restringida (CR-LDP) y al Protocolo de Reservación de Recursos con Ingeniería de Tráfico (RSVP-TE). El primero de estos protocolos ofrece, en adición a LDP, características de ingeniería de tráfico, de manera que sea posible negociar con anticipación una ruta en especial. Esto permite establecer LSPs punto a punto con calidad de servicio en MPLS.

Mediante estos últimos protocolos y la aplicación de distintas estrategias de ingeniería de tráfico es posible asignar diferentes niveles de calidad de servicio en redes MPLS.

Como ya mencionamos anteriormente la arquitectura no impone ningún protocolo específico para la distribución de etiquetas [RFC3036]. De hecho se están normalizando distintos protocolos de distribución de etiquetas. A grandes rasgos podemos distinguir entre los protocolos nuevos definidos exclusivamente para la distribución de etiquetas y los que incorporan la etiqueta encima de protocolos existentes de enrutamiento a el llamado piggybacking, por lo que se han extendido protocolos existentes para que se pueda utilizar la distribución de etiquetas usando piggybacking.

La ventaja fundamental de utilizar piggybacking es que nunca tendremos condiciones de carrera, es decir, como se utiliza un protocolo de enrutamiento para la distribución de etiquetas, nunca se dará el caso de que tengamos la asociación de la etiqueta y no tengamos la información de enrutamiento asociada (asociación entre FECs y siguientes saltos). Otra ventaja radica en el hecho de que al estar utilizando un protocolo existente no sobrecargamos el sistema con nuevos mensajes. El inconveniente es que no siempre es sencillo extender protocolos existentes, puesto que podría ser necesario modificar los mensajes y por tanto tener problemas de compatibilidad con versiones anteriores[18].

Las desventajas de utilizar protocolos nuevos de distribución de etiquetas son la dificultad de evitar las condiciones de carrera y el hecho de estar añadiendo más mensajes en el sistema, por lo que aumenta su complejidad. La ventaja de utilizar protocolos nuevos de distribución de etiquetas es poder dar soporte a dicha distribución de etiquetas cuando no se puede utilizar piggybacking.

Así mismo, a continuación veremos una descripción de cada un a de los protocolos que se pueden utilizar en MPLS

5.4.2.1 BGP

BGP (*Border Gateway Protocol*) es un protocolo de enrutamiento usado entre sistemas autónomos. Está siendo utilizado ampliamente para conectar grandes redes de proveedores. El protocolo utiliza mensajes que se envían utilizando conexiones TCP. Los distintos tipos de mensajes que maneja este protocolo son [STAL02]:

- Open: se utiliza para establecer una relación de vecindad con otro enrutador.
- Actualización (Update): se utiliza para transmitir información a través de una ruta y/o enumerar múltiples rutas que se van a eliminar.
- Mantenimiento (Keepalive): utilizado para confirmar un mensaje Open y para confirmar periódicamente la relación de vecindad.
- Notificación: este tipo de mensajes se envían cuando se detecta una condición de error.

Los procedimientos funcionales de BGP son:

- Adquisición de vecinos: ocurre cuando dos enrutadores situados en diferentes sistemas autónomos se ponen de acuerdo para intercambiar información de enrutamiento regularmente. Un enrutador le enviará a otro un mensaje Open. Si el destino acepta la solicitud le devolverá un mensaje de mantenimiento.
- Detección de vecino alcanzable: una vez realizada la adquisición de vecinos se utiliza este procedimiento para mantener la relación. Periódicamente ambos dispositivos de enrutamiento se envían mensajes de mantenimiento para asegurarse que su par sigue existiendo y desea continuar con la relación de vecindad.
- Detección de red alcanzable: cada enrutador mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para alcanzar dichas redes. Cuando se realiza un cambio a esta base de datos, el enrutador enviará un mensaje de actualización por difusión. De esta forma el resto de los enrutadores BGP podrán construir y mantener la información de enrutamiento [18]

5.4.2.2. MPLS-BGP

En MPLS se puede utilizar BGP para distribuir la información de asociación de etiquetas para cada ruta que se anuncie. Esto es posible gracias a las extensiones multiprotocolo (*MPEs: Multiprotocol Extensions*) de BGP versión 4 [RFC2283].

Para distribuir las etiquetas se utilizan los mensajes de actualización (utilizando piggybacking), los cuales también se utilizan para distribuir la información de las rutas. La etiqueta se codifica en el campo NLRI (*Network Layer Reachability Information*) y para indicar que el campo NLRI contiene una etiqueta, se utiliza el campo SAFI (*Subsequent Address Family Identifier*). Un hablante BGP no podrá utilizar BGP para la distribución de etiquetas hacia un igual a no ser que dicho igual le indique que puede procesar mensajes de actualización con el campo SAFI especificado.

Ventajas de la utilización de MPLS-BGP:

- Si dos LSRs adyacentes también son hermanos BGP (peers), entonces la distribución de etiquetas se puede realizar sin necesidad de tener otro protocolo de distribución de etiquetas.
- Supongamos una red con dos clases de LSRs: LSRs exteriores, que hacen de interfaz con otras redes, y LSRs interiores, los cuales sólo transmiten tráfico entre los LSRs exteriores. Si los LSRs exteriores también son hablantes BGP y distribuyen etiquetas MPLS con la información de enrutamiento, entonces los LSRs interiores no necesitan recibir ninguna de las rutas BGP de los hablantes BGP.

Como se comentó anteriormente, las etiquetas se transportan como parte del campo NRLI en los atributos de extensión multiprotocolo. El AFI indica la familia de direcciones de la ruta asociada. Si el campo NLRI contiene una etiqueta, se le dará un valor de cuatro al campo SAFI para identificar esta situación [19].

El campo NLRI se codifica en una o más tripletas <longitud, etiqueta, prefijo> de la siguiente forma:

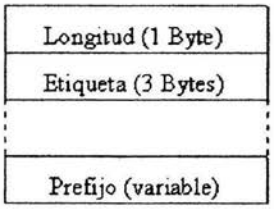


Figura 5.4.2.2.1. *Campo NLRI*

- Longitud: este campo se utiliza para indicar la longitud en bits del prefijo de dirección más la etiqueta.
- Etiqueta: el campo de la etiqueta sirve para transportar una o más etiquetas (lo que corresponde a la pila de etiquetas). Cada etiqueta se codifica en 3 Bytes, donde los 20 bits de más peso contienen el valor de la etiqueta y los bits de menos peso contienen la parte baja de la pila.
- Prefijo: este campo contiene los prefijos de dirección seguidos de bits de relleno para conseguir que el campo ocupe un número exacto de Bytes.

Para retirar una ruta anunciada previamente un hablante BGP podrá:

- Anunciar una nueva ruta (y una etiqueta) con la misma NLRI que la ruta previa.

- Listando la NLRI de la ruta previa en el campo de retirada de rutas (*Withdrawn Routes Field*) de un mensaje de actualización.

Si se termina una sesión BGP también se retiran todas las rutas anunciadas previamente.

Anuncio de múltiples rutas a un destino

Un hablante BGP puede mantener (y anunciar a sus hermanos) más de una ruta hacia un mismo destino siempre que cada ruta tenga sus propias etiquetas.

La codificación mencionada previamente permite que un solo mensaje de actualización contenga múltiples rutas, cada una con su(s) propia(s) etiqueta(s).

Para el caso en el que un hablante BGP anuncie múltiples rutas a un destino, si la ruta es retirada y la etiqueta(s) se especifica a la vez que la retirada, sólo dicha ruta con su correspondiente etiqueta es retirada. Si la ruta se retira y no se especifica etiqueta, entonces sólo la ruta sin etiquetar correspondiente se retira y se mantienen las rutas etiquetadas.

Hermanos BGP que no son adyacentes

Veámoslo con un ejemplo:

Figura 5.4.2.2.2. Hermanos BGP que no son adyacentes

D le distribuye a A la etiqueta L. A no podrá simplemente apilar L en la pila de etiquetas del paquete y enviar dicho paquete hacia B. D debe ser el único LSR que vea L en la cima de la pila. Antes de que A le envíe el paquete deberá apilar otra etiqueta que habrá obtenido previamente de B. B remplazará esta etiqueta con otra que obtuvo de C. Dicho de otra forma, de haber un LSP entre A y D. Si no existiera dicho LSP, A no podría usar la etiqueta L. Esto siempre será cierto cuando las etiquetas se distribuyan

entre LSRs que no son adyacentes, no importando si la distribución se hace por BGP o por cualquier otro método.

5.4.2.3. LDP

El protocolo de distribución de etiquetas LDP (*Label Distribution Protocol*) se ejecuta sobre TCP y, por tanto, es un protocolo de estado duro. Dado que se ejecuta sobre TCP, éste le proveerá de fiabilidad en el envío de mensajes. Posteriormente se verá que la única excepción la encontramos en los mensajes de anuncio que se ejecutan sobre UDP.

El uso más sencillo de LDP consiste en establecer enlaces unitarios de LSPs. Para hacer esto se puede usar la distribución de etiquetas por transito de salida no solicitado y transito de salida por demanda y es compatible con el control ordenado y con el control independiente. Se podrá usar el modo de retención de etiquetas conservador o el liberal. Pero habrá combinaciones no factibles.
Veámoslo con un par de ejemplos:

- Si los LSRs vecinos utilizan la distribución de etiquetas de transito de salida no solicitado y el LSR local utiliza el modo conservador de retención de etiquetas, habrá mucho tráfico de liberación de etiquetas.
- Si los LSRs vecinos utilizan la distribución de etiquetas de transito de salida por demanda y el LSR local utiliza el modo liberal de retención de etiquetas habrá mucho tráfico de petición de etiquetas.

LDP es un protocolo muy útil para los casos en los que se desea establecer un LSP a través de LSRs que no soporten piggybacking (básicamente esta es la única ventaja de LDP). LDP es bidireccional y podrá operar entre LSRs adyacentes o no adyacentes.

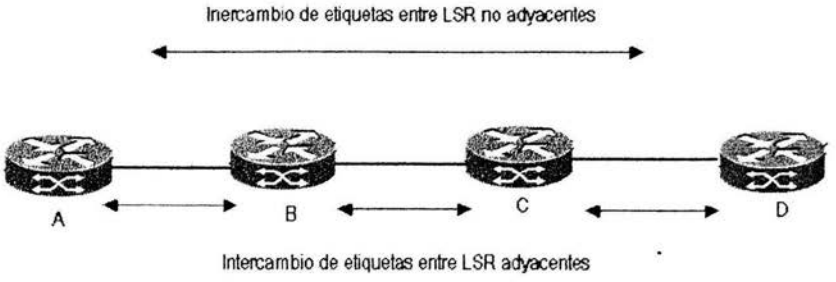


Figura 5.4.2.3.1. LDP es bidireccional y podrá operar entre LSRs adyacentes o no adyacentes.

El protocolo de distribución de etiquetas asocia una FEC con cada LSP que crea. Dos LDPs serán pares LDP (LDP peers) cuando ambos LSRs intercambien información de asociaciones de etiquetas y FECs. Para intercambiar dicha información establecerán una sesión LDP.

Mensajes LDP

Los pares LDP se podrán intercambiar cuatro clases de mensajes [RFC3036]:

1. Mensajes de descubrimiento (discovery messages): se usan para anunciar y mantener la presencia de un LSR en la red. Un LSR mandará periódicamente por la red mensajes HELLO a través de un puerto UDP con la dirección multicast "todos los enrutadores de esta subred".
2. Mensajes de sesión: se utilizan para establecer, mantener y terminar sesiones entre pares LDP. Cuando un LSR descubre a otro por medio de mensajes HELLO utilizará un procedimiento de iniciación LDP por medio de TCP.
3. Mensajes de anuncio (advertisement messages): se usan para crear, modificar y eliminar asociaciones de etiquetas a FECs. Se transportan vía TCP. Cuando se haya establecido la asociación los pares LDP podrán intercambiarse este tipo de mensajes.
4. Mensajes de notificación: Los mensajes de notificación también se transportan via TCP. Hay dos tipos de mensajes de notificación: notificaciones de error y notificaciones de aviso. El primer tipo se utiliza para notificar errores fatales, en cuyo caso terminará la sesión y se descartarán todas las asociaciones de etiquetas aprendidas en dicha sesión. El segundo tipo se utiliza para pasarle a un LSR información de la sesión LDP o el estado de algún mensaje anterior.

Formato de los mensajes [RFC3036]

El intercambio de mensajes entre LSRs pares se realiza mediante el envío de PDUs (*Protocol Data Unit*) LDP. Cada PDU LDP puede transportar más de un mensaje.

Cada PDU LDP está compuesto por una cabecera seguida de uno o más mensajes LDP. El formato de la cabecera es el siguiente:

Codificación TLV (*Type-Length-Value*)

El protocolo LDP utiliza el esquema de codificación de mensajes conocido como TLV.

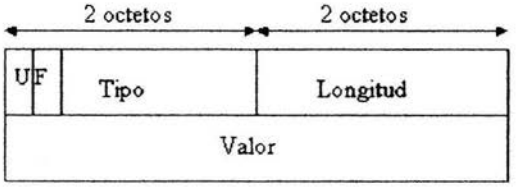


Figura 5.4.2.3.2. Formato de TLV

- U: bit de desconocido (Unknown). Si se recibe una TLV desconocida y U = 0, se debe enviar un mensaje de notificación al LSR origen y se ignora el mensaje. Si U = 1 se ignora el mensaje sin notificación.
- F: bit de reenvío de una TLV desconocida (Forward Unknown). Este campo sólo se utiliza cuando el bit U está activo. Si F = 0 la TLV desconocida no es reenviada. Si F = 1 la TLV desconocida se reenvía .
- Tipo: campo de 14 bits que define el tipo de mensaje y por tanto indica cómo debe ser procesado el campo Valor.
- Valor: campo de tamaño variable con la información a ser interpretada como lo especifique el campo Tipo. Este campo puede tener a su vez TLVs.

Codificaciones TLV para los parámetros usados frecuentemente

TLVs definidas en la versión 1 del protocolo:

- FEC: esta TLV contendrá las FECs que se intercambian los LSRs. Una FEC podrá ser un prefijo de dirección o una dirección completa de un host. El elemento FEC comodin se utiliza exclusivamente en los mensajes de liberación y retiro de etiquetas.
- Etiquetas: estas TLVs sirven para codificar etiquetas. Las TLVs de etiquetas son transportadas por los mensajes de anuncio, petición liberación y retiro de etiquetas. Tipos de TLVs de etiquetas:
- Etiqueta genérica: un LSR utiliza este tipo de TLV para codificar etiquetas que se van a usar en enlaces para los que los valores de las etiquetas son independientes de la tecnología del nivel de enlace subyacente (por ejemplo, PPP y Ethernet).
- Etiqueta ATM: un LSR utiliza este tipo de TLV para codificar etiquetas a usar en enlaces ATM. Esta TLV contendrá los valores ATM VPI/VCI.
- Etiqueta de retransmisión de tramas (Frame Relay): un LSR utilizará la TLV de etiqueta de retransmisión de tramas para codificar etiquetas a usar en enlaces Frame Relay. Contendrá los valores DLCI de Frame Relay.
- Lista de direcciones: la TLV de lista de direcciones aparece en los mensajes de dirección y retiro de etiquetas. Actualmente sólo está definido IPv4.
- Cuenta de saltos: esta TLV aparece como un campo opcional en los mensajes que establecen los LSPs. Calcula el número de saltos LSR a través de un LSP a medida que el LSP se establece. Se puede usar para la detección de bucles.
- Vector camino: se utiliza conjuntamente con la TLV de cuenta de saltos en los mensajes de petición y asociación de etiquetas para implementar el mecanismo opcional de detección de bucles. Su uso en el mensaje de petición de etiquetas registra el camino de LSRs que ha atravesado la petición. En el mensaje de asociación de etiquetas, registra el camino de LSRs que el mensaje de aviso (Advertisement) ha atravesado para establecer el LSP.
- Estado: los mensajes de notificación transportan TLVs de estado para especificar los eventos que se están señalizando.
- Estado extendido: extiende la TLV anterior con información adicional.
- PDU devuelta: esta TLV puede operar con la TLV de estado. Un LSR la utilizará para devolver parte de la PDU LDP que le envió otro LSR. El valor de esta TLV será la cabecera de la PDU y tantos datos de la PDU como sean necesarios por la condición que marque el mensaje de notificación.

- Mensaje devuelto: se puede usar conjuntamente con la TLV de estado. Sirve para devolver parte de un mensaje LDP al LSR que lo envió.
- Parámetros HELLO comunes: esta TLV contiene parámetros comunes para manejar los mensajes HELLO.
- Dirección de transporte IPv4: esta TLV permite que se use una dirección IPv4 al abrir una conexión TCP para una sesión LSP.
- Número de secuencia de configuración: identifica el estado de configuración del LSR emisor. Se usa para que el LSR receptor pueda detectar cambios en la configuración.
- Dirección de transporte IPv6: esta TLV permite que se use una dirección IPv6 al abrir una conexión TCP para una sesión LSP.
- Parámetros comunes de la sesión: esta TLV tendrá los valores propuestos por el LSR emisor para los parámetros que pretende negociar en una sesión LDP [20].

Mensajes

Todos los mensajes LDP tienen el siguiente formato:

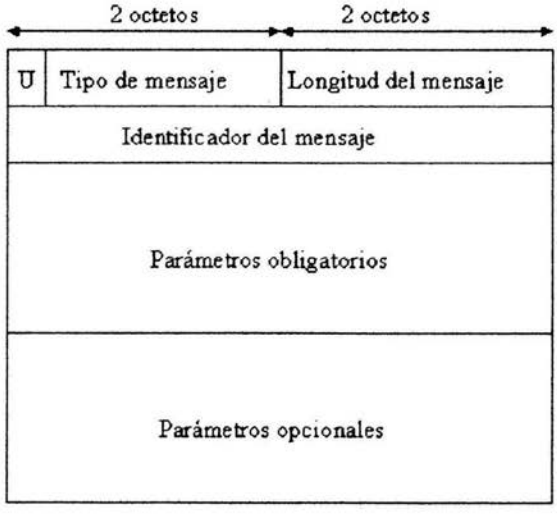


Figura 5.4.2.3.3. Formato de un mensaje LDP

- U: bit de mensaje desconocido. Cuando se reciba un mensaje desconocido, si U = 0 se enviará una notificación al origen del mensaje. Si U = 1 simplemente se ignorará.
- Tipo de mensaje: identifica el tipo del mensaje.
- Longitud del mensaje: longitud del identificador del mensaje, de los parámetros obligatorios y de los parámetros opcionales
- Identificador del mensaje: identificador del mensaje.

- Parámetros obligatorios: conjunto de todos los parámetros obligatorios de los mensajes. Este campo tiene una longitud variable. Algunos mensajes no tienen parámetros obligatorios.
- Parámetros opcionales: conjunto de los parámetros opcionales de los mensajes. Este campo también es de longitud variable.

Todo lo que aparece en un mensaje LDP se podría codificar en una TLV, pero la especificación no utiliza dicha codificación para todos los casos.

Los tipos de mensajes que define la especificación son los siguientes:

Mensaje de notificación

Este tipo de mensajes es utilizado por un LSR para notificarle a su par LSR de una condición de error o para suministrarle información de aviso.

Cuando un LSR recibe un mensaje de notificación que contiene un código de estado que indica un error fatal, éste terminará la sesión LDP cerrando conexión TCP de la sesión y descartará todo estado asociado a la sesión, incluyendo todas las asociaciones de etiquetas a FECs aprendidas en dicha sesión LDP.
Clasificación de los eventos que este tipo de mensajes señalizan:

- PDU mal formada o mensaje mal formado.
- TLV desconocida o mensaje desconocido.
- Expiración del temporizador del mantenimiento de la sesión.
- Terminación de la sesión unilateralmente.
- Eventos de mensajes de iniciación.
- Eventos resultantes de otros mensajes
- Errores internos.
- Eventos diversos.

Mensaje HELLO

Este tipo de mensajes son intercambiados entre pares LDPs durante la fase de descubrimiento.

Mensaje de iniciación

Este mensaje se utiliza cuando dos pares LDP desean establecer una sesión LDP. Son los mensajes que se envían al inicio de una sesión. Estos incluyen valores de los contadores KeepAlive y el rango de etiquetas a ser usadas en el enlace entre los dos LSRs. Ambos enrutadores pueden enviar los mensajes de inicialización. Al recibirlos deberán responder con mensajes KeepAlive si los parámetros son aceptables. Si algún parámetro no fuera aceptable, el LSR responde con una notificación de error y la inicialización de la sesión se da por terminada.

Mensaje de mantenimiento *(KeepAlive)*

Estos mensajes los intercambian pares LSRs para monitorizar la integridad de la conexión de transporte de la sesión LDP. Son mensajes enviados periódicamente en ausencia de algún otro mensaje con el fin de asegurar que cada enrutador conoce a sus demás vecinos y que se encuentren trabajando correctamente. En ausencia de un mensaje KeepAlive o algún mensaje LDP en el intervalo apropiado de tiempo, un LSR concluye que su vecino (ò su conexión a èl) se ha caído y termina la sesión

Mensaje de dirección

Este mensaje se lo manda un LSR a su par LSR para notificarle las direcciones de sus interfaces. El LSR que reciba este mensaje utilizará las direcciones aprendidas para actualizar una base de datos para las correlaciones entre los identificadores LDP de los pares y las direcciones de los siguientes saltos.

Mensaje de retiro de direcciones

Este mensaje se utiliza para retirar las direcciones de interfaces notificadas anteriormente.

Mensaje de petición de etiquetas

Este mensaje se lo manda un LSR a su par LSR cuando quiere solicitarle una asociación de etiquetas.

