TRABAJO ESPECIAL DE GRADO

ESTUDIO DE LOS PROTOCOLOS DE ENRUTAMIENTO DE INTERNET Y SU UTILIZACIÓN EN LA ARQUITECTURA DE RED MPLS

Presentado ante la Ilustre
Universidad Central de
Venezuela para optar al Título
de Especialista en Redes de Datos y Comunicaciones
Por la Ing. Guas Ojeda, Daliah Sahily

Caracas, Enero de 2004

TRABAJO ESPECIAL DE GRADO

ESTUDIO DE LOS PROTOCOLOS DE ENRUTAMIENTO DE INTERNET Y SU UTILIZACIÓN EN LA ARQUITECTURA DE RED MPLS

TUTOR ACADÉMICO: Esp. Franklin Planchart

Presentado ante la Ilustre
Universidad Central de
Venezuela para optar al Título
de Especialista en Redes de Datos y Comunicaciones
Por la Ing. Guas Ojeda, Daliah Sahily

Caracas, Enero de 2004

Guas O., Daliah S.

ESTUDIO DE LOS PROTOCOLOS DE ENRUTAMIENTO DE INTERNET Y SU UTILIZACIÓN EN LA ARQUITECTURA DE RED MPLS

Tutor Académico: Esp. Franklin Planchart. Tesis. Caracas, U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Año 2004, 84 p.

Palabras Claves: Redes, Protocolos, Enrutamiento, Etiqueta y Multiprotocolo.

Resumen.

La popularización del uso de Internet en los últimos años ha impuesto un ritmo acelerado en el crecimiento de las redes de datos. No sólo sigue aumentando el volumen de tráfico en la red sino que además se desea una cierta calidad de servicio, en concreto para las aplicaciones multimedia. Por lo que se hace necesario disponer de enrutadores ("routers") de gran capacidad para poder procesar y encaminar grandes cantidades de paquetes por segundo. En esta evolución para acelerar las funciones de encaminamiento de los routers surge el concepto de conmutación de nivel 3. En la carrera para disponer de routers de alta velocidad aparecen varias propuestas para acelerar el transporte de paquetes IP a través de la red. Muchas de estas alternativas están relacionadas con el uso de conmutadores ATM; por ello la integración de IP con las redes ATM es de capital importancia. Actualmente la propuesta de "Multiprotocol Label Switching" (MPLS) es el resultado de este proceso de convergencia y de integración. MPLS pretende resolver problemas presentados en las redes actuales, tales como: velocidad y retardo, escalabilidad, manejo de la calidad de servicio QoS, e ingeniería de tráfico.

El concepto de conmutación de etiquetas ("label switching") se define para no usar ninguna de las denominaciones propietarias presentadas anteriormente (Tag Switching, IP Switching, CSR y ARIS) y facilitar así la estandarización. En cuanto al término multiprotocolo, la idea original es no excluir ningún protocolo de red (IP, IPX, Appletalk, etc.) pero hasta ahora en los trabajos del grupo sólo se ha considerado el protocolo IP.

Índice de Contenido

Universidad Central de Venezuela
Facultad de Ingeniería
Escuela de Ingeniería Eléctrica

ESTUDIO DE LOS PROTOCOLOS DE ENRUTAMIENTO DE INTERNET Y SU UTILIZACIÓN EN LA ARQUITECTURA DE RED MPLS

Introducción

El tópico de enrutamiento ha sido estudiado por más de dos décadas, pero fue sólo a finales de los años 80 cuando logró popularidad en el ámbito comercial. La razón principal para que esto sucediera es que en los años 70 las redes resultaban bastante simples, y se encontraban en ambientes homogéneos.

Desde que las grandes redes de Internet se hicieron populares, una de las funciones más importantes es el enrutamiento de datos ya que facilita la comunicación entre los distintos nodos existentes en Internet. Esta tarea es realizada por los protocolos de enrutamiento, los cuales mantienen actualizadas las tablas de enrutamiento.

Debido a que no existe un protocolo único obligatorio para actualizar las tablas de enrutamiento y que los administradores de red siempre han tenido completa libertad para elegir cualquier protocolo de enrutamiento que cubriese sus requisitos internos. Con el tiempo se han diseñado muchos protocolos, y se han mejorado tanto por grupos de normalización como por fabricantes. Por tradición a estos protocolos se les llama Protocolos de Pasarela Interna (IGP - *Interior Gateway Protocol*)

Los enrutadores Cisco utilizan el Protocolo de enrutamiento de pasarela de Internet (IGRP- *Internet Gateway Routing Protocol*) o el IGRP mejorado (EIGRP - Enhanced IGRP). Y existen organizaciones que utilizan el protocolo entre Sistemas Intermedios (IS-IS – *Intermediate System to Intermediate System*) de OSI. Aunque en algunas redes se implanta el Protocolo Primero el Camino Abierto más Corto (OSPF - *Open Shortest Path First*).

La posibilidad de elegir el protocolo interno de enrutamiento ha resultado una gran ventaja y ha funcionado muy bien. Sin embargo, al interconectar redes de proveedores de servicio se requiere de un estándar. Aunque sigue usándose el obsoleto Protocolo de Pasarela Exterior (EGP - *Exterior Gateway Protocol*), actualmente muchos proveedores utilizan el Protocolo de Pasarela de Frontera (BGP – *Border Gateway Protocol*)

Además, el crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y más sofisticados servicios, supone cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas a mitad de los años 90. El éxito de la Internet está muy vinculado al uso de los protocolos TCP/IP para soportar las aplicaciones y los servicios que existen sobre ella, pero hoy en día no es capaz de satisfacer las nuevas necesidades que están surgiendo. Una carencia fundamental de esta red es la incapacidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de los usuarios. La idea original de Internet es proveer acceso a las distintas ubicaciones y distribuir contenido. El tratamiento de la voz y los datos es diferente por sus características intrínsecas, la voz como proceso isócrono es susceptible al

retardo mientras que los datos son poco sensibles al retardo pero la integridad de los mismos es fundamental por lo que debe garantizarse que no se corrompa en su camino entre el emisor y el transmisor. Por ejemplo, no puede tratarse de la misma manera un paquete de voz que requiere poco ancho de banda, el retardo permitido está acotado y la pérdida de paquetes no es tan importante, que una transmisión FTP con unos requerimientos de ancho de banda mucho mayores, alta sensibilidad ante la pérdida de paquetes y relativamente poco sensible con el retardo. Por lo que se hace necesario proveer a Internet de herramientas que permitan ofrecer distinto tratamiento a diferentes tipos de tráfico, o por qué no? hacer que la estructura filosófica de Internet no esté basada en lo que conocemos actualmente como IP.

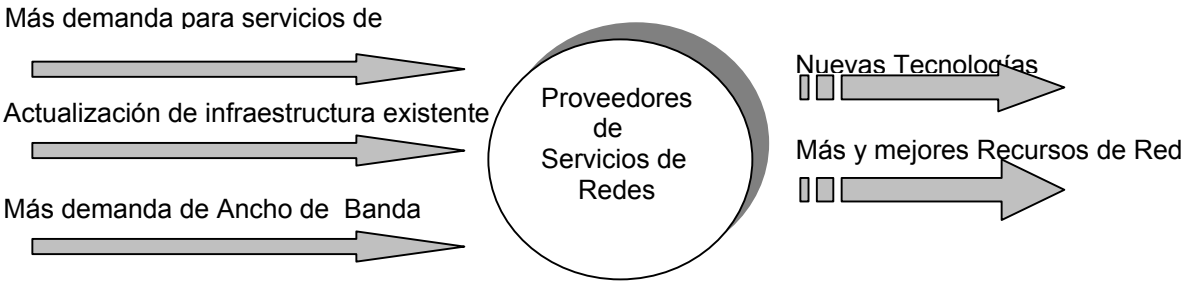


Fig. 1. Los retos de los proveedores de servicio.

Por esto el Multiprotocolo de Conmutación de Etiqueta (MPLS - *Multiprotocol Label Switching*) está emergiendo como tecnología estándar de corto plazo que ofrece nuevas cualidades para redes de IP de gran escala.

Esta tecnología ofrece la flexibilidad para entregar y enrutar tráfico en los casos de fallas de enlace, congestión y cuellos de botella. Además permite a los enrutadores que se encuentran en los límites de la red "etiquetar" los paquetes (o tramas) para permitir el flujo de la información. La tecnología MPLS integra la capacidad de ejecución y de manejo de tráfico de la capa 2 o de enlace de datos con la escalabilidad y flexibilidad del enrutamiento de la capa 3 (o de red). También se aplica en redes que utilizan cualquier tipo de conmutación en la capa 2, pero tiene mejores prestaciones cuando se aplica a redes ATM. A continuación se mencionan dos de sus aplicaciones claves en las que su desempeño es superior a cualquier tecnología disponible de IP:

- Ingeniería de tráfico, que le da a los operadores de red la habilidad de dictaminar el camino que tomará el tráfico dentro de su red.
- Redes Privadas Virtuales[1].
- Calidad de servicio.

En el primer capítulo de este trabajo de investigación se analiza la evolución del enrutamiento en la Internet desde mitad de los 90 y en el segundo capítulo se analiza la tecnología de Modo de Transmisión Asíncrona o ATM.

En el tercer capítulo se estudian las motivaciones que han llevado a la adopción del estándar MPLS. Así como lo concerniente a la arquitectura básica de una red MPLS, sus antecedentes y la descripción funcional de los componentes involucrados.

En el cuarto capítulo se indaga acerca del aspecto fundamental de la tecnología MPLS, que consiste en la clara separación entre las funciones de enrutamiento (es decir el control de la información sobre la topología y tráfico en la red), de las funciones de envío (es decir el envío en sí de datos entre elementos de la red). Así como también, los principales componentes que intervienen en esta arquitectura y de la actuación conjunta de los mismos. En el quinto capítulo

[1] (VPN - Virtual Private Network).

se pasa a discutir el tema de las aplicaciones de MPLS: ingeniería de tráfico, clase de servicio y VPN.

En el sexto y último capítulo se realiza un análisis acerca de los posibles escenarios que involucran a cada una de las tecnologías en las que se basa MPLS, esto es, IP, ATM y el mismo MPLS en sí.

ESTUDIO DE LOS PROTOCOLOS DE ENRUTAMIENTO DE INTERNET Y SU UTILIZACIÓN EN LA ARQUITECTURA DE RED MPLS

Problemática

El Protocolo Internet (IP – *Internet Protocol*) es un protocolo basado en paquetes usado para intercambiar datos entre redes de computadoras. El protocolo IP maneja: direccionamiento, fragmentación, reensamblaje y protocolos de multiplexaje. Es un protocolo de capa de red, por lo que posee información de direccionamiento y control con lo que se logra que los paquetes de datos pueden ser enrutados.

Por otro lado, el Protocolo de Control de Transmisión (TCP - *Transmission Control Protocol*) se encuentra sobre la capa IP. Este es un protocolo orientado a conexión que especifica el formato de los datos y los reconocimientos (acknowledgments) usados en la transferencia de datos. TCP también especifica los procedimientos que los dispositivos de la red usan para asegurar que los datos llegan correctamente. TCP permite le ejecución de múltiples aplicaciones simultáneas debido a que el tráfico de entrada es enviado a las aplicaciones correspondientes.

En el mundo IP, cada vez que llega un paquete IP a un router o enrutador, se procesa toda su cabecera, a pesar de que, realmente, lo único que hay que hacer con ese paquete es ver cual es su siguiente salto, y además para calcular el mismo no se necesita conocer toda la información que lleva la cabecera IP. Por ello, al final se optó por usar un método de conmutación similar al usado en ATM.

Hasta ahora, los protocolos de enrutamiento de IP siempre han tenido que ver con ATM (ATM – *Asynchronous Transfer Mode*) o Frame Relay sin integración real. Por ejemplo, para los ISPs (ISP - *Internet Server Provider*) se han construido nubes ("cores") de ATM o Frame Relay dentro de sus redes enrutadas y han sido usadas para crear conexiones entre los límites. En otras palabras, dos redes enrutadas utilizando IP están conectadas usando PVCs (PVC-*Private Virtual Circuit*) dentro de la nube ATM o Frame Relay. Esto crea un modelo solapado que no resulta ni escalable ni manejable (Fig. 2a), lo que sucede principalmente porque todos los enrutadores de la nube se convierten en vecinos IP. Además, este modelo usa de manera ineficiente los recursos de la red dado que los enlaces ATM son invisibles para el enrutamiento IP. Esto significa que, por ejemplo, un PVC que usa muchos saltos es usado por el enrutamiento IP sólo como un salto sencillo PVC, como si ambos PVCs son encontrados por un solo salto IP.[2]

Las diferencias antes mencionadas se deben básicamente a que IP y ATM son dos tecnologías que fueron diseñadas de manera independiente y para tareas completamente diferentes. Las principales diferencias entre ambas son:

[2] MPLS and Quality Service in Service Provider ATM Networks. Cisco Systems. 2000.

- Servicio no orientado a conexión (IP) vs. Servicio orientado a conexión (ATM), lo que causa el establecimiento y mantenimiento de un gran número de circuitos virtuales ATM de control.
- Modelos de direccionamiento diferentes.
- Utilizan protocolos de enrutamiento diferentes, lo que produce un desempeño poco óptimo.
- Protocolos de señalización diferentes.

Diferentes esquemas de ubicación de recursos.

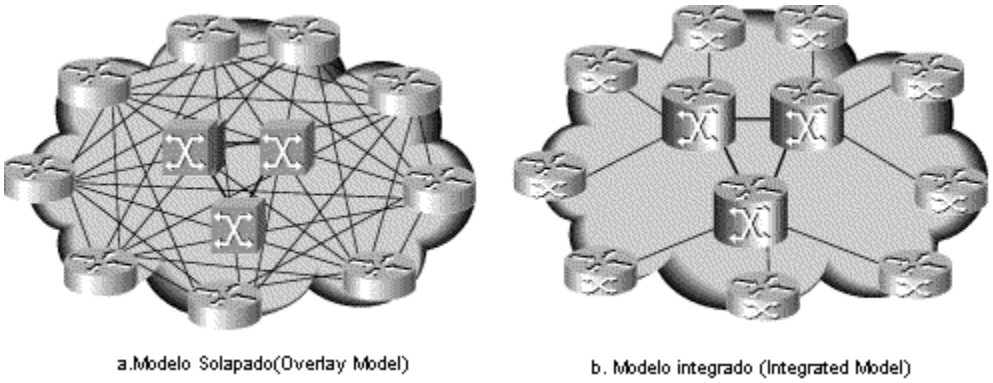


Fig. 2. IP sobre ATM.

Fuente: MPLS and Quality Service in Service Provider ATM Networks. Cisco Systems. 2002.

Por otro lado, se presenta otro problema debido a que el Protocolo de Enrutamiento Primero el Camino más Corto (OSPF - *Open Shortest Path First*) no se ejecuta muy bien grandes redes debido a la duplicación de la actualización del enlace de estado y el gran número de vecinos que son mantenidas. La oscilación de la ruta causada por daños en los circuitos puede enviar la utilización del CPU del enrutador a la raíz y puede ocasionar un comportamiento de convergencia indeterminada de ruta. Se ha demostrado por experiencia que esto se convierte en un problema cuando existen entre 30 y 50 enrutadores.

Por su parte, MPLS soluciona el problema de malla virtual permanente eliminando la noción de "nube" ATM. Los enlaces de ATM son tratados como enlaces IP y cada conmutador ATM puede comportarse como un enrutador IP (ver Fig. 1b). Utilizando la inteligencia de IP dentro de los conmutadores ATM se resuelve el problema de escalabilidad en IP, ya que se elimina el solapamiento de los enlaces de IP sobre ATM, y se realiza un mapeo uno a uno entre ellos. Esta integración de las capas ofrece un modelo distribuido de enrutamiento/conmutación que toma ventaja de lo ofrecido en cada capa. El componente enrutador permite el uso de los algoritmos de enrutamiento tales como OSPF y BGP, para intercambiar información de rutas óptimas y cálculo de caminos. El componente de control en MPLS es necesario para traducir la información de rutas óptimas en elementos que puedan ser entendidos por los conmutadores. Finalmente, el componente de conmutación utiliza las ventajas de equipos avanzados para conmutar los datos a grandes velocidades.

De manera que el protocolo MPLS intenta simular la forma que tiene ATM de conmutar paquetes en función de un identificador como en este caso es el par VPI/VCI. Esta forma de conmutación se basa en crear una pequeña tabla formada por dos campos de entrada y dos campos de salida (VPI/VCI e interfaz). Esta forma de conmutar células se caracterizaba por tener unos retardos muy reducidos.

Por lo antes mencionado, conmutar en MPLS es mejor que conmutar en IP ya que conmutar por etiquetas es más eficiente que hacerlo por direcciones jerárquicas. La búsqueda en una tabla de un prefijo más o menos largo de coincidencia máxima es siempre más lento que la búsqueda de una coincidencia total de un patrón de bits corto.

CAPÍTULO 1

1 Protocolos de enrutamiento

Se define "enrutamiento" al proceso de mover un paquete de datos desde una fuente a un destino dentro de una red (Ver Fig. 1.1). El enrutamiento es una característica clave dentro de las redes de Internet, ya que permite a los paquetes de datos pasar de una máquina o varias máquinas a uno o varios puntos destinos dentro de una red de datos, este proceso se divide en:

- Enrutamiento estático. Es aquel definido por el administrador de la red en tablas fijas de rutas. Presenta el inconveniente de que no escala bien y es difícil de mantener dado que utiliza tablas fijas de rutas.
- *Enrutamiento dinámico*. Es el realizado por los distintos protocolos de enrutamiento de datos. Es el más utilizado por su conveniencia.

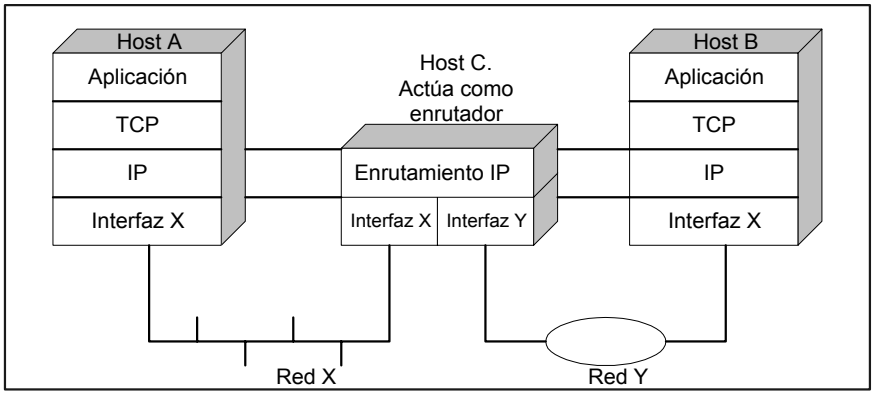


Fig. 1.1. Operación de enrutamiento IP.

Fuente: Rodríguez, Adolfo. TCP/IP tutorial and technical Overview. IBM. 2001.

En este punto es recomendable aclarar que generalmente los términos enrutamiento y conmutación tienden a generar confusión, ya que podría parecer que ambos ejecutan el mismo proceso. Sin embargo, la diferencia principal reside en que el primero se ejecuta en capa 3 (capa de datos) del modelo de referencia OSI y el segundo en capa 2 (capa de enlace).

Otro concepto importante relacionado con el enrutamiento de datos, es el de Sistema Autónomo que se define como una porción lógica de una gran red IP y que comprende un conjunto de enrutadores con una simple política de enrutamiento y que están bajo una simple administración técnica. Los Sistemas Autónomos son identificados por el ASN (*Autonomous System Numbers*), que es un número único de 16 bits asignado por el ARIN[3,4]. Igualmente, se entiende por Protocolo de Internet (IP-*Internet Protocol*) al protocolo que define el formato de los paquetes o datagramas y al esquema de direccionamiento utilizado en Internet a través de números de 4 octetos[5]. (Ver Fig. 1.2)

[3] ARIN del ingles: American Registry for Internet Numbers.

[4] Halabi, Bassam: *Internet Routing Architectures*. 1997. Pag. 96

[5] http://webopedia.internet.com/TERM/I/IP.html

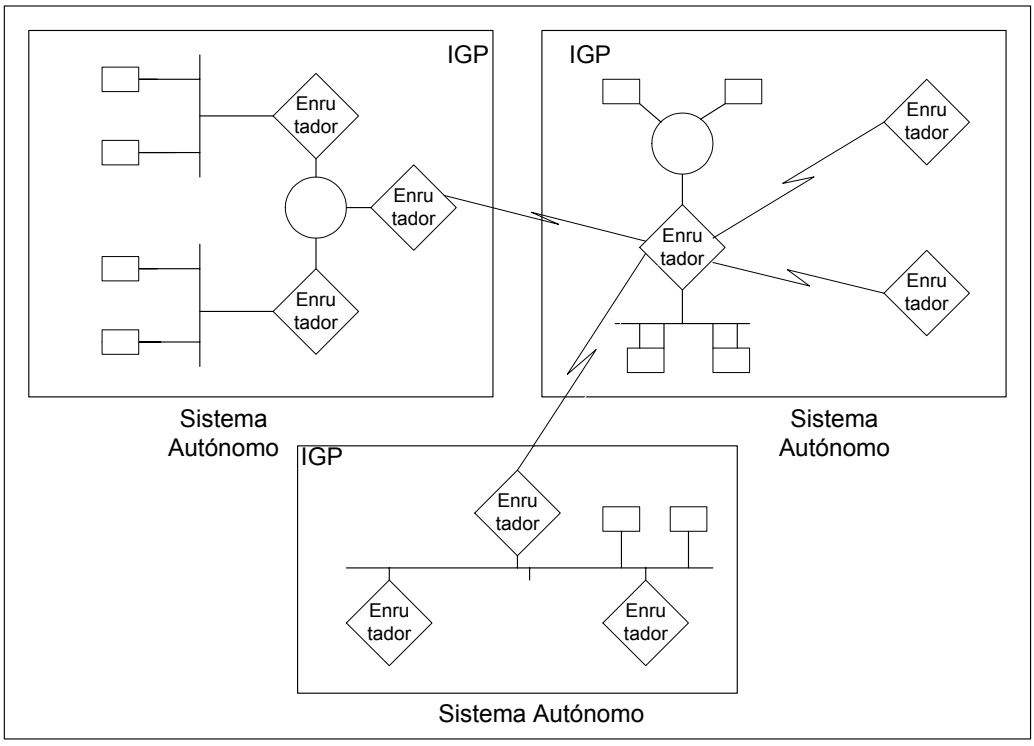


Fig. 1.2. Sistema autónomo.

Fuente: Rodríguez, Adolfo. TCP/IP tutorial and technical Overview. IBM. 2001.

La escogencia de un protocolo de enrutamiento resulta una tarea compleja, en donde se deben considerar los siguientes puntos:

- Tamaño y complejidad de la red de trabajo de Internet.
- Que permita el uso de máscaras de subred de longitud variable (VLSM – *Variable Length Subnet Masks*). Los siguientes protocolos lo permiten: EIGRP, IS-IS, rutas estáticas y OSPF.
- Niveles de tráfico de la red de trabajo.
- Seguridad.
- Confiabilidad.
- Características de retardo de la red de trabajo.
- Políticas organizacionales.

Es importante mencionar que los protocolos de enrutamiento pueden utilizar algoritmos de vector distancia o de estado de enlace[6]. Los cuales se detallan a continuación:

- *Algoritmo de vector distancia*. El enrutamiento basado en algoritmos vector distancia es muy simple. Mantiene una lista de rutas en una tabla, donde cada entrada identifica una red de destino y da la distancia a ese destino medida en saltos (enrutadores intermedios). Cada enrutador determina el camino más corto hacia cada destino basándose en la información recibida. El protocolo clásico de este tipo es el RIP ampliamente utilizado en entornos de redes de área local.

[6] Sirgo, J.A. El Protocolo TCP/IP. Universidad de Oviedo. Pág. 11

- *Algoritmo de estado de enlace*. El enrutamiento basado en algoritmos de estado de enlace proporciona un mecanismo por el cual cada enrutador comunica a los demás el estado de todas sus líneas y cada enrutador "conoce" a sus vecinos e intercambia información de estado de enlace con ellos. Cuando el estado de una línea cambia, los demás enrutadores son informados automáticamente. El protocolo OSPF es de este tipo.

A continuación se detallarán en forma general los principales protocolos de enrutamiento de datos utilizados en Internet. Se hará mención a los protocolos de enrutamiento usados dentro de un mismo Sistema Autónomo o Backbone, o Protocolos de Pasarela Interna (IGP - *Interior Gateway Protocol*). Y a los protocolos usados a nivel ínter dominios o entre sistemas autónomos, definidos como Protocolos de Pasarela Externa (EGP - *Exterior Gateway Protocol*)[7].

1.1 Protocolos de Pasarela Interior

Estos protocolos de enrutamiento son usados en redes que están bajo una administración de red común. Todos los protocolos IP de enrutamiento de pasarela interior deben estar especificados dentro de una lista de redes asociadas antes de iniciar las actividades de enrutamiento. Algunos de estos protocolos se mencionan a continuación:

- Enrutamiento por demanda (ODR - *On-Demand Routing*)
- Protocolo de Información de Enrutamiento (RIP - *Routing Information Protocol*)
- Protocolo de Enrutamiento de Pasarela de Internet (IGRP - *Internet Gateway Routing Protocol*)
- Primero el Camino Abierto más Corto (OSPF – *Open Shortest Path First*)
- Protocolo Mejorado de Enrutamiento de Pasarela de Internet (EIGRP – *Enhanced Internet Gateway Routing Protocol*)
- Protocolo entre Sistemas Intermedios (IS-IS – *Intermediate System to Intermediate System*)

1.1.1 Protocolo de Información de Enrutamiento (RIP)

Dentro de los protocolos de enrutamiento de datos a nivel de IP más importantes tenemos al Protocolo de Información de Enrutamiento (RIP - *Routing Information Protocol*). Se trata de un protocolo "no propietario". Es del tipo vector distancia (también llamado algoritmo Bellman-Ford), fue desarrollado en 1980, que usa el conteo de saltos en su métrica. RIP se usó ampliamente durante muchos años antes de crearse el estándar en la RFC 1058 (1988) y 1723 (1994) y 1724. En 1993 se propuso una segunda versión y se mejoró en 1994[8].

