UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PROYECTOS DE COMUNICACIONES WAN SOBRE BACKBONE MPLS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

OSCAR ANÍBAL, JAIMES JAIMES

PROMOCIÓN
1991 - II
LIMA – PERÚ
2006

PROYECTOS DE COMUNICACIONES WAN

SOBRE BACKBONE MPLS

Dedico este trabajo a:

Mi Padre y en memoria a mi Madre, inspiración plena

de lucha y sacrifico,

Mis Hermanos, por el apoyo incondicional en mi carrera,

SUMARIO

El presente trabajo describe plataformas de comunicaciones de redes de área extensa WAN (*Wide Area Network*) soportado en la arquitectura MPLS (*Multiprotocol Label Switching*), tecnología que se ha impuesto como la dominante en el ámbito de la conectividad de redes.

En el capitulo I se presenta una visión acerca de requerimientos de comunicaciones de las empresas enfocado hacia la interconexión de sus oficinas centrales con las oficinas remotas.

En el capitulo II se introduce al concepto teórico que soporta a las plataformas de comunicaciones, partiendo de la definición de comunicación de datos hasta los protocolos de comunicaciones base del *backbone* de las redes de las empresas proveedoras de servicios de telecomunicaciones (*Service Provider*), que finalmente nos lleva hasta el protocolo MPLS (*Multiprotocol Label Switching*), soporte de los proyectos de comunicaciones de redes en la actualidad.

El capitulo III resume criterios de diseño para redes WAN identificando requerimientos técnicos, para implantar la alternativa MPLS como *backbone* de las plataformas de comunicaciones.

En el capitulo IV se describe la ingeniera que involucra plantear una solución técnica de redes WAN sobre la arquitectura MPLS, enfocado a un caso de estudio para una entidad financiera a nivel nacional.

Asimismo se enumera determinadas condiciones comerciales que se asocian a una propuesta de Red WAN previa a la implantación del proyecto y se da a conocer las responsabilidades a que están sujetas las empresas.

Finalmente se describen las conclusiones y las recomendaciones.

ÍNDICE

PRÒLOGO

El hombre en su afán de comunicarse entre sí, ha empleado diversos medios desde las señales de humo hasta lo que hoy día llamamos la maravilla de la red de redes, Internet.

Las telecomunicaciones en la actualidad han alcanzado un gran desarrollo que permite brindar servicios cubriendo mayor parte de las necesidades de usuarios y empresas. Contribuye a ello la rápida evolución de los dispositivos electrónicos, la arquitectura computacional y el desarrollo de programas de control de procesos e interconexión de dispositivos; lo que en la actualidad nos trae nuevas redes de comunicaciones y la ampliación de cobertura de las mismas.

Fundamentalmente la investigación actual va encaminada al desarrollo de una red única, capaz de soportar simultáneamente todos los servicios de voz, datos y video con suficientes garantías para la calidad de servicio y tiempo de respuesta a las distintas aplicaciones y que permita la conexión a ella de todas las redes ya existentes, tanto de área local como de área extensa.

La evolución del sector de las telecomunicaciones, es resultado de la conjunción de los avances tecnológicos, la gran expansión de las aplicaciones de las tecnologías de la información, las economías de escala y las caídas de precios de las redes de acceso representan el factor fundamental que permiten explotar a fondo esta evolución.

En razón de ello existe una fuerte tendencia a la convergencia de las redes de datos con las redes de telefonía, en definitiva de las redes de conmutación de circuitos (telefonía) con las redes de datos (conmutación/encaminamiento de datos). Anteriormente existió la convergencia de ambas redes a nivel de los enlaces de transmisión y de los accesos. Se usaban ambos elementos de las redes para transportar datos y telefonía simultáneamente y restaba unificar bajo una misma plataforma los nodos de distribución y acceso.

Una red de nueva generación es una red funcional multiservicios basada en tecnología IP, producto de la evolución de las actuales redes. Con la posibilidad

de ofrecer servicios diferenciados y acordes a la calidad de servicio demandada por las aplicaciones del cliente.

En medio de dicho contexto se presenta la arquitectura de red basada en el Protocolo MPLS (*Multiprotocol Label Switching*) el cual es un método para enviar ("*forwardear*") paquetes a través de una red usando información contenida en etiquetas añadidas a los paquetes IP, su primer objetivo era crear redes flexibles y escalables con un incremento en el desempeño y la estabilidad, esto incluye ingeniería de tráfico y soporte de redes privadas virtuales (VPNs), ofreciendo calidad de servicio con múltiples clases de servicio.

