Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED *IP/ATM* A *MPLS*

Carlos Augusto de León González
Asesorado por el Ing. Enrique Edmundo Ruiz Carballo

Guatemala, abril de 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED *IP/ATM* A *MPLS*

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

CARLOS AUGUSTO DE LEÓN GONZÁLEZ
ASESORADO POR EL INGENIERO ENRIQUE EDMUNDO RUIZ CARBALLO

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO ELECTRÓNICO

GUATEMALA, ABRIL DE 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADORA	Inga. Ingrid Salomé Rodríguez García de Loukota
EXAMINADOR	Ing. Gustavo Adolfo Villena Vásquez
EXAMINADOR	Ing. Fernando Waldemar de León Contreras
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED *IP/ATM* A *MPLS,*

tema que me fuera asignado por la Dirección de la Escuela de Mecánica Eléctrica, el 2 de marzo de 2006.

Carlos Augusto de León González

Guatemala, 6 de noviembre del 2,006

Señor Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Señor Coordinador

Por medio de la presente, me permito informarle que he revisado completamente el trabajo de graduación titulado: "ANALISIS DE LA FACTIBILIDAD TECNICA Y ECONOMICA PARA LA MIGRACION DE UNA RED IP/ATM A MPLS", desarrollado por el señor Carlos Augusto de León González, dicho trabajo cumple con los objetivos propuestos en el anteproyecto de tesis

Por lo tanto, el autor de este trabajo y yo, como su asesor, nos hacemos responsables por el contenido y conclusiones de la misma.

Atentamente,

Ing. Enrique Edmundo Ruiz Carballo
Asesor Nombrado
Colegiado 2225

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 17 de noviembre 2006.

Señor Director
Ing. Mario Renato Escobedo Martínez
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: **ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED IP/ATM A MPLS.** desarrollado por el estudiante; Carlos Augusto de León González, por considerar que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador Area de Electrónica

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA

JCSP/sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

El Director de la Escuela de Ingenierìa Mecànica Elèctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Area, al trabajo de Graduación del estudiante; Carlos Augusto de Leòn Gonzàlez titulado: **ANÀLISIS DE LA FACTIBILIDAD TÈCNICA Y ECONÒMICA PARA LA MIGRACIÒN DE UNA RED IP/ATM A MPLS,** procede a la autorización del mismo.

Ing. Mario Renato Escobedo Martínez
DIRECTOR

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA
MECANICA ELECTRICA
DE GUATEMALA

GUATEMALA, 20 DE NOVIEMBRE 2,006.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG. 113.2007

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED IP/*ATM* A *MPLS***, presentado por el estudiante universitario **Carlos Augusto de León González,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

Guatemala, abril de 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

/gdech

AGRADECIMIENTOS A

DIOS	La Fuerza Vital que ha estado conmigo en todos momentos, y me guió por el camino del entendimiento para encontrar el conocimiento y la felicidad.
MIS PADRES	Carlos Augusto de León Juárez y Dolia Rossana de de León, quienes me apoyaron y dieron el aliento necesario para lograr mis objetivos.
MIS HERMANOS	Verónica, Juan José y Pablo Jesús, por su apoyo y comprensión.
MIS TÍOS	Manuel de León y Lourdes Cruz de de León, por su paciencia y apoyo en todos estos años.
MI NOVIA	Por su apoyo, cariño, amor y comprensión que me brindo durante estos años.
FAMILIARES	Que me brindaron consejos y me apoyaron.
COMPAÑEROS Y AMIGOS	Con quienes el camino de la universidad resultó ser una experiencia agradable y única.
FACULTAD DE INGENIERÍA	Por haberme brindado la oportunidad de estudiar una carrera universitaria.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE ABREVIATURAS

ATM (Asynchronous transfer mode) Red de modo de transferencia asíncrono.

ATM – LSR (ATM Label Switch router) Conmutador ATM modificado para actuar como router conmutador de Etiquetas.

BGP (Border Gateway Protocol) Protocolo de acceso de borde o frontera

CPE (Customer Premises Equipment) Equipo de acceso del cliente

FEC (Forwarding Equivalent Class) Clase de envío equivalente =

IGP (Interior Gateway Protocol) Protocolo de Acceso Interno.

IS – IS (Intermediate System to Intermediate System) Sistema Intermedio a sistema intermedio

LAN (Local Area Network) Red de Área Local o simplemente Red Local.

LDP (Label Distribution Protocol) Protocolo de distribucion de etiquetas.

LER (Layer Edge Router) Conmutador Frontera entre capas.

LSP (Label Swichet Path) Camino Conmutado de Etiquetas.

LSR (Label Switch Router) Conmutador de Etiquetas.

MAN (Metropolitan Area Network) Red de Área Metropolitana .

MPLS (Multi-Protocol Level Swiching) Multi-Protocolo de conmutación de etiquetas.

OSI (Open System Interconection) Interconexión de Sistemas Abiertos.

OSPF (Open Shortest Path Frist) Primero la ruta más corta.

QoS (Quality of Service) Calidad de servicio

SDH (Synchronous Digital Hierarchy) La Jerarquía digital síncrona.

STM1 (Synchronous Transport Module level 1) Módulo síncrono de transporte nivel uno.

RFC (Request For Comments): Conjunto de notas técnicas y organizativas, donde se describen los estándares o recomendaciones de Internet.

TCP/IP (Transport Control Protocol / Internet Protocol) Protocolo de control de transporte / Protocolo de internet

TTL (Time To Live) Tiempo de Vida.

VPN (Virtual Private Network) Red Privada Virtual.

GLOSARIO

Ancho de Banda Capacidad de transmisión en unidades de datos por segundo de un calan físico de comunicaciones.

Backbone Área de una red de transmisión dedicada a la conmutación de paquetes a alta velocidad.

Celdas Término que especifica la unidad mínima de transmisión en una red.

Delay Retraso en la transmisión de información punto a punto.

Escalabilidad Característica de la red para poder evolucionar a nuevas tecnologías sin modificar su topología.

Ethernet Tecnología de redes de computadoras de área local (LANs) basada en tramas de datos que define las características de cableado y señalización de nivel físico, y los formatos de trama del nivel de enlace de datos del modelo OSI.

Etiqueta Un identificador de longitud corta constante que se emplea para identificar una Clase de envío Equivalente.

FEC (*Forwarding Equivalent Class*) Clase de envío equivalente. Es un subconjunto de paquetes IP que son tratados de la misma manera por un *router*.

Frame Relay Tecnología de transmisión de datos en forma de paquetes que permite ofrecer soluciones a servicios que demandan gran ancho de banda.

LAN (*Local Area Network*) Red de Área Local o simplemente Red Local, es la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de unos pocos kilómetros.

LDP (*Label Distribution Protocol*) Protocolo de distribución de etiquetas, es un protocolo mediante el cual un LSR comunica a otros LSRs asignaciones de etiquetas, utilizadas para enviar tráfico entre ellos. Por medio de este protocolo los LSRs crean caminos de conmutacion de etiquetas LSP a través de una red.

LER (*Layer Edge Router*) Conmutador Frontera entre capas: es el dispositivo LRS frontera entre IP y MPLS. Este equipo se encarga de asociar una etiqueta a una FEC determinada.

LSP (Label Swichet Path) Camino Conmutado de Etiquetas: camino compuesto por uno o más LSRs dentro de un nivel jerárquico por el que un paquete, que pertenece a un determinado FEC, circula.

LSR	(*Label Switch Router*) Conmutador de Etiquetas: es un equipo que realiza el envío de paquetes basándose en la información de la etiqueta del paquete recibido.
MPLS	(*Multi-Protocol Level Swiching*) Es un protocolo que está basado en el intercambio de etiquetas, una independiente y única etiqueta es insertada en cada uno de los paquetes; esta etiqueta es usada para intercambiar y rutear los paquetes a través de la red.
OSPF	(*Open Shortest Path Frist*) Primero la ruta más corta: Algoritmo de enrutamiento IGP jerárquico de estado enlace propuesto como sucesor del RIP.
QoS	(*Quality of Service*) Calidad de servicio: técnicas usadas para garantizar que se transmitirá cierta cantidad de paquetes de datos en un tiempo dado, por ejemplo paquetes de voz o video.
Trama	En telecomunicaciones una trama es una unidad de envío de datos. Sinónimo de paquete de datos o Paquete de red. Normalmente, una trama constará de cabecera, datos y cola.
TTL	(*Time To Live*) Tiempo de Vida; es un concepto usado en redes de computadores para indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen.

RESUMEN

MPLS fue presentado originalmente como una solución para mejorar la velocidad en los enrutadores, pero ahora está emergiendo como una tecnología de estándares crucial, la cual ofrece nuevas capacidades para redes IP a gran escala. Ejemplos de aplicaciones de MPLS son: Ingeniería de tráfico (la habilidad de los operadores de la red para dictaminar el camino que seguirá el tráfico a través de la red), y soporte para redes privadas virtuales VPN). Estos son dos ejemplos de aplicaciones clave donde MPLS es superior a cualquier tecnología IP disponible en la actualidad. Aunque MPLS fue concebido para ser independiente de la capa 2, gran parte del interés generado por MPLS gira alrededor de la promesa de implementar de una forma más efectiva redes IP a través de *backbones* WAN-ATM.

Los enrutadores IP convencionales contienen “tablas de enrutamiento”, las cuales son utilizadas en base al encabezado IP del paquete para tomar la decisión de cómo el paquete será enviado. Estas tablas son construidas basándose en protocolos de enrutamiento IP (ej. OSPF o RIP), los cuales transportan información de topología y alcance en la red en forma de direcciones IP. En la práctica encontramos que el plano de envío (búsqueda de dirección IP en la tabla) y el plano de control (generación de las tablas de enrutamiento) están íntimamente ligados. En cambio en MPLS el envío está basado en etiquetas, es posible separar de forma clara el plano de envío basado en etiquetas del plano de control. Separando estos dos planos cada uno puede ser modificado de forma independiente. Con esta separación no es necesario cambiar los dispositivos de envío, por ejemplo para migrar a una nueva estrategia de enrutamiento en la red.

En este trabajo se describe por qué fue inventado MPLS, qué hace, cómo funciona, qué ventajas proporciona y hacia donde está encaminado; así como un análisis técnico y económico de la migración de una red IP/ATM a MPLS.

OBJETIVOS

- **General**

  Analizar la factibilidad técnica y económica de migrar de una red IP/ATM a una red MPLS.

- **Específicos**

  1. Análisis de la migración de una red montada sobre ATM a una red sobre MPLS.

  2. Análisis de las diferencias y similitudes de los protocolos ATM y MPLS

  3. Análisis de las ventajas y desventajas que traería para las empresas la migración a MPLS.

  4. Documentación de características, lineamientos y procedimientos necesarios para realizar la migración de la red a MPLS.

  5. Análisis de la factibilidad técnica y económica de la migración a MPLS.

INTRODUCCIÓN

El enorme crecimiento de Internet, así como la aparición de nuevas aplicaciones en las áreas educativa, de investigación y comercial, con transmisión de video, datos, voz y aplicaciones multimedia, traen consigo la necesidad de mecanismos que hagan posible el funcionamiento eficaz de tales aplicaciones y motivan la creación de otras más innovadoras, así como los mecanismos que permitan la transición a un esquema de red de convergencia (donde no se tenga que tener redes diferentes para diferentes aplicaciones). Todo esto ha sido la motivación principal para la realización de este trabajo en donde se propone la migración de IP/ATM a tecnología MPLS (Multi Protocol Label Switching) como una solución versátil para hacer frente a las necesidades en la actualidad, como son: velocidad, escalabilidad, manejo de calidad del servicio (QoS) e ingeniería de tráfico. MPLS representa el siguiente nivel de evolución en estándares, donde se combinan las tecnologías de conmutación de capa dos (enlace de datos) y tecnologías de enrutamiento (capa 3). MPLS aparece como una solución elegante para alcanzar los requerimientos de ancho de banda y servicios para la nueva generación de redes *backbone* basadas en el protocolo IP.

En países como Guatemala no es la excepción de los problemas vistos anteriormente, muchas de las empresas de telecomunicaciones utilizan distintas plataformas y tecnologías para el transporte de datos e Internet, este proyecto propone además los lineamientos técnicos y económicos necesarios para la transición de una red IP/ATM a MPLS y dar el paso a la convergencia de servicios, obtener mejor administración de la red y aumentar la rentabilidad de la empresa.

1 INTRODUCCIÓN IP – ATM

El protocolo TCP / IP es hoy día una solución clásica y estándar al transporte de información en las redes. Aceptado por toda la comunidad de Internet, ha sido hasta hoy una solución aceptable para el envío de información, utilizando ruteo de paquetes con ciertas garantías de entrega. A su vez, los avances en el hardware y en las metodologías de ingeniería del tráfico están dando lugar al empleo creciente de las tecnologías de Conmutación, encabezadas por la tecnología ATM. Aportando velocidad, calidad de servicio y facilitando la gestión de los recursos en la red.

De aquí derivan los siguientes problemas: el paradigma del ruteo está muy extendido en todos los entornos, tanto empresariales como académicos, etc. El rediseño total del software existente hacia la Conmutación supondría un enorme gasto de tiempo y dinero. Igualmente sucede con el hardware que está funcionando hoy día.
Existen ciertas funcionalidades hoy día en las que sigue interesando emplear IP, esto no quita que las tramas IP estén siendo transportadas por paquetes ATM.

Debido al diseño de Internet, cualquier red deberá tener métodos que le permitan unirse al resto de las redes que la rodean. El ancho de banda de las redes que emplean ATM es desaprovechado cuando portan paquetes IP debido a los altos tiempos de proceso que necesita el Ruteo que se está ejecutando sobre ellas. En sí, se debe encontrar una solución puente entre ambas tecnologías para permitir:

- Adaptación de las tramas IP sobre las redes y protocolos ATM sin que por ello se pierdan las características de ATM, estas son: velocidad, garantías de calidad de servicio y gestión de tráfico en la red.

- Convivencia de ambas soluciones sobre un mismo escenario, permitiendo así una migración gradual hacia las nuevas tecnologías.
- Reutilización: se debe aprovechar lo ya existente y evitar en la medida de lo posible la alteración de la programación y del hardware ATM.

1.1 Protocolo IP

El Protocolo Internet (Internet Protocol), o Ipv4 es la parte central del paquete de protocolos de Internet. IP (RFC 791, RFC 1122) es un protocolo de red que ofrece un servicio de envío de paquetes no orientado a conexión. Sobre éste trabajan los protocolos de transporte, siendo el más común de ellos el protocolo TCP. Por esto en la terminología habitual nos encontremos con el término TCP/IP en referencias al funcionamiento conjunto de ambos protocolos.

IP es un protocolo orientado a datagramas que trata cada paquete de manera independiente, de modo que cada paquete deberá contener toda la información necesaria para ser direccionado de manera correcta. No tiene garantías de entrega de paquetes ni garantías de integridad en la información recibida ya que ni emplea el checksum para comprobar el contenido del paquete, ni posee mecanismos de confirmación para determinar si el paquete ha alcanzado su destino.

El protocolo IP junto con protocolos como ARP, RARP o ICMP define el formato del datagrama, direccionamiento, procesamiento de paquetes, routing y mecanismos para mostrar errores en Internet. Tal y como se describe en el RFC 1122, un host que esté ejecutando el protocolo IP, normalmente también admitirá ARP y ICMP.

El Protocolo IP proporciona un sistema de distribución que es poco fiable incluso en una base sólida. El protocolo IP especifica que la unidad básica de transferencia de datos en el TCP/IP es el datagrama.

Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en una secuencia incorrecta o fragmentados intencionadamente para permitir que un nodo con un buffer limitado pueda procesar todo el datagrama. Es la responsabilidad del protocolo IP reensamblar los fragmentos del datagrama en el orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar ningún mensaje mientras que en otras situaciones los mensajes de error son recibidos por la maquina origen (esto lo hace el protocolo ICMP).

El protocolo IP también define cual será la ruta inicial por la que se enviarán los datos. Cuando los datagramas viajan de unos equipos a otros, es posible que atraviesen diferentes tipos de redes. El tamaño máximo de estos paquetes de datos puede variar de una red a otra, dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (Maximum Transmission Unit), y ninguna red puede transmitir un paquete de tamaño mayor a esta MTU. El datagrama consiste en una cabecera y datos. (Ver Figura 1)

Longitud de la Cabecera

Este campo ocupa 4 bits, y representa el número de octetos de la cabecera dividido por cuatro, lo que hace que este sea el número de grupos de 4 octetos en la cabecera.

Versión

El campo versión ocupa 4 bits. Este campo hace que diferentes versiones del protocolo IP puedan operar en la Internet. En este caso se trata de la versión 4.

Tipo de servicio

Este campo ocupa un octeto de la cabecera IP, y especifica la precedencia y la prioridad del datagrama IP. Los tres primeros bits del octeto indican la precedencia. Los

valores de la precedencia pueden ser de 0 a 7. Cero es la precedencia normal, y 7 esta reservado para control de red. Muchas puertas de enlace ignoran este campo. Los otros 4 bits definen el campo prioridad, que tiene un rango de 0 a 15. Las cuatro prioridades que están asignadas son: 0, (por defecto, servicio normal), 1 (minimizar el coste monetario), 2 (máxima fiabilidad), 4 (Maximizar la transferencia), 8 (El bit +4 igual a 1, define minimizar el retraso). Estos valores son utilizados por los routers para direccionar las solicitudes de los usuarios.

Longitud Total

Este campo se utiliza para identificar el número de octetos en el datagrama total.

Identificación

El valor del campo identificación es un numero secuencial asignado por el Host origen. El campo ocupa dos octetos. Los números oscilan entre 0 y 65.535, que cuando se combinan con la dirección del Host forman un número único en la Internet. El número se usa para ayudar en el reensamblaje de los fragmentos de datagramas.

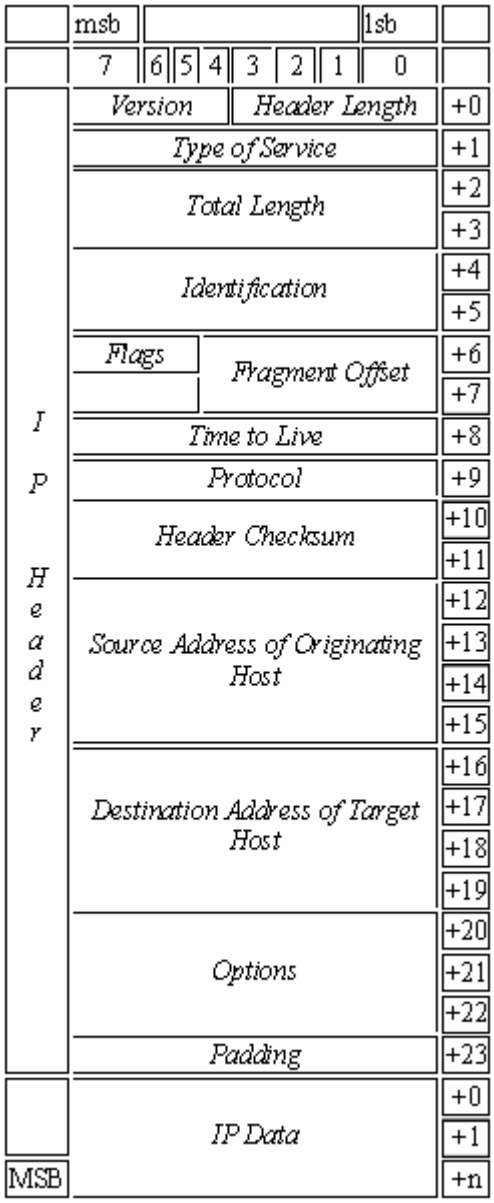
Fragmentos Offset

Cuando el tamaño de un datagrama excede el MTU, este se segmenta. El fragmento Offset representa el desplazamiento de este segmento desde en inicio del datagrama entero.

Fragmentos Offset

Cuando el tamaño de un datagrama excede el MTU, este se segmenta. El fragmento Offset representa el desplazamiento de este segmento desde en inicio del datagrama entero.

Figura 1. Formato del Datagrama IP



Fragmentos Offset

Cuando el tamaño de un datagrama excede el MTU, este se segmenta. El fragmento Offset representa el desplazamiento de este segmento desde en inicio del datagrama entero.

Banderas (Flags)

El campo flag ocupa 3 bits y contiene dos flags. El bit +5 del campo flags se utiliza para indicar el último datagrama fragmentado cuando toma valor cero. El bit +7 lo utiliza el servidor origen para evitar la fragmentación. Cuando este bit toma valor diferente de cero y la longitud de un datagrama excede el MTU, el datagrama es descartado y un mensaje de error es enviado al Host de origen por medio del protocolo ICMP.

Tiempo de Vida

El campo tiempo de vida ocupa un octeto. Representa el numero máximo de segundos que un datagrama puede existir en Internet, antes de ser descartado. Un Datagrama puede existir un máximo de 255 segundos. El número recomendado para IP es 64. Quien origina del datagrama manda un mensaje ICMP cuando el datagrama es descartado.

Protocolo

El campo protocolo se utiliza para identificar la capa de mayor nivel más cercana usando el IP. Este es un campo de 0 bits, que normalmente identifica tanto la capa TCP (valor 6), como la capa UDP (valor 17) en el nivel de transporte, pero puede identificar hasta 255 protocolos de la capa de transporte.