El mensaje de petición de etiquetas lo utiliza un LSR que esta en el tráfico de entrada para solicitarle explícitamente al LSR que está tráfico de salida una asociación de etiquetas.

Un LSR puede enviar un mensaje de petición de etiquetas sí:

- El LSR reconoce una nueva FEC vía la tabla de reenvío y el siguiente salto es un par LDP, y además el LSR no tiene una asociación del siguiente salto para dicha FEC.
- El siguiente salto para la FEC cambia y el LSR no tiene todavía la asociación de su siguiente salto para dicha FEC.
- El LSR recibe una petición de etiquetas para una FEC de su par LDP que está en el tráfico de entrada, el siguiente salto de la FEC es un par LDP, y el LSR no tiene la asociación de su siguiente salto [21].

Mensaje de petición de abandono de etiqueta

Este mensaje abandona una petición de etiquetas pendiente.

Mensaje de retiro de etiquetas

Este mensaje se utiliza para retirar una asociación de etiquetas que está siendo usada. Un LSR le enviará este tipo de mensaje a su par LSR para indicarle que no puede continuar usando la asociación que previamente anunció. De esta forma se rompen las asociaciones entre etiquetas y FECs.

Un LSR enviará este tipo de mensajes bajo las siguientes condiciones:

1. El LSR no reconoce una FEC que antes reconocía para la que ha anunciado una etiqueta.
2. El LSR ha decidido unilateralmente (por ejemplo, vía configuración) que no va a realizar la conmutación de etiquetas para la FEC o FECs con la asociación que se va a retirar.

Un LSR que reciba este tipo de mensaje debe responder con un mensaje de liberación de etiquetas.

Mensaje de mapeo de etiqueta

Estos mensajes son el corazón de la distribución de etiquetas, pues son usados para anunciar una relación entre una dirección IP y una etiqueta.

Mensaje de liberación de etiquetas

Este mensaje se utiliza cuando un LSR quiere informar a su par LSR que ya no necesita una asociación pedida o advertida anteriormente por su par LSR.

Un LSR debe transmitir este mensaje si:

1. El LSR que mandó la asociación ya no es el siguiente salto para la FEC asociada y el LSR está configurado para operar en modo conservativo.
2. El LSR recibe una asociación de un LSR que no es el siguiente salto para la FEC, y el LSR está configurado para operar en modo conservativo.
3. El LSR recibe un mensaje de retiro de etiquetas.

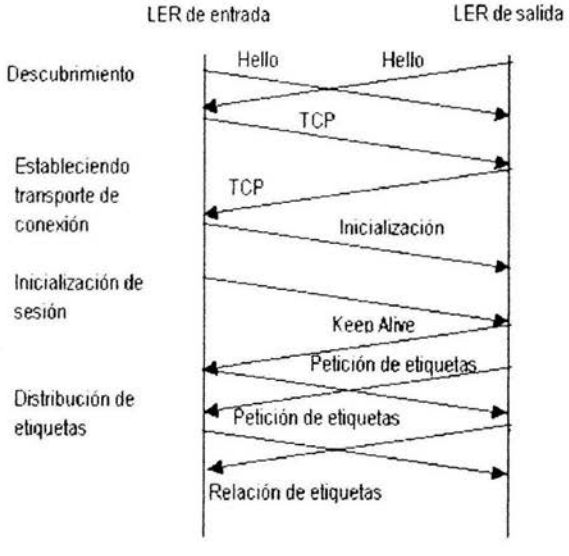


Figura 5.4.2.3.4. Mensajes en LDP

FECs e identificadores

Una FEC identificará a un conjunto de paquetes IP que podrán ser enviados a través de un LSP. LDP define dos tipos de FECs:

- Prefijo de dirección
- Dirección de host

Habrá una correspondencia entre una dirección particular y un prefijo de dirección si la dirección comienza con el prefijo. Habrá una correspondencia entre un paquete y un LSP si existe una correspondencia entre el prefijo de dirección del LSP y la dirección de destino del paquete.
El procedimiento para correlacionar un paquete a un LSP está formado por una serie de reglas. Estas reglas se aplicarán hasta que el paquete pueda ser correlacionado a un LSP. Las reglas son:

- Si hay exactamente un LSP con un elemento FEC de dirección host con la misma dirección destino que el paquete, entonces el paquete se correlacionará con ese LSP.
- Si hay varios LSPs, cada uno con un elemento FEC de dirección host idéntica a la dirección destino del paquete, entonces el paquete se correlacionará con uno de esos LSPs.
- Si hay una única equivalencia entre un paquete y un LSP, entonces el paquete se correlacionará con ese LSP.
- Si hay múltiples equivalencias entre un paquete y varios LSPs, entonces el paquete se correlacionará con el LSP que tenga mayor porcentaje de igualdad en el prefijo (es decir, el más largo).
- Si un paquete debe atravesar un enrutador frontera, y existe un LSP con un elemento FEC de prefijo de dirección que es una dirección de ese enrutador, entonces el paquete se correlacionará con ese LSP [22].

Identificadores LDP

Un identificador LDP se utiliza para identificar el espacio de etiquetas de un LSR. Se compone de seis octetos, de los cuales los cuatro primeros identifican al LSR y los dos últimos identifican el espacio de etiquetas de dicho LSR. Como se comentó en capítulos anteriores, el espacio de etiquetas puede ser por interfaz o por plataforma. Si los dos últimos octetos tienen un valor de cero el espacio de etiquetas será por plataforma.

La especificación de LDP [RFC3036] utiliza la siguiente nomenclatura para representar un identificador LDP:

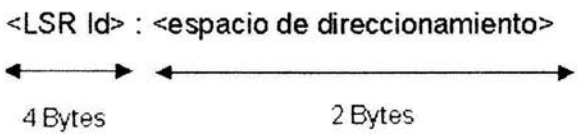


Figura 5.4.2.3.5. identificador LDP

Sesión LDP

Cuando un LSR utiliza LDP para anunciar más de un espacio de etiquetas a otro LSR, utilizará diferentes sesiones LDP para cada espacio de etiquetas. Como se comentó anteriormente, LDP utiliza TCP. Cuando dos LSRs requieren múltiples sesiones LDP, se establecerán sesiones TCP distintas para cada sesión LDP.

En la especificación del protocolo [RFC3036] se definen dos fases para el establecimiento de la sesión LDP:

- Descubrimiento
- Establecimiento y mantenimiento de sesiones LDP

Descubrimiento

El protocolo de descubrimiento de LDP utiliza UDP como protocolo de transporte. Existen dos modalidades de descubrimiento: básica y extendida.

En la modalidad básica el LSR envía periódicamente mensajes HELLO a un puerto bien conocido con la dirección multicast "todos los enrutadores de esta red". Los enrutadores están escuchando continuamente en este puerto a la espera de recibir mensajes HELLO. Por tanto, llegará un momento en el que el LSR conocerá todos los LSRs con los que tiene una conexión directa. Por tanto este mecanismo se utiliza si los LSRs están conectados directamente por medio de un enlace.

Los mensajes HELLO transportarán el identificador LDP con el espacio de etiquetas que LSR pretende usar en esa interfaz, además de otro tipo de información.
Con la modalidad extendida se permite que dos LSRs que no están conectados directamente establezcan una sesión LDP. Con esta modalidad, un LSR emite periódicamente mensajes HELLO a un puerto (UDP) bien conocido y con una dirección específica, que habrá aprendido de algún modo (por ejemplo, por configuración). Los mensajes HELLO transportarán el identificador LDP con el espacio de etiquetas que LSR pretende usar, además de otro tipo de información. El LSR al que se le están enviando los mensajes HELLO podrá responder o ignorar dicho mensaje. Si decide responder a dicho mensaje deberá mandar periódicamente mensajes HELLO al LSR que inició el proceso[23].

La modalidad extendida es útil cuando se ha configurado un LSP entre dos LSRs por ingeniería de tráfico, deseando mandar paquetes ya etiquetados a través de ese LSP. El LSR situado al principio del LSP necesitará saber como etiquetar los paquetes que le enviará la LSR situado al final del LSP.

Establecimiento y mantenimiento de sesiones LDP

Una vez conocidos los vecinos se podrá establecer la sesión. Cada uno de los LSRs implicados puede jugar un papel activo o pasivo. El establecimiento de una sesión consta de dos fases:

Establecimiento de la conexión de transporte. Esta fase consiste en el establecimiento de una conexión TCP entre los LSRs implicados, para una nueva sesión LDP.

Inicio de la sesión. Una vez establecida la conexión TCP los LSRs deben negociar los parámetros de la sesión. Esto se hace intercambiando mensajes de iniciación. Estos parámetros incluyen la versión del protocolo LDP, el método de distribución de etiquetas, valor de los temporizadores, etc.
Si el LSRa juega el papel activo, éste iniciará la negociación de los parámetros de la sesión enviando un mensaje de iniciación al LSRb. Este mensaje contendrá tanto el identificador LDP del LSRa como el identificador del LSRb.

Cuando un LSR recibe un mensaje de iniciación, mirará dicho mensaje para determinar si los parámetros son aceptables. Si lo son, responderá con su propio mensaje de iniciación proponiendo los parámetros que desea usar y un mensaje de mantenimiento (KeepAlive) para notificar al otro LSR que acepta los parámetros. Si los parámetros no son aceptables, responderá con un mensaje de notificación de error de parámetros rechazados.

5.4.2.4. RSVP

El Protocolo de Reserva de Recursos, RSVP(*Resource reSerVation Protocol*) se utiliza para reservar recursos para una sesión en un entorno de red IP. Es un protocolo de estado blando, por lo que con este tipo de protocolos si no se reciben los mensajes de actualización (update) o refresco de la información de estado, se marcará dicho estado como no válido y se descartará la información. Estos protocolos son adecuados en entornos no fiables.

RSVP pretende proporcionar calidad de servicio estableciendo una reserva de recursos para un flujo determinado. Un host hace una petición de una calidad de servicio específica sobre una red para un flujo particular de una aplicación.

Características de RSVP

- Protocolo de reserva de recursos.
- Se diseña para trabajar con cualquier servicio de QoS (los objetos propios de la QoS no están definidos por el protocolo).
- Permite Unicast y Multicast. No es un protocolo de enrutamiento, sino que está pensado para trabajar conjuntamente con éstos.
- No transporta datos de usuario.
- Los protocolos de enrutamiento determinan dónde se reenvían los paquetes mientras que RSVP se preocupa por la QoS de los paquetes reenviados de acuerdo con el enrutamiento.
- Es un protocolo simplex: petición de recursos sólo en una dirección, diferencia entre emisor y receptor. El intercambio entre dos sistemas finales requiere de reservas diferenciadas en ambas direcciones.
- Reserva iniciada por el receptor (protocolo orientado al receptor).
- Mantenimiento del estado de la reserva (estado blando) en los enrutadores. El mantenimiento de la reserva es responsabilidad de los usuarios finales.
- Permite diferentes tipos de reservas.
- Protocolo transparente para los enrutadores no RSVP.
- Soporta IPv4 e IPv6 aunque no sea un protocolo de transporte.

Mensajes

Existen dos tipos fundamentales de mensajes RSVP:

Mensajes Path. Estos mensajes los generan los emisores. Describen el flujo del emisor y proporcionan la información del camino de retorno hacia el emisor. Este mensaje lo utilizan los emisores para establecer el camino de la sesión. Estos mensajes pueden atravesar enrutadores que no entiendan RSVP puesto que tienen una dirección IP origen y una dirección IP destino.

Mensaje Resv Estos mensajes los generan los receptores y sirven para hacer una petición de reserva de recursos. Crean el "estado de la reserva" en los enrutadores. Generalmente, una petición de recursos implicará una reserva de éstos en todos los nodos del camino del flujo de datos. Estos mensajes siguen exactamente el camino inverso al de los datos.

Por tanto, el mensaje Path es el responsable del inicio de la operación y es mandado a los participantes potenciales de la sesión. El mensaje Resv se manda en respuesta al mensaje Path.
La siguiente figura muestra el uso de estos mensajes:

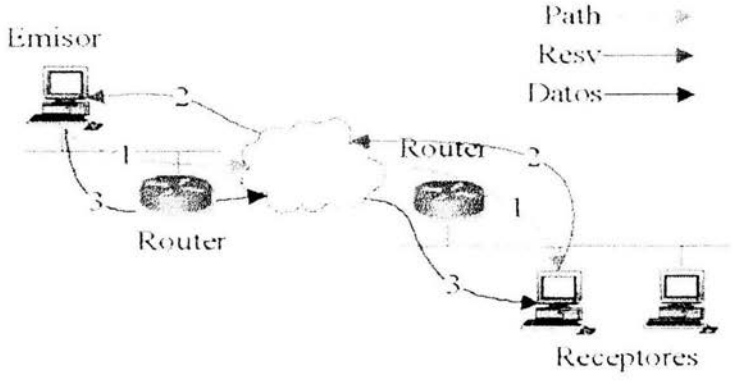


Figura 5.4.2.4.1. Mensajes fundamentales de RSVP

Flujos de datos

Existen tres conceptos básicos asociados con los flujos de datos que maneja el protocolo [STAL02]:

1. Sesión RSVP: es un flujo de datos identificado por su destino y por un protocolo de transporte particular. Sus componentes son:

- Dirección IP destino: dirección IP destino de los paquetes (unicast o multicast)
- Identificador del protocolo IP.
- Puerto destino (opcional).

2. Descriptor de flujo: se llama así a una petición de reserva realizada por un sistema final. Está compuesto de:

- Flowspec: especifica la calidad de servicio deseada. Incluye:
- Service class: clase de servicio.
- Y dos parámetros numéricos: Rspec, que define la QoS deseada (Reserve) y

3. Tspec, que describe el flujo de datos (Traffic)

Filter spec: designa un conjunto arbitrario de paquetes dentro de una sesión a los que aplicar la QoS definida por el flowspec . El formato depende de si se utiliza IPv4 o IPv6, pero básicamente es: Dirección IP fuente + puerto UDP/TCP fuente

Un mensaje RSVP está formado por una cabecera común, seguida de un número variable de objetos de longitud variable. [STAL02]

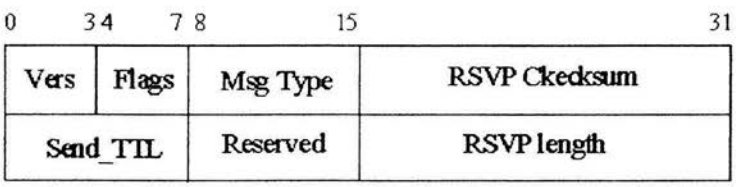


Figura 5.4.2.4.2. Formato de la cabecera

Campos de la cabecera

- Vers: versión del protocolo RSVP. Actualmente la 1.
- Flags: no definido.
- Msg Type: tipo de mensaje. A continuación se enumeran.

    1. Path
    2. Resv
    3. Path_Err
    4. Resv_Err
    5. PathTear
    6. ResvTear
    7. ResvConf

- RSVP Checksum: campo de verificación.
- Send_TTL: indica el tiempo de vida (Time To Live) del mensaje.
- RSVP Length: longitud total del mensaje expresada en bytes, incluyendo la cabecera y el cuerpo.

Funcionamiento

La fuente envía un mensaje Path a los destinos. Dicho mensaje se manda a una dirección que es una dirección de sesión. Podrá ser una dirección unicast o multicast. Cuando el destino reciba el mensaje Path podrá enviar un mensaje Resv a la fuente, que viajará justo por el camino inverso al mensaje Path. Dicho mensaje Resv identificará la sesión para la que se quiere hacer la reserva. El mensaje será reenviado hacia la fuente por los enrutadores. Éstos reservarán los recursos necesarios analizando dicho mensaje.

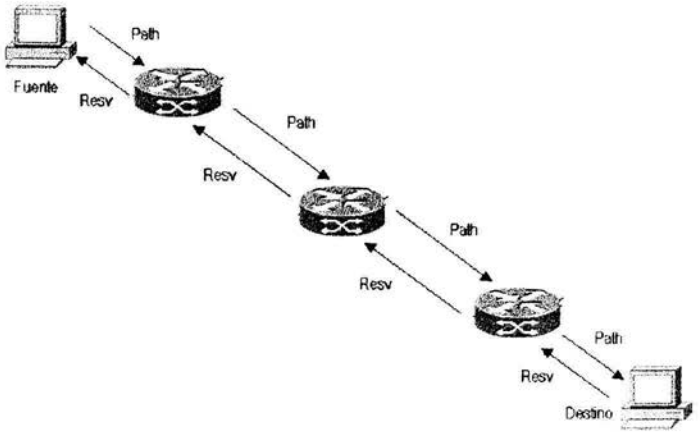


Figura 5.4.2.3.3. Funcionamiento de RSVP

Como vimos anteriormente, RSVP es un protocolo simplex. Los enrutadores reconocerán los paquetes pertenecientes a un flujo examinando la dirección origen y destino, el puerto origen y destino y el número de protocolo (ej: UDP). Puesto que RSVP es un protocolo de estado blando, se deberán mandar periódicamente mensaje Path y Resv para refrescar el estado [18].

Como vimos anteriormente para la aplicación de Ingeniería de traficó MPLS se vale de dos aproximaciones de protocolos RSVP y CR-LSP, como a continuación se dará una breve explicación

5.4.2.5. RSVP-TE

RSVP-TE (*Resource reSerVation Protocol with Traffic Engineering Extensions*) [RFC3209], son extensiones de RSVP para túneles LSP

Se puede utilizar RSVP para establecer LSPs usando la distribución de etiquetas de tráfico de salida por demanda [RFC3209].

Creación de un ER-LSP:

1. El LER de entrada quiere establecer un nuevo LSP hacia el LER de salida. Los parámetros de tráfico determinan por dónde debe pasar la ruta, así que el LER de

entrada envía un mensaje PATH con la ruta explícita hacia el LER de salida y con los parámetros de tráfico que requiere la sesión.

2. Cada nodo de la ruta que recibe el mensaje determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje PATH eliminándose de la ruta. En cualquier caso cada LSR creará una nueva sesión.
3. Una vez llega al LER de salida, éste determina qué recursos ha de reservar y devuelve un mensaje RESV que distribuirá la etiqueta que ha elegido para ese LSP y contendrá los detalles de la reserva.
4. Los LSRs intermedios emparejan los mensajes PATH y RESV que han recibido según el identificador de LSP, reservan los recursos que indica RESV, asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje RESV.
5. El LER de entrada, cuando lo recibe, enviará un mensaje de confirmación RESVConf para indicar que se ha establecido el LSP [24].

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

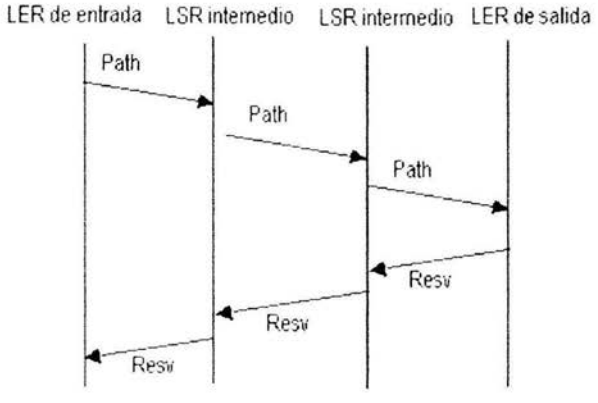


Figura 5.4.2.5.1. Mensajes de RSVP

Una de las mayores ventajas del hecho de usar RSVP para establecer túneles LSP es que permite la asignación de recursos a través del camino. Pero no es obligatorio realizar la reserva de recursos cuando se establece el LSP. Se puede establecer un LSP sin reservar ningún tipo de recursos.

5.4.2.6. CR-LDP

Antes de desarrollar CR-LDP (*Constraint-based Enrutamiento LDP*) Enrutamiento basado en restricciones LDP, conviene aclarar lo que se entiende por enrutamiento basado en restricciones.

Enrutamiento basado en restricciones

Con el enrutamiento convencional, es decir, con IP, la elección de un camino se basa en algún algoritmo que optimice alguna métrica escalar. Por ejemplo, con RIP la métrica que se usa es el número de saltos. RIP elige el camino que minimice el número de saltos.

Con el enrutamiento basado en restricciones, entre cada par de nodos se deberán satisfacer una serie de restricciones. Las restricciones entre nodos diferentes podrán ser diferentes. Por supuesto, además de satisfacer dichas restricciones, también existirá una métrica particular como sucedía en el enrutamiento convencional. Una vez establecido el camino, el enrutamiento basado en restricciones será el responsable de establecer y mantener el estado del reenvío a través de dicho camino .

Las restricciones podrán ser de rendimiento, calidad de servicio como demora, variación de demora o tasa de pérdidas, administrativas o una mezcla entre ellas [BRIT01] . Ejemplo de restricción de rendimiento puede ser el encontrar un camino que tenga un mínimo ancho de banda, y ejemplo de restricción administrativa sería que determinado tráfico atravesara sólo ciertos enlaces de la red.

El grupo de trabajo sobre MPLS del IETF ha definido extensiones para que el protocolo LDP soporte el enrutamiento basado en restricciones. A esta extensión del protocolo se le denomina CR-LDP.

Es un protocolo de estado duro y utiliza sesiones TCP entre compañeros LSR.

Creación de un ER-LSP:

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

2. Cada nodo de la ruta que recibe el mensaje reserva los recursos y determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje LABEL_REQUEST eliminándose de la ruta. Puede reducir la reserva si los parámetros de tráfico están marcados como negociables.

3. Una vez llega al LER de salida, éste realiza cualquier negociación final sobre los recursos y hace la reserva. Asigna una nueva etiqueta al nuevo LSP y la distribuye en un mensaje LABEL_MAPPING que contiene los parámetros de tráfico finales reservados para el LSP.

4. Los LSRs intermedios emparejan los mensajes LABEL_REQUEST y LABEL_MAPPING que han recibido según el identificador de LSP, asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje LABEL_MAPPING.

