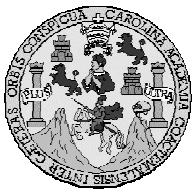


Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

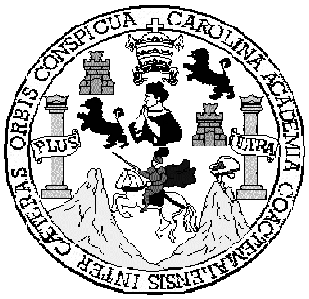
DISEÑO DE UNA RED PARA LA COMUNICACIÓN DE LAS MUNICIPALIDADES DE GUATEMALA, UTILIZANDO MPLS SOBRE ATM

Rodolfo Estuardo Arriaga Herrera

Asesorado por: Ing. Héctor Domínguez Oajaca

Guatemala, julio de 2004

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

DISEÑO DE UNA RED PARA LA COMUNICACIÓN DE LAS MUNICIPALIDADES DE GUATEMALA, UTILIZANDO MPLS SOBRE ATM

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA POR

RODOLFO ESTUARDO ARRIAGA HERRERA

ASESORADO POR: ING. HÉCTOR DOMÍNGUEZ OAJACA

**AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS**

Guatemala, julio de 2004

UNIVERSIDAD DE SAN CAROLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David García Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Ricardo Morales Prado
EXAMINADOR	Ing. César Fernández
EXAMINADOR	Ing. Guillermo Sánchez Barrios
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:

DISEÑO DE UNA RED PARA LA COMUNICACIÓN DE LAS MUNICIPALIDADES DE GUATEMALA, UTILIZANDO MPLS SOBRE ATM

Tema que me fuera asignado por la coordinación de la Carrera de Ingeniería en Ciencias y Sistemas, con fecha 15 de septiembre de 2003.

Rodolfo Estuardo Arriaga Herrera

ACTO QUE DEDICO

A DIOS: Sobre todas las cosas.

A MIS PADRES: Mardoqueo Arriaga Barahona
Alicia Margarita Herrera Dubón

A MIS ABUELOS: Rodolfo Antonio Herrera M. (QEPD)
Blanca Rosa Dubón Dubón

A MI HERMANO: Mardoqueo
por todo su apoyo incondicional y comprensión.

A MIS TÍOS: En especial Cristóbal y Mary Leny
Por todo su apoyo incondicional y compresión.

A MIS PRIMOS: En especial Elida y Hannia
que les sirva de ejemplo de que todo se puede hacer en la vida si se lo proponen.

A MIS AMIGOS Y COMPAÑEROS: Con mucho cariño hacia todos, por todos los momentos que tuvimos estudiando y divirtiéndonos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

1. PROTOCOLO DE COMUNICACIÓN ATM

1.1 Evolución de las redes ATM

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

Para obtener el mismo nivel de rentabilidad en las redes de próxima generación, los proveedores de servicios deben evolucionar su infraestructura de red rápidamente para adaptarse a la demanda explosiva de nuevos servicios y mayor ancho de banda. Deben hacer esto a la vez que protegen las fuentes de ingresos de los servicios actuales de telefonía y datos. En el mercado actual de las telecomunicaciones, donde escasea la financiación y el objetivo es construir fuentes de ingresos que generen rentabilidad, el mensaje clave es obtener resultados.

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

La consolidación reducirá la complejidad y el coste de construir, configurar y operar redes separadas, y proporcionará la infraestructura necesaria para soportar nuevos servicios. Para permitir esta transición de arquitectura, los suministradores de equipos deben proporcionar soluciones escalables que tomen la calidad *carrier grade* como punto de partida para construir valor, a la vez que se cumple la demanda de menores costes a corto plazo.

Para las redes ATM existentes, donde se usan líneas alquiladas para transportar el tráfico troncal y existe una significativa infraestructura en el núcleo de paquetes, es posible obtener un gran ahorro consolidando este tráfico troncal en el núcleo de la red IP-MPLS. Para algunos proveedores de servicio adoptar esta estrategia puede suponer ahorrar millones de dólares en costes, impactando directamente en la rentabilidad del negocio.

1.2 Descripción de ATM

Fundamentalmente, ATM es una tecnología que simultáneamente trasmite tráfico de datos, voz y vídeo sobre circuitos de alto ancho de banda, generalmente cientos de mega bits por segundo (Mbps) en 1997 y giga bits por segundo (Gbps), ahora en el 2004. La plataforma de hardware y software de ATM crea una arquitectura de comunicaciones basada en switching (alternación) y transmisión de pequeñas unidades de información, llamadas células (cells).

La primera diferencia entre redes basadas en ATM y otros sistemas de comunicaciones existentes, como Internet protocolo IP, Frame Relay, Switched Multimegabit Data Service (SMDS) y Ethernet, es que ATM es la primera tecnología y protocolo estructurado para integrar efectivamente voz, vídeo y datos sobre un mismo canal de comunicaciones a cualquier velocidad.

Las diferentes formas de ATM

ATM juega muchos roles dentro de las redes modernas de comunicaciones. Primero, provee la interfase user-to-network (UNI) para la transferencia simultánea de voz, vídeo y datos. Segundo, actúa como protocolo de señalización para controlar los servicios de ATM. Después, los multiplexores y swiches ATM, utilizan ATM como una tecnología para la implementación de redes de gran tamaño y velocidad. También muchos proveedores de servicios ven a ATM como un método de acceso de red integrada y económica. Finalmente, ATM actúa como una plataforma multiservicio para redes públicas. En resumen, ATM muestra las siguientes formas:

- Interfase
- Protocolo
- Tecnología
- Acceso integrado y económico
- Infraestructura escalable
- End-to-End Service

1.3 Fundamentos sobre tecnología ATM

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

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

Bajo una concepción celular de las comunicaciones, una red ATM es capaz de transferir cualquier tipo de información entre dos puntos sin modificar su naturaleza íntima. Ya sea voz, imagen o datos, el ATM cose un traje a la medida de las necesidades de cada tipo de tráfico. Simplificando al máximo, podemos ver que una red ATM está compuesta por nodos de conmutación, elementos de transmisión y los equipos terminales de usuarios.

Los nodos serán capaces de encaminar la información empaquetada en células a través de unos caminos conocidos como conexiones de canal virtual. El routing, en los nodos conmutadores de células, es un proceso a nivel hardware, mientras que el establecimiento de conexiones y el empaquetamiento y desempaquetamiento de las células son procesos a nivel software.

El principio de funcionamiento básico de ATM es la creación de un circuito virtual, se crea una conexión extremo-a-extremo en la que se han definido unos puntos de finalización y rutas pero que no tiene un ancho de banda preestablecido y dedicado en exclusiva para él. El ancho de banda lo asigna dinámicamente la red según la demanda de tráfico para transmitir. ATM también define varios tipos de servicios, según una amplia serie de requerimientos de las aplicaciones.

Bajo el punto de vista basado exclusivamente en la transmisión, el ATM se puede dividir en dos niveles, el primero de los cuales está a su vez dividido en otros dos; ambas se combinan de forma jerárquica de modo que cada capa superior puede tener uno o varios de los elementos inferiores.

Dentro del nivel ATM distinguimos dos subniveles o tipos de conexiones: las trayectorias virtuales (VP), que se identifican por medio de identificadores de trayectoria virtual (VPI), y los canales virtuales (VC), que se identifican por la combinación de un VPI y un VCI (identificador de canal virtual).

1.4 Modelo de referencia ATM

1.4.1 Nivel físico

Tiene que ver con el medio físico: voltajes, temporización de bits y varias consideraciones más. ATM no prescribe un conjunto de reglas en particular, pero en cambio dice que las celdas ATM se pueden enviar por sí solas por un cable o fibra, o bien se pueden empacar dentro de la carga útil de otros sistemas portadores. En otras palabras, ATM se diseñó para que fuera independiente del medio de transmisión.

1.4.2 Nivel ATM

Este nivel o capa tiene que ver con las celdas y su transporte; define la organización de las celdas y dice lo que significan los campos del encabezado. Esta capa también tiene que ver con el establecimiento y la liberación de circuitos virtuales, y aquí es donde se localiza el control de la congestión.

1.4.3 Nivel de adaptación ATM (AAL)

El nivel de adaptación AAL (ATM Adaption Layer) se encarga de las relaciones con el mundo externo, y sería básicamente análoga a la capa de enlace de datos del modelo OSI. Esta capa es la responsable de aislar los protocolos de capas superiores de los detalles de los procesos de ATM, así como de:

- Adaptación a la velocidad de los usuarios.
- Segmentación de los datos en células de 48 bytes.
- Detección de células erróneas y perdidas.
- Mantenimiento del sincronismo entre terminales.

Este nivel puede a su vez dividirse en diversas capas de adaptación:

- AAL-1:

La AAL-1, un servicio orientado a la conexión es adecuado para el manejo de aplicaciones de emulación de circuitos como voz y vídeoconferencia. El servicio de emulación de circuitos también da cabida a la conexión de equipo que utiliza actualmente líneas privadas hacia una red troncal de ATM. La AAL-1 requiere la sincronización de temporización entre origen y destino. Por esta razón, la AAL-1 depende de un medio como SONET, que soporta la temporización.

El proceso de AAL-1 prepara una celda para su transmisión en tres pasos. Primero, las muestras síncronas (por ejemplo, 1 byte de datos a una velocidad de muestreo de 125 microsegundos) se insertan en el campo Carga útil. Segundo, el campo SN (Número de secuencia) y el campo SNP (Protección del número de secuencia) se suman para ofrecer información que la AAL-1 de recepción utiliza para verificar que se han recibido las celdas en orden correcto. Tercero, el residuo del campo Carga útil se llena con una cantidad suficiente de bytes individuales hasta llegar a los 48.

SN: (Sequence number): Permite detectar células que faltan o con errores.
SNP (Sequence Number Protection): Código auto-corrector del nº de secuencia.

- AAL-3/4:

Soporta datos orientados y no orientados a la conexión. Fue diseñada para proveedores de servicios de red y se parece al SMDS (Servicio de datos conmutados a multimegabit). En un futuro se utilizará AAL3/4 para transmitir paquetes SMDS a través de una red ATM.

AAL-3/4 prepara una celda para su transmisión en cuatro pasos: Primero, CS (Subcapa de convergencia) crea una PDU (Unidad de datos de protocolo) colocando al inicio un encabezado de etiqueta de comienzo/final a la trama y agregando al final un campo de longitud como finalizador. Segundo, la subcapa SAR (Segmentación y reensamblaje) fragmenta la PDU y le coloca un encabezado al inicio. Después, la subcapa SAR agrega un finalizador CRC-10 a cada fragmento PDU para el control de errores. Por último, la unidad de datos del protocolo SAR se convierte por completo en el campo Carga útil de una celda ATM a la cual la capa ATM coloca al comienzo el encabezado estándar de ATM.

Un encabezado AAL-3/4 de la PDU de SAR consta de los campos tipo, número de secuencia e identificador del multiplexaje. Los campos tipo (ST) identifican si una celda es el comienzo, la continuación o el final de un mensaje. Los campos del número de secuencia (SN) identifican el orden en el que las celdas se deben reensamblar. El identificador de multiplexaje (MID) determina qué celdas, provenientes de diferentes fuentes de tráfico, se entrelazan en el mismo VCC para que las celdas correctas se reensamblen en el destino. Después de los datos aparecen dos otros campos: un campo de longitud (LI) que indica el número de octetos significados si la célula está parcialmente llena, y un campo CRC (Cyclic Redundancy Check) que representa el código de errores calculado sobre el campo de datos.

- AAL-5:

AAL-5 es la AAL principal para datos y soporta datos orientados y no orientados a la conexión. Se utiliza para transferir la mayor parte de los datos que no son SMDS, como el IP clásico a través de ATM y LANE. A AAL-5 también se le conoce como SEAL (Capa de adaptación simple y eficiente), ya que la subcapa SAR simplemente acepta la PDU de CS y la segmenta en PDU de SAR de 48 octetos sin agregar ningún campo adicional.

AAL-5 prepara una celda para su transmisión en tres pasos: Primero, la subcapa CS agrega al final de una trama un relleno de longitud variable y un finalizador de 8 bytes. El relleno asegura que la PDU resultante quede en el límite de 48 bytes de una celda ATM. El finalizador incluye la longitud de la trama y una CRC (Verificación de redundancia cíclica) de 32 bits calculada a través de toda la PDU. Esto permite que el proceso de recepción de la AAL-5 detecte errores de bits, celdas perdidas o celdas que están fuera de secuencia. Segundo, la subcapa SAR segmenta la PDU de CS en bloques de 48 bytes. No se agrega un encabezado ni un finalizador (como en la AAL-3/4), por lo que los mensajes no pueden estar entrelazados. Por último, la capa ATM coloca cada bloque en el campo Carga útil de una celda ATM.

En todas las celdas, excepto la última, se fija en cero un bit en el campo PT (Tipo de carga útil) para indicar que la celda no es la última de una serie que representa una sola trama. En la última celda, el bit en el campo PT se fija en uno.

La importancia del nivel de adaptación a la capa ATM (AAL) es que sirve para ofertar la calidad de servicio (QoS) adecuada para cada tipo de tráfico y es la base para proporcionar una gran variedad de servicios.

1.5 Clases de servicio

Los servicios se clasifican según tres parámetros que relacionan origen y destino:

A. Caudal. Define el volumen de información que puede ser enviada en un periodo de tiempo. Si el tráfico es constante, el parámetro es único: velocidad de pico; pero si el tráfico es a ráfagas, está expresado por tres parámetros de conexión: velocidad de pico, velocidad-media y duración de la ráfaga.

B. Retardo definido. Por su media y su varianza que relaciona el retardo global medio de toda la transmisión y la variación entre los retardos individuales que afectan a cada célula.

C. Nivel de seguridad. Se refiere a la tolerancia de un determinado tipo de tráfico a la pérdida de células que puede ocurrir durante períodos de congestión.

1.5.1 Servicio clase A

Servicio con conexión. Proporciona una velocidad de acceso constante (CBR) y una relación sincronizada entre los usuarios. En otras palabras, es un servicio que emula las prestaciones de un circuito. Un tráfico de este tipo es el generado por la telefonía sin comprimir. (Redes de largas distancias)

1.5.2 Servicio clase B

Servicio con conexión. Permite velocidades de tráfico variable (VBR), por lo que resulta adecuado para aplicaciones en tiempo real que necesitan una sincronización, aunque no una velocidad constante. La transmisión de la señal de vídeo comprimido utiliza este servicio.