Este protocolo es la base de los *backbones* de comunicaciones de las redes de una empresa proveedora de servicios de telecomunicaciones, (*carriers* o *service providers*).

En el presente informe mostraremos un caso de estudio sobre un proyecto donde se ha diseñado e implantado una plataforma de comunicaciones WAN soportado en el *backbone* MPLS de las empresas proveedoras.

CAPITULO I
RESUMEN EJECUTIVO

1.1 Descripción del Problema.

Estando inmersos en la era de la actualización tecnológica y transición a nuevas plataformas, en el ámbito de las redes de las empresas, existe la necesidad de una continua mejora en la calidad y confiabilidad de las comunicaciones, enmarcado a soportar nuevas aplicaciones tecnológicas para el usuario final. En el presente informe de suficiencia profesional presentamos la evolución de las plataformas de comunicaciones de las empresas, para brindar servicios de ultima generación, robustos, confiables y escalables dando respuesta a necesidades de:

- Implantación de nuevas aplicaciones
- Reingeniería de las aplicaciones actuales
- Reingeniería de los procesos
- Aplicación de las políticas de reducción de costos.
- Incremento de anchos de banda con respecto a servicios actuales.
- Disminución de horas perdidas por caída en los sistemas.
- Disminución del costo de larga distancia nacional para el tráfico de voz.
- Ahorro en los enlaces privados.
- Aumento del numero de oficinas remotas.
- Mejora de la productividad a través del uso de nuevas aplicaciones.
- Mejor información para toma de decisiones oportunas.
- Mejores y más servicios a los ciudadanos.
- Incremento en el beneficio social al poder prestar los servicios de mejor manera en más lugares.

Como base del diseño de redes de última generación surge el protocolo de comunicaciones MPLS en los *backbones* de comunicaciones de las empresas proveedoras (*Carriers o Service Providers*), hacia el cual convergen los accesos de ultima milla, que en conjunto conforman las redes de área extensa WAN (*Wide Area Network*) para atender a las empresas clientes de las empresas proveedoras

de telecomunicaciones. Dichas redes permiten trasmitir tráfico de voz, datos y video. Los *carriers* o *service provider* en su afán de estar a la vanguardia del desarrollo tecnológico, están implantando la infraestructura que será su herramienta para impulsar las redes de banda ancha y contar con accesos por distintos medios de comunicaciones a los nodos MPLS.

1.2. Objetivos del Trabajo.

El presente informe detalla los alcances, características, operación y ventajas de la formación de redes privadas virtuales (VPNs) IP, en voz y datos que dan origen a intranets de empresas (Clientes de las Empresas proveedoras de Telecomunicaciones), mediante enlaces de comunicaciones soportados en el protocolo de conmutación de etiquetas MPLS. La arquitectura en mención es aplicada en los distintos diseños de soluciones técnicas para plataformas de comunicaciones de empresas. Dichas soluciones técnicas frecuentemente están a cargo de empresas proveedoras de servicio de telecomunicaciones. La cobertura abarca implantar una plataforma de comunicaciones a nivel nacional e internacional en función a la disponibilidad de facilidades técnicas de la arquitectura MPLS de dichos proveedores.

Es preciso tener claro que en los últimos tiempos no solo se viene hablando de la convergencia de los servicios de voz, video y datos sobre una misma plataforma, sino también de la necesidad de la migración de servicios "*legacy*" (heredados) como SNA, ATM y Frame Relay a una nueva generación de redes "*IP based VPNs*" (Redes Privadas Virtuales basadas en protocolo IP) como son las "MPLS VPNs" (Redes Privadas Virtuales basadas en MPLS), con las ventajas de:

- Flexibilidad
- Escalabilidad
- Accesibilidad
- Eficiencia
- Calidad de servicio y clases de servicio
- Administración
- Monitoreo y SLAs (acuerdos de nivel de servicio)
- Fácil migración
- Seguridad
- Bajo costo

Se aúna a dichas ventajas, el que se tenga independencia de equipos de cliente (CPE: *Customer Premise Equipment*), al no requerir hardware costoso para implantar una VPN en el local del cliente y brindar la convergencia, es decir, la integración de distintos servicios y aplicaciones sobre una misma plaforma.