5. En cuanto llegue al LER de entrada se habrá establecido el LSP [25].

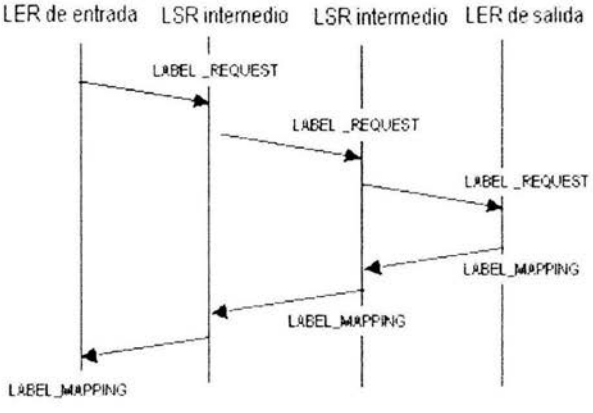


Figura 5.4.2.6.1 Mensajes de CR-LDP

Las limitaciones de CR-LDP en la actualidad son las siguientes [RFC3213]:

- Sólo soporta LSPs punto a punto.
- Sólo soporta el establecimiento unidireccional de LSPs.
- Sólo soporta una única etiqueta por LSP.

Lógicamente, se está trabajando para encontrar soluciones a las presentes limitaciones [26].

Comparación de CR-LDP vs RSVP-TE .

RSVP-TE es *soft state*, lo cual significa que la información es intercambiada cuando se establece el LSP, pero se deben enviar mensajes periódicos para notificar que la conexión todavía se requiere. Por el contrario, CR-LDP es *hard state*, es decir, toda la información se intercambia al iniciar la conexión y no se produce más información adicional hasta que el LSP se elimine [26].

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

CR-LDP utiliza conexiones TCP lo que hace que éstas sean más fiables y seguras, mientras que TE-RSVP utiliza UDP o datagramas IP para establecer las comunicaciones, lo que supone mayor vulnerabilidad aunque puede utilizar IPSec o algún otro esquema de encriptación[27].

Las conexiones TCP de CR-LDP permiten detectar un fallo mediante notificaciones propias de TCP. Esta notificación se procesa rápidamente así que las acciones oportunas sean iniciadas. Sin embargo, una conexión fallida en RSVP-TE será detectada cuando no se reciba un determinado mensaje de refresco y, dependiendo de cómo se haya configurado, detectar un fallo tardará segundos o minutos antes de que puedan iniciarse las acciones de recuperación [28].

Ambos protocolos soportan re-enrutamiento (*re-enrutamiento*):

- RSVP-TE puede crear una nueva ruta a partir de un salto diferente en un LSR, así, en el momento en que se detecte el fallo refrescará esta nueva ruta que pasará a ser operativa y, la antigua se eliminará cuando deje de recibir mensajes de refresco.
- Otra alternativa que soportan ambos protocolos es crear una ruta completa alternativa mientras se usa la antigua, en el momento que se produzca un fallo la nueva ruta será operativa y se eliminará la antigua.

CR-LDP soporta que un LSP dé servicio a muchos *hosts* mediante la designación de FECs, mientras que RSVP sólo reserva ancho de banda a una única dirección IP.

La elección entre los diferentes protocolos se deberá a factores como la complejidad de la red, si las conexiones van a ser cortas o permanentes, qué grado de tolerancia a fallos se requiere, etc, por lo que actualmente no hay un consenso sobre si uno es superior tecnológico al otro [29].

REFERENCIAS

[1] MPLS: Una arquitectura de backbone para la Internet del siglo XXI, José Barberá

www.rediris.es/rediris/boletin/53/enfoque1.1.gif

[2] Ofreciendo Calidad de Servicio mediante MPLS:Fundamentos y aplicación a las redes de cable *Luis Gabriel Sienra*

www.aniret.org.mx/pdf/articulos/mpls.pdf

[3] MPLS

http://www.cisco.com/warp/public/732/Tech/mpls/

[4] Curso de Teleducación sobre MPLS, Fernando Alcober Bayo, Mayo 2001

www.fi.upm.es/~jgarcia/Curso_MPLS/capitulo3.html

[5] Curso de Teleducación sobre MPLS, Fernando Alcober Bayo, Mayo 2001

www.fi.upm.es/~jgarcia/Curso_MPLS/capitulo4.html

[6] Multiprotocol Label Switching. (MPLS), María Dolores Ferrer Martínez.

www.uv.es/~montanan/redes/trabajos/MPLS.doc

[7] Application Brief Cisco MPLS Tunnel Builder Objective and Audience

www.cisco.com/warp/public/732/Tech/mpls/docs/tbab.pdf

[8]MPLS (Implementing Cisco MPLS)

www.globalknowledge.com/training/course.asp?PageID=9&catid=206&courseid=2601&country=United+S

[9] Introduction To MPLS

www.riverstonenet.com/support/mpls/label_processing_and_values.htm

[10]Multiple Protocol Label Switching (MPLS) - A Control Plane View

www.ntu.edu.sg/home5/pg03053527/Research/MPLS_ControlPlaneView_Pub.ppt

[11] Multiprotocol Label Switching Architecture

http://www.rfc-editor.org/rfc/rfc3031.txt

[12] MPLS forwarding: ILM and NHLF tables

http://perso.enst.fr/~casellas/mpls-linux/ch07.html

[13] Multiprotocol Label Switching

www.ee.ust.hk/~eejie/mpls/mpls.PPT

[14] Extensión de los métodos Hop-by-Hop, CR-LDP y RSVP-TE para Multicast IP sobre MPLS, Yezid Donoso Meisel

http://eia.udg.es/~atm/bcds/pdf/ydonoso_clei2002.pdf

[15] MPLS multicast

http://www.fiuba6662.com.ar/6648/presentaciones/tordillo/Informe-htm-Tordillo/MPLS.htm

[16] Agregando más Valor a IP con Redes Orientadas a Conexión, Dan Proch, Ingeniero Líder, Estrategia de Tecnología y Arquitectura de Red de Marconi.

http://www.marconi.com/media/cala_ipconnection.pdf

[17] MPLS Pieza Clave para el Desarrollo de Servicios de Banda Ancha, Unitronics Comunicaciones, Octubre 2002, Adolfo García Yagüe

www.aslan.es/madrid2002/presentaciones/unitronics.ppt

[18] Curso de Teleducación sobre MPLS, Fernando Alcober Bayo, Mayo 2001

www.fi.upm.es/~jgarcia/Curso_MPLS/capitulo5.html

[19] MPLS-BGP based LSP setup techniques

http://csdl.computer.org/comp/proceedings/icn/2003/2037/00/20370279.pdf

[20] Label Distribution Protocol (LDP) is often used to establish MPLS

www.dataconnection.com/mpls/ldp.htm

[21] Label Distribution Protocol Transport

http://www.opalsoft.net/qos/MPLS-28.htm

[22]Two mode MPLS Label Distribution Protocol

http://cell.onecall.net/mhonarc/mpls/1997-Aug/msg00086.html

[23] LDP Specification

http://www.rfc-editor.org/rfc/rfc3036.txt

[24] Signaling in MPLS Networks With RSVP-TE - Technology Information

http://articles.findarticles.com/p/articles/mi_m0TLC/is_11_34/ai_67447072

[25] CR-LDP implementation in CISCO IOS

http://cell.onecall.net/mhonarc/mplsrc/2001-Jul/msg00154.html

[26] MPLS protocols family

http://www.protocols.com/pbook/mpls.htm

[27] Configuring MPLS Basic Traffic Engineering Using IS-IS

http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093fcb.shtml

[28] Advanced Topics in MPLS-TE Deployment

http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800a4472.shtml

[29] Protocolos de señalización CR-LDP en la Arquitectura MPLS y un análisis con simulación de calidad de servicio y prioridad de recursos, Ing. Rafael Bustamante Alvarez

http://electronica.unmsm.edu.pe/fie001/investigacion/Rev11/bustamante.pdf

CAPÍTULO 6

APLICACIONES DE MPLS

6.1. Calidad de Servicio en redes MPLS

La tendencia tecnológica actual consiste en la consolidación de los tipos de tráfico más importantes en el protocolo IP. Las soluciones de telefonía, videoconferencia y las aplicaciones científicas de banda ancha están cada día más solicitadas. Además, los flujos audio y vídeo corresponden a servicios en tiempo real. Por ello exigen tiempos de transporte muy cortos y una transferencia con muy poca inestabilidad, es decir, regular. Las aplicaciones tradicionales (web, correo electrónico, transferencia de archivos) admiten plazos más importantes pero, en cambio, requieren una tasa de pérdida de paquetes fiable. Junto a los servicios de punto a punto tradicionales también empiezan a aparecer servicios multipuntos, servicios de difusión y servicios de redes privadas virtuales para los que hay que gestionar la Calidad de Servicio (*QoS: Quality of Servicie*) [1].

El QoS y la CoS (*Class of Service*) permiten que el proveedor de servicios ofrezca niveles de servicio basados en paquetes IP diferenciados. QoS se refiere a la habilidad de una red para proveer mejores servicios a cierto tráfico seleccionado. En particular, las características de QoS proporcionan mejores servicios y más predecibles en la red a partir de lo siguiente:

- Ancho de banda dedicado
- Mejoramiento de características que producen pérdidas.
- Prevención y administración de congestión de la red
- Establecimiento de prioridades de tráfico a través de la red.

MPLS ofrece al entorno IP sin conexión un cierto control que convenía a las tecnologías basadas en las conexiones (Frame Relay ATM). Esta tecnología, basada en la conmutación de paquetes de datos en función de una etiqueta , añadida al encabezamiento, es flexible y ofrece múltiples posibilidades ya que una etiqueta puede caracterizar el camino, el origen, el destino, la aplicación, la calidad del servicio, etc. Algunos enrutadores analizan la cabecera de capa de red para seleccionar el siguiente salto y para determinar la preferencia o clase de servicio. MPLS facilita inferir la preferencia o clase de servicio desde la etiqueta.

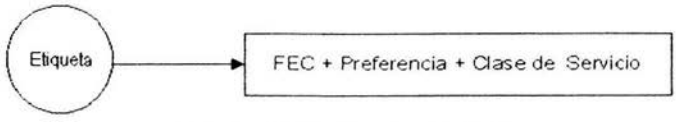


Figura 6.1.1. Calidad de Servicio en la etiqueta

El protocolo de reservación de recursos RSVP (Re*source Reservation Protocol)* es una propuesta muy polémica de QoS puesto que propone reservar los canales dedicados dentro de una red IP pública, estableciendo una conexión punto a punto. RSVP es un protocolo de señalización que para un flujo específico reserva recursos a lo largo de un camino entre el nodo origen y el nodo destino lo que le permite garantizar la Calidad de Servicio. Además a MPLS se le ha especificado el funcionamiento de los protocolos de señalización RSVP-TE y el CR-LDP para asegurar parámetros de Calidad de Servicio como por ejemplo la reserva de recursos y el retardo máximo podría experimentar una transmisión de un flujo de información sin afectar su calidad para un flujo de información, por lo que podemos decir que la QoS se obtiene reservando un ancho de banda en cada uno de los canales que conforman los distintos LSPs que conducen la información, lo que trae como consecuencia un mejor tiempo de transmisión [2].

En MPLS Cuando un paquete entra en la red, un enrutador frontera busca la dirección de destino del paquete y lo marca con una etiqueta que especifica la ruta y, opcionalmente, los atributos de la clase de servicio, es decir, MPLS utiliza etiquetas para determinar el siguiente salto del camino, de manera que los enrutadores realicen menos trabajo y puedan actuar como simples conmutadores. Según los paquetes marcados se adentran en la red, cada enrutador utiliza la etiqueta del paquete para seleccionar el destino y, opcionalmente, la CoS del paquete, en lugar de buscar el destino en las tablas de enrutamiento para cada paquete. Cuando el paquete sale del núcleo de la red, el enruteador frontera utiliza la dirección destino del paquete para enviarlo a su destino final. Los paquetes siguientes del mismo flujo son automáticamente etiquetados de esta forma y de esta manera se gana velocidad.

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

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

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

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

6.1.1 Clases de Servicio (CoS)

CoS (*Class of Service*) se refiere a los métodos que proporcionan servicios diferenciados, en los cuales la red entrega un tipo particular de servicio según la clase de servicio especificado en cada paquete. CoS provee diferentes categorías específicas de servicio . Los paquetes pertenecientes a una misma Clase de Servicio tienen en común los mismos requerimientos de tratamiento en cuanto a ancho de banda necesario, retardo, variación del retardo (*jitter*) y pérdida de paquetes, es decir, de Calidad de Servicio (QoS) [3].

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

IntServ (*Integrated Services*):

Apoyándose en RSVP, se reservan los recursos necesarios asociándose a LSPs concretos.

DiffServ (*Differenciated Services*):

Orientado al tráfico IP, 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 (Direfenciate Service). Esta es la técnica QoS de marcar los paquetes que se envían a la red. En la arquitectura de servicios diferenciados los paquetes se clasifican sólo en el dispositivo de acceso a la red y cuando estos están dentro de la red es en este momento cuando recibirán un trato distinto dependiendo del contenido del encabezado. Las funciones que deben de realizar los nodos de ingreso a la red y los nodos internos de la misma deben estar tanto especificadas como diferenciadas. Los primeros se encargan de la clasificación y de especificar el contenido del campo DS; al llegar un paquete a un enrutador frontera antes de pasar a un dominio DiffServ, es en este momento cuando hay que controlar, o marcar dichos paquetes, esto consiste en asignar un valor del campo "*codepoint* " DS, un valor especifico de la parte DSCP(*DiffServ Code Point*) del campo DS usado para seleccionar un PHB (*Per Hop Behaviour*), es decir, cada nodo intermedio tratará el paquete de la forma adecuada. A este comportamiento se le denomina PHB implementado mediante diferentes algoritmos de colas como PQ (*Priority Queuing*), WPQ (*Weighted Priority Queuing*) o WRR (*Weighted Round Robin*). Los nodos internos se encargan de reenviar los paquetes según el contenido del campo DS[41].

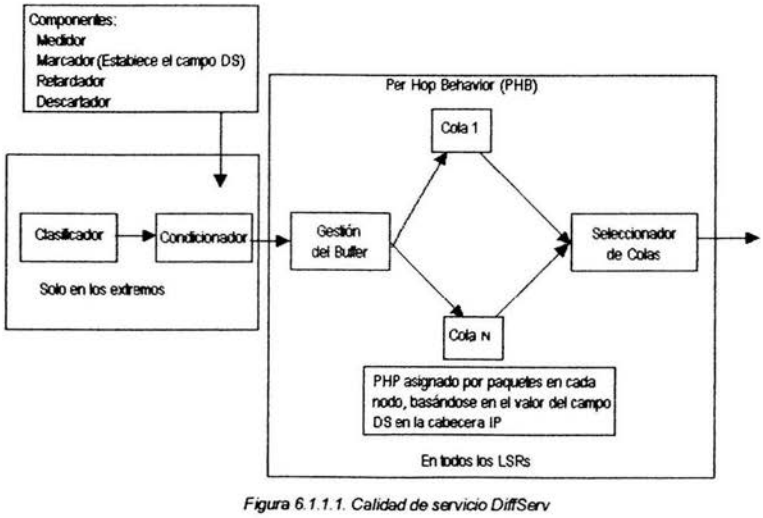


Figura 6.1.1.1. Calidad de servicio DiffServ

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas 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 frontera 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, en el cual se garantiza ancho de banda y establece límites máximos de retardo, otro para una prioridad media, no garantiza el cumplimiento de las limitaciones estrictas que garantizan la cobertura de las necesidades del tiempo real y un tercero para tráfico best-effort. Tres niveles de servicio, primera, preferente y turista, que lógicamente tendrán distintos precios. Por lo que podemos decir que diferentes clases de servicio requieren diferentes LSP[5].

CoS de MPSL soporta las siguientes servicios diferenciados en una red MPLS:

- Clasificación del paquete
- Evitar la congestión
- Gestión de la congestión

A continuación se describirán las CoS de MPLS y sus funciones [6]:

Servicio	CoS Función	Descripción
Clasificación del Paquete	CAR (Committed Access Rate). Los paquetes son clasificados en el nodo exterior de la red antes de ser etiquetado.	CAR usa los bits de ToS (Type of Service)de cabecera IP para clasificar los paquetes desacuerdo a la velocidad de transmisión de entrada y de salida. CAR es a menudo configurado en las interfaces exteriores de las para controlar el flujo del tráfico dentro y fuera la red. Se pueden usar comandos de clasifica para clasificar y reclasificar un paquete
Evitar la congestión	WRED (Weighted random early detection). Las clases de servicios son diferenciadas.	WRED monitorea el tráfico de la red para anticipar y prever cuellos de botella establecie umbrales para el descarte controlado de paquetes cuando la situación así lo requiere; WRED, también puede diferenciar la clases d servicios .

Gestión de la Congestión	WFQ (Weighted Fair Queueing). Los paquetes son diferenciados basándose en el ancho de banda requerido y las características de retardo.	WFQ usa prioridades para determinar la cantidad de ancho de banda que es asignada cada clase de tráfico.
	MDRR (Modified Deficit Round Robin) Para plataformas GSR .	MDRR es similar a al WFQ, da prioridad de tráfico para las diferentes clases de servicio, basándose en el valor de cada paquete.

Tabla 6.1.1.1 Clases de Servicio en MPLS y sus funciones

6.2. Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red tales como el ancho de banda global disponible y el balanceo de carga óptima, por lo que permite forzar a determinados paquetes a seguir una ruta particular, para encontrar el mejor camino para un determinado tipo de tráfico. 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, así evitando la congestión en cualquier camino [7].

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

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los enrutadores 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, es decir cuánto tráfico se cursa y de qué tipo. Con esta información se puede utilizar en la planificación de la red y como herramienta de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura y ofrezca un uso mas eficiente de la red .
- Permite hacer Enrutamiento 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, permitiendo así la reserva de enlaces para determinada clases de servicios [8].

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.

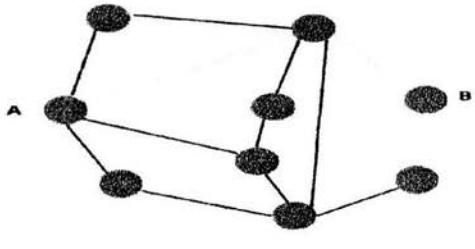


Figura 6.2.1. Ingeniería de Tráfico

Como mencionamos anteriormente la ingeniería de tráfico permite al proveedor hacer un mejor uso de los recursos y permitir reservar enlaces para determinadas clases de servicio o clientes.

Aquí encontramos el caso de las rutas forzadas. La ruta que un LSP puede 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[9].

Para calcular estas rutas existen dos métodos:

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

Los dos métodos pueden combinarse si en alguna parte de la ruta la información no está disponible.

Pero no basta sólo con obtener la ruta, es necesario reservar los recursos para poder satisfacer el servicio requerido.

Existen dos aproximaciones: RSVP-TE y CR-LDP, ambas utilizan el enrutamiento explícito para crear los LSPs e introducen una sobrecarga de información adicional al crear, mantener destruir un LSP, pero ésta, es mínima comparada con la generada al procesar la cabecera IP. Ver capítulo 5.4

6.3. Redes Privadas Virtuales basadas en MPLS

6.3.1 Definición de Red Privada Virtual

Una Red Privada Virtual, VPN (*Virtual Private Network*), es un sistema por el cual dos o más redes privadas están conectadas mediante una red pública, como Internet, lo que significa que es muy importante escoger un proveedor de servicio (ISP) de alta calidad.

Una VPN, es un túnel privado y seguro de comunicación entre una máquina individual y una red privada, o entre una LAN remota y una red privada. También puede ser vista como un sistema cliente servidor,

donde el servidor VPN puede ser software o hardware que actúa como un gateway en una red, está atento a la llamada de un cliente para conectarse con él y atender a su pedido. Un cliente VPN, en tanto es a menudo software, aunque podría ser una pieza de hardware también[10].

Esta conversación se inicia cuando el cliente VPN inicia una llamada al servidor VPN, éste lo autentica y si es aceptado entra en conexión con él, a partir de entonces queda establecida entre ambos una comunicación en una red virtual.

Adicionalmente, las VPNs monitorean su tráfico de formas muy sofisticadas que aseguran que los paquetes nunca sean alterados mientras viajen por la red pública.

Tunneling

Una VPN debe ser implementada utilizando tecnología de túneles, debido a que el túnel que conecta dos nodos terminales de una VPN es el elemento base del cual se parte y se construye los demás servicios VPN.

La tecnología de túneles (Tunneling), es una forma de transferir datos entre 2 redes sobre una red intermedia. Implica la encapsulación de un paquete de datos construido bajo el formato de determinado protocolo de red (IPX, NetBEUI, AppleTalk u otro) dentro del paquete de algún otro protocolo, en este caso TCP/IP [11].

En VPN se añade otra característica a la encapsulación: la encriptación, la cual asegura que los paquetes de datos enviados sean ilegibles para los extraños. Estos paquetes encapsulados y encriptados viajan a través de la red pública hasta que alcanzan su destino, ya ahí, los paquetes se separan y vuelven a su formato original.

Una de las principales razones del despliegue de MPLS en proveedores de servicios y redes empresariales son los servicios de VPNs .

Por lo anterior definimos una red privada virtual como una red en la que la conectividad entre múltiples lugares se realiza a través de una infraestructura compartida con las mismas políticas de acceso y seguridad que en una red privada. Una compañía en la que su intranet corra encima de un servicio de VPN tendrá la misma seguridad, fiabilidad, etc, que el resto de sus redes privadas. Por tanto, el objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables.