1.5.3 Servicio clase C

También proporciona una velocidad de acceso variable pero no basada en el tiempo, por lo que resulta apropiado para datos insensibles al retardo. La distribución de software podría ser una aplicación que hiciera uso de este servicio.

1.5.4 Servicio clase D

Servicio sin conexión equivalente al modo datagrama de las redes de paquetes. Acepta tramas que contienen la información suficiente para el direccionamiento del paquete, de manera que llegue a su destino sin necesidad de establecimiento de una conexión previa. La interconexión de LAN está basada para utilizar este servicio.

1.5.5 Servicio clase Y

Permite a los usuarios finales pedir a la red cuánto ancho de banda y que clase de servicio son necesarios para una transmisión dada; la red acepta o rechaza este requerimiento. Es un servicio ABR (Available Bit Rate) adecuado para un tráfico no crítico cuyos requerimientos de tráfico varían de una transmisión a otra.

1.5.6 Servicio clase X

Denominado también UBR (Unspecified Bit Rate) no garantiza ni el caudal del tráfico, ni el retardo. Es ideal para aplicaciones que generan tráfico de muy baja prioridad. A modo de resumen, podemos ver la siguiente tabla que nos relaciona las diferentes capas AAL con los servicios sobre los que actuarían, con algunos ejemplos reales de aplicaciones existentes:

Tabla 1. Relación capa AAl con servicios

Clase	AAL	Características	Ejemplos
A	1	Velocidad constante, origen y destino intercambian información de sincronismo, los errores se detectan pero no se recuperan.	Circuitos punto a punto, telefonía, imágenes.
B	2	Transferencia de información generada a velocidad variable, pero sincronizada, los errores se detectan pero no se recuperan.	Vídeo on demand, difusión de TV.
C & D	3 y 4	Para datos sensibles a las pérdidas de células aunque no al retardo. Fueron dos AAL diferentes, hoy están unificadas.	Frame Relay, TCP/IP, WWW
C & D	5	Es una mejora del tipo ¾ que reduce el overhead y mejora la detección de errores.	Emulaciones de LAN, Internet

1.6 Protocolos asociados

1.6.1 Protocolo nativos ATM

Las aplicaciones nativas ATM están específicamente pensadas para usar la tecnología ATM y para explotar al máximo sus especiales características. Los protocolos nativos se encargan, por tanto, de ofrecer esas características intrínsecas de las redes de tecnología ATM (soporte de QoS, señalización, direccionamiento, etc.) a las aplicaciones nativas ATM (VoD, pizarras compartidas, vídeo-conferencia, etc.).

Ademas, existen también activas investigaciones para conseguir soportar sobre redes ATM aplicaciones no nativas ATM desarrolladas para otras tecnologías (IP, Frame Relay, SMDS, etc.).

En el ATM Forum, el termino native ATM services define servicios ATM específicos disponibles para el software y hardware residentes en dispositivos de usuario UNI ATM. Por consiguiente, el programador de aplicaciones dispone de nuevos servicios entre los que se pueden destacar las transferencias de datos (fiables o no) usando la capa ATM y varias capas de adaptación (AALs).

Disponibilidad de circuitos virtuales conmutados (SVCs) y circuitos virtuales permanentes (PVCs). Consideraciones relativas a la gestión de tráfico (clases de servicio, garantías de QoS, etc.). Posibilidad de distribución de conexiones y de participación local en la administración de la red (protocolos ILMI y OAM).

El propósito de los servicios nativos ATM es ofrecer el acceso a las clases de servicio o a las características de QoS en redes ATM. Estos servicios nativos también ofrecen soporte a un amplio y heterogéneo rango de flujos con diversas propiedades y requerimientos recomendados en el ATM Forum.

Los protocolos de transferencia nativos ATM gestionan la señalización UNI para establecer los SVCs, configurar PVCs y mapear los perfiles de QoS en la correspondiente clase de servicio. Los protocolos nativos ademas realizan funciones clásicas como las de transporte, mecanismos de control de errores, transferencia de datos, y controles de flujo y de congestión.

1.6.2 Protocolos de transporte para redes ATM

Uno de los componentes del ámbito de las comunicaciones que ha recibido mayor atención es la capa de transporte, la cuarta capa del OSI de los protocolos de comunicaciones. TCP e ISO son los dos más populares protocolos de transporte. Pero centrándonos más concretamente en el ámbito de ATM, vistas, en resumen, a continuación.

La siguiente tabla muestra un conjunto de nueve básicos servicios ortogonales que pueden ser combinados para obtener los requerimientos de determinadas aplicaciones. Actualmente, la capa de transporte referenciada en soporta tres clases de servicio o combinación de servicios. La marca X indica el servicio básico soportado en cada clase de servicio general.

1.6.3 Protocolos Multi-Point para redes ATM

El crecimiento de las redes ATM viene motivado, en parte, por la demanda de servicios multimedia para grupos dispersos de usuarios. El tráfico multicast tiene características particulares descritas para ATM en UNI 4.0 y anteriores. La distribución de información punto-a-multipunto (uno-a-muchos) o multipunto-a-multipunto (muchos-a-muchos) es un objetivo básico propuesto por varios protocolos y arquitecturas ATM que ofrecen el soporte multimedia y/o multicast como audio-conferencia, vídeo-conferencia, trabajos colaborativos o VoD.

ATM es aún una tecnología emergente diseñada para ser usada por aplicaciones de datos, audio y vídeo, lo que requiere un buen comportamiento de las transferencias unicast y multicast. User Network Interface (UNI 3.0) para ATM define conexiones punto-a-multipunto, y las conexiones multipunto-a-multipunto sólo pueden ser obtenidas de las dos siguientes formas:

- El primer esquema consiste en configurar N conexiones punto-a-multipunto para conseguir conectar todos los nodos en una topología completamente mallada todos-con-todos. Aunque esta topología ofrece conexiones multipunto-a-multipunto, hay que destacar que no escala bien cuando el número de participantes es elevado.

- Una alternativa al anterior esquema es el uso de un servidor que actúa a modo de raíz en el árbol multipunto. Este método sólo requiere un nodo raíz para almacenar información, pero la desventaja son las potenciales congestiones en el servidor cuando debe encargarse de envíos y retransmisiones de las conexiones multipunto-a-multipunto.

1.7 Características para el desarrollo de ATM

1.7.1 Gestión del ancho de banda

La técnica de división en el tiempo que usan las redes de transporte digital tradicionales (redes basadas en multiplexores PDH, SDH) no es válida para el transporte del tráfico LAN, que es uno de los tipos de datos que más ha crecido en los últimos años y que más insistentemente pide un lugar en las redes de banda ancha.

El tráfico de datos se caracteriza por una necesidad muy grande de ancho de banda, pero en momentos muy puntuales. El uso de técnicas TDM para la multiplexación del tráfico de LAN sobre los troncales de comunicaciones lleva a un compromiso demasiado duro. Por un lado, si se le asigna un time-slot de poco ancho de banda, el rendimiento de las comunicaciones no será aceptable. Por otro lado, si se le asigna un time-slot de gran ancho de banda, se malgastará demasiado espacio del canal cuando no se efectúen transferencias.

ATM, como nueva tecnología de transporte digital de banda ancha, dispone de mecanismos de control dinámico. De este modo, cuando una fuente de datos deja de emitir, el ancho de banda que resulta liberado del canal de comunicación se reasigna a otra fuente.

La gestión dinámica del ancho de banda va acompañada de unos complejos mecanismos de control de congestión que aseguran que el tráfico sensible (voz, vídeo, etc.) siempre dispondrá de la calidad de servicio requerida.

1.7.2 Soporte del trafico Broadcast

La evolución de las aplicaciones que requieren transporte digital muestra, desde hace tiempo, un claro cambio de rumbo de entornos punto a punto a entornos punto a multipunto. Aplicaciones como vídeoconferencias, tráfico LAN, broadcasting de vídeo, etc. requieren de soporte broadcast en la capa de transporte. Antes de ATM, las tecnologías de transporte digital se basaban en la multiplexación sobre canales punto a punto y, por lo tanto, no podían enfrentarse a este nuevo requerimiento de servicio.

ATM, aunque es una tecnología orientada a la conexión, contempla el uso de circuitos punto-multipunto que permiten ofrecer funciones de broadcasting de información. Los datos se replican en el interior de la red allí donde se divide el circuito punto-multipunto. Esta aproximación minimiza el ancho de banda asociado a tráfico broadcast y permite la extensión y crecimiento de estos servicios hasta niveles muy elevados.

1.7.3 Canales conmutados

Otro requerimiento que se le pidió a ATM fue que dispusiera de mecanismos para el establecimiento de circuitos conmutados bajo demanda del DTE. Estas funcionalidades que, hasta la fecha sólo se exigían a las redes de banda estrecha (RTC, RDSI, X.25, FrameRelay, etc.), se hacen cada vez más necesarias en la capa de banda ancha (Cable-TV, Vídeoconfencia, etc.).

ATM define un protocolo de señalización entre el DTE y la red, llamado UNI, que permite a este segundo la negociación de canales conmutados bajo demanda. El protocolo, basado en el Q.931 de RDSI, permite al DTE la creación de un canal (punto a punto o multipunto) con una determinada calidad de servicio (ancho de banda, retardo, etc.).

Otro protocolo (NNI) se encarga de la propagación de la petición de llamada dentro del interior de la red hacia el destino para su aceptación. El NNI es un protocolo no orientado a la conexión que permite la propagación de llamadas por múltiples caminos alternativos. En el momento de definición de ATM, se optó por un sistema de numeración de 20 bytes (basado en la numeración actual de la red telefónica básica) para los puntos terminales.

1.7.4 Escalabilidad

Uno de los principales problemas con los que se encuentran los administradores de las redes de transporte es cómo actuar frente a los continuos y cada vez más frecuentes cambios en los requerimientos, tanto de cobertura como de ancho de banda.

ATM se diseñó como una red inteligente. El objetivo era que los nodos que componían la red fueran capaces de descubrir la topología (nodos y enlaces) que les rodeaba y crearse una imagen propia de como estaba formada la red.

Además, este procedimiento debía ser dinámico para que la inserción de nuevos nodos o enlaces en la red fueran detectados y asimilados automáticamente por los otros nodos. Esta filosofía de red, que es muy común en las redes de banda estrecha (redes de routers, FrameRelay, etc.), se implanta en la banda ancha con la tecnología ATM.

Los administradores de la red de transporte ATM pueden decidir libremente el cambio de ancho de banda de un enlace o la creación de uno nuevo (por ejemplo, para disponer de caminos alternativos) sin tener que, por ello, reconfigurar de nuevo la red. Todos los nodos afectados por la modificación topológica actuarán inmediatamente como respuesta al cambio (por ejemplo, usando el nuevo enlace para balancear tráfico). Los problemas de cobertura tampoco significan ningún problema. Un nodo que se inserta en la red descubre, y es descubierto por, el resto de nodos sin ninguna intervención por parte del administrador.

1.8 Puntos clave de tecnología ATM

1.8.1 Estandarización

Si bien sus orígenes se remontan a los años 60, es a partir de 1988 cuando el CCITT ratifica a ATM como la tecnología para el desarrollo de las redes de banda ancha (B-RDSI), apareciendo los primeros estándares en 1990. Desde entonces hasta nuestros días, ATM ha estado sometida a un riguroso proceso de estandarización, destinado no solamente a una simple interoperabilidad a nivel físico (velocidades SONET y SDH), sino a garantizar la creación de redes multifabricantes a nivel de servicio, normando aspectos como señalización (UNI, NNI), control de congestión, integración LAN, etc.

Esta característica garantiza la creación de redes multifabricante, que posibilitan la inversión y permiten un fuerte desarrollo del mercado, con la consiguiente reducción de costes.

1.8.2 Multiplexación basada en celdas

Para que se pueda gestionar correctamente el ancho de banda sobre un enlace, es necesario que las diferentes fuentes que lo utilizan presenten sus datos en unidades mínimas de información.

Para ATM se decidió una unidad mínima de 53 bytes fijos de tamaño. El uso de un tamaño fijo permite desarrollar módulos de hardware muy especializados que conmuten estas celdas a las velocidades exigidas en la banda ancha (actual y futura). La longitud de la unidad debe ser pequeña para que se a multiplexar rápidamente, sobre un mismo enlace, celdas de diferentes fuentes y así garantizar calidad de servicio a los tráficos sensibles (voz, vídeo, etc.) .

1.8.3 Orientada a la conexión

Que ATM sea una tecnología orientada a la conexión permitía, entre otras cosas, conseguir una unidad mínima de información de tamaño pequeño. Como se ha dicho anteriormente, las previsiones de crecimiento para ATM obligaban al uso de un sistema de numeración de terminales de 20 bytes. Las tecnologías no orientadas a la conexión requieren que cada unidad de información contenga en su interior las direcciones tanto de origen como de destino. Obviamente, no se podían dedicar 40 bytes de la celda para ese objetivo (la sobrecarga por cabecera sería inaceptable).

Los únicos datos de direccionamiento que se incluye en la celda es la identificación del canal virtual que supone, únicamente, 5 bytes de cabecera (48 bytes útiles para la transmisión de información).

1.8.4 Calidad de servicio

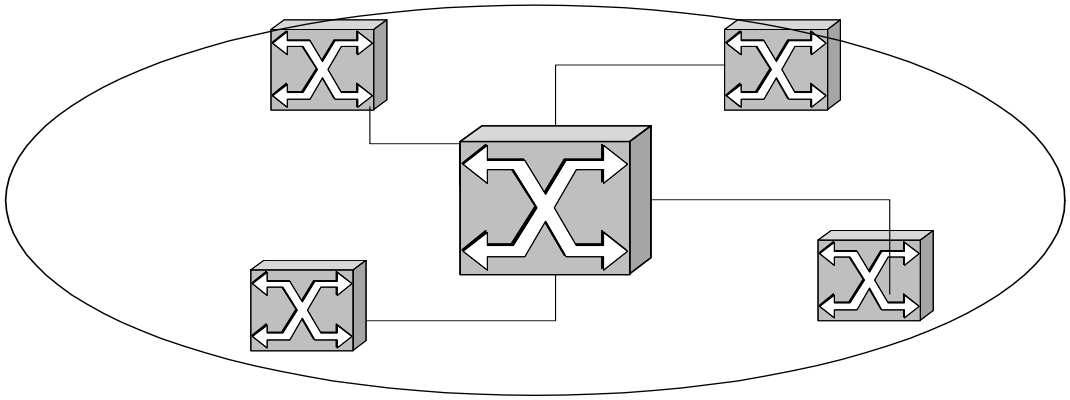
Se definen cuatro categorías de tráfico básicas: CBR (Constant Bit Rate), VBR (Variable Bit Rate), UBR (Undefined Bit Rate) y AVR (Available Bit Rate). En el momento de la creación, el DTE caracteriza el tráfico que va a enviar por el circuito mediante cuatro parámetros (PCR, SCR, CDVT y MBS) dentro de una de esas cuatro categorías. La red propaga esa petición internamente hasta su destino y valida si los requerimientos exigidos se van a poder cumplir. En caso afirmativo, la red acepta el circuito y, a partir de ese momento, garantiza que el tráfico se va a tratar acorde a las condiciones negociadas en el establecimiento.