CAPITULO II
PRESENTACIÓN

2.1 Comunicación de datos

Para trasladarnos al escenario de las redes de datos, iniciamos ilustrando la comunicación de datos que es el proceso de comunicar información en forma binaria (unidad más pequeña de información). entre dos o más puntos, que esta formado por cuatro elementos básicos que son:

- Emisor: dispositivo que emite los datos
- Mensaje: lo conforman los datos a ser transmitidos
- Medio: consiste en el recorrido de los datos desde el origen hasta su destino
- Receptor: dispositivo de destino de los datos

Se puede establecer la comunicación a través de un simple cable o a través de una masa compleja de equipos de concentración y conmutación.

El medio que los une a los puntos puede ser:

- Aéreos, que están basados en señales radio-eléctricas (utilizan la atmósfera como medio de transmisión), en señales de rayos láser o rayos infrarrojos.
- Sólidos: principalmente el cobre en par trenzado o cable coaxial y la fibra óptica.

Los tipos de transmisión son clasificados en: simple, *half-duplex* y *full-duplex.* En los tres casos, asociado al sentido de la transmisión de datos y también por el sincronismo en la transmisión, se tiene al tipo asíncrono (donde cada *byte* de datos incluye señales de arranque y parada al principio y al final) y al tipo de transmisión sincronía(donde se utilizan canales separados de reloj que administran la recepción y transmisión de los datos). Al inicio de cada transmisión se emplean unas señales preliminares llamadas bits de sincronización en los protocolos orientados a *bit.* (son aquellos en los cuales los bits por si solos pueden proveer información, trabajan en tramas de longitud variable).

La transmisión de datos entre dos o más computadoras deben efectuarse sobre la base de un conjunto de reglas denominado protocolo de comunicaciones.

También es identificada una arquitectura de niveles: desarrollada con el propósito de reducir la complejidad de la comunicación de datos agrupando lógicamente ciertas funciones en áreas de responsabilidad (niveles). Cada nivel provee servicios al nivel superior y recibe servicios del nivel inferior.

La Organización Internacional de Estandarización (ISO *Internacional Organization for Standardization*) desarrolló un modelo de referencia abierto para la interconexión de sistemas (OSI *Open Systems Interconnection*).

En este modelo, el propósito de cada nivel es proveer servicios al nivel superior, liberándolo de los detalles de implementación de cada servicio. La información que se envía de un computador a otro debe pasar del nivel superior al nivel inferior atravesando todos los demás niveles de forma descendente dentro del computador que origina los datos. A su paso por cada nivel a los datos se les adiciona información que será removida al llegar a su destino. La información adicionada se clasifica en:

- Información de control, dirigida a su nivel correspondiente en el computador de destino. Cada nivel se comporta como si estuviera comunicándose con su contraparte en el otro computador.
- Información de interfase, dirigida al nivel adyacente con el cual se está interactuando. El objetivo de esta información es definir los servicios provistos por el nivel inferior y como deben ser accesados estos servicios. Esta información tras ser empleada por el nivel adyacente es removida.

El modelo OSI se estructura en 7 niveles:

- **Nivel Físico**: este nivel dirige la transmisión de flujos de bits, sin estructura aparente, sobre un medio de conexión. Se encuentra relacionado con condiciones eléctricas-ópticas, mecánicas y funcionales de la interfaz al medio de transmisión. A su vez esta encargado de aportar la señal empleada para la transmisión de los datos generados por los niveles superiores.

  En este nivel se define la forma de conectarse el cable a las tarjetas de red, cuanto pines debe tener cada conector y el uso funcional de cada uno de ellos. Define también la técnica de transmisión a emplear para el envío de los datos sobre el medio empleado. Se encarga de activar, mantener y desactivar un circuito físico. Este nivel trata la codificación y sincronización de los bits y es el responsable de hacer llegar los bits desde un computador a otro.