El formato de paquete RIP y RIP-2 está formado por nueve campos como se muestra en la siguiente figura. En cada campo se indica el número de bytes que le corresponde.

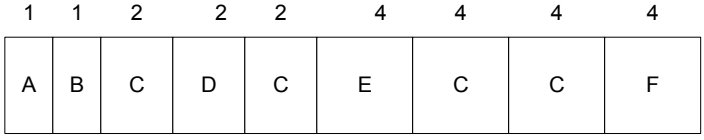


Fig. 1.3. Formato IP de paquete RIP y RIP-2.

[7] Stewart III, John W.: *BGP4. Inter-Domain Routing in the Internet.* 1999. Pag. 18

[8] Feit, Sidnei. TCP/IP Arquitectura, protocolos e implantación con Ipv6 y seguridad de IP. 1997. Pág. 173

A continuación se describen los campos del formato de paquete ilustrado en la Fig. 1.3:

A = Comando

B = Número de Versión

C = Cero

D = Identificador de Dirección de familia

E = Dirección

F = Métrica

- *Comando* - Indica si el contenido del paquete corresponde a una petición o a una respuesta. En el caso de petición se le pide al enrutador que envíe toda o parte de su tabla de enrutamiento. La respuesta puede ser una actualización no solicitada de enrutamiento regular o una respuesta a la petición. Las respuestas contienen entradas a tablas de enrutamiento. Múltiples paquetes de RIP se usan para obtener información de grandes tablas de enrutamiento.
- *Número de Versión* - Especifica la versión de RIP usada. Este campo puede señalizar potenciales incompatibilidades de versión.
- *Cero* - No se usa.
- *Identificador de Dirección de Familia (*AFI- *Address Family Identifier)* - Especifica la dirección de familia usada. RIP está diseñado para llevar información de enrutamiento para diferentes protocolos. Por ejemplo, el AFI para IP es 2.
- *Dirección* - Especifica la dirección IP para la entrada.
- *Métrica* - Indica cuantos saltos (enrutadores) han sido usados en el viaje hacia el destino. Este valor se encuentra entre 1 y 15 para una ruta válida, o 16 para una ruta inalcanzable.

El formato de paquete RIP-2 está formado por nueve campos como se muestra en la siguiente figura.

Longitud de campos en octetos

1	1	1	2	2	4	4	4	4
Comando	Versión	No usado	AFI	Etiqueta de ruta	Dirección IP	Máscara de subred	Próximo salto	Métrica

Fig. 1.4. Formato de paquete IP para RIP-2.

- *Comando* – Indica si el contenido del paquete corresponde a una petición o a una respuesta. Igual al anterior.
- *Versión* – Específica la versión. En este caso vale 2.
- *No usado* – Vale cero.
- *Identificador de Dirección de Familia (*AFI- *Address-Family Identifier)* – El valor de este campo es 2. Si el AFI para la primera entrada del mensaje es OxFFFF, indica que contiene información de autenticación.
- *Etiqueta de ruta* – Ofrece un método para distinguir entre rutas internas (aprendidas por RIP) y rutas externas (aprendidas de otros protocolos).
- *Dirección IP* - Especifica la dirección IP para la entrada.
- *Máscara de Subred* – Contiene la máscara de subred. Si el campo es cero, indica que no se ha especificado máscara de subred.

- *Próximo salto* – Indica la dirección IP del próximo salto al cual los paquetes deben ser enviados.
- *Métrica* - Indica cuantos saltos (o enrutadores) han sido usados en el viaje hacia el destino. Este valor se encuentra entre 1 y 15 para una ruta válida, o 16 para una ruta inalcanzable.

RIP distingue entre dispositivos activos que difunden sus tablas de rutas a través de la red y pasivos que se limitan a escuchar y actualizar sus propias tablas a partir de la información que reciben. Típicamente, los dispositivos activos son los enrutadores y los pasivos los servidores de red. Aunque en el caso de tener RIP configurado con enrutamiento estático, un enrutador puede también actuar como dispositivo pasivo y no propagar información[9].

Los paquetes de RIP son transmitidos en una red como datagramas UDP (UDP – *User Datagram Protocol*), los cuales a su vez son transmitidos dentro de datagramas IP. El protocolo RIP envía y recibe datagramas usando el puerto 520 de UDP. Los datagramas de RIP tienen un tamaño máximo de 512 octetos.

Su métrica está basada en el conteo del número de nodos o "saltos", teniendo como limite máximo 16 saltos, y a cada salto se le asigna un coste que normalmente es 1. La métrica total de un salto es la suma de los costes de salto. RIP elige el siguiente salto para que los datagramas sigan un camino de coste mínimo[10].

Como ventajas de este protocolo se pueden mencionar su simplicidad y disponibilidad. Sin embargo, como limitantes tenemos que no considera parámetros de tiempo real, tales como la carga de los recursos de la red y el retardo en la transmisión de paquetes, así como tampoco puede ser implantado en redes grandes y de gran complejidad, sino sólo en redes de estructura pequeña y poco complejas. Igualmente, realiza el intercambio de grandes tablas de enrutamiento que contienen la información completa de la red, lo cual es ineficiente por generar retardo y carga en la red[11].

Es importante mencionar que RIP fue adoptado por grandes fabricantes, entre ellos 3Com, Novell, Ungermann-Bass, Banyan y XEROX.

1.1.2 Protocolo de Enrutamiento de Pasarela de Internet (IGRP)

El Protocolo de Enrutamiento de Pasarela de Internet (IGRP – *Internet Gateway Routing Protocol*) es un protocolo del tipo vector distancia, de Cisco Systems, desarrollado a mediados de los años 80 para grandes y complejas redes basadas en los protocolos IP y OSI, que resuelve los problemas de RIP.

Su métrica la construye basándose en parámetros de tiempo real de la red, a saber: retardo, ancho de banda, Máxima Unidad de Transmisión (MTU - *Maximum Transmission Unit*), confiabilidad, y carga de los recursos de la red. Cabe mencionar que la métrica también puede ser modificada por el administrador de la red según el valor configurado en los parámetros antes mencionados.

Una de las características importantes de este protocolo es permitir el enrutamiento de una o varias subredes a través de múltiples caminos (enlaces), convergiendo (o redireccionando) el tráfico en caso de ocurrir fallas en alguno de los enlaces.

Adicional a lo anteriormente expuesto, IGRP incluye tres tipos importantes de paquetes de actualizaciones que permiten ampliar la estabilidad de este protocolo, a saber:

- mantenimiento (“hold-down”),
- horizonte dividido (“split horizon”) e

[9] Sirgo, J.A. El Protocolo TCP/IP. Universidad de Oviedo. Pág. 11

[10] Feit, Sidnei. TCP/IP Arquitectura, protocolos e implantación con Ipv6 y seguridad de IP. 1997. Pág. 173

[11] http://www.cisco.com/warp/public/732/Tech/rtp_pc.htm

- inversa envenenada ("poison-reverse").

Los mensajes de mantenimiento previenen reinserciones inapropiadas de rutas no óptimas durante cierto período de tiempo, originadas por falla en algún enrutador o enlace de datos. Este período es calculado de manera que sea superior que el tiempo necesario para anunciar a la red entera de algún cambio en el enrutamiento. Las actualizaciones de horizonte dividido trabajan bajo la premisa de no enviar al enrutador origen información referente al enrutamiento de determinadas subredes, con el fin de evitar lazos de enrutamiento. Los mensajes de tipo inversa envenenada tienen por finalidad evitar grandes lazos de enrutamiento. Estos mensajes se envían para eliminar la ruta afectada y ponerla en modo mantenimiento.[12].

1.1.3 Protocolo Primero el Camino Abierto más Corto (OSPF)

En 1998, la Fuerza de Trabajo de Ingeniería (IETF - *Internet Engineering Task Force*) empezó a trabajar en un nuevo protocolo estándar para sustituir al RIP. El resultado fue el Protocolo de Pasarela Interior Primero el Camino Abierto más Corto (OSPF – *Open Shortest Path First*). Este protocolo es una tecnología pública sin propietario y que está definida en la RFC 1583[13] y el OSPF versión 2 está definido en la RFC 2328.

Este es un protocolo de enrutamiento con estructura "jerárquica", basado en una primera versión del protocolo IS-IS del modelo OSI, desarrollado por la IETF. Y que trabaja basándose en el algoritmo del camino más corto, así como también basándose en algoritmos de estado de enlace. OSPF es un protocolo importante porque posee un número de ventajas que no se encuentran en ningún otro protocolo de pasarela interior. Lo que lo hace la opción preferida en las nuevas redes IP, especialmente en grandes redes.

Sus actualizaciones incluyen información referente a interfaces conectadas y métricas usadas, entre otras variables. Estas actualizaciones son enviadas a los enrutadores dentro del "área común de enrutamiento" cuando existe algún cambio en el estado de los enlaces. La métrica se calcula basándose en el estado de los enlaces, y la misma permite al enrutador determinar cual es el camino más corto hacia uno o varios nodos.

Este protocolo tiene como características adicionales el enrutamiento basado en múltiples caminos con igualdad de costos, y el enrutamiento basado en requerimientos de Tipos de Servicios (TOS - Type of Service) de las capas de alto nivel del modelo ISO/OSI; este tipo de enrutamiento soporta aquellos protocolos que puedan especificar ciertos tipos de servicios. Por ejemplo, una aplicación puede requerir que ciertos datos sean enviados urgentemente, y esto es posible si el OSPF tiene disponibilidad de enlaces de alta prioridad.

El OSPF calcula su métrica basándose en la inversa del ancho de banda disponible en las interfaces de los enrutadores. Además, soporta una o más métricas. Si una métrica es usada, no se considera el TOS. Si más de una métrica es usada, el TOS es usado a través del uso de una métrica aparte (y por consiguiente, utilizándose una tabla de enrutamiento separada) para cada una de las ocho combinaciones creadas por los tres bits IP del TOS (a saber: el retardo, la eficiencia y la disponibilidad)[14].

En la Figura 1.5 se muestra un ejemplo de lo que puede ser una red basada en OSPF. En la misma se observan que las redes basadas en OSPF están organizadas en áreas. Las áreas pueden ser definidas basándose en la ubicación o a una región, o pueden estar basadas en límites administrativos. Todas las redes OSPF están formadas al menos por un área, el backbone, y tantas áreas adicionales como sean necesarias.

[12] http://www.cisco.com/warp/public/732/Tech/rtrp_pc.htm

[13] Feit, Sidnei. TCP/IP Arquitectura, protocolos e implantación con Ipv6 y seguridad de IP. 1997. Pág. 190

[14] http://www.cisco.com/warp/public/732/Tech/rtrp_pc.htm

Dentro de un área OSPF todos los enrutadores mantienen la topología de base de datos, intercambiando información de estado de enlace para mantener su sincronización. Esto asegura que los enrutadores pueden calcular el mismo mapa de red para una misma área.

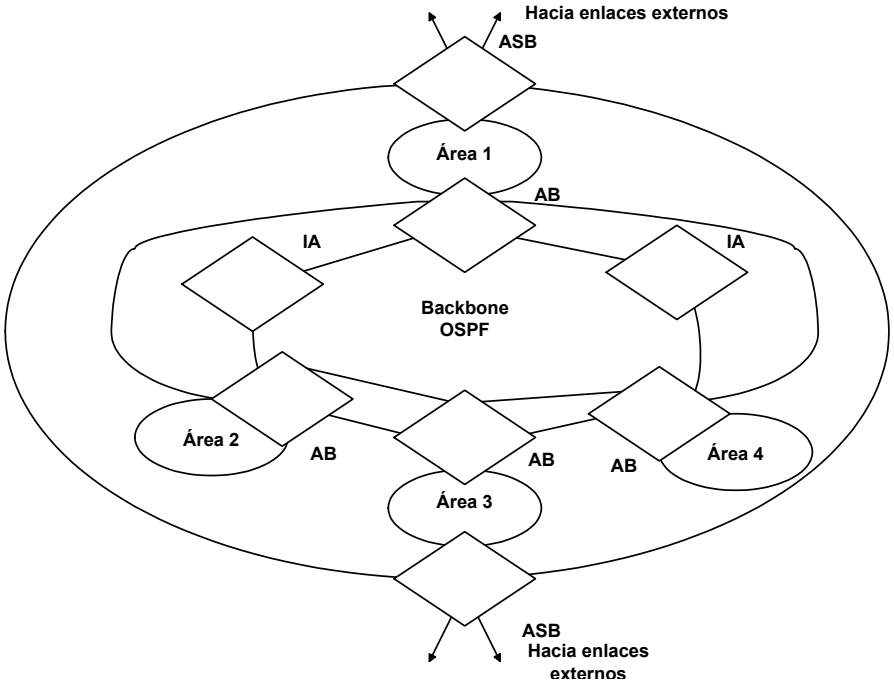


Fig. 1.5. Ejemplo de una red OSPF.

Fuente: Rodríguez, Adolfo. TCP/IP tutorial and technical Overview. IBM. 2001.

Además de las áreas, una red OSPF está compuesta por otras entidades, las cuales se listan a continuación[15]:

- *El backbone OSPF*. Esta área debe formar parte de cualquier red OSPF, a la misma se le asigna como identificador de área 0.0.0.0. El backbone tiene todas las propiedades del área, pero además tiene la responsabilidad de distribuir la información de enrutamiento a las áreas que están conectadas al mismo.
- Enrutadores de Intra-Área, límite de área y de frontera. Se pueden apreciar en la Figura 1.6. y a continuación se detalla su funcionamiento.

Enrutadores de Intra-Área (Intra-Area Routers). Estos enrutadores se encuentran situados dentro del área OSPF. Todos estos enrutadores entregan avisos de enlaces de enrutadores en esta área para definir los enlaces a los cuales se encuentran "conectados".

Enrutadores de límite de Área (Area Border Routers). A los enrutadores que se encuentren conectados a más de dos áreas se les denomina Enrutadores de límite de área. Se encargan de mantener la topología de base de datos para cada una de las áreas a las que están "conectados".

Enrutadores de Frontera (AS Boundary Routers). Estos son los enrutadores que se encuentran ubicados en la periferia de una red OSPF e intercambian información con los enrutadores en otros Sistemas Autónomos usando protocolos de pasarela exterior.

[15] Murhammer, Martin W. TCPIP Tutorial and Technical Overview. IBM

Los mensajes de OSPF se transmiten directamente en datagramas IP. Todos los mensajes OSPF comparten una cabecera común, la cual se muestra en la Fig. 1.6. Cabecera común de OSPF. Esta cabecera contiene información general, como por ejemplo: el identificador de área (ID del área) y el identificador de enrutador origen[16] (ID del enrutador o router), entre otros. Un campo define cada paquete OSPF como una de los siguientes cinco tipos posibles:

Saludo (Hello). Se usa para identificar a los vecinos, elegir un enrutador designado para una red de multienvío, para encontrar a un enrutador designado existente y para enviar señales de "estoy vivo"[17].

Descripción de la base de datos (Database description). Durante el inicio, se usa para intercambiar información de manera que un enrutador pueda descubrir los datos que le faltan en la base de datos.

Petición del estado de enlace (Link state request). 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 de enlace (Link state update). Se usa como respuesta a los mensajes de Petición del estado de enlace y también para informar dinámicamente de los cambios en la topología de la red.

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

El identificador del enrutador, identificador de área y la información de autenticación son configurables en cada enrutador OSPF.

1.1.4 Protocolo Mejorado de Enrutamiento de Pasarela de Internet (EIGRP)

El Protocolo Mejorado de Enrutamiento de Pasarela de Internet (EIGRP- *Enhanced Internet Gateway Routing Protocol*) desarrollado por Cisco Systems, combina la facilidad del uso de los protocolos tradicionales con las ventajas del rápido re-enrutamiento de los protocolos con algoritmos de estado de enlace, suministrando así capacidades avanzadas en la convergencia rápida y las actualizaciones parciales.

1.1.5 Protocolo Mejorado de Enrutamiento de Pasarela de Internet (EIGRP)

El Protocolo Mejorado de Enrutamiento de Pasarela de Internet (EIGRP- *Enhanced Internet Gateway Routing Protocol*) desarrollado por Cisco Systems, combina la facilidad del uso de los protocolos tradicionales con las ventajas del rápido re-enrutamiento de los protocolos con algoritmos de estado de enlace, suministrando así capacidades avanzadas en la convergencia rápida y las actualizaciones parciales.

Se usan mensajes simples periódicos de *saludo* para descubrir a los vecinos y para comprobar que aún están activos. Otra mejora importante de este protocolo es el uso del Algoritmo de Actualización por Difusión (DUAL – *Diffusing Update ALgorithm*). La idea básica de DUAL es simple. Se basa en la siguiente observación: *Si una ruta consistente te lleva más directo a un destino, la ruta no puede ser un bucle*.

[16] Del ingles: Originating Router Identifier

[17] Feit, Sidnei. TCP/IP Arquitectura, protocolos e implantación con Ipv6 y seguridad de IP. 1997. Pág. 198-199

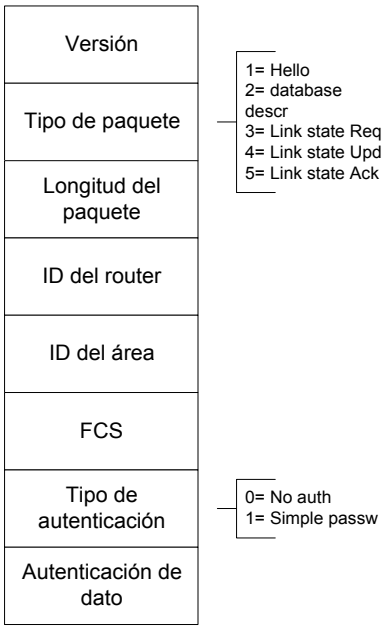


Fig. 1.6. Cabecera común de OSPF.

Fuente: Rodríguez, Adolfo. TCP/IP tutorial and technical Overview. IBM. 2001.

Cuando ocurre un cambio en la topología de la red el algoritmo de difusión, realiza la convergencia en menos de 5 segundos en la mayoría de los casos; esto equivale a la convergencia ejecutada por protocolos de enlace de estado tales como OSPF, Novell Link Services Protocol (NLSP) y por el IS-IS. Adicionalmente, EIGRP sólo envía actualizaciones de re-enrutamiento cuando ocurren cambios a los enrutadores directamente afectados.

Otra de las ventajas de este protocolo radica en que soporta protocolos de red además de IP, tales como el AppleTalk y Novell Internetwork Packet Exchange (IPX). Por otra parte, el EIGRP soporta enmascaramiento de redes con longitud variable (VLSM - *Variable-Length Subnet Mask*). EL protocolo IPX Novell Enhanced IGRP soporta actualizaciones increméntales en el Servicio de Protocolo de Aviso (SAP - *Service Advertisement Protocol*), elimina la limitación del RIP en el número máximo de saltos (a saber, de 15 saltos), y provee uso de caminos óptimos. Un enrutador ejecutando AppleTalk Enhanced IGRP realiza actualizaciones parciales y limitadas de enrutamiento y provee balanceo de cargas y uso de caminos óptimos[18].

1.1.6 Protocolo entre Sistemas Intermedios (IS-IS)

El Protocolo de Enrutamiento de entre Sistemas Intermedios (IS-IS – *Intermediate System to Intermediate System*), se definió inicialmente para los enrutadores de OSI, pero se ha extendido a redes IP[19]. (RFC 1195). Al igual que OSPF, IS-IS es un protocolo de estado de enlace que dispone de enrutamiento jerárquico, enrutamiento por tipo de servicio, división del tráfico por varias rutas y autenticación.[20]

IS-IS tiene dos tipos de rutas:

- Enrutamiento de nivel 1 dentro de un área, y

[18] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs004.htm

[19] NOTA: OSI utiliza el término *Sistema Intermedio* en lugar de enrutador o pasarela.

[20] Feit, Sidnei. TCP/IP Arquitectura, protocolos e implantación con Ipv6 y seguridad de IP. 1997. Pág. 190

- Enrutamiento de nivel 2 para enrutamiento a destinos fuera del área.

El IS-IS hace uso de dos niveles de jerarquía en el enrutamiento. Un dominio de enrutamiento es dividido en áreas. Esto es, los enrutadores del nivel 1 conocen la topología de su área, incluyendo los demás enrutadores y sistemas en su área. Sin embargo, los enrutadores de nivel 1 no conocen la identidad o los destinos de los enrutadores fuera de su área. Éstos enrutadores de nivel 1 envían todo el tráfico con destinos fuera de su área a enrutadores de nivel 2 en su área. De manera similar, los enrutadores de nivel 2 conocen la topología de nivel 2, y saben cuales direcciones están accesibles a través de un enrutador de nivel 2. Sin embargo, los enrutadores de nivel 2 no necesitan conocer la topología dentro de cualquier área de nivel 1, excepto aquellas en las que un enrutador de nivel 2 sea un enrutador de nivel 1 dentro de una sola área. Sólo los enrutadores de nivel 2 pueden intercambiar paquetes de datos o información de enrutamiento directamente con enrutadores externos localizados fuera del dominio de enrutamiento. En pocas palabras, Los enrutadores de nivel 1 se podrían ver de forma análoga a los enrutadores de la red troncal en OSPF. Un enrutador de un Sistema intermedio de nivel 1 reenvía el tráfico a destinos fuera del área a su enrutador de nivel 2 más cercano.[21]

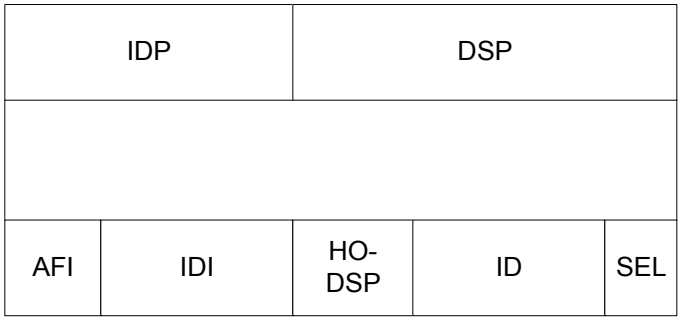


Fig. 1.7. Estructura de dirección jerárquica ISO.

Según se ilustra en la figura 2, las direcciones ISO están subdivididas en: parte del domino inicial (IDP-*Initial Domain Part*), y la parte del dominio específico (DSP-*Domain Specific Part*). El IDP está estandarizado por ISO, y específica el formato y la autoridad responsable para asignar el resto de las direcciones. El DSP es asignado por cualquier autoridad de direccionamiento especificada por el IDP. El DSP está subdividido en: HO-DSP (Hihg Order of DSP), un identificador de sistema (ID), y un selector de NSAP (SEL). El IDP junto al HO-DSP (también denominada dirección de área) identifican el dominio de enrutamiento y el área dentro del dominio de enrutamiento.

Una ventaja del uso de IS-IS integrado tiene que ver con el esfuerzo en la gestión de redes. Ya que el IS-IS integrado provee un protocolo de enrutamiento simple, dentro de un dominio de enrutamiento coordinado que utiliza un solo backbone, existe menos información que configurar.

Otra ventaja del IS-IS integrado es que utiliza menos recursos. Esto es, menos recursos de implantación (ya que sólo se utiliza un protocolo), menos recursos de CPU y memoria son usados por el enrutador, y menos recursos de red. Lo que se traduce en reducción de costos.

1.2 Protocolos de Pasarela Exterior

Los protocolos de pasarela exterior son usados para intercambiar información de enrutamiento entre redes que no comparten una administración común. Estos protocolos requieren la siguiente información antes de iniciar las tareas de enrutamiento:

- Una lista de enrutadores vecinos con los cuales intercambiar información de enrutamiento.

[21] Callon, R. Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (RFC 1195). 1990.

- Una lista de redes de acceso directo.
- El número de sistemas autonómos del enrutador local.

A continuación se detallarán los protocolos de pasarela exterior tales como el Protocolo de Pasarela Exterior (EGP – *Exterior Gateway Protocol*) y el Protocolo de Pasarela de Frontera (BGP - *Border Gateway Protocol*)

1.2.1 Protocolo de pasarela exterior (EGP)

El Protocolo de Pasarela Exterior (EGP - *Exterior Gateway Protocol*) es el primer protocolo de enrutamiento al nivel de interdominios usado entre los enrutadores del backbone principal de la Internet, documentado en el RFC 904 de Abril de 1984.

A pesar de ser un protocolo de enrutamiento dinámico, no usa métricas ni hace decisiones "inteligentes" de enrutamiento, sino que sus actualizaciones contienen la disponibilidad de redes, asumiendo que las mismas son alcanzables a través de determinados enrutadores. Éstas se efectúan entre determinados enrutadores vecinos por intervalos regulares de tiempo, indicando cada enrutador las subredes directamente conectadas al mismo. Ver Figura 1.2.

Aunque el EGP se había usado bien por algunos años, el mismo había comenzado a mostrar ciertas fallas. Por ejemplo, el EGP no tenía manera de tratar con los *lazos* de enrutamiento que ocurrían en redes con múltiples caminos, también las actualizaciones frecuentemente eran muy largas y pesadas. Además, el EGP no podía realizar decisiones de enrutamiento inteligente porque no soportaba métricas de enlaces[22], esto se logra con el protocolo BGP.

1.2.2 Protocolo de Pasarela de Frontera (BGP)

El Protocolo de Pasarela de Frontera (BGP - *Border Gateway Protocol*), definido en la RFC 1771, es un protocolo de enrutamiento externo (o entre sistemas autónomos) diseñado para corregir las fallas presentadas por el EGP, ya que detecta los *lazos* de enrutamiento y usa una métrica con el fin de realizar decisiones de enrutamiento inteligente.

Este protocolo también puede ser utilizado dentro de los sistemas autónomos, y sus actualizaciones consisten en direcciones IP de las subredes y en caminos hacia distintos sistemas autónomos. Estos caminos contienen información de sistemas autónomos a través de los cuales ciertas subredes pueden ser alcanzadas. Estas actualizaciones son enviadas usando los mecanismos de transporte al nivel de TCP.