Los conmutadores ATM ejecutan un algoritmo llamado dual leaky buckets que garantiza, celda por celda, que se está ofreciendo la calidad de servicio requerida. Está permitido que el DTE envíe los datos por un circuito a más velocidad de la negociada. En ese caso, el conmutador ATM puede proceder al descarte de las celdas correspondientes si existe saturación en algún punto de la red.

1.9 Topología de red ATM

Con tecnología ATM se consigue crear una red de transporte de banda ancha de topología variable. Es decir, en función de las necesidades y enlaces disponibles, el administrador de la red puede optar por una topología en estrella, malla, árbol, etc. con una configuración libre de enlaces (E1, E3, OC-3, etc.).

Figura 1. ATM no tiene topología asociada



La gran ventaja es la indiscutible capacidad de adaptación a las necesidades que ATM puede ofrecer. Una empresa puede empezar a desarrollar su red de transporte de banda ancha en base a unas premisas de ancho de banda y cobertura obtenidas a raíz de un estudio de necesidades. La evolución de las aplicaciones puede conducir a que una de esas premisas quede obsoleta y que se necesite una redefinición del diseño. En este caso, el administrador dispone de total libertad para cambiar enlaces o añadir nodos allí donde sea necesario.

2. PROTOCOLO DE COMUNICACIÓN MPLS

Conceptos fundamentales sobre Label Switching

2.1.1 Principales características MPLS

- Su principal objetivo es crear redes flexibles con un incremento en el desempeño y la estabilidad. Esto incluye soporte de traficos y de VPNs, el cual ofrece calidad de servicio (QoS) con múltiples clases de servicio (CoS).
- Para tecnologías basadas en celdas ATM, están contenidas en los campos del VPI y VCI.
- MPLS realiza la decisión del reenvío de paquetes basado en el contenido de una etiqueta, en lugar de realizar un complejo lookup basado en la dirección IP destino. Esta técnica brinda muchos beneficios a las redes basadas en IP como son: VPNs, ingeniería de tráfico, calidad de servicio.

2.1.2 Qué es MPLS

MPLS (MultiProtocol Label Switching) es un grupo de trabajo específico del IETF (Internet Engineering Task Force) que trata sobre el encaminamiento, envío y conmutación de los flujos de tráfico a través de la red.

Las principales funciones de MPLS son:

- Especificar mecanismos para gestionar flujos de tráfico de diferentes tipos (Ej.: flujos entre diferente hardware, diferentes máquinas, etc.).

- Quedar independiente de los protocolos de la capa de enlace y la capa de red.
- Disponer de medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes.
- Ofrecer interfaces para diferentes protocolos de routing y señalización.
- Soportar los protocolos de la capa de enlace de IP, ATM y Frame Relay.

En MPLS la transmisión ocurre en caminos de etiquetas conmutadas (LSP- Label Switched Path), que son secuencias de etiquetas en cada nodo del camino desde el emisor al receptor. Hay dos formas de requerir los LSPs:

1. Antes de la transmisión de datos (control-driven).
2. Una vez detectado un cierto flujo de datos (data-driven).

Las etiquetas se distribuyen utilizando un protocolo de señalización como LDP (Label Distribution Protocol) o RSVP (ReSource reserVation Protocol), o también añadidas a protocolos de routing como BGP u OSPF.

Las etiquetas son insertadas al comienzo del paquete en la entrada de la red MPLS. En cada salto el paquete es encaminado según el valor de la etiqueta y sale por la interfaz correspondiente con otra etiqueta. Se obtiene una gran rapidez en la conmutación gracias a que las etiquetas son insertadas al principio del paquete y son de longitud fija, lo que hace que pueda hacerse una conmutación vía hardware.

2.1.3 Componentes de MPLS

2.1.3.1 FEC (Forward Equivalence Class)

Conjunto de paquetes que comparten unas mismas características para su transporte, así todos recibirán el mismo tratamiento en su camino hacia el destino. La asignación de un paquete a un determinado FEC se produce una vez el paquete entra en la red. Cada FEC puede representar unos requerimientos de servicio para un conjunto de paquetes o para una dirección fija.

2.1.3.2 LSR (Label Switched Router)

Router de gran velocidad en el núcleo de una red MPLS. Sus funciones son las siguientes:

- Participar en el establecimiento de los LSPs usando un protocolo de señalización apropiado.
- Conmutar rápidamente el tráfico de datos entre los caminos establecidos.

Para que los LSPs puedan usarse, las tablas de envío de cada LSR deben contener: (interfaz de entrada, etiqueta asociada)→(interfaz de salida, etiqueta asociada). A este proceso se le llama distribución de etiquetas.

2.1.3.3 LER (Label Edge Router)

Router en la frontera de la red al que se pueden conectar diversas redes (Frame Relay, ATM, Ethernet). Envía el tráfico entrante a la red MPLS utilizando un protocolo de señalización de etiquetas y distribuye el tráfico saliente entre las distintas redes.

2.1.3.4 LSP

Cuando un paquete entra en la red MPLS, se examina para determinar qué LSP debe asociársele y, a partir de aquí, qué etiqueta asignarle. Esta decisión se debe a factores como la dirección de destino, QoS y el actual estado de la red.

2.1.4 Componentes del nivel de red

2.1.4.1 Componentes de despacho

Es el responsable de despachar paquetes desde una entrada a una salida en un switch o un router.

Para esta función, el componente del despacho usa estas dos fuentes de información:

- Tabla de despacho mantenida por el router.
- Información que proporciona el mismo paquete.

2.1.4.1.2 Granularidad del FEC

Se puede pensar que los algoritmos que usa el componente de despacho son un medio de dividir el conjunto de todos los paquetes que recibe un router, en número finito de subconjuntos disjuntos. Todos los paquetes de un mismo subconjunto se tratan de la misma forma. Estos subconjuntos se denominan FEC.

Un conjunto importante del FEC es la granularidad en su despacho.

- Extremos de espectro:

  - Un FEC puede incluir todos los paquetes cuya dirección de red calce con prefijos de dirección particulares (granularidad gruesa).
  - Un FEC puede incluir paquetes que pertenezcan a aplicaciones particulares que corran en un par de computadores, es decir, se incluyen sólo paquetes con las mismas direcciones, fuente y destino (granularidad fina).

2.1.4.1.3 Tablas de despacho en Label Switching

- La tabla de despacho es registrada por el valor de la etiqueta.
- Además de la información de despacho (el siguiente salto) se incluye la información relacionada con recursos que se utilizaran colas de salida).
- Un LSR puede mantener una tabla simple de despacho una tabla de despacho para cada una de sus interfaces.

2.1.4.1.4 Qué es una etiqueta

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

Pasos para la asignación de etiquetas:

1. Cada paquete se clasifica como un nuevo FEC o se le asigna un FEC ya existente.
2. Se asigna una etiqueta a cada paquete. Éstas se derivan de la capa de enlace, es decir, para redes Frame Relay, ATM o redes ópticas, los identificadores de la capa 2 (DLCIs, VPIs/VCIs y longitud de onda DWDM1, respectivamente) pueden servir como etiquetas. Para redes como Ethernet y PPP (Point to Point Protocol), a la etiqueta se le añade una cabecera shim entre las cabeceras de la capa de enlace y la capa de red, que contendrá el campoTTL (Time To Live).

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

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

- Etiqueta (20 bits): contiene la etiqueta asignada.
- CoS (3 bits): indica la clase de servicio que requiere el paquete.
- Pila (1 bit): permite apilar etiquetas en un paquete para realizar un encaminamiento jerárquico.
- TTL (8 bits): tiene el mismo significado que en IP, se denomina cabecera shim.

Bucles

El campo TTL indica el tiempo máximo de vida del paquete contado en saltos entre LSRs, este mecanismo permite mitigar los efectos de la creación de un bucle en la red, haciendo desaparecer el paquete en el momento que supere este tiempo.

En ATM o Frame Relay, donde no es posible utilizar TTL, los efectos de los bucles se minimizan mediante la limitación del espacio en buffers para un único VC (Virtual Channel).

Otra alternativa para detectar bucles es mediante la técnica Vector de rutas (Path Vector). Este vector contiene la lista de los LSRs que atraviesa el LSP, cuando un LSR propaga un mensaje de control del LDP (Label Distribution Protocol) añade su identificador al vector que irá en ese mensaje, por lo tanto, cuando un LSR reciba un mensaje en cuyo vector de caminos se encuentre su propio identificador se detectará el bucle.

Los bucles sólo se producirán en el encaminamiento salto a salto y en el encaminamiento explícito tolerante que se verá más adelante.

Pila de etiquetas

Permite operaciones jerárquicas en MPLS. Cada nivel en la pila de etiquetas pertenece a un nivel jerárquico, esto facilita la creación de túneles en MPLS.

MPLS permite varios protocolos de señalización para la distribución de etiquetas entre LSRs; el uso de cada uno de ellos dependerá del hardware de la red MPLS y de las políticas de administración de ésta.

Protocolos de routing como BGP permiten llevar piggybacked información sobre las etiquetas entre los contenidos propios del protocolo, se utilizan para etiquetas externas en VPNs.

Además, MPLS tiene su propio protocolo LDP para señalización y gestión del espacio de etiquetas. A éste se le han añadido extensiones para soportar, también requerimientos de QoS y CoS (Class of Service), así tenemos CR-LDP (Constraint-based – LDP).

Dominio MPLS: (conjunto de dispositivos habilitados en MPLS.)

Dentro de un dominio MPLS, un camino es establecido para que un paquete dado viaje con un determinado FEC. Existen dos mecanismos para establecer un LSP:

- Encaminamiento salto a salto: cada LSR selecciona independientemente el próximo salto para un FEC determinado (similar a la metodología utilizada en redes IP). El LSR utiliza cualquier protocolo de routing disponible como OSPF, ATM PNNI (ATM Private Network-Node Interface), etc.

- Encaminamiento explícito: El LER de entrada determina la secuencia de saltos explícita desde la entrada hasta la salida (ER-LSP, Explicit Routing LSP). Puede que la ruta no esté completamente especificada, es decir, puede haber un conjunto de nodos (Nodo abstracto) que es representado como un único salto en la ruta. También puede contener un identificador de sistema autónomo que permite que el LSP sea encaminado a través de un área de la red que está fuera del control administrativo de quien inició el LSP. Dentro de estos dos casos se hará un encaminamiento salto a salto.

Puede clasificarse como estricto, aquel camino que incluye todos los nodos, nodos abstractos y sistemas autónomos por los que pasa y el orden establecido; o como tolerante, aquél que incluye todos los saltos y mantiene el orden, pero puede incluir saltos que sean necesarios para alcanzar algún salto específico.

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

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

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

2.1.4.1.5 Algoritmo de despacho

El algoritmo se basa en una técnica llamada Label Swapping:

- Al recibir un paquete, el LSR le extrae la etiqueta y la usa como índice en su tabla de despacho.
- Una vez encontrada la entrada, para cada sub entrada, el router reemplaza la etiqueta del paquete con la etiqueta de salida de la sub entrada y se envía el paquete por la interfaces especificadas en la sub entrada.

2.1.4.2 Componentes de control

El componente de control consiste en uno o más protocolos de enrutamiento que permiten intercambiar información de enrutamiento entre routers, y algoritmos que permiten convertir esta información en tablas de despacho. Ejemplos de protocolos son OSPF, BGP y PIM.

2.1.4.2.1 Etiquetas y salto siguiente

- El componente de control de una arquitectura convencional no es suficiente para soportar Label Switching ya que se requiere de un mapeo entre etiquetas y saltos.
- Esto requiere de procedimientos para:
  - Ligar etiquetas con un FEC (clase de equivalencia de despacho).
  - Informar a otros LSR de los enlaces que se crean.
  - Utilizar los elementos anteriores para construir y mantener las tablas de despacho

2.1.4.2.2 Ligado a etiquetas

El ligado puede ser local o remoto:

- Ligado local: Se elige y se asigna localmente una etiqueta
- Ligado remoto: Se recibe de otro LSR información de ligado de otro router.

El ligado puede ser aguas arriba o aguas abajo:

- Aguas abajo: Etiquetas del ligado local se usan como etiquetas de entrada. Etiquetas de ligado remoto se usan como etiquetas de salida.

El ligado aguas abajo se llama así porque el ligado de una etiqueta que lleva un paquete y un FEC particular, al cual pertenece el paquete, es creado por el LSR que está aguas abajo (respecto al flujo de paquetes) del LSR que pone la etiqueta en el paquete.

Los paquetes que llevan una etiqueta particular fluyen en la dirección opuesta al flujo de información del ligado respecto a la etiqueta.

- Aguas arriba: Etiquetas del ligado local se usan como etiquetas de salida y etiquetas de ligado remoto se usan como etiquetas de entrada.

El ligado aguas arriba se llama así porque el ligado entre una etiqueta que lleva un paquete y un FEC particular, al cual pertenece el paquete, es creado por el mismo LSR que pone la etiqueta en el paquete, es decir, el creador del enlace está aguas arriba respecto al flujo de paquetes.