Checksum

El checksum proporciona la seguridad de que el datagrama no ha sido dañado ni modificado. Este campo tiene una longitud de 16 bits. El checksum incluye todos los

campos de todos los campos de la cabecera IP, incluido el mismo, cuyo valor es cero a efectos de cálculo. Una puerta de enlace o nodo que efectué alguna modificación en los campos de la cabecera (por ejemplo en el tiempo de vida), debe recalcular el valor del checksum antes de enviar el datagrama. Los usuarios del IP deben proporcionar su propia integridad en los datos, ya que el checksum es solo para la cabecera.

Dirección de Origen

Este campo contiene un identificador de red (Netid) y un identificador de Host (Hostid). El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C. como se vera mas adelante.

Dirección de Destino

Este campo contiene el identificador de red (Netid) y un identificador de Host (Hostid) del destino. El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C o D.

Opciones

La existencia de este campo viene determinada por la longitud de la cabecera. Si esta es mayor de cinco, por lo menos existe una opción. Aunque un Host no esta obligado a poner opciones, puede aceptar y procesar opciones recibidas en un datagrama. El campo Opciones es de longitud variable. Cada octeto esta formado por los campos Copia, Clase de Opción y Número de Opción.

- El campo Copia sirve para que cuando un datagrama va a ser fragmentado y viaja a través de nodos o Puertas de Enlace. Cuando tiene valor 1, las opciones son las mismas para todos los fragmentos, pero si toma valor 0, las opciones son eliminadas.

- Clase de Opción es un campo que cuando tiene valor 0, indica datagrama o control de red; Cuando tiene valor 2, indica depuración o medida. Los valores 1 y 3 están reservados para un uso futuro.
- El Número de Opción indica una acción específica.

Tabla I Características de la Opción IP

Clase de Opción	*Numero de Opción*	*Octetos*	*Descripción*
0	*0*	*1*	*Fin de alineamiento*
0	*1*	*1*	*Para alinear dentro de una lista de*
0	*2*	*11*	*Seguridad (aplicaciones militares)*
0	*3*	*var*	*Ruteo del Origen*
0	*7*	*var*	*Grabar/trazar ruta*
0	*9*	*var*	*Ruteo estricto del Origen*
2	*4*	*var*	*Fecha y hora de Internet*

Padding

Cuando esta presente el campo Pad, consiste en 1 a 3 octetos puestos a cero, si es necesario, para hacer que el número total de octetos en la cabecera sea divisible por cuatro.

Datos

El campo datos consiste en una cadena de octetos. Cada octeto tiene un valor entre 0 y 255. El tamaño de la cadena puede tener un mínimo y un máximo, dependiendo del medio físico. El tamaño máximo esta definido por la longitud total del datagrama.

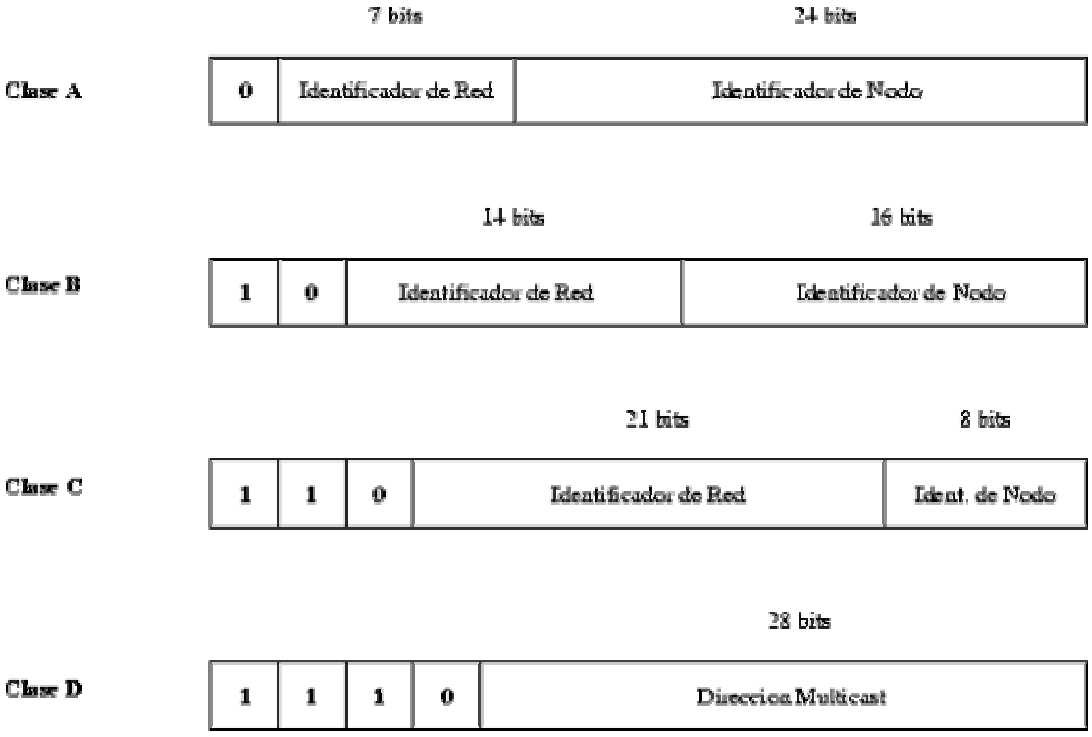
Direcciones IP

Las direcciones IP hacen que el envío de datos entre ordenadores se haga de forma eficaz, de un modo similar al que se utilizan los números de teléfono. Las

direcciones IP tienen 32 bits, formados por cuatro campos de 8 bits separados por puntos. Cada campo puede tener un valor comprendido entre 0 y 255. Esta compuesta por una dirección de red, seguida de una dirección de subred y de una dirección de host.

Existen cinco clases de subredes, tal y como muestra la Figura 2

Figura 2 Clases de Direcciones IP



- La clase A contiene 7 bits para direcciones de red, con lo que permite tener hasta 128 redes, con 16.777.216 ordenadores cada una. Las direcciones estarán comprendidas entre 0.0.0.0. y 127.255.255.255., y la mascara de subred será 255.0.0.0.
- La clase B contiene 14 bits para direcciones de red y 16 bits para direcciones de hosts. El numero máximo de redes es 16.536 redes, con 65.536 ordenadores por red. Las direcciones estarán comprendidas entre 128.0.0.0. y 191.255.255.255., y la mascara de subred será 255.255.0.0.

- La clase C contiene 21 bits para direcciones de red y 8 para hosts, lo que permite tener un total de 2.097.142 redes, cada una de ellas con 256 ordenadores. Las direcciones estarán comprendidas entre 192.0.0.0. y 223.255.255.255., y la mascara de subred será 255.255.255.0.
- La clase D se reserva todas las direcciones para multidestino (multicast), es decir, un ordenador transmite un mensaje a un grupo específico de ordenadores de esta clase. Las direcciones estarán comprendidas entre 224.0.0.0. y 239.255.255.255.
- La clase E se utiliza exclusivamente para fines experimentales. Las direcciones están comprendidas entre 240.0.0.0. y 247.255.255.255.

1.2 Tecnología ATM

El Modo de Transferencia Asíncrono (ATM) es la base de un estándar internacional propuesto como un sistema de conmutación de paquetes para el transporte de datos basado en celdas o células de longitud fija y de pequeño tamaño (53 octetos). Se caracteriza también ATM por ofrecer funciones de gestión de tráfico para la transferencia óptima de información en tiempo real (tráfico multimedia) y tiempo no-real (datos o imágenes estáticas), aportando la atractiva ventaja de la integración de diferentes flujos de información.

La tecnología ATM recibe su máximo impulso cuando es elegida por CCITT como la base para la implementación de la RDSI-BA (Red Digital de Servicios Integrados de Banda Ancha). Desde ese momento, y a lo largo de más de una década, la tecnología ha experimentado una continua evolución siendo fuente de constantes investigaciones que han permitido que sea en la actualidad la solución más sólida en las troncales internacionales de largo alcance. Otra de las ventajas de ATM es precisamente su escalabilidad lo que le permite ser implantada tanto en entornos WAN como MAN y LAN.

La integración de servicios y la escalabilidad, ligadas al extraordinario rendimiento de los medios de transmisión ópticos que soportan velocidades de transferencia del orden de Gbps, con probabilidades de error en torno a 10-12, han permitido que ATM de respuesta a las actuales necesidades de comunicación a través de aplicaciones de toda índole.

La característica orientada a la conexión de ATM es uno más de los aspectos diferenciadores con otras tecnologías claramente implantadas como las redes IP. El hecho de ser una tecnología orientada a conexión hace que las transferencias se realicen a través de circuitos virtuales (VPI/VCI) establecidos extremo-a-extremo, y los cuáles se mantienen abiertos durante todo el tiempo que dura la comunicación. Estos circuitos virtuales son creados en la fase de establecimiento de la conexión que es cuando el usuario de la red puede especificar los parámetros de tráfico que va a generar, o los recursos de red que va a requerir. Así, el usuario negocia la calidad del servicio que espera recibir, de forma que la propia red dispone de mecanismos de gestión de recursos como la función CAC (Control de Admisión de la Comunicación), y como la función UPC (Control de Parámetros de Uso). La función CAC, usada para la negociación de la conexión, actúa a modo de control de flujo impidiendo la entrada de usuarios para los que la red no dispone de recursos, y evitar la sobrecarga de ésta. La función UPC se encarga de velar, durante la comunicación, por el buen cumplimiento del contrato de tráfico que los usuarios han negociado con la función CAC en el establecimiento de la conexión.

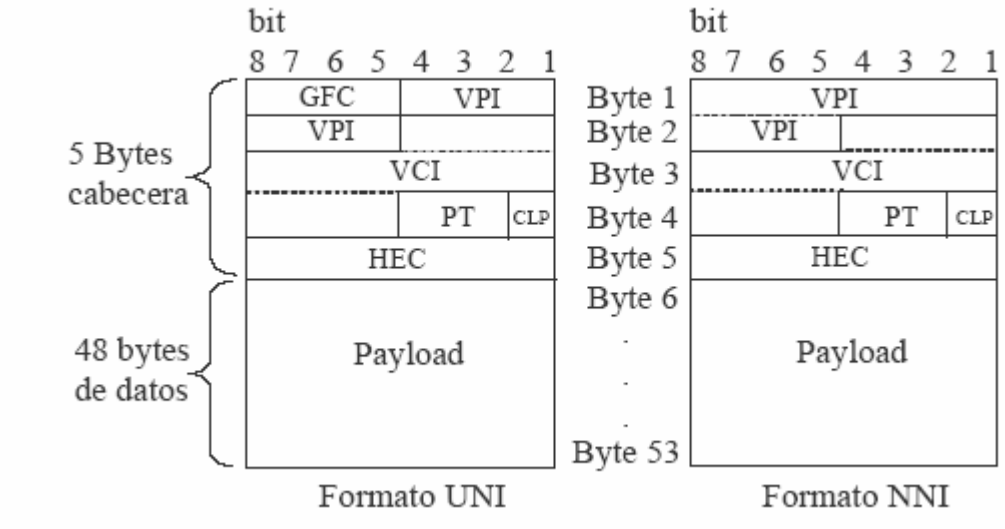
Vemos como ATM no sólo se encarga de atender las necesidades de conexiones concretas, sino también del estado general de la misma, de forma que se intentan evitar situaciones de sobredimensión que conduzcan a congestiones o sobrecargas. A la vista de esta descripción general de las características más importantes de la tecnología podemos adivinar que, aunque muchos aspectos de la misma están resueltos, aún quedan

muchos otros que son foco de atención de la comunidad investigadora que realiza propuestas para mejorar la tecnología.

Características Principales de la Tecnología ATM

La célula constituye la unidad de transferencia de las redes ATM que, como hemos dicho antes, son de tamaño fijo y relativamente pequeñas si se compara con otras tecnologías. De los 53 octetos totales, 5 bytes se emplean para las cabeceras y los 48 restantes se emplean para la carga útil de datos. La Figura 3 muestra cada uno de los campos de las cabeceras con sus tamaños en bits. Se puede observar separadamente el formato de las células UNI (User Network Interface) usadas entre extremos de la comunicación y la red, y el de las células NNI (Network to Network Interface) usadas entre los conmutadores de la red.

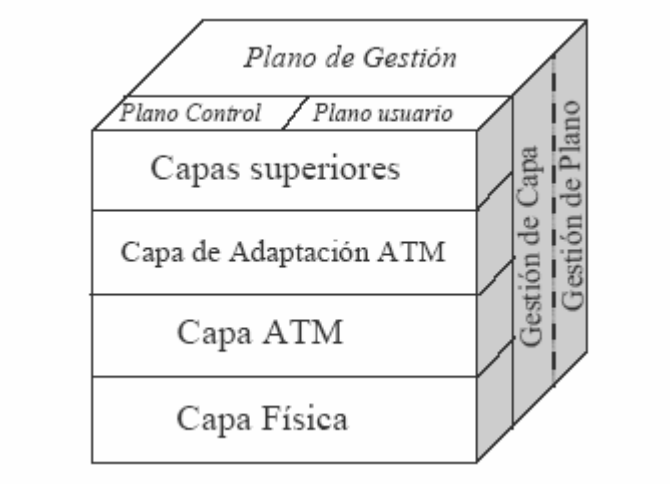
Figura 3 Formato de células ATM



Cada célula lleva en su cabecera un identificador de camino virtual (VPI) de 8 bits y un identificador de canal virtual (VCI) de 16 bits. El campo PT (Payload Type) de 3 bits se usa para indicar el tipo de información contenida en el campo de carga de datos

de la célula. El bit CLP (Cell Loss Priority) lo emplea el emisor para especificar la prioridad deseada cuando aparecen situaciones de congestión. Las células con CLP = 1 tienen más baja prioridad y serán las primeras en ser descartadas por los conmutadores cuando se congestionan. El campo HEC (Header Error Control) se usa como mecanismo de detección de los errores producidos en las transmisiones de las cabeceras. Con los 8 bits del campo HEC se detectan todos los errores de los 32 bits restantes de la cabecera, aportando un mecanismo realmente poderoso ligado a las bajas tasas de error de la fibra óptica que hemos comentado antes.

Figura 4 Modelo Arquitectónico ATM



Una cuestión básica para nosotros es la comprensión del modelo arquitectónico ATM ya que sobre éste vamos a realizar aportaciones con la doble intención de mantenerlo para respetar las características nativas del modelo en nuestra arquitectura, y a la vez de modificarlo para conseguir nuestros objetivos de mejora de la tecnología. Describimos por esto el modelo presentado en la Figura 4 donde podemos observar las tres capas principales de la pila de protocolos que constituyen la arquitectura tridimensional ATM.

El modelo ATM se apoya en las capas Física, ATM y de Adaptación ATM, cada una de ellas con una serie de funciones especificadas para permitir las transferencias de las células.

Algo esencial para el servicio ofrecido por las redes ATM es la capa de Adaptación ATM que permite adaptar los flujos de la capa Física (basados en células) a paquetes, datagramas o flujos de bits propios de las capas superiores de la pila de protocolos. La capa AAL está formada por dos subcapas: en la parte superior la Subcapa de Convergencia (SC) y por debajo de ésta la Subcapa de Segmentación y Reensamblado (SAR). Las funciones de estas capas son las siguientes:

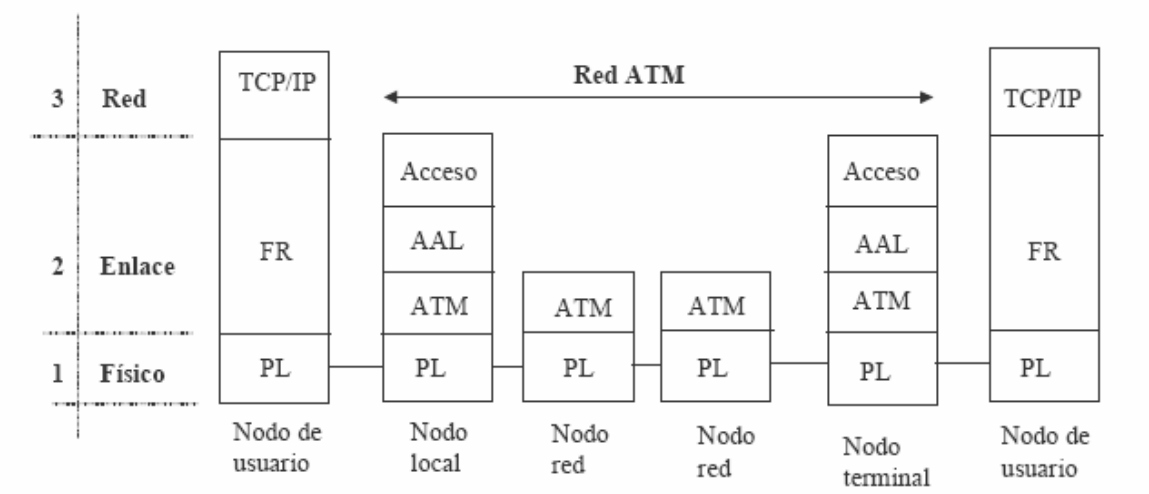
- Subcapa de Convergencia: Realiza la adaptación a la velocidad de transferencia del usuario, la corrección de errores y mantiene la sincronización extremo a extremo y se encarga del control de flujo.

- Subcapa SAR: en el caso del emisor, es la responsable de segmentar el tráfico continuo de tramas de información a células de 48 octetos que son pasadas a la capa ATM inferior. También detecta posibles células erróneas y/o perdidas. En el caso del receptor esta misma subcapa se encarga del reensamblado de las células que recibe desde la capa ATM para convertirlas en PDUs o tramas que van a ser pasadas a los protocolos de las capas superiores.

Una visión complementaria del modelo ATM de la Figura 4 puede ser obtenida observando la Figura 5 donde se representan las capas de la arquitectura, tanto en los nodos de la red como en los nodos locales y en los de usuario. Podemos ver cómo los nodos de la red o conmutadores no disponen de capa de adaptación AAL, ya que el tráfico en la red es completamente nativo ATM y lo que se transmite entre conmutadores son células. Los nodos o conmutadores locales sí soportan la capa AAL, ya que necesitan ajustar el tráfico generado desde los nodos terminales de usuario que, como

podemos observar, pueden hacerlo a través de cualquier protocolo de comunicación como TCP/IP. En realidad, las células no son visibles por los usuarios que lo que hacen es generar las tramas propias del protocolo que están usando. Estas tramas son las que AAL se encargará de segmentar en células que pasan a la capa ATM, que no es otra cosa que un modo de transporte de células que son transferidas a la capa Física. La Figura 5 representa también las tres primeras capas del modelo de referencia OSI aportando una comparativa entre los dos modelos arquitectónicos, aunque en este aspecto no existe demasiado consenso sobre la relación entre las capas de cada uno de los modelos.

Figura 5 Modelo arquitectónico ATM y RM-OSI



Clases de Servicio ATM

La tecnología ATM fue diseñada y desarrollada para soportar e integrar varias clases de servicio como los datos y la información multimedia, generada o no, en tiempo real. Una conexión es establecida como resultado de la negociación entre el usuario y la red donde se estipula la Clase de Servicio (CoS) a adoptar. La clase de servicio es definida por los parámetros de tráfico de la conexión y por sus parámetros de Calidad de Servicio

(QoS). El ATM Forum ha propuesto varias CoS, en función de las capacidades de transferencia de información ATM. Cada una especifica un conjunto de parámetros y procedimientos de capa ATM para sustentar un modelo de servicio y un conjunto de valores de QoS asociados. Cada CoS es especificada en términos de un modelo de servicio, un descriptor de tráfico, unos procedimientos específicos, una definición de conformidad y los compromisos de QoS demandados por cada conexión, los cuáles la red se compromete a cumplir. A continuación se definen brevemente las cinco categorías de servicio enunciadas por el ATM Forum:

- CBR (Constant Bit Rate): Se emplea para las conexiones que solicitan un tamaño de ancho de banda estático que deberá estar completamente disponible para la aplicación durante todo el tiempo que dure la conexión. El tamaño del ancho de banda se caracteriza por el valor PCR (Peak Cell Ratio). Esta categoría de servicio puede emplearse, tanto para VPCs como para VCCs. El servicio CBR está pensado para soportar aplicaciones en tiempo real con pequeñas variaciones de retardo (voz, vídeo, emulación de circuitos) pero no queda únicamente restringida a estas aplicaciones.

- rt-VBR (real time-Variable Bit Rate) pensada para aplicaciones de tiempo real que requieren mínimo retardo y mínimas variaciones de retardo, apropiadas para aplicaciones de voz y vídeo. Sus fuentes de información pueden entenderse como ráfagas y se espera que transmitan ratios distintos a lo largo del tiempo. Las conexiones de este tipo se caracterizan por los valores PCR, SCR (Sustainable Cell Rate) y MBS (Maximum Burst Size).

- nrt-VBR (non-real-time-Variable Bit Rate) pensada para aplicaciones sin requerimientos de tiempo real y con tráfico a ráfagas. La aplicación tiene un ratio bajo de pérdidas de células y no existen límites de retardo.