Las Redes Privadas Virtuales (VPN's) permiten unificar en una sola red todos los accesos externos, reducen notablemente los costes empresariales, proporcionan mayor valor añadido, facilitan el acceso a internet y generan ventajas competitivas.

Las dos características más importantes de una VPN desde el punto de vista del usuario son la seguridad y la privacidad.

Las primeras WANs usaban líneas dedicadas y alquiladas para realizar sus conexiones. Estas redes tienen el inconveniente de ser caras, debido a la necesidad del alquiler de las líneas. Posteriormente, con la introducción de las VPNs, se pueden conectar múltiples sitios usando la espina dorsal (backbone) de un proveedor de servicios. Dicho proveedor ofrecerá servicios VPN a un precio inferior que con líneas dedicadas ya que el proveedor de servicios podrá utilizar los recursos de su espina dorsal de forma compartida para múltiples clientes. Estas tecnologías de VPN se basaban fundamentalmente en protocolos de capa de red, típicamente Frame Relay, si bien también X.25.

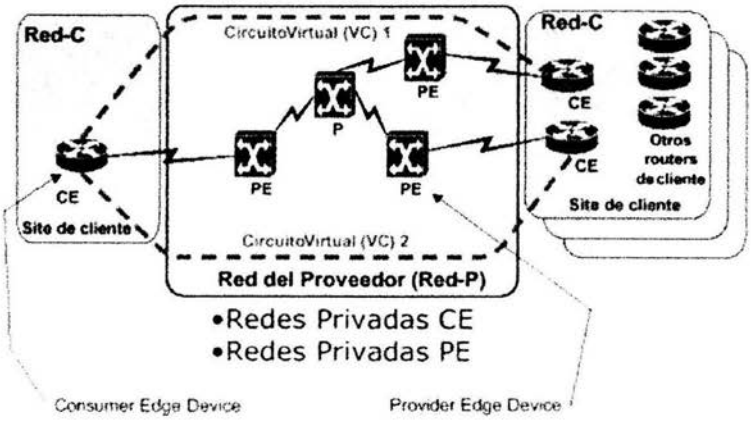


Fig. 6.3.1.1. Principales elementos de una Red Privada Virtual (VPN)

Debido a que las soluciones existentes de aquel entonces no eran compatibles surgió un gran interés por las redes privadas virtuales basadas en IP que funcionaran en la red de redes (Internet) y que utilizaran estándares que funcionaran a través de múltiles proveedores de servicios. De esta forma se consigue

una mayor flexibilidad en el diseño e implantación con unos menores costes de gestión y provisión del servicio. La forma de conseguir VPNs IP es construyendo túneles IP de diversos modos. El objetivo de un túnel IP es crear una asociación permanente entre dos extremos de modo que funcionalmente parezcan conectados.

El inconveniente de este tipo de soluciones es que:

- Están basadas en conexiones punto a punto.
- La configuración es manual: una nueva conexión supone alterar todas las configuraciones.
- Plantean problemas de crecimiento.
- La gestión de la QoS es posible pero costosa.

6.3.2. MPLS VPN

El problema que plantean las VPNs IP es que están basadas en el modelo superpuesto, por lo que el número de adyacencias es elevado y la escalabilidad limitada. Con MPLS se solucionan estos problemas, puesto que tendremos un modelo acoplado.

Las VPNs MPLS se basan en el uso de túneles LSP para el reenvío de los datos entre los enrutadores frontera de un proveedor de servicios. Al etiquetar los datos que entran en la VPN, un LSR podrá separar los flujos VPN del resto de los datos que fluyen por la espina dorsal del proveedor de servicios.

La tecnología emergente MPLS promete potenciar el mercado de servicios de red privada virtual (VPN) y el rendimiento de las troncales IP .

Aunque ATM puro tiene la seguridad y el rendimiento requeridos, carece de una base instalada crucial. La unión de IP y ATM abriría el mercado VPN, pero sólo si se garantiza una característica clave: creación de VPN de forma automática que reduzca el alto coste que supone su despliegue a gran escala . MPLS proporciona este método automático crítico, fusionando las ventajas de IP y ATM para hacer posible el despliegue con éxito de VPN .

MPLS es una tecnología diseñada para acelerar el tráfico a través de redes de routers. Cisco Systems, Ascend Communications, Hughes Network Systems y Lucent Technologies, entre otros fabricantes, ya

han adoptado recientemente la norma para soportar intranets IP y VPN que requieran retardos de red limitados .

Cisco lanzó el más amplio portafolio en la industria de tecnología que habilitan los servicios administrados centralmente de VPNs sobre MPLS. Estas nuevas tecnologías están incluidas en el software Cisco IOS y ofrecen mayor simplicidad y funcionalidad para arquitecturas MPLS VPN [12] .

MPLS fusiona la seguridad y garantía de rendimiento de los circuitos virtuales con el direccionamiento IP global y conectividad bajo demanda mediante la automatización de la creación de circuitos virtuales para servicios VPN. Sobre redes Frame Relay o ATM, MPLS crea caminos basándose en la actual tecnología de circuito virtual. En redes IP puras, tales como paquetes sobre SONET (*Synchronous Optical Network*) , la norma inserta una cabecera MPLS en frente de la cabecera IP creando un camino directo a través de la red IP . Estos caminos MPLS proporcionan los beneficios de los circuitos virtuales sobre una infraestructura mixta IP/ATM/Frame Realy.

6.3.3. Ventajas de MPLS VPN

En los últimos tiempos, no sólo se viene hablando de la famosa convergencia de voz, video y Datos sobre una misma plataforma, sino también de la necesidad de la migración de servicios "Legacy" (heredados) como ATM o Frame Relay a una nueva generación de Redes Privadas Virtuales basadas en protocolo IP como los son las "MPLS VPNs" (*Redes Privadas Virtuales basadas en Multiprotocol Label Switching*).

Sin embargo, resistencia sigue siendo la primera palabra que se asocia cuando se habla de "cambios", mucho más aún, cuando se trata de migraciones de servicios de comunicaciones, críticos para una empresa.

A continuación, encontraremos 10 razones claves para hacer frente a la mencionada "resistencia" a los cambios cuando una empresa, corporación u organismo este pensando en migrar su infraestructura Legacy actual a una IP-Based MPLS VPN

1 - Flexibilidad.

Cada empresa, corporación u organismo tiene desarrollada su propia estructura interna, tanto en infraestructura como en recursos humanos, generadas en base a sus necesidades y recursos disponibles. En base a ésta estructura, muchas veces única, se montan los servicios de comunicaciones para acomodar de la mejor manera posible y al menor costo, el transporte de la información interna, así como también externa, con sus clientes y proveedores.

La topología de una MPLS VPN puede acomodarse acorde a cada necesidad, dada su naturaleza que brinda conexiones "Any-to-Any" (cualquiera con cualquiera) entre los distintos puntos que comprenden la VPN, contando así con el mejor camino o ruta entre cada punto. A su vez se puede obtener mayor flexibilidad realizando configuraciones híbridas con Hub-and-Spoke (estrella), por ejemplo en las conexiones con clientes [13].

2 - Escalabilidad

Con un nuevo concepto de aprovisionamiento, llamado "Point-to-Cloud" (punto a la nube), se implementan los nuevos puntos de la VPN. Este concepto proviene del hecho de que cada vez que sea necesario "subir" un nuevo punto a la VPN, sólo habrá que configurar el equipamiento del proveedor de servicio que conecte este nuevo punto. De esta forma, evitamos tareas complejas y riesgosas, como las que se producen cuando se activa un nuevo punto en una red basada en circuitos virtuales de Frame Relay o ATM, en donde es necesario re-configurar todos los puntos involucrados.

3 - Accesibilidad

La arquitectura de MPLS VPN permite utilizar prácticamente todos las tecnologías de acceso para interconectar las oficinas del cliente con su proveedor de servicios.

Por dicho motivo, la versatilidad que nos permite utilizar xDSL o un enlace Wireless Ethernet en las oficinas más pequeñas y hasta incluso en usuarios móviles, mientras que en el headquarter utilizamos leased lines (TDM) en altas capacidades como E3/T3, nos permite dimensionar cada punto de la VPN acorde a sus necesidades sin limitar o restringir la de otros puntos.

IFX Networks posee acuerdos de interconexión con proveedores líderes de Estados Unidos, Europa y Asia para extender su cobertura de servicios MPLS VPN a cualquier lugar del planeta.

4 - Eficiencia

En una infraestructura 100% IP, es decir, aquellas empresas en donde todo el equipamiento involucrado y las aplicaciones utilizadas son IP, el uso de servicios de transporte ATM o Frame Relay someten al cliente a incurrir en un costo adicional por el overhead que los protocolos de transporte introducen. Mediante MPLS VPN un servicio IP basado en VPN el costo extra desaparece.

5 - Calidad de servicio (QoS) y Clases de servicio (CoS).

Las necesidades de comunicación entre dos lugares remotos, hoy en día van mucho más allá de la simple transferencia de datos vía email, web u otras aplicaciones. Siendo incluso insuficiente muchas veces, la interesante combinación de voz y datos bajo una misma plataforma. Es por esto, que la ya mencionada convergencia de datos con aplicaciones tiempo real y/o interactivas, voz y también video de alta calidad, necesitan de una eficiente plataforma de transporte.

Mediante la utilización de técnicas y herramientas de Calidad de Servicio (QoS), se ofrecen distintas Clases de Servicio (CoS) dentro de una MPLS VPN para cumplimentar los requerimientos de cada servicio o aplicación.

6 - Administración.

Las MPLS VPN son denominadas Network-Based, ésta característica proviene del hecho en que el servicio es implementado sobre la infraestructura del proveedor de servicio; implicando, entre otras cosas, que la administración de enrutamiento es llevada a cabo por el proveedor de servicio; quien por su naturaleza, es especialista en dicha tarea desligando así al cliente de llevarla a cabo.

7 - Monitoreo y SLAs

Las MPLS VPN son monitoreadas, controladas y con un constante seguimiento en forma permanente, las 24 horas los 7 días de la semana, por parte del proveedor de servicio. Además, se extienden acuerdos de nivel de servicio para garantizar y asegurar la estabilidad y performance que el cliente necesite.

8 - Fácil Migración

La simplicidad de la tecnología determina que las tareas de aprovisionamiento, administración y mantenimiento sean actividades sencillas para el proveedor de servicio; lo cual se traslada directamente al cliente, obteniendo una migración del servicio actual sin complicaciones.

9 - Seguridad

Análisis y estudios realizados por los distintos fabricantes y entidades especializadas en el área, determinaron que los niveles de seguridad entregados por una MPLS VPN son comparables con los entregados por los circuitos virtuales de Frame Relay y ATM.

Sin embargo, en escenarios donde estos niveles no son suficientes, como por ejemplo en las necesidades de entidades financieras, una MPLS VPN puede también ser combinada con la encriptación y autenticación que IPSec brinda, elevando aún más la seguridad de la VPN.

10 -Bajo Costo

Son varios los motivos que permiten afirmar que un servicio MPLS VPN ofrece "más por menos", entre ellos podemos destacar:

- Independencia de equipos de cliente (CPE). La implementación de la VPN no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente.
- Se puede integrar distintos servicios y aplicaciones sobre una misma plataforma.

De este modo, empresas que al día de hoy mantienen distintos y costosos servicios para soportar sus necesidades de voz, datos y video; pueden unificar estos requerimientos concluyendo en un ahorro significativo y manteniendo relación con un único proveedor de servicios.

REFERENCIAS

[1] MPLS valor añadido para la interconexión
Revista de telecomunicaciones de Alcatel.-tercer trimestre 2002.- Hoebeke, M. Aïssaoui, T. Nguye, pag 8

[2] Agregando más Valor a IP con Redes Orientadas a Conexión, *Dan Proch, Ingeniero Líder, Estrategia de Tecnología y Arquitectura de Red de Marconi.*
http://www.marconi.com/media/cala_ipconnection.pdf

[3] MPLS: Convergencia entre el nivel de transmisión y el nivel de enrutamiento, Ana Gonzalez
www.coitt.es/antena/pdf/150/11b_Internet.pdf

[4] Cisco IOS MPLS Quality of Service
http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800a4455.shtml

[5]Servicios Diferenciados y MPLS, Santiago Felici
www.cic.teleco.ulpgc.es/rst/publicaciones/umtsoverip/UMTS%20sobre%20IP.ppt

[6]MPLS Class of Service
http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a00800e977a.html

[7] Traffic Engineering with MPLS
http://safari.ciscopress.com/?XmlId=1-58705-031-5

[8] Advanced Topics in MPLS-TE Deployment
http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mwglp_wp.htm

[9] Traffic Engineering With Multiprotocol Label Switching
www.avici.com/technology/whitepapers/mpls_wp.pdf

[10] Introducción to MPLS VPN Technology. Cisco VPN Solution Center Software, 2002.
http://www.cisco.com/en/US/products/sw/netmgtsw/ps23277products_technical_reference_chapter09186a0080087c9c.html

[11] MPLS and VPN architecture, Jim Guichard y Ivan Pepelnjak; Cisco Press, EU, 2002, Capítulo 8, pp 145-163.

[12] Redacciòn Virtual, CISCO Systems.
http://www.ciscoredaccionvirtual.com/redaccion/titulares/default.asp?Id=225.

[13] Razones para migrar a MPLS.

www.ifxnetworks.com/document/10razones_mpls.pdf - 20 Sep 2004

CAPÍTULO 7

7. TENDENCIAS EN EL MERCADO DE MPLS

7.1. Redes ópticas basadas en MPLS

Desde 1995 se ha producido un aumento dramático en el tráfico de datos, debido principalmente al crecimiento explosivo de Internet así como a la proliferación de Redes Privadas Virtuales (VPNs). Poco antes de finalizar el milenio, el volumen de tráfico de datos a nivel mundial sobrepasaba al tráfico de voz y continuará aumentando en los próximos años. Al mismo tiempo se aumenta la demanda por parte de los clientes de mantener bajo el coste de acceso. Estos factores dan lugar a una situación en la que los proveedores de servicio necesitan soluciones que les permitan transportar un gran volumen de tráfico de la manera más eficiente posible en cuanto al coste. Las redes ópticas en la actualidad presentan un gran número de capas, para solucionar este tipo de problemas. Cada una de estas capas está preparada para manejar un determinado tipo de tráfico y proporcionar unos servicios específicos. Con el tiempo han surgido incluso equipos independientes que están especializados en una capa y en un tipo de tráfico como por ejemplo: enrutadores IP, conmutadores ATM, dispositivos SONET/SDH o conmutadores DWDM (*Dense Wavelength-Division Multiplexing*). Sin embargo MPLS para solucionar este problema, se extiende como GMPLS(*Generalized Multiprotocol Label Switching*), el cual logra reducir estas capas al conmutar servicios y transporte sobre una única infraestructura óptica, por lo que es capaz de manejar simultáneamente tráfico de paquetes, TDM y longitudes de onda a velocidades ópticas, en una solo fibra.

7.1.2. Qué es GMPLS

GMPLS (*Generalized Multiprotocol Label Switching*), es una extensión de MPLS para redes ópticas. El LSR es ahora un OXC (*cross-connects*),Conector Cruzado Óptico y las etiquetas utilizadas son longitudes de onda.

GMPLS tiene una completa serie de capacidades que pueden utilizarse para unir diversas partes de la red diseñadas para transportar múltiples tipos de tráfico. La figura 7.1.2.1 representa esquemáticamente la jerarquía de interfaces conmutados de GMPLS. De este modo, sobre una misma fibra podemos

transportar simultáneamente longitudes de onda opacas o transparentes, canales SONET/SDH y paquetes IP, conmutando y gestionando todos estos servicios en los nodos ópticos de una forma completamente flexible.

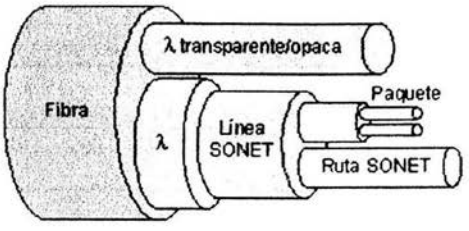


Figura 7.1.2.1.Jerarquía de interfaces conmutados de GMPLS.

Los expertos aseguran que la arquitectura de red óptima estaría basada en dos capas: una capa de enrutamiento IP y una capa de transmisión óptica (Figura 7.1.2.2). En esta red los enrutadores toman decisiones sobre los paquetes, mientras que la capa de transmisión proporciona rutas de conexión flexibles entre estos enrutadores. Los nodos de transmisión, tales como OXCs, se encargan de las labores de conmutación entre las fibras, longitudes de onda individuales, o incluso ranuras temporales del interior de las longitudes de onda. La conexión entre las capas IP y óptica se realizaría mediante GMPLS [1].

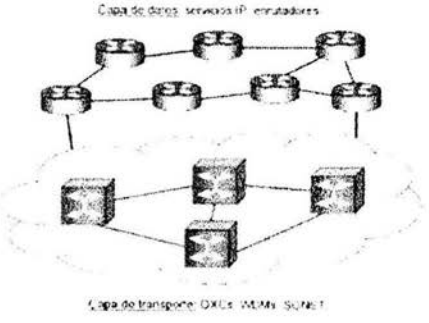


Figura 7.1.2.2. Modelo de red óptica basado en 2 capa

Este planteamiento de separar el enrutamiento y el transporte óptico resulta bastante lógico, aunque algunas personas argumentan que en un futuro la red se consolidará en una única capa completamente óptica.

Mientras las capacidades de los enrutadores y OXCs aumentan rápidamente, las altas tasas de datos del transporte óptico sugieren la posibilidad de eliminar las capas SONET/SDH y ATM. Para llegar a este punto los routers, OXCs y DWDMs deben implementar las funciones necesarias de dichas capas.

Como resultado final obtendremos una red más sencilla y eficiente en coste que transportará un amplio rango de flujos de datos y volúmenes de tráfico muy elevados.

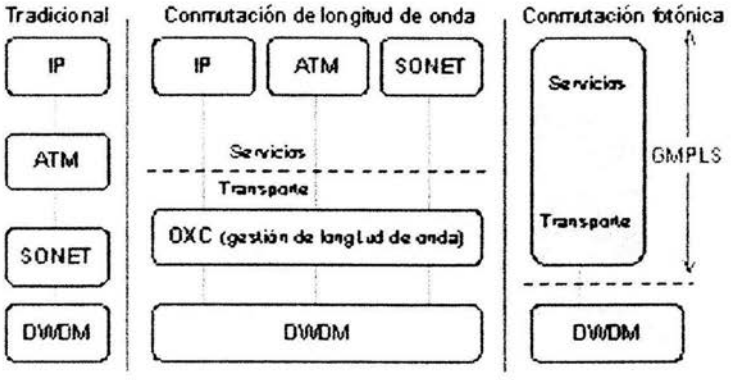


Figura 7.1.2.3 Evolución del modelo de capas

En los últimos años el enrutamiento IP ha evolucionado para incluir nuevas funcionalidades desarrolladas en la arquitectura MPLS. Recientemente se ha extendido MPLS como un plano de control que puede utilizarse con nuevos dispositivos como los OXCs.

Esta generalización proporciona el plano de control común estandarizado necesario en la evolución de redes ópticas abiertas e interoperables. En primer lugar, un plano de control común simplifica las operaciones y la gestión, lo que reduce el coste de las operaciones. En segundo lugar, un plano de control común proporciona un amplio rango de escenarios de desarrollo.

7.1.3. Diferencias entre MPLS y GMPLS

GMPLS difiere básicamente de MPLS en que él soporta básicamente múltiples tipos de tráfico (TDM, lambda, fibra). Para incluir estos tipos adicionales de conmutación se han extendido ciertas funciones base de MPLS. Estos cambios y añadidos afectan a las propiedades básicas de los LSP, a cómo se solicitan y comunican las etiquetas, a la naturaleza unidireccional de los LSPs, a cómo se propagan los errores y a la información proporcionada para sincronizar los LER de entrada y salida (frontera) [2].

La arquitectura original de MPLS se ha extendido para incluir un nuevo conjunto de interfaces en los LSR. Estas interfaces se clasifican en:

1. Interfaz PSC *(Packet-Switch Capable)* Representa la MPLS tradicional. Son interfaces que reconocen los límites de células y paquetes y pueden enviar información basada en el contenido de sus cabeceras. Ejemplos incluyen interfaces en enrutadores que envían información basada en la cabecera «*shim*», o interfaces sobre ATM-LSRs que envían información basada en los VPI/VCI de ATM.

2. Interfaces L2SC (Layer-2 Switch Capable). Estas interfaces reconocen los límites de tramas/celdas y pueden enviar datos basándose en el contenido de la cabecera de las tramas/celdas.

3. Interfaz TDM *(Time- Division Multiplex Capable)* Son interfaces que envían información basada en el IT (Intervalo de Tiempo) asignado (cíclico). El ancho de banda de una fibra puede ser dividido en IT. Aquí la señal óptica es vista como una secuencia de tramas de información, con «N» tramas cada una de tamaño «t» viajando cada segundo «S» (el ancho de banda total de la fibra es NxS), y entonces el ancho de banda se asigna a un flujo particular, simplemente reservando una porción de cada trama. Un ejemplo de tal interfaz es aquella sobre un *crossconnect* de SDH/SONET. Los tamaños de las tramas básicas y sus jerarquías por medio de las cuales las tramas pueden ser divididas en IT son el tema de los estándares de Jerarquías Digitales Sincrónicas.

4. Interfaz LSC *(Lambda-Switch Capable)* Son interfaces que envían información basada en la longitud de onda sobre la que ella es recibida. Dentro de una fibra, su ancho de banda disponible puede ser dividido por frecuencia (longitud de onda o lambda). Un OXC puede operar a niveles

de longitudes de onda individuales, y este OXC pudiera conmutar toda la información que viene en la longitud de onda «A» de la fibra entrante, hacia la longitud de onda «B» de la fibra saliente.