Los paquetes que llevan a una etiqueta particular fluyen en el mismo sentido que la información del ligado respecto a la etiqueta

3. INTEGRACIÓN ENTRE ATM Y MPLS

3.1 Evolución de la integración de IP

3.1.1 El camino hacia la convergencia de niveles: IP sobre ATM

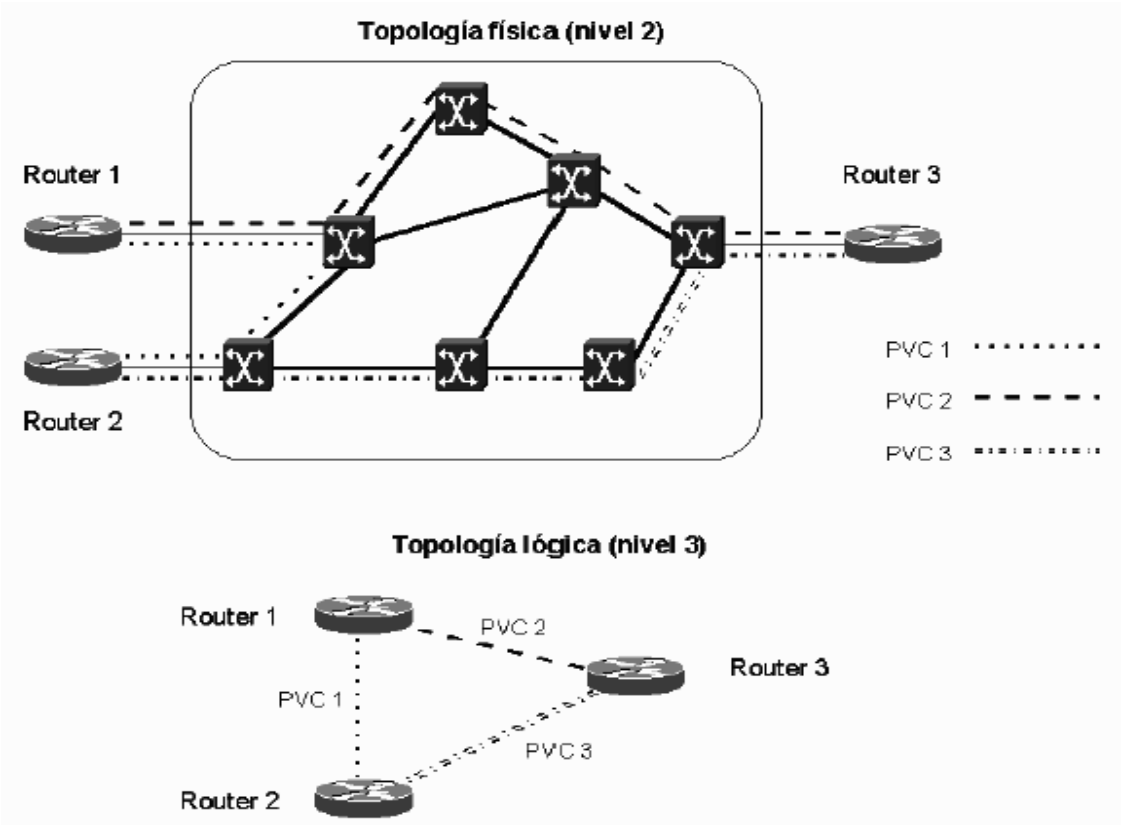
A mediados de los 90, IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI, etc.). Por otro lado, hay que recordar que los *backbones* IP que los proveedores de servicio (NSP) habían empezado a desplegar en esos años, estaban construidos basados en *routers* 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 respuesta 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 (1995-97) 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.

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. Éstos, 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.

Figura 2. Topología física ATM y topología lógica IP superpuesta

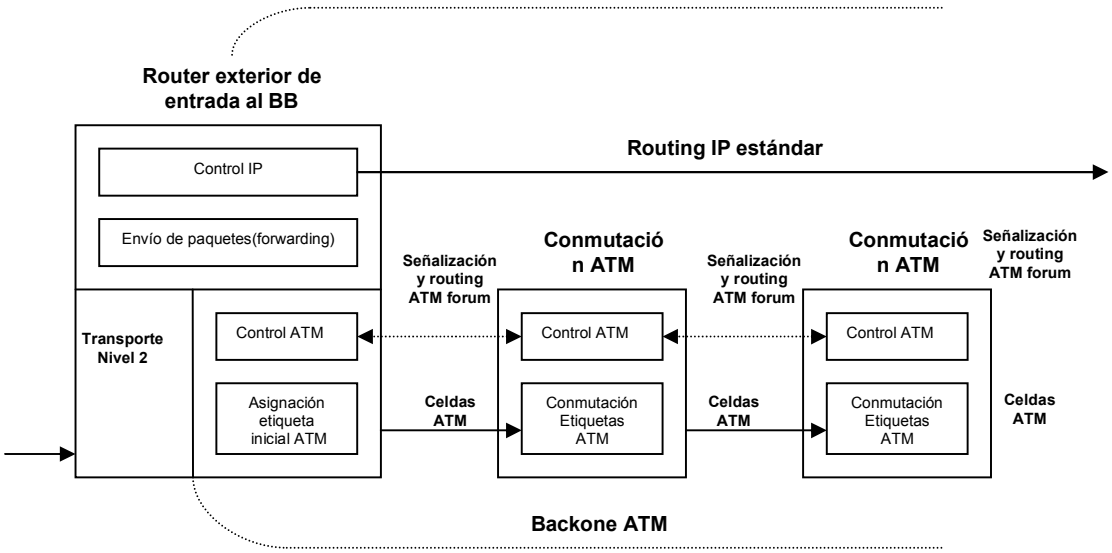


La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y *routing*) y el envío de las celdas por hardware (conmutación).

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 2 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 3. 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 (la mayor parte telcos), 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 UBR6 (*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 IGP7.

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. Piénsese, por ejemplo, en una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM. Son necesarios 5 x 4 = 20 PVCs (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura (6 x 5 = 30). Un problema adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP.

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.

3.1.2 Un paso más en la convergencia hacia IP: Conmutación IP

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señalas anteriormente. Esas técnicas se conocieron como "conmutación IP" (*IP switching*) o "conmutación multinivel" (*multilayer switching*).

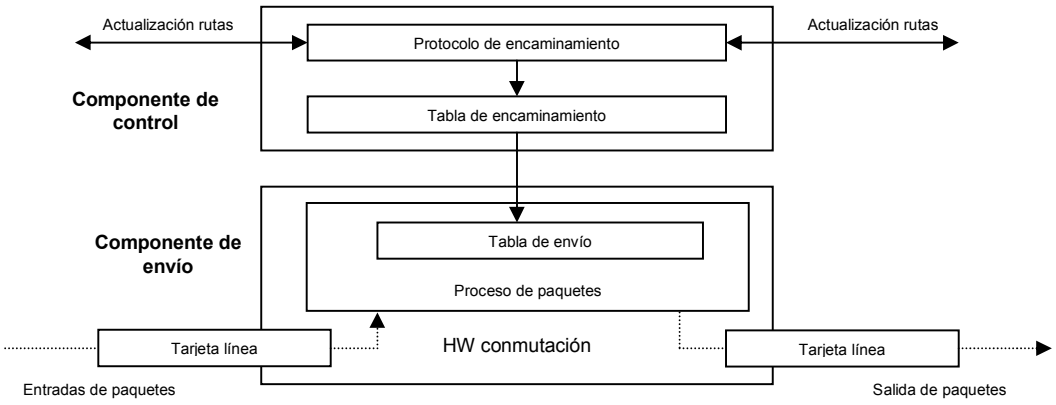
Una serie de tecnologías privadas —entre las que merecen citarse: *IP Switching* de Ipsilon Networks, *Tag Switching* de Cisco, *Aggregate Route-Base IP Switching (ARIS*) de IBM, *IP Navigator* de Cascade/Ascend/Lucent y *Cell Switching Router (CSR)* de Toshiba— condujeron finalmente a la adopción del 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 4. Separación funcional de encaminamiento y envío.



En la figura de separación funcional de encaminamiento y envío 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 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.

3.1.3 La Convergencia real: 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.

3.1.3.1 Ideas preconcebidas sobre MPLS

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

Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM.
- MPLS debía soportar el envío de paquetes tanto unicast como multicast. MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP8.
- MPLS debía permitir el crecimiento constante de la Internet.
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

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

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

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

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

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

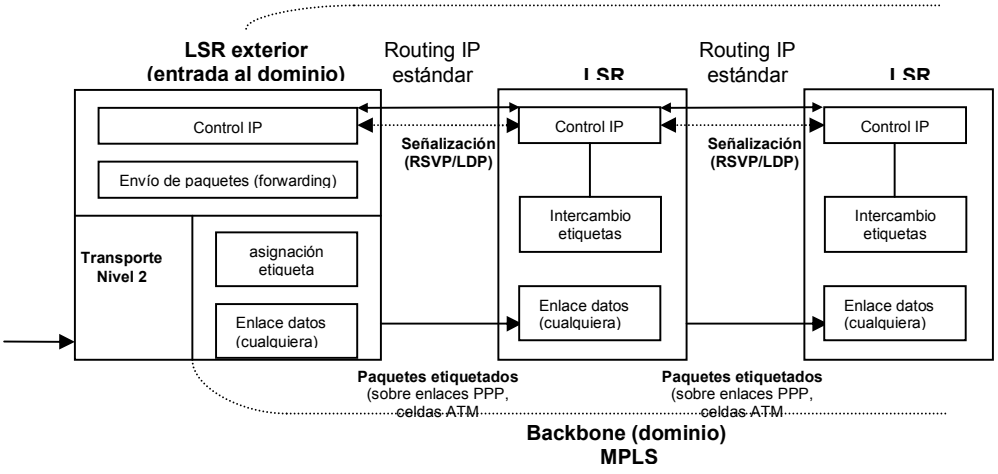
3.1.3.2 Descripción funcional

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.

3.1.3.2.1 Funcionamiento del envío de paquetes en MPLS

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simples 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.

Figura 5. Esquema funcional del MPLS.



Al igual que en las soluciones de conmutación multinivel, MPLS separa los 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.

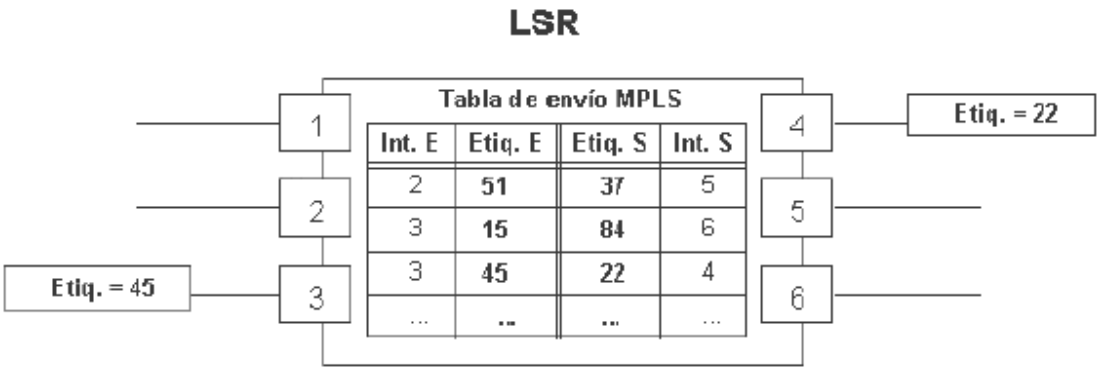
Actualmente ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte 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. 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). A un paquete que llega al LSR por la interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

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



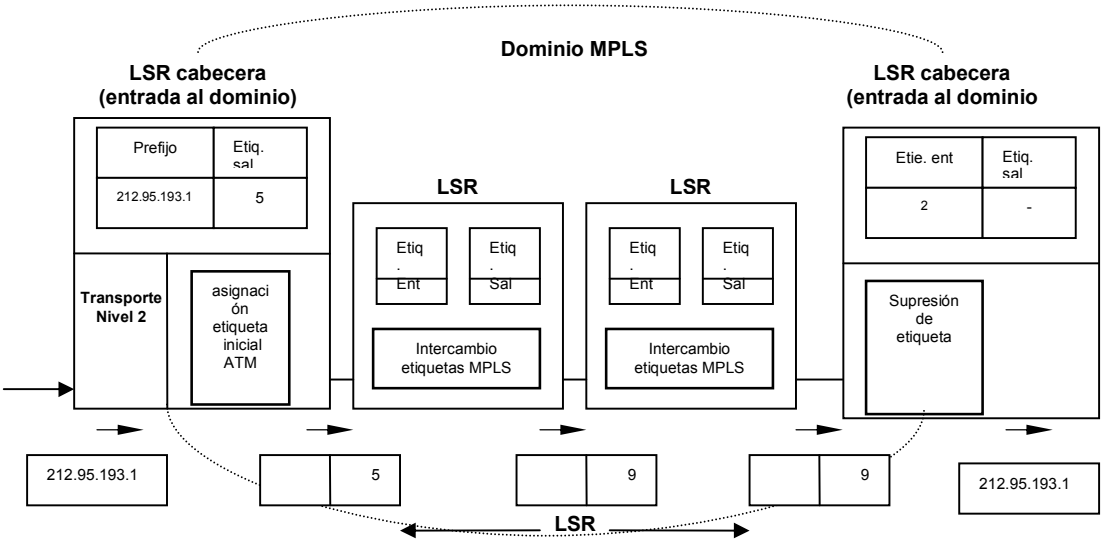
El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 7, el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta 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.

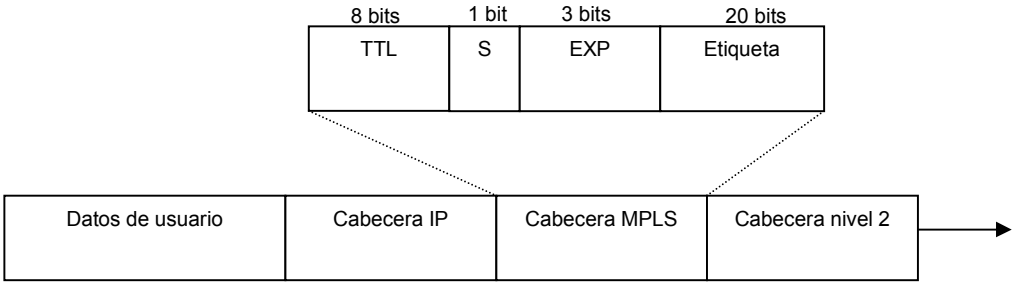
Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativo para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas por ejemplo 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 7. Ejemplo de envío de un paquete por un LSP.



En la gráfica siguiente 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 8. Estructura de la cabecera genérica MPLS.



3.1.3.2.2 Control de la información en MPLS

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, conlleva dos aspectos fundamentales, los cuales son:

1. Cómo se generan las tablas de envío que establecen los LSPs.
2. 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 r*outing* 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, etc.) 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.