Los datos inicialmente intercambiados entre dos enrutadores que manejen BGP se representan en una tabla completa de rutas. Las actualizaciones posteriores son enviadas cuando cambian las tablas de enrutamiento. A diferencia de otros protocolos de enrutamiento de datos, éste no requiere renovaciones periódicas y completas de las tablas de enrutamiento. En su lugar, estos enrutadores retienen la última versión de las tablas de enrutamiento de el(los) enrutador(es) vecino(s) con el(los) cual(es) se esté(n) ejecutando sesiones BGP. Aunque el BGP mantiene una tabla de enrutamiento con todos los posibles caminos hacia una subred en particular solamente anuncia el camino óptimo.

BGP usa una métrica simple para determinar el mejor camino hacia una o varias redes en particular. Esta métrica consiste en un número arbitrario que especifica el "grado de preferencia" de un enlace en particular. Comúnmente esta métrica es asignada sobre cada enlace por el administrador de la red, y este valor puede ser basado en ciertos parámetros, incluyendo el número de sistemas

[22] http://www.cisco.com/warp/public/732/Tech/rtrp_pc.htm

autónomos a través de los cuales se enrutan los datos (los caminos con el menor número de sistemas autónomos son generalmente los mejores), la estabilidad, velocidad, el retardo o el costo[23].

El protocolo BGP está compuesto por cuatro pasos principales:

- Apertura y confirmación de una conexión BGP con un enrutador vecino.
- Mantenimiento de la conexión BGP.
- Envío de información de rutas óptimas.
- Notificación de condiciones de error.

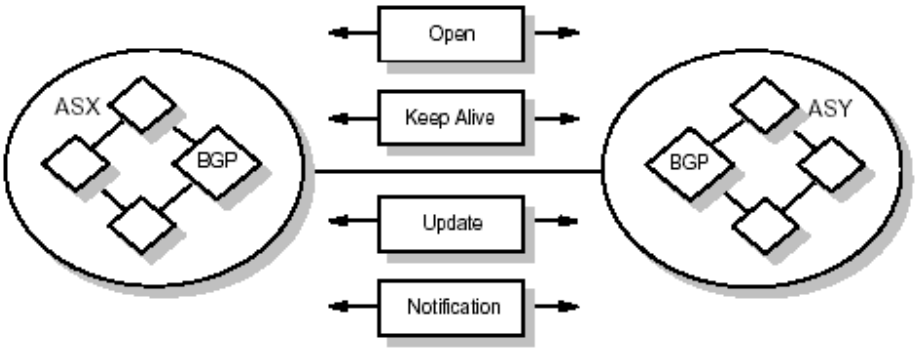


Fig. 1.8. Flujo de mensajes BGP.

Fuente: Rodríguez, Adolfo. TCP/IP tutorial and technical Overview. IBM. 2001.

Apertura y confirmación de una conexión BGP con un enrutador vecino. La comunicación BGP entre dos enrutadores se inicia con el establecimiento de la conexión del protocolo de transporte TCP. Una vez que esta conexión se establece, cada enrutador puede enviar un mensaje abierto a su vecino.

El mensaje abierto de BGP consiste de una cabecera estándar más contenidos específicos de tipo paquete. La cabecera estándar consta de un campo de 16 octetos, los cuales se ponen en todos uno cuando la el código de autenticación es 0, la longitud del mensaje de BGP (el formato de la cabecera de BGP se muestra en la figura 1.9), y el campo de tipo que especifica si el mensaje puede ser de uno de los siguientes tipos:

OPEN.

UPDATE.

NOTIFICATION.

KEEPALIVE.

El mensaje abierto define el número de AS del enrutador originador, su identificador de enrutador BGP y el tiempo de mantenimiento para la conexión. Si no se reciben mensajes keepalive, update o notification, el enrutador originador asume que existe un error y envía un mensaje de notificación y corta la conexión. El formato del mensaje abierto se muestra a continuación.

Mantenimiento de la conexión BGP. Los mensajes BGP deben ser intercambiados periódicamente entre vecinos. Si no se reciben mensajes durante un período de tiempo, el cual puede ser configurado entre 30 y 90 segundos, se asume que hubo un error de conexión. BGP usa mensajes KEEPALIVE para mantener la conexión entre vecinos. Estos mensajes KEEPALIVE consisten de un mensaje BGP solamente, no posee datos.

[23] http://www.cisco.com/warp/public/732/Tech/rtrp_pc.htm

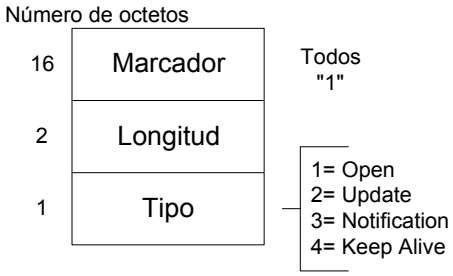


Fig. 1.9. Cabecera del mensaje BGP.

Fuente: Rodríguez, Adolfo. TCP/IP tutorial and technical Overview. IBM. 1998.

Envío de información de rutas óptimas. Esta información se intercambia entre vecinos BGP a través de mensajes de actualización. Estos mensajes de actualización son utilizados para indicar una ruta posible o para retirar del servicio rutas imposibles. A continuación se mencionan bloques básicos de un mensaje de actualización (UPDATE):

- Información de rutas óptimas de capa de red (NLRI - *Network Layer Reachability Information*).
- Atributos de camino.
- Rutas eliminadas.

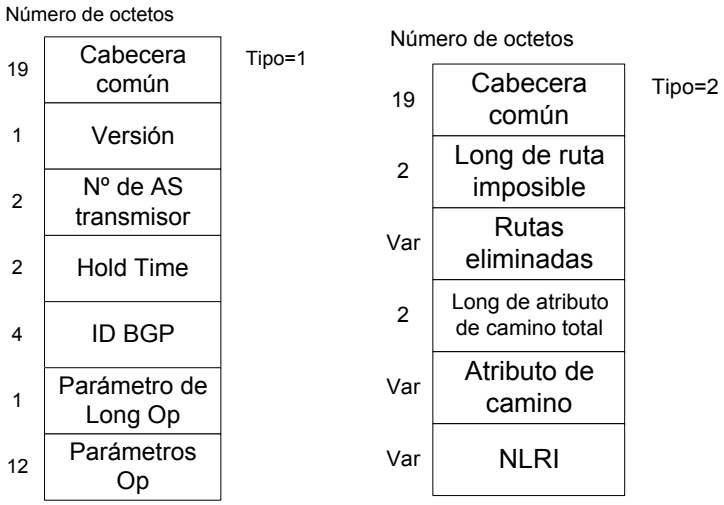


Fig. 1.10. Mensaje abierto de BGP y Formato del mensaje de actualización de BGP.

Fuente: Rodríguez, Adolfo. TCP/IP tutorial and technical Overview. IBM. 1998.

Información de Rutas Óptimas de Capa de Red (NLRI - *Network Layer Reachability Information*). Este es un mecanismo a través del cual BGP permite el enrutamiento sin clase (Classless routing). El valor de NLRI se indica en un campo variable. NRLI se representa como <longitud, prefijo>. Por ejemplo, <14,220.24.106.0> indica una ruta alcanzable de la forma 220.20.106.0 y máscara de red 255.252.0.0 o 220.24.106.0/14.

Atributo de camino. Cada atributo de camino consiste de un grupo de tres valores: bandera de atributo, tipo de atributo y valor de atributo. Cada una de las banderas proveen información acerca del estado de los tipos de atributo, y puede ser opcional o conocida, transitiva o no transitiva y parcial

o completa. Las banderas de atributo deben ser leídas en conjunto con sus tipos de atributo asociados. Existen siete tipos de atributo:

- Origen. Es un atributo obligatorio (tipo código 1), y define el origen de la ruta como un IGP, un EGP o INCOMPLETE (en el caso de una ruta estática).
- Camino AS. Es un atributo obligatorio (tipo código 2), y define los sistemas autónomos que deben ser atravesados para llevar el aviso a la red.
- Próximo salto es un atributo obligatorio (tipo código 3), y define la dirección IP del ASBR (es el próximo salto en el camino de los destinos listados).
- Multi_exit_disc es un atributo no transitivo (tipo código 4), usado por los equipos que "hablan" BGP en su proceso de decisión para discriminar entre múltiples puntos de salida hacia un sistema autónomo vecino.
- Local_pref es un atributo discrecional (tipo código 5), usado por el equipo que "habla" BGP para informar a otros equipos que "hablan" BGP acerca de otros equipos BGP en su propio AS.
- Atomic_aggregate, es un atributo discrecional (tipo código 6), usado por un equipo BGP para informar a otros equipos BGP que el sistema local ha seleccionado una ruta menos específica sin seleccionar una ruta más específica en la cual está incluida.
- Aggregator, es un atributo opcional transitivo (tipo código 7), que indica el último número de AS que formó parte de la ruta agregada, seguida por la dirección IP del equipo BGP que forma parte de la ruta agregada.

Rutas eliminadas. Una ruta imposible indica la longitud total del campo de rutas eliminadas en octetos. Si su valor es cero, indica que ninguna ruta ha sido eliminada del servicio. Este campo es de longitud variable.

Notificación de errores. Estos mensajes de notificación son enviados hacia un enrutador vecino cuando las condiciones de error son detectadas. La conexión de transporte de BGP se cierra inmediatamente después de que aparece un mensaje de notificación.

CAPÍTULO 2

2 Modo de Transferencia Asíncrona

2.1 Generalidades

ATM[24] es un estándar de la ITU-T (Unión Internacional de Telecomunicaciones) que puede ser considerado como una tecnología de conmutación de paquetes para alta velocidad con una serie de características muy particulares:

- Los paquetes son de tamaño pequeño y constante (53 bytes).
- Es una tecnología de naturaleza conmutada y orientada a conexión.
- Los nodos que componen la red no tienen mecanismos para el control de errores de flujo.
- El "header" o cabecera, de las celdas tiene una funcionalidad limitada.

En ATM el flujo de información está organizado en celdas constituidas por un campo de información y un encabezado que se transmiten en un circuito virtual y el enrutamiento se realiza basándose en un Identificador de Circuito Virtual (VCI) y a un Identificador de Camino Virtual (VPI) contenidos en el encabezado (Ver Fig. 2.1)

Cada conexión virtual es identificada por un número, cuyo significado es solo local, es decir está asociado a cada enlace. Esta función de identificación es ejecutada por dos subcampos del encabezamiento de la celda: el VPI y el VCI. El VCI identifica a un VC específico en un VP dado. Un VC es un concepto usado para describir un transporte unidireccional de celdas ATM y un VP es un concepto usado para describir un transporte unidireccional de celdas ATM pertenecientes a VCs. [25]

El propósito de los VCs y de los VPs es el de usar los conceptos de enlace virtual y conexión virtual. Los VPs permiten que la capacidad disponible en el medio físico sea dividida en un número de canales con velocidad de bit variable. Por otro lado, los VCs permiten una subdivisión más pequeña de la capacidad disponible en un VP. La conmutación puede ser ejecutada tanto a nivel del medio físico, del VP o VC. El multiplexaje y la conmutación en ATM son siempre realizados primero en los VPs y después en los VCs .

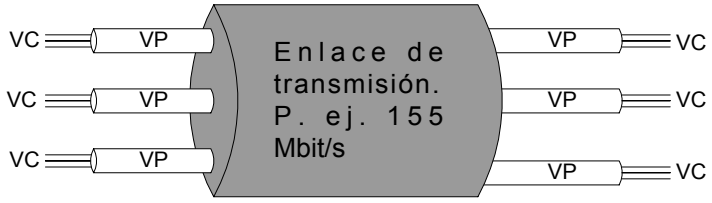


Fig. 2.1. Relación entre VC y VP.

Fuente: Understanding Telecommunications. Vol. 1.Ericsson Telecom AB, 1998.

[24] Del inglés ATM: *Asynchronous Transfer Mode*

[25] Salazar de Angulo, Maritza. Dimensionamiento de una red pública ATM. 2000. Pag. 29.

Un VC es análogo a un circuito virtual X.25 o a una conexión Frame Relay. Un camino virtual (o VP, Virtual Path) es un conjunto de VCs que tienen los mismos puntos finales. Este concepto fue desarrollado para las redes de alta velocidad con el fin de disminuir el costo del manejo de las señales de control.

Las conexiones virtuales ATM pueden proporcionarse utilizando gestión de red. Estas conexiones se denominan canales virtuales permanentes (PVC-Permanent Virtual Channels). Así mismo, los canales virtuales pueden establecerse dinámicamente utilizando procedimientos de señalización ATM. Estos canales virtuales se denominan canales virtuales conmutados (SVCs- Switched Virtual Channels).

En ATM no se asignan ranuras de tiempo específico periódicas al canal. La capacidad disponible es segmentada en las unidades de información de tamaño fijo (celdas), por tanto ATM se comporta de forma asíncrona porque transmite celdas que no necesitan ser periódicas. Se considera que ATM es un modo de transferencia eficiente y flexible, ya que al asignar ranuras según la demanda, se pueden acomodar fácilmente servicios de velocidad variable. ATM puede ganar también eficiencia en el manejo del ancho de banda multicanalizando estadísticamente fuentes de tráfico de tipo ráfaga, donde aparecen celdas a una velocidad muy alta por un período de tiempo muy corto. Este tipo de fuente no requiere una asignación continua de ancho de banda a su velocidad máxima y un gran número de estas fuentes puede compartir el mismo ancho de banda

ATM es capaz de soportar todo tipo de servicio (con y sin conexión), inclusive emulación de LAN y de circuitos, Frame Relay, WAN. Además puede soportar todo tipo de tráfico (voz, video, dato y combinaciones).

2.2 Formato de datos de las celdas ATM

Una celda ATM está formada por 53 bytes, de los cuales 5 bytes son de encabezado y 48 bytes de información (ó carga útil). Los bytes son enviados en orden creciente, empezando con el primer byte del encabezado. Dentro de un byte, los bits son enviados en forma decreciente, comenzando por el bit 8. Para todos los campos de una celda ATM, el primer bit enviado es también el bit más significativo (MSB).

El encabezado está dividido en diferentes campos, como se puede apreciar en la figura 2.2. El campo más importante es el campo de dirección, ya que identifica el circuito y provee una dirección de enlace único entre dos nodos de red, a través de los VPI y VCI.

El campo identificador de tipo de carga (PTI – *Payload Type Identifier*) específica si la celda contiene información del usuario o información a ser usada por la red misma para operación y mantenimiento por ejemplo, que permiten supervisar la calidad de la conexión y señalan eventuales congestiones presentes en los elementos de la red. El campo que define la prioridad de pérdida de celdas (CLP - *Cell Loss Priority*) permite diferenciar dos niveles de prioridad para las celdas de una misma conexión y el valor del bit CLP puede ser asignado tanto por el usuario como por la red, en el caso de que no exista espacio suficiente para todas las celdas.

El último campo del encabezado contiene un control de código cíclico (*HEC – Header Error Control*) que permite detectar y corregir un error aislado en un bit del encabezamiento y además detectar un número de errores superior o igual a dos, en cuyo caso se desecha la celda. Este último campo desempeña un papel muy importante, ya que el enrutamiento de las celdas y la propia integridad de las conexiones dependen de la interpretación del encabezamiento.

En la interfaz entre el usuario y la red (*UNI – User-Network Interface*), cuatro bits del campo VPI son reemplazados por el campo de control de flujo genérico (*GFC – Generic Flow Interface*), el

cual se emplea para controlar el uso de la capacidad de la red entre el terminal y la red. Esto es, permite implementaciones básicas de multiplexaje, es decir, puede ser utilizado por la red para controlar, en la instalación del usuario, el flujo de algunas conexiones y arbitrar el acceso a la red de varios terminales.

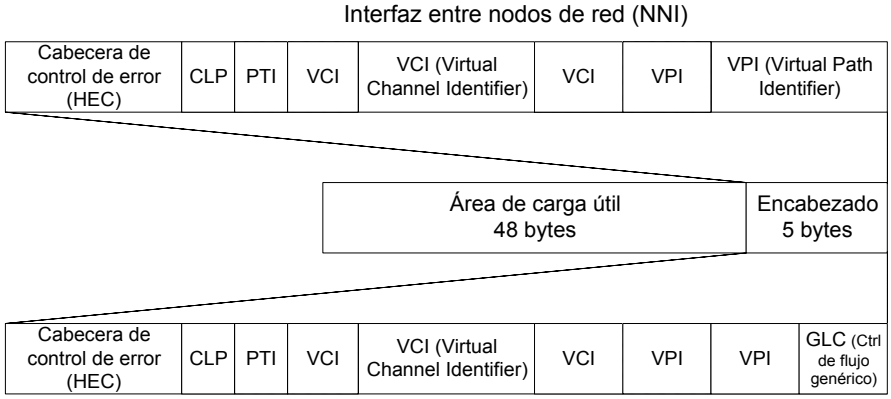


Fig. 2.2. Estructura de una celda ATM.

Fuente: Understanding Telecommunications. Vol. 1.Ericsson Telecom AB, 1998.

En la interfaz entre el usuario y la red (*UNI – User-Network Interface*), cuatro bits del campo VPI son reemplazados por el campo de control de flujo genérico (*GFC – Generic Flow Interface*), el cual se emplea para controlar el uso de la capacidad de la red entre el terminal y la red. Esto es, permite implementaciones básicas de multiplexaje, es decir, puede ser utilizado por la red para controlar, en la instalación del usuario, el flujo de algunas conexiones y arbitrar el acceso a la red de varios terminales.

2.3 Clasificación de servicios[26]

La UIT-T ha estandarizado un modelo de protocolo referencia, el cual muestra similitudes con el modelo OSI (Ver Fig. 2.3). Las tres capas más bajas son:

- Capa 1, la capa física, la cual transporta información (bits/celdas). ATM no prescribe un conjunto de reglas en particular, pero en cambio dice que las celdas ATM se pueden enviar por sí solas por un cable o fibra o bien se pueden empacar dentro de la carga útil de otros sistemas portadores. En otras, palabras, ATM se diseñó para que fuera independiente del medio de transmisión[27].
- Capa 2, la capa ATM, la cual principalmente ejecuta conmutación/enrutamiento y multiplexación. Define la organización de las celdas y dice lo que significan los campos del encabezado. Esta capa también tiene que ver con el establecimiento y la liberación de circuitos virtuales. En esta capa se localiza el control y la congestión.
- Capa 3, la capa de adaptación de ATM (AAL – *ATM Adaptation Layer*), la cual principalmente es responsable de la adaptación de los servicios de información de las celdas ATM. Esta capa permite a los usuarios enviar paquetes mayores a una celda porque la mayor parte de las aplicaciones no quieren trabajar de manera directa en celdas. Por lo que esta capa segmenta estos paquetes, transmite las celdas en forma individual y las reensambla en el otro extremo.

[26] Understanding Telecommunications. Vol. 1.Ericsson telecom AB, 1998.

[27] Tanenbaum, E. Redes de computadoras. 3era edición. Prentice-Hall. 1997. Pág. 63.

El modelo que presenta ATM es un modelo tridimensional (Ver Fig. 2.3). El *plano de usuario* se encarga del transporte de los datos, el control de flujo, la corrección de errores y otras funciones de usuario. Mientras que el *plano de control* tiene que ver con la administración de la conexión. Las funciones de gestión de capas y planos se relacionan con la administración de recursos y la coordinación intercapas.

Para permitir la transferencia de datos y servicios isócronos, la información debe ser adaptada a la red en diferentes maneras. Por esta razón, ATM ha sido dividida en cuatro clases de servicios (A, B, C y D) basándose en tres parámetros:

1. servicios isócronos y asíncronos;
2. rata de variable de bit (VBR) y constante (CBR);
3. orientado a conexión y no orientado a conexión.

Además se pueden mencionar cuatro protocolos: AAL 1, AAL 2, AAL 3/4 y AAL 5 (Ver Fig. 2.4).

En las redes ATM cada vez que una aplicación necesita establecer una conexión entre dos usuarios, debe negociarse un contrato de tráfico que especifica, entre otras cosas, la clase de servicio de la conexión. La clase de servicio ATM cubre una gama de parámetros de calidad de servicio. Estos parámetros de calidad de servicio pueden definir los niveles mínimos de ancho de banda requeridos y los límites en el retardo de las celdas y la tasa de pérdida de celdas. A continuación se detalla brevemente éstas clases de servicio.

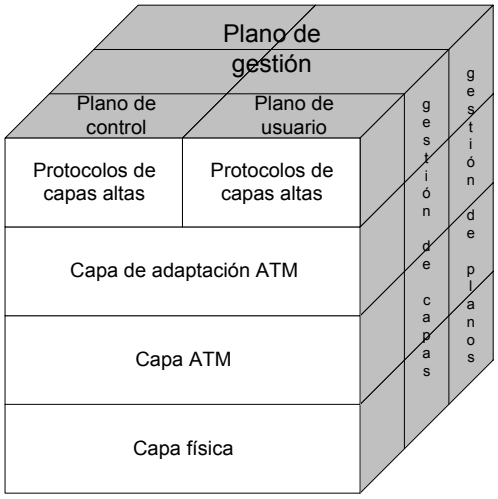


Fig. 2.3. Modelo de Capas de ATM

Constant Bit Rate (CBR): Es el tipo más sencillo de las clases de servicio ATM. Cuando una aplicación negocia el establecimiento de una conexión CBR, la red garantiza una velocidad de celda de cresta (PCR - *Peak Cell Rate*), la cual es la máxima velocidad de datos que la conexión ATM puede soportar sin riesgos de pérdida de celdas. No existen límites para la velocidad de datos que se puede negociar en una conexión CBR, pero cualquier tipo de tráfico por encima de la velocidad negociada puede ser descartado por la red.

La clase de servicio CBR provee un circuito virtual de transmisión de ancho de banda fijo y está pensada principalmente para aquellas aplicaciones que requieren un suministro de ancho de banda estable, tales como video en tiempo real y tráfico vocal.

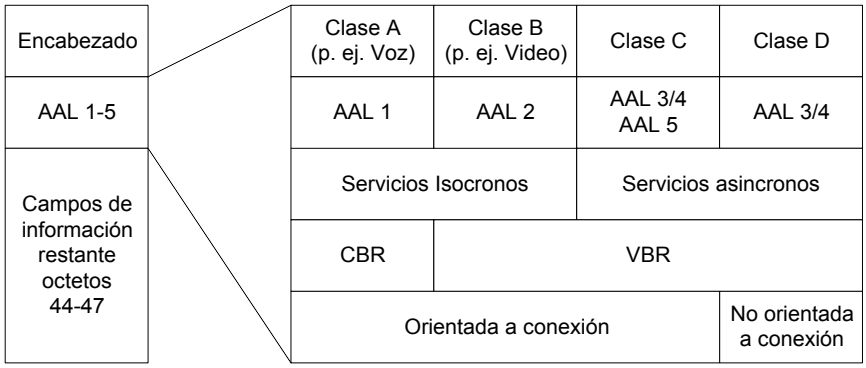


Fig. 2.4. Descripción de los servicios en la capa AAL de ATM.

Fuente: Understanding Telecommunications. Vol. 1.Ericsson Telecom AB, 1998.

Real-Time Variable Bit Rate (rt-VBR): Se parece a la clase de servicio CBR en el sentido que deseamos un retardo por bajo tránsito pero el tráfico puede variar su velocidad. Los datos pueden ser video comprimido, voz comprimida con supresión de silencio, o emulación de enlaces DIC.

Non-Real-Time Variable Bit Rate (nrt-VBR): Este es un servicio de entrega garantizado, donde el retardo de tránsito y el "jitter" son quizás menos importantes que el caso de rt-VBR. Un ejemplo de su aplicación puede ser la distribución de video codificado MPEG-2. En este caso, la información proviene de un disco y su distribución de la señal TV es de una vía. Un retardo de tránsito en la red de unos cuantos segundos no representa un problema aquí. Pero lo que sí deseamos es un servicio garantizado ya que la pérdida de algunas celdas en video comprimido tiene un efecto severo en la calidad de la conexión.[28]

Unspecified Bit Rate (UBR): No provee garantías sobre la velocidad de bits especificada, ni sobre los parámetros de tráfico ni sobre la calidad de servicio. La clase de servicio UBR ofrece una solución parcial para aquellas aplicaciones de ráfagas imposibles de predecir que no se ajustan realmente a los parámetros del contrato de tráfico. Cuando la red se congestiona, las conexiones UBR continúan su transmisión.

Las conexiones UBR no tienen contrato de gestión con la red y por lo tanto las primeras celdas que se pierden son las suyas. El caudal de tráfico exitoso puede caer a niveles inaceptables, menos del 50%. Este tipo de servicio se puede aplicar a conexiones que puedan enviar datos a través de la red sin requerir garantía de cómo y cuándo estos datos lleguen a su destino. Desde el punto de vista de la red, la clase UBR utiliza excedentes de ancho de banda que de otro modo no se emplearían.

Available Bit Rate (ABR): La clase de servicio ABR también hace uso de los excedentes del ancho de banda, pero utiliza técnicas de gestión de tráfico para estimar congestión de la red y evitar pérdidas de celdas.

Cuando una aplicación solicita una conexión ABR, la misma negocia con la red una velocidad de celda de cresta, sin embargo no negocia los parámetros específicos de tolerancia de variación de retardo de celda o de tolerancia de ráfaga. En realidad la aplicación y la red negocian un requerimiento de velocidad mínima, el cual garantiza a la aplicación un pequeño ancho de banda (la mínima requerida para mantener la aplicación establecida y funcionando). El usuario ABR acuerda no transmitir a velocidades superiores a la PCR y la red acuerda siempre proveer por lo menos la velocidad mínima (Minimum Cell Rate= MCR).

[28] IBM Corporation. Internetworking over ATM: An Introduction. Sep, 1996. Pág. 199

Dado que la clase ABR provee garantía mínimas de ancho de banda para mantener las aplicaciones en funcionamiento (pero no garantiza el retardo de la celda), ella es apta para aplicaciones en tiempo no real en las cuales los datos no son demasiado sensibles al retardo.

2.4 Señalización ATM

Señalización es el proceso mediante el cual los usuarios ATM y la red intercambian información de control, peticiones para el uso de los recursos de la red, o negociaciones para el uso de parámetros de circuitos. El par VPI/VCI y el ancho de banda requerido son escogidos como resultado de un intercambio de señalización exitoso.