- UBR (Unspecified Bit Rate) pensada para aplicaciones sin necesidades de tiempo real ni de bajo retardo ni variaciones de retardo. Son aplicaciones típicas de esta categoría de servicio la transferencia de ficheros y el correo electrónico. Los servicios UBR no permiten especificar ninguna garantía de servicio a sus tráficos de información.

- ABR (Available Bit Rate). En esta categoría de servicio las características de la capa de transferencia ATM, que han sido ofrecidas por la red, pueden cambiar después de establecida la conexión. Se especifican mecanismos de control de flujo que soportan varios tipos de realimentación para controlar el ratio de la fuente en respuesta a los cambios de las características de transferencia de la capa ATM. La realimentación es convenida en la fuente a través de las células específicas de control llamadas RM. Se espera que un sistema final sea capaz de adaptar su tráfico según la realimentación, alcanzando así un bajo ratio de pérdidas y conseguir compartir justamente el ancho de banda de acuerdo a la política de asignación especificada. ABR no está pensada para soportar aplicaciones en tiempo real y por eso no requiere límite de retardo ni variaciones en el retardo. En el establecimiento de la conexión el sistema final especifica a la red el máximo ancho de banda que necesita (PCR) y el mínimo ancho de banda utilizable (MCR). El ancho de banda disponible en la red puede cambiar con el tiempo, pero no será menor al valor de MCR.

La tabla II muestra algunas de las características principales de las CoS definidas por el ATM-Forum.

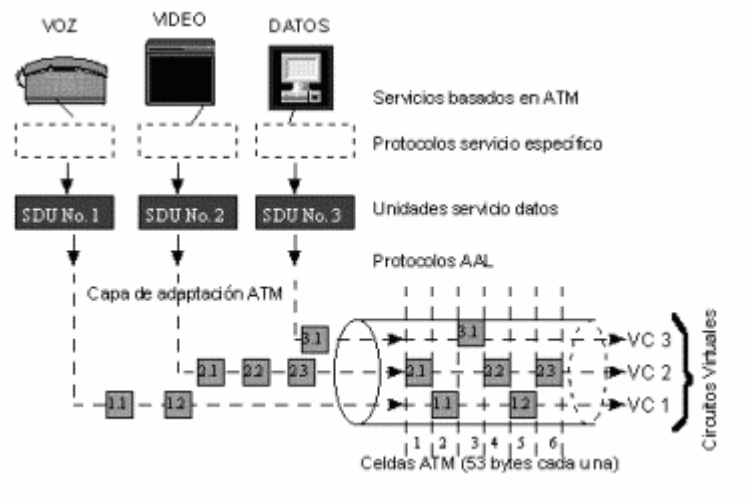
Tabla II Características de las Clases de Servicio ATM

Características	CBR	RT-VBR	NRT-VBR	ABR	UBR
Ancho de Banda Garantizado	SI	SI	SI	Opcional	NO
Adecuado para el tráfico tiempo real	SI	SI	NO	NO	NO
Adecuado para el tráfico a ráfagas	NO	NO	SI	SI	SI
Realimentación en Congestiones	NO	NO	NO	SI	NO

Multiplexacion en ATM

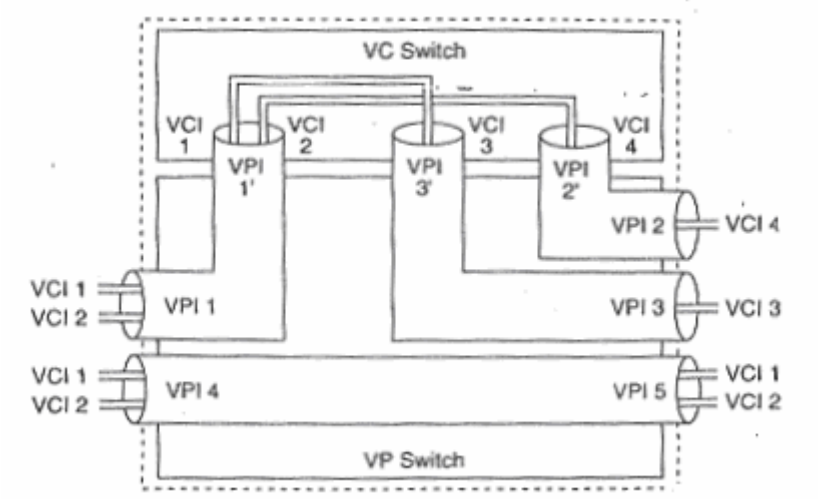
La figura 6 muestra un formato básico y la jerarquía de ATM. Una conexión ATM, consiste de "celdas" de información contenidos en un circuito virtual (VC). Estas celdas provienen de diferentes fuentes representadas como generadores de bits a tasas de transferencia constantes como la voz y a tasas variables tipo ráfagas (bursty traffic) como los datos. Cada celda compuesta por 53 bytes, de los cuales 48 (opcionalmente 44) son para trasiego de información y los restantes para uso de campos de control (cabecera) con información de "quién soy" y "donde voy"; es identificada por un "virtual circuit identifier" VCI y un "virtual path identifier" VPI dentro de esos campos de control, que incluyen tanto el enrutamiento de celdas como el tipo de conexión. La organización de la cabecera (header) variará levemente dependiendo de sí la información relacionada es para interfaces de red a red o de usuario a red. Las celdas son enrutadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local - ya que pueden ser cambiados de interfase a interfase.

Figura 6 Formato Básico y la Jerarquía ATM



La técnica ATM multiplexa muchas celdas de circuitos virtuales en una ruta (path) virtual colocándolas en particiones (slots), similar a la técnica TDM. Sin embargo, ATM llena cada slot con celdas de un circuito virtual a la primera oportunidad, similar a la operación de una red conmutada de paquetes. La figura 7 describe los procesos de conmutación implícitos los VC switches y los VP switches.

Figura 7 Procesos de Conmutación en ATM



Los slots de celda no usados son llenados con celdas "idle", identificadas por un patrón específico en la cabecera de la celda. Este sistema no es igual al llamado "bit stuffing"en la multiplexación Asíncrona, ya que aplica a celdas enteras.
Diferentes categorías de tráfico son convertidas en celdas ATM vía la capa de adaptación de ATM (AAL - ATM Adaptation Layer), de acuerdo con el protocolo usado.

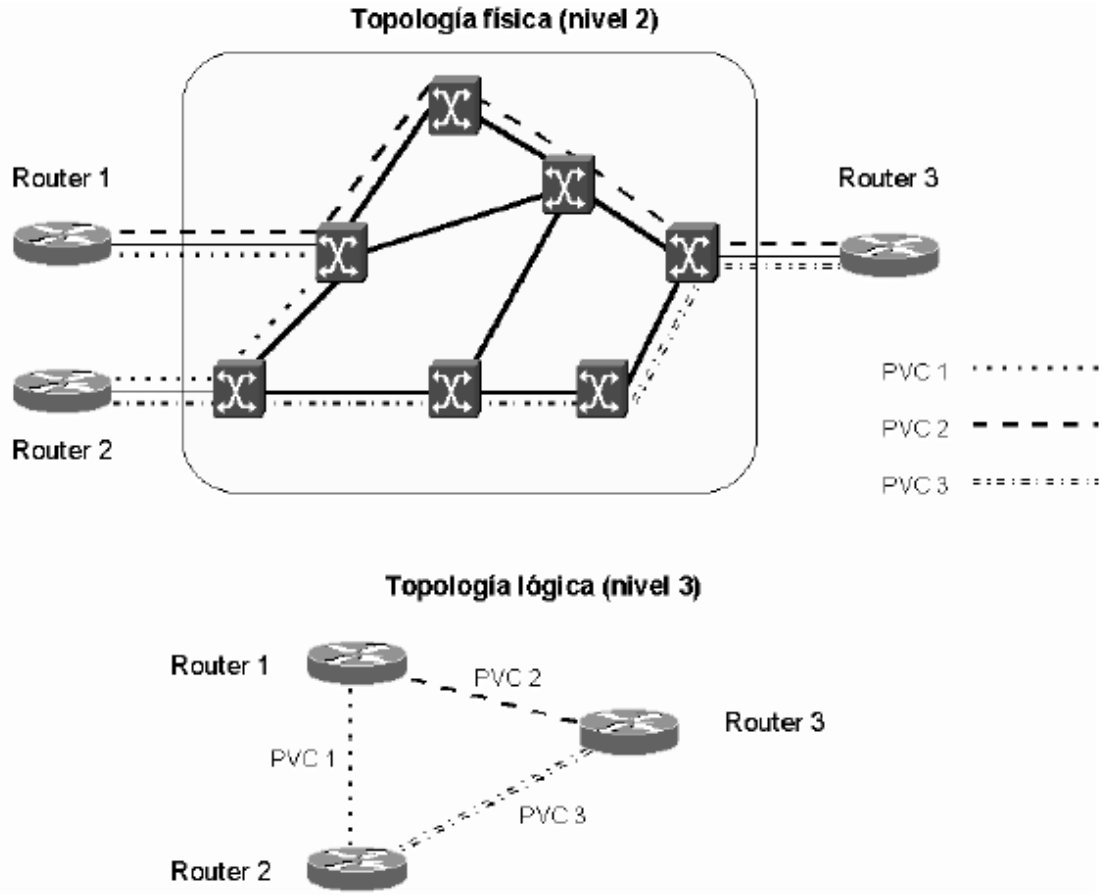
1.3 El protocolo IP sobre ATM

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI...). Por otro lado, hay que recordar que los *backbones* IP que los proveedores de servicio (NSP) habían empezado a desplegar en esos años, estaban construidos basados en *routers* conectados por líneas dedicadas T1/E14 y T3/E35. El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. Las respuestas de los NSPs fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los NSPs 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. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los *routers* tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de

telecomunicación. Estas redes ofrecían entonces una buena solución a los problemas de crecimiento de los NSPs. Por un lado, proporcionaba mayores velocidades (155 Mpbs) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de NSPs, 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.

Figura 8 Topología física ATM y topología lógica IP superpuesta.

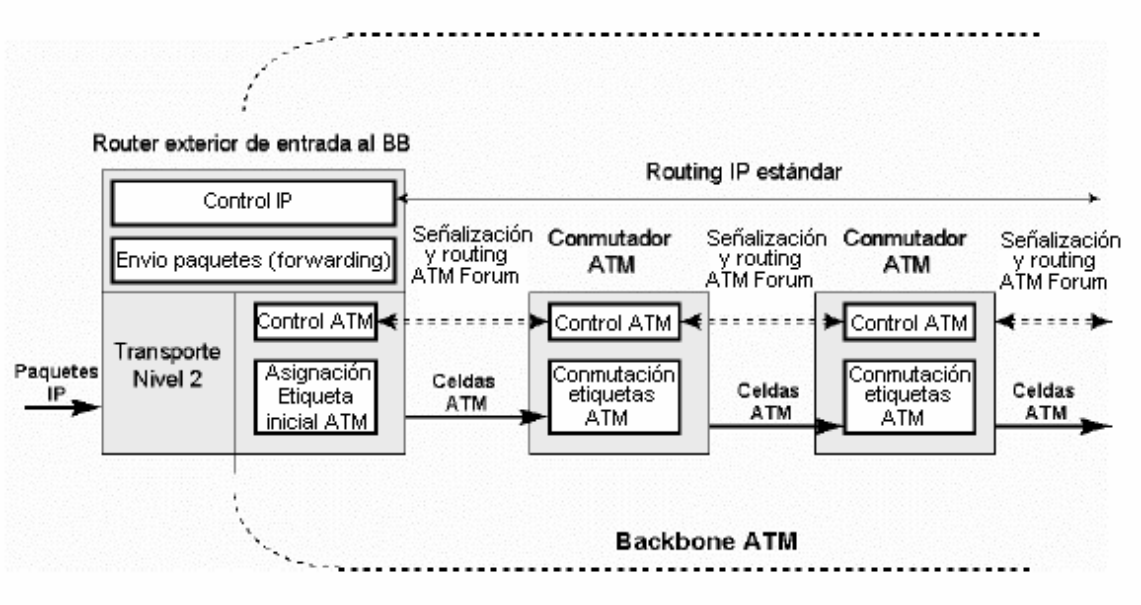


El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El *backbone* ATM se presenta como

una nube central (el núcleo) rodeada por los routers de la periferia. Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la figura 8 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 la anterior.

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y *routing*) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. (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 routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En la figura 9 se representa el modelo IP/ATM con la separación de funciones entre los que es *routing* 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, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

Figura 9 Modelo Funcional IP sobre ATM.



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 NSPs de primer nivel, ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de las necesidades del tráfico IP, utilizando la clase de servicio ATM 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 *routers* los PVCs necesarios, con una topología lógica entre routers totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los subinterfaces en los *routers* con los PVCs, a través de los cuales se intercambian los *routers* la información de encaminamiento correspondiente al protocolo interno IGP. Lo habitual es que, entre cada par de routers, 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 costes de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", un *overhead* aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada.

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

1.4 Alternativas de IP/ATM

En este apartado se van a describir las propuestas más destacadas que intentan solucionar el problema ya mencionado de IP/ATM . Dado el carácter investigador de muchas de las soluciones aquí descritas, es difícil a priori realizar una evaluación precisa del rendimiento que aportan, o del coste tanto en tiempo como en recursos que su implantación supone. Por el contrario, al tener definidos los modelos teóricos, la arquitectura y los protocolos, resulta más efectivo realizar evaluaciones de puntos tales como si admiten Multicast, IP nativo, ATM nativo, complejidad de los procedimientos, necesidad de modificaciones en el hardware existente, etc.

Y lo más importante, habrá que evaluar la flexibilidad de las soluciones para admitir modificaciones en el diseño sobre la marcha para, una vez realizada la

implementación, admitir el mayor número de cambios en los parámetros de la red (QoS, enrutado, tarificación, ancho de banda, etc),

1.4.1 LANE

LANE es una buena solución para interconectar equipos LAN en una red privada, aprovechando al máximo la alta velocidad de transmisión ATM con cambios mínimos en los equipos. Además, no se necesita modificar ninguna aplicación ni protocolo de las capas superiores a IP. Es una solución rápida que ya está operativa. Además, supone una buena opción para una integración progresiva de LAN a ATM en una red corporativa. Las mejoras que LANE aporta el concepto de LAN Virtual, aportando una flexibilidad mejorada a la hora de configurar parámetros de la red y una manipulación de estos mucho más sencilla que las LAN clásicas. Sin embargo, se le pueden encontrar ciertas limitaciones:

- Oculta por completo las funcionalidades en QoS que aporta ATM, esto es debido a cómo está concebida su arquitectura, emulando la tecnología de medio compartido de ciertas LANs clásicas.
- No puede correr protocolos en modo nativo.
- Su alcance está limitado a una subred lógica (LAN virtual o VLAN).
- Todo el tráfico entre VLANs debe pasar a través de routers, incluso si pudiera darse una conexión directa mediante ATM. Como consecuencia los routers pueden dar lugar a cuellos de botella en el flujo de datos.
- La conversión de direcciones LANE es ineficiente debido a que las direcciones se convierten de direcciones de la capa 3 a direcciones MAC y posteriormente direcciones ATM, empleando dos mecanismos de resolución de direcciones.
- El funcionamiento de LANE requiere muchas conexiones, limitando el número de equipos que pueden pertenecer a una LAN Emulada. No dispone de mecanismos de recuperación en el servidor, de modo que no admite la

posibilidad de definir LES y BUS de “seguridad” para actuar en situaciones de emergencia.

- Posee límites en el tamaño de la MTU.

1.4.2 IP Clásico sobre ATM

La principal ventaja que aporta es su compatibilidad total con IP estándar. Permitiendo a la gran mayoría de protocolos y aplicaciones que se encuentran por encima de éste ejecutarse de manera transparente sobre ATM, aprovechando el gran ancho de banda de ATM.

Otra ventaja que aporta es la facilidad de integrar servicios basados en IP con servicios basados en ATM. (Por ejemplo, servicios de voz). El principal problema de esta solución es que no puede utilizar las funcionalidades en garantías de QoS de ATM debido a los siguientes motivos:

- Las conexiones ATM directas solo se pueden establecer dentro de un LIS, pero no a lo largo de los extremos. Debido que la resolución de direcciones está limitada a una sola Subred Lógica IP (LIS Logical IP Subset), el tráfico IP entre nodos en diferentes LIS, siempre circulará por algún router intermedio, que sólo puede emplear el paradigma IP del best efort en garantías de QoS.
- Todos los flujos de datos IP entre dos hosts comparten el ancho de banda de un solo Circuito Virtual. De modo que resulta imposible a una aplicación individual conseguir una garantía de QoS para su flujo de datos concreto.

Otro problema de IP clásico sobre ATM es la imposibilidad de realizar multicast (ni unicast). Además no existe un camino por defecto para enviar datagramas IP antes de que se establezca una conexión, provocando un retraso alto al circular el primer

datagrama. Aunque esta solución no permite aprovechar muchos de los equipos LAN clásicos, ofrece un tamaño mayor, y más apropiado de MTU.

1.4.3 NHRP

La ventaja principal de esta solución es que puede resolver el problema de múltiples saltos a través de distintas subredes ofreciendo la Resolución de Direcciones inter - LIS. Permitiendo así el establecimiento de una conexión directa entre las redes NBMA, (NMBA: Non Broadcast Multi Access Networks) si éstas son ATM, se establece un Circuito Virtual directo entre varios LIS, mpleando QoS para el ‡ujo de datos IP entre los extremos del Circuito Virtual.

Pero NHRP (Next Hop Resolution Protocol) sólo podrá realizar esto si el camino de la ruta es abarcado por completo por subredes NBMA, y sólo bajo las condiciones que admite NHRP.
Además, al igual que IP clásico sobre ATM, una conexión IP directa será compartida por el tráfico generado por todas las aplicaciones comunes entre los dos extremos, de modo que resulta imposible dar QoS a una aplicación específica.

Otro problema con NHRP es que se pueden dar bucles en el routing, si las estaciones de inicio y de respuesta NHRP son routers, que estén conectados además a otra red. Evitar estos bucles supone imponer restricciones en la configuración de la red.

Otro problema que puede aparecer es el efecto dominó. Se da cuando un router crea una petición de resolución NHRP para un paquete que llegue sobre uno de sus interfaces NHRP. Si éste envía los paquetes de datos sin esperar a que se establezca un nuevo camino, el siguiente router que reciba el paquete puede crear su propia petición de resolución y reenviar el paquete, y así sucesivamente.

El empleo de NHRP requiere la introducción de software específico en todos los hosts y routers conectados a la red NBMA. Además, la especificación actual sólo está pensada para comunicaciones unicast, no se adapta a broadcast o multicast. NHRP es un borrador y es poco probable que sea admitido de manera genérica.

1.4.4 MPOA

Se trata de una tecnología muy compleja. Hasta la aparición de MPLS era la tecnología más prometedora aportando los siguientes beneficios :

- Da conectividad a un entorno que emplee routing. Admitiendo tanto multicast como broadcast en la capa 3.
- Aprovecha al máximo las ventajas de ATM, ofreciendo conexiones ATM directas entre dispositivos MPOA, sin saltos intermedios. Además admite ATM nativo, adaptando la QoS en la pila de protocolos.
- Reduce los costes en la infraestructura definiendo una nueva arquitectura de red. Aprovechando al máximo la funcionalidad de conmutación, que es muy barata y puede realizarse en hardware. Y dejando el routing, más caro y con más necesidades de rendimiento, en los Dispositivos Frontera.
- Da una solución universal para cualquier protocolo de la capa 3 sobre ATM.
- Se integra fácilmente con LANE.

Las principales desventajas, son su complejidad, debiendo desarrollar mucho código sobre las máquinas. Y la necesidad de cambiar la pila de protocolos en los hosts.

1.4.5 Arequipa

Como principales ventajas que aporta podemos indicar:

- Mejora el IP clásico sobre ATM para que las aplicaciones basadas en IP empleen todas las características de garantías de QoS de ATM permitiéndoles establecer y controlar sus propios Circuitos Virtuales.
- Es un software bastante sencillo que solo necesita estar ejecutándose sobre los hosts sin necesidad de NHRP o RSVP.
- Se pueden evitar los cuellos de botella de los routers estableciendo conexiones directas punto a punto.
- No es sólo una propuesta teórica, ya existen aplicaciones que la utilizan.
- Coexiste con la pila normal de IP sobre ATM permitiendo que aplicaciones normales y mejoradas por Arequipa corran simultáneamente.

La mayor desventaja es el factor de que las aplicaciones actuales IP deben ser modificadas para aprovechar al máximo sus funcionalidades. Aunque estos cambios resulten mínimos. Además no deja de ser una propuesta privada, con pocas posibilidades de convertirse en un estándar.

1.4.6 IP swiching

IP switching se describe como una manera óptima y escalable de soportar IP sobre ATM. Emplea las partes fuertes tanto de IP como de ATM para aumentar el rendimiento de Internet:

- El hardware ATM aporta alta velocidad a un precio aceptable.

- El routing IP es mucho más sencillo que el los protocolos de direccionamiento, routing y signalling para ATM (UNI, PNNI).