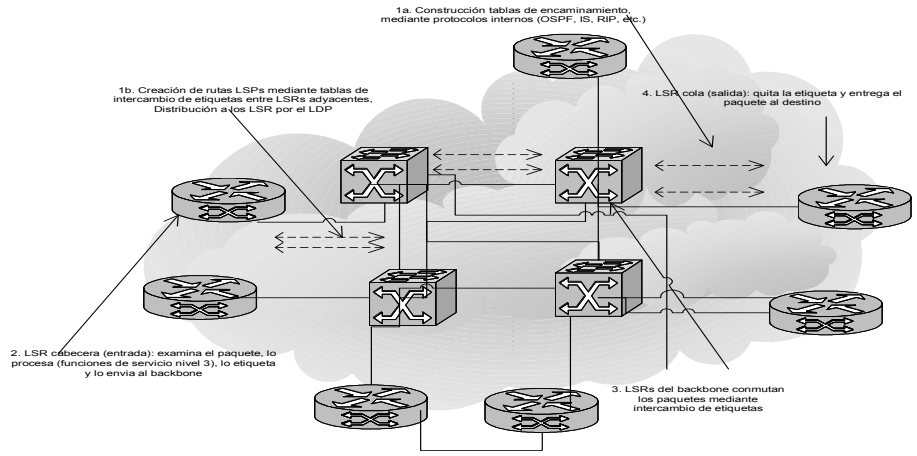
El segundo aspecto se refiere a la información de "señalización", pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo 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).

3.1.3.2.3 Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura funcionamiento de una red MPLS, 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, tal como se explica en la sección siguiente.

Figura 9. Funcionamiento de una red MPLS.



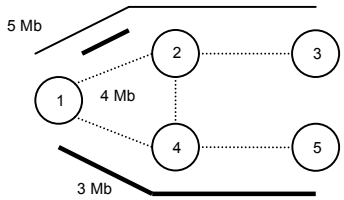
3.1.3.3 Gestión de recursos

MPLS permite establecer LSP y además establecer LSP de respaldo asociados a los de trabajo. El establecimiento de todos estos LSP se realiza usando algoritmos de encaminamiento con calidad de servicio que buscan la ruta óptima, tanto desde el punto de vista de la calidad de servicio requerida como desde el punto de vista del uso de los recursos de la red. A partir de este punto la gestión de recursos, básicamente se encarga de ajustar los LSP establecidos en la red adaptándolos al uso real que se esté haciendo de ellos, de forma parecida a la realizada en ATM.

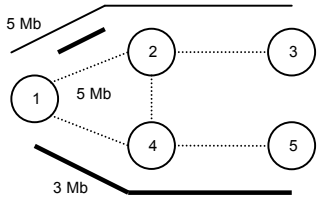
Para conseguir esta adaptación al tráfico real de la red, los mecanismos de ingeniería del tráfico deben realizar tareas de monitorización. Por lo tanto, se puede afirmar que los mecanismos de gestión de recursos están constantemente pendientes del estado real de la red y fuertemente relacionados con el establecimiento de LSP de trabajo y de respaldo con algoritmos de encaminamiento con calidad de servicio. Por este motivo, la gestión de recursos también cubre la detección de las alarmas en el momento en que se produce un fallo en la red y la activación de los LSP de respaldo. Por lo tanto, la gestión de recursos cubre la monitorización del estado real de la red y procede a su adaptación (cambiando los LSP existentes) al tráfico real y a los posibles fallos que puedan surgir (activando los LSP de respaldo necesario).

Una vez establecidos los LSP, éstos tendrán una cierta vida, corta o larga, durante la cual pueden sufrir una serie de problemas. Se puede establecer un LSP con un cierto ancho de banda asignado para una cierta cantidad de tráfico con una cierta calidad de servicio.

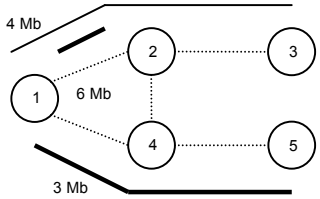
Figura 10. Gestión de banda ancha.



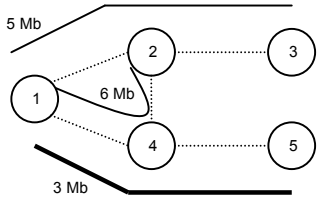
a) Situación inicial: 3 LSPs de 3, 4 y 5 Mb de ancho de banda. El de 4 Mb es el que está congestionado y requiere incrementar su banda. El de 4 Mb es el que está congestionado



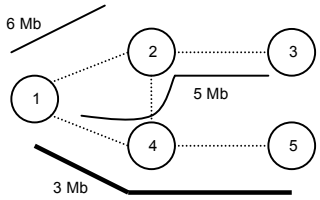
b) Cambio del ancho de banda del LSP de 4 Mb a 5 Mb. Se supone que existen suficientes recursos disponibles en el enlace 1-2.



c) Cambio del ancho de banda del LSP de 4 Mb a 6 Mb tomando parte de esta banda del LSP que inicialmente era de 5. Se supone que no la estaba usando.



d) Cambio del ancho de banda del LSP de 4 Mb a 6Mb. Debido a que no existe suficiente banda libre en el enlace 1-2 ni suficiente banda no usada en el LSP de 5 Mb, se reencamina el LSP conflictivo a través de 1-4-2



e) Cambio del ancho de banda del LSP de 4 Mb a 6 Mb. Debido a que no existe suficiente banda libre en el enlace 1-2 ni suficiente banda libre en los enlaces 1-4-2, se reencamina el LSP de 5 Mb.

Sobre este LSP puede suceder que, al cabo de un cierto tiempo, la demanda de tráfico supere la reserva inicial y se produzca un rechazo de tráfico de entrada. Este rechazo o bloqueo se produce debido a algún tipo mecanismo de control de admisión necesario para garantizar la calidad de servicio de las distintas conexiones existentes, y puede cuantificarse calculando la probabilidad de bloqueo para cada LSP.

Otro fenómeno que puede suceder es que, una vez reservada una cierta cantidad de ancho de banda para un cierto LSP, después de cierto tiempo este LSP esté poco utilizado y se estén desperdiciando los recursos de la red, cuando posiblemente otros LSP puedan estar congestionados y rechazando tráfico.

La técnica habitual para adaptar el ancho de banda de los LSP al tráfico real es la reasignación de banda de los mismos, incrementándola o decrementándola según sea el caso. Para poder incrementar la banda de un LSP es necesario que a lo largo del camino que sigue este LSP (los diferentes enlaces físicos que atraviesa) existan los suficientes recursos libres (figura 10 b). Si esto no sucede, existen dos posibles acciones a tener en cuenta. La primera es buscar en qué enlaces físicos no se cumple la condición de que no exista suficiente banda disponible y, posteriormente, en estos enlaces comprobar si existe algún otro LSP infrautilizado y del que se pueda tomar la banda necesaria (figura 10 c). En otras palabras, consiste en traspasar banda de LSP poco usados a un LSP congestionado y que necesita incrementar su banda.

La segunda posibilidad, en el caso de que la primera no sea posible, es reencaminar el LSP que necesita mayor ancho de banda a través de otro camino que pueda satisfacer sus necesidades (figura 10 d). También en este caso, si no es posible reencaminar al LSP congestionado, existe la posibilidad de reencaminar uno o varios de los demás LSP con los que comparte los mismos enlaces físicos, con lo cual se liberan recursos y permite incrementar su banda (figura 10 e).

En los casos en los que hay que reencaminar LSP, se puede hacer uso de los algoritmos de encaminamiento dinámicos y con calidad de servicio. De ahí que estos mecanismos de gestión de recursos estén estrechamente relacionados con los mecanismos de establecimiento de LSP de trabajo y de respaldo con calidad de servicio, creando un entorno global de ingeniería del tráfico.

Otro aspecto a tener en cuenta es qué mecanismos toman la decisión de adaptar la banda de los LSP y realizar las operaciones anteriormente descritas. Existen diferentes ejemplos en la literatura, y dependiendo de dónde se tome la decisión, se puede hablar de mecanismos centralizados o distribuidos. Estos mecanismos, por las tareas que realizan, se situarían dentro del plano de gestión.

Tradicionalmente, la gestión, en este caso de recursos y de fallos, se ha realizado de forma centralizada, lanzando algoritmos de optimización que, disponiendo de los datos de monitorización de toda la red, calculan la distribución óptima de los LSP. En redes troncales relativamente grandes por las que circula gran cantidad de LSP es muy difícil disponer de todos los datos de monitorización de forma centralizada y calcular la distribución óptima a tiempo antes de que el estado de la red ya haya cambiado.

Una de las opciones que aparecen en la literatura reciente es tratar de mantener la distribución de LSP lo más cercana posible a la óptima haciendo pequeños ajustes, usando algoritmos distribuidos. La ventaja principal de estos últimos es que disponen de la información de forma local y permanentemente actualizada. La desventaja está en que no se dispone de una visión global de la red.

Otro tema importante es la frecuencia con la que se realizan las adaptaciones de los LSP. Existen mecanismos que las realizan periódicamente, otros que las realizan cada vez que se detecta un problema, etc. La frecuencia máxima sería cada vez que se realiza una conexión nueva o finaliza una conexión antigua. Por el contrario, una frecuencia mínima sería no cambiar nunca los LSP.

Con respecto a los mecanismos periódicos, depende del periodo y de cómo se calcule la nueva distribución de LSP, pero, en general, pueden calcular la nueva distribución cuando no se está produciendo el problema.

Una frecuencia excesiva provocaría una gran generación de mensajes de señalización en la red con un efecto contrario al buscado, un empeoramiento del rendimiento de la red. Parece que de nuevo es necesario realizar los cambios en cuanto se detectan los problemas, pero evaluando correctamente si vale la pena o no realizar el cambio en ese momento, por lo que de nuevo se precisa una cierta inteligencia en estos mecanismos.

3.1.3.4 Protección de entorno MPLS

Los enlaces físicos o virtuales de una red están expuestos a fallos de conectividad. El objetivo de los mecanismos de protección es minimizar el riesgo de desconexión. Dichos métodos de protección siguen un ciclo, que va desde la detección de un fallo en un camino de datos, hasta que el tráfico puede reestablecerse en dicho camino.

Este ciclo involucra a varios componentes: un método de encaminamiento que selecciona caminos de trabajo y de respaldo; un método de reserva de banda en ambos caminos; un método de señalización para configurar (distribuir las etiquetas) en los caminos de trabajo y respaldo; un mecanismo de detección y otro de notificación de fallos, necesarios para indicar al nodo responsable de tomar las acciones de respuesta al fallo que se ha producido; y, finalmente, un mecanismo para desviar el tráfico desde el camino de trabajo (en el que se ha producido el fallo) hasta el camino de respaldo (acción de *switchover*).

Opcionalmente, podemos disponer de un mecanismo de detección de la recuperación del camino original y de los elementos necesarios para volver a restablecer el tráfico.

Un aspecto que distingue a MPLS de otros mecanismos de protección es que podemos aplicar protección a diferentes niveles. En los dominios MPLS, podemos disponer de mecanismos de protección para todo el camino o bien para un segmento de éste. En la protección a nivel de toda la ruta, la protección siempre vendrá activada por los nodos extremos del LSP, independientemente de dónde se origine el fallo. Estos mecanismos implican propagar la señal de indicación de fallo FIS (*fault indication signal*) hasta el nodo inicial (*ingress node*), lo cual implica un cierto coste en términos de tiempos de restauración.

En la protección por segmentos o protección local, las acciones de recuperación se activan en el propio nodo que detecta el fallo. Este LSR tiene que estar provisto de funcionalidades PSL (*protection source LSR*). En el otro extremo tendremos otro nodo con funcionalidades de PML (*path merge LSR*) que permiten mezclar los tráficos que provienen del propio camino de trabajo y el de respaldo en un solo LSP.

Evidentemente, si bien este mecanismo es más rápido que el anterior, no permite proteger todo el camino. Para ello tendríamos que proteger cada uno de los segmentos del camino de trabajo con el coste en recursos que esto implica.

Figura 11. Mecanismos de protección MPLS

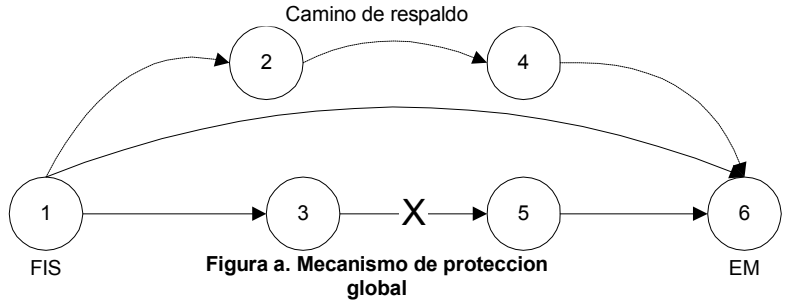


Figura a. Mecanismo de proteccion global

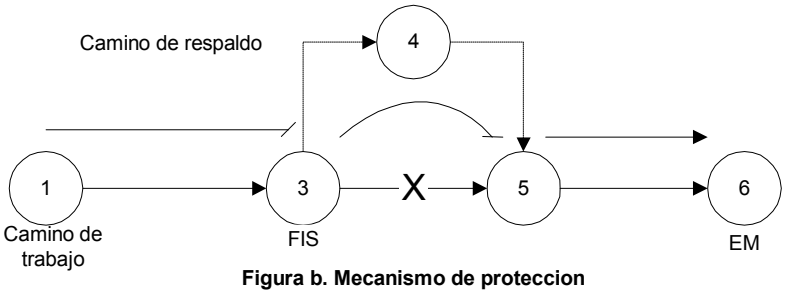


Figura b. Mecanismo de proteccion local

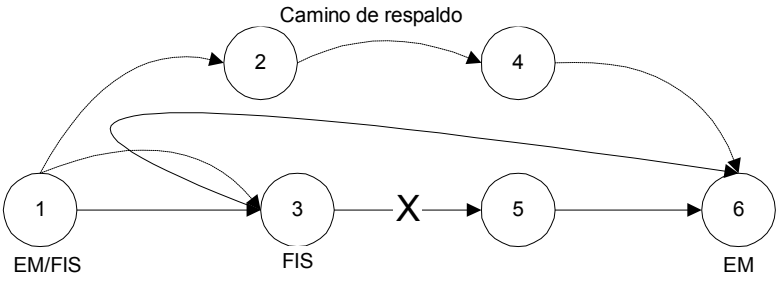


Figura c. Mecanismo de proteccion inversa

3.1.3.5 Métodos de protección MPLS

3.1.3.5.1 Método global

En este modelo, el nodo inicial (*ingress node*) es el responsable de resolver la restauración cuando la FIS llegue. Este método necesita de un camino de respaldo disjunto al camino de trabajo.