Dos son los organismos que han definido los diferentes estándares de señalización utilizados por ATM. Por un lado el ITU-T (antiguo CCITT) definió el estándar Q.2931 basado en el Q.931 de la N-ISDN (Narrow-ISDN o red de servicios integrados de banda estrecha) y, por otro lado, el ATM Forum que propuso la señalización UNI 3.0 (Julio de 1993, aunque existen versiones posteriores: 3.1, y 4.0), basada en el Q.2931, que permite la interoperatividad entre diversos fabricantes y concreta aspectos genéricos de la señalización como:

1) En la Q.2931 no existe un canal común para señalización (canal D), sino un canal virtual independiente para cada terminal.

2) En lugar de negociar el acceso a un canal B, lo que se negocia es la asignación del par VCI/VPI que determina una conexión de canal virtual entre los extremos de la comunicación.

Los procedimientos de señalización Q.2931 (ITU-T) se utilizan para establecer conexiones punto a punto. La figura 2.5 muestra los mensajes extremo a extremo SETUP (Establecer) y CONNECT (Conexión) utilizados para conexiones punto a punto. Los otros mensajes como CALL PROCEEDING (Llamada en proceso) y CONNECT_ACK (Conexión reconocida) tienen significado local. Los mensajes de señalización se identifican mediante la "referencia de llamada" y se protegen utilizando temporizadores de supervisión. Cuando expira el temporizador, la llamada terminará si no existe respuesta. Esta capacidad proporciona a los mensajes de señalización unicidad e indica que son recientes/nuevos. Para SVCs, se puede incluir en los mensajes SETUP y CONNECT mecanismos de autentificación e intercambio de claves. Si el usuario llamado pone a uno una determinada bandera del mensaje CONNECT, el emisor enviará utilizando la opción de mensaje "conexión disponible". Los elementos de información serán similares a los utilizados en los flujos OAM (Operation, Administration and Maintenance).

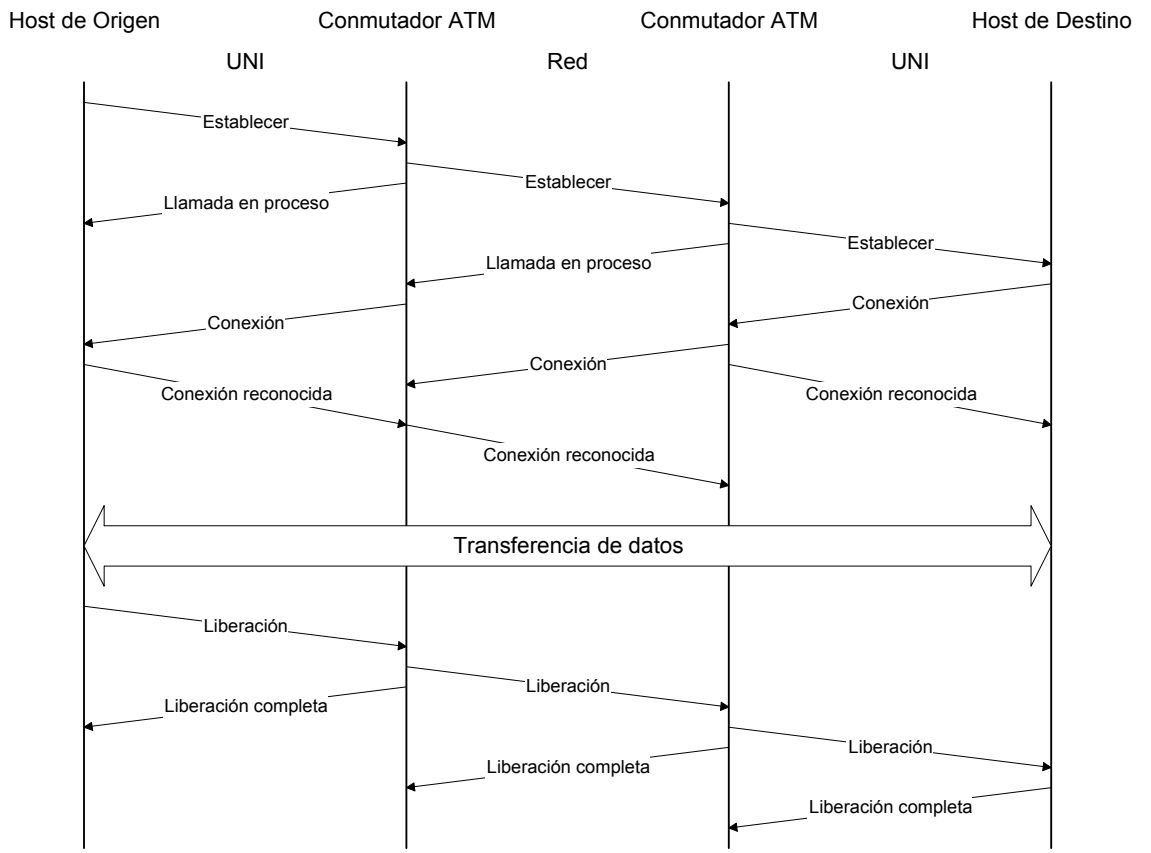


Fig. 2.3. Establecimiento y liberación de una conexión en una red ATM.

Fuente: Tanenbaum, Andrew. Redes de Computadoras. 3era Edición. Pág. 454.

2.5 Direccionamiento

La tecnología ATM se ha identificado como el modo de transferencia para implementar la RDSI (Red Digital de Servicios Integrados) de banda ancha, una red universal que soporta diferentes aplicaciones y categorías de clientes. Muchas de estas aplicaciones implican datos sensibles o flujos de información muy valiosa. Por tanto, la seguridad de red es una cuestión crítica en los servicios ATM ofrecidos. El Forum ATM se encuentra actualmente desarrollando una arquitectura de seguridad para los servicios de red ATM, en ella se divide el problema de la seguridad en:

- Seguridad del Plano de Usuario (extremo a extremo o conmutador a conmutador).
- Seguridad del Plano de Control.
- Seguridad del Plano de Gestión.
- Control de Acceso.

La seguridad del Plano de Usuario tiene que ver con la seguridad de los Canales Virtuales (o VCs) establecidos entre usuarios finales. Al igual que otros tipos de redes, la seguridad del VC del plano de usuario extremo a extremo implica soportar las siguientes necesidades:

1.- Autentificación de las entidades del plano de usuario. La autentificación requiere que la entidad a ser autentificada tenga un nombre distinguible (o ID, Identifier) y una clave asociada. Las entidades de ATM pueden identificarse utilizando dos formatos de direcciones, mediante formato NSAP (especificada por el Forum ATM) y con el formato E.164.

2.- Confidencialidad de los VCs, lo que supone protegerse contra posibles escuchas clandestinas.

3.- Integridad de Datos en los VCs, lo que significa detectar los posibles esfuerzos para alterar los datos

Una de las diferencias entre ATM y los protocolos convenciones como X.25 y TCP/IP es que los protocolos convencionales incluyen señalización de control en el mismo canal que la transferencia de datos, mientras que ATM utiliza señalización de canal común que se encuentra separada del canal de transferencia de datos. El OAM (Operations, Administration and Maintenance) de las conexiones ATM es una parte del plano de gestión, que realiza las funciones de coordinación relativas a los planos de usuario y de control. Las funciones incluyen monitorización del rendimiento, detección de fallos y defectos, localización de fallos y gestión del sistema.

El estándar de direccionamiento propuesto por la ITU-T se basa en el uso de direcciones (parecidas a los números telefónicos) para redes ATM (B-ISDN) públicas. Mientras que el ATM Forum, extendió el direccionamiento de ATM para incluir redes privadas, eligiendo el modelo de direccionamiento de subred, en el que la capa ATM es la responsable del mapeo de direcciones de la capa de red hacia direcciones de la capa ATM. Este modelo de subred es una alternativa para el uso de direcciones de protocolo de la capa de red (como el IP y el IPX) y los protocolos de enrutamiento existentes (como el IGRP y el RIP). Asimismo definió un formato de direcciones que se basa en la estructura de las direcciones de los NSAP (Puntos de Acceso al Servicio de la Red) de OSI, que tiene una longitud fija.

Modelo de direccionamiento de la subred:

El modelo de direccionamiento de la subred desacopla la capa ATM de cualquier protocolo existente en las capas superiores como pudiera ser el IP o el IPX. Como tal, requiere un esquema de direccionamiento y un protocolo de enrutamiento completamente nuevos, es por ello que a todos los sistemas ATM se les debe asignar una dirección ATM, además de cualquier otra dirección de los protocolos de las capas superiores. Para poder realizar todo esto se requiere un ATM_ARP (Protocolo de Resolución de Direcciones ATM) con el que comparar las direcciones de las capas superiores con las direcciones ATM correspondientes.

Direcciones ATM con formato NSAP:

En la norma **ITU-T E.164** se ha definido la forma de numeración para ATM en la red pública. Se trata de una secuencia decimal jerárquica similar a la telefónica. El ATM Forum extendió el concepto para redes privadas mediante un direccionamiento similar al NSAP del servicio CLNP de ISO. Se requiere de un protocolo de resolución de direcciones ATM (**ATM_ARP**) para mapear las direcciones de niveles superiores.

Para su uso dentro de las redes privadas ATM, se designan direcciones ATM con formato NSAP de 20 bytes, en tanto que las redes públicas típicamente utilizan direcciones E.164, conformadas tal y como lo define la ITU-T. El Forum de ATM especificó una codificación NSAP para direcciones E.164, que se utilizará para codificar direcciones E.164 en redes privadas, sin embrago, algunas de éstas también pueden utilizar esta dirección. Una dirección ATM completa puede ser escrita de la siguiente forma: 47.0091.8100.0000.0800.200c.1001.0800.200c.1001.01.

Dichas redes privadas pueden basar su propio direccionamiento (formato NSAP) en la dirección E.164 de la UNI (Interfase de red de usuario) pública a la que están conectadas y pueden tomar el prefijo de la dirección del número E.164, identificando los nodos locales por medio de los bits de orden inferior.

Todas las direcciones ATM con el formato NSAP constan de tres componentes: **AFI** (Identificador de Autoridad y de Formato), **IDI** (Identificador del Dominio Inicial) y **DSP** (Parte Específica del Dominio). AFI identifica el tipo y formato de IDI, que, a su vez, identifica la ubicación de la dirección y la autoridad administrativa. La DSP contiene la información real del enrutamiento.

Los tres formatos de direccionamiento privado de ATM difieren en cuanto a la naturaleza de AFI e IDI. En el formato E.164 codificado por NSAP, el IDI es un número E.164. en el formato DCC, el DNI es un DCC (Código de Datos del País), que identifica a los diferentes países, como lo especifica la ISO 3166. Dichas direcciones son administradas por el Cuerpo Nacional de Miembros de la ISO en cada país. En el formato ICD, el IDI es un ICD (Asignador de Códigos Internacionales), asignado por la autoridad de registro del ISO 6523 (el Instituto Británico de Estándares). Los códigos ICD identifican a las diferentes organizaciones internacionales particulares.

El Foro de ATM recomienda que las organizaciones o los proveedores de servicios de redes privadas utilicen ya sea el formato DCC o el ICD para conformar su propio plan de numeración.

La figura siguiente muestra los tres formatos de direcciones ATM que se utilizan en las redes privadas.

Campos dirección en ATM:

AFI	DCC (2)	DFI	AA	Reservado	RD (2)	AREA (2)	ESI (6)	SEL

Formato ATM de DCC

AFI	ICD (2)	DFI	AA	Reservado	RD (2)	AREA (2)	ESI (6)	SEL

Formato ATM de DCC

AFI	E.164 (8)	RD (2)	AREA (2)	ESI (6)	SEL

Formato E.164 de NSAP

Las descripciones siguientes se refieren a los campos que se muestran en la figura anterior:

- *Identificador de la Autoridad y del Formato (AFI-Authority and Format Identifier):* 1 Byte que identifica el tipo de formato de la dirección (E.164, ICD o DCC, respectivamente: 45, 47 o 39).

- Código de datos del País (DCC-Data Country Code): Identifica a los países en particular.

- Parte Específica del Dominio de Orden Superior (HO-DSP- High Order Domain Specific Part): consta de 1 byte. Combina el RD (Dominio de Enrutamiento) y el Identificador de Área (AREA) de las direcciones NSAP. El Foro de ATM combinó estos campos para soportar una jerarquía de direccionamiento multinivel flexible para los protocolos de enrutamiento basados en prefijos.

- Parte Específica del Dominio (DFI -Domain Specific Part -DSP- Format Identifier): Consta de 1 Byte. Indica el formato de la continuación de la dirección.

- *Autoridad Administrativa (AA-Administration Authority)*: 3 Bytes. Precisa la autoridad administrativa en carga del dominio de direccionamiento.

- *RD (Routing Domain)*: Define el número de dominios de encaminamiento (2 Bytes).

- Identificador del Sistema Terminal (ESI-End System Identifier): Especifica la dirección MAC de 48

bits que administra el IEEE.

- *SEL (Selector):* Se utiliza para el multiplexaje local dentro de las estaciones terminales y no tiene significado en la red.

- Designador del Código Internacional (ICD-International Code Designator): Identifica a las organizaciones internacionales particulares.

- *E.164*: Indica la dirección E.164 de B-ISDN (8 octetos es decir 16 cifras).

2.6 ATM frente a IP

En estos últimos años se está debatiendo mucho entre los potenciales proveedores de servicio acerca de cual va a ser el estándar para las conexiones con los clientes finales en los próximos años, IP sobre redes 10baseT o bien ATM. Ambas soluciones son relativamente similares y sólo se diferencian en el equipo específico que requieren y no en la cantidad del mismo. A modo de resumen podríamos citar los siguientes puntos.

Ventajas de IP:

- Ethernet 10baseT es básicamente autoregulable.
- Ya existen tarjetas de red para plataformas PC a muy bajo coste.
- 10baseT es un estándar de la industria.
- Las redes LAN están muy extendidas y funcionan correctamente.
- Hay gran cantidad de expertos en esta tecnología.
- El software y los drivers necesarios ya están implementados.

Ventajas de ATM:

- El transporte de video streaming ya ha sido probado con éxito.
- Mezclar diferentes tipos de servicio es mucho más simple que en IP (voz, datos, video,...)
- Las velocidades de transmisión cumplen los estándares de tasa de transporte para telefonía (DS-3, STS-1).
- Alta implementación vía conmutación hardware con conmutadores que trabajen a terabits en un futuro cercano
- Ancho de banda dinámico para tráfico intenso y según el requerimiento de la aplicación permitiendo un alto aprovechamiento de los recursos de la red; la mayoría de las aplicaciones son o pueden ser vistas como de tipo a ráfagas.
- Posibilidad de simplificación vía arquitectura VC
- Escalabilidad en velocidad y tamaño de la red.
- Arquitectura común para LAN/WAN.
- Las nuevas aplicaciones y drivers se están diseñando para soportar ATM.

Este tema parece bastante candente en la actualidad porque ambas arquitecturas confluyen y conviven en la actualidad, de hecho en muchos casos las redes de ordenadores corren sobre IP y los backbones sobre los que se sostienen están implementadas en ATM, creando autenticas WAN sobre ATM. De todos modos, la principal discusión se centra en los costes reales de montar una u otra red, los servicios que serán capaces de soportar y el tiempo de respuesta que serán capaces de proporcionar. Parece ser que si la necesidad es para servicios de tipo datos como pudieran ser conexiones a Internet, teletrabajo u otros similares la opción clara es la de una red sobre IP dado que el hardware y software requerido para implementarlas está ya disponible a muy bajo coste. Las redes ATM serían la solución idónea para toda una serie de nuevos servicios que están apareciendo como videoconferencias o vídeo bajo demanda, que necesariamente requieren de cierta QoS. Es cierto que paralelamente se está intentando adaptar la tecnología IP para poder ofrecer este tipo de servicios, y ya se han hecho diversas pruebas con, por ejemplo, protocolos RSVP o depuraciones de telefonía sobre IP que proporcionan una mayor eficiencia. La paradoja es

que todas estas nuevas adaptaciones no están todavía disponibles en su gran mayoría mientras que los estándares ATM están prácticamente completos y probados con éxito en diferentes entornos. Eso y el hecho de que ya existan en la actualidad gran cantidad de redes ATM nos lleva a pensar que difícilmente pueda llegar, en un futuro próximo, a sustituir IP a ATM, más bien que seguirán entrelazándose y cubriendo sus carencias mutuas, creando como casi siempre en telemática una curiosa y compleja amalgama de protocolos estándares y dispositivos.

CAPÍTULO 3

3 Arquitectura MPLS.

3.1 Antecedentes

Para entender mejor las ventajas de la solución MPLS, demos un vistazo a las tecnologías de integración de los niveles 2 y 3 que la precedieron.

- IP sobre ATM
- Conmutación IP

3.1.1 IP sobre ATM

A mediados de los años 90 IP fue conquistando terreno como protocolo de red ante otras arquitecturas que se encontraban en uso como: SNA, IPX, AppleTalk, OSI, etc. El gran auge de la Internet y su explosivo crecimiento generó un déficit de ancho de banda, ya que los "backbones" IP de los proveedores de servicio (NSP-*Network Service Provider*) estaban construidos con enrutadores conectados por líneas dedicadas, lo que ocasionaba congestión y saturación de las redes. Había entonces que idear otras alternativas de ingeniería de tráfico.

La respuesta de los proveedores o ISPs fue el incremento del número y de la capacidad de los enlaces. Del mismo modo, se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo.[29]

Por lo tanto, los esfuerzos se centraron en aumentar el rendimiento de los enrutadores tradicionales, tratando de combinar de diversas maneras, la eficacia y rentabilidad de los conmutadores ATM (capa 2 del modelo OSI) con las capacidades de control de IP (capa 3 del modelo OSI).

A favor de integrar los niveles 2 y 3 estaban las infraestructuras de redes ATM que comenzaban a desplegar los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los ISPs. Por un lado, proporcionaba mayores velocidades (155 Mpbs) y, además, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implantación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de ISPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de enrutadores IP sobre una topología real de conmutadores ATM. Cada enrutador se comunica con el resto

[29] Canalis, María Sol. MPLS “Multiprotocol Label Switching”. Universidad Nacional del Nordeste. Argentina. 2002.

mediante los circuitos virtuales permanentes (PVC) que se establecen sobre la topología física de la red ATM, desconociendo la topología real de la infraestructura ATM que sustenta los PVC. En la figura 3.1 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre ATM.

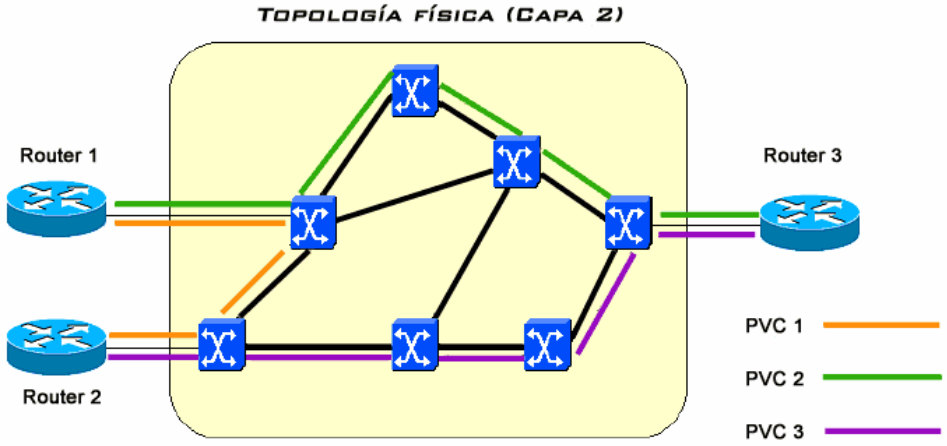


Fig. 3.1. Topología Física (capa 2)

Fuente: MPLS: Una arquitectura de backbone del siglo XXI. Revista Red IRIS.

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y enrutamiento) y el envío de las celdas por hardware (conmutación). En realidad los circuitos (PVCs) se establecen a base de intercambiar etiquetas en cada conmutador de la red, por lo tanto asociando etiquetas entre todos los elementos ATM se determinan los PVCs.

Más adelante se verá que el intercambio de etiquetas es uno de los componentes fundamentales en la arquitectura MPLS. Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas. La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del backbone; el papel de los enrutadores IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software.

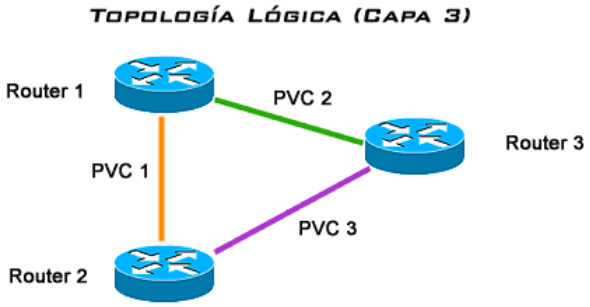


Fig. 3.2. Topología Lógica (Capa 3).

Fuente: MPLS: Una arquitectura de backbone del siglo XXI. Revista Red IRIS.

En la figura 3.2 se representa el modelo IP/ATM con la separación de funciones entre lo que es enrutamiento IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2

(control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y 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. En los casos de ISPs de primer nivel que poseen y operan el backbone ATM para ofrecer el servicio de sus redes IP, los caminos físicos de los PVCs se calculan a partir de la necesidades del tráfico IP, utilizando la clase de servicio ATM UBR (UBR - Unspecified Bit Rate), ya que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes del ATM para control de la congestión y clases de servicio). La ingeniería de tráfico se hace a base de proporcionar a los enrutadores los PVCs necesarios con una topología lógica entre enrutadores totalmente superpuestos. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de las 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.

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costos de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", una cabecera aproximada 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 superpuestas. Por ejemplo, en una red con 5 enrutadores externos con una topología virtual totalmente superpuesta sobre una red ATM. Son necesarios 5 x 4 =20 PVCs (uno en cada sentido de transmisión). Si se añade un sexto enrutadores se necesitan 10 PVCs más para mantener la misma estructura (6 x 5=30). Una ventaja adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP.

3.1.2 Conmutación IP[30]

Nació como respuesta a los requerimientos de mantener una convergencia entre el enrutamiento de IP y la conmutación ATM [2]. El nombre de conmutación de *IP,* (IP s*witching*) engloba dos términos antagónicos. *IP:* un protocolo no orientado a conexión, basado en enrutamiento, y *Conmutación*: método empleado por las redes ATM, gracias a la cual son posibles todas sus funcionalidades. Se basa en un mecanismo de intercambio de etiquetas al igual que Tag Switching.

Se caracteriza por no ocultar la verdadera topología de la red a la capa IP, evitando, entre otras cosas complejidad y duplicación de funcionalidad.. Sin embargo, ciertos artículos que analizan pruebas sobre este sistema indican que el protocolo no ha sido lo suficientemente cuidadoso con el manejo de direcciones. Esto conlleva a que su escalabilidad se ve limitada en redes grandes debido al gran número de circuitos virtuales que se requieren para cada conexión.

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

[30] Canalis, María Sol. MPLS “Multiprotocol Label Switching”. Universidad Nacional del Nordeste. Argentina. 2002.

switching) o "conmutación multinivel" (multilayer switching). Una serie de tecnologías privadas - entre las que merecen mencionarse: 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 Router (CSR) de Toshiba, condujeron finalmente a la adopción del actual estándar MPLS del IETF. El problema que presentaban tales soluciones era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3). A continuación se mencionan los fundamentos de esas soluciones integradoras, ya que permitirá luego comprender mejor la esencia de la solución MPLS.

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

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

En la figura 3.3 se representa la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros enrutadores para la construcción y el mantenimiento de las tablas de encaminamiento. Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde el interfaz de entrada al de salida a través del correspondiente hardware de conmutación.

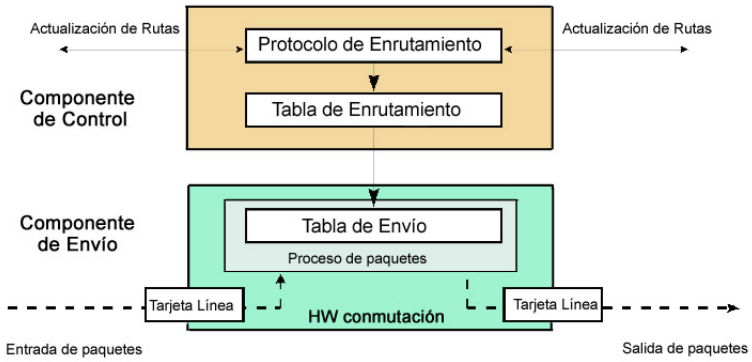


Fig. 3.3. Componente de control y componente de envío.

Fuente: Fuente: MPLS: Una arquitectura de backbone del siglo XXI. Revista Red IRIS.

Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ellas se puede implementar y modificar independientemente. El único requisito es que la componente de encaminamiento 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 encaminamiento.

En cuanto a la etiqueta que marca cada paquete, decir que es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo y que identifica una "clase equivalente de envío" (FEC - *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 encaminamiento convencional IP por prefijos de red (longest-match) una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo. 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.

Para el envío de datos, se realiza un intercambio de etiquetas (2). Una etiqueta es un campo de unos pocos bits y de longitud fija, que se añade a la cabecera del paquete y que identifica a una "clase equivalente de envío" (FEC, "Forwarding Equivalente Class"). Como se verá más adelante al explicar con detalle el protocolo MPLS, una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aún cuando sus destinos finales sean diferentes.

3.2 MPLS

El problema fundamental que presentaban las diferentes soluciones de conmutación IP era la falta de interoperatividad entre los productos de diferentes fabricantes. Además de esto, la mayoría de estas soluciones usaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas.

El protocolo MPLS aparece como una solución que se adapta al rápido crecimiento y a la diversidad en los servicios de Internet y los requerimientos de combinar tráfico de datos, voz y multimedia y que permite resolver el problema de las demandas en el incremento de ancho de banda.