Los flujos de datos duraderos, por ejemplo la transferencia de ficheros, se comportan de manera óptima en ATM, ya que una vez establecido el Circuito Virtual, no es necesario volver a analizar los datagramas IP para realizar routing. Por el contrario, las conexiones cortas se comportan de manera más eficiente empleando el routing de IP, sin tener que esperar a establecer conexiones fijas ATM.

La QoS punto a punto puede en un principio llevarse a cabo en una red totalmente equipada con IP switching. Sin embargo, esta QoS se expresa en términos de prioridad para un flujo de datos, y no en los términos comunes de ATM. Además, no es la aplicación en sí, sino la red, la que inicia el establecimiento de la sesión, haciendo imposible a las aplicaciones establecer sus necesidades de QoS.

1.4.7 Tag swching

Tag Switching, creada por Cisco Systems es una manera potente de integrar la conmutación de celdas con el direccionamiento y el routing simple de tecnologías de conmutación de datagramas. Mejora el rendimiento del reenvío con una buena relación coste/rendimiento. Asociando un rango amplio de granularidad de envío con una tag (etiqueta), se puede soportar una gran variedad de funciones de routing (routing basado en el destino, multicast, basarse en la QoS, o jerarquías).

Se diferencia de IP Switching en que las etiquetas nunca se asocian basándose en el análisis del flujo de datos, sino en la topología de la red. Debido a que esta topología es bastante estática, se adquieren mejoras en el rendimiento respecto a IP switching. Otra diferencia es que Tag Switching es una tecnología multiprotocolo.

Si se emplea Tag Switching con IP y ATM, se puede sustituir todo el plano de control de ATM (UNI, PNNI) por la componente de control de IP Switching, que es mucho más sencilla de implementar.

Una desventaja de Tag Switching al utilizarlo con ATM es que los conmutadores ATM que lo emplean deben participar como pares en el protocolo IP y necesitarán soportar envío de la capa de red. Si se emplea junto con un protocolo de reserva, como RSVP, es posible dar conexiones tipo Circuito Virtual con garantías de QoS extremo a extremo para flujos IP.

Tag switching es principalmente una tecnología de backbones, que se adapta bien al enrutado del tráfico en Internet de los proveedores de servicio a través de una tecnología ATM.

Los temas de seguridad y facturación no se han tenido en cuenta, dejando a los protocolos que corran por encima estas tareas.

1.4.8 MPLS

El beneficio más importante de MPLS es que aporta una base que permite a los proveedores de Internet (ISPs) llevar nuevos servicios que no pueden ser tan fácilmente soportados por el routing IP.

Con MPLS es factible controlar el coste, dar mejores niveles de servicios, asignar rutas, y QoS.
Otras ventajas:

- Simplifica el paradigma de envío. Aumentando las prestaciones precio/ rendimiento y el tiempo de vida en el mercado.
- Permite a los switches ATM ser reutilizados como routers.
- El envío es independiente de :
    - La capa de red.
    - Capas inferiores: ATM, Frame Relay, ethernet, Sonet, etc.
    - Los criterios empleados para asociar paquetes en clases de equivalencia (FEC). Además, los cambios en estos criterios son transparentes, aportando robustez en los posibles cambios en las decisiones futuras.
- El criterio de envío no está basado exclusivamente en la cabecera del paquete (por ejemplo, podría estar basado en el puerto de entrada, asociando cada puerto con un FEC). Estos criterios pueden llegar a ser tan complejos como se desee, sin que tengan ningún efecto negativo en los LSRs internos de la red.
- El etiquetado es un mecanismo más eficiente que el encapsulado para emplear túneles.
- El envío MPLS puede emplear switches que no puedan analizar las cabeceras de la capa de red, basta con que puedan sustituir las etiquetas de los paquetes.
- Un paquete que entre en la red por un router concreto puede ser etiquetada de manera distinta que en el caso de haber entrado por otro router, como resultado, las decisiones den envío que dependen del router de entrada pueden realizarse fácilmente.

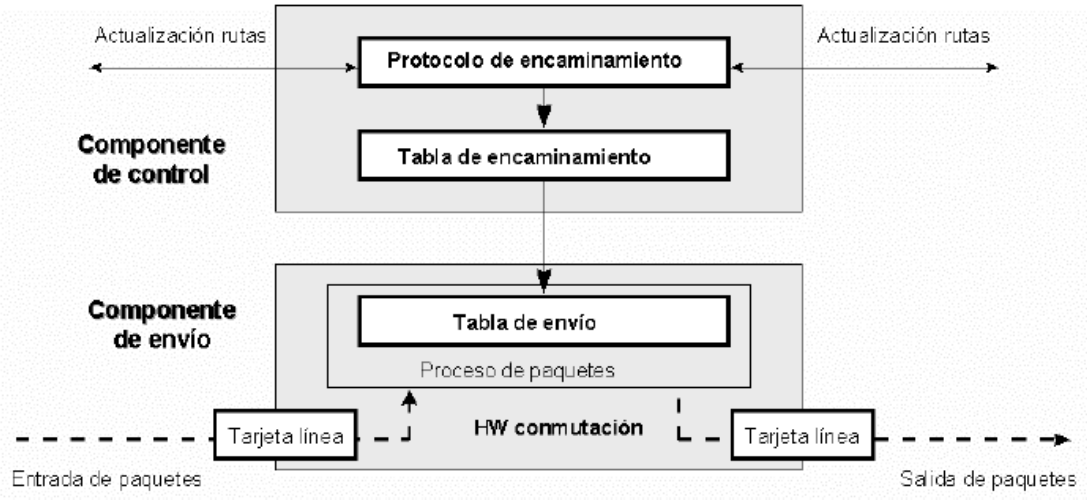
2 MPLS (Multi Protocol Label Switching)

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señalas anteriormente. Esas técnicas se conocieron como "conmutación IP" (*IP switching*) o "conmutación multinivel" (*multilayer switching*). Una serie de tecnologías privadas —entre las que merecen citarse: *IP Switching* de Ipsilon Networks, *Tag Switching* de Cisco, *Aggregate Route-Base IP Switching (ARIS*) de IBM, *IP Navigator* de Cascade/Ascend/Lucent y *Cell Switching 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). Se resume a continuación 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.

Figura 10 Separación funcional de encaminamiento y envío.



En la figura 10 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 *routers* 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 la interfaz de entrada al de salida a través del correspondiente hardware de conmutación.

Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ella 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 la interfaz física 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" (*Forwarding Equivalence Class*, FEC). 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.

2.1 Introducción a MPLS

Ya se dijo anteriormente que el problema principal que presentaban las diversas soluciones de conmutación multinivel era la falta de interoperatividad entre productos privados de diferentes fabricantes. Además de ello, la mayoría de esas soluciones

necesitaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas (Frame Relay, PPP, SONET/SDH y LANs). Se quería obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace. De aquí que el Grupo de Trabajo de MPLS que se estableció en el IETF en 1977 se propuso como objetivo la adopción de un estándar unificado e interoperativo.

En sí MPLS, trata de emplear los switches como Routers de Label Switching o Routers de conmutación de etiquetas. Los switches ATM ejecutan algoritmos de routing de la capa de red, y el envío de sus datos se basa en los resultados de esos algoritmos de routing. No se necesita direccionamiento ni routing específico para ATM. Los switches ATM que se emplean de esta manera son conocidos como ATM-LSRs.

Los puntos principales de MPLS son:

- Etiqueta: clasificación de paquetes que se enviarán por el mismo camino.
- Las etiquetas se asocian en la entrada de la red MPLS.
- El envío de paquetes se basa en la etiqueta.
- El criterio empleado para clasificar los paquetes en etiquetas se puede basar en una decisión local, al entrar en la red MPLS o en base a decisiones preestablecidas.
- Las etiquetas asignadas deben comunicarse a todos los nodos a lo largo del camino de la clase de paquetes asociados con la etiqueta.
- Las etiquetas puede apilarse: un paquete puede tener varias etiquetas.
- Las etiquetas se eliminan en la salida de la red MPLS.
- LSR : router - conmutador que soporta MPLS.

2.1.1 Objetivos de MPLS

El propósito del grupo de trabajo de MPLS es estandarizar una tecnología que sirva de base y que combine el empleo de la conmutación de paquetes con el routing .Para ello, se necesita integrar este módulo en la componente de control (que utiliza routing) en la capa de red. Para llevarlo a cabo, se desarrolló esta propuesta, con el propósito de satisfacer los siguientes requerimientos:

- MPLS podrá ejecutarse sobre cualquier tecnología en la capa de red, como puede ser, ATM.
- Deberá soportar flujos de tráfico tanto unicast como multicast.
- Deberá ser compatible con el modelo de Servicios Integrados de la IETF, incluyendo RSVP.
- Deberá ser escalable, para soportar el crecimiento constante de las estructuras corporativas, y, más globalmente, la expansión de Internet.
- Deberá admitir herramientas de soporte, administración y mantenimiento al menos tan flexibles como las que soportan las redes actuales IP4.

2.1.2 Conceptos erróneos sobre MPLS

Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas falsas o inexactas sobre el alcance y objetivos de MPLS. Hay quien piensa que MPLS se ha desarrollado para ofrecer un estándar a los vendedores que les permitiese evolucionar los conmutadores ATM a *routers* de *backbone* de altas prestaciones.

Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel, los recientes avances en tecnologías de silicio ASIC permiten a los *routers* funcionar con una rapidez similar para la consulta de tablas a las de los conmutadores

ATM. Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de envío de paquetes, éste no era el principal objetivo del grupo del IETF.
También ha habido quien pensó que el MPLS perseguía eliminar totalmente el encaminamiento convencional IP por prefijos de red. Esta es otra idea falsa y nunca se planteó como objetivo del grupo, ya que el encaminamiento tradicional de nivel 3 siempre sería un requisito en la Internet por los siguientes motivos:

- El filtrado de paquetes en los cortafuegos (FW) de acceso a las LAN corporativas y en los límites de las redes de los NSPs es un requisito fundamental para poder gestionar la red y los servicios con las necesarias garantías de seguridad. Para ello se requiere examinar la información de la cabecera de los paquetes, lo que impide prescindir del uso del nivel 3 en ese tipo de aplicaciones.

- No es probable que los sistemas finales (*hosts*) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (nivel 3) que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En este primer salto se puede decidir enviarlo por *routing* convencional o asignar una etiqueta y enviarlo por un LSP.

- Las etiquetas MPLS tienen solamente significado local (es imposible mantener vínculos globales entre etiquetas y *hosts* en toda la Internet). Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: por *routing* convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.

2.2 Arquitectura de MPLS

2.2.1 Visión General

Cada router analiza la cabecera del paquete y ejecuta un algoritmo de routing, basándose en la información de esta cabecera. Las cabeceras de los paquetes contienen mucha más información que la necesaria para elegir el siguiente salto. Elegir el siguiente salto puede ser visto como la composición de dos funciones:

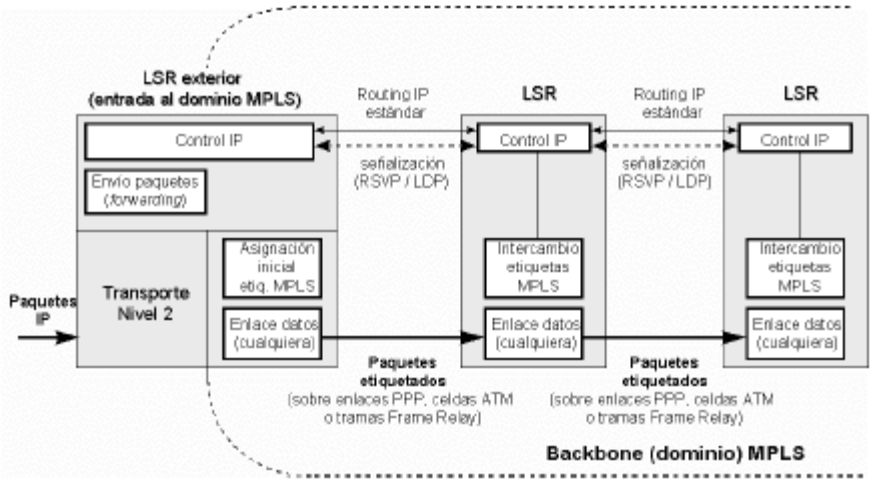
- Particionar el conjunto de posibles paquetes en clases de envío equivalentes (FECs).
- Asociar cada uno de estos FECs con algún destino.

En lo que respecta a la decisión de reenvío, diferentes paquetes clasificados dentro de un mismo FEC son considerados idénticos. Todos los paquetes pertenecientes a un mismo FEC seguirán el mismo camino.
En el envío IP, un router considerará a dos paquetes dentro del mismo FEC si hay algún prefijo de dirección X en la tabla de routing del router el cuál sea la mayor concordancia para la dirección de destino de los paquetes. A medida que el paquete sigue circulando por la red, cada router realiza la misma operación de asignación en un FEC.

En MPLS, esta asignación se efectúa solamente cuando el paquete entra en la red, como se observa en la figura 11. Tras esto, el FEC al que el paquete ha sido asignado se codifica en un valor llamado Etiqueta. Cuando un paquete va a ser enviado al siguiente nodo, se le añade la etiqueta.

En el resto de los nodos del camino, no se necesitará realizar análisis de la cabecera del paquete. La etiqueta que acompaña al paquete servirá para encontrar el siguiente salto y una nueva etiqueta, procediendo así a repetir el proceso de envío.

Figura 11 Esquema funcional del MPLS.



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

Funcionamiento del envío de paquetes en MPLS

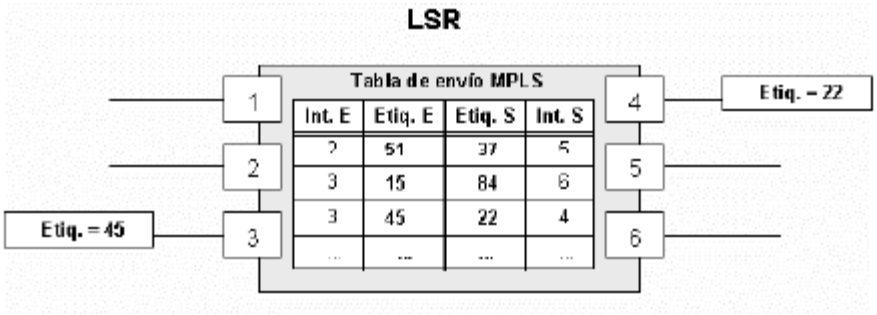
La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); para el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (*hops*) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (*Label-Swiching Router)* a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.

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 implementa mediante el *intercambio de etiquetas* en los LSPs. Sin

embargo, 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 (el *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 encaminamiento 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. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según 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 figura 12 se ilustra un ejemplo del funcionamiento de un LRS del núcleo MPLS. A un paquete que llega al LSR por la interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

Figura 12 Detalle de la tabla de envío de un LSR.

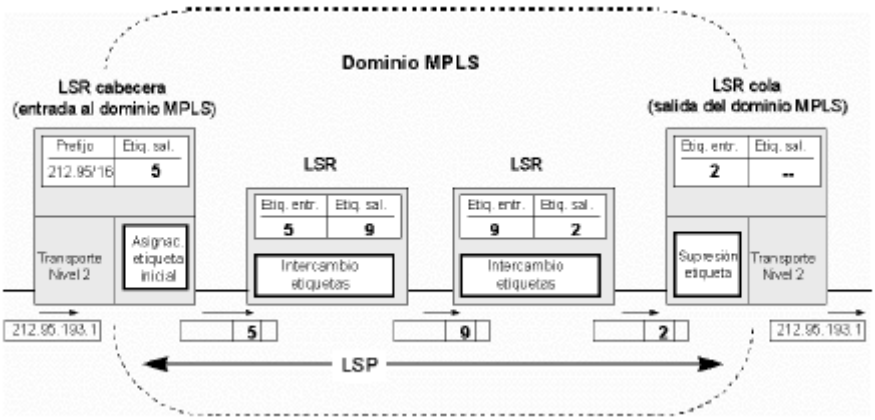


El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera.
En la figura 13 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta 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 por *routing* convencional.

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativo para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada

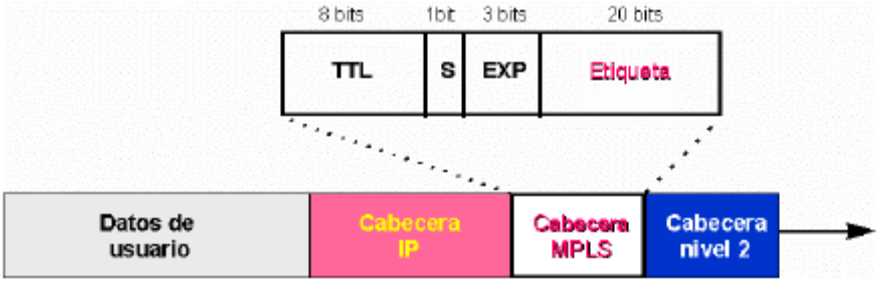
no soporta un campo para etiquetas p. ej. enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

Figura 13 Ejemplo de envío de un paquete por un LSP.



En la figura 14 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS), 1 bit de *stack* para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (*time-to-live*) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

Figura 14 Estructura de la cabecera genérica MPLS.



Control de la información en MPLS

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

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

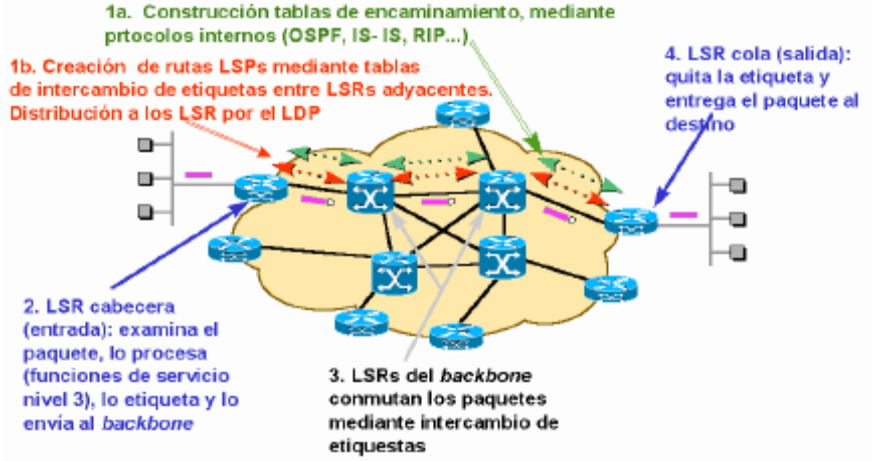
El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de *routing* para establecer los caminos virtuales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

El segundo aspecto se refiere a la información de "señalización", pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF (recuérdese que ése era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del *Label Distribution Protocol* (LDP).

Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura 15, 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 *routers* IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de *routers* a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs 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 *routers*). 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.

Figura 15 Funcionamiento de una red MPLS .



2.2.2 Encapsulamiento

Los procedimientos descritos en esta sección sólo afectan a los LSRs frontera del domino LSR-ATM. Los LSRs-ATM no modifican por sí mismos el encapsulado de ninguna manera.

La etiqueta MPLS es el principal mecanismo para reenviar los paquetes en una red MPLS. Las etiquetas usadas en la red MPLS pueden ser incluidas de dos maneras diferentes:

- *Agregando la cabecera genérica de MPLS*: si la tecnología de nivel 2 empleada no soporta un campo para etiquetas p. ej. enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 (de la figura 14) que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3)..

- *Usando la encapsulación nativa de capa 2*: Usada con tecnologías de transporte en capa 2, tales como ATM y Frame Relay, que ya contienen un campo para

etiquetas (los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativos para las etiquetas.

En lo que a nos concierne, concretaremos la atención en la codificación MPLS-ATM, que consiste en combinar los campos VPI - VCI de las células ATM para transportar las etiquetas y tratar los switches ATM como LSRs.

ATM - LSRs: Los procedimientos de envío de MPLS son similares a los switches ATM. Estos emplean el puerto de entrada y el VPI-VCI entrante como índice en una tabla, obteniendo un puerto de salida y un valor VPI-VCI de salida. De modo que si una o más etiquetas pueden codificarse directamente en los campos a los que estos switches acceden, podremos hacer que los switches ATM se comporten como LSRs.

Posibles codificaciones de etiquetas sobre las células ATM:

- *Codificación SVC*: se emplea el campo VPI/VCI para codificar la etiqueta de la cima de la pila. Esta técnica se puede emplear en cualquier red. Cada camino LSP se trata como un SVC ATM, y el protocolo de distribución de etiquetas será el protocolo de señalización ATM. Los LSRs ATM no pueden extraer ni poner etiquetas en la cima de la pila.

- *Codificación SVP*: se emplea el campo VPI para codificar la etiqueta de la cima de la pila, y el VCI para codificar la segunda etiqueta de la pila, si existe. Esta técnica confiere algunas ventajas sobre la anterior: permite el empleo de conmutación de VP ATM. El camino LSP se trata como un SVP ATM, y el protocolo de distribución de etiquetas será el protocolo de señalización ATM. Esta técnica no podrá ser empleada si la red incluye un VP ATM a través de una red ATM no MPLS, entonces, el campo VPI no estará libre para ser empleado por MPLS.