Las acciones de protección siempre se activan en el *ingress node*, independientemente de donde ocurra el fallo (a lo largo del camino de trabajo). Esto significa que la información del fallo tiene que propagarse desde el nodo donde éste es detectado hasta el nodo inicial. Si no disponemos de ningún LSP inverso, la detección del fallo se tendrá que realizar con otro tipo de mecanismo, como el chequeo continuo del camino de trabajo.

Este método tiene la ventaja de tener que configurar una única ruta de respaldo para cada camino de trabajo y, además, es un método centralizado, lo que significa que un único nodo tiene que ser provisto de las funciones de PSL. Por otro lado, este método presenta un alto coste en términos de tiempos de restauración y pérdida de paquetes.

La figura 11.a nos enseña un escenario simple formado por seis LSR donde el camino de trabajo (LSR1-LSR3-LSR5-LSR6) y el camino de respaldo (LSR1-LSR2-LSR4-LSR6) están preestablecidos. En condiciones normales, el tráfico se transmite desde el *ingress node* LSR1 hasta el *egress node* LSR6 a través del camino de trabajo. Cuando se detecta un fallo (por ejemplo entre el nodo LSR5 y LRR6), el tráfico cambia hacia el camino de respaldo.

3.1.3.5.2 Método local

En este método la restauración se activa en el mismo punto donde se produce el fallo; es, por lo tanto, un método transparente al *ingress node*. Su principal ventaja es que ofrece mejores tiempos de restauración que los métodos globales.

En este método la dificultad principal reside en tener que proveer de funcionalidades PSL (y en su caso PML) a todos los nodos (origen-destino) de los segmentos del camino de trabajo que queramos proteger. Además, tendremos que buscar tantos caminos de respaldo como segmentos a proteger (a diferencia del esquema global, donde era necesario un único *backup*). Otra ventaja, sin embargo, es que en este método no se producen pérdidas de paquetes como en el esquema global.

La figura 11.b muestra este caso. El modelo de red es el mismo: tenemos un camino de trabajo formado por los nodos (LSR1-LSR3-LSR5-LSR6) y una ruta de respaldo formada por LSR3-LSR4-LSR6. Cuando se produce un fallo (por ejemplo, entre LSR5-LSR6) se restaura el tráfico en el mismo punto usando la ruta de respaldo local.

3.1.3.5.3 Método inverso

La principal idea de este método es devolver el tráfico al nodo inicial (*ingress node*) usando un backup inverso desde el punto donde se produce el fallo. Así se evitan las pérdidas de paquetes.

La principal desventaja es que tiene un tiempo de restauración igual al del método global. Además, necesita introducir una nueva ruta de respaldo, con lo cual la utilización de los recursos es aún peor que en el método global. Su única ventaja es que disminuye la pérdida de paquetes y simplifica la notificación del fallo.

La figura 11.c muestra un ejemplo de utilización del método inverso. Se establecen los caminos de trabajo y respaldo igual al modelo global y además añadimos una ruta de respaldo inversa desde LSR5 (LSR5-LSR3-LSR1) hacia el *ingress node*. Cuando se detecta un fallo en el LSP (LSR5-LSR6), el tráfico se desvía hacía el LSR1 (*ingress node*) a través de la ruta de respaldo inversa; una vez allí, el modelo se comporta igual que el global.

3.1.3.6 Arquitectura del sistema de gestión del ancho de banda y protección

En esta sección describimos la arquitectura básica del módulo a desarrollar y sus principales dependencias funcionales. Sus componentes básicos son: el módulo de encaminamiento el módulo de gestión de recursos.

A partir de la red física y de la definición de tráfico inicial, el módulo de encaminamiento con calidad de servicio configurará una topología de red lógica inicial. Para ello se deben utilizar algoritmos de encaminamiento que establezcan tanto la ruta de trabajo como la de respaldo; de esto se encargará el módulo de encaminamiento. Ambos caminos deben asegurar la calidad de servicio acordada con los usuarios. La obtención de estos caminos no es simple, y se debe establecer un compromiso entre la eficiencia en la utilización de los recursos de red y la velocidad de respuesta a las peticiones de conexión que impliquen la evaluación de nuevas rutas.

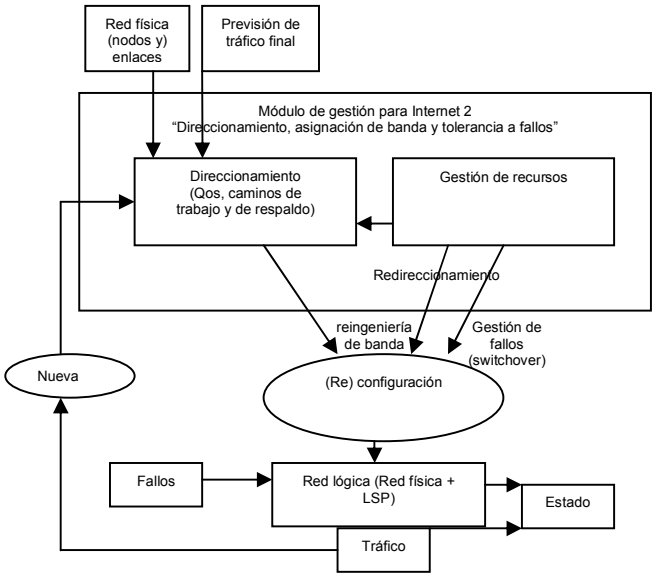
Las técnicas conocidas que obtienen los mejores resultados son inapropiadas para respuestas dinámicas o bajo demanda (*on-line*). El establecimiento de ese equilibrio es uno de los objetivos de esta arquitectura. Básicamente este módulo tiene en cuenta tanto los parámetros de calidad de servicio del encaminamiento de caminos de trabajo: maximización de los recursos, optimización del número de peticiones aceptadas y balanceo de la carga, como los de las rutas de respaldo: pérdidas de paquetes, tiempos de respuesta ante fallos y utilización de recursos.

El módulo de reconfiguración actúa simplemente de interfaz entre el módulo de encaminamiento, el de gestión de recursos y la red real. Utilizará los procedimientos estandarizados más adecuados al escenario propuesto. En este sentido, resulta muy interesante la posibilidad de programar este módulo de configuración para que pueda interactuar con los nodos de una red real usando el protocolo de gestión SNMP (*simple network management protocol*). Este protocolo es el estándar de gestión en IP y lo soportan prácticamente todos los *routers* y conmutadores.

El módulo de gestión de recursos observa de manera continua el estado de la red. Éste está compuesto, entre otros, por los siguientes parámetros:

- Ocupación de cada LSP (banda utilizada)
- Retraso
- Pérdidas
- Probabilidad de bloqueo ante la petición de nuevas conexiones
- Caídas de enlaces y nodos

Figura 12. Arquitectura del SGBP.



En función del estado de la red, el módulo de gestión de recursos puede "decidir" acciones de reconfiguración de la red que podemos resumir en las tres siguientes:

1. Reasignación de banda. A partir de un análisis del estado de la red, se decide que la acción a tomar es la de reasignar banda (o bien tomándola del conjunto de banda residual disponible, o bien tomándola de caminos donde no se utiliza exhaustivamente, *preemption*). La acción se lleva a cabo reconfigurando la red de forma directa.
2. Reencaminamiento. Un problema detectado puede ser de características tales que no tenga solución mediante una reasignación de banda y se debe modificar la topología de la red. En este caso, debe intervenir el módulo de encaminamiento. Aquí caben dos estrategias:

a) recalcular todas las rutas para obtener una nueva solución al sistema, o
b) obtener una solución al problema de forma rápida y con el mínimo de cambios en la topología. Aquí aparece de nuevo el compromiso entre eficiencia en la utilización de recursos y una respuesta más ágil (simple) al problema.

3. Gestión de fallos de red (funciones de *switchover*). Esta acción se corresponde con la detección de una caída de un enlace (o nodo). La casuística aquí es muy variada, desde la simple activación de las tablas de encaminamiento hacia los caminos de respaldo previamente establecidos y con banda asignada, pasando por la captura de banda y nuevos encaminamientos si fuera necesario. La característica principal de estas funciones es que deben dar una respuesta rápida. Estos aspectos son objeto de investigación del proyecto, como se detallará más adelante.

El módulo de encaminamiento se basa en modelos complejos pero generalmente bien definidos, mientras que para el módulo de gestión de recursos podrán utilizarse diversas técnicas que permitan solucionar la toma de decisiones.

3.2 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).

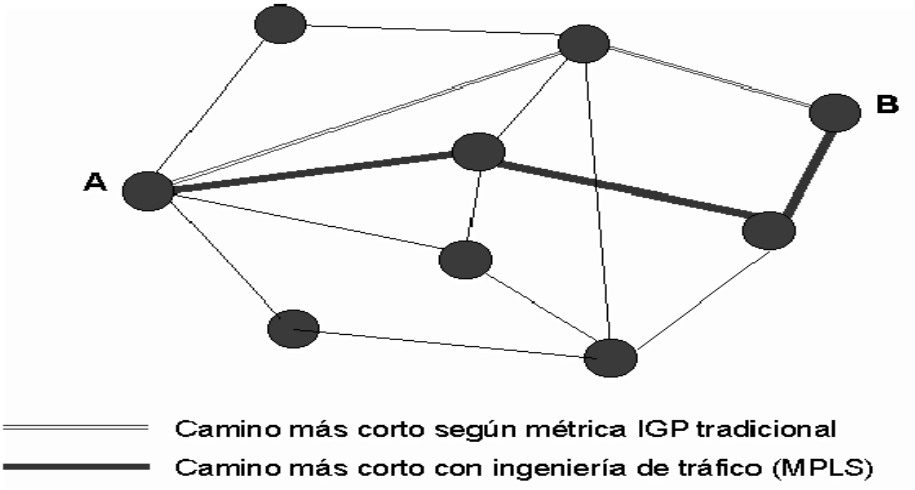
3.2.1 Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén 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 la gráfica siguiente se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

Figura 13. 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. 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.

3.2.2 Clases de servicio (CoS)

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

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que el tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.

- Entre cada par de LSR exteriores se pueden aprovisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico *best-effort*, tres niveles de servicio, primero, preferente y turista, que, lógicamente, tendrán distintos precios.

3.2.3 Redes privadas virtuales (VPNs)

Una red privada virtual (VPN) se construye basada 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 vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

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

Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores 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 IPSec10 del IETF.
- En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un NSP.

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

Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

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

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

- Están basadas en conexiones punto a punto (PVCs o túneles).
- La configuración es manual.
- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.

Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales. La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

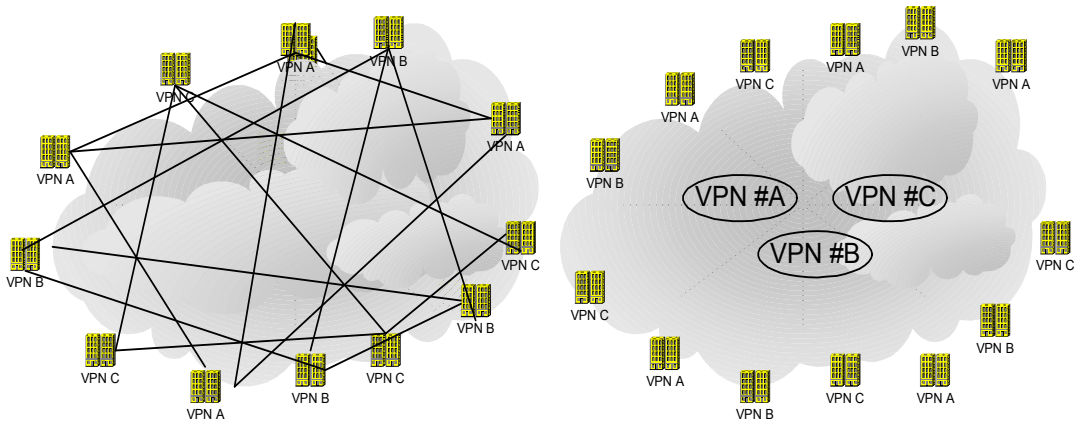
El problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, basados en túneles extremos a extremo (o circuitos virtuales) entre cada par de *routers* de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad 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 14. Modelo "superpuesto" (túneles/PVCs) vrs. modelo "acoplado" (MPLS).



En la figura 14 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) es 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 garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación, etc.), lo que es necesario para un servicio completo VPN.

3.2.4 Calidad de servicio (QoS)

En las aplicaciones de vídeo stream o vídeoconferencia multipunto es necesario cumplir los requerimientos de QoS: ancho de banda asignado para el vídeo y tener acotado el delay máximo para la voz. Para hacer multidifusión con calidad de servicio a través de MPLS, necesitamos desarrollar dos componentes: un encaminamiento con calidad de servicio para determinar la ruta según la métrica considerada (por ejemplo, mínimo número de saltos o ancho de banda residual) y un algoritmo de señalización que nos permita reservar los recursos demandos por la petición. En el encaminamiento explícito (como también ocurre en el encaminamiento en el origen) el LSR origen dispone de la lista de nodos por los que se construirá el ERLSP.

A través de los mensajes de establecimiento de etiquetas (LABEL_REQUEST) se indican cuáles son los nodos que forman parte del LSP en la trayectoria desde el LSR origen hasta el LSR destino. Algoritmos de encaminamiento basados en origen como IP, en casos concretos pueden proporcionar rutas congestionadas cuando pueden haber otras que estén infrautilizadas. MPLS mediante el encaminamiento explicito proporciona las herramientas para evitar este tipo de situaciones. Aparte de esta característica podemos utilizar el protocolo de señalización CR-LDP o RSVP-TE ajustado a multidifusión, para que los recursos puedan ser reservados a lo largo de distintos LSPs y de esta manera asegurar calidad de servicio (QoS).

En las simulaciones que se presentan en el apartado siguiente, la QoS se obtiene reservando un ancho de banda en cada uno de los canales que conforman los distintos LSPs que conducen la información.

3.3 Costo de beneficio de MPLS

- MPLS emplea IP como direccionamiento de nivel 3.