Debido a esta problemática, el grupo de trabajo de ingeniería en Internet (IETF - *Internet Engineering Task Force*) decidió desarrollar un nuevo protocolo llamado Multiprotocolo de Conmutación de Etiqueta (MPLS - *Multiprotocol Label Switching*) el cual está basado en un protocolo de conmutación desarrollado por Cisco, conocido como Tag Switching Protocol. La arquitectura de una red MPLS se encuentra definida en la RFC 3031.

Sin embargo, no es sino hasta finales de los años 90 cuando la tecnología MPLS comienza a emerger como una manera de mejorar el desempeño de las redes IP. A medida que los trabajos acerca de la tecnología MPLS progresaban, el interés de la industria en esta tecnología y sus aplicaciones crecía rápidamente. De manera, que los proveedores de servicio comenzaron a crear redes experimentales y muchos suplidores incorporaron la tecnología MPLS dentro de sus dispositivos.[31]

Tradicionalmente, sólo las redes clásicas de conmutación de circuitos ATM permitían la diferenciación de servicios y ofrecían políticas de calidad de servicio (QoS). Sin embargo, esto implicaba altos costos de infraestructura y amplio conocimiento por parte del operador. Como una solución a esta situación el protocolo MPLS resulta ser una solución efectiva y a buen costo con la cual se pueden lograr los requerimientos antes mencionados. El protocolo MPLS facilita el uso de múltiples servicios sobre redes IP sin necesidad de tener múltiples redes con: mecanismos de transporte, protocolos de enrutamiento y direccionamiento completamente diferentes.

En resumen los objetivos establecidos por ese grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM.

[31] MPLS: Ready for Revenue. MPLS Forum, 2002.

- MPLS debía soportar el envío de paquetes tanto bajo demanda unidifusión (unicast) como multidifusión (multicast).
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP.
- MPLS debía permitir el crecimiento constante de la Internet.
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

3.3 Protocolos y funciones en una red MPLS

3.3.1 Conceptos básicos en la conmutación de etiquetas

Antes de explicar como trabaja una red MPLS, deben ser aclarados varios conceptos básicos que aplican para cualquier tecnología de conmutación. A saber: [32]

a. Enrutamiento. Éste es un término usado para describir las acciones tomadas para mover paquetes a través de una red. Los protocolos de enrutamiento tales como: el RIP y el OSPF le permiten a cada máquina saber cuál es la dirección que corresponde al "próximo salto" necesario para que el paquete llegue a su destino.

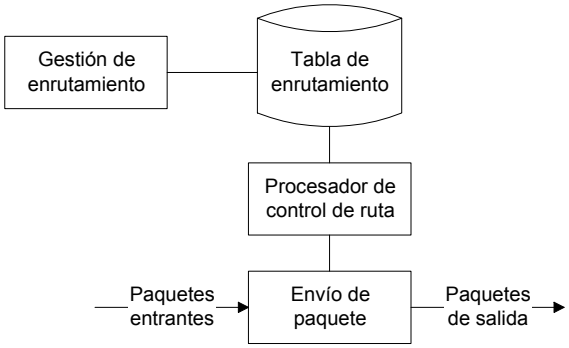


Fig. 3.2. Funciones que ocurren en un enrutador.

b. Conmutación. Es un término generalmente usado para describir la transferencia de datos desde un puerto de entrada hasta un puerto de salida de una máquina.

c. Conmutación de etiqueta. *Éste es un término utilizado para describir la tecnología genérica que combina las tecnologías de capa 2 (capa de enlace de datos) y capa 3 (capa de red). La solución de conmutación de etiqueta puede caracterizarse por el uso del envío de paquetes con etiquetas intercambiadas combinada con los protocolos de control de IP y un mecanismo de distribución de etiqueta.*

d. La componente de control *crea y mantiene una tabla de envíos para el nodo en uso. Trabaja en conjunto con los componentes de control de otros nodos para distribuir la información de enrutamiento de manera consistente y segura, y también asegura los procedimientos para crear las tablas de envíos locales. Los protocolos estándares de enrutamiento tales como:*

[32] Ryan, Jerry. Multiprotocol Label Switching (MPLS). 1998. Página 13.

OSPF, BGP y RIP, son usados para intercambiar la información de enrutamiento entre los componentes de control.

e. La componente de envío *realizan los envíos de los paquetes, utilizando información de la tabla de envío, que es mantenida por el enrutador. Esta información es enviada o por el paquete mismo y por un paquete de procedimientos locales para tomar las decisiones de envío.*

f. Una tabla de envío *(forwarding table). Está formada por un grupo de entradas a una tabla que provee información para ayudar al componente de envío a ejecutar la función de conmutación. La tabla de conmutación debe asociar cada paquete con una entrada que provee instrucciones de donde debe ir el paquete.*

g. Una equivalencia de clase de envío (FEC – Forwarding Equivalence Class). Es un conjunto de *paquetes; que comparten los mismos atributos (dirección destino, VPN, entre otras) y/o requieren el mismo servicio (multicast, QoS, etc.), que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes. El FEC se asigna en el momento en que el paquete entra a la red. Todos los paquetes que forman parte del FEC, siguen un mismo LSP. Por ejemplo, en el encaminamiento convencional IP por prefijos de red una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo. Un ejemplo de una clase de equivalencia de envío es el grupo de paquetes unicast cuyas direcciones de destino son iguales a un prefijo particular de una dirección IP. Otro ejemplo, se trata de un grupo de paquetes cuyas direcciones fuente y destino son la misma. Ver Fig. 3.3.*

h. *Una* etiqueta *(label) es un identificador relativamente corto, de longitud compuesta y no estructurado que puede ser usado en el proceso de envío. Las etiquetas están asociadas con un FEC a través de un proceso de ordenamiento (binding). Las etiquetas poseen un carácter local para un determinado enlace de datos, y por lo tanto no poseen carácter global como lo tiene una dirección. Un paquete puede tener una o más etiquetas apiladas (jerarquía). Cuando un paquete atraviesa dominios interiores a otros dominios, es cuando se produce el apilamiento de etiquetas. El LSR siempre consultará la etiqueta de nivel superior. La etiqueta se añade, de forma general, entre las cabeceras de nivel 2 y 3 (Ethernet, PPP...). En el caso de ATM y FR, se utilizan espacios en las cabeceras existentes de nivel 2 (VPI/VCI y DLCI respectivamente). Casos análogos a las etiquetas son los DLCIs (DLCI-*Data Link Connection Identifier*) usados en una red Frame Relay o los VPI/VCIs (VPI/VCI-*Virtual Path Identifier/Virtual Circuit Identifier*) utilizados en un entorno ATM.*

i. *Camino de etiqueta conmutada (LSP - Label-Switched Path) sobre el cual ocurre la transmisión de datos. Los LSPs son una secuencia de etiquetas a lo largo de cada uno de los nodos en el camino de la fuente al destino. Los LSPs se establecen bien sea por prioridad en la transmisión de datos (control de envío) o por detección de un cierto flujo de datos (envío de datos). Además, este camino puede establecerse tanto mediante protocolos de enrutamiento como manualmente. Ver Fig. 3.4.*

j. *Dominio MPLS. Es una porción de una red que contiene dispositivos que entienden MPLS. Ver Fig. 3.4.*

k. *El Enrutador de etiqueta de frontera (LER - Label Edge Router). Es un dispositivo que opera en los límites de acceso de la red y dentro de un dominio MPLS. Y permite utilizar la información de enrutamiento para asignar etiquetas a datagramas y entonces enviarlos a un dominio MPLS. Este enrutador permite la conexión de múltiples puertos conectados a redes diferentes (tales como Frame Relay, ATM, y Ethernet) y envía este tráfico a una red MPLS luego de establecer los caminos de etiqueta conmutada (LSP - Label-Switched Path), usando el protocolo de señalización de etiqueta (LSP – Label Signalling Protocol) en el ingreso y la distribución del tráfico de vuelta a las redes de acceso en la salida. Los LER juegan un rol importante en la asignación y remoción de etiquetas, cuando el tráfico ingresa o cuando sale de una red MPLS.*

l. *El enrutador de etiqueta conmutada (LSR - Label switching router) es un dispositivo de alta velocidad que posee el componente de control IP (por ejemplo, protocolos de enrutamiento,*

RSVP, etc.) y un componente de envío de etiquetas intercambiadas (label swapping) y que típicamente reside en el medio de una red y es capaz de enviar datagramas basados en etiquetas. Es importante acotar que los LSRs pueden ser interior o extremo. Los LSRs de los extremos o límites de la red añaden o eliminan etiquetas. En un LSR, un algoritmo de intercambio de etiquetas usa la etiqueta del paquete y una tabla de envíos basada en etiquetas para obtener una nueva "etiqueta" y una interfaz de salida para el paquete, y así establecer un camino de etiqueta conmutado (LSP – Label-Switched Path).

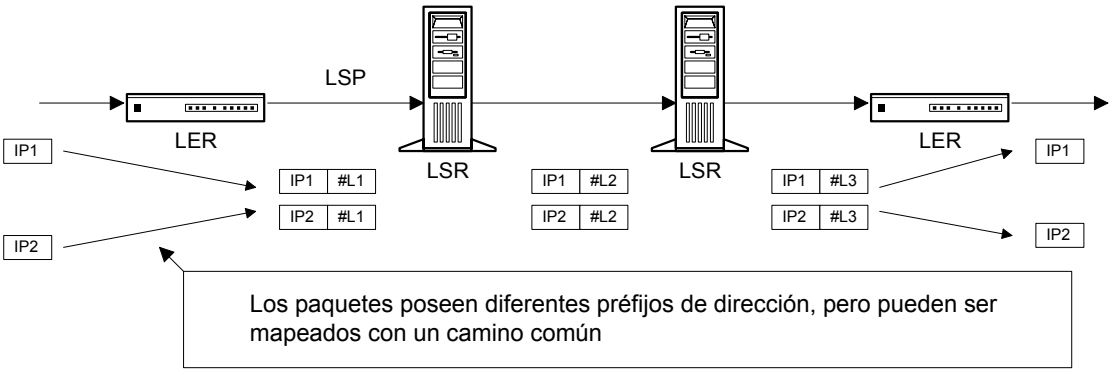


Fig. 3.3. Ilustración del funcionamiento de la clase de equivalencia de envío.

Fuente: Marshak, Marik. Multi Protocol Label Switching. 2000.

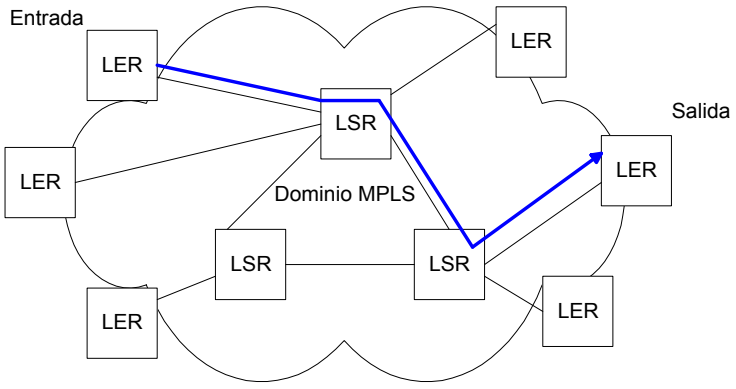


Fig. 3.4. Diferentes conceptos dentro de una red MPLS.

Fuente: Marshak, Marik. Multi Protocol Label Switching. 2000.

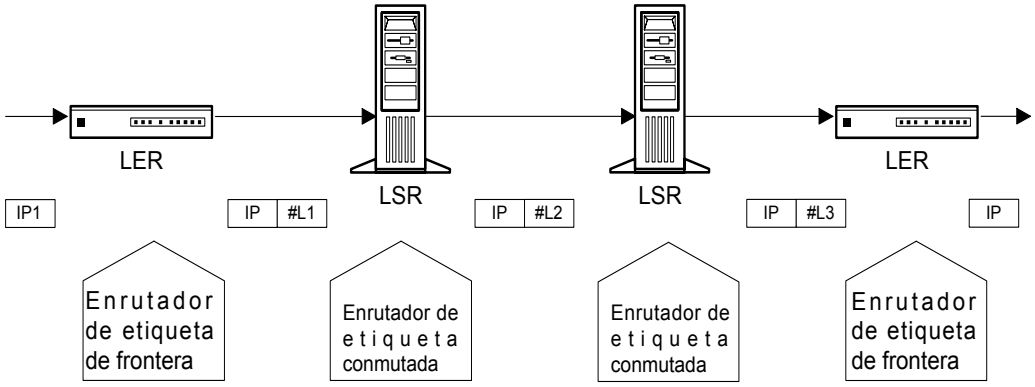


Fig. 3.5. Etiquetado en la frontera, intercambio en el medio.

Fuente: Marshak, Marik. Multi Protocol Label Switching. 2000.

3.4 Descripción funcional de MPLS

La operación de la tecnología MPLS se basa en los componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí. Básicamente, el funcionamiento del protocolo MPLS debe seguir los siguientes pasos:

- Creación y distribución de etiquetas
- Creación de tablas en cada enrutador
- Creación de LSPs
- Agregar etiquetas a los paquetes con la información de la tabla.
- Envío del paquete

3.4.1 Funcionamiento del envío de paquetes en MPLS

La base de la tecnología MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (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. Cada LSP se crea a base de concatenar uno o más saltos en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Switching Router) a otro, dentro del dominio MPLS. Un LSR no es sino un enrutador especializado en el envío de paquetes etiquetados por MPLS.

En la Fig. 3.6 se puede ver la funcionalidad de MPLS. Compárese con los esquemas vistos antes en las figuras 2 y 3 para observar las analogías y diferencias. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (forwarding). Del mismo modo, el envío se implanta mediante el intercambio de etiquetas en los LSPs. Sin embargo, la tecnología MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento 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: Label Distribution Protocol, LDP, 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 encaminamiento ATM: esto lo resuelve el procedimiento de

intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos basado en celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. Los equipos entre ambos son LSRs interiores del dominio MPLS. Un LSR es como un enrutador que funciona a base de intercambiar etiquetas basándose en una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control, según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la Fig. 3.7 se ilustra un ejemplo del funcionamiento de un LSR del núcleo MPLS. A un paquete que llega al LSR por la interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por la interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

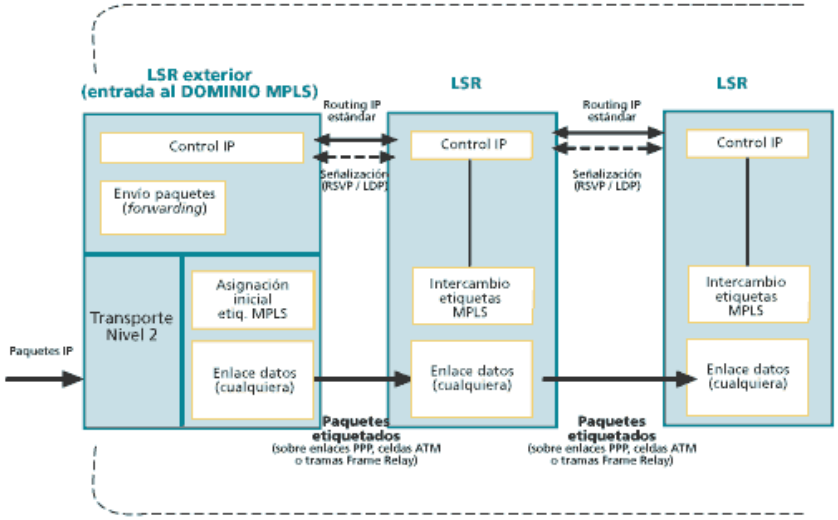


Fig. 3.6. Esquema funcional de MPLS.

Fuente: MPLS: Una arquitectura de backbone del siglo XXI. Revista Red IRIS.

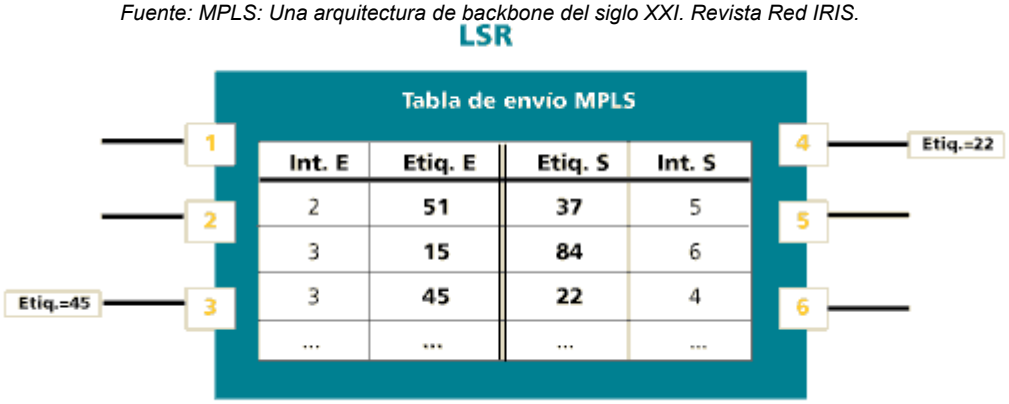


Fig. 3.7. Detalle de la tabla de envío de un LSP.

Fuente: MPLS: Una arquitectura de backbone del siglo XXI. Revista Red IRIS.

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 LSR de cabecera. En la figura 3.8 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera 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 LSR de cola (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 utilizando enrutamiento convencional.

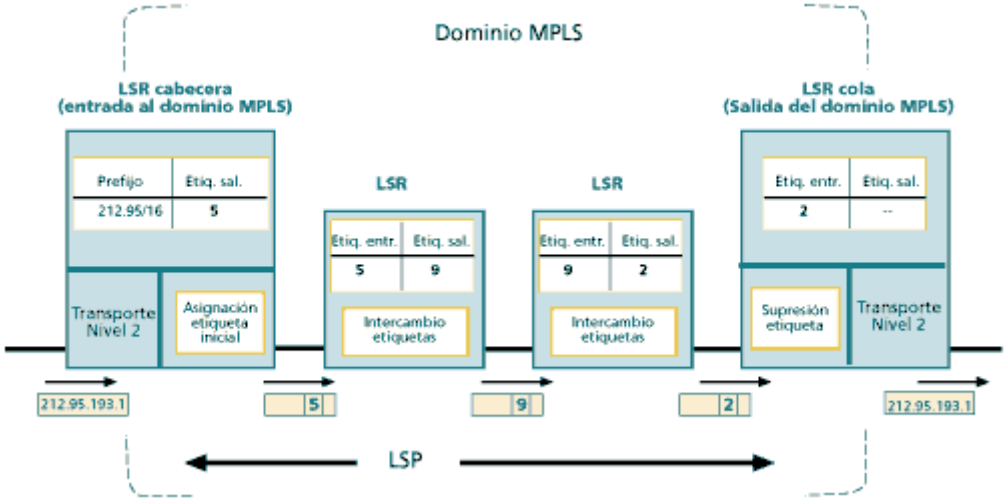


Fig. 3.8. Ejemplo de envío de un paquete por un LSP.

Fuente: MPLS: Una arquitectura de backbone del siglo XXI. Revista Red IRIS.

3.4.2 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 tales como: topología, patrón de tráfico y características de los enlaces, entre otros. Ésta información es la que manejan los protocolos internos IGP (OSPF, IS-IS, RIP, entre otros) para construir sus tablas de encaminamiento (recuérdese que los LSR son enrutadores con funcionalidad añadida). MPLS utiliza la información de estos protocolos para establecer los caminos virtuales o LSPs. Para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las rutas 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 o no orientada a conexión). 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 para soportar MPLS; uno de ellos es el protocolo RSVP[33] y BGP en las formas conocidas como MPLS-BGP, MPLS-RSVP-TUNNELS. También se están definiendo nuevos protocolos específicos para la distribución de etiquetas, como lo es el LDP (Label Distribution Protocol) y CR-LDP (Constraint Based Routing Label). RSVP es preferido por IETF, LDP por Cisco y el CR-LDP por Nokia.

Las diferentes variaciones en el intercambio de etiquetas son:

- LDP: mapea los destinos IP (unicast) en etiquetas.
- RSVP, CR_LDP: es usado para ingeniería de tráfico y reserva de recursos.
- BGP: para etiquetas externas (VPN).

3.4.3 Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la Fig. 3.9, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de enrutadores IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de enrutadores a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología de malla (directamente o por los PVCs de ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de enrutadores). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario.

A continuación se hará una breve descripción de cómo funciona MPLS (Ver Figura 3.9)[34]:

Paso 1. La red automáticamente crea las tablas de enrutamiento, utilizando protocolos de pasarela interior tales como OSPF, IS-IS, RIP, entre otros. El protocolo LDP usa la topología de enrutamiento en las tablas para establecer los valores de las etiquetas entre dispositivos adyacentes. Esta operación crea los LSPs, preconfigurando mapas entre puntos de destino. Contrario a lo que sucede con los circuitos virtuales permanentes (PCV) usados en ATM, los cuales requieren una asignación manual de VPIs/VCIs, las etiquetas son asignadas de manera automática.

Paso 2. Un paquete ingresa al FSR frontera (Edge LSR) de entrada, y éste procede a determinar cuales servicios de la capa 3 son requeridos como por ejemplo QoS y manejo de ancho de banda. El LSR de frontera, basado en el enrutamiento y las pólizas, selecciona y asigna una etiqueta a la cabecera del paquete y lo entrega al backbone.

---

[33] RSVP del Modelo de Servicios Integrados del IETF (recuerde que ése era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, que es el caso del LDP (Label Distribution Protocol). Para mayor información se recomienda consultar las referencias correspondientes del IETF.

[34] Redford, Rob. Enabling Business IP Services with Multiprotocol Label Switching. Cisco Systems, 1999. Pág. 3.

Paso 3. El LSR de la nube lee la etiqueta de cada paquete, la reemplaza con una nueva según se lista en su tabla de enrutamiento, y entrega el paquete al destino. Los LSRs de la nube (backbone) conmutan los paquetes mediante el intercambio de etiquetas.

Paso 4. El LSR de frontera (Edge LSR) de salida elimina la etiqueta, lee la cabecera del paquete y lo envía a su destino final.

El uso de etiquetas permite separar los tipos de tráfico tales como tráfico de mejor esfuerzo y tráfico para misión crítica, lo que hace a MPLS una solución altamente escalable. Las etiquetas usadas en MPLS tienen significado local, lo cual hace casi imposible quedarse sin etiquetas. Esta característica es esencial para implementar servicios avanzados de IP tales como: QoS, VPNs, e ingeniería de tráfico. En la figura 3.10 se presenta un ejemplo para examinar la manera en que los paquetes son enviados.[35]

- Como se puede apreciar en la Fig. 3.10, llega un paquete al LSR de frontera, el cual lee el prefijo de destino del paquete, que resulta ser 128.89.Resto, el LSR frontera busca la dirección de destino en su tabla de conmutación e inserta la etiqueta correspondiente, en este caso 4, luego envía el paquete a través de la interfaz 1.
- El LSR de la red MPLS lee la etiqueta y verifica si se encuentra en su tabla de conmutación, luego reemplaza la etiqueta 4 por la etiqueta 9, y lo envía a través de la interfaz 0.
- El enrutador de salida lee y busca la etiqueta 4 en su tabla, el cual indica que se debe eliminar la etiqueta y enviar el paquete a través de la interfaz 0.

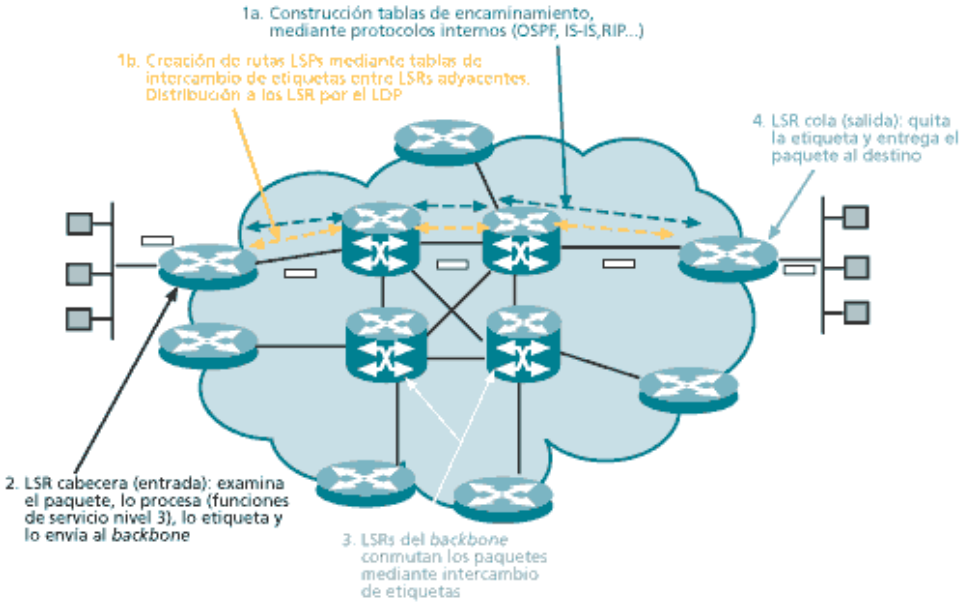


Fig. 3.9. Funcionamiento de una red MPLS.

Fuente: MPLS: Una arquitectura de backbone del siglo XXI. Revista Red IRIS.

[35] Redford, Rob. Enabling Business IP Services with Multiprotocol Label Switching. Cisco Systems, 1999. Pág. 4.

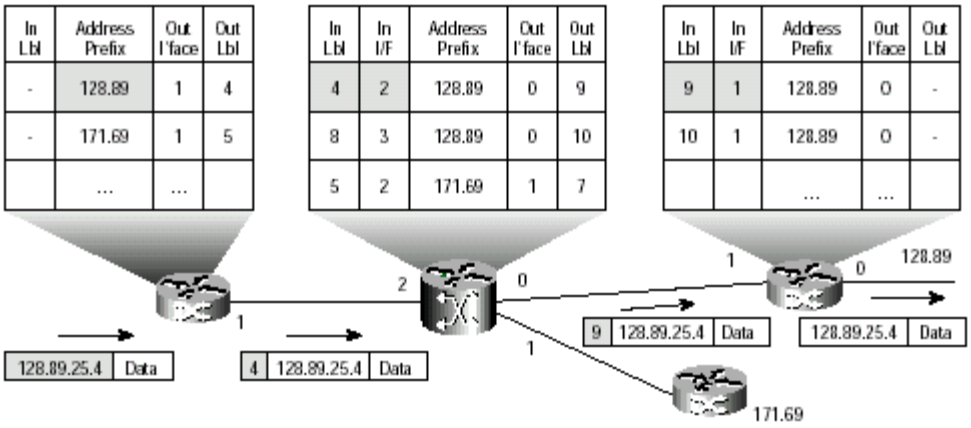


Fig. 3.10. Tratamiento de los paquetes enviados a una red MPLS.