5. Interfaz FSC *(Fiber-Switch Capable)* Son interfaces que envían información basada en la posición física espacial que ésta tiene. Un ejemplo de esta interfaz es la de un OXC que pueda operar a nivel de una o varias fibras. Aquí toda la información que arriba en una fibra (entrante) es conmutada para ser trasmitida hacia otra fibra saliente. Un circuito se puede establecer únicamente entre, o a través de interfaces del mismo tipo. Dependiendo de la tecnología usada por la interfaz, puede recibir diferentes nombres: circuito SDH, *optical trail, light path*, etc. En el contexto de GMPLS, todos estos circuitos representan los LSPs. Otras características a ser tomadas en cuenta por las redes ópticas es la señalización fuera de banda, la jerarquización de los LSPs, su bidireccionalidad, y el concepto de la interfaz OUNI

La arquitectura de MPLS se ha definido para soportar el envío de Información basado en una etiqueta; en este sentido, se asume que los LSRs tengan un plano de envío que sea capaz de
(a) reconocer límites de células y de paquetes, y (b) poder procesar estas cabeceras. Esta arquitectura original se ha extendido recientemente para incluir LSRs cuyos planos de envío y la decisión tomada esté basada en IT (Intervalo de tiempos). Por otro lado el ancho de banda disponible en una red óptica es más parecido al de un sistema de trenes, en los cuales éstos parten a intervalos regulares, y cualquier persona que desee viajar en ellos (información enviada) debe reservar un asiento (longitud de onda o IT). Una vez que se reserva este asiento, el viaje es completamente confiable y no hay posibilidad de congestión [3].

7.1.3.1.Etiquetas en Redes Ópticas

Se añade una etiqueta de longitud de onda a cada flujo de bits y cada paquete IP se acomoda en una determinada ruta de longitud de onda en el enrutador de entrada. El mecanismo de ruta por longitud de onda consiste en reservar una determinada longitud de onda para una ruta desde el enrutador de entrada hasta el de salida. Otra posibilidad consiste en una ruta de longitud de onda virtual, según la cual se cambia la longitud de onda tras cada enlace.

A diferencia de las etiquetas *no* generalizadas (MPLS), en la cual cada paquete está marcado,

ahora los paquetes de información, en GMPLS, no presentan ninguna marca de etiqueta, en vez de esto, «el valor de la etiqueta» se encuentra implícito en el hecho que la información es transportada dentro de una banda de frecuencia acordada, ésta es» la etiqueta». G-MPLS extiende así el concepto de etiqueta, de un número de 32 bits, a un arreglo de bytes de longitud variable e introduce mejoras, como ya se ha mencionado, en los protocolos de enrutamiento: OSPF (*Open Shortest Path First Internet Routing Protocol*) e IS-IS (*Intradomain Routing Protocol*), para que los OXCs puedan intercambiar información sobre la topología de la red, estado de enlaces y cualquier otro dato referente a disponibilidades de recursos ópticos. También se introducen mejoras en los protocolos de señalización «RSVP» y «LDP» para así ayudar en los procesos de establecimiento de conexiones, a este efecto se introducen los conceptos de «Objeto de Etiqueta Generalizada» *(Generalized Label Object en RSVP)*, y «TLV de Etiqueta Generalizada » *(Generalized Label TLV en CR-LDP)*. A continuación las etiquetas generalizadas:

- Etiquetas para fibras *(Whole Fiber Labels)*. Un enlace entre LSRs puede consistir de un conjunto de fibras ópticas. En este caso el valor de la etiquetes el número de la fibra seleccionada dentro del conjunto. La interpretación del número de fibra/puerto tiene únicamente significado local entre los LSR directamente involucrados.

- Etiquetas para lambdas *(Wavelength Labels)*. En fibras donde exista WDM, un LSR óptico puede escoger una lambda para cursar un tráfico. En este caso, el valor de la etiqueta es el de la lambda seleccionada.

- Etiquetas para conjuntos de lambdas *(Waveband Labels)*. Si se agrupan longitudes de onda consecutivas dentro de una banda *(waveband)*, de tal forma que todas puedan ser conmutadas de la misma forma, el valor de la etiqueta es un número que identifica a esta banda *(waveband ID)*, y existe un par de números (identificadores de canal) que identifican las lambda extremos de esta banda.

- Etiquetas para IT *(Timeslot Labels)*. En fibras donde su ancho de banda esté dividido en IT, por TDM, un conmutador óptico puede usar uno o más IT para cursar un tráfico. El valor de etiqueta TDM será suficiente para especificar el IT asignado. Una etiqueta SDH/SONET está representada por una secuencia de 5 números (S, U, K, L, M), los cuales seleccionan diferentes partes de la jerarquía en cuestión. Para todos los tipos de etiquetas G-MPLS descritas aquí, el valor de la etiqueta directamente implica el ancho de banda disponible para el tráfico en particular. Es decir, si una etiqueta denota un simple VT-6 de SONET, entonces el ancho de banda disponible es el de un intervalo VT-6, el razonamiento es similar para los otros tipos de etiquetas.

7.1.3.2. Solicitando etiquetas generalizadas para una conexión

La filosofía utilizada en MPLS para lograr acuerdo de valores de etiquetas, previo al establecimiento de un LSP, básicamente no varía en las redes ópticas:

El LSR inferior envía una respuesta al LSR superior *(Resv)* en RSVP o *(Label Mapping)* en CRLDP, el cual comunica el valor de etiqueta seleccionado. GMPLS generaliza este mensaje de solicitud de conexión por dos razones: 1) para distinguirlo de una solicitud no generalizada, y 2) para permitirle el llevar parámetros adicionales.

En RSVP se hace esto a través del «Objeto de Solicitud de Etiqueta Generalizada», en vez del «LABEL_REQUEST» en el *Path message*, y en CR-LDP añadiendo un «TLV de Solicitud de Etiqueta Generalizada» al *Label Request message*.

Algunas informaciones que necesita el Rd para asignar la etiqueta apropiada, ya se encuentra implícita en el contexto, pero es necesario sin embargo, que el LSR superior especifique el «Tipo de Codificación LSP» *(LSP encoding type)*, el cual especifica que la etiqueta a ser usada deba ser un IT, o un lambda, u otra cosa. Este campo soporta los siguientes valores:

- ANSI PDH
- ETSI PDH
- SDH
- SONET
- DIGITAL WRAPPER
- LAMBDA
- FIBRA

Ya que algunos enlaces pueden anunciar, a través del IGP, su capacidad para soportar más de un tipo de tráfico, el «Objeto de Solicitud de Etiqueta Generalizada/ TLV» contiene un campo que indica el modo de tráfico que se aplica a un LSP particular: fibras, lambdas, etc. En el caso de etiquetas SDH/SONET, puede ser necesario solicitar que el BW total para un LSP sea dividido en múltiples IT, entonces cuando el «Tipo de Codificación LSP» es SDH o SONET, la «solicitud de etiqueta generalizada» lleva campos adicionales que especifican cuántos IT se deben combinar para satisfacer la solicitud *(Requested*

Number of Components, RNC field), y cómo estos IT deberían ser concatenados, incluyendo la información si deberían ser contiguos *(Requested Grouping Type, RGT field)* [4].

7.1.3.3. Características de desempeño en GMPLS

Las características de desempeño de las redes ópticas, a menudo, son muy diferentes de las de las redes de tráfico de paquetes no ópticas, para el cual fue desarrollado originalmente MPLS, ya que:

1. El tiempo necesario para establecer un LSP óptico puede ser mayor que el correspondiente para un LSP no óptico, debido más que todo a la mecánica del HW del Tráfico óptico. Los conmutadores ópticos pueden ser relativamente lentos para programar. Aunque el tiempo para seleccionar y ajustar los componentes de tráfico puede ser muy rápido, el tiempo tomado por estos componentes para estabilizarse después de su programación puede ser mucho mayor (medido en milisegundos). Por ejemplo, un microespejo puede ser programado rápidamente, pero este espejo puede tomar décimas de milisegundos para estabilizarse y parar de vibrar después de su ajuste, entonces no es nada confiable para un LSR el que envíe una señal de respuesta hacia su vecino LSR superior mientras el espejo esté vibrando, ya que de repente el LER de entrada pudiera de inmediato comenzar a enviar información, y ésta pudiera ser conmutada incorrectamente o perdida, de permanecer algo de esta vibración en el espejo [5].

2. Las redes ópticas son particularmente estables, una vez que un LSP a través de una red óptica se ha establecido, es probable que permanezca así por un tiempo prolongado.

3. De fallar el enlace óptico, la discrepancia entre velocidades (mensajes de señalización contra información) hace que los métodos tradicionales de recuperación de enlaces en MPLS, no sean los más apropiados.

4. El concepto de LSPs jerárquicos o sea, LSP dentro de otro LSP, ya disponible en el MPLS tradicional, permite aquí, en GMPLS, el poder construir una verdadera jerarquía de envío, es decir, una jerarquía de LSPs. Esta jerarquía de LSPs puede ocurrir sobre una misma interfaz, o entre diferentes interfaces.

5. En la parte superior de esta jerarquía se encuentran las interfaces FSC, seguida por las LSC, las TDM, y luego las PSC. De esta manera un LSP que comienza y termina en una interfaz PSC, puede estar incluido dentro de otro LSP que comienza y finaliza en una interfaz TDM. Este LSP, a su vez,

pudiera estar incluido (en conjunto con otros LSPs) dentro de otro LSP que comienza y termina en una interfaz LSC, éste a su vez se puede incluir dentro de otro LSP que comienza y termina en una interfaz FSC.

6. El plano de control de GMPLS está compuesto de bloques funcionales relacionados con protocolos de enrutamiento y señalización actualizados. Existe también un protocolo especializado para dar soporte a la gestión de las operaciones de GMPLS, este es el LMP *(Link Management Protocol)*. LMP se desempeña entre los nodos del plano de información *(data- plane)*, y es usado tanto para aprovisionamiento de enlaces, como para aislamiento de fallas Igualmente son necesarias las extensiones a los algoritmos y protocolos de enrutamiento para codificar y poder llevar informaciones referidas a «ingeniería de tráfico» TE (*Traffic Engineering*), así como también para la formación de rutas explícitas [6].

Además la señalización debe ser ahora capaz de transportar parámetros del circuito requerido (LSP), tales como ancho de banda, tipo de señal, protección deseada, su posición en un múltiplex particular, etc. GMPLS extiende estos conceptos hacia TDM, LSC y FSC. También GMPLS extiende los dos protocolos de señalización definidos para MPLS-TE: RSVP-TE y CR-LDP. GMPLS, sin embargo no especifica cuál de estos dos protocolos de señalización debe ser usado. Esto se deja en manos de los fabricantes y operadores, según los intereses respectivos. Ya que GMPLS está basada en RSVP-TE y CR-LDP, debe usar una distribución y asignación de etiquetas bajo demanda en sentido descendente, con un control ordenado iniciado en su Ingreso.

Bidireccionalidad

En las especificaciones originales de MPLS, las conexiones bidireccionales requerían el establecimiento de dos LSPs unidireccionales, y esto implica una cierta coordinación entre los dos puntos en cuestión. Temas relacionados con la gestión de los mensajes y protocolos de señalización, el hecho de construir las dos direcciones utilizando trayectos totalmente diferentes, así como la coordinación de estos dos LSPs unidireccionales, que de hecho, conformaban un circuito, son muy delicados. Se logró, a tal efecto, algunas mejoras, pero aún existía el tema pendiente de que se necesitaban 4 mensajes de señalización (solicitud y respuesta en cada sentido) para el establecimiento del LSP [7].

G-MPLS extendió y mejoró este concepto, necesitando un sólo mensaje para el establecimiento de este LSP bidireccional. Esto trae obviamente como beneficio el requerir menos señalización y mejor coordinación entre las dos direcciones de flujo.

En este caso, se define al *head end* del LSP como el «iniciador » o nodo de ingreso, y el *tail end* como el «terminador» o nodo de egreso.

Aquí, G-MPLS introduce un nuevo «objeto» en la solicitud de establecimiento de un LSP, el cual es la *«Etiqueta Ascendente» (Upstream Label).* Ésta permite que un Rp señalice al Rd, cuál debería ser la etiqueta que debería tener el sentido ascendente (es decir, del terminador hacia el iniciador).

7.2. Red de Constelaciones Satelitales basadas en MPLS

Los satélites ya son muy utilizados actualmente para proporcionar servicios de datos basados en IP, especialmente a zonas remotas cuya infraestructura terrestre es limitada.

La convergencia de voz y datos cobra por tanto sentido también en redes por satélite, debido a que los satélites tradicionales se utilizan como simples repetidores de información entre lugares fijos. Por otro lado, las redes satelitales emergentes con múltiples haces de transmisión (spot beams) y procesamiento abordo (OBP) tendrán nuevas capacidades para enrutar dinámicamente la información entre los distintos haces.

Por tanto, los satélites geoestacionarios (GEO) pueden proporcionar transporte a aplicaciones en tiempo real como la telefonía IP, que es particularmente sensible al retardo y a su variación (jitter).

En internet, los retardos de los paquetes pueden depender de la carga de la red. El enrutado de tráfico por satélite puede reducir el numero de enrutadores intermedios, aunque el retardo de propagación en satélites GEO puede aumentar considerablemente el retardo total, al rango de 250-270 ms. Es un verdadero reto de ingeniería el implementar aplicaciones en tiempo real, como la telefonía IP sobre satélites, ofreciendo la calidad de servicio requerida [8] .

ATM sería un interesante candidato, para la topología de las redes satelitales debido a su concepto de VP/VCI y a que proporciona diferentes niveles de calidad de servicio, debido a que se basa en el paradigma de orientado a conexión.

Desafortunadamente, la más dominante de las conexiones, IP no provee mecanismo para ingeniería de tráfico como ATM, lo cual conduce a la importancia de añadir una conexión orientada a IP. MPLS, una

técnica diseñada para el núcleo de las redes de internet, es un interesante candidato para compensar esta deficiencia.

MPLS ya ha sido propuesto para los Satélites Geoestacionarios(GEO) . Sin embargo, debido al enorme volumen de tráfico, tiene que ser conmutado entre varios decenas o centenas de puertos de entradas/salidas, para los distintos haces de transmisión .

Se considera a los usuarios de tierra o estaciones, simplemente como enrutadores MPLS de una red respectiva. El factor que regula y frecuenta handovers aparece entre los nodos de la red (enrutadores), por lo que es importante saber donde colocar los limites de la red MPLS, es decir los LERs.

Estos LERs, pueden ser satélites en la tierra o satélites en el espacio .Los satélites en la tierra, serán operados sin estrictos requerimientos para formar un LSP, sin embargo puede tener varias desventajas. Veamos a continuación con mas detalle.

Los LERs como ya mencionamos anteriormente en capítulos anteriores, constituyen el camino inteligente de la red, ellos controlan la distribución de las etiquetas y en algunos casos desempeñan cálculos de enrutamiento

Si el LER es colocado en el espacio o es colocado el la tierra siempre el flujo de tráfico fluye de tierra a tierra. Sin embargo hay una diferencia entre estos dos casos. En el caso de los satélites LERs. La estación tierra podría provocar un " handover" de un nuevo a un viejo satélite LER, al preguntar para el LSP del viejo satélite y hacer la petición para la activación de un nuevo LSP para el nuevo satélite LER, consecuentemente, una nueva fase de activación de LSP comienza al relacionar la negociación de QoS y su control de admisión. En el segundo caso, cuando los LERs son colocados en tierra , los LERs no negocian QoS, ni un control de admisión, es decir el LSP ya esta activo y sus atributos son ya conocidos, por lo tanto los LSPs tienen que ser mantenidos con el mismas características [9].

En conclusión no hay buena ventajas que valgan la pena para implementar LERs en el espacio.

Desarrollar una red MPLS para una constelación de satélites implica considerar varios protocolos envueltos en MPLS

Todas las funciones relevantes de MPLS en una red satelital pueden ser resumidas en cuatro principales bloques funcionales:

1) Estado de red : Se encarga en particular del monitoreo y el estado de la distribución de la información, por lo que utiliza los protocolos OSPF o IS-IS
2) Calidad de servicio. Para clasificar el tráfico según el ancho de banda, retardo, prioridad

3) Ingeniería de tráfico
4) Establecimiento del LSP

Para ver donde debe ser físicamente implementado la funcionalidad de enrutamiento de la red, se definirán a continuación tres diferentes escenarios:

Escenario 1 : Enrutamiento distribuido y gestión del LSP

Todos los LERs en la tierra y los LSRs satelitales en el espacio, conservan un LSDB(*Link State Databases*) el cual representa un entero estado de la red . Los enrutadores son programados en los puntos de ingreso de la red, se encarga de establecer el LSP, deacuerdo a la información distribuida en su LSDB, y por lo tanto este recibe continuas actualizaciones para el LSDB.

El OSPF- TE es usado como protocolo para distribuir información sobre el estado de la red y para sincronizar el anuncio del estado de enlace LSA (*Link State Advertisemnets*) en el LSDBs de los nodos. Los LSDBS son actualizados periódicamente debido a los cambios ne la topología de la red, pero la nueva información de la red es distribuida muy rápidamente con el fin de evitar errores de enrutamiento

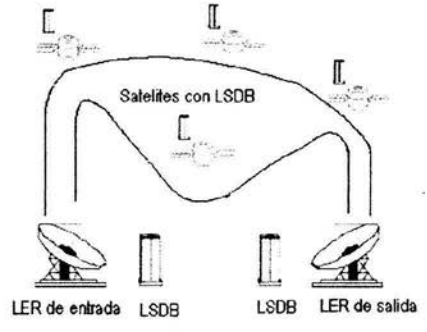


Figura 7.2.1 Escenario 1 LSDBs distribuidos: enrutamiento distribuido y gestión del LSP

Escenario 2: Enrutamiento Centralizado y Gestión del LSP distribuido

Una eficiente ingeniería de tráfico puede ser desempeñada con una vista global de la red. Para esto, es necesario que cada LER de entrada, envíe parámetros de tráfico como categoría, ancho de banda etc, a la central de base de datos, la cual tiene total conocimiento del estado de la red y se encarga de un óptimo camino para la solicitud de entrada. Entonces la central de base de datos contesta un mensaje contenido en un ER (Explict Route) para un LSP, el cual es creado por el LER. En paralelo, la central LSBD puede enviar un nuevo ER al LSR de entrada para mantener el LSPs, con el fin de provocar eventos de handover y así lograr una mejor utilización de la red [10].

Estas aproximaciones tienen dos buenas ventajas: Los satélites, no pueden mantener los LSDBs y desempeñar cálculos de rutas y segundo la utilización de la red es incrementada drásticamente. Sin embargo, los inconvenientes podrían ser la necesidad de un nuevo protocolo, para intercambiar información entre el LER de entrada y la Central LSDB y mas o menos precisar la información de las estaciones de la tierra. En el escenario 1, solamente necesitan información acerca de la visibilidad y distancia para determinad LSP y el tiempo para conmutar a una nueva ruta.

El escenario 2, ofrece dos posibilidades para considerar el tiempo de reenrutamiento: La central LSDB ofrece una o varias alternativas para la ER.

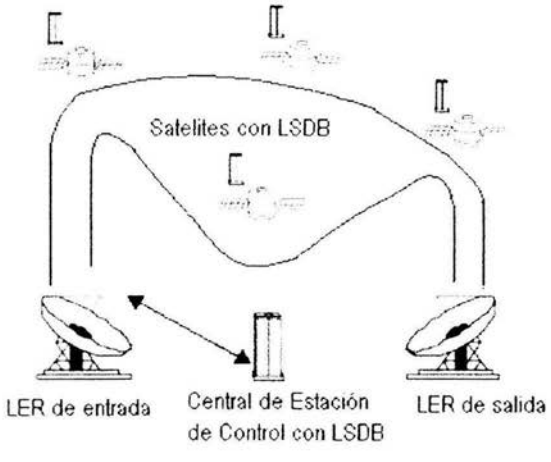


Figura 7.2.2. Escenario 2 Enrutamiento Centralizado y Gestión del LSP distribuido

Escenario 3 : Enrutamiento Centralizado y Gestión de LSP

Aquí los puntos de entrada ya no establecen LSPs : todos los nodos de la red consiguen sus tablas para el intercambio de etiquetas directamente de la central de base de datos, por medio de enlaces lógicos, Cualquier decisión acerca de la ingeniería de tráfico o eventos de handover son impuestos por el LSDB.

Una ventaja de esta aproximación es la rápida instalación de LSPs. La central LSDB distribuye el intercambio de etiquetas de las tablas entre los satélites directamente después de la solicitud de uno de los LERs, y debido a un handover o evento de reenrutamiento. Entonces este envía un reconocimiento para el origen de la solicitud de conexión y esta podría inmediatamente empezar a usar el ya existente LSP, sin tenerlo que establecerlo el mismo.

En el caso de eventos de handover y reenrutamiento, el procedimiento tiene que ser cuidadosamente considerado con respecto a los requisitos de sincronización: todos las tablas actualizadas podrían empezar a ser utilizadas al mismo tiempo. Una posible solución es actualizar todas las nuevas tablas a lo largo de el nuevo LSP con el LER de entrada siendo este el ultimo nodo actualizado. Un inconveniente de este escenario es el diseñar un nuevo protocolo para distribuir etiquetas entre los LSRs.