- Hace uso de los protocolos de routing IP heredados. Mediante ellos, MPLS dispone de un conocimiento preciso del estado de la red.

- Se habilitan mecanismos de señalización, su empleo siempre precederá al establecimiento de una comunicación extremo-extremo. LDP y RSVP son los protocolos de señalización elegidos.

- Cada conexión transita por un trayecto virtual extremo a extremo. Este trayecto es pactado y establecido según el estado de la Red y las necesidades de la conexión.

- El proceso de forward no actúa sobre el contenido de nivel 3 de cada paquete. Se añade una etiqueta a cada paquete, en función de ésta se realiza el forward. La interpretación y sustitución de cada etiqueta se circunscribe a un ámbito local, es decir, en cada conmutador MPLS.

- MPLS añade al routing IP capacidades TE orientadas a recursos. Estos protocolos de routing se establecen como plano de control.

- MPLS añade a IP un nivel orientado a la conexión

- IP dispondrá de señalización TE orientada a tráfico (RSVP-TE) o clase de servicio (CR-LDP).

- En MPLS se acelera y simplifica el proceso de Forward

- El proceso de Forward se abstrae de los niveles superiores. Permitiendo desarrollar MPLS en los actuales conmutadores ATM, Frame Relay, Ethernet y, por supuesto, routers/switches IP.

4. CASO DE ESTUDIO DE LA ESTRATEGIA DE IMPLEMENTACIÓN DE PROTOCOLO MPLS EN GUATEMALA

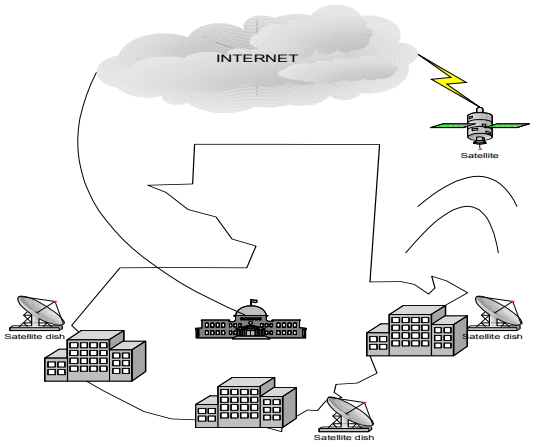
4.1 Explicación del escenario de Guatemala

En Guatemala existe una gran necesidad de establecer un medio de comunicación entre el gobierno central y sus demás corporaciones descentralizadas, a las cuales se les llama municipalidades, de esta forma nos referiremos a ellas de aquí en adelante en el contenido de este capítulo.

Tal necesidad es porque el gobierno necesito conocer la información sobre el nivel de ingresos y egresos y así llevar un mayor control del manejo de los fondos municipales.

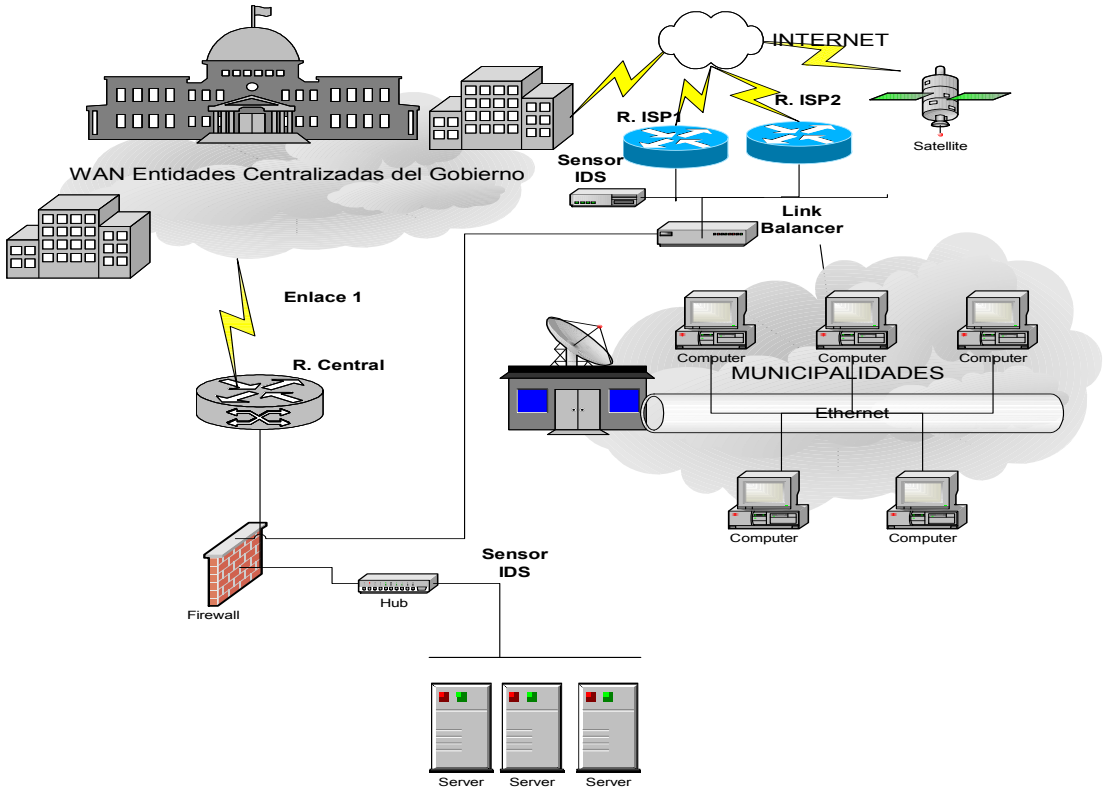
Lo que necesitan es una red tecnológica en la que podamos hacer envío de datos y, además, prestar otros servicios como voz, imágenes, etc. Para esto mostraremos cómo quedaría el diseño de una red ATM para el transporte de información y el diseño de una red MPLS para el manejo de caminos a seguir en nuestra red.

Figura 15. Mapa de Guatemala



Para realizar el estudio nos basaremos solamente en 7 municipalidades.

Figura 16. Diseño de red tecnológica para la comunicación de municipalidades



Como vemos en la gráfica anterior, toda la información importante de las municipalidades es almacenada en unos servidores de base de datos por medio de una conexión satelital. En ésta se podrá manejar buena cantidad de información en tiempo real utilizando la mejor y más innovadora tecnología. Cada transacción que realicen las municipalidades será mostrada al gobierno central y demás entidades interesadas, como el Instituto Nacional de Estadística, el Registro Civil o el Tribunal Supremo Electoral para llevar un control de gastos.

4.2 Consideraciones de las herramientas para la implementación

Entre las herramientas y dispositivos para la implementación de esta red de comunicación entre las municipalidades de Guatemala, tenemos como principales elementos los siguiente:

- Router series 7600 de cisco

  Soporta MPLS y VPN, esto nos servirá para crear nuestro domino MPLS.

- Internet

  Como mínimo necesitamos que nos provean de este servicio 2 ISP's.

- Link Balancer

  Para compartir la carga de las peticiones de ancho de banda y tener redundancia en el servicio de Internet.

- Contratar un servicio satelital

  Para el servicio de envío de datos en municipalidades muy alejadas que necesiten obtener alguna información, o bien para enviar información de importancia al gobierno central.

- Router ATM cisco

  Para soportar el dominio ATM en el uso interno entre municipalidades del mismo departamento.

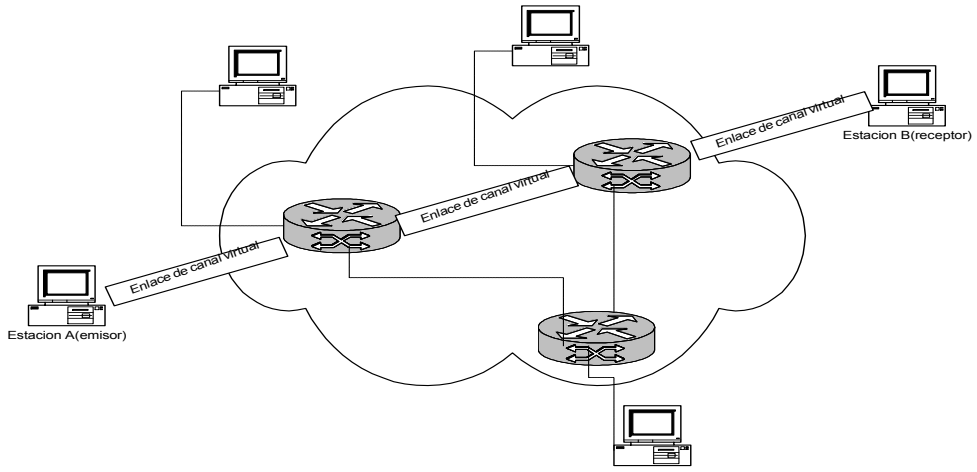
- Cableado de red listo.

- Id Sensor

  Para detectar intrusos que quieran usurpar la nuestra red.

4.3 Arquitectura ATM a utilizar

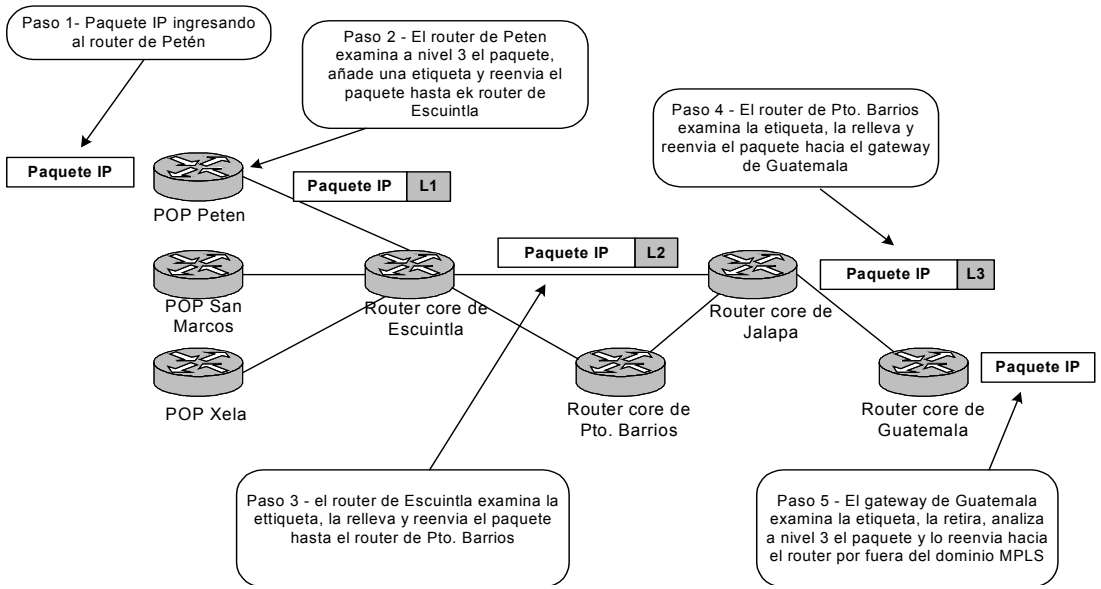
Figura 17. Arquitectura ATM a utilizar



Esta arquitectura se utilizará para la comunicación entre las entidades municipales de un mismo departamento, en la cual podremos tener los servicios de voz, datos e imágenes entre las municipalidades. Cada departamento de Guatemala será un dominio comunicado por ATM y que luego se comunicará a otro Router MPLS para su comunicación con el gobierno.

4.4 Arquitectura MPLS a utilizar

Figura 18. Dominio MPLS entre Router de las ciudades de Guatemala

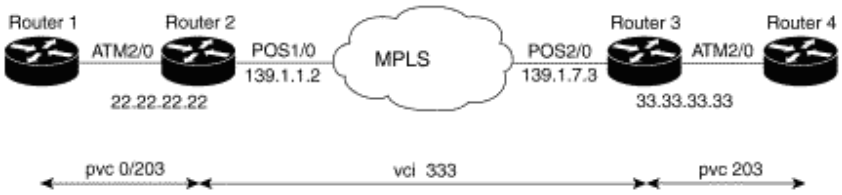


Como se puede observar en las 7 ciudades que nos servirían para demostrar nuestra red de comunicación, la información llega por paquetes y se le agregan etiquetas en cada router de la ciudad en que se encuentra, hasta llegar a la salida del dominio MPLS y así enviar información o traerla de un determinado lugar.

4.5 Ejemplo de configuración entre router ATM y MPLS

Esquema de configuración entre municipalidades. Una municipalidad será un router ATM queriendo comunicarse con otro router MPLS, pasando por un túnel o una VPN de MPLS para la comunicación entre diferentes municipalidades. Para una mejor apreciación, veamos la forma de configurar este esquema:

Figura 19. Ejemplo de configuración entre router ATM y MPLS



Configuración de ATM sobre túneles de MPLS:

A continuación veremos los forma de configuración entre los router 2 y router 3 que se encuentra sobre el dominio MPLS, en la cual podemos tomar el router de Escuintla y el router de Puerto Barrios, y el router 1 y el router 2 que están sobre el dominio ATM:

Configuración del Router 2

interface Loopback0 !Configuración interface loopback

ip address 22.22.22.22 255.255.255.255

interface Tunnel33 !Configuración dinámica del túnel del Router 3.

mpls atm-transport !activación del transporte ATM al otro lado del túnel.

mpls label protocol ldp !Usar la etiqueta LDP para el túnel.

tunnel destination 33.33.33.33 !Especifica como túnel destino el loopback del router 3

tunnel source Loopback0

tunnel mode mpls dynamic !Crea un túnel dinámico MPLS

tunnel key 2233 !Especifica el identificador del túnel

interface ATM2/0

pvc 0/203

atm route interface tunnel33 333 !Rutea pvc 0/203 en el Tunel33 con

!vci 333 al otro lado del dominio de MPLS.

interface POS1/0 !Configura la interface del dominio MPLS.

ip address 139.1.1.2 255.255.255.0

mpls ip !Activa el switcheo dinámico de MPLS

mpls label protocol ldp !Utiliza etiqueta LDP de distribución. Asume que el router está

!usando la interface LDP.

router ospf 10 !Configura ruteo OSPF

passive-interface Loopback0

network 22.22.22.22 0.0.0.0 área 0

network 139.1.1.0 0.0.0.255 área 0

Configuracion del Router 3

interface Loopback0 ! Configuración interface loopback

ip address 33.33.33.33 255.255.255.255

interface Tunnel22 ! Configuración dinámica del túnel del Router 2.

mpls atm-transport ! activación del transporte ATM al otro lado del túnel.

mpls label protocol ldp ! Usar la etiqueta LDP para el túnel.

tunnel destination 22.22.22.22 ! Especifica como túnel destino el loopback del router 2

tunnel source Loopback0

tunnel mode mpls dynamic ! Crea un túnel dinámico MPLS

tunnel key 2233 ! Especifica el identificador del túnel

interface ATM1/0

pvc 0/203

atm route interface tunnel22 333 ! Rutea pvc 0/203 en el Tunel22 con

!vci 333 al otro lado del dominio de MPLS 333.

interface POS2/0 ! Configura la interface del dominio MPLS.

ip address 139.1.7.3 255.255.255.0

mpls ip ! Activa el switcheo dinámico de MPLS

mpls label protocol ldp ! Utiliza etiqueta LDP de distribución. Asume que el router está

!usando la interface LDP.

router ospf 10 ! Configura ruteo OSPF

passive-interface Loopback0

network 33.33.33.33 0.0.0.0 área 0

network 139.1.7.0 0.0.0.255 área 0

Configuración de una municipalidad o un router ATM en el PVC para la comunicación con los router MPLS.