Fuente: Redford, Rob. *Enabling Business IP Services with Multiprotocol Label Switching. Cisco.*

CAPÍTULO 4

4 Descripción funcional de MPLS

4.1 Conmutación de etiquetas. Descripción y componentes básicos

La conmutación de etiquetas es una forma avanzada de envíos de paquetes que reemplaza el envío convencional de direcciones y que posee un algoritmo de intercambio de etiquetas más eficiente. Se pueden mencionar las tres principales diferencias entre conmutación de etiquetas y el enrutamiento convencional a continuación:

	Enrutamiento convencional	Conmutación de etiquetas
Análisis completo del encabezado IP	Ocurre en todos los nodos.	Ocurre sólo una vez en la frontera de la red, cuando la etiqueta es asignada.
Permite Unicast y Multicast	Requiere múltiples algoritmos complejos de envío.	Requiere de sólo un algoritmo de envío.
Decisiones de enrutamiento	Basada sólo en la dirección.	Puede estar basada en cualquier número de parámetros, tales como QoS, membresía a una VPN.

Tabla 4.1. Comparación entre conmutación de etiquetas y enrutamiento convencional.[36]

La Fig. 4.1 muestra una red sencilla de conmutación de etiquetas. En ella podemos apreciar que el LSR de frontera (Edge LSR) provee las funciones de entrada y salida, y el LSR del núcleo ofrece la conmutación de alta velocidad.

Una red de conmutación de etiquetas tiene el mismo propósito que cualquier red de enrutamiento convencional: entrega el tráfico a uno o más destinos. La adición de envío basado en etiquetas complementa el enrutamiento convencional pero no lo reemplaza.

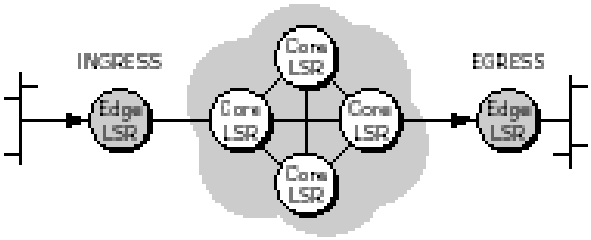


Fig. 4.1. Red simple de conmutación de etiquetas.

[36] Marshak , Marik . Multiprotocol label switching. 2000.

4.1.1 Componente de envío

Una etiqueta puede ser asociada a un paquete en varias maneras. Algunas redes pueden introducir la etiqueta en la cabecera de la capa de enlace de datos (como sucede con los VCI/VPI de ATM, y los DLCI de Frame Relay). Otra opción es forzarlo a estar dentro de una pequeña cabecera que se encuentra entre la cabecera de enlace de datos y las unidades de protocolo y datos del enlace de datos (por ejemplo, entre la cabecera de la capa 2 y los datos entregados por la capa 3).

En la frontera de una red MPLS, los LSR de frontera (Edge LSR) hacen la clasificación y toman decisiones de envío al examinar las cabeceras IP en los paquetes sin etiquetar. Como resultado, se le colocan etiquetas apropiadas a dichos paquetes y estos son enviados a un LSR que funciona como el próximo salto hacia el destino final.

La generación por parte de un LSR de “etiquetas” de longitud variable, como una representación corta de la cabecera del paquete IP, reduce la complejidad de procesamiento en los nodos subsecuentes de la red. Es importante recordar que la etiqueta se genera durante el procesamiento de la cabecera en el nodo LSR. Por supuesto que la etiqueta cambia en cada LSR de la red.

Por otro lado, en el caso de paquetes que deben salir de una red MPLS, los LSR de frontera se encargan de remover cualquier etiqueta antes de permitir el envío de los mismos.

Cuando un LSR dentro de un dominio MPLS (llamado también Core LSR) recibe un paquete etiquetado, ésta es extraída y es usada como un índice dentro de una tabla de envío que posee el LSR en cuestión. Cuando se encuentra la entrada indexada por la etiqueta entrante, la etiqueta de salida se extrae y adiciona al paquete, luego el paquete se envía hacia la interfaz de salida hacia el próximo salto(s) que están especificados en la entrada.

4.1.2 Componente de control

El componente de control utiliza los protocolos estándar de enrutamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros enrutadores para la construcción y el mantenimiento de las tablas de enrutamiento. Al llegar los paquetes, el 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.

Las etiquetas son agregadas a los paquetes por los LSR de subida (upstream). Los LSR de bajada (downstream) que reciben estos paquetes deben saber o descubrir que hacer con ellos. Esta tarea es ejecutada por el componente de control en la conmutación de etiqueta. El componente de control utiliza el contenido de una entrada de la tabla de envío para conmutación de etiqueta como guía.

El establecimiento y el mantenimiento de estas tablas de entradas son funciones esenciales y deben ser ejecutadas por cada LSR. El componente de control es responsable por la distribución de la información de enrutamiento a cada LSR en una manera consistente y de ejecutar los procedimientos que son usados por los LSR para convertir esta información en una tabla de envío.

Basado en la información de enrutamiento provista por OSPF o IS-IS, LDP (*Label Distribution Protocol*) intercambia las etiquetas requeridas por la función de envío. En un entorno de

paquetes, LDP se utiliza en el esquema de asignación de etiqueta de bajada, el cual trabaja de la siguiente manera: por cada ruta de entrada a su tabla de enrutamiento, el enrutador de etiqueta conmutada (LSR- *Label Switch Router*) localiza una etiqueta y crea una entrada en su Base de información de etiqueta enviada (LFIB- *Label Forwarding Information Base*) con la de etiqueta entrante. El LSR entonces advierte el indexado entre la etiqueta (entrante) creada y la ruta a otros enrutadores de etiqueta conmutada adyacentes. Cuando un LSR recibe información de indexado de etiqueta para una ruta y esa información es originada para el próximo salto de esa ruta, el conmutador le asigna un valor a la etiqueta de salida en la entrada asociada del LFIB asociado con la ruta. El procedimiento mencionado se muestra en la figura siguiente.

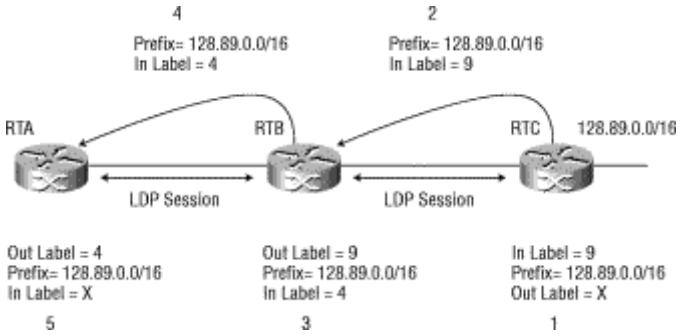


Fig. 4.2. Asignación de etiqueta de bajada.

Fuente: MPLS and IP Quality of Service In Service Provider ATM Networks. Cisco Systems. 2002

Los protocolos de enrutamiento proveen a los LSR el mapeado entre los FEC y el próximo salto de las direcciones. Además, el LSR debe:

- Crear índices entre las etiquetas y los FEC.
- Distribuir esos índices a otros LSRs.
- Construir su propia tabla de etiquetas de envío.

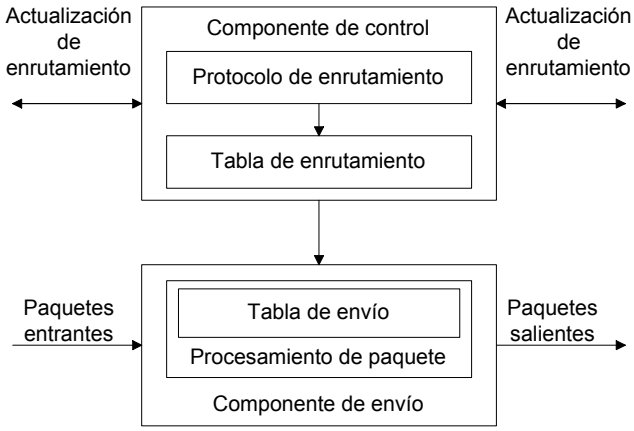


Fig. 4.3. Componentes de envío y de control.

4.1.2.1 Creación de etiquetas e índices (bindings)

Una etiqueta, en su forma más sencilla, identifica el camino que el paquete seguirá. Una etiqueta es llevada o encapsulada dentro de la cabecera del paquete en capa 2. La cabecera de MPLS se conoce también con el nombre de "Tag". Al recibir el paquete el enrutador lo examina y según el

contenido de la etiqueta determina el próximo salto. Una vez que el paquete ha sido etiquetado, el resto del viaje del paquete se basa en conmutación de etiquetas. Los valores de la etiqueta poseen significado local, lo que significa que realizarán saltos entre LSRs solamente.

Una vez que un paquete ha sido clasificado con una clase de equivalencia (FEC) nueva o ya existente, se le asigna una etiqueta al mismo. Dado que el encapsulado de MPLS se realiza sobre diferentes tipos de medios, los valores de las etiquetas se derivan de la capa de enlace de datos. Por ejemplo, si la tecnología de capa 2 permite campos de etiqueta (tales como: los VPI/VCI de ATM o los DLCI de Frame Relay), ésta encapsulará la etiqueta de MPLS. Sin embargo, si la tecnología de capa 2 no permite el uso de campos de etiqueta (por ejemplo, PPP/LAN), la etiqueta de MPLS es encapsulada en una cabecera MPLS estandarizada, denominada cabecera "shim", la cual se inserta entre la capa 2 y las cabeceras de IP. Ver Fig. 4.4 La cabecera MPLS permite que cualquier tecnología pueda manejar etiquetas MPLS lo cual facilita el manejo de los valores de las etiquetas.

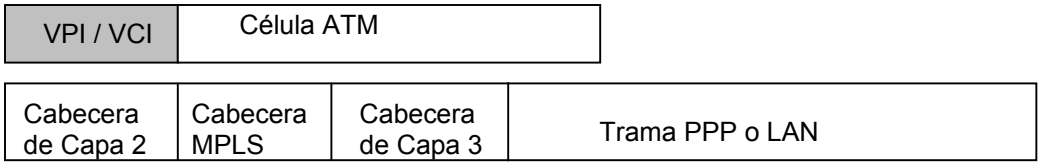


Fig. 4.4. Etiquetas MPLS en ATM y PPP/LAN.

La cabecera de MPLS de 32 bits contiene los siguientes campos. No tiene cola, sino solamente cabecera. Esta cabecera está formada por cuatro campos, gráficamente representados en la Fig. 4.5:

- **Etiqueta.** Este campo lleva el valor de la etiqueta de MPLS. Tiene una longitud de veinte bits, con lo que puede haber hasta 2^{20} = 1.048.576 valores. Aunque realmente hay dieciséis valores menos, ya que desde el valor cero hasta el quince están reservados.
- **CoS (Clase de servicio).** Este campo consta de tres bits que permiten diferenciar distintos tipos de tráfico y favorecer un tipo de tráfico con respecto otro. Con tres bits se dispone de ocho posibles valores para el tipo de servicio. Por esto este campo se usa cuando la red entra en congestión, en cuyo caso los paquetes sufren retardos. La idea es minimizar el retardo en ciertos paquetes que son muy sensibles a él, como por ejemplo los de voz sobre IP, y penalizar con un poco de retardo el tráfico menos sensible como el WebHTTP, que realmente no tiene especificaciones importantes en este sentido.
- **Stack (S).** Este bit indica si hay varias cabeceras MPLS o si la que se está usando en ese momento es la única. Además, permite que exista una pila de jerarquía de etiqueta. Las cabeceras MPLS se comportan como si estuvieran apiladas una sobre otra. El enrutador siempre va a ver la que esté en lo alto de la pila y si se inserta una nueva cabecera, esta se pondrá encima de las anteriores.
- **TTL.** El campo de time-to-live, de 8 bits. El campo TTL tiene la misma función que en un paquete IP. Su utilidad reside en que cuando un paquete IP entra en un entorno MPLS, el campo TTL que en ese momento lleva el paquete IP se copia en esta parte de la cabecera MPLS. A partir de ese momento se usa de la misma forma que si fuese un paquete IP (se decrementa una unidad por cada salto). Al llegar al enrutador de salida (egress router), el valor que en ese momento está activo en la cabecera MPLS es el que se copia en el paquete IP. A partir de este momento la red se comportaría como IP pura.

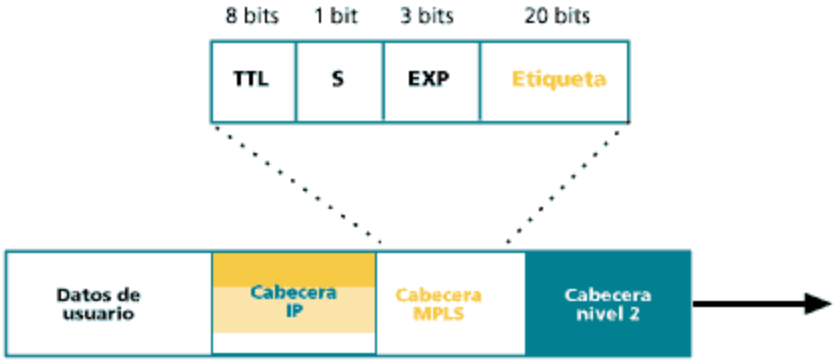


Fig. 4.5. Campos de la cabecera de MPLS.

Como se puede ver, ni los valores del CoS ni los de Stack ni los de TTL son útiles a la hora de determinar el próximo salto del paquete, pero sí son importantes a la hora de tratar el paquete en un nodo intermedio. Por ello fueron introducidos en la cabecera MPLS.

Merece la pena recordar el significado local de las etiquetas. Una etiqueta sólo tiene significado en un enrutador. Por eso, el mismo paquete va cambiando esta etiqueta en cada salto que da (a no ser que ocurra una coincidencia y sean iguales en algunos saltos). Las etiquetas son requeridas por la clase de equivalencia de envío (FEC), y por tanto necesarias, cuando ocurren eventos que indican la necesidad de binding. Estos eventos pueden ser divididos en dos categorías:

- **Índice de datos entregados** (Data-driven bindings) ocurren cuando el tráfico comienza a fluir, siendo entregados al LSR (LSR- Label Switching Router) y reconocido como un candidato para conmutación por etiqueta.
- **Índice de control de entregas** (Control-driven bindings), los cuales se establecen como un resultado de la actividad en el plano de control y son independientes de los datos. Los índices de etiqueta (Label bindings) pueden ser establecidos en respuesta a una actualización en el enrutamiento o la recepción de mensajes RSVP. Este método permite escalar los procesos de mejor manera que el método mencionado anteriormente. Y por esta razón es usado en MPLS.

Las decisiones de asignación de etiquetas pueden ser basadas en los siguientes criterios de envío:

- Enrutamiento de destino unicast.
- Ingeniería de tráfico.
- Multicast.
- Red virtual privada (VPN).
- QoS.

Las etiquetas usadas por un LSR para ubicación de etiquetas FEC utilizan las siguientes categorías:

- **Por plataforma.** Los valores de las etiquetas son únicos a través de todo el LSR. Las etiquetas son asignadas en un grupo común. De manera que no pueden existir dos etiquetas distribuidas en diferentes interfaces que tengan el mismo valor.
- **Por interfaz.** Los rangos de etiquetas están asociados con interfaces. De manera que diferentes grupos de etiquetas son definidas por las interfaces, y las etiquetas provistas en esas interfaces son asignadas por grupos separados. Los valores de la etiqueta asignados por diferentes interfaces podrían ser iguales.

4.1.2.2 Distribución de la etiqueta de información

Una entrada para una tabla de envíos de conmutación de etiquetas debe proveer, al menos, información acerca de la interfaz de salida y una nueva etiqueta. También debe contener otra información como por ejemplo, indicar la disciplina para tratar (queuing) de realizar el envío del paquete saliente. La etiqueta entrante solo identifica una entrada simple a esta tabla.

La distribución de etiqueta se realiza utilizando uno de los dos métodos siguientes:

- **Distribución de etiqueta "downstream"** (Downstream Label Distribution). Con este método el LSR de subida (upstream) descubre el "próximo salto" para un FEC particular, genera una etiqueta para el FEC, y comunica el indexado (binding) al LSR de bajada (downstream). Si el LSR de subida (upstream) es el próximo salto para el FEC, puede usar esa etiqueta sabiendo que su significado será entendido.
- **Distribución de etiqueta downstream por demanda** (Downstream-on-Demand Label Distribution). El LSR de bajada (downstream) reconoce al LSR de subida (upstream) como el próximo salto para el FEC. Se realiza una búsqueda en el LSR upstream para obtener un indexado entre el FEC y una etiqueta. Si el LSR de subida (upstream) reconoce el FEC y tiene un próximo salto para él, éste crea un indexado y lo reenvía al LSR de bajada (downstream). En este momento, ambos LSRs tienen una información común.

Cada etiqueta distribuida debe ser indexada a una entrada en la tabla de envío. Para MPLS, las entradas en una tabla de envíos se establecen como se muestra en la Tabla 4.2.

La arquitectura MPLS usa control local (que consiste en que el LSR puede decidir crear y avisar un índice sin necesidad de esperar la recepción de un índice para el mismo FEC por parte de un vecino) y control de salida (el LSR espera un índice por parte de su vecino de bajada antes de ubicar una etiqueta y avisarlo de subida).

Algunos mecanismos de señalización se mencionan a continuación:

- **Solicitud de etiqueta** (Label request). Al usar este mecanismo, los LSR solicitan una etiqueta a su vecino de bajada (dowstream) de manera que puede identificar a un FEC específico. Este mecanismo puede ser utilizado desde la cadena de LSRs hasta los LER de salida, esto es, el punto en el cual el paquete deja el dominio MPLS.
- **Mapeado de etiqueta** (Label mapping). Representa la respuesta a la solicitud de etiqueta, un LSR de bajada enviará una etiqueta a un iniciador de subida usando este mecanismo.

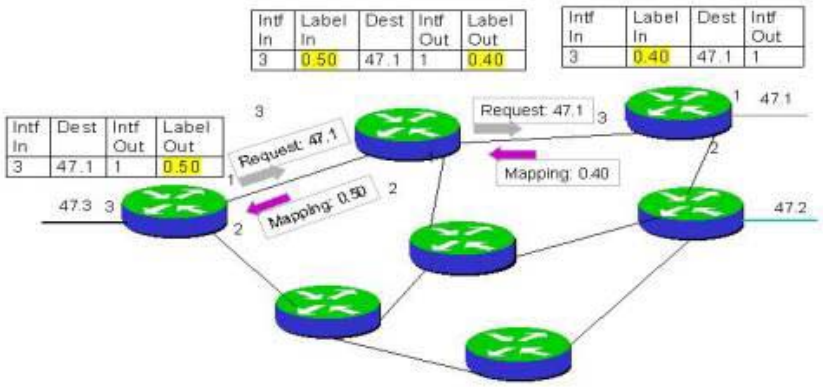


Fig. 4.6. Distribución de etiqueta en MPLS.

Fuente: Marshak, Marik. Multi Protocol Label Switching. 2000.

4.2 Protocolos de distribución de información de etiqueta

La arquitectura de MPLS define un protocolo de distribución de etiquetas como un grupo de procedimientos mediante los cuales un enrutador de etiqueta conmutada (LSR – *Label Switched Router*) informa a los demás del significado de las etiquetas usadas para enviar tráfico entre y a través de ellos.

Existe un número de diferentes protocolos de distribución estandarizados. Los protocolos existentes han sido extendidos de manera que la distribución de etiquetas pueda ser anexada a su estructura. Los nuevos protocolos han sido ideados con el propósito explícito de manejar distribución de etiquetas[37].

La etiqueta de información puede ser distribuida de dos maneras:

a.- "*Piggybacking*" en un protocolo de enrutamiento.

En MPLS la información del índice de etiqueta puede ser agregada a los protocolos convencionales de enrutamiento para distribución aunque solo los esquemas de control de entregas pueden soportar este método. El uso de "Piggybacking" en la operación normal de protocolos de enrutamiento asegura consistencia en la entrega de información y evita la necesidad de otro protocolo. Lamentablemente, no todas las subredes usan enrutamiento y no todos los protocolos permiten un manejo fácil de las etiquetas.

b.- Protocolo de distribución de etiquetas (LDP – *Label Distribution Protocol*).

Siguiendo el modelo TDP (TDP – *Tag Switching Protocol*) de Cisco, el grupo de trabajo para MPLS ha comenzado a trabajar en la definición de un nuevo protocolo específicamente para la distribución de información de índices de etiquetas denominado Protocolo de distribución de etiquetas. Éste puede ser usado para esquemas tanto de control de entregas como de datos

[37] Anderson, L.Doolan, P. LDP specification. RFC 3036. Enero 2001.

entregados. La desventaja de usar LDP [RFC 3036] es que agrega complejidad (aunque se requería de un nuevo protocolo) y su uso necesita ser coordinado con otros protocolos de enrutamiento.

4.3 Protocolo de Distribución de Etiquetas LDP

El protocolo de distribución de etiquetas, LDP, es un grupo de procedimientos y mensajes a través de los cuales los LSR establecen caminos de etiqueta conmutada (LSP – *Label Switched Paths*) a través de una red "mapeando" información de enrutamiento de la capa de red directamente sobre los caminos conmutados en la capa de enlace de datos.

LDP asocia una equivalencia de clase de envío (FEC) con cada LSP que crea. El FEC asociado a un LSP especifica cuales paquetes son "mapeados" a ese LSP. Los LSPs son creados a través de la red mientras cada LSR une las etiquetas de entrada para un FEC dado con la etiqueta de salida asignada al próximo salto por el FEC dado.

Las sesiones de LDP se establecen entre LDP del mismo nivel dentro de la red MPLS, aunque no necesariamente adyacente. Los mensajes intercambiados son los siguientes (ver Fig. 4.7):

- **Discovery messages**. Anuncian y mantienen la presencia de un LSR dentro de la red.
- **Mensajes de sesión** (Session messages). Son usados para establecer, mantiener y finalizar sesiones entre LDP que se encuentran al mismo nivel.
- **Mensajes de aviso** (Advertising messages). Usados para crear, cambiar y eliminar los mapeados de etiqueta realizados por los FEC.
- **Mensajes de notificación** (Notification messages). Proveen mensajes de información de alerta y de señales de error.

Los diferentes esquemas usados para intercambio de etiquetas se mencionan a continuación:

- LDP (Label distribution protocol). Convierte destinos unicast IP en etiquetas.
- RSVP (Resource Reservation Protocol), CR-LDP. Usados para ingeniería de tráfico y reserva de recursos.
- Protocolo independiente de multicast (PIM). Usado en mapeados de multicast.

BGP (Border gateway protocol). Usado para etiquetas externas (VPN).

4.4 Función de un LSR de frontera

Una de las responsabilidades de los LSR de frontera es clasificar el tráfico y colocar o remover etiquetas a los paquetes. Como ya se ha mencionado, las etiquetas pueden ser asignadas sobre la base de factores y no basándose en la dirección de destino. Los LSR de frontera determinan cual tráfico posee un flujo de larga duración, implanta políticas de gestión y control de acceso, y ejecuta la unificación de tráfico en flujos mayores cuando es posible. Estas son todas las funciones que deben ser ejecutadas en los límites entre los mundos de IP y MPLS. Por lo que, las capacidades de los LSR de frontera serán claves en el éxito de un ambiente de conmutación de etiquetas. También resultan ser un punto de control y gestión para el proveedor de servicio.

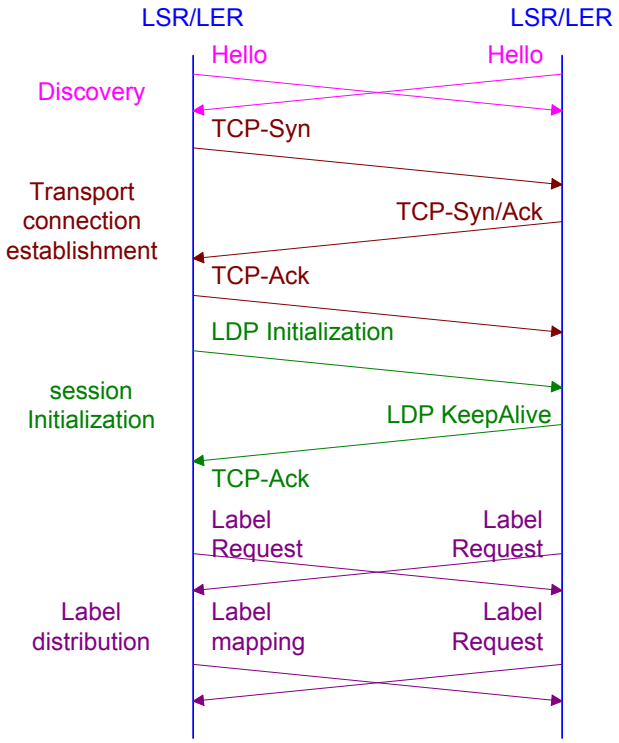


Fig. 4.7. Inicialización LDP.

Fuente: Marshak, Marik. Multi Protocol Label Switching. 2000.

CAPÍTULO 5

5 Utilización de LDP y Conmutación ATM VC en MPLS

5.1 Los conmutadores ATM como LSRs

Los procedimientos de envío usados para MPLS son similares a los usados por los conmutadores ATM. Los conmutadores ATM utilizan el puerto de entrada y el valor del VPI/VCI entrante como un "índice" dentro de la tabla de "cross-conexión", de la cual se obtiene un puerto de salida y un valor de VPI/VCI saliente. Por lo tanto, si una o más etiquetas pueden ser codificadas directamente dentro de los campos a los cuales acceden estos conmutadores, entonces estos conmutadores pueden ser usados como LSRs con solo hacerle una actualización de software. Por lo general, estos dispositivos se denominan ATM-LSRs.