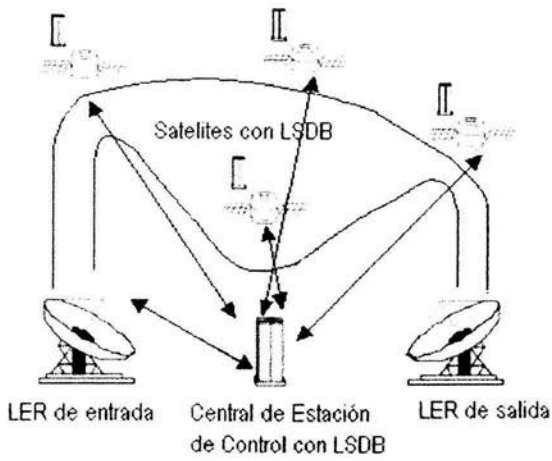


Figura 7.2.3. Escenario 3 : Enrutamiento Centralizado y Gestión de LSP

Ambos escenarios centralizados (2 y 3) presentan problemas de escabilidad con respecto al numero de LSPs : la estación central es solo capaz de manejar un numero limitado de LSPs.

Como se ha podido analizar, las constelaciones satelitales basadas en MPLS aun exigen nuevos protocolos para su máxima utilidad, sin embargo MPLS es bien colocado para el uso adecuado en una topología dinámica, proporcionando calidad de servicios, algoritmos de enrutamiento para multicast, y una carga de tráfico balanceada en las constelaciones.

7.3. MPLS en redes de acceso

7.3.1. Introducción

Mientras que está claro que la MPLS jugará un importante papel en las infraestructuras de telecomunicación de la próxima generación, con el tiempo probablemente será también útil en las redes de agregación de acceso. La explosión de los servicios de banda ancha para los clientes de empresas y residenciales ha dado origen a nuevos requisitos para las redes de agregación de acceso. Escalabilidad, rentabilidad, personalización de los servicios, seguridad y entrega a tiempo son esenciales para el éxito de las redes de acceso multi-servicio de la próxima generación. Actualmente, el ATM suministra una solución sólida que cumple estos requisitos. No obstante, ya que están aumentando los servicios basados en IP, el IP se extenderá inevitablemente hacia las redes de extremo y de acceso, un proceso gradual «IPficación» [11].

Aunque el IP puede ser una capa de agregación de tráfico adecuada para múltiples servicios, no cumple con todos los requisitos de una verdadera red de agregación. Un método de capa 2 es preferible en las redes de acceso/agregación para realizar una solución viable económicamente y escalable. La MPLS aparece de forma prometedora en este contexto ya que combina las propiedades multi-protocolo y multi-servicio del ATM con la flexibilidad de la tecnología IP en la que los servicios se añaden, cumpliendo así todos los requisitos de una red de agregación. Otra ventaja más es que un plano de control MPLS suministra una forma unificada de establecer conexiones sobre las diferentes tecnologías de capa 2 que se encuentran tradicionalmente en las redes de acceso y agregación (ATM, Frame Relay, Ethernet).

7.3.2. MPLS: Calidad de Servicio de extremo a extremo

Hoy, la MPLS está definida para ir desde el extremo del suministrador al extremo de suministrador sobre la red central del suministrador de servicios. Su principal papel es posibilitar una tecnología central y un servicio de borde. En tanto los suministradores de servicios introduzcan con éxito servicios VPN de capa 2 y capa 3, habrá una amplia demanda para hacer la MPLS adecuada para las redes de operador. Esto requiere la introducción de facilidades adicionales, tales como:

• Reserva permanente de los planos de enrutamiento y señalización: Las VPNs basadas en la red de MPLS tienen su principal fundamento en el BGP para la distribución de la información de accesibilidad y auto-descubrimiento. Por tanto, una pila BGP redundante permanentemente es inevitable.

• Facilidades mejoradas de la operación, administración y mantenimiento del MPLS para gestión de fallos, verificación proactiva de la conectividad y seguimiento del rendimiento.

• Calidad de servicio de extremo a extremo: En servicios VPN basados en red, las redes de acceso se basan en gran parte en las facilidades existentes de gestión de tráfico de capa 2. Por lo tanto es importante asegurar el interfuncionamiento entre las funciones de gestión de tráfico de la red de acceso (ATM, Frame Relay o Ethernet) y la red IP/MPLS basada en DiffServ. Además, es necesario definir clases de servicios para ser capaz de respetar los objetivos QoS en toda la red y para informar a los clientes VPN donde se encuentra en la red IP/MPLS el SLA contratado.

• Facilidades de diagnóstico, tal como una facilidad de acceso de prueba para realizar mantenimiento en un LSP en un punto específico de la red: Esto incluye la verificación del rendimiento (por ejemplo, tasa de errores del caudal de producción y de la carga útil) y el diagnóstico de un fallo en un nodo específico después que haber sido localizado por el sistema.

• Facilidades de tarificación: Las redes MPLS suministrarían estadísticas de uso para tarificación con soporte para los SLAs por ejemplo, clase de servicio, nivel de protección, nivel de seguridad.

Los operadores de las redes de cable actuales tienen en sus manos la oportunidad que siempre anhelaron: convertirse en multi-proveedores de servicios. Para alcanzar esta meta deberán enfrentarse a un sin fin de retos que comienzan con la transformación de sus redes, originalmente unidireccionales, en sistemas bidireccionales. Uno de los principales retos para aquellos que quieran ofrecer servicios

multimedia y de telefonía de siguiente generación, será garantizar una estricta Calidad de Servicio a través de toda su red.

Las especificaciones de CableLabs (*CableLabs o Cable Television Laboratories es un consorcio de investigación y desarrollo fondeado por la industria del cable de Norteamérica*) para la transmisión de datos de alta velocidad y para telefonía, conocidas como DOCSIS y PacketCable (*DOCSIS y PacketCable son marcas registradas de CableLabs*), respectivamente, ofrecen la calidad de servicio necesaria para proveer estas aplicaciones dentro de las redes de acceso de banda ancha. Sin embargo, las redes metropolitanas y "*backbones*" de las que dependen dichas redes, deberán garantizar también una calidad de servicio similar. Puesto que las anteriores especificaciones de CableLabs, el brazo tecnológico de la industria del cable en los Estados Unidos, se ocupan únicamente de las redes HFC de los operadores, es necesario encontrar una solución que garantice la calidad de servicio de las redes a las que éstas se encuentran interconectadas [12] .

Aun cuando las redes de acceso de los operadores de cable son considerablemente rápidas, las interconexiones que tienen hacia otras redes no lo son, provocando retrasos y "cuellos de botella" en los puntos de acceso. La manera en que tradicionalmente se hace el enrutamiento de paquetes IP en los conmutadores y enrutadores localizados en los nodos de red consiste en procesar el encabezado de la capa de red del protocolo IP, que contiene la dirección de destino de cada paquete. En cada enrutador, esta dirección es comparada contra una tabla de enrutamiento para determinar el siguiente salto de los paquetes en su trayectoria. El hecho de examinar estos paquetes en cada uno de los puntos de tránsito que deberán recorrer para llegar a su destino final significa un mayor tiempo de procesamiento en cada nodo y, por ende, una mayor duración en el recorrido.

Revisemos ahora el aspecto de calidad de servicio en las redes IP convencionales. Podemos inferir, a partir de la explicación anterior, que los paquetes que viajan a través de las redes IP pueden seguir rutas diferentes, aun tratándose de paquetes que conforman un mismo archivo. Un paquete enviado antes que otro puede llegar al mismo destino después de que el segundo haya alcanzado su meta. Este concepto de red, al que se le conoce como "no orientado a conexión" es opuesto a las redes "orientadas a conexión", en las que previamente se establece una ruta o circuito dedicado para la transmisión de datos. Por su propia naturaleza, la calidad de servicio no es una característica de las redes no orientadas a conexión, considerándose no óptimas para servicios de telefonía y multimedia en tiempo real. Ver capitulo 3.2

Pero entonces, ¿cómo puede garantizarse la calidad de servicio en las redes IP a las que se encuentran interconectadas las redes de cable de los propios operadores? La solución más adecuada consistiría en evitar todo el procesamiento que se lleva a cabo en los nodos, asignando desde un principio la ruta que

los paquetes seguirán. MPLS, ofrece una alternativa eficiente de solución ante esta problemática, pues combina el desempeño y velocidad de la capa de enlace de datos del modelo OSI con la escalabilidad y flexibilidad de la capa de red. Para hacer esto, en lugar de emplear el enrutamiento tradicional antes comentado, MPLS utiliza etiquetas cortas de longitud fija que son añadidas a los paquetes de datos en el momento en que éstos ingresan a la red MPLS. Las etiquetas asignadas a cada paquete son las que determinan las decisiones de enrutamiento dentro del dominio MPLS.

Como se comentó al principio de este capítulo, las redes metropolitanas y los *"backbones"* en IP de los que dependen los operadores de las redes de cable, deben garantizar un estricto nivel de calidad de servicio similar al de las redes DOCSIS. Emplear un ambiente basado en estándares DOCSIS, PacketCable y MPLS, no sólo permitirá a los operadores de redes de cable establecer vínculos con proveedores externos, sino también ofrecer distintos niveles de QoS de extremo a extremo para los servicios que prestan.

En conclusión, los operadores de las redes de cable pueden beneficiarse de MPLS para garantizar la calidad de servicio que demandan sus suscriptores. No se trata de una tecnología exclusiva del cable, sino de una novedosa alternativa con múltiples aplicaciones dentro del área de las telecomunicaciones y las redes de datos. MPLS no es un protocolo que venga a reemplazar a IP, sino una tecnología que lo complementa. Es el protocolo que dará nueva vida a nuestro ampliamente utilizado Protocolo de Internet.

7.4. Implementación de MPLS en las empresas

MPLS es un estándar diseñado para el futuro que permite a las empresas simplificar sus redes al poder integrar todos los servicios en una sola plataforma. Combina la fiabilidad de los protocolos orientados a la conexión, como ATM, con la flexibilidad y la facilidad de ampliación del protocolo IP. MPLS también ofrece a las empresas soluciones a medida, servicios garantizados y rentabilidad desde el punto de vista económico.

Veamos con mas detalle cada uno de los aspectos mas importantes que ofrece MPLS a las empresas.

Costo de un servicio MPLS a una empresa.

Realmente, el servicio MPLS puede ahorrar dinero a las empresas al hacer posible la convergencia de varias redes en una sola plataforma y adoptar toda la flexibilidad y la facilidad de ampliación de la conectividad entre dispositivos cualesquiera. Al controlar los costes mediante la unificación de sus redes, no hay necesidad de tener excedentes de ancho de banda

Una red IP VPN que funciona por una red MPLS puede servir como base para la entrega de una amplia variedad de servicios emergentes basados en IP para el rango completo de 56 kbps a 40 Gbps. Como red única para todo propósito para aplicaciones de voz, datos y video, la red MPLS reduce el costo operativo mediante la convergencia mientras que las IP VPN eliminan los costos de ingeniería y la administración de pasos y rutas de interconexiones tipo rueda con centro y rayos. Al utilizar la inteligencia de los dispositivos CPE, los datos, señales y administración de pasos entre CPE y la red, resulta relativamente simple para los proveedores de servicios activar servicios tales como VoIP (Voz sobre IP) o firewalls.

Tiempo de implementación

El tiempo de implementación depende de dónde esté emplazada cada sede, pero en general, una empresa puede tener la instalación realizada y operativa en el plazo de un mes.

Conexión

MPLS no requiere conexiones, sólo necesita un circuito de acceso en cada sede, en vez de enlaces preconfigurados o Circuitos Virtuales Permanentes (PVCs), como ocurre con las VPNs tradicionales. En este caso, la configuración la hace automáticamente la red.

Todo esto incrementa enormemente la flexibilidad del servicio porque se pueden añadir nuevas sedes rápida y fácilmente. Además, al suministrarlo como un servicio gestionado, se reduce el coste y el tiempo empleado en la implementación y el mantenimiento de la red.

7.4.1. A quién va dirigido

MPLS es una oferta comercial dirigida al mercado de las pequeñas y medianas empresas (PYMES) y grandes empresas. En particular, dirigida a compañías con las siguientes necesidades:

- Compañías que necesitan conectividad global en una única plataforma .
- Compañías que requieren conectividad punto a punto .

- Compañías que desean tener la posibilidad de priorizar distintas aplicaciones.
- Compañías que requieren distintos niveles de rendimiento para diferentes tipos de aplicaciones .
- Compañías que necesitan una red que pueda adaptarse a su estrategia de expansión.
- Compañías que necesitan conectividad de LAN a LAN o de WAN a WAN a través de redes privadas.
- Compañías que desean reducir los costes de conexión a redes y mejorar la velocidad de salida al mercado de sus productos .

MPLS la mejor opción entre los proveedores de servicios de telecomunicaciones.

MPLS ya es la elección preferida por más de 200 empresas líderes en telecomunicaciones con las que hemos trabajado. Por ejemplo, con MPLS , AT&T ofrece 17 servicios administrados diferentes para resolver las necesidades variables de los clientes por medio de una sola red convergente. Telia Denmark está aprovechando las capacidades de tiempo de llegada al mercado de su red MPLS implementando servicios en menos de 90 días. Bell Canada, con su flexible red MPLS puede ofrecer ancho de banda por demanda para tráfico de voz, datos y video. Bell Canada admite estos servicios con QoS de extremo a extremo y confiabilidad esencial para operaciones de gran importancia, como por ejemplo, una cirugía telerrobótica realizada por un cirujano en un hospital importante en un paciente que se encuentra en un centro médico muy pequeño a cientos de millas de distancia. BellSouth, British Telecom, SBC, Verizon y muchas otras empresas telefónicas también están procurando MPLS como la base para sus servicios administrados.

Una red IP VPN que funciona por una red MPLS puede servir como base para la entrega de una amplia variedad de servicios emergentes basados en IP para el rango completo de 56 kbps a 40 Gbps. Como red única para todo propósito para aplicaciones de voz, datos y video, la red MPLS reduce el costo operativo mediante la convergencia mientras que las IP VPN eliminan los costos de ingeniería y la administración de pasos y rutas de interconexiones.

7.4.2. MPLS en el mundo

La comercialización de esta nueva tecnología se inició en Gran Bretaña, donde se solventaron perfectamente los históricos problemas que conlleva la voz sobre IP. Allí como aquí el producto se dirige a medianas y grandes empresas que cuenten, al menos, con dos delegaciones. MPLS se considera fundamental en la construcción de los nuevos cimientos para la Internet del próximo siglo.

MPLS se ofrece en Europa, América del Sur y Central, América del Norte y la región Asia Pacífico. Actualmente, MPLS se ofrece en más de 500 puntos de presencia (PoP) de más de 60 países de todo el mundo.

Europa Occidental	**Europa del Este, Oriente Medi**	**América Central y América del Sur**
Austria	**África**	Argentina
Bélgica (10 PoP)	República Checa	Brasil
Dinamarca	República Eslovaca	Chile
Finlandia	Egipto	Colombia
Francia (8 PoP)	Hungría	Venezuela
Alemania (116 PoP)	Israel Polonia	
Grecia	Rumania	**Región de Asia Pacífico**
Irlanda (27 PoP)	Rusia	Australia (5 PoP),
Italia (2 PoP)	Sudáfrica	China
Luxemburgo		Hong Kong
Países Bajos (37 PoP)	**Norteamérica**	India
Noruega Portugal	Canadá	Indonesia
España (50 PoP)	México	Japón (7 PoP)
Suecia	Estados Unidos (100 PoP)	Malasia
Suiza (34 PoP)		Nueva Zelanda
Reino Unido (cobertura completa		Filipinas Singapur
		Corea del Sur
		Taiwán
		Tailandia

Tabla 7.4.2.1 Puntos de presencia de MPLS en el mundo

7.4.3. Fabricantes de equipo que manejan MPLS.

MPLS aparece como una posible solución para proporcionar QoS e Ingeniería de tráfico a una red global que soporte todo tipo de tráfico. Es una solución con grandes posibilidades de éxito debido a la facilidad a la hora de migrar una red actual (FR, ATM, Ethernet...) a MPLS, siendo el primer paso la coexistencia entre ellas mediante software añadido a equipos actuales. Una importante ventaja de una red única es la simplificación en cuanto a administración de una sola red, sobre la se pueden crear tantas redes virtuales como sea necesario. Esto facilitará enormemente la labor a los proveedores de servicio al tiempo que les permitirá ofrecer servicios de valor añadido, pues es lo que en definitiva acabará marcando la diferencia entre ellos. A fecha de hoy, ya hay operadores migrando a esta solución como es el caso de, por ejemplo, Cable & Wireless, Equant, Genuity y MCI World- Com.

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

Cisco ofrece cuatro nuevas tecnologías para redes MPLS VPN: multicast, NAT (Network Address Translation), ODAP (On Demand Address Pools) y VPN Selecta. Una vez que están dentro de la red, los servicios pueden migrar a la red del proveedor del servicio, ofreciendo nuevas oportunidades de ingresos a los proveedores de servicio, al tiempo que reducen los costos de implementación y administración. Las empresas se benefician con una mayor flexibilidad, al poder contratar con terceros la administración de los servicios.

Cisco Systems introdujo una nueva solución de protección de banda ancha MPLS que entrega una alternativa a bajo costo para protección de SONET/SDH.

La solución de protección de banda ancha MPLS es una arquitectura de red que utiliza MPLS Traffic Engineering Fast Reroute y una aplicación fuera de línea llamada Tunnel Builder Pro, la cual está diseñada para maximizar los servicios de protección a un nivel amplio de la red, y para incrementar la capacidad de la red.

Esta solución ayuda a los proveedores de servicio a minimizar y eliminar los circuitos redundantes no productivos, para ofrecer servicios globales de protección de banda ancha a bajo costo, dando como resultado acuerdos de servicio de clase carrier (SLAs), y la generación de nuevas oportunidades de ingresos.

La tecnología MPLS de Cisco, desplegada ampliamente y cuya base es el software Cisco IOS, entrega capacidades de ingeniería de tráfico que facilitan la eficiencia y las operaciones responsables de la red, mientras que, simultáneamente, optimiza la utilización de recursos de la red y el desempeño de ésta.

Los perfeccionamientos de Cisco en MPLS han dado eficiencias mejoradas y mayores funcionalidades para clientes VPN, La solución MPLS se integra fácilmente en la infraestructura y ofrece gran interoperabilidad que, a fin de cuentas, da ahorros operativos como carrier al tiempo que permite entregar sin problema nuevos servicios a los clientes.

Anteriormente, los servicios debían ser replicados a lo largo de todas las VPNs para poder conectar a los empleados, socios y clientes con los servicios. Además del ineficiente uso de los recursos de la red, administrar todas estas VPNs puede ser complejo.

La funcionalidad Multicast VPN minimiza el tiempo de configuración y su complejidad, incrementa la escalabilidad de la red y ofrece la habilidad de fácilmente construir servicios empresariales amigables tales como redes virtuales multicast. Sin soporte multicast nativo, muchas de las redes existentes no pueden manejar la distribución a gran escala de datos, voz, y streams de video de gran tamaño para aplicaciones multimedia, transacciones financieras y teletrabajo. Al reducir la replicación de paquetes en la red MPLS, esta funcionalidad permite la distribución escalable de datos, voz y streams de video.

Cisco también ha agregado soporte para acceso de banda ancha en las nuevas funcionalidades VPN, permitiéndole a los usuarios que cuentan con conexiones de alta velocidad el poder conectarse a la VPN corporativa, sin importar quién es su proveedor de servicio. Por primera vez, los proveedores de servicio pueden ofrecer conectividad corporativa escalable a usuarios de banda ancha sobre redes MPLS VPN.

AT&T dispone de una de las redes más potentes del mundo, ofreciendo un acceso de la mayor amplitud geográfica, con más de 2.500 puntos de presencia (POPs) globales.

Los profesionales de redes de AT&T proporcionan valor percibido a los clientes. Gestionando la complejidad de las redes para alcanzar un entorno de comunicaciones de voz y datos verdaderamente integrado, fiable y libre de conflictos. Transformando lo que ya existe, para ayudar a los clientes en la utilización de las tecnologías de redes para mejorar el rendimiento de su negocio.

AT&T Business combina la amplitud de servicios, las tecnologías de próxima generación y expertos muy calificados para suministrar las soluciones de red dinámicas, fiables y flexibles que permitan a las empresas alcanzar el éxito en la actualidad.

Millones de empresas confían en AT&T como proveedor de soluciones extremo a extremo. Son conscientes de que las soluciones de red integradas, trasladan el entorno de comunicaciones a un nivel superior de rendimiento y valor y de que la marca AT&T representa servicios que proporcionan a sus clientes una ventaja sobres sus competidores en la economía "en red" de hoy en día.

AT&T Business ayuda a sus clientes de cualquier tamaño para que puedan suministrar acceso y cobertura a los empleados, clientes y colaboradores e incrementar al máximo su presencia en la Web.

AT&T tiene experiencia en el diseño, implementación y gestión de redes verdaderamente globales. En la actualidad, gestiona una de las mayores redes troncales de IP del mundo con presencia en 850 ciudades en 60 países. Comenzando con redes basadas en IP, AT&T ha seguido una vía de evolución ofreciendo redes basadas en protocolos Frame Relay y ATM y se encuentra en disposición de ofrecer MPLS y redes preparadas con Clase de Servicio (CoS) y proporcionando a los clientes la posibilidad de añadir la Calidad de Servicio (QoS) a sus intranets. Para soportar de forma adicional los requerimientos de las aplicaciones basadas en red, como por ejemplo Voz sobre IP, AT&T ha incluido la tecnología MPLS en su red troncal y soporta una introducción paulatina de MPLS en los servicios de Redes Privadas Virtuales basadas en IP. AT&T implementa Calidad de Servicio (QoS) y principios de Ingeniería de Tráfico en la Red Privada Virtual del cliente con las ventajas de la cobertura, fiabilidad, seguridad y servicios de valor añadido de la red global de AT&T [13].