- *Codificación SVP Multipunto*: Se emplea el campo VPI para codificar la etiqueta de la cima de la pila, parte del campo VCI para codificar la segunda etiqueta, si existe, y el resto del campo VCI para identificar el LSP de entrada. Con esta técnica se puede emplear la conmutación de VPs ATM para tener VPs multipunto-a-punto. Células de diferentes paquetes llevarán así diferentes valores de VPI. Esto permite emplear mezcla de etiquetas, sin tener problemas de interleaving, en switches ATM que pueden dar VPs multipunto-a-punto pero que no tienen la capacidad de mezcla de VC. Esta técnica depende de la existencia de una capacidad de asignar VCIs de 16 bits a cada switch ATM de tal forma que no se asignen valores VCI iguales a dos switches diferentes.

Si se necesitan más de dos etiquetas en la pila, la codificación ATM deberá combinarse con el encapsulado genérico.

Interoperabilidad entre las técnicas de codificación:

Es posible que dentro de un LSP existan diferentes técnicas de codificación: cuando llega un paquete a un LSR, este deberá: decodificarlo para determinar el valor actual de la pila de etiquetas, entonces deberá operar sobre la pila para determinar el nuevo valor de esta y posteriormente codificar el nuevo valor de forma apropiada antes de transmitir el paquete etiquetado a su siguiente salto. Por desgracia, los switches ATM no tienen capacidad de traducir de una técnica de codificación a otra. La arquitectura MPLS requiere que en cuando sea posible para dos switches ATM consecutivos, estos empleen la misma técnica de codificación.

Con las redes MPLS que contengan una combinación de switches ATM operando como LSRs y otros LSRs que estén empleando una cabecera reflejo, estos podrán intercambiar una pila de etiquetas codificada en ATM y sustituirla con una cabecera reflejo MPLS.

2.2.3 Protocolo de Intercambio de Etiquetas LDP

La arquitectura MPLS define un protocolo de distribución de etiquetas como un conjunto de procedimientos mediante los cuales un LSR comunica a otro LSR asignaciones de etiquetas, utilizadas para enviar tráfico entre ellos. El protocolo LDP es uno, no el único, de estos protocolos de distribución de etiquetas, ha sido creado para cumplir éste propósito. Es el conjunto de procedimientos y mensajes mediante los cuales los LSRs crean caminos de conmutación de etiquetas (LSP) a través de una red, mapeando la información de routing directamente a caminos conmutados. Estos caminos podrán acabar en vecinos conectados entre sí directamente (como si fuese IP salto a salto) o pueden acabar en un nodo de salida de cierta red, activando entonces la conmutación entre todos los nodos intermedios. Así mismo, los LDPs asocian una Clase de Envío Equivalente (FEC) con cada camino LSP que creen. Los FEC asociados con cierto camino, especifican que paquetes IP van a ir por ese camino.

Pares LDP

Dos LSRs que emplean el protocolo LDP para intercambiar información de asociación etiqueta / FEC son llamados pares LDP con respecto a esa información, manteniéndose entre ellos una sesión LDP. Una sesión LDP permite a cada par aprender la información de las etiquetas del otro. El protocolo es bidireccional.

Intercambio de mensajes LDP

Existen cuatro categorías de mensajes:

- *Mensajes de descubrimiento*: empleados para anunciar y mantener la presencia de un LSR en la red.

- *Mensajes de sesión*: empleados para establecer, mantener y finalizar las sesiones entre los pares.
- *Mensajes de anuncio*: empleados para crear, cambiar y borrar asociaciones de etiquetas con FECs.
- *Mensajes de notificación*: empleados para da información de aviso o de error.

Los mensajes de descubrimiento anuncian la presencia de un LSR en la red, estos se realizan enviando el mensaje Hello periódicamente. Éste es transmitido como un paquete UDP por el puerto LDP en la dirección multicast del grupo todos los Routers de esta Subred. Cuando un LSR desea establecer una sesión con otro LSR, aprendido gracias al mensaje Hello, empleará el procedimiento de inicialización LDP sobre TCP. Si se lleva a cabo de forma correcta el procedimiento de inicialización LDP, los dos LSRs son ya pares LDP, y pueden intercambiar mensajes de anuncio.
Cuándo pedir cierta etiqueta, o anunciarla a un par, será una decisión local a cada LSR. En general, el LSR pide una etiqueta a su vecino cuando la necesita y la anuncia cuando desea que el vecino la comience a utilizar.

El funcionamiento correcto del protocolo LDP requiere una recepción fiable y ordenada de mensajes. Para ello, se emplea el protocolo TCP para mensajes de sesión, de anuncio y de notificación. Es decir, para todo el proceso, excepto para los mensajes de descubrimiento, que viajan sobre UDP.

Estructura del mensaje LDP

Todos los mensajes LDP tienen una estructura común que emplea una metodología de codificación Tipo - Longitud - Valor. La parte Valor de un objeto TLV puede a su vez contener uno o más TLVs.

Modos de Operación

Sesiones LDP entre LSRs no conectados directamente

Para llevar a cabo sesiones LDP entre LSRs que no están conectados directamente en el nivel de enlace se deberían dar ciertas características. Por ejemplo, consideremos una aplicación en la que LSRa envía tráfico que cumple cierto criterio por un camino a un LSRb no conectado directamente a él. El camino entre LSRa y LSRb incluiría uno o más LSRs intermedios (LSR1, ... , LSRn). Se crearía una sesión LDP entre LSRa y LSRb, que permitiría a LSRb conmutar el tráfico etiquetado procedente del camino con LSRa, permitiendo a LSRb emplear métodos para anunciar a LSRa etiquetas para este propósito.
En esta situación, LSRa aplicaría dos etiquetas para mandar los datos a LSRb:

- Una etiqueta aprendida de LSR1 para enviar tráfico por el camino desde LSRa a LSRb.
- Una etiqueta aprendida de LSRb para permitir a LSRb conmutar el tráfico etiquetado que llegue por el camino.

LSRa primero añade la etiqueta aprendida en su sesión LDP con LSRb a la pila de etiquetas del paquete y luego añadirá a esta la etiqueta aprendida de LSR1 para entrar en este camino.

Descubrimiento LDP

El descubrimiento es un mecanismo mediante el cual un LSR descubre los posibles pares. Gracias al descubrimiento, no es necesario configurar de manera explícita los pares LDP.

Mecanismo de descubrimiento básico:

Un LSR envía de forma periódica Hellos de enlace. Éstos, se envían como paquetes UDP dirigidos al puerto LDP de descubrimiento, con la dirección multicast del grupo todos los Routers de la subred. Un mensaje Hello lleva el identificador LDP para el espacio de etiquetas que el LSR trata de usar, y alguna otra posible información adicional. La recepción de un mensaje Hello identifica una adyacencia con un posible par LDP accesible a nivel de enlace así como el posible espacio de etiquetas que el par trata de emplear.

Mecanismo de descubrimiento extendido:

Se emplea para realizar sesiones LDP entre LSRs que no están conectados directamente. Para ello, un LSR envía Hellos direccionados a una dirección IP específica. Éstos son enviados como paquetes UDP direccionados al puerto de la dirección específica. Un Hello Direccionado enviado por un LSR lleva el identificador LDP para el espacio de etiquetas que el LSR trata de usar, y alguna otra posible información adicional.
Igualmente, la recepción de un mensaje Hello identifica una adyacencia con un posible par LDP accesible a nivel de enlace así como el posible espacio de etiquetas que el par trata de emplear.

Establecimiento y Mantenimiento de Sesiones LDP

El establecimiento de una sesión sigue dos pasos:

- Establecimiento de la conexión de transporte.
- Inicialización de la sesión.

A continuación se describe el establecimiento de una sesión LPD entre LSR1 y LSR2 desde el punto de vista de LSR1. Se asume el intercambio de Hellos especificando el espacio de etiquetas LSR1:a para LSR1 y LSR2 :b para LSR2.

Establecimiento de la conexión de transporte

Si LSR1 no posee una sesión LDP para el intercambio de los espacios de etiquetas LSR1:a y LSR2:b intentará abrir una conexión TCP para tener una nueva sesión LDP con LSR2.

- LSR1 determina las direcciones de transporte a emplear por el mismo (dirección A1) y por LSR2 (dirección A2).
- La dirección A1 se determinará de la siguiente forma:
    - Si LSR1 emplea TLV en los Hellos que envía a LSR2 para anunciar una dirección, A1 será la dirección que LSR1 anuncia en estos Hellos.
    - Si LSR1 no emplea TLV, A1 será la dirección IP de origen empleada en los Hellos.
    - De igual forma, la dirección A2 se determinará de manera análoga empleando los Hellos de LSR2.

LSR1 determina si jugará el rol activo o pasivo en el establecimiento de sesión comparando el valor entero sin signo de las direcciones A1 y A2. Si A1 > A2, LSR1 tendrá el papel activo, en otro caso, será el papel pasivo. Si LSR1 es activo, intentará establecer la conexión TCP LDP conectando con el puerto configurado LDP en la dirección A2. Si LSR1 es pasivo, esperará a que LSR2 establezca la conexión TCP con su puerto LDP.

Inicialización de Sesión

Tras haber establecido la conexión de Transporte, los pares negocian los parámetros de sesión intercambiando mensajes de inicialización LDP. Los parámetros negociados incluyen: versión del protocolo LDP, método de distribución de etiquetas, valores de los temporizadores, rangos VPI / VCI para ATM, ó rangos DLCI si se trata de Frame Relay la capa de enlace, etc. Si la negociación ha tenido éxito, se establece la sesión entre los dos pares. A continuación se describen los pasos que se dan en la inicialización de una sesión. Si LSR1 es el par activo, inicia la negociación de los parámetros de sesión enviando un mensaje de inicialización a LSR2. Si es el par pasivo, esperará a que LSR2 inicie la negociación.

Mantenimiento de Sesiones LDP

LDP emplea la recepción regular de PDUs LDP en la conexión de transporte de la sesión para monitorizar la integridad de la sesión. Un LSR mantiene un temporizador KeepAlive (sigo vivo) para cada par, si este temporizador expira sin haber recibido una PDU LDP del par, el LSR deduce que la conexión TCP está mal, o que el par ha fallado, y termina esta sesión cerrando la conexión TCP.

Manejo y Distribución de Etiquetas

La arquitectura MPLS permite a un LSR distribuir un enlace con un FEC respondiendo a una petición que le haga otro LSR. A esta acción se la denomina Distribución de Etiquetas Downstream Bajo Demanda. También permite a un LSR distribuir sus enlaces con los FEC a LSRs que no se lo han solicitado. A esta acción se la denomina Distribución de Etiquetas Downstream sin Solicitar.

Ambas técnicas se pueden emplear en la misma red al mismo tiempo. Sin embargo, para cada sesión LDP los pares deberán saber que método de distribución de etiquetas emplean.

Asignación y Distribución de Etiquetas

En la arquitectura MPLS, la decisión de enlazar cierta etiqueta L con un FEC F la realiza el LSR que es DOWNSTREAM con respecto a ese enlace. Así, el LSR downstream informa al LSR upstream del enlace. Estas etiquetas son asignadas de forma downstream y los enlaces de etiquetas se distribuyen en la dirección downstream hacia upstream. Si un LSR ha sido diseñado de tal manera que sólo pueda buscar etiquetas que se encuentren en cierto rango numérico, entonces necesitará asegurar que solo enlaza etiquetas que se encuentren dentro de ese rango.

3 APLICACIONES 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).

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

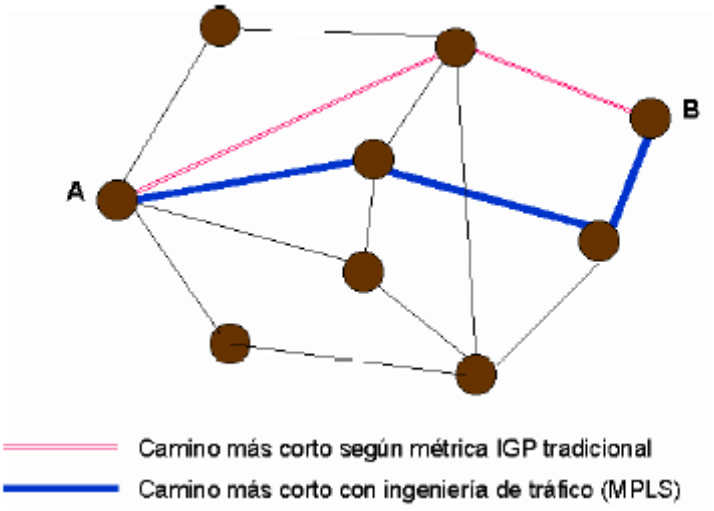
3.1 Ingeniería de Tráfico

3.1.1 Conceptos y descripciones

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

aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura 16 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

Figura 16 Comparación entre camino más corto IGP con Ingeniería de tráfico.



El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes hagan aconsejable la utilización del camino alternativo indicado con un salto más.

3.1.2 Ventajas

MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

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

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

3.2 Clases de Servicio (CoS)

3.2.1 Conceptos y descripciones

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DifServ 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, DifServ 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 DifServ 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.

3.2.2 Ventajas

Como se vio en el apartado anterior 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. P. ej., un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-efort, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

3.3 Redes Virtuales Privadas (VPNs)

3.3.1 Conceptos y descripciones

Una red privada virtual (VPN) se construye basado en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la

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

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

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPNs sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones.

Los túneles IP en conexiones dedicadas (no se va a tratar aquí de las conexiones conmutadas de acceso) se pueden establecer de dos maneras:

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

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

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

3.3.2 Ventajas

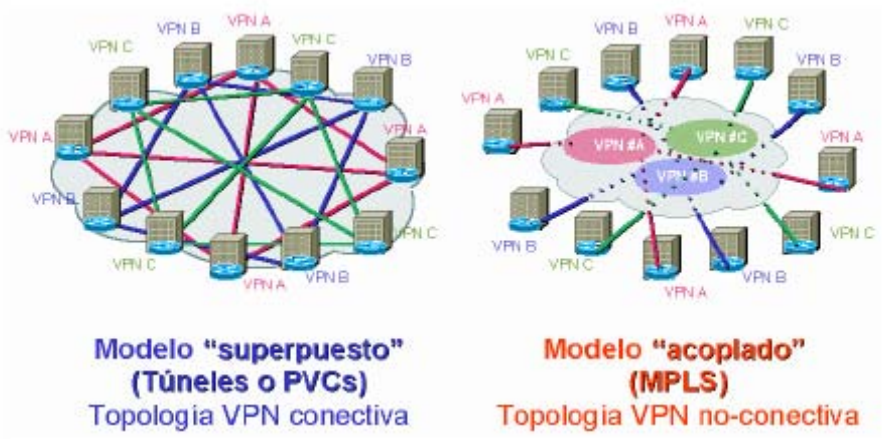
A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

- 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, basados en túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo.

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

Figura 17 Modelo "superpuesto"
(túneles/PVCs) vs. modelo "acoplado" (MPLS).



En la figura 17 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, basados en LSPs, y no de extremo a extremo a través de la red.

Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

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

4 ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN *IP/ATM* A *MPLS*

4.1 Las redes de transporte de hoy

En esta parte del capitulo hacemos una breve presentación de las distintas tecnologías de transporte utilizadas para llevar datos de un punto a otro. Es muy difícil hacer comparaciones porque son totalmente distintas, vamos a mencionar las ventaja y desventajas de cada una.

4.1.1 Redes IP/ATM

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

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y *routing*) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la

conmutación de celdas. La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del *backbone*; el papel de los routers IP queda relegado a la periferia. Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

4.1.2 Redes SDH

La Jerarquía digital síncrona (SDH) (**S**ynchronous **D**igital **H**ierarchy), se puede considerar como la evolución de los sistemas de transmisión, como consecuencia de la utilización de la fibra óptica como medio de transmisión, así como de la necesidad de sistemas más flexibles y que soporten anchos de banda elevados. La jerarquía SDH se desarrolló en EEUU bajo el nombre de SONET y posteriormente el CCITT en 1989 publicó una serie de recomendaciones donde quedaba definida con el nombre de SDH. Uno de los objetivos de esta jerarquía estaba en el proceso de adaptación del sistema PDH (**P**lesiochronous **D**igital **H**ierarchy), ya que el nuevo sistema jerárquico se implantaría paulatinamente y debía convivir con la jerarquía plesiócrona instalada. Esta es la razón por la que la ITU-T normalizó el proceso de transportar las antiguas tramas en la nueva. La trama básica de SDH es el STM-1 (Synchronous Transport Module level 1), con una velocidad de 155 Mbps. Cada trama va encapsulada en un tipo especial de estructura denominado contenedor. Una vez se ha encapsulado se añaden cabeceras de control que identifican el contenido de la estructura y el conjunto, después de un proceso de multiplexación, se integra dentro de la estructura STM-1. Los niveles superiores se forman a partir de multiplexar a nivel de Byte varias estructuras STM-1, dando lugar a los niveles STM-4,STM-16 y STM-64.

Ventajas y desventajas de SDH

La SDH presenta una serie de ventajas respecto a la jerarquía digital plesiocrona (PDH).

Algunas de estas ventajas son:

- El proceso de multiplexación es mucho más directo. La utilización de punteros permite una localización sencilla y rápida de las señales tributarias de la información.
- El procesamiento de la señal se lleva a cabo a nivel de STM-1. Las señales de velocidades superiores son síncronas entre sí y están en fase por ser generadas localmente por cada nodo de la red.
- Las tramas tributarias de las señales de línea pueden ser subdivididas para acomodar cargas plesiócronas, tráfico ATM o unidades de menor orden. Esto supone mezclar tráfico de distinto tipo dando lugar a redes flexibles.
- Compatibilidad eléctrica y óptica entre los equipos de los distintos suministradores gracias a los estándares internacionales sobre interfaces eléctricos y ópticos.

En cuanto a las desventajas tenemos que:

- Algunas redes PDH actuales presentan ya cierta flexibilidad y no son compatibles con SDH.
- Necesidad de sincronismo entre los nodos de la red SDH, se requiere que todos los servicios trabajen bajo una misma referencia de temporización.
- El principio de compatibilidad ha estado por encima de la optimización de ancho de banda. El número de Bytes destinados a la cabecera de sección es muy grande, lo que nos lleva a perder eficiencia.

4.1.3 Redes Frame Relay

Frame Relay es un servicio de transmisión de datos en modo paquete basado en una tecnología digital que permite ofrecer soluciones a servicios que demandan gran ancho de banda. Frame Relay proviene de la evolución de las redes X.25 y de los circuitos punto a punto. Constituye un soporte muy adecuado para comunicaciones de empresa u organizaciones, especialmente para aquellas que requieran tráfico a ráfagas -como en la interconexión de redes locales-.

Frame Relay está basado en una tecnología de conmutación rápida de tramas con baja tasa de error en los enlaces y procesadores de alto rendimiento en los nodos. Dicha tecnología se configura a partir de cuatro aspectos principales:

- *Baja tasa de error*. Optimiza el rendimiento de la transmisión evitando retransmisiones innecesarias entre nodos. Esto es posible debido a la alta fiabilidad de las redes actuales -dotadas de fibra óptica-.

- *Posibilidad de multiplexar* la información en un mismo punto de acceso procedente de diferentes equipos, permitiendo integrar distintos sistemas y redes.

- *Compartición dinámica del ancho de banda.* Frame Relay garantiza una velocidad mínima de transmisión (CIR), que puede excederse cuando los recursos de la red lo permitan.

- *Longitud de las tramas flexible*, adaptándose según el tipo de datos a transmitir con el fin de optimizar retardos y tasas netas de transmisión.

Circuitos Virtuales

La conexión a la red se realiza mediante los llamados circuitos virtuales. Una vez establecidos dichos circuitos quedan constituidos unos canales entre los distintos puntos a interconectar. Los circuitos virtuales pueden definirse a priori (circuitos virtuales permanentes, CVP) o dinámicamente durante el establecimiento de la llamada (circuitos virtuales conmutados, CVC) y se caracterizan por una serie de parámetros que se seleccionan en el momento de la contratación:

- Velocidad de acceso
- CIR (Commited Information Rate)
- EIR (Excess Information Rate)
- Identificador de circuito (DLCI)
- Commited Burst (Bc) y Excess Burst (Be)

Aplicaciones y ventajas

El servicio Frame Relay es el soporte tecnológico de una amplia gama de aplicaciones entre las que destacan:

- Interconexión de redes de área local.
- Servicios de voz sobre Frame Relay.
- Acceso a redes ATM.
- Acceso a bases de datos y aplicaciones remotas, transferencias masivas de ficheros e imágenes de alta velocidad.
- Integración de diferentes servicios.
- Conexión a Internet.
- Aplicaciones interactivas que requieran un elevado ancho de banda y bajo retardo.

Las ventajas que supone la tecnología Frame Relay frente a otras alternativas son:

- Compartición del ancho de banda.
- Flexibilidad en el dimensionamiento de la red.
- Alta velocidad de la transmisión con bajo retardo.
- Simplificación en la gestión de la red.
- Garantía de tráfico.
- Multiplexación de información.