Existen tres maneras de codificar las etiquetas dentro de una cabecera de celda ATM (asumiendo que se usa AAL5):

- Codificación SVC. Utiliza el campo VPI/VCI para codificar la etiqueta la cual se encuentra ubicada en la parte superior de la pila. Esta técnica puede ser usada en cualquier red. Con esta técnica de codificación, cada LSP se convierte en un SVC de ATM, y el LDP se convierte en el protocolo de "señalización" de ATM. Con esta técnica de codificación, los ATM-LSRs no pueden ejecutar operaciones de "PUSH" o "POP" en la pila de la etiqueta.
- Codificación SVP. Esta técnica utiliza el campo VPI para codificar la etiqueta la cual que se encuentra ubicada en la parte superior de la pila, y el campo VCI para codificar la segunda etiqueta de la pila, si una existe. Esta técnica presenta algunas ventajas sobre la anterior, en aquella se permite el uso de "Conmutación VP" de ATM. Esto es, los LSPs son usados como SVPs de ATM, con el LDP sirviendo como protocolo de señalización ATM.
- Sin embargo, esta técnica no puede ser usada siempre. Si la red incluye un camino virtual de ATM (ATM VP) a través de una red que no utiliza MPLS, entonces el campo VPI no está necesariamente disponible para el uso de MPLS. Cuando esta técnica de codificación es utilizada, el ATM-LSR a la salida del VP efectivamente realiza una operación "POP".
- Codificación Multipunto SVP. Esta técnica utiliza el campo VPI para codificar la etiqueta que se encuentra ubicada en la parte superior de la pila, utiliza también parte del campo VCI para codificar la segunda etiqueta, si ya una está presente, y utiliza el campo VCI para identificar el LSP de entrada.
- Si se usa esta técnica, la capacidad convencional de la conmutación ATM-VP puede ser usada para ofrecer VPs multipunto a punto. Las celdas de diferentes paquetes llevaron entonces diferentes valores de VCI. Esto nos permite realizar la entrega de la etiqueta (merging), sin necesidad de tener que desencadenar ningún problema de entrelazado de celdas. Esta técnica depende de la existencia de capacidad de asignarle valores de 16 bits a los VCI a cada conmutador ATM, de manera que ningún valor de VCI sea asignado a dos conmutadores diferentes.

5.2 Definiciones[38]

Una interfaz ATM controlada por conmutación de etiqueta (LC-ATM: Label Switching Control and Forwarding ATM) es una interfaz ATM controlada por el componente de control de la conmutación de etiquetas. Cuando un paquete que atraviesa tal interfaz es recibido, es tratado como un paquete etiquetado. La etiqueta superior del paquete se conoce bien de los contenidos del campo VCI o de la combinación de los contenidos de los campos VPI y VCI. Cualquier par de LDP que estén conectados a través de una interfaz LC-ATM podrá usar negociaciones LDP para determinar cual de estos casos mencionados se aplica a esa interfaz.

Un ATM-LSR es un LSR con un número de interfaces LC-ATM las cuales entregan celdas entre estas interfaces, usando etiquetas llevadas en el campo VCI o VPI/VCI, sin reensamblar las celdas en tramas antes de realizar el envío.

Un LSR basado en tramas es un LSR que envía tramas completas entre sus interfaces. Es importante mencionar que tal LSR puede tener cero, uno o más interfaces LC-ATM.

Algunas veces una caja se puede comportar como un ATM-LSR con respecto a ciertas interfaces, pero también pueden comportarse como LSR basados en tramas con respecto a otras interfaces. Por ejemplo, un conmutador ATM con una interfaz Ethernet puede funcionar como un ATM-LSR cuando entrega celdas entre sus interfaces LC-ATM, pero puede funcionar como LSR basado en tramas cuando entrega tramas desde su Ethernet a una de sus interfaces LC-ATM. En tales casos, se puede considerar que el equipo se comporta como “coresident”, dado que realiza las dos funciones: ATM-LSR y LSR basado en tramas.

Un dominio ATM-LSR consta de un grupo de LSR basados en tramas los cuales están conectados mediante interfaces LC-ATM.

El VC-merge es el proceso mediante el cual un conmutador recibe celdas de varias celdas VCI de entrada y las transmite en un solo VCI de salida sin ocasionar que las celdas de diferentes AAL5 PDUs se solapen.[39]

5.3 Características Especiales de los Conmutadores ATM

Mientras la arquitectura MPLS permite una flexibilidad considerable en la implantación de LSR, un ATM-LSR está limitado por las capacidades de hardware y las restricciones en materias tales como el formato de las celdas impuesto por ATM. Debido a estas restricciones, se deben realizar algunos procedimientos especiales para ATM-LSRs. Algunas de las ventajas claves de los conmutadores ATM que afectan su comportamiento como LSR son:

- La función de “swapping” de las etiquetas se ejecuta en los campos (VCI y/o VPI) dentro de las cabeceras de celda; esto indica el tamaño y ubicación de la(s) etiqueta(s) dentro de un paquete.
- Los VCs multipunto-punto y multipunto-multipunto no son soportados generalmente. Esto significa que la mayoría de los conmutadores no puede soportar el “VC merge”.
- Generalmente no existe la capacidad de ejecutar una función “decremento TTL” como se ejecuta en las cabeceras IP en los enrutadores.

[38] RFC 3035. MPLS using LDP and ATM VC Switching. January 2001.

[39] RFC 3035.

5.4 Componente de Control de conmutación de etiqueta para ATM

Para permitir la conmutación de etiquetas en un conmutador ATM se debe implantar el componente de control de conmutación de etiqueta. Esto consiste básicamente de la ubicación, distribución, y procedimientos de mantenimiento de la etiqueta. La búsqueda de información en la etiqueta se realiza básicamente por el LDP.

En la RFC 3035, sólo se ha considerado el caso en el cual el componente de control utiliza información que ha sustraído directamente de la red a través de los protocolos de enrutamiento, tales como: OSPF, IS-IS.

En algunos casos, los LSRs hacen uso de otros protocolos (por ejemplo, RSVP, PIM, BGP) para distribuir las etiquetas. En estos casos, un ATM-LSR necesitaría utilizar estos protocolos.

5.5 Conmutadores Híbridos

La existencia del componente de control para conmutación de etiqueta en un conmutador ATM no excluye la posibilidad de trabajar con el componente de control definido por la ITU y el Forum ATM en el mismo conmutador y las mismas interfaces. Los dos componentes de control, el de conmutación de etiqueta y el definido por el Forum ITU/ATM, operarían independientemente.

5.6 Uso de VPI/VCIs

La conmutación de etiqueta es llevada a cabo a través de la asociación de etiquetas con Clases de Equivalencia de Envíos (FEC), y utilizando el valor de la etiqueta para el envío de paquetes, incluso la determinación del valor de cualquier etiqueta de reemplazo. En un ATM-LSR, la etiqueta es llevada en el campo VPI/VCI, o, cuando dos ATM-LSRs se conectan a través de un "Camino Virtual" de ATM, dentro del campo de VCI.

Los paquetes etiquetados deben ser transmitidos usando la encapsulación "null".

Además, si dos LDP están conectados a través de una interfaz LC-ATM capaz de llevar paquetes IP no etiquetados, se hace obligatoria una conexión a red no MPLS. Esta conexión no MPLS es usada para llevar paquetes entre dos pares o enrutadores de la misma jerarquía, y puede también ser usada para paquetes no etiquetados (tales como paquetes OSPF, etc.). La encapsulación LLC/SNAP[40] debe ser usada en una conexión no MPLS.

Puede ser posible configurar una interfaz LC-ATM con VPI/VCIs adicionales que son usados para llevar información de control o paquetes no etiquetados. En ese caso, los valores VCI no deben estar en el rango de 0 a 32. Estos deben usar bien la encapsulación "null", como la definida en la sección 6.1 de la RFC 2684, o la encapsulación LLC/SNAP (definida en la sección 5.1 de la RFC 2684).

[40] Para mayor información ver la sección 6.1 de la RFC 2684.

5.7 Conexiones directas

Se dice que dos LSRs están ”directamente conectados” sobre una interfaz LC-ATM si todas las celdas transmitidas fuera de la interfaz por un LSR alcanzan el otro, y no existe conmutadores ATM entre los dos LSRs. Cuando dos LSRs están directamente conectados a través de una interfaz LC-ATM, ellos controlan conjuntamente la ubicación de los VPIs/VCIs sobre la interfaz que los conecta. Así que ellos pueden “acordar” usar el campo VPI/VCI para codificar una sola etiqueta.

El valor por defecto del VPI/VCI para una conexión no MPLS es VPI=0, VCI=32. Cualquier otro valor puede ser configurado siempre y cuando las partes estén al tanto de dicho valor.

En el caso de un valor VPI/VCI para el cual el VCI están en el rango de 0 a 32 inclusive éste no debe ser usado para la codificación de una etiqueta.

Con la excepción de aquellos valores que están reservados, los valores VPI/VCI usados en dos direcciones del enlace pueden ser creados como espacios independientes.

Los rangos de valores permitidos de VCIs son comunicados a través de LDP.

CAPÍTULO 6

6 *Aplicaciones de MPLS*

Las principales aplicaciones que hoy en día tiene MPLS son:

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

A continuación serán tratadas brevemente las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

6.1 Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. Esto es, equilibrar de forma óptima la utilización de esos recursos, evitando que un subconjunto (enlaces, equipos, etc.) de la red se sature mientras otro subconjunto de la misma se encuentra infrautilizado, evitando así posibles cuellos de botella y mejorando el rendimiento de la red global.

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 Fig. 6.1 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 redes, ya que:

- El administrador de red puede establecer rutas específicas por LSRs concretos, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso de cada LSP en detalle, es decir, cuánto tráfico se cursa y de qué tipo. Con esta información, se puede replanificar la red de forma que ofrezca un uso más eficiente de los recursos, lo que resulta bastante útil en planes de expansión futura.
- Permite hacer Encaminamiento Restringido (CBR - Constraint-Based Routing), de modo que se pueden seleccionar rutas específicas para transportar el tráfico de un tipo en concreto con unos requerimientos requerimientos específicos. Esta posibilidad está directamente ligada a los Acuerdos de Nivel de Servicio (*SLAs, Service Level Agreements*) que un proveedor

acuerde con el cliente, al que puede facturar así de un modo mucho más flexible y adaptable a sus necesidades.

La ventaja de la Ingeniería de Tráfico MPLS es que se puede aplicar directamente sobre una red IP, independientemente de la infraestructura que le de soporte, con un mayor nivel de detalle y de forma más sencilla y eficiente que como se venía haciendo hasta el momento.

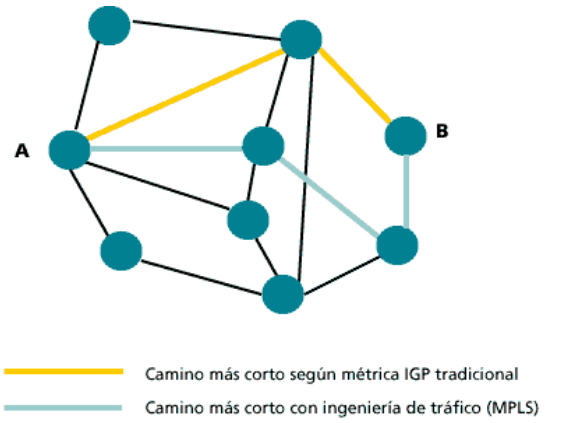


Fig. 6.1 – Ingeniería de tráfico MLS vs. IGP tradicional.

Fuente: MPLS: Una arquitectura de backbone del siglo XXI. Revista Red IRIS.

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.

En el ejemplo de tráfico de ingeniería de la figura 6.2 que se muestra a continuación, existen dos caminos desde el enrutador C al enrutador E. Si el enrutador selecciona uno de estos caminos como el camino más corto desde C hasta E, entonces llevará todo el tráfico que sea destinado a las redes que se encuentren disponibles a través del enrutador E. El volumen de tráfico resultante en ese camino puede causar congestión, mientras que otro puede estar sobrecargado. Para maximizar el desenvolvimiento a lo largo de toda la red, puede resultar conveniente desviar una fracción de tráfico desde un enlace a otro. Mientras en este ejemplo se pudiera establecer que el costo del camino CD-D-E es igual al costo del camino C-F-G-E, de manera tal que se logra un balance de cargas.

La solución al problema de ingeniería de tráfico recae en el hecho de que las etiquetas y caminos de etiqueta conmutada (Label-Switched Paths) pueden ser establecidos por una variedad de diferentes módulos de control. Por ejemplo, el módulo de control de tráfico de ingeniería puede establecer un camino de etiqueta conmutada A–C–D–E y otro B–C–F–G–E.

6.2 Clase de servicio (CoS)

La filosofía de una red orientada a ofrecer Calidad de Servicio en la agrupación de los distintos Tipos de Tráfico en un cierto número de Clases se Servicio, con diferentes prioridades. Los paquetes pertenecientes a una misma Clase de Servicio tienen en común los mismos

requerimientos de tratamiento en cuanto a ancho de banda necesario, retardo, variación de retardo, jitter, y pérdidas de paquetes, es decir, Calidad de Servicio (QoS).[41]

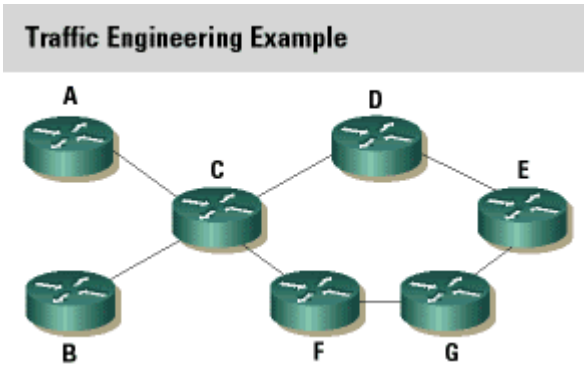


Fig.6.2. Ejemplo de Ingeniería de tráfico.

Fuente: Davie, Bruce. Multiprotocol Label Switching, Service Providers to Benefit from New Functionality. Cisco Systems, Inc. Packet™ Magazine Archives, Second Quarter 1999.

La capacidad de poder asegurar que un paquete en concreto recibirá, a lo largo de todo el dominio, el tratamiento requerido, se apoya en dos posibilidades 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, basa su funcionamiento en la clasificación del tráfico a la entrada de la red y en la asociación de prioridades a estos tipos de tráfico mediante el Campo de 8 bits DSCP(DiffServ Code Point), campo ToS (Type of Service)en Ipv4 y Clase de tráfico en Ipv6. En función de este campo, cada nodo intermedio tratará el paquete de la forma adecuada. MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- el tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP
- entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero

[41] González, Ana. MPLS: Convergencia entre el nivel de Transmisión y el nivel de enrutamiento. Antena de telecomunicación. Diciembre 2002.

para tráfico best-effort, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

6.3 Redes Privadas Virtuales (VPNs)

Una Red Privada Virtual (VPN - *Virtual Private Network*) está orientada a proporcionar conectividad a un cliente sobre una infraestructura compartida, con las funcionalidades de red y seguridad equivalentes a las de una red privada, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y el término privada indica que el usuario cree que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las principales características de una VPN son[42]:

- Escalabilidad: debe ser capaz de asumir cambios de conectividad y capacidad de forma muy ágil. MPLS ofrece conectividad «todos-con-todos», lo que la convierte en una red realmente flexible con unos requerimientos de configuración mínimos a la hora de añadir un nuevo extremo a la VPN, pues sólo hay que configurar el nuevo extremo, sin tener que tocar la configuración del resto de extremos. MPLS evita la complejidad de los túneles y PVCs.
- Seguridad: debe asegurar que el tráfico de cada cliente es confidencial; ningún usuario ajeno a la VPN debe ser capaz de acceder a la información que viaja por ésta. La seguridad de una VPN MLS es comparable a la de FR o ATM.
- QoS: debe asegurar la priorización del tráfico crítico o sensible al retardo sin despreciar tampoco el resto del tráfico gestionando el ancho de banda asignado a cada tipo de tráfico. MPLS soporta la diferenciación de tráfico de una forma estandarizada y permite garantizar SLAs para dichos tipos de tráfico, pudiéndose implementar herramientas, incluso vía web, que permitan a los usuarios controlar el funcionamiento de su red en todo momento.
- Gestión: una VPN con una gestión ágil y eficiente resulta imprescindible para poder cumplir con los objetivos anteriores y alcanzar unos SLAs competitivos. La posibilidad de aplicar técnicas de Ingeniería de Tráfico es la herramienta básica para la gestión en una red MPLS.
- Fiabilidad: es indispensable para poder prever y garantizar una gran disponibilidad del servicio. La red MPLS «sabe» de la existencia de una VPN, ya que se trata de un modelo acoplado y no superpuesto.

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

[42] González, Ana. MPLS: Convergencia entre el nivel de Transmisión y el nivel de enrutamiento. Antena de telecomunicación. Diciembre 2002.

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los ISPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costos de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. Los túneles IP en conexiones dedicadas (no se va a tratar aquí de las conexiones conmutadas de acceso) se pueden establecer de dos maneras:

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

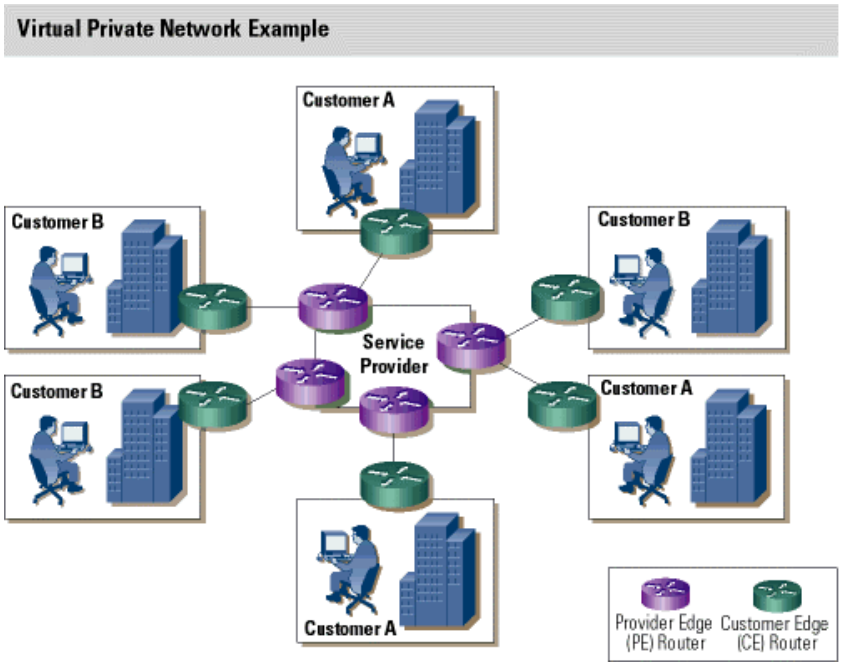


Fig. 6.3. Modelo de una Red Privada Virtual.

Fuente: Davie, Bruce. Multiprotocol Label Switching, Service Providers to Benefit from New Functionality. Cisco Systems, Inc. Packet™ Magazine Archives, Second Quarter 1999.

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios enrutadores de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos ISPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas,

ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

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

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

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

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, basándose en túneles extremos a extremo (o circuitos virtuales) entre cada par de enrutadores de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una Internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

En la figura 6.4 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, a partir de LSPs, y no de extremo a extremo a través de la red.

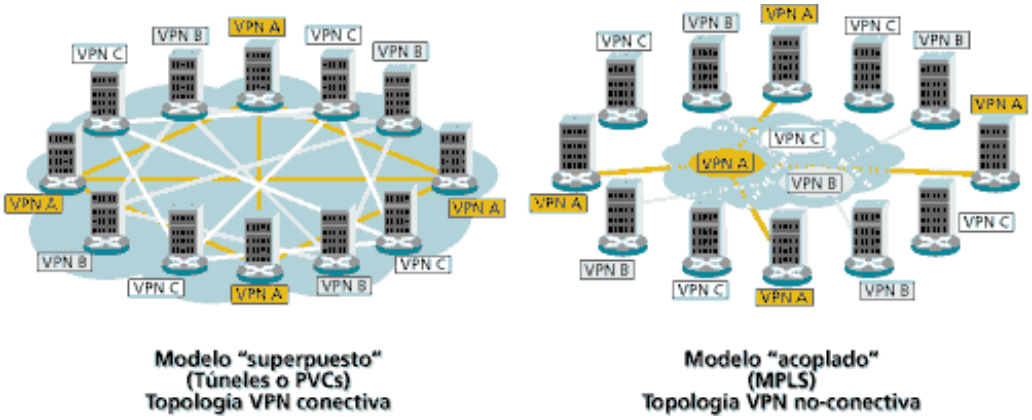


Fig. 6.4. Topología de VPN conectiva vs. Topología de VPN no-conectiva.

Fuente: MPLS: Una arquitectura de backbone del siglo XXI. Revista Red IRIS.

6.4 GMPLS

MPLS generalizado *(*GMPLS - *Generalized MultiProtocol Label Switching*), inicialmente denominado MPλS (MPLambdaS), extiende el concepto de MPLS de etiquetas con caminos conmutados (Label switched paths) y su capacidad de controlar TDM, Lambda y redes de fibras ópticas a través de la ingeniería de tráfico. Esto permite ofrecer una arquitectura de control sencilla y unificada para múltiples capas de conmutación, mediante la adaptación de la señalización existente de MPLS y los protocolos de enrutamiento de IP para las redes de transporte.

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*).

Para todos los tipos de etiquetas G-MPLS, 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.

Esto hace posible a los proveedores de servicio administrar un gran rango de elementos de red, desde paquetes conmutados hasta cross-conexiones digitales y ópticas, de manera uniforme. Además les permite aparentemente gestionar paquetes y circuitos.[43]

GMPLS automatiza buena parte de los procesos de planificación de circuitos y proceso de configuración, de esta manera reduce la complejidad operacional, el tiempo y los costos transformando todo el proceso de configuración en un proceso de tiempo real.

[43] MPLS Forum. Test&Plan Results. NGN 2002. Octubre 2002.

Para entender mejor el interés en GMPLS, es útil revisar algunos de los servicios de entrega que los proveedores de servicios afrontan. Hoy en día, para permitir servicios de voz y nuevos servicios de datos, los proveedores de servicio mantienen redes compuestas de una diversidad de equipos de redes de transporte, que incluye equipos ópticos y de cross-conexión óptica, multiplexores add/drop, elementos ópticos de transporte, además de elementos de datos tales como enrutadores IP y conmutadores ATM.

Desafortunadamente, los elementos tienen limitaciones, solo basta mirar los recursos de la red y su topología. Por otro lado, no existen estándares para que los elementos de datos automáticamente pidan los servicios de la red de transporte, ya que no existe un plano unificado entre estos elementos. En cambio, los proveedores de servicio cuentan con un grupo de procedimientos operacionales que resultan complejos y costosos Sistemas de Soporte de Operaciones (OSS - Operations Support Systems). Estas limitaciones hacen que el servicio de entrega se convierta en un proceso costoso, que consume mucho tiempo y que requiere de una considerable cantidad de interacción humana.

A continuación se resumen los diferentes beneficios que se presentan al extender las funciones de MPLS a redes ópticas:

- Se pueden potenciar las técnicas desarrolladas para MPLS y ofrecer una metodología para proveer canales ópticos en tiempo real. Esto promueve el rápido desarrollo de estas tecnologías.
- Proveer un manejo uniforme de la gestión de la red en entornos de datos como ópticos. Esto simplifica todos los esfuerzos de gestión.
- Se puede lograr una arquitectura sencilla permitiendo a un LSP atravesar un enrutador mixto y dispositivos OXC. Esto permite que la red ofrezca ancho de banda real.

La extensión de las funciones MPLS a redes ópticas se basa en un número de similitudes entre los dos tipos de redes:

- En MPLS, un LSP describe el camino punto a punto a seguir por un grupo de paquetes etiquetados. En MPλS, un canal óptico se usa para describir la conexión óptica punto a punto entre dos puntos de acceso.
- En una red MPLS, un LSR establece una relación entre una dupla [puerto de entrada, etiqueta de entrada] y una dupla [puerto de salida, etiqueta de salida]. De manera similar, en una red óptica de transporte, un OXC establece una relación entre una dupla [puerto de entrada, canal de entrada óptico] y una dupla [puerto de salida, canal óptico de salida]. Una vez establecidas, estas relaciones no pueden ser alteradas por el contenido de ningún paquete de datos.
- En una red MPLS, un LSR descubre, distribuye y mantiene el estado de la información asociado con la red. En un OXC, el OTN es responsable por estas mismas funciones.
- En una red MPLS, un LSR es responsable por la creación y el mantenimiento de los LSPs asociados con las pólizas de ingeniería de tráfico existentes. En un OXC, el OTN es responsable por estas mismas funciones.
- En una red MPLS, un LSP es unidireccional. En un OTN, un canal óptico es también unidireccional.

En un entorno MPλS, será posible representar la fibra dentro del OTN como un grupo de enlaces, donde cada enlace representaría un grupo de canales.

Un enrutamiento IP (con extensiones) distribuirá la información acerca de la topología de la red óptica: ancho de banda disponible, y otras informaciones pertinentes. Esta información será utilizada para calcular las rutas explícitas para los canales ópticos. Los protocolos de distribución de MPLS crearan estos caminos.[44]

Por lo antes mencionado, G-MPLS se perfila como una parte integral muy importante dentro de la próxima generación de redes, dado que G-MPLS provee los enlaces necesarios entre la capa IP y la fotónica, permitiendo así la evolución efectiva y de mutua colaboración entre estas dos tecnologías. Hoy en día las redes de información tienen típicamente 4 capas: IP para soportar servicios y aplicaciones, ATM para ingeniería de tráfico, SONET/SDH para transporte, y DWDM para capacidad física.