Configuración del Router 1

interface ATM2/0

no ip address

no ip directed-broadcast

no ip route-cache

no ip mroute-cache

no shut

no atm enable-ilmi-trap

no atm ilmi-keepalive

interface ATM2/0.100 point-to-point

ip address 1.0.0.2 255.255.255.224

no ip directed-broadcast

no ip route-cache

no ip mroute-cache

no shut

no atm enable-ilmi-trap

pvc 0/203

broadcast

4.6 Plan de implementación

Este plan contará con 4 pasos generales, los cuales son los siguientes:

- Paso 1: Preparación.
  - Pruebas extensivas en laboratorio (pruebas de regresión, funcionalidades)
  - Revisar el hardware y software en todos los enrutadores de la red, para que soporten MPLS, LDP, VPN.
  - Enrutamiento: IGP (protocolo de estado de línea), BGP (BGP4 con soporte a multiprotocolo BGP).

- Paso 2: Habilitar MPLS en el dominio
  - Habilitar MPLS en todos los enrutadores.

- Paso 3: Conectividad MPLS, ATM, CPN básica
  - Habilitar MBGP entre los enrutadores que brindaran el servicio de túnel.

- Paso 4: Habilitar calidad de servicio en toda la red
  - Mecanismos de sheduling
  - Mecanismos de encolamiento
  - Mecanismos de prevención y recuperación de congestión

4.7 Beneficios con los que contarán las municipalidades de Guatemala

Un protocolo ATM siempre ha sido usado para transferencia de datos, imagen y, su mayor ventaja, para la difusión de voz por medio de una red de este tipo a altas velocidades de transferencia. Además MPLS sería un canal de comunicación hacia los departamentos o hacia el.

Si en caso se realizara una red gubernamental, se obtendrían los siguientes beneficios:

- Transferencia de datos más eficiente, rápida y segura por medio de ATM entre municipalidades de un departamento.

- Transferencia de imágenes, por ejemplo, del desarrollo de algún proyecto local que quisieran conocer otras municipalidades, para evitar así los gastos que inciden en hacer un viaje largo y el tiempo que se pierde en viajar.

- Para el caso de las comunicaciones entres municipalidades, el servicio más importante sería la comunicación por voz y vídeo, en las que se ahorrarían muchos recursos económicos, ya que el gobierno podría tener su propia red.

- Debido a que entablar una red pura con ATM sería muy costoso para la comunicación de la red gubernamental con las redes exteriores (Internet), se incluye MPLS, que es el mecanismo en el que nos podremos comunicar con cualquier otro protocolo sin incurrir en mayores costes, creando una red privada virtual para la comunicación entre los departamentos de Guatemala.

- Los departamentos de Guatemala solamente realizarán su red ATM local por departamentos, y la comunicación entre ellos se hará a través de un proveedor de Internet que proporcione el servicio de enrutadores MPLS, con el cual tendremos comunicación permanente de forma segura.

- Se podrán manejar vídeoconferencias, llamadas de voz, transferencias de datos en tiempo real. Conforme pase el tiempo, esta red será cada día de más utilidad, pues reduciría los costos de asistir a reuniones en algunos puntos de Guatemala cada cierto tiempo y se podrían tener congresos virtuales, capacitaciones a personal a distancia, etc.

- Con esta tecnología, Guatemala no sólo estará completamente comunicada hacia ella misma, sino al exterior, para intercambiar conferencias de capacitación, motivación, etc.

- La inversión al principio del proyecto de comunicación será grande, pero con el tiempo se recuperaría gracias a los beneficios obtenidos.

El siguiente ejemplo nos ilustra de la manera como una inversión puede ser recuperada.

Para esta explicación se utilizaran datos reales analizados de las páginas públicas del Instituto Nacional de Estadística. Como sabemos, Guatemala cuenta con 331 municipios. Esta entidad necesita información de la población de cada uno de ellos para efectuar estudios de diferente índole, como los datos del registro civil.

Actualmente, sin arquitectura de comunicaciones	**Después, utilizando la nueva arquitectura de comunicaciones**
Cada municipio es el responsable de recabar información sobre los nacimientos, defunciones y mortinatos, posteriormente deben llenar un boletín estadístico y luego esperar a que se presente personal del I.N.E. para llevarse dichos formularios hacia la cede central.	Los responsables de cada municipio tendrán que capturar la información, pero ahora la información importante viajará replicada a la cede central del I.N.E. para su procesamiento en tiempo real, y así se evitará todo el tiempo que se pierde en viajar al interior de la república.
Los formularios por departamento no siempre están completos, ya que no todos los municipios tienen listos los boletines para el I.N.E.	En el momento que se estén realizando las inscripciones y creen el mismo boletín, se estarán enviando a la institución interesada para que ya no existan retrasos.
Cada uno de los registradores civiles de cada municipio recibe e ingresa los nacimientos, defunciones y mortinatos como ellos lo crean conveniente, sin tener un amplio conocimiento de las leyes del Código Civil.	Con la nueva arquitectura se podrá dar capacitaciones a distancia, para todos los registradores civiles a través de vídeoconferencia.
La información de cada municipio se puede perder por cualquier accidente, incendio, ataque terrorista a la información, sin posibilidades de recuperarla.	Con esta arquitectura podremos tener una réplica de la información más importante de cada municipio, que se encontrará almacenada en la sede central de la institución y podremos consultar en tiempo real la información.

No se cuenta con un medio adecuado para resolver una duda en el momento de hacer una inscripción, por la cual los registradores la ingresan según lo creen conveniente, afectando directamente a las estadísticas reales.	Ahora podremos tener comunicación directa con personal calificado del I.N.E. que podrá resolver dudas de los registradores civiles o encargados ya sea por voz, imágenes o vídeo.
Los municipios no tienen una estrecha relación con entidades descentralizadas del gobierno, en consecuencia son olvidados y no se les presta mucha ayuda.	Con esta tecnología y la capacidad de captar y procesar información rápidamente, la institución sabrá qué comunidades son las más necesitadas de hospitales, escuelas, etc. De acuerdo a su tasa de natalidad, tasa de defunciones. Y así enviar ayuda inmediatamente a estas poblaciones.
Actualmente, el I.N.E. tiene un atraso de 2 años para entregar estadísticas de toda la nación, la cual es obsoleta al momento de entregarla.	Esto se resuelve con el proyecto de comunicación ya que el procesamiento de datos es en tiempo real, pudiendo tomar decisiones en cualquier momento, para reforzar algo que se este haciendo mal o que haga falta en las comunidades.
Las estadísticas no representan la realidad, ya que muchas comunidades se encuentran en el área rural lejos de cualquier medio de comunicación y esta información se pierde.	Ahora todas la comunidades alejadas de cualquier medio de comunicación podrán enviar sus datos con igual eficiencia que los municipios más grandes, ya que se contará con enlaces satelitales para aquellas comunidades.

Como se observa en la comparación, toda la inversión se recupera a través de la información recopilada en la república, y así se provee de mayores y mejores servicios a las comunidades mas necesitadas.

- Las municipalidades de Guatemala, al tener esta infraestructura, podrían sacarle provecho realizando talleres a distancia para vecinos de su localidad, para así entablar un mejor camino hacia el desarrollo, suministrando de información técnica, cultural, y tecnológica actualizada a sus comunidades.

CONCLUSIONES

1. Sabemos que una de las ventajas más grandes que tiene ATM es la transferencia de vídeo y voz con una calidad y velocidad muy eficiente.

2. Unas de las ventajas más importantes de MPLS es la comunicación con cualquier protocolo que exista en el mercado, así como el óptimo manejo de paquetes ip, cuestión que se hace muy difícil con el protocolo ATM.

3. Con el protocolo ATM resulta muy difícil y tedioso comunicarse con otros protocolos, además de bajar en el rendimiento del mismo, en cambio con MPLS esto se hace muy sencillo ya que lo hace de forma dinámica.

4. Utilizando esta arquitectura de comunicación, Guatemala, tendrá mayores posibilidades de alcanzar el desarrollo, ya que se realizará con transparencia la utilización de recursos del Estado, tanto en las entidades centralizadas como descentralizadas.

5. Con la creación de su red gubernamental, se obtendrá más seguridad en el cambio de información tanto en entidades centralizadas como descentralizadas.

6. Para un proyecto de comunicación tan grande debe hacerse un estudio de la inversión inicial requerida, para definir si el país tiene el suficiente capital para invertir, de lo contrario necesitará solicitar ayuda internacional para su elaboración.

7. La capacitación a distancia es uno de los servicios más requeridos en la actualidad, por su bajo costo y la capacidad de llegar a lugares muy apartados de la civilización.

8. Por la situación deficiente que tiene el gobierno de Guatemala en sus comunicaciones, es necesario realizar un proyecto de comunicación tecnológica, para que así el país se pueda retroalimentar con la información de todas las entidades que lo conforman y agilizar muchos de los procesos que en estos momentos se llevan meses y hasta años en finalizarse.

9. Para la construcción de una infraestructura ATM/MPLS en Guatemala, se debe tomar en cuenta una buena administración de calidad de servicio para aquellos procesos que deban estar siempre activos, así como un buen control de ingeniería de trafico para resolver procesos en el menor tiempo.

10. Siendo el gobierno de Guatemala una entidad centralizadora de información y contando con entidades descentralizadas geográficamente, el proyecto de comunicación debe incluir a todos los departamentos del país para su éxito.

RECOMENDACIONES

1. Verificar que la empresa nos vaya a proveer de servicios de Internet, tenga dentro de sus servicios comunicación satelital, para así no dejar aisladas a las comunidades que se encuentran muy alejados.

2. Debe considerarse, antes de realizar inversiones en infraestructura, la cantidad de beneficios que se obtendrán, para validar si un cambio en la comunicación nos brindará más ganancias que pérdidas de información.

3. El gobierno de Guatemala debe de verificar que la empresa proveedora de servicios de Internet cuente en su infraestructura con enrutadores MPLS, para que no se tengan problemas de comunicación con otras redes.

4. Se debe adquirir equipo con posibilidades de expansión, ya que la tecnología actual avanza muy rápidamente.

5. La comunicación entre entidades tanto centralizadas como descentralizadas de gobierno debe ser promovida, para hacer más productivo al país.

BIBLIOGRAFÍA

1. TENENBAUM, Andrew. Redes de Computadoras. 3ª. Ed., México: Editorial Prentice Hall Hispanoamérica, S.A., 1997

2. BLACK, Uyless. Tecnologías Emergentes para Redes de Computadoras. 2ª. Ed., México: Editorial Prentice Hall Hispanoamérica, S.A., 1997

3. Conmutadores MPLS. http://www.riverstonenet.com/pdf/spanish_ rs38k.pdf, 2002

4. Conmutadores ATM. Revista Electrónica http://www.mundo-lectronico.com/ PDF/Any1999/300_julio/Conmutacion.pdf, 1999

5. LARCES.Tutorial de MPLS. http://www.larces.uece.br/tutoriais /MPLS_MARCIO_TUTORIAL.PDF, 2002

6. Unitronics. Tecnología ATM, España. http://www.comunicaciones.unitronics .es/tecnologia/atm.htm 2001

7. Evolución MPLS. http://www.inf.utfsm.cl/~jcanas/SistemasCom/Apuntes /Capitulo5.pd 2002

8. Andrikopoulos-I, Pavlou-G. Supporting differentiated services in MPLS networks. Seventh International Workshop on Quality of Service. IWQoS'99. (Cat.No.98EX354). Piscataway, NJ, USA. 1999

9. Armitage-G. MPLS: the magic behind the myths [multiprotocol label switching]. IEEE Communications Magazine. Enero, 2000. Volumen 38. Número 1.

10. Arup-Acharya, Griffoul-F, Ansari-F. IP multicast support in MPLS. IEEE ATM Workshop '99 Proceedings (Cat. No. 99TH8462). Tokyo, Japón, 1999.

11. Awduche-DO. MPLS and traffic engineering in IP networks. IEEE Communications Magazine. Diciembre, 1999. Volumen 37. Número 12.

12. José Barberá. MPLS: Una arquitectura de backbone para la Internet del siglo XXI. Boletín RedIRIS. Septiembre, 2000. Nº 53.

13. Brittain, Farrel. MPLS Virtual Private Networks. Data Connection. Noviembre, 2000.

14. Ghanwani-A, Jamoussi-B, Fedyk-D, Ashwood-Smith-P, Li-Li, Feldman-N. Traffic engineering standards in IP-networks using MPLS. IEEE Communications Magazine. Diciembre, 1999. Volumen 37. Número 12.

15. Holness-F, Griffiths-J. Multiprotocol label switching within the core network. British Telecommunications Engineering. Agosto, 1999. Volumen 18.

16. Li-T. MPLS and the evolving Internet architecture. IEEE Communications Magazine. Diciembre, 1999. Volumen 37. Número 12.

17. Stephenson-A. Diffserv and MPLS: a quality choice. Data Communications International. Noviembre, 1998. Volumen 27. Número 17.

18. Swallow-G. MPLS advantages for traffic engineering. IEEE Communications Magazine. Diciembre, 1999. Volumen 37. Número 12.

19. Xipeng-Xiao, Hannan-A, Bailey-B, Ni-LM. Traffic engineering with MPLS in the Internet. IEEE Network. Abril-Marzo, 2000. Volumen 14. Número 2.