4.1.4 Redes Metro

Servicios Metro Ethernet son actualmente ofrecidos por una gran cantidad de operadores, algunos de estos extienden estos servicios más allá de una red metropolitana y cubren una gran área. Miles de clientes esta ya utilizando servicios Ethernet y el número esta creciendo rápidamente. Estos clientes son atraídos por los beneficios que los servicios Ethernet brindan:

- Fácil uso
- Bajo Costo
- Flexibilidad

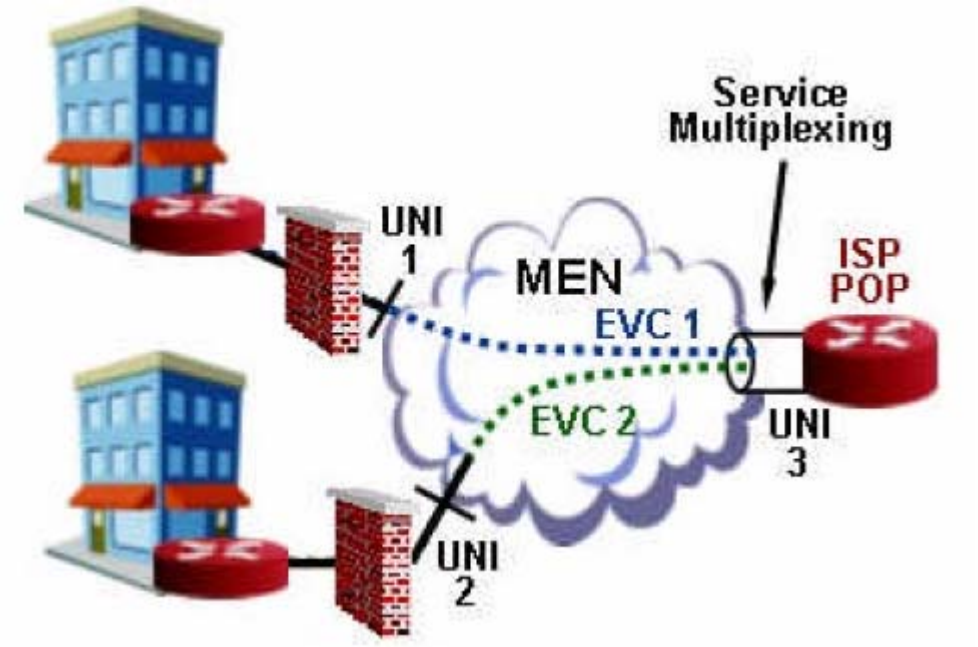
Ethernet es una tecnología fácil de entender y extremadamente efectiva en costos. Por estas razones, el 98% de las conexiones en redes de área local (LAN) se encuentran basadas en este momento en Ethernet. La combinación de flexibilidad, simplicidad y costes efectivos de Ethernet junto con la fiabilidad, velocidad y alcance de la óptica permite a los usuarios extender su entorno de red LAN a redes MAN y WAN.

Con las redes Ethernet (Metro Ethernet), los operadores pueden ofrecer en las ciudades y zonas metropolitanas servicios innovadores de banda ancha para el intercambio de voz, video y datos por medio de las actuales infraestructuras de fibra óptica. Las redes Metro Ethernet permiten transmitir datos a una velocidad de 10 Mbits/segundo desde su origen hasta el punto de conexión del usuario.

Aplicaciones

Acceso dedicado a Internet: Clientes buscan continuamente conexiones a Internet de alta velocidad que soporte el objetivo de sus negocios. Una Conexión Virtual Ethernet (Ethernet Virtual Conection EVC) puede ser el camino ideal para conectar el sitio del cliente a la red de un proveedor de Internet (ISP Internet Service Provider).
El servicio mas común para acceso a Internet es un servicio de linea Ethernet punto a punto, como se ve en la figura 18

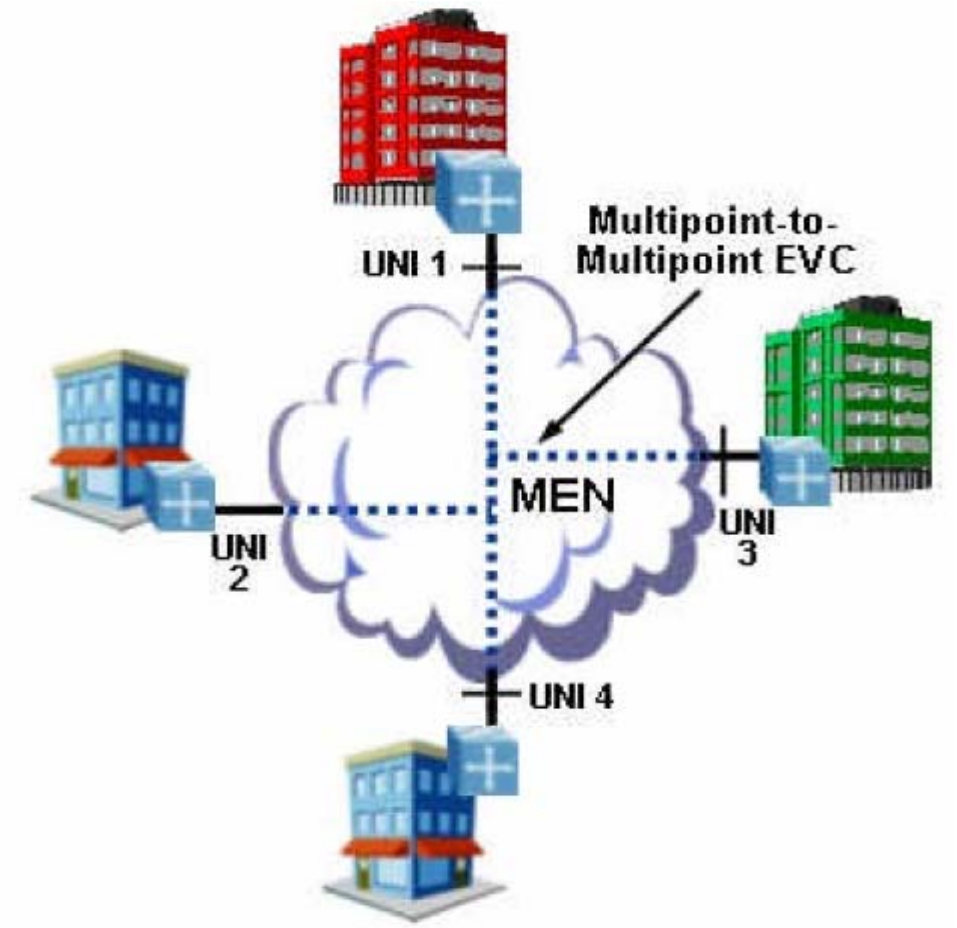
Figura 18 Servicio dedicado de Internet



En este simple escenario, se puede usar servicios de datagramas no etiquetados en el sitio del cliente. Un cliente podría utilizar BGP para tener 2 o mas provedores. En este caso el cliente podría usar líneas Ethernet separadas para cada proveedor. Si el cliente desea usar la misma UNI para tener Internet y Intranet o extranet, podría entonces usar EVCs distintos para cada servicio.

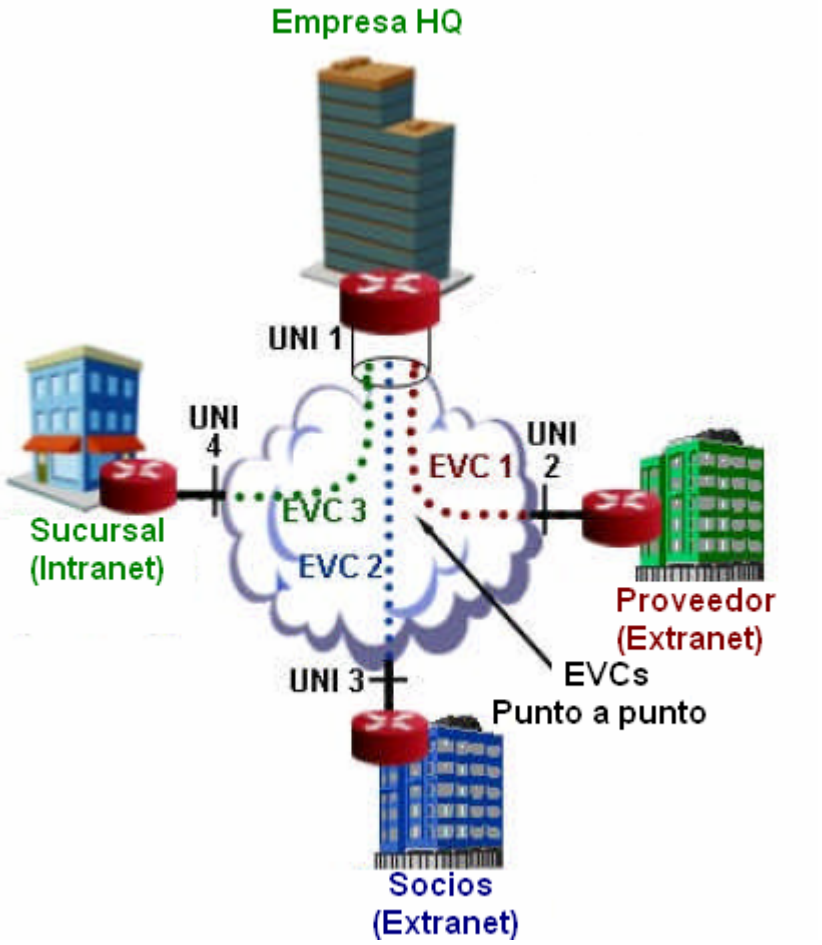
Extensión de LAN: Un cliente podría tener varios sitos dentro de un área metropolitana que desea que estén interconectados a altas velocidades, que los sitios aparezcan en la misma LAN, que tengan características equivalentes y que puedan acceder las mismas fuentes de almacenamiento o servidores de la red local a la vez sin necesidad de un ruteo intermediario entre los sitios.

Figura 19 Extensión de LAN usando E-LAN



Para conectar solamente dos sitios se puede usar una línea Ethernet punto a punto. Para conectar tres o mas sitios puede usar múltiples líneas Ethernet o un servicio Ethernet – LAN (E-LAN). Una extensión de LAN generalmente requiere mas transparencia que un acceso a Internet. Por ejemplo si la red del cliente usa VLANs (Virtual LAN) para separar tráfico, el cliente necesita que estas sean transportadas a múltiples sitios, se requiere que los equipos del cliente soporten mapear VLANs para que sean transportadas a través de la conexión de la Red Metro. La figura 19 de una extensión de LAN Interconectando cuatro sitos a través de la Red Metro.

Figura 20 Intranet / Extranet L2 VPN



Intranet / Extranet VPNs Capa 2: Los servicios Ethernet pueden ser una buena elección para llevar conexiones internas a otros sitios y conexiones externas con otras fuentes, clientes y proveedores. En la figura 20 muestra la empresa HQ conectándose a otros tres sitios. Uno de los sitios remotos es una sucursal de la empresa HQ (Intranet), mientras que los otros dos son sitios externos (Extranet) un proveedor o una empresa asociada.

Los servicios Metro Ethernet pueden soportar un rango de aplicaciones más fácilmente, eficientemente y con costos bajos que otros tipos de redes. Usando interfaces Ethernet estándar los clientes pueden tener una estructura segura y privada (EVCs) en una Red Metro, conectandose a sucursales, proveedores, socios o Internet.

4.2 Análisis técnico de la migración a MPLS

4.2.1 Visión de la nueva red de transporte MPLS.

Las grandes redes de transporte de hoy en día tienen implementadas una variedad de tecnologías para el transporte de los datos, en las que sobresalen:

- IP que es una tecnología orientada a paquetes que no tiene garantías de entrega
- ATM es una tecnología orientada a conexiones, aunque esta si soporta calidad de servicio e ingeniería de tráfico es una tecnología muy complicada.

Otras tecnologías que se podrían mencionar son las Redes Metro Ethernet, Frame Relay, SDH, entre otras.

Cada una de estas tecnologías tienen características y forma de administración distintas y esto obliga al operador a manejar redes separada para el transporte de los datos.

Unas de las metas de estos días es la convergencia de todas estas tecnologías en una sola red y que la administración se mucho mas fácil y eficiente. MPLS es una de las soluciones con más aceptación en estos días y continúa ganando terreno en el mundo de las redes de transporte.

MPLS permite a los proveedores de servicios converger en una sola infraestructura todos los servicios que actualmente prestan, además de prestar nuevos servicios y simplificar el aprovisionamiento de los mismos.
Por la forma de operación de MPLS soporta apropiadamente el rápido crecimiento de las aplicaciones y servicio en IP; además de admitir la integración de servicios emulados en una administración común.

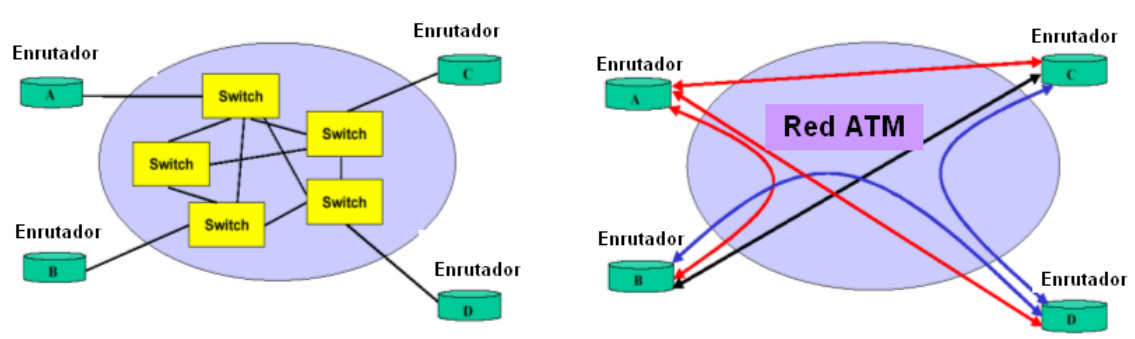
Los objetivos más importantes para proveedores de servicios y las empresas de transporte son: a) reducir costos de operación, b) mantener los servicios existentes, c) introducir nuevos y eficientes servicios. Como hemos visto MPLS es apta para desarrollar nuevos servicios y migrar los de los servicios existentes a una nueva red. Con la convergencia de servicios nuevos y existentes sobre una red MPLS pueden introducir eficiencia para reducir los costos de operación.

Como resultado de lo anterior MPLS ha tenido un significante progreso en el desarrollo de nuevas redes alrededor del mundo en los últimos años y continúa evolucionando rápidamente como una tecnología estándar para backbones.

4.2.2 Pasos para la transición a la nueva red

Mientras las tecnologías de conmutación toman presencia en el centro de la red, el enrutamiento IP continua dominando las periferias de la misma. La necesidad de conectar estas dos tecnologías ha incrementado la utilización de modelos de redes superpuestas en donde la tecnología de acceso IP se superpone sobre la tecnología de núcleo ATM o frame relay; estos modelos utilizan los recursos de red de forma ineficiente, ya que los enlaces ATM son invisibles para el enrutamiento IP. Este concepto se muestra en la figura 21.

Figura 21 IP sobre ATM



Cuando una red IP es superpuesta sobre una red de conmutación como ATM, todos los enrutadores aparecen como si estuvieran conectados entre ellos en la capa de red por lo tanto en este modelo se requiere que cada enrutador tenga una adyacencia con cada enrutador en la red. Ya que las adyacencias deben establecerse vía conexiones (ej: VCs ATM) la red ahora requiere una mezcla de VCs para interconectar los enrutadores. Mientras se incrementa el número de enrutadores, el número de VCs requerido se incrementa a una razón de

$$n(n-1)/2$$

al que generalmente se refiere como el problema n2, lo que resulta en una red con un gran número de VCs, la cual presenta problemas de escalabilidad y resulta muy difícil de administrar.

Como ejemplo, una red superpuesta con n = 4 enrutadores

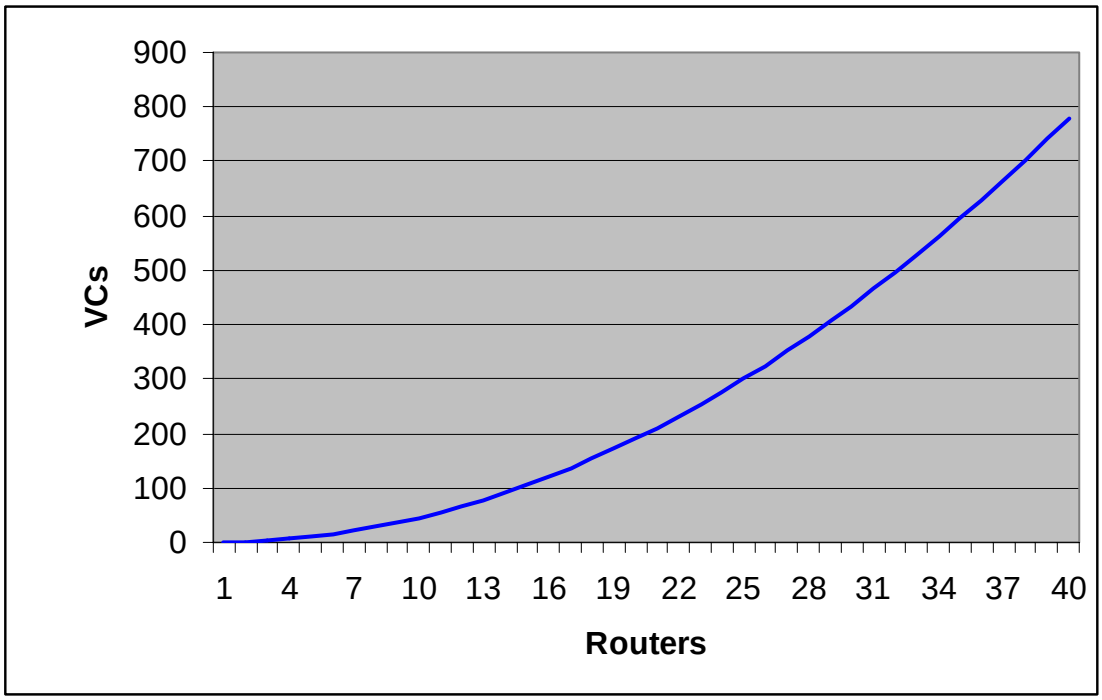
$$n(n-1)/2 = 4(4-1)/2 = 6$$

requiere seis VCs. Y cuando se agrega un quinto enrutador (n = 5)

$$n(n-1)/2 = 5(5-1)/2 = 10$$

el número de VCs se incrementa exponencialmente a 10, limitando por lo tanto, la escalabilidad de la red completa. Como se ve en la grafica siguiente se convierte en un problema cuando se tiene un número mayor a 20 enrutadores.

Figura 22 Grafica VCs frente a Routers



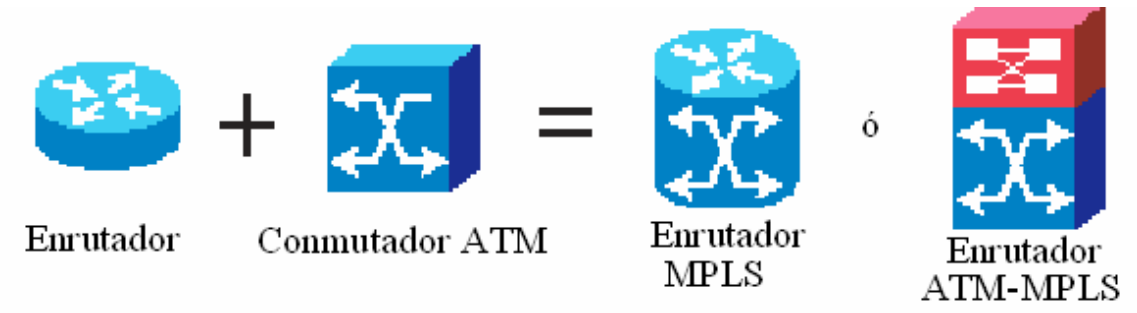
Integración de MPLS y ATM

MPLS resuelve el problema de tener que crear una nube ATM. Con MPLS los enlaces ATM son tratados como enlaces IP y cada conmutador se convierte en un par de enrutamiento IP (modelo integrado). Implementando la inteligencia IP en los

conmutadores ATM, los diseñadores pueden eliminar la superposición de enlaces IP en ATM logrando una correspondencia uno a uno entre ellos, lo cual resuelve la mayoría de los problemas de escalabilidad IP. Además la integración de las capas permite un modelo que toma ventaja de las mejores características de cada capa.