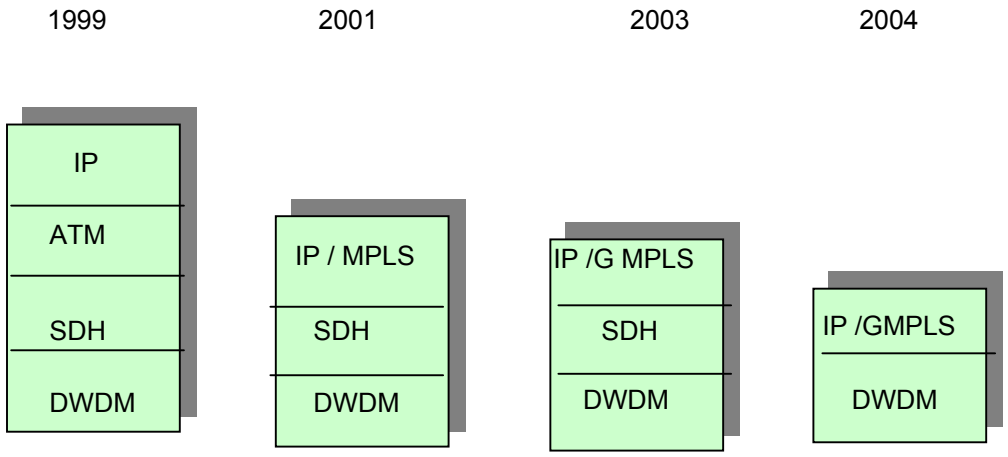


Fig. 6.5. Posible evolución de las redes.

[44] González, Ana. MPLS: Convergencia entre el nivel de Transmisión y el nivel de enrutamiento. Antena de telecomunicación. Diciembre 2002.

ESCENARIOS

FUTURO IP

El protocolo IP presenta tres problemas que son resultado de un crecimiento tremendo de la Internet en los últimos años y que se mencionan a continuación[45]:

- Más de la mitad de las direcciones clase B han sido asignadas.
- Las direcciones IP de 32 bits en general no resultan adecuadas para el crecimiento a largo plazo de la Internet.
- La estructura actual de enrutamiento no es jerárquica sino plano, y requiere una tabla de enrutamiento por red. Al aumentar el número de redes, utilizando múltiples direcciones clase C por sitio con múltiples redes, en vez de una sola dirección clase B, el tamaño de la tabla de enrutamiento aumenta.

La solución al tercer problema lo representa el CIDR[46] que extiende de manera bastante útil la actual versión de IP (IP versión 4).

Se han presentado cuatro propuestas para una la nueva versión de IP, algunas veces llamada IPng (IPng – *IP next generation*)[47]. Y son las siguientes:

1. Protocolo de Internet Simple (SIP - *Simple Internet Protocol*). Propone una cantidad mínima de cambios en el protocolo IP que utiliza direcciones de 64 bits y un formato de cabecera diferente. (Los primeros cuatro bits de la cabecera seguirán representando la versión del protocolo).

2. El protocolo "P" de Internet (PIP- *The "P" Internet Protocol*). Esta propuesta usa direcciones jerárquicas más grandes y con longitud variable con un formato diferente de cabecera.

3. TCP y UDP con direcciones más grandes (TUBA – "*TCP and UDP with Bigger Addresses*"). Esta propuesta está basada en el modelo CLNP de OSI (CLNP - *Connectionless Network Protocol*), un protocolo OSI similar a IP. Permite direcciones más grandes con longitud variable de hasta 20 bytes. CLNP es un protocolo existente mientras que SIP y PIP son

[45] Stevens, Richard. TCP/IP Illustrated. Volume 1.The Protocolos.

[46] CIDR - *Classless Interdomain Routing.*

[47] Más información en el *IEEE Network* (Vol. 7, no. 3). Contiene resumen de las tres primeras propuestas, junto con un artículo de CIDR. También la RFC 1454 [Dixon 1993].

propuestas, por lo que ya existe documentación acerca del mismo[48]. También se conoce como IPv9 y representa una alternativa de direcciones variables frente a SIPP.

4. TP/IX[49]. Tal como en SIP, utiliza direcciones de IP de 64 bits, pero cambia las cabeceras de TCP y UDP, de la siguiente manera: número de puerto de 32 bits para cada protocolo, junto con una secuencia de números de 64 bits, y ventanas para TCP de 32 bits. Tal como con SIP, utiliza 64 bits para las direcciones IP, pero también cambia las cabeceras de TCP y UDP: Puerto número 32 para ambos protocolos, junto con una secuencia de números de 64 bits, 64 bits de números de reconocimientos y 32 bits de ventana para TCP.

Las primeras tres propuestas usan básicamente las mismas versiones de TCP y UDP para la capa de transporte.

Sin embargo, la aparición de redes IPv6 depende de las novedades que ésta versión ofrezca o de la disminución de direcciones IPv4. Y de la disposición de las organizaciones por adoptar nuevos esquemas. Por ejemplo, las organizaciones comerciales con grandes redes internas basadas en IPv4 no estarán deseosas de actualizar miles de enrutadores y hosts que trabajan con IPv4, aunque tengan problemas con limitaciones de direcciones dentro de sus propias redes. Sin embargo, sí se sentirán animados en invertir en nuevos equipos IPv6 si las nuevas aplicaciones críticas de negocios necesitan de las facilidades que sólo están disponibles en IPv6 o si ellos requieren conectarse con otra organización que está usando direcciones IPv6 solamente.

Algunas empresas que están implementando redes IP por primera vez, podrían estar interesadas en algunas ventajas del IPv6, como la autoconfiguración de direcciones. Sin embargo, cualquiera que piense invertir en IPv6 necesita estar seguro de que el protocolo está en una fase más avanzada. Vale decir, en este punto que IPv4 también está en desarrollo, dado que se están produciendo constantemente nuevas RFCs y borradores.

Por lo expuesto anteriormente acerca de los avances realizados en torno a IPv6, no todo el mundo está a favor de IPv6. Aquellos que están en contra, argumentan que los problemas de asignación de direcciones y problemas de enrutamiento pueden ser controlados con otros mecanismos. Uno de estos mecanismos que ha demostrado ser especialmente polémico es el Traductor de Direcciones de Red (NAT – *Network Address Translation*). Los que apoyan a NAT afirman que es la solución completa a los problemas de dirección de UPv4.

Algunos sostienen que NAT será la solución a los problemas de direcciones de IPv4. Otros, por su parte, sostienen que NAT puede ser peligroso, ya que inhabilita los criterios de seguridad en la red. Esto sucede debido a que cada datagrama que pasa a través de un red NAT debe ser convertida, lo cual hace imposible el uso de los protocolos de seguridad en IP (IPsec – IP Security). Aunque, NAT hace posible esconder totalmente las redes detrás de una sencilla dirección IP, lo que resulta una forma de seguridad en sí misma.[50]

[48] RFC 1347 [Gallon 1992] posee detalles acerca de TUBA.

[49] Descrito en la RFC 1475 [Ullmann 1993].

[50] Ladid, Latif. IPv6-The new-generation Internet. Ericsson Review Nº 1. 2000. Pág. 8.

ATM

La idea de que ATM algún día se convertirá en la base de transporte para Internet resulta muy atractiva, pero las razones desde el punto de vista de los negocios parecen indicar que esto no va a pasar muy pronto. La gente se está dando cuenta que Internet puede jamás llegar a ser completamente ATM, y por lo tanto muchas funciones que estarían disponibles con ATM (por ejemplo, multicasting o transmisión de datos en tiempo real) deben ser prestadas por la misma Internet. La RFC 1633 describe las razones por las que la arquitectura de Internet debe permitir tráfico IP en tiempo real. Los autores de dicha RFC escriben[51]:

En las reuniones de la IETF sobre multicast en la Internet se han realizado experimentos a gran escala para enviar voz y video digitalizado a través de una infraestructura de conmutación de paquetes. Estos experimentos dependen de las siguientes tres tecnologías:

- Muchas estaciones de trabajo modernas vienen equipadas con circuitos que facilitan la comunicación multimedia, incluyendo codecs de audio y codificadfores de campos de video, por lo que el equipamiento con video resulta económico.
- El multicastinp IP, el cual no está aún disponible de manera general en enrutadores comerciales, está siendo provisto por el MBONE, un backbone de multicast temporal.
- Han sido desarrolladas aplicaciones de audio y video altamente sofisticadas.

Entonces por qué MPLS?

Al aparecer una nueva tecnología nos surgen las siguientes preguntas:

- ¿Qué beneficios aporta?
- ¿Será rentable la inversión?
- ¿Me causa algún perjuicio el no implantarlo en mi red?

Unas respuestas rápidas a estas preguntas podrían ser las siguientes:

- ¿Qué beneficios aporta?

La tecnología MPLS es capaz de integrar muchos servicios y funcionalidades sobre una única plataforma, permitiendo un uso óptimo de los recursos, una provisión de servicios más rápida y un mantenimiento más simple. Sus principales funcionalidades son la ingeniería de tráfico, la calidad de servicio y las redes privadas virtuales (VPN).

- ¿ Será rentable la inversión?

Esta pregunta no tiene una respuesta única, ya que cada empresa tendrá su necesidades y limitaciones particulares. Por lo que en cada caso conviene analizarlo de forma singular y en base a algunas variables económicas importantes, y evaluando los escenarios posibles para poder conocer la rentabilidad del proyecto.

- ¿Me causa algún perjuicio no implantarlo en mi red?

[51] IBM corporation. Internetworking over ATM. An Introduction. Septiembre, 1996. Pág. 183.

No causa ningún perjuicios, pero con esta tecnología la escalabilidad de las redes es más simple y barato y, lo que resulta aún más importante, se podrán suministrar mejores calidades de servicio. Sin estas ventajas se será menos competitivo y el rendimiento de los recursos será inferior. Y Como complemento, se podría plantear la obsolescencia de nuestra propia red en la natural evolución de las mismas.

Conceptos erróneos sobre MPLS

Es importante tocar este punto de manera que permita aclarar varias ideas erróneas acerca de la tecnología MPLS, y así entender mejor su utilidad y área de aplicación.

Se ha extendido la idea de que MPLS es un estándar que permite a los fabricantes transformar los conmutadores ATM en enrutadores backbone de altas prestaciones. Sin embargo actualmente, los avances en la tecnología están consiguiendo que motores de búsqueda de rutas IP basados en ASIC[52] sean tan rápidos como MPLS o motores de búsqueda ATM. De modo que la ventaja que MPLS aporta al rendimiento del envío de paquetes no es la primera ventaja.

También se piensa que MPLS fue diseñado para eliminar por completo el enrutamiento IP. Esto no ha sido nunca un objetivo del Grupo de Trabajo de MPLS, porque sus miembros entienden que el enrutamiento tradicional en la capa 3 siempre será necesario en Internet, ya que:

- El filtrado de paquetes es un componente fundamental para la seguridad y administración en la red, y requiere un examen detallado de las cabeceras de los paquetes; el enrutamiento de la capa 3 sigue siendo necesario.
- Es imposible que un gran número de hosts implementen MPLS, por tanto, cada paquete transmitido necesita ser enviado por un dispositivo en la capa 3, donde la cabecera pueda ser examinada antes de enviarse el paquete empleando el enrutamiento convencional, como asignarle una etiqueta y enviar el paquete por un camino etiquetado conmutado (LSP)
- En el último salto anterior al host de destino, el paquete debe ser enviado empleando enrutamiento tradicional porque no resulta práctico asignar una etiqueta por separado para cada host en la subred de destino.

[52] Circuito integrado de aplicación específica (ASIC - *Application Specific Integrated Circuit*)

CONCLUSIONES

Algunas tecnologías nacen, pero tardan años en encontrarse aplicaciones prácticas para ellas; otras, ni siquiera llegan a hacerse un hueco en el mercado, pero algunas pocas consiguen un éxito sin precedentes. Como ejemplo de lo antes mencionado tenemos la tecnología IP, ATM y MPLS, de las cuales se trató en este trabajo.

Actualmente, IP es la solución que destaca a la hora de proporcionar servicios a través de Internet. Lo que supone que con unos cambios tecnológicos adecuados podrá fortalecerse hasta convertirse en los cimientos que asientan la transferencia de datos a través de Internet, permitiendo la difusión de servicios avanzados en tiempo real y de respuesta prioritaria. Entre los cuales podemos citar: Proyectos de tele información, servicios avanzados de atención médica y hospitalaria, servicios multimedia, transmisión de voz sobre Internet, entre otros.

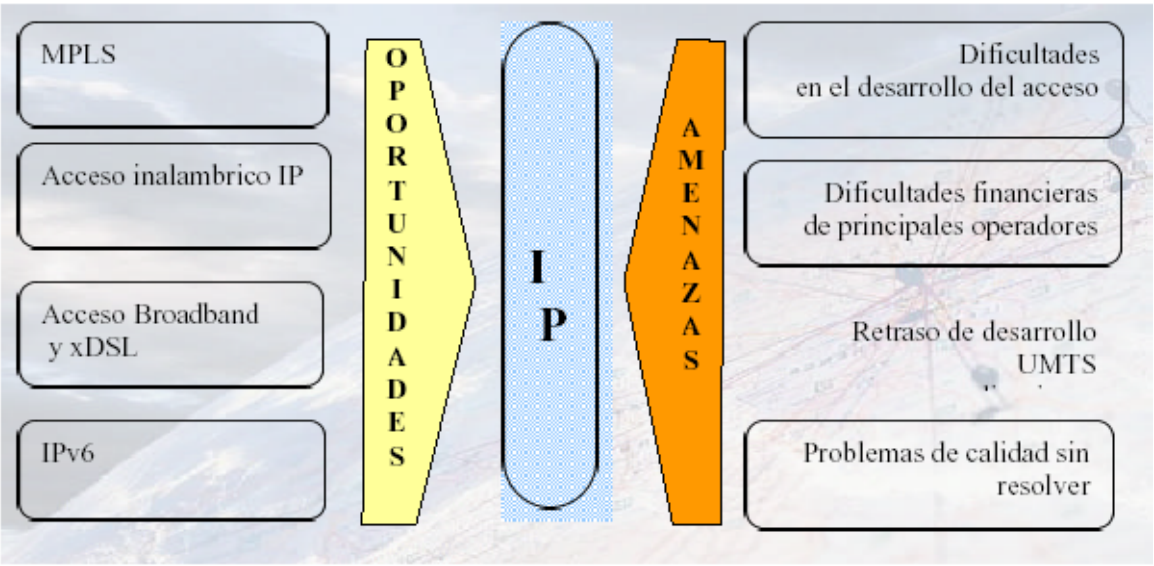
Estos servicios exigirán una serie de necesidades crecientes para los ISPs y carriers que deberán incorporar a sus redes troncales mecanismos para mantener un control sobre el tráfico, una gestión de recursos, un ancho de banda disponible, así como una adecuada calidad de servicio.

Es de suponer que la propia estructura técnica de Ipv4 pueda llegar a suponer un elemento limitador para el desarrollo de los nuevos servicios por Internet, sin embargo aún queda por descubrir cual va a ser el papel de nuevos desarrollos como MPLS y IPSec como elementos que sirvan para explotar al máximo de sus posibilidades.

El tráfico IP está aumentando a una tasa que supera el 100 % anual, y está creciendo con menor centralización en Estados Unidos. Esta tendencia significa que la naturaleza del tráfico está siendo más regional y más internacional. Donde cada vez mas los factores de contenidos están teniendo un papel predominante. Así la lengua de los contenidos es un factor que ya está afectando al desarrollo global de Internet y donde el papel que vaya de desarrollar el castellano está aún por determinar. Influirá sin duda las perspectiva de desarrollo económico en Latinoamérica y la expansión del castellano en pases como Brasil y EEUU, donde ya hay más hispanohablantes que en España.

El mercado IP no es un mercado maduro sino uno de alto crecimiento donde las posibilidades de desarrollo van a venir empujadas por las necesidades cada vez más complejas de los clientes.

Por otro lado, los avances en las tecnologías de transporte basadas en conmutación, encabezadas por la tecnología ATM, proporcionan alta velocidad, calidad de servicio y facilitan la gestión de los recursos en la red, que hemos comentado anteriormente.



Dentro de las soluciones de IP sobre ATM, destaca MPLS como una solución que está destinada a constituir una nueva base para la próxima generación de multiusuario y redes de multiservicio. La promesa es una mejor ejecución, incremento en la escalabilidad, funcionalidades mejoradas y expandidas, y la flexibilidad de igualar los requerimientos de calidad de servicio de los usuarios. Este protocolo permite una mejor integración de IP y ATM, y ofrece nuevas oportunidades para ingeniería de tráfico y VPN.

MPLS combina el uso de intercambio de etiquetas en el componente de envío con enrutamiento IP y protocolos de distribución estándares (basados en señalización IP y etiquetas) en el componente de control. En otras palabras, permite superar ciertas deficiencias de los niveles superiores, como por ejemplo TCP/IP, y a la vez mejora el factor transmisión debido a que en vez de realizar el envío de paquetes a través de enrutamientos basados en direcciones IP este se realiza mediante conmutación a través de etiquetas.

Al agregar etiquetas de tamaño variable a los paquetes, el procesamiento de los paquetes puede ser mejorado, el control de la QoS puede ser aplicada fácilmente, facilitando esto la construcción de grandes redes públicas. Y a un menor costo.

MPLS es una nueva tecnología que está empezando a ser beneficiosa. Se espera que esta tecnología sea usada tanto en redes públicas como en redes privadas.

BIBLIOGRAFÍA

Anderson, L.Doolan, P. LDP specification. RFC 3036. Enero 2001.

Callon, R. Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (RFC 1195). 1990.

Canalis, María Sol. MPLS "Multiprotocol Label Switching". Universidad Nacional del Nordeste. Argentina. 2002.

Comer, Douglas. Internetworking with TCP/IP. Volume I. Principles, protocols, and architecture. Tercera Edición. Prentice-Hall, Inc. 1995.

Cisco Systems. MPLS and IP Quality of Service in Service Provider ATM Networks. 2000.

Davie, Bruce. Multiprotocol Label Switching, Service Providers to Benefit from New Functionality. Cisco Systems, Inc. Packet™ Magazine Archives, Second Quarter 1999.

Feit, Sidnei. TCP/IP Arquitectura, protocolos e implantación con Ipv6 y seguridad de IP. 1997. Pág. 190.

González, Ana. MPLS: Convergencia entre el nivel de Transmisión y el nivel de enrutamiento. Antena de telecomunicación. Diciembre 2002.

Halabi, Bassam. Internet Routing Architectures. 1997. Pág. 96.

IBM Corporation. Internetworking over ATM: An Introduction. Sep, 1996. Pág. 183.

Marshak , Marik . Multiprotocol label switching. 2000.

MPLS Forum. MPLS: Ready for Revenue. 2002.

MPLS: Ready for Revenue. MPLS Forum, 2002.

Murhammer, Martin W. TCPIP Tutorial and Technical Overview. IBM

Ryan, Jerry. Multiprotocol Label Switching (MPLS). 1998. Página 13.

Sirgo, J.A. El protocolo TCP/IP. Universidad de Oviedo. Pág. 11.

Salazar de Angulo, Maritza. Dimensionamiento de una red pública ATM. 2000. Pág. 29.

Stewart III, John W. BGP4. Inter-Domain Routing in the Internet. 1999. Pág. 18.

Rodríguez, Adolfo. TCP/IP tutorial and technical Overview. IBM. 2001.

Ryan, Jerry. Multiprotocol Label Switching (MPLS). 1998. Pág. 13.

Understanding Telecommunications. Vol. 1.Ericsson telecom AB, 1998.

LECTURAS RECOMENDADAS

A continuación se listan algunas RFC que pueden resultar de interés.

ATM:
RFC 1483 Multiprotocol Encapsulation over AAL 5
RFC 1633 Integrated Services in the Internet Architecture: An Overview
RFC 1932 IP over ATM: A Framework Document

BGP:
RFC 1771 A border Gateway Protocol 4 (BGP–4)
RFC 1773 Experience with the BGP-4 Protocol
RFC 1772 Application of the Border Gateway Protocol in the Internet

EGP:
RFC 904 Exterior Gateway Protocol Formal Specification

IP:
RFC 1753 The recommendation for the IP next generation protocol
RFC 1883 Internet Protocol, Version 6
RFC 2373 – IP Version 6 Addressing Architecture
RFC 2893– Transition Mechanisms for IPv6 Hosts and Routers

MPLS:
RFC 3031 Multiprotocol Label Switching Architecture
RFC 3036 LDP Specification

OSPF:
RFC 1583 OSPF Version 2
RFC 1793 Extending OSPF to Support Demand Circuits
RFC 1586 Guidelines for Running OSPF Over Frame Relay Networks
RFC 1584 Multicast Extensions to OSPF
RFC 1403 BGP OSPF Interaction
RFC 2328 OSPF Version 2
RFC 1245 OSPF Protocol Analysis
RFC 1246 Experience with the OSPF Protocol
RFC 1850 OSPF Version 2: Management Information Base

RIP:
RFC 1058 Routing Information Protocol
RFC 1009 - Requirements for Internet Gateways
RFC 1388,1389 - *RIP Version 2*
RFC 1723 RIP Version 2 Carrying Additional Information
RFC 1582 Extensions to RIP to Support Demand Circuits
RFC 1721 RIP Version 2 Protocol Analysis
RFC 1722 RIP Version 2 Protocol Applicability Statement
RFC 1724 RIP Version 2 MIB Extension

REFERENCIAS

Para mayor información acerca de la tecnología MPLS, se sugieren los siguientes sitios web:

Grupo de trabajo de MPLS, http://www.ietf.org/html.charters/mpls-charters.html
MPLS Resource Center, http://www.mplsrc.com
Las RFCs de MPLS en http://www.eitf.org/ids.by.wg/mpls.html
Cisco, http://www.cisco.com/warp/public/ 784/packet/apr99/6.html
Cisco, http://www.cisco.com/warp/public/732/Tech/rtrp_pc.htm
Cisco, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs004.htm
Micom Communications Corp, http://www.micom.com/product/vip.html
V/IP Netxchange Communications Ltd., http://www.ntxc.com
Internet Xchange, http://webopedia.internet.com/TERM/I/IP.html
Data Connection Portable MPLS Products, http://www.datcon.co.uk/mpls/MPLSidx.htm.
UUNET - MPLS Conference, http://info.uu.net/ads/techconf/.
MPLS-DESC, http://www.renater.fr/jmu/QTP/mpls-desc.html.
NetPlane Control Plane Software for Next Generation Networks, http://www.netplane.com/main.html.
CANet MPLS Project Page, http://ardnoc41.canet2.net/mpls/.
MPOA, MPLS, and IP Switching References, http://www.cis.ohio-state.edu/~jain/refs/ipsw_ref.htm#csr.

ACRÓNIMOS

ACRÓNIMO	INGLÉS	CASTELLANO
AAL	ATM Adaptation Layer	Capa de adaptación de ATM
ACK	An Acknowledgment	Una confirmación
ANSI	American National Standards Institute	Instituto americano de normalización
AS	Autonomous System	Sistema autónomo
ATM	Asynchronous Transfer Mode	Modo de Transferencia Asíncrono
Backbone	Conexión de alta velocidad dentro de una red que interconecta los principales sitios de la Internet.	
BGP	Border Gateway Protocol	Protocolo de Pasarela de Frontera
CIDR	Classless Interdomain Routing	Enrutado sin clase entre dominios Internet
CLNP	Connectionless Network protocol	Protocolo de red no orientado a conexión
CoS	Class of Service	Clase de Servicio
DLCI	Data Link Connection Identifier	Identificador de conexión del enlace de datos
EGP	Exterior Gateway Protocol	Protocolo de Pasarela Exterior
FEC	Forwarding Equivalence Class	Clase de Equivalencia de Envío
HTML	Hypertext Markup Language	Lenguaje de marcas hipertextuales
IETF	Internet Engineering Task Force	Grupo de trabajo de Internet
IGP	Interior Gateway Protocol	Protocolo de Pasarela Interior
ILM	Incoming Label Map	
IP	Internet Protocol	Protocolo de Internet
IPng	IP next generation	IP de próxima generación
IPv4	Internet Protocol version 4	Protocolo de Internet versión 4
IPv6	Internet Protocol version 6	Protocolo de Internet versión 6
IS-IS	Intermediate System to Intermediate System	Sistemas Intermedios
ISP	Internet Service Provider	Proveedor de servicios de Internet
LDP	Label Distribution Protocol	Protocolo de distribución de etiquetas
L2	Layer 2	Capa 2 o capa de enlace de datos
L3	Layer 3	Capa 3 o capa de red
LSP	Label Switched Path	Camino de etiqueta conmutada
LSR	Label Switching Router	Enrutador de conmutación de etiqueta
MPLS	MultiProtocol Label Switching	Multiprotocolo de conmutación de etiqueta
NHLFE	Next Hop Label Forwarding Entry	
OSI	Open Systems Interconnected	Interconexión de sistemas abiertos
OSPF	Open Shortest Path First	Primero el Camino Abierto más corto
PIP	The “P” Internet Protocol	Protocolo “P” de Internet
PVC	Permanent Virtual Circuit	Circuito virtual permanente
QoS	Quality of Service	Calidad de servicio
RFC	Request for Comments	Petición de comentarios
RIP	Routing Information Protocol	Protocolo de Información de Enrutamiento
SVC	Switched Virtual Circuit	Circuito virtual conmutado

ACRÓNIMO	INGLÉS	CASTELLANO
SVP	Switched Virtual Path Switch	Camino virtual conmutado Conmutador
TCP	Transmission Control Protocol	Protocolo de Control de Transmisión
TCP/IP	Transmission Control Protocol/ Internet Protocol	Protocolo de Control de Transmisión/ Protocolo de Internet
TDM	Time Division Multiplexing	Multiplexaje por Divisón de Tiempo
TTL	Time-To-Live	Tiempo de vida
UDP	User Datagram Protocol	Protocolo de Datagramas de Usuario
VC	Virtual Circuit	Circuito virtual
VCI	Virtual Circuit Identifier	Identificador de canal virtual
VP	Virtual Path	Trayecto (camino) virtual
VPN	Virtual Private Network	Red virtual privada
VPI	Virtual Path Identifier	Identificador de camino virtual

ÍNDICE DE FIGURAS y TABLAS