AT&T ofrece a las empresas el amplio espectro de posibilidades de acceso a la red, ya sea local o global, incluyendo servicios IP, Frame Relay, MPLS, ATM y nuevas tecnologías (cable, GPRS, servicios xDSL). Desarrolla un catálogo completo de soluciones para soportar interconexión entre oficinas, delegaciones y conectividad de banda ancha punto a punto.

En México aun no se implementa totalmente la tecnología MPLS para mejorar la calidad de servicio, apenas empieza a introducirse al mercado, en cambio en España se ha dado un gran impulso a esta tecnología, por lo que en la compañía Telefónica de España se desplegará los switch-routers metropolitanos RS 38000 y RS 8600 de Riverstone para crear y suministrar servicios premium a sus clientes de empresa, con ancho de banda garantizado, tiempos de recuperación rápidos, recursos de backup personalizados y servicios avanzados basados en conmutación de etiquetas multiprotocolo (MPLS). Aprovechando la tecnología MPLS líder de Riverstone, Telefónica aportará conexión y fiabilidad tipo SONET a su red Ethernet para proporcionar redes privadas virtuales (VPNs) IP, líneas privadas virtuales y servicios LAN privados virtuales.

La tecnología MPLS de Riverstone también permite a Telefónica conceder prioridad al tráfico y garantizar la calidad del servicio (QoS) en su red. En el marco de la estrategia de la nueva red Ethernet de Telefónica, los switch-routers metropolitanos de Riverstone interactuarán con las tecnologías existentes y diversos dispositivos de equipos en las instalaciones del cliente (CPE).

Telefónica de España es una filial propiedad al 100% de Telefónica, operador de telecomunicaciones líder en el mundo de habla hispana y portuguesa. Es la mayor compañía española por capitalización bursátil y una de las principales compañías del mundo en el sector de las telecomunicaciones. Telefónica proporciona una gama completa de servicios de comunicaciones que abarcan telefonía fija, telefonía móvil, transmisión de datos, servicios a empresas, acceso a Internet, guías telefónicas y servicios y contenido CRM. Cuenta con más de 80 millones de clientes y un mercado potencial de 550 millones. Sus principales mercados abarcan 16 países, si bien está presente en casi 50.

REFERENCIAS

[1] Arquitectura GMPLS, Generalized Multiprotocol Label Swtching
http://www.ahciet.net/revista/96/08.pdf

[2]GMPLS and the Optical Control Plane: An Analysis of Profitability and Performance in Optical Networks
http://www.pioneerconsulting.com/report.php3?report=33

[3]Redes ópticas basadas en GMPLS, Prof. Dr. Francisco Ramos Pascual
http://ttt.upv.es/~framos/Fibra/gmpls.html

[4] Conmutación de etiquetas multiprotocolo generalizada en redes óptica, Carlos J. Fuenmayor Toro
http://people.ac.upc.es/asalaver/awgmpls1.pdf

[5] GMPLS Outstanding Issues, International Engineering Consortium
http://www.iec.org/online/tutorials/gmpls/topic04.html

[6]Generalized Multiprotocol Label Switching: An Overview of Routing and Management Enhancements, internet technology series, *Ayan Banerjee, John Drake, Cisco Systems*
http://www.calient.net/files/GMPLS.pdf

[7]Generalized Multiprotocol Label Switching
http://www.nigeriancomputersociety.com/contentimages/Generalized%20Multiprotocol.pdf

[8] Servicios de voz sobre IP en redes de satélites
www.tid.es/presencia/publicaciones/comsid/esp/23/06.pdf

[9] MPLS-based satellite constellation networks
http://ieeexplore.ieee.org/xpl/abs_free.jsp?arNumber=1281968

[10] MPLS over GEO Satellite Systems*Catherine Rosenberg, Tolga Ors, Nortel Networks*
http://dynamo.ecn.purdue.edu/~cath/mini/cath.pdf

[11] MPLS: valor añadido para la interconexión, escrito por Ruby Hoebeke, Tri T. Nguyen.

Revista de Telecomunicaciones de Alcatel. 3 er trimestre 2002

[12] Ofreciendo Calidad de Servicio mediante MPLS: Fundamentos y aplicación a las redes de cable *por Luis Gabriel Sienra*

http://www.aniret.org.mx/pdf/articulos/mpls.pdf

[13] Mailbag: How many MPLS nodes does AT&T have?
www.nwfusion.com/newsletters/isp/2004/0405isp2.html-49k-19Jun2004

CONCLUSIONES

En los capítulos anteriores hemos visto como el protocolo IP por si solo es incapaz de ofrecer aplicaciones de banda ancha tales como videoconferencia, voz, telefonía, multimedia etc, debido a que su infraestructura y protocolos han sido optimizados sólo para datos. Muchos de estos protocolos de enrutamiento están basados en algoritmos para obtener el camino más corto, sin tener en cuenta métricas adicionales como retardo, *jitter* y congestión del tráfico, de tal manera que IP esta limitado a ofrecer diferentes niveles de servicio, para las diferentes aplicaciones, además, el reenvío tradicional basado en software es demasiado lento para manejar las grandes cantidades de tráfico de Internet o de las redes interconectadas. El tiempo de la búsqueda en las tablas de enrutamiento es demasiado elevado. Esto se traduce en pérdida de paquetes y conexiones.

La tecnología MPLS ofrece al entorno IP, QoS, Ingeniería de Trafico y mas, debido a que esta basada en una etiqueta, que se añade al encabezamiento de los paquetes, donde el valor de la etiqueta, es asociado a un flujo aplicativo específico, lo cual permite distinguirlo de los otros, todo lo contrario que en el protocolo IP, que no diferencia las aplicaciones. Las aplicaciones que exigen una banda de paso garantizada y estable, pueden recibir un trato prioritario, ya que en la etiqueta se infiere la clase de servicio o prefencias en cada FEC, de tal forma que se da más prioridad a unos FECs sobre otros. Por ejemplo, se pueden asociar FECs de alta prioridad a tráfico de voz en tiempo real, así como de baja prioridad a correo, etc. Además al añadir la etiqueta permite implementar ingeniería de trafico, ya que lo que hace la etiqueta es forzar a determinados paquetes a seguir una ruta particular, configurada de antemano, y así encontrar el mejor camino para un determinado tipo de tráfico de la manera mas rápida (no tendría que examinar la cabecera IP en cada nodo, solo lo haría cuando entra el paquete a la red); y permitiendo a la red re-enrutar el tráfico rápido y automáticamente cuando se detectan condiciones de falla o congestión.

Una etiqueta MPLS puede asociarse a un origen o destino y con ello se facilita la creación de circuitos virtuales privados (VPN) que comparten una infraestructura física común. Estos VPN permiten agregar tipos de tráfico que presentan características comunes, lo cual tiene ventajas tanto en lo que se refiere a los recursos de la red como a la seguridad y a la gestión de la facturación. Además, la jerarquía de las etiquetas MPLS permite construir VPN que no necesitan ninguna modificación en el espacio de la dirección IP de los clientes y que coexisten con la red MPLS que algunos clientes podrían establecer entre sus diferentes sitios.

Análisis y estudios realizados por los distintos fabricantes y entidades especializadas en el área, determinaron que los niveles de seguridad entregados por una MPLS VPN son comparables con los entregados por los circuitos virtuales de Frame Relay y ATM. Sin embargo, en escenarios donde estos niveles no son suficientes, como por ejemplo en las necesidades de entidades financieras, una MPLS VPN puede también ser combinada con la encriptación y autenticación que IP brinda, elevando aún más la seguridad de la VPN.

La arquitectura de MPLS VPN permite utilizar prácticamente todos las tecnologías de acceso para interconectar las oficinas del cliente con su proveedor de servicios. Por dicho motivo, la versatilidad que nos permite utilizar xDSL o un enlace Wireless Ethernet en las oficinas más pequeñas y hasta incluso en usuarios móviles, nos permite dimensionar cada punto de la VPN acorde a sus necesidades sin limitar o restringir la de otros puntos.

De manera general, podemos decir que MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios (voz, videoconferencia, multimedia, etc) mediante QoS (Calidad de Servicio), Ingeniería de Trafico y Servicio de VPN`s, sin embargo hace falta resaltar un aspecto muy importante que ofrece MPLS y que ninguna otra tecnología ha podido lograr con éxito, y es que MPLS dispone de los medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes tales como Ethernet, DWDM, ATM y Frame Relay, etc. La convergencia de varias redes en una sola plataforma y adoptar toda la flexibilidad y la facilidad de ampliación de la conectividad entre dispositivos cualesquiera, permite a las empresas obtener varias ventajas tales como: simplificación en cuanto a la administración de una sola de red, esto facilitará enormemente la labor a los proveedores de servicio al tiempo que les permitirá ofrecer servicios de valor añadido, pues es lo que en definitiva acabará marcando la diferencia entre ellos; así también ayudará a optimizar los actuales recursos, a abaratar los costes de operación y mantenimiento y hará que sean innecesarios ciertos equipos adicionales que actualmente hay en las redes y cuyas funcionalidades son soportadas por MPLS, lo cual logrará a las empresas un gran ahorro de dinero.

Así mismo, MPLS se ha convertido en la única tecnología capaz de llevar acabo la convergencia de voz, video y datos sobre una misma plataforma.

MPLS pueden existir desde una capa de una red, hasta y a través de otra, incluso si esas redes están compuestas de múltiples tecnologías de transporte, logrando QoS de extremo a extremo. Los operadores de las redes de cable actuales tienen en sus manos la oportunidad que siempre anhelaron: convertirse en multi-proveedores de servicios. Para alcanzar esta meta deberán enfrentarse a un sin fin de retos que comienzan con la transformación de sus redes, originalmente unidireccionales, en sistemas

bidireccionales. Uno de los principales retos para aquellos que quieran ofrecer servicios multimedia y de telefonía de siguiente generación, será garantizar una estricta QoS a través de toda su red

Las redes metropolitanas y los "*backbones*" en IP de los que dependen los operadores de las redes de cable, deben garantizar un estricto nivel de calidad de servicio similar al de las redes de cable. Emplear un ambiente basado en MPLS, no sólo permitirá a los operadores de redes de cable establecer vínculos con proveedores externos, sino también ofrecer distintos niveles de QoS de extremo a extremo para los servicios que prestan.

MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de enrutamiento IP, ya que permite a IP entrar a un mercado más amplio, como el de los satélites y la telefonía. La convergencia de voz y datos está teniendo lugar no solo en los enlaces terrestres sino también en enlaces por satélite. Con su cobertura global y alcance a áreas remotas, los satélites están bien posicionados para permitir el crecimiento de los servicios de voz sobre IP; y MPLS hace posible esta misión ofreciendo a IP calidad garantizada. Por todo ello, MPLS aparece ahora como la gran promesa y esperanza para poder mantener el ritmo actual de evolución de la Internet hacia otros mercados en las telecomunicaciones.

Así también MPLS esta en constante evolución para ofrecer su tecnología al mercado óptico, hay una versión mas avanzada de MPLS llamada GMPLS, la cual es capaz de manejar simultáneamente tráfico de paquetes, TDM y longitudes de onda a velocidades ópticas, en una solo fibra.

MPLS aparece como una posible solución para proporcionar QoS e Ingeniería de tráfico a una red global que soporte todo tipo de tráfico. Es una solución con grandes posibilidades de éxito debido a la facilidad a la hora de migrar una red actual (FR, ATM, Ethernet...) a MPLS, siendo el primer paso la coexistencia entre ellas mediante software añadido a equipos actuales.

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

Así mismo, por las razones que hemos expuesto, podemos decir que MPLS se ha convertido en el punto clave para que las nuevas tecnologías basadas en IP puedan soportar servicios integrados de voz, y datos de banda ancha en una sola plataforma.

Sin embargo en México, el uso de este protocolo apenas inicia y prácticamente no existen ingenieros familiarizados con dicho protocolo, lo cual implica una falta de recursos humanos para la implantación de éste en nuestro pais. Es por eso que a través de esta investigación se les invita a interesarse mas es esta nueva tecnología que dejara al igual que en otros países un importante paso a la evolución de la Internet.

GLOSARIO

ATM (*Modo de transferencia asíncrono, Asynchrous Transmition Modo*).Tecnología utilizada tanto para redes locales como redes de área amplia. Utiliza conmutadores que establecen circuitos lógicos entre sistemas finales por lo que hay una garantía de QoS. Esta tecnología se utiliza como espina dorsal en redes de proveedores y en grandes compañías. Tiene una alta escalabilidad.

ADLS (*Asymmetric Digital Subscriber Line). Una* nueva tecnología que permite enviar mas datos sobre las l,ineas de cobre. ADSL soporta tasas de datos de 1.5 a 9 Mbps en la recepción de datos (tasas de datos conocidas como downstream) y de 16 a 640kbps en el envió de datos(tasas conocidas como upstream). ADLS requiere un módem especial.

Agregación de direcciones. Procedimiento mediante el que se asocia una única etiqueta a una unión de FECs, que será a su vez una FEC (en algún dominio) y que aplica dicha etiqueta a todo el tráfico de la unión.

Algoritmo de enrutamiento. Parte del software de un enrutador responsable de tomar las decisiones relacionadas con el enrutamiento de los paquetes. Cuando se reciba un paquete deberá decidir por qué línea de salida deberá transmitir el paquete.

Ancho de banda. La diferencia entre las frecuencias superior e inferior disponible para las señales de red. Además, la capacidad de rendimiento de un determinado medio o protocolo de red.

ANSI (*Instituto nacional americano de normalización, American National Standards Institute).* Una organización de voluntarios compuesta por miembros de empresas, agencias gubernamentales y otras entidades que coordinan actividades relacionadas con los estándares, que aprueba estándares para los EE.UU. y que desarrolla posiciones de país en las organizaciones de estándares internacionales. El ANSI ayuda a desarrollar estándares internacionales y norteamericanos relacionados con las comunicaciones y las redes (entre otras cosas). El ANSI es miembro de la IEC y de la Organización internacional para la normalización.

ARIS (*Aggregate Route-based IP Switching*). Solución en el entorno de la conmutación de etiquetas de IBM.

ARP *(Protocolo de resolución de direcciones, Address Resolution Protocol).* Un protocolo de Internet que

se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826. Compárese con RARP.

ARPANET (*Red de la agencia de proyectos de investigación avanzada, Advanced Research Projects Agency Network*). Una red de conmutación de paquetes establecida en 1969. ARPANET fue desarrollada en los años setenta por BBN y fundada por ARPA (posteriormente DARPA). Al final se convirtió en Internet. El término ARPANET fue retirado oficialmente en 1990.

Backbone. El núcleo estructural de la red, que conecta todos los componentes de la red, de forma que tenga lugar la comunicación.

Best-effort. "Lo mejor posible". Los paquetes se entregan de la mejor forma posible.

BGP *(Protocolo de pasarela externa, Border Gateway Protocol).* Protocolo de enrutamiento usado entre sistemas autónomos.

Bucle. Una ruta en la que los paquetes nunca llegan a su destino, sino que se repiten a través de una serie constante de nodos de red.

Búfer de memoria. El área de memoria donde el switch almacena el destino y la transmisión de datos.

Célula. Paquete de longitud fija utilizado en ATM. Una célula tiene 48 octetos de información y 5 octetos de control. El hecho de utilizar células de tamaño fijo permite el uso de nodos de conmutación a velocidades muy altas.

Cola. Conjunto de paquetes en espera de ser procesados.

Colisión. En Ethernet, el resultado de dos nodos transmitiendo a la vez. Las tramas de cada dispositivo colisionan y quedan dañadas cuando confluyen en el medio físico.

Congestión. El exceso de tráfico que supera la capacidad de la red.

Conmutación de circuitos. Un sistema de conmutación en el que debe existir una ruta de circuito físico dedicado entre el remitente y el receptor durante el transcurso de la "llamada". Muy utilizado en las redes de las compañías telefónicas. La conmutación de circuitos se diferencia de la contención y del paso de símbolos como método de acceso a canal, y con la conmutación de mensajes y la conmutación de paquetes como técnica de conmutación.

Conmutación de etiquetas. Término genérico usado para refererirse al reenvío de paquetes IP usando el algoritmo de intercambio de etiquetas.

Conmutación de paquetes. Un método de networking en el que los nodos comparten entre sí ancho de banda enviándose paquetes.

Conmutación. El proceso de tomar una trama de entrada desde una interfaz y de enviarla a través de otra interfaz.

CoS (*Clase de Servicio , Class of Service*). Categoría basada en el tipo de usuario, aplicación o criterio que los sistemas de QoS usan para proporcionar diferentes servicios.

CR-LDP *(Enrutamiento basado en restricciones LDP, Constraint-based Routing LDP).* Extensión de LDP utilizado para tráfico sensible al retardo.

Datagrama. Término utilizado para referirse a un paquete en una arquitectura no orientada a conexión.

Difusión. Un paquete de datos que se envía a todos los nodos de una red. Las difusiones vienen identificadas por una dirección de difusión.

Dirección IP. Una dirección de 32 bits que se asigna a los hosts por medio de TCP/IP. Una dirección IP pertenece a una de cinco clases (A, B, C, D o E) y está escrita como cuatro octetos separados por puntos (es decir, en formato decimal con puntos). Cada dirección consta de un número de red, un numero de subred opcional y un número de host. Los números de red y subred se usan para el enrutamiento, y el número de host se utiliza para dirigirse a un host individual de la red o subred. Una máscara de subred se usa para extraer información de red y subred de la dirección IP. También se llama dirección de Internet.

DLCI (*Identificador de la conexión del enlace de datos, Data Link Connection Identifier*). Número de circuito virtual conmutado en una red de retransmisión de tramas. Está situado en la cabecera de la trama e identifica el circuito lógico por el que van los datos. Ver identificador de la conexión del enlace de datos.

DNS *(Sistema de denominación de dominio, Domain Name System).* Un sistema que se emplea en Internet para traducir los nombres de los nodos de red en direcciones.

Dúplex. La capacidad de transmisión de datos simultánea entre una estación emisora y otra receptora.

Encabezado de un paquete. Información de control de un sistema definido que precede a los datos del usuario.

Encabezado genérico MPLS. Campo que sirve para transportar la etiqueta y que permite que MPLS funcione con cualquier tecnología del nivel de enlace. Está situado entre la cabecera del nivel de enlace y la cabecera del nivel de red.

Enrutador. Dispositivo de nivel 3. Analiza la información de la cabecera de nivel 3 para reenviar los paquetes a través de la red.

Enrutamiento basado en restricciones. Enrutamiento en el que además de optimizar alguna métrica escalar, se deberán satisfacer una serie de restricciones.

Enrutamiento salto a salto. Enrutamiento usual en redes IP. Cada LSR elegirá el siguiente salto hacia donde reenviar los paquetes de una FEC de forma independiente.

Encapsular. Información de control que le añade una entidad del protocolo a los datos obtenidos de un usuario de protocolo.

Enrutamiento. El proceso de localizar una ruta a un host de destino. El enrutamiento es muy complejo en redes muy grandes, debido a los numerosos destinos intermedios potenciales que podría atravesar un paquete antes de llegar a su host de destino.

Espacio de etiquetas por interfaz. Una etiqueta se podrá interpretar de distinta forma dependiendo de la interfaz de entrada de dicha etiqueta.

Espacio de etiquetas por plataforma. Una etiqueta se interpretará de la misma forma independientemente de la interfaz de entrada de dicha etiqueta, siempre y cuando estas interfaces sean comunes con su par LSR.

Espacio de etiquetas: Alcance de una etiqueta en un LSR y cómo este alcance se relaciona con su par adyacente. Se hablará de alcance por interfaz y alcance por plataforma.

Ethernet. IEEE 802.3 (CSMA/CD). Red de difusión basada en bus con control descentralizado que opera a 10, 100, 1000 Mbps. En una red ethernet, los computadores pueden transmitir cuando quieran. Si dos o más paquetes colisionan, los computadores esperarán un tiempo aleatorio y probarán a retransmitir más tarde.

Etiqueta. identificador de tamaño fijo que tiene significado local. Se usa para reenviar paquetes. Un dispositivo de conmutación de etiquetas reemplazará la etiqueta de un paquete antes de reenviarlo.

Fast Ethernet. Cualquiera de las especificaciones Ethernet de 100 Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces superior al de la especificación 10BaseT Ethernet, conservando cualidades como el formato de trama, los mecanismos MAC y la MTU. Tales similitudes permiten el uso de las aplicaciones 10BaseT existentes y las herramientas de gestión de red en redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3.

FDDI *(Interfaz de datos distribuidos por fibra, Fiber Distributed Data Interface).* Un estándar LAN, definido por la X3T9.5 del ANSI, que especifica una red de transmisión de testigos de 100 Mbps que utiliza cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI utiliza una arquitectura de anillo doble con el fin de proporcionar redundancia.

FEC (*Clase Equivalente de Reenvío, Forwarding Equivalence Class).* Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes. Por ejemplo, en el enrutamiento convencional IP por prefijos de red (longest-match) una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo.

Fiabilidad. Tasa media de error en la red.

FIB (*Base de información del reenvío, Forwarding Information Base*). Tabla que forma parte de un LSR y que contiene la NHLFE, la ILM y la FTN. Se utiliza para reenviar paquetes.

FIFO *(Primero que entra primero que sale, First In First Out*). Término que se utiliza para referirse a una pila.

Firewall. Un router de un servidor de acceso, o varios routers de servidores de acceso, que está designado como búfer entre cualquier red pública conectada y una red privada. Un router firewall utiliza listas de control de acceso y otros métodos para garantizar la seguridad de la red privada.

Fragmentación. El proceso de división de un paquete en unidades más pequeñas cuando se transmite sobre un medio de red que no puede soportar el tamaño original del paquete.

Frame Realay. Retransmisión de tramas: Forma de conmutación de paquetes basada en el uso de tramas del nivel de enlace. No existe capa de red.

Frame. Un conjunto de bits ordenados y bien definida con significado para un protocolo en especifico.