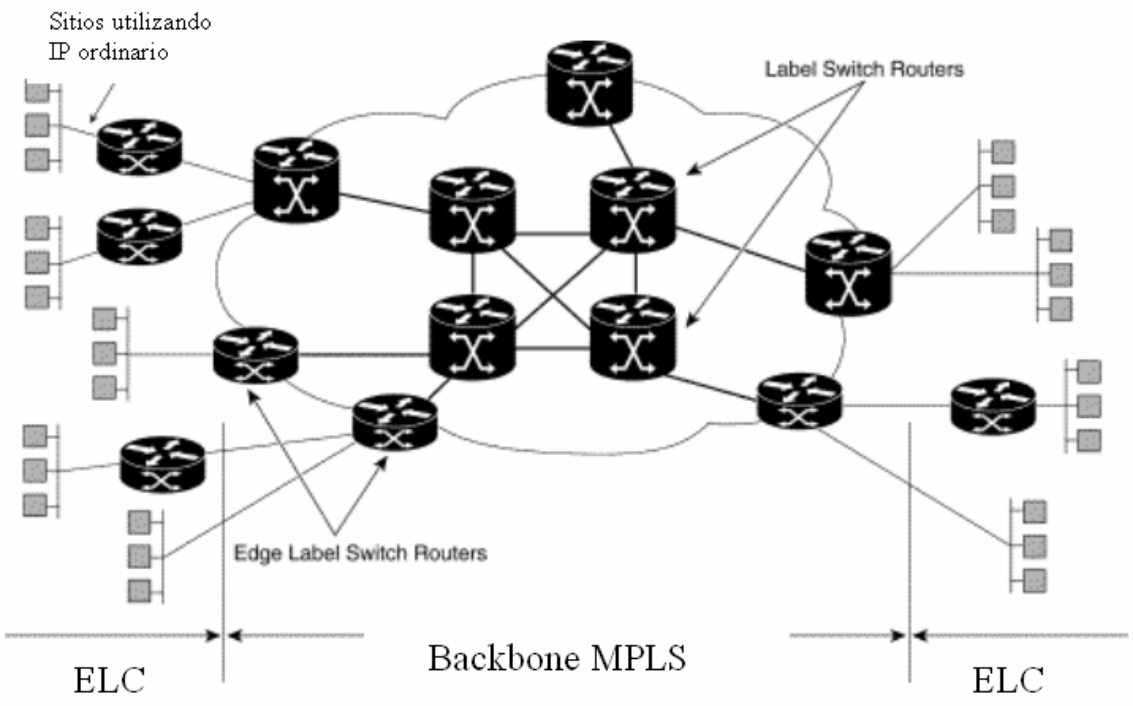
Un concepto básico de MPLS es convertir el equipo de capa 2 en la red (por ejemplo, los conmutadores ATM) en ATM-LSRs, el cual puede ser visto como una combinación de un sistema de conmutación ATM y un enrutador tradicional, compuesto por la unidad de control y la unidad de envío como se muestra en la figura siguiente:

Figura 23 Conmutadores MPLS



Una arquitectura típica para MPLS en una red de tipo “carrier- IP”, consiste en una serie de LER alrededor de un núcleo de conmutadores LSR. Los usuarios (sitios) se conectan a la red MPLS por medio de los LER. En la figura 24 se muestran 9 sitios de usuario y 6 LER, pero normalmente hay cientos de sitios por LER. El equipo local del cliente (ELC) corre IP convencional y normalmente no corre MPLS. Si el ELC corre MPLS lo hace de manera independiente del proveedor.

Figura 24 Arquitectura típica de MPLS.

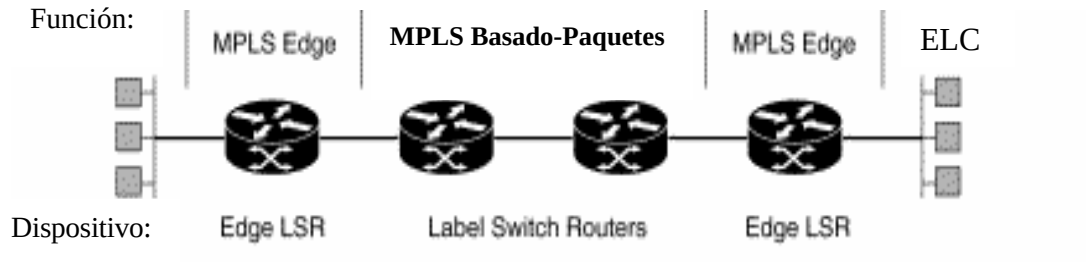


MPLS basada en paquetes

Es la topología más simple para la estructura de una red MPLS, la cual se aplica para estructuras de red con solo enrutadores, las cuales deben utilizar MPLS para soportar VPN o ingeniería de tráfico. En esta estructura los usuarios están conectados directamente a LERs basados en plataformas de enrutadores. Estos LER se conectan a otros LSR basados también en plataformas de enrutadores.

Los enrutadores se interconectan virtualmente con cualquier tipo de enlace: serial, Ethernet, paquetes-sobre -SONET, etc.

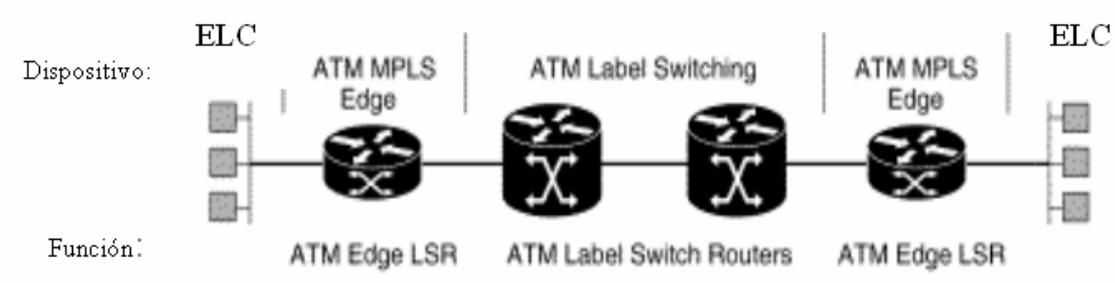
Figura 25 Arquitectura típica de una red MPLS.



ATM MPLS

La estructura de red MPLS-ATM más simple es la siguiente: los sitios se conectan directamente al LER, los cuales se conectan con el núcleo de la red con enlaces ATM. Los conmutadores ATM transportan paquetes con etiquetas ATM-MPLS (etiqueta VCI).

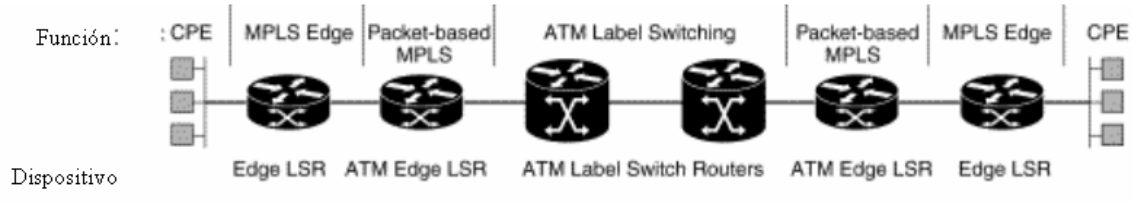
Figura 26 Arquitectura MPLS-ATM



Mezcla de ATM MPLS y MPLS de paquetes

Es posible mezclar ATM-MPLS y MPLS de paquetes en una red. Algunos enlaces corren ATM MPLS, y otros MPLS de paquetes. Los dispositivos que se conectan entre MPLS de paquetes y ATM MPLS son los mismos enrutadores que actúan como ATM-LER.

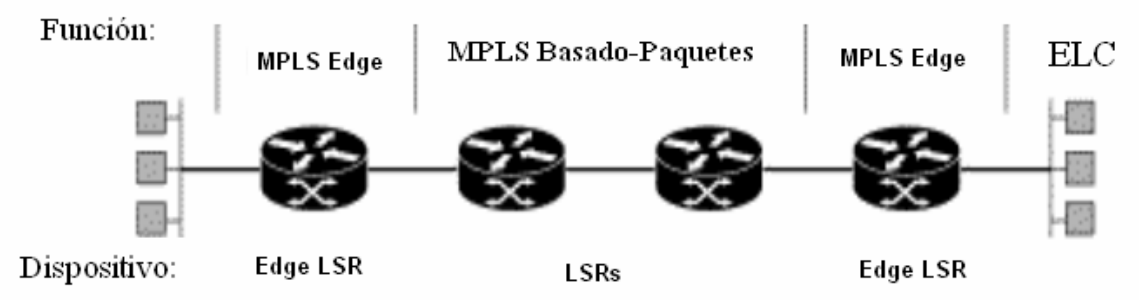
Figura 27 Mezcla de ATM MPLS y MPLS de paquetes.



ATM MPLS con dispositivos IP+ATM

En esta configuración un solo dispositivo de acceso proporciona servicios MPLS y ATM (PVC ó SVC).

Figura 28 Mezcla de ATM MPLS y MPLS de paquetes.



Como parte de la configuración inicial de la red el operador asigna recursos de la red ATM a PNNI y a MPLS (por ejemplo, ancho de banda en enlaces, espacios VPI/VCI en los enlaces, espacios de tabla de conexión de VC). Esta partición de recursos es algo flexible, con una división de recursos arbitraria entre los diferentes planos de control. Se pueden definir asignaciones fijas de recursos entre diferentes planos de control. Como la red puede utilizarse para proporcionar simultáneamente servicios MPLS y conmutación ATM tradicional, se le denomina “ship-in the-night”

Pasos Para La Migración

Si se están desarrollando servicios IP a través de una infraestructura IP/ATM, seguramente se tendrán problemas de rendimiento y escalabilidad que comenzaran a impactar la red. Para asegurar la calidad de los servicios podemos medirlos en términos de la complejidad de la red y resultados de los costos de operación así también el rendimiento que es requerido para los clientes.

Anteriormente discutimos las limitaciones de IP/ATM, como impacta la operación de una red y que MPLS ofrece una solución para estas limitaciones. Hay dos estrategias potenciales de transición que podríamos considerar:

- Transición a una red MPLS Cell-relay
- Transición a una red MPLS frame

La siguiente tabla muestra una comparación:

Tabla III comparación de las características entre IP/ATM, Cell-relay MPLS y frame MPLS

Característica	IP/ATM	MPLS en Celdas	MPLS en paquetes
Eliminación de cuellos de botella para SAR	NO	NO	YES
Administración en un solo plano de control	NO	YES*	YES
Administración de un solo equipo	NO	NO	YES
Eliminación del Encabezado ATM	NO	NO	YES
Soporte de calidad de Servicio Nativa de IP	NO	NO	YES
Eliminación del IGP Stress	NO	YES	YES

*Solo si son servicios basados en paquetes, no ATM nativo.

Al examinar esta tabla podemos observar que hay características donde MPLS en celdas tiene algunas ventajas que IP sobre ATM, pero hay también hay varios casos donde MPLS en celdas no ofrece una mejora significativa sobre redes IP/ATM. En

contraste con MPLS en paquetes es superior a IP/ATM en todos los aspectos y hay un número importante de casos donde MPLS en Celdas es inferior a MPLS en paquetes, si la meta es desarrollar servicios basados en IP, entonces es claro que MPLS en paquetes es superior a MPLS en celdas.

MPLS puede ser introducido en una red ATM gradualmente, comenzando con un solo par de ATM-LER en una red puramente ATM.

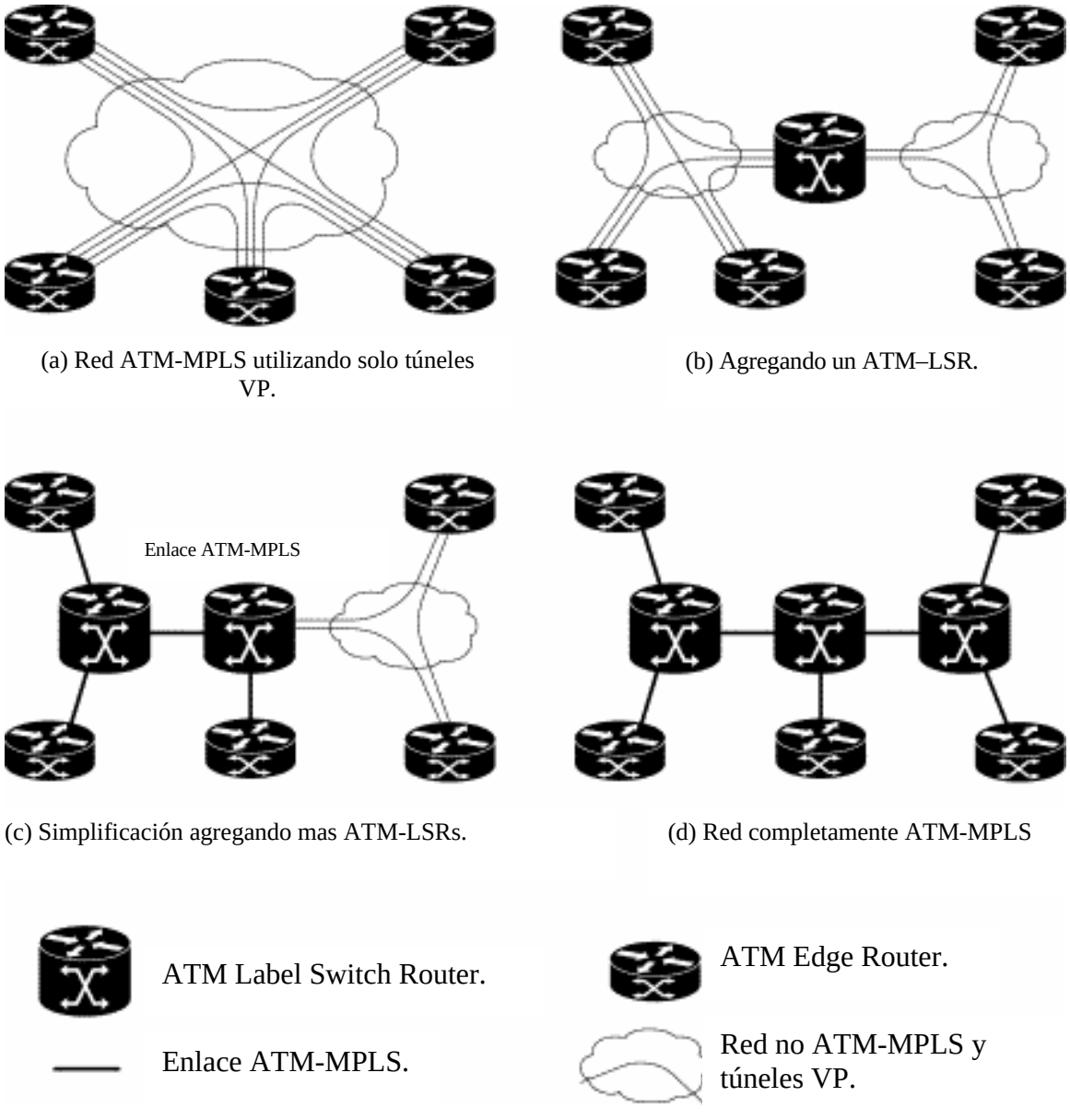
MPLS puede ser desplegado a través de conmutadores sin la capacidad de MPLS, utilizando conexiones VP a través de conmutadores ATM tradicionales; estas conexiones son llamadas túneles VP ya que permiten a MPLS “hacer un túnel” a través de conmutadores ATM tradicionales.

La figura 29 muestra una estrategia posible de migración para introducir MPLS en una red existente ATM.

La Figura 29 (a) muestra la posición inicial con enrutadores conectados a través de PVPs a través de una nube ATM, lo cual tiene la mayoría de las desventajas de las redes IP-sobre-ATM tradicionales, un muy mal escalamiento y mala eficiencia de ancho de banda, sin embargo puede proporcionar los servicios MPLS-VPN.

Desplegando algunos ATM-LSRs en la red como se muestra en la figura 29 (b) y 29 (c) mejora la escalabilidad: el número de PVCs a cada LER puede reducirse a uno (dos si hay conexión de respaldo), y en algunos casos a cero, si un LER es adyacente a un ATM-LSR. El ATM-LSR puede ser interconectado con conmutadores ATM ordinarios de varias formas. El despliegue cuidadoso de ATM-LSR y PVCs puede ser utilizado para que la malla de PVCs se asemeje lo mas posible a la topología de enlaces ATM y por lo tanto mejore la eficiencia de ancho de banda.

Figura 29 Migrando de ATM a MPLS



(a) Red ATM-MPLS utilizando solo túneles VP.

(b) Agregando un ATM–LSR.

(c) Simplificación agregando mas ATM-LSRs.

(d) Red completamente ATM-MPLS

Ya que un ATM-LSRs puede soportar servicios ATM, los conmutadores ATM ordinarios pueden ser retirados, permitiendo el despliegue completo de la red ATM-MPLS como se muestra en la figura 29 (d), la utilización de PVP ya no es requerida.

4.2.3 Nuevos servicios implementados.

MPLS es la clave que permite ofrecer los servicios de IP; implementar servicios inteligentes de extremo a extremo, de bajo costo y gran valor agregado.

VPNs (Virtual Private Networks):

VPNs Capa 2 (AToM - cualquier transporte sobre MPLS)}, VPNs Capa 3 (IP VPNs), este tipo de aplicación se configura solamente en los routers de los bordes LER y se utiliza el método de apilamiento de etiquetas (Label Snack) y se utiliza una pila de dos etiquetas, Etiqueta Interior y Etiqueta Exterior. La Etiqueta Exterior indica como llegar al router del borde del otro extremo de la red MPLS, los equipos en la nube MPLS conmutan en base a esta etiqueta. La Etiqueta Interior se saca y pone en los routers de los bordes, identifica a que VPN pertenece ese paquete, los equipos dentro de la nube MPLS no ven esta etiqueta ya que estos no tienen conocimiento de las aplicaciones configuradas en los routers de los bordes.

AToM (Cualquier transporte sobre MPLS)

Para servicios de transporte de tráfico en capa 2 punto a punto (Ethernet, PPP, HDLC, Frame Relay, ATM). Esta aplicación al igual que las VPNs solamente se configura en los routers del borde y usa también el método de apilamiento de etiquetas.

Calidad de Servicio / Clases de Servicio (QoS / CoS)

Múltiples Clases de servicio para implementar distintas políticas de comportamiento en el backbone.

Ingeniería de Tráfico (Traffic Engineering TE)

Provee un incremento en la utilización del Ancho de Banda de la red y protección de servicios (Fast re-route), como se vio anteriormente.

Funcionalidad Multicast

Aplicado para servicios de distribución como el video por ejemplo.

4.3 Análisis económico de la migración a MPLS

Todas las empresas buscan aumentar su rentabilidad para poder competir en el mercado y ofrecerle al cliente un mejor servicio. Para poder competir en el mundo tan cambiante de las telecomunicaciones hay que realizar constantemente cambios, caminar al paso de los avances tecnológicos, y brindar un mejor desempeño en los servicios. Cualquier empresa que desee realizar cambios necesita hacer una inversión de capital que permita implementar nuevos servicios.

En esta parte del trabajo hacemos un estudio financiero para evaluar la rentabilidad de la migración de una red IP/ATM a MPLS, para lograr esto nos valemos de distintas herramientas y la interpretación de los resultados de las mismas como por ejemplo el Valor Actual Neto (VAN) y la Tasa Interna de Retorno (TIR)

Vamos a definir una red IP/ATM como la que se muestra en la siguiente figura, para poder hacer el estudio financiero mas fehaciente de una migración a MPLS. Como podemos observar esta red consta de varios enlaces entre swtiches ATM que proveen conectividad entre los diferentes sitos y para conectarse a las redes IP se cuenta con routers con interfaces ATM e interfase Ethernet o GigaEthernet. También podemos conectarnos a las redes en Frame Relay, Clear Chanel o en ATM nativo.

Figura 30 Red propuesta para la migración

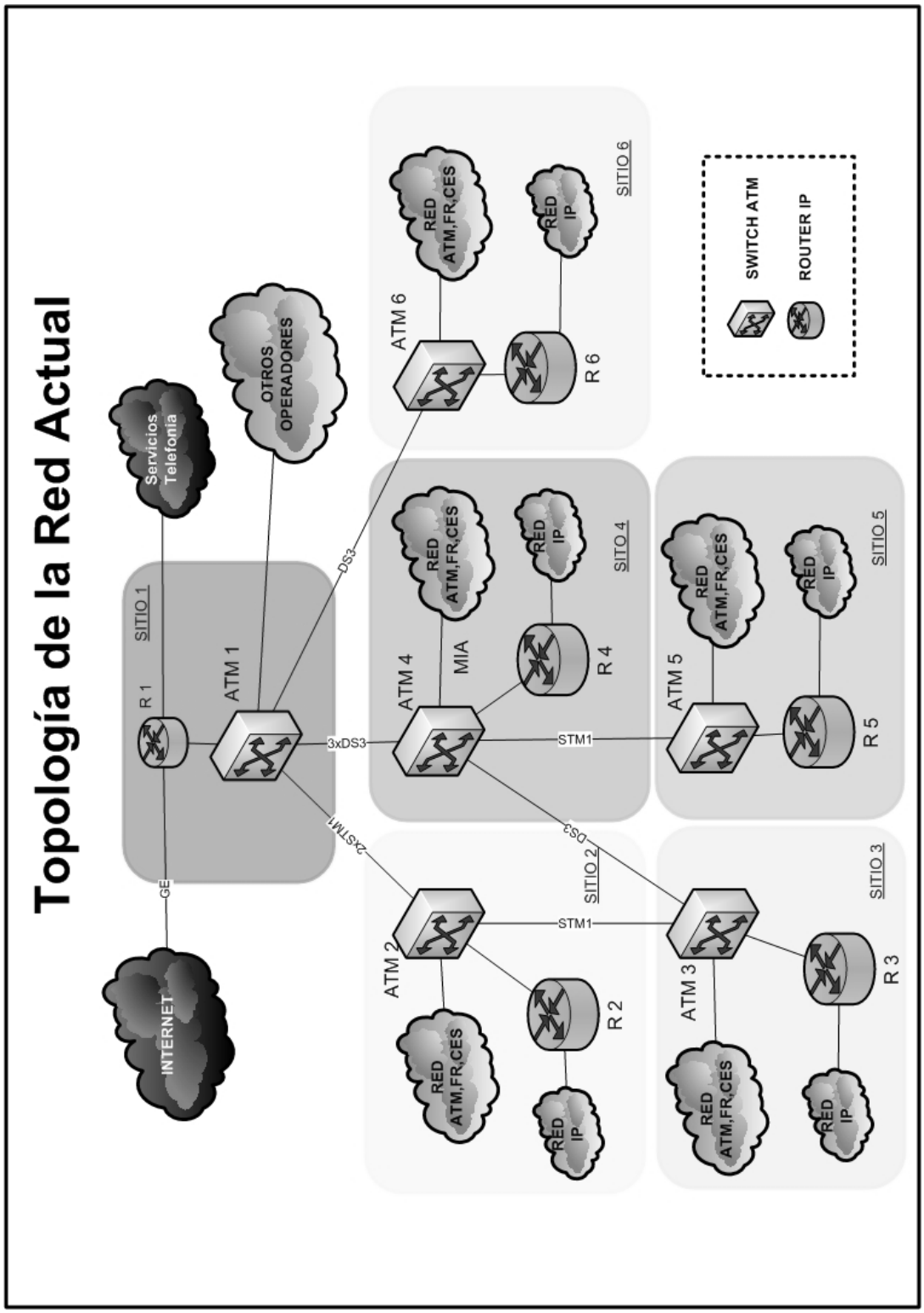
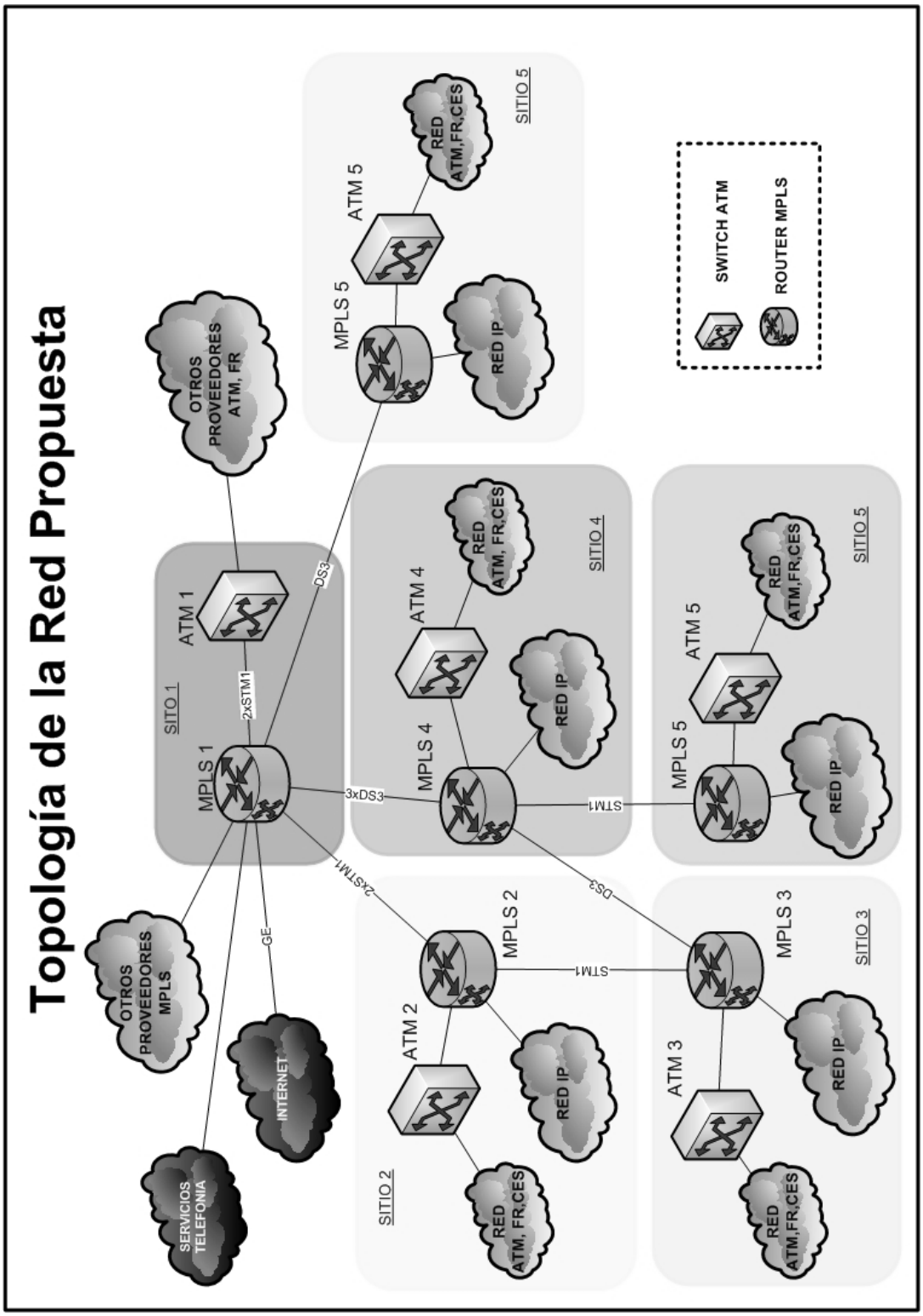


Figura 31 Topología de la red MPLS



Como vimos en la sección anterior para poder obtener todas la ventajas que brinda MPLS hay que migrar a MPLS basado en paquetes (IP routed MPLS) y de esa manera obtener un mejor desempeño de la red y servicios con calidad aceptable. Para lograr esto se propone migrar la red IP/ATM que se vio anteriormente a la red que se muestra en la figura 31 y sobre esa red nos basaremos para hacer el estudio financiero. Básicamente la propuesta trata de sustituir los conmutadores ATM por LSRs y conectar los conmutadores ATM a los bordes del dominio MPLS para aplicaciones que no puedan migrarse a la red MPLS como por ejemplo CES o ATM nativo, con esto el Backbone de la red seria MPLS al que se conecta directamente la red IP y ATM. Como veremos mas adelante esto trae beneficios a la red, por ejemplo el ahorro de ancho de banda, mejor manejo de la calidad de servicio, entre otros.

Estudio Financiero:

La parte fundamental de esta parte del estudio es la matriz financiera que incluye los gastos como inversión y los ingresos por los beneficios y servicios que genera el proyecto. Esta matriz permite encontrar los parámetros de decisión: el Valor Actual Neto (VAN) y la Tasa Interna de Retorno (TIR). Se ha tomado en cuenta el valor del dinero en el tiempo suponiendo una tasa de ganancia durante cinco años de 7% no acumulativa que es el porcentaje típico de pago anual por bancos locales o tasa interna aceptable. Para poder decidir si el proyecto es económicamente viable, el criterio de decisión sera:

- Que el Valor Actual Neto (VAN) calculado en la matriz financiera deberá ser mayor o igual a cero.
- Que la Tasa Interna de Retorno (TIR) calculada en la matriz financiera sea mayor que la tasa interna aceptable.
- Que la relación Beneficio/Costo sea igual o mayor a cero.

Si estos criterios se cumplen significa que el proyecto deja ganancias considerables.

MATRIZ FINANCIERA

		Periodos					
Costos	**Descripción**	**0**	**1**	**2**	**3**	**4**	**5**
Costos de Construcción del Sistema	Routers MPLS	$378,000.00					
	Tarjetas de Routers MPLS	$102,000.00					
	Servidor DMBS	$5,600.00					
	Capacitación a los Instaladores	$10,000.00					
	Costos de comunicación	$2,280,000.00	$2,280,000.00	$2,280,000.00	$2,280,000.00	$2,280,000.00	$2,280,000.00
Costos de Instalación	Capacitación del Usuario	$10,000.00					
	Instalacion y configuración de los Equipos	$10,000.00					
	Costo de Pruebas	$5,000.00					
	Migración de los servicios	$5,000.00					
	Otros gastos de instalación	$5,000.00					
Costos de Operación y Mantenimiento	Mantenimiento preventivo de los equipos		$5,000.00	$5,000.00	$5,000.00	$5,000.00	$5,000.00
	Reparación de los Equipos		$5,000.00	$5,000.00	$5,000.00	$5,000.00	$5,000.00
	Actualizaciones de Software y soporte		$3,000.00	$3,000.00	$30,000.00	$3,000.00	$3,000.00
	Otras instalaciones		$3,000.00	$3,000.00	$3,000.00	$3,000.00	$3,000.00
	Recurso Humano	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00
TOTAL INVERSION		$2,820,600.00	$2,306,000.00	$2,306,000.00	$2,333,000.00	$2,306,000.00	$2,306,000.00
Beneficios	**Descripcion**	**0**	**1**	**2**	**3**	**4**	**5**
Beneficos Tangibles	Ahorro de Ancho de Banda		$500,000.00	$500,000.00	$500,000.00	$500,000.00	$500,000.00
	Mejor y facil administración de la red		$5,000.00	$5,000.00	$5,000.00	$5,000.00	$50,000.00
	Facil provisionamiento		$5,000.00	$50,000.00	$5,000.00	$5,000.00	$5,000.00
	Ahorro en costos de operación y mantenimiento		$10,000.00	$10,000.00	$8,000.00	$7,000.00	$6,000.00
	Ahorro en equipos		$50,000.00	$40,000.00	$35,000.00	$30,000.00	$30,000.00
Beneficios Estrátegicos	Implementación de nuevos servicios		$100,000.00	$80,000.00	$60,000.00	$50,000.00	$50,000.00
	Incursión en nuevos mercados		$60,000.00	$40,000.00	$20,000.00	$10,000.00	$10,000.00
	diversificación de productos		$40,000.00	$30,000.00	$30,000.00	$30,000.00	$30,000.00
	Atraer nuevos clientes		$50,000.00	$40,000.00	$30,000.00	$20,000.00	$20,000.00
	Ampliar el volumen de operación y crecimiento		$100,000.00	$90,000.00	$80,000.00	$80,000.00	$60,000.00
Proyeccion de Ventas			$2,000,000.00	$2,500,000.00	$2,700,000.00	$2,900,000.00	$3,100,000.00
BENEFICIOS TOTALES			$2,920,000.00	$3,385,000.00	$3,473,000.00	$3,637,000.00	$3,861,000.00
FLUJO NETO EFECTIVO		-$2,820,600.00	$614,000.00	$1,079,000.00	$1,140,000.00	$1,331,000.00	$1,555,000.00

Tabla IV Matriz Financiera

4.3.1 Valor Actual Neto (VAN)

Tomando como referencia la Matriz Financiera se calcula el VAN

Tabla V Cálculo del Valor Actual Neto

Flujo neto de Efectivo suponiendo 7% de interés anual	
Año 0	-$2,820,600.00
Año 1	$614,000.00
Año 2	$1,079,000.00
Año 3	$1,140,000.00
Año 4	$1,331,000.00
Año 5	$1,555,000.00

VAN	$1,750,358.78

Según este criterio el proyecto es aceptable y factible económicamente.

4.3.2 Tasa Interna de Retorno (TIR)

Tomando como referencia la Matriz Financiera se calcula el TIR

Tabla VI Cálculo de la Tasa Interna de Retorno.

Flujo neto de Efectivo suponiendo 7% de enteres anual	
Año 0	-$2,820,600.00
Año 1	$614,000.00
Año 2	$1,079,000.00
Año 3	$1,140,000.00
Año 4	$1,331,000.00
Año 5	$1,555,000.00

TIR	25%

Según este criterio, la Tasa Interna de Retorno es de 25% mayor que la tasa mínima aceptable (7%) que se tomo para este proyecto, por lo tanto el proyecto es aceptable y factible económicamente

4.3.3 Punto de Equilibrio

Tomando como referencia la Matriz Financiera se calcula el Punto de Equilibrio

Tabla VII Cálculo del Punto de Equilibrio

Flujo neto de Efectivo suponiendo 7% de interés anual	
Año 0	-$2,820,600.00
Año 1	$614,000.00
Año 2	$1,079,000.00
Año 3	$1,140,000.00
Año 4	$1,331,000.00
Año 5	$1,555,000.00

PE	2.47
	2 años, 6 meses

Según el calculo anterior la inversión se recuparerará en 2.47 años o en 2 años y 5 meses aproximadamente.

4.3.4 Análisis Costo - Beneficio

Tomando como referencia la Matriz Financiera se calcula el Punto de Equilibrio

Tabla VIII Cálculo Relación Beneficio/Costo

	Inversión	Ingresos
Periodo	suponiendo 7% de interés anual	
Año 0	$2,820,600.00	$0.00
Año 1	$2,306,000.00	$2,920,000.00
Año 2	$2,306,000.00	$3,385,000.00
Año 3	$2,333,000.00	$3,473,000.00
Año 4	$2,306,000.00	$3,637,000.00
Año 5	$2,306,000.00	$3,861,000.00

VAN	Q12,297,695.33	Q14,048,054.11
Beneficio / Costo		1.14

Según este criterio la Relación Beneficio / Costo es mayor a cero, lo que nos lleva a la conclusión de que los beneficios del proyecto son mayores que los costos y esto lo hace económicamente viable.

Se puede ver en los cálculos anteriores que se cumplen los criterios de decisión que citamos al principio del estudio financiero:

- El Valor Actual Neto $1,750,358.78 es mayor a cero.
- La Tasa Interna de Retorno de 25% es mayor a la Tasa Interna Aceptable 7%.
- La relación Beneficio / Costo 1.14 es mayor a cero.

En base a lo anterior podemos concluir que el proyecto es económicamente viable y que deja ganancia considerable y la recuperación de la inversión según las ganancias anuales se calcula en 2.47 años o 3 años y 5 meses.

CONCLUSIONES

1. La idea básica de MPLS de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles de capa 2 y 3, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura.
2. MPLS utiliza equipo existente y direccionamiento IP (en conjunto con los mecanismos de señalización adecuados), por lo que no se tienen que hacer grandes cambios para utilizarlo.
3. En Guatemala, muchas empresas usan diversas tecnologías para la transmisión de información y el hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte —no sólo sobre infraestructuras ATM— va a facilitar de modo significativo la migración para la próxima generación de servicios.
4. MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino). Además de poder hacer ingeniería de tráfico IP, MPLS permite mantener clases de servicio y soporta con gran eficacia la creación de VPNs.

RECOMENDACIONES

1. En redes donde los conmutadores ATM no soporten una actualización para aplicaciones MPLS, es necesario reemplazarlos por conmutadores o routers que soporten MPLS y utilizar estos conmutadores ATM para entregar servicios ATM nativos.
2. Migrar a MPLS de celdas o a MPLS de paquetes, depende de la inversión que la empresa desea realizar, aunque MPLS de celdas no tiene todas las ventajas de MPLS de paquetes, puede ser utilizada como un primer paso de migración a MPLS de paquetes.
3. Para evitar impactos fuertes sobre las redes, deben realizarse pruebas de las configuraciones de los parámetros en una red MPLS (LDP, LSP, etc.), para que se ajuste a los requerimientos de la red que se desea migrar.

BIBLIOGRAFÍA

Yakov Rekther, Bruce Davie **MPLS: Tecnology and Applications**, Primera edición. Academic Prees, 2000.

Martín Tardío, Miguel Ángel y Otros **Análisis de la integración entre tráfico IP y redes ATM. Simulador MPLS,** Área de Ingeniería Telemática. Departamento de Informática. Universidad de Extremadura.

Stephenson, Ashley **MPLS: A Quality Choice**, Tutorial técnico, Cisco Systems, Noviembre de 1999.

O'Brien, Colm. **An Introduction to MPLS** The MPLS Forum Marketing Awareness & Education Committee. 2003.

Izzo, Paul. **Migrating to MPLS.** An MPLS Forum Sponsored Tutorial. 2003.

Sol Canalis, María. **MPLS Multiprotocol Label Switching: Una Arquitectura de Backbone para el internet del siglo XXI** Depto de Informática. Universidad del Nordeste, Corrientes Argentina. 2002.

AXIA. **Multiprotocol Lavel Switching (MPLS) Conformance an Performance Testing**. Whitepaper. 2004.

Semeria, Chuck. **Migration Strategies for IP Service Growth: Cell-switched MPls or IP-routed MPLS**, Juniper Networks. 2002.

ANEXOS

Calidad de Servicio (QoS) en IP: DiffServ

La primera arquitectura propuesta para ofrecer QoS en IP fue la arquitectura de Servicios Integrados o IntServ (rfc 1633). Esta arquitectura se basaba en garantizar calidad de servicio a través de reservar recursos de punta a punta en la red (de host a host) para cada flujo. Esta arquitectura utiliza el protocolo RSVP (rfc 2205), para efectuar la reserva de recursos y para mantenerla a lo largo de la red. Esta arquitectura si bien garantiza calidad de servicio, no es escalable y es impracticable en un backbone. Para solucionar el problema de escalabilidad de IntServ en la segunda mitad de la década de los 90 en el IETF comenzó a desarrollarse la arquitectura de servicios diferenciados o DiffServ. Esta arquitectura se basa en dividir el tráfico en clases, controlar la cantidad de tráfico que cada cliente envía a la red de cada clase de tráfico y asegurar requerimientos de calidad de servicio utilizando en cada enlace.

En este modelo se establecen acuerdos con el cliente SLA (Service Level Agreements), en el cual entre otras cosas se le garantizan para ciertas clases de tráfico ciertas garantías de calidad de servicio siempre que el cliente envíe el tráfico dentro de un cierto perfil (normalmente definido por valores de media, pico y tamaño máximo de burst).
Veremos a continuación brevemente los conceptos básicos de esta arquitectura.
Como mencionamos el tráfico es separado en clases en el ingreso a la red y marcado para registrar la clase a la que pertenece. Esa marca llamada DSCP (Differentiated Service Code Point) usa 6 bits para distinguir una clase de otra. Estos seis bits se registran en el byte de Tipo de Servicio (Type of Service) en el encabezado de IPv4 o en el de Clase de Trafico (Traffic Class) en el de IPv6.
A cada DSCP le corresponderá luego un tratamiento específico en cada nodo de la red.

Este tratamiento específico que se le brinda a cada clase de tráfico se llama en DiffServ PHB (Per Hop Behavior). El DSCP es seteado en la frontera de la red y en los routers internos es examinado para asociarlo con el PHB correspondiente. En este sentido la mayor complejidad residirá en los nodos de la frontera, aunque en los nodos interiores habrá que configurar políticas de manejo de colas y descarte de paquetes que pueden ser complejas.

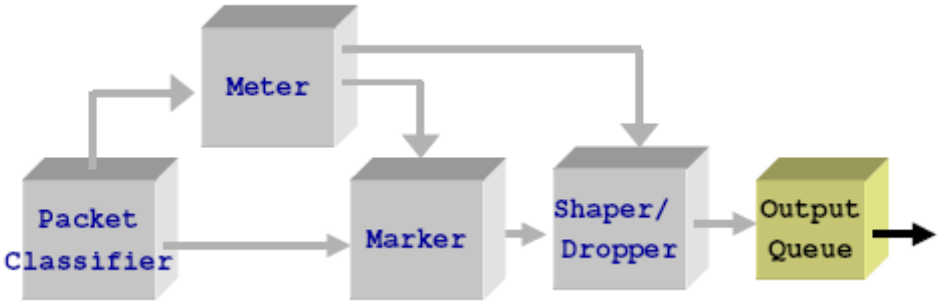


Figura A1. Arquitectura de un nodo exterior en Diffserv

En la figura A1 vemos la arquitectura de un nodo exterior en Diffserv. Existen dos funciones principales en esta arquitectura:

- El clasificador, que selecciona paquetes de acuerdo a ciertos criterios y los redirecciona en base a esta selección.

- El acondicionador de tráfico, que de acuerdo al SLA y en particular al perfil de tráfico acordado, acondiciona el tráfico que ingresa de cada clase.

La clasificación puede ser de dos tipos: MF (MultiField), es decir que analizando diferentes campos del paquete se define la clase a la que pertenece el paquete o simplemente basado en el campo DSCP si el paquete ya venía marcado. El paquete en este modelo puede venir marcado desde el cliente (sea este un usuario final u otro ISP).
La función de acondicionamiento del tráfico clasifica los paquetes en un grupo entrante (In-Profile) ó un grupo saliente (Out-Prifile). Los paquetes entrantes pueden ser

mandados sin ningún otro procesamiento. Los paquetes salientes podrán ser Re-acondicionados, Re-marcados (en alguna clase más baja por ejemplo) o descartados. Esto dependerá del acuerdo establecido con el cliente.
Los componentes básicos del acondicionador son:

- Meter: realiza mediciones temporales del conjunto de paquetes seleccionados por el clasificador contra el TCA (Traffic conditioning agreement).

- Marker: Setea el campo DS con un código particular y lo asocia así a una clase particular.

- Shaper: retarda algunos o todos los paquetes para que cumplan con el traffic profile.

- Dropper: descarta algunos o todos los paquetes para que cumplan con el traffic profile

Fuente:
Stephenson, Ashley **MPLS: A Quality Choice**, Tutorial técnico, Cisco Systems, Noviembre de 1999.