FTN (*Correlación de la FEC con la NHLFE, FEC-to-NHLFE*). Esta entrada de la FIB se utiliza cuando se quieren reeviar paquetes que no llegan etiquetados, pero que se quieren reenviar etiquetados.

FTP *(Protocolo de transferencia de archivos, File Transfer Protocol).* Un protocolo de aplicación, parte de la pila del protocolo TCP/IP, que se usa para transferir archivos entre nodos de red. FTP está definido en la RFC 959.

Fusión de etiquetas. Reemplazo de múltiples etiquetas de entrada para una FEC particular por una sola etiqueta de salida.

Gateway. Es el nodo de una red que sirve como entrada a otra red. Por ejemplo, cuando un usuario se conecta a Internet, esencialmente se conecta al servidor que muestra las paginas Web al usuario. Estos dos dispositivos son hosts, no gateways. En las corporaciones, el gateway es la computadora que enruta el tráfico de una estación de trabajo hacia fuera de la red. En el caso de las computadoras personales, el gateway es el ISP, el cual conecta al usuario con la Internet. En el caso de las empresas, el gateway generalmente actúa como un servidor proxy y un firewall. El gateway esta asociado también a los switches.

Gigabit Ethernet. Modalidad de Ethernet que alcanza una velocidad de transmisión de hasta 1Gbps

GMPLS (*MPL Generalizado, Generalized Multiprotocol Label Switching*). Es una extensión de MPLS para redes ópticas. El LSR es ahora un OXC Conector Cruzado Óptico (*cross-connects*) y las etiquetas utilizadas son longitudes de onda. Es capaz de manejar simultáneamente tráfico de paquetes, TDM y longitudes de onda a velocidades ópticas, en una solo fibra.

Host. Es un sistema de computación que es a la se tiene acceso por un usuario en un lugar remoto. Tipicamente el término se usa cuando existen dos computadoras conectadas por medio de módems y líneas telefónicas. La computadora que contiene los datos se llama host, mientras que la computadora a la que se conecta se le denomina terminal.

Hub. Por regla general, un dispositivo que sirve como centro de una red de topología en estrella. También llamado repetidor multipuerto. 2) Un dispositivo de hardware o software que contiene múltiples módulos independientes (pero conectados) de equipos de red e internetwork. Los hubs pueden ser activos (donde repiten las señales que se envían a través de ellos) o pasivos (no repiten, sólo dividen, las señales que se envían a través de ellos).

ICMP *(Protocolo de mensajes de control en Internet, Internet Control Message Protocol).* Un protocolo de Internet de la capa de red que indica errores y proporciona información relevante para el procesamiento

de paquetes IP. Documentado en la RFC 792.

IETF. Abreviatura de Internet *Engineering Task Force*, la principal organización de Internet. La IETF es una gran comunidad abierta internacionalmente de diseñadores de red, operadores, vendedores e investigadores preocupados por la evolución de la arquitectura y la operación del Internet.

IGP (*Prototocolo de pasarela Interior, Interior Gateway Protocol*). Es utilizado para intercambiar información de enrutamiento en los enrutadores dentro de un Sistema autónomo. Ejemplo : RIP y OPSPF

ILM *(Correlación de la etiqueta entrante, Incoming Label Map).* Entrada de la FIB que sirve para correlacionar cada etiqueta entrante con un conjunto de NHLFEs. Se utiliza cuando se reenvían paquetes que llegan como paquetes etiquetados.

Ingeniería de tráfico. Persigue adaptar flujos de tráfico a recursos físicos de la red, de tal forma que exista un equilibrio entre dichos recursos. De esta forma se conseguirá que no haya recursos excesivamente utilizados, con cuellos de botella, mientras existan recursos poco utilizados.
intercambiar información de enrutamiento dentro de un sistema autónomo. IGRP.

Intercambio de etiquetas. Algoritmo empleado por el componente de reenvío de un LSR. Cuando un LSR recibe un paquete extrae el valor de la etiqueta y accede con él a la tabla de enrutamiento. En dicha tabla de enrutamiento encontrará el nuevo valor de la etiqueta que ha de ponerle al paquete antes de reenviarlo, así como la interfaz de salida por donde ha de mandarlo. También podrá encontrar información sobre si debe o no encolar el mensaje.

Interfaz. Zona de contacto o conexión entre dos aplicaciones o entre un usuario y una aplicación. 1) Una conexión entre dos sistemas o dispositivos. 2) En terminología de enrutamiento, una conexión de red. 3) En telefonía, un límite compartido definido por las características de la interconexión física comunes, las características de la señal y los significados de las señales intercambiadas. 4) Un límite entre las capas adyacentes del modelo de referencia OSI.

Internet. La red global más grande, que conecta decenas de miles de redes a nivel mundial y que se centra en la investigación y en la normalización en base al uso en la vida real. Muchas de las tecnologías de redes más avanzadas proceden de la comunidad Internet. Internet se desarrolló a partir de ARPANET. Se le llamó DARPA Internet, término que no hay que confundir con el término general internet.

IP *(Protocolo de Internet, Internet Protocol).* Un protocolo de capa de red de la pila TCP/IP que ofrece un

servicio de internetwork sin conexión. IP proporciona funciones para el direccionamiento, la especificación de tipo de servicio, la fragmentación y el reensamblado y la seguridad. Se define en la RFC 791. IPv4 (Protocolo Internet versión 4) es un protocolo de conmutación de paquetes sin conexión y de máximo esfuerzo de entrega

ISP *(Proveedor de servicios Internet, Internet Service Provider).* Organización que da acceso a Internet ofreciendo una serie de servicios.

LAN *(Red de área local, Local-Area Network).* Una red de datos de alta velocidad y de bajo índice de errores que cubre un área geográfica relativamente pequeña (hasta unos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área limitada geográficamente. Los estándares LAN especifican el cableado y la señalización de las capas de enlace de datos y física del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas.

LDP *(Protocolo de distribución de etiquetas, Label Distribution Protocol).* Conjunto de los procedimientos gracias a los cuales un LSR le informa a otro del significado de las etiquetas usadas para reenviar el tráfico a través de ellos.

LDP peers. Pares o iguales LDP.

LER de entrada. LSR que recibe tráfico de usuario (por ejemplo datagramas IP) y lo clasifica en su correspondiente FEC. Genera una cabecera MPLS asignándole una etiqueta y encapsula el paquete junto a la cabecera MPLS obteniendo una PDU MPLS.

LER de salida. LSR que desencapsula un paquete removiendo la cabecera MPLS. Ver LSR de salida.

LER *(Enrutador Frontera de Etiquetas , Label Edge Router).* Nodo que conecta un dominio con un nodo externo al dominio.

LFIB *(Base de información del reenvío de la etiqueta, Label Forwarding Information Base).* Es una tabla similar a la FIB sólo que en lugar de utilizar direcciones, se emplean etiquetas de entrada y de salida asociadas a la interfaz por la que saldra el paquete.

LIB *(Base de información de la etiqueta, Label Information Base*). Es la tabla generada a partir de la asignación de una etiqueta a cada una de las entradas de la FIB.

LSP *(Camino de conmutación de etiquetas, Label Switched Path).* Camino a través de uno o más LSRs en un nivel de la jerarquía que siguen los paquetes de una FEC particular.

LSR frontera. LSR encargado de etiquetar los paquetes que entran en la red. Para poder realizar este trabajo, dicho LSR deberá implementar el componente de control y el componente de reenvío tanto del enrutamiento convencional como de la conmutación de etiquetas.

LSR intermedio. LSR que realiza el intercambio de etiquetas examinando exclusivamente la cabecera MPLS (obteniendo la etiqueta para poder realizar la búsqueda en la tabla de enrutamiento).

MAC *(Control de acceso al medio, Media Access Control).* La parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen *y* del destino, así como el modo de obtener permiso para transmitir. Véase también capa de enlace de datos *y* LLC.

MAN *(Red de área metropolitana, Metropolitan Area Network).* Una red que abarca un área metropolitana. Por regla general, una MAN abarca un área geográficamente más pequeña que la de una WAN. Compárese con LAN *y* WAN.

Máscara de dirección. Una combinación de bits que se usa para describir qué parte de una dirección hace referencia a la red o subred *y* qué parte hace referencia al *host.* A veces se denomina, sencillamente, máscara.

Máscara de subred. Una máscara que se usa para extraer información de redes *y* sobre las subredes de la dirección IP.

MAU *(Unidad de conexión al medio, Media Attachment Unit).* Un dispositivo que se usa en redes Ethernet e IEEE 802.3 que proporciona la interfaz entre el puerto AUI de una estación *y* el medio común de la Ethernet. La MAU, que puede estar dentro de una estación o que puede ser un dispositivo separado, realiza funciones de capa física, entre las que se incluyen la conversión de datos digitales de la interfaz Ethernet, la detección de colisiones *y* la inyección de bits en la red. A veces se denomina unidad de acceso al medio (su abreviatura también es MAU) o transceptor.

Mensaje. Un agrupamiento de información lógico de capa de aplicación, generalmente compuesto por una serie de agrupamientos lógicos de capa inferior, como los paquetes. Los términos datagrama, trama, paquete *y* segmento se usan también para describir los agrupamientos lógicos de información de las distintas capas del modelo de referencia OSI *y* de los distintos círculos tecnológicos.

MPLS (*Conmutación de etiquetas multiprotocolo, Multiprotocol Label Switching*). Es una iniciativa de la IETF que integra información de capa 2(ancho de banda, retardo) en capa 3 en un Sistema Autónomo con el fin de simplificar y mejorar el intercambio de paquetes IP.

MRU. Abreviatura de *Maximuym Receive Unit.* Es el tamaño máximo de un paquete que una red puede recibir.

MTU (*Unidad máxima de transmisión, Maximum Transmissíon Unít*). Tamaño máximo de un paquete, en bytes, que puede manejar una determinada interfaz.

Multidifusión. Paquetes únicos copiados por una red *y* enviados a una serie de direcciones de red. Estas direcciones están especificadas en el campo de dirección de destino. Compárese con difusión *y* unidifusión.

Multiplexación. Función que permite a dos o más fuentes de datos compartir un medio de transmisión común de tal forma que cada fuente de datos tenga su propio canal.

NHLFE (*Entrada para el reenvío con la etiqueta del siguiente salto, Next Hop Label Forwarding Entry*). Entrada de la FIB utilizada para reenviar paquetes etiquetados.

NHRP (*Protocolo de resolución del siguiente salto, Next Hop Resolution Protocol*). Protocolo usado para permitir que dos dispositivos pertenecientes a distinta LIS puedan comunicarse.

Orientado a la conexión. Transferencia de datos que requiere el establecimiento de un circuito virtual.

OSI (Internetworking de sistemas abiertos, Open System Interconnection). Un programa de normalización internacional creado por la 190 *y* la ITU para desarrollar estándares para *networking* de datos que facilita la interoperabilidad de equipamiento de múltiples fabricantes.

OSPF (*Protocolo abierto del primer camino más corto, Open Shortest Path First*). Protocolo de enrutamiento IP que está sustituyendo rápidamente a RIP. OSPF y RIP son ejemplos de IGP de internet comunes.

Paquete. Un agrupamiento lógico de información que incluye una cabecera que contiene información de control *y* (generalmente) datos de usuario. Los paquetes suelen utilizarse para hacer referencia a unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos lógicos de información de las distintas capas del modelo de referencia OSI *y* de varios círculos tecnológicos.

Par de distribución de etiquetas. LSRs que utilizan un protocolo de distribución de etiquetas para intercambiar información de asociaciones de etiquetas a FECs.

PBX. Abreviatura de *Private Brancg Exchange*. Se refiere a una telefónica privada usada dentro de una empresa. Los usuarios del PBX comparten ciertos números de líneas de salida para efectuar llamadas externas al PBX. Las compañías suelen usar el PBX porque es mucho mas barato conectar sus líneas a él, que conecta cada línea de la organización a la red pública. Además, es mas fácil llamar a alguien dentro de la organización a través del PBX, ya que el número marcado se reduce a tres o cuatro dígitos.

Peer-to-peer. Entre pares o iguales.

PHB . Per-Hop-Behaviour, Comportamiento por salto.

Piggybacking. En MPLS, protocolos que incorporan la etiqueta encima de protocolos existentes de enrutamiento.

POP *(Punto de presencia, Point Of Presence).* El punto de interconexión entre las utilidades de comunicación que proporciona la compañía telefónica *y* el armario de distribución principal del edificio.
Se trata de un número telefónico que, al marcarlo, permite el acceso a Internet. Los ISPs proporcionan los POPs.

PPP (*Protocolo punto a punto, Point-to-Point Protocol).* Sucesor de SLIP, es un protocolo que proporciona conexiones de *router* a *router y* de *host* a red sobre circuitos síncronos *y* asíncronos.

Prefijo de dirección. En vez de utilizar la máscara de subred se puede utilizar un valor llamado valor de prefijo. El valor de prefijo describe cuántos bits se deben usar como máscara.

Protocolo de enrutamiento. Los protocolos de enrutamiento sirven para determinas los caminos y mantener las tablas de enrutamiento.

Protocolo de estado blando. Protocolos en los que si no se reciben mensajes de actualización o refresco de la información de estado, marcan dicho estado como no válido y descartan la información.

Protocolo de resolución de direcciones. Protocolo TCP/IP que convierte direcciones IP en direcciones físicas, como por ejemplo una dirección ethernet. Un host que desee obtener una dirección física enviará una petición ARP a la red. El host con la dirección IP que contenga la petición ARP responderá con su dirección física.
Protocolo Internet. Cualquier protocolo que forme parte de la pila del protocolo TCP/IR Véase IP. Véase

también TCP/IP.

Protocolo. Una descripción formal de una serie de reglas y convenciones que rigen cómo los dispositivos de una red intercambian información.

Protocolos de estado duro. Protocolos en los que en ausencia de eventos que disparen una respuesta del protocolo, el estado del protocolo permanece sin cambio alguno durante un periodo de tiempo ilimitado.

PSTN. Abreviatura de *Public Switched Telephone Network*. Se refiere al sistema telefónico internacional basado en líneas de cobre que transportan voz analógica. El servicio telefónico transportado por PSTN es llamado POTS (*Plain Old Telephone Service*).

Puente. Un dispositivo que conecta y pasa paquetes entre dos segmentos de red que usan el mismo protocolo de comunicaciones. Los puentes operan en la capa de enlace de datos (la Capa 2) del modelo de referencia OSI. Por regla general, un puente filtra, reenvía o inunda una trama de entrada en base a la dirección MAC de esa trama.

PVC (Circuito Virtual Permanente, *Permanent Virtual Circuit*). Un PVC consiste de una dirección de elemento de red Frame Relay origen, identificador de control del enlace de datos de origen, dirección del elemento de red Frame Relay destino e identificador de control del enlace de datos destino. Origen se refiere al interface de acceso desde el cual el PVC es iniciado. Destino se refiere al interface de acceso en el cual el PVC acaba. Los equipos de datos que necesitan una comunicación continua utilizan PVCs.

QoS (Calidad de Servicio,Qulity Service). Nivel de prestaciones de una red, basada en parámetros tales como la velocidad de transmisión, la variación del retardo, el rendimiento y la pérdida de paquetes.

RARP (Protocolo de resolución inversa de direcciones, *Reverse Address Resolution Protocol).* Un protocolo de la pila TCP/IP que proporciona un método de localización de direcciones IP basándose en las direcciones MAC. Compárese con ARP.

Red totalmente mallada. Red en la que todos los nodos están conectados entre sí.
Reenvío: Operación que realizan tanto conmutadores como encaminadores. Consiste básicamente en encaminar un paquete recibido por la línea de entrada en base a unos campos que contiene el paquete.

RSVP *(Protocolo de reserva de recursos, Resource reSerVation Protocol).* Protocolo de estado blando utilizado para reservar recursos en una sesión en un entorno IP. Es un protocolo simplex. Este protocolo permite la asignación de diferentes niveles de servicio a diferentes usuarios. Se utiliza para ofrecer discriminación de servicio a las aplicaciones sensibles al retardo mediante la asignación de recursos.

SAFI *(Identificador de familias de direcciones consecutivas, Subsequent Address Family Identifier).* Campo que sirve para indicar que el campo NLRI contiene una etiqueta en MPLS-BGP.

Salto de conmutación de etiquetas: Salto entre dos nodos MPLS en los que el reenvío se hace usando etiquetas.

SDH. Abreviatura de *Synchronous digital Hierarchy.* Estándar internacional para la transmisión de datos síncronos sobre fibra óptica. Su equivalente en Estados Unidos es SONET.

SONET. Abreviatura de *Syncronous Optical Netework.* Es un estándar para conectar sistemas de transmisión de fibra óptica. Define tasas de interfaces que permiten que los datos sean multiplexados a diferentes velocidades.

SWITCH . Dispositivo que filtra y envía paquetes entre segmentos de una red LAN. Operan en la capa 2 del modelo de referencia OSI y algunos veces sobre la capa 3. Soportan cualquier protocolo .

Tabla de enrutamiento. Una tabla almacenada en un *router* o cualquier otro dispositivo de *internetworking* que controla las rutas a destinos de red concretos *y*, en algunos casos, la métrica asociada a estas rutas.

TCP *(Protocolo para el control de la transmisión, Transmission Control Protocol).* Un protocolo de capa de transporte orientado a la conexión que proporciona la transmisión de datos dúplex fiable. TCP forma parte de la pila del protocolo TCP/IP.

TCP/IP *(Protocolo para el control de la transmisión/Protocolo Internet, Transmission Control ProtocoUInternet Protocol).* Pila de protocolos de Internet. Un nombre común para el conjunto de protocolos desarrollado por el DoD de los EE.UU. en los años setenta para soportar la construcción de *internetworks* a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

Telnet. Un protocolo de emulación de terminal estándar de la pila del protocolo TCP/IP. Telnet se usa para la conexión de terminales remotos, permitiendo a los usuarios conectarse a sistemas remotos *y* utilizar los recursos como si estuvieran conectados a un sistema local. Telnet está definido en la RFC 854.

ToS *(Tipo de servicio, Type of Service).* Campo del encabezado IP utilizado por los elementos de la red para realizar una solicitud con un determinado nivel de QoS.

Trama. Un agrupamiento lógico de información que se envía como unidad de capa de enlace de datos por un medio de transmisión. Suele hacer referencia a la cabecera *y* a la información final *y* se usa en la sincronización *y* el control de errores de los datos de usuario que contiene la unidad. Los términos datagrama, mensaje, paquete y segmento también se emplean para describir agrupamientos lógicos de información de las distintas capas del modelo de referencia OSI *y* de distintos círculos tecnológicos.

TTL (Tiempo de vida ,Time To Live). Número de nodos que puede atravesar un paquete. Cuando este campo llega a cero se desacarta el paquete.

Tunneling. Es una tecnología que permite a una red enviar sus datos a través de una conexión a otra red. Tunneling trabaja encapsulando un protocolo de red en paquetes que son transportados a la segunda red. Por ejemplo, PPTP, GRE, L2TP, L2F, etc.

UDP *(Protocolo de datagrama de usuario, User Datagram Protocol).* Un protocolo de capa de transporte sin conexión de la pila del protocolo TCP/IP. UDP es un protocolo sencillo que intercambia datagramas sin acuse de recibo ni entrega garantizada, requiñendo que el procesamiento de errores *y* la retransmisión sean gestionados por otros protocolos. UDP se define en la RFC 768.

UNI *(Interfaz del usuario a la red, User-to-Network Interface).* UNI es un término usado en ATM. Es la interfaz enmtre un equipo privado y un equipo público.

Unidifusión. Un mensaje que se envía a un solo destino de la red.

URL *(Localizador universal de recursos, Uniform Resource Locator).* Un esquema de direccionamiento estandarizado que sirve para acceder a documentos de hipertexto *y* a otros servicios por medio de un navegador.

UTP *(Par trenzado sin apantallar, Unshielded Tu'isted-Pair).* Un medio de cableado de cuatro pares que se usa en varios tipos de redes. El UTP no requiere el espacio fijo entre conexiones que es necesario en las conexiones de tipo coaxial. Existen cinco tipos de cableado UTP: el cableado de Categoría 1, el cableado de Categoría 2, el cableado de Categoría 3, el cableado de Categoría 4 *y* el cableado de Categoría 5. Compárese con STP.

VC *(Canal virtual ,Virtual Channel)*. En ATM, término genérico para describir la capacidad de comucicación unidireccional para transportar células ATM.

VCC *(Conexión de canal virtual ,Virtual Channel Connection)*. Conexión lógica de ATM.

VCI *(Identificador de Canal Virtual, Virtual Channel Identifier)*. Etiqueta que identifica al canal virtual en cada enlace. Es una conexión establecida a través de la red desde el origen hacia el destino, donde los paquetes, tramas o celdas se enrutan sobre el mismo trayecto para la duración de la llamada.

VPC *(Conexión de trayecto virtual ,Virtual Path Connection)*. Conjunto de VCCs que tienen el mismo punto de terminación. Las células del conjunto de los VCCs se conmutarán conjuntamente en una VPC.

VPI (*Identificador de trayecto virtual , Virtual Path Identifier)*. Etiqueta que identifica al trayecto virtual en cada enlace.

VPN *(Red Privada Virtual , Virtual Private Network*). Es una red construida usando líneas públicas hacia los nodos de conexión. Existe cierto numero de sistemas que permiten crear redes usando Internet como medio de transmisión. Dichos sistemas usan cifrado y otros mecanismos de seguridad para garantizar que sólo los usuarios verificados puedan tener acceso a la red y que los datos no sean interceptados.

X.25. Primera red internacional normalizada de conmutación de paquetes. X.25 se diseñó para ser una red datos pública a nivel mundial. Tecnología orientada a conexión para la transmisión en medios no fiables.