- **Nivel de Enlace de Datos**: este nivel se encarga, en el computador de origen, de alojar en una estructura lógica de agrupación de bits, llamada trama (*Frame*), los datos provenientes de los niveles superiores. En el computador de destino, se encarga de agrupar los bits provenientes del nivel físico en tramas de datos que serán entregadas al nivel de red. Este nivel es el responsable de garantizar la transferencia de tramas libres de errores de un computador a otro a través del nivel físico.
- **Nivel de Red**: es responsable del direccionamiento de mensajes y de la conversión de las direcciones lógicas y nombres en direcciones físicas. Está encargado también de determinar la ruta adecuada para el trayecto de los datos, basándose en condiciones de la red, prioridad del servicio, etc. El nivel de red agrupa pequeños fragmentos de mensajes para ser enviados juntos a través de la red.
- **Nivel de Transporte**: se encarga de la recuperación y detección de errores. Garantiza también la entrega de los mensajes del computador originados en el nivel de aplicación. Es el nivel encargado de informar a los niveles superiores del estatus de la red.
- **Nivel de Sesión**: permite que dos aplicaciones residentes en computadoras diferentes establezcan, usen y terminen una conexión llamada sesión. Este nivel realiza reconocimientos de nombres y las funciones necesarias para que dos aplicaciones se comuniquen a través de la red como en el caso de funciones de seguridad.
- **Nivel de Presentación**: determina el formato a usar para el intercambio de datos en la red. Puede ser llamado el traductor de la red. Este nivel también maneja la seguridad de emisión, pues provee a la red servicios como el de encriptación de datos.
- **Nivel de Aplicación**: sirve como ventana para los procesos que requieren acceder a los servicios de red.

El desarrollo de las redes informáticas planteó su conexión mutua.

Las redes de área local (LAN *Local Area Network*) han sido creadas para responder a ésta problemática. El crecimiento de las redes locales hizo que cambiase nuestra forma de comunicarnos con los ordenadores y la forma en que los ordenadores se comunicaban entre sí.

La importancia de las LAN reside en que se puede conectar un determinado número de ordenadores que puede ser ampliado a medida que crecen las necesidades.

2.2 Redes de área local (LAN)

Una red de área local es un conjunto de elementos físicos y lógicos que proporcionan interconexión a una gran variedad de dispositivos de comunicación de información en un área privada restringida (recinto, edificio, campus, etc.)

En esta definición formal aparecen los siguientes elementos con significado propio: conjunto de elementos físicos y lógicos que proporcionan interconexión, es decir, son un conjunto de elementos que configuran una red de comunicación que facilita la transmisión de bits entre un dispositivo y otro. Por otra parte, se habla de una gran variedad de dispositivos de comunicación, esto es, a la red pueden conectarse dispositivos de todo tipo tales como computadoras, terminales, periféricos, sensores, aparatos telefónicos, equipos facsímil, etc. Otro aspecto incluido en la definición es el ámbito geográfico de la red local que, en general, es pequeño y no sale más allá de los límites de un departamento situado en un edificio o conjunto de edificios próximos. Por último cabe destacar el carácter privado de una red local que, generalmente, no necesita otros medios de comunicación suministrados por empresas o redes de comunicación.

Las características más representativas de una red de área local son las siguientes:

- **Alcance**. El área de conexión se limita a una extensión moderada, generalmente desde unos pocos metros a unos pocos kilómetros.
- **Velocidad** de transmisión. En estas redes, la velocidad es elevada en comparación con otros circuitos de comunicación, variando entre 1, 100Mbps y 1Gbps.
- **Conectividad.** Los distintos equipos que integran la red se encuentran conectados entre sí con posibilidades de comunicación. Además de que todos los dispositivos conectados a una red de área local puedan comunicarse entre sí, también se incluye la capacidad de conexión con otras redes locales o de área extensa como pueden ser la red telefónica conmutada o las redes SNA, X.25, TCP/IP, etc.

- **Propiedad Privada**. Una red de área local es propiedad de la organización o empresa en lugar de ser un elemento público para otros usos externos. Por lo general, la organización es propietaria de la red y todo el conjunto de dispositivos conectados a ella.
- **Fiabilidad.** Estas redes presentan una baja tasa de error en las transmisiones de datos en comparación con el resto de modalidades de comunicación. Un sistema distribuido de computadoras conectadas en red local es inherentemente más fiable que un sistema centralizado.
- **Compartición de recursos**. Permiten la integración en la misma red de una gran diversidad de dispositivos. Los recursos de almacenamiento, las impresoras y los elementos de comunicación pueden ser utilizados por todas las estaciones de trabajo. Los dispositivos conectados a la red comparten datos, aplicaciones, periféricos y elementos de comunicación
- **Proceso distribuido.** Las redes de área local permiten el trabajo distribuido, es decir, cada equipo puede trabajar independientemente o cooperativamente con el resto.
- **Flexibilidad.** Una red local puede adaptarse al crecimiento cuantitativo referido al número de equipos conectados, así como adaptarse a cambios cualitativos de tipo tecnológico.
- **Cableado estructurado.** Estas redes por sus cableados y conexiones, facilitan mucho la movilidad de los puestos de trabajo de un lugar a otro.
- **Optimización.** Las redes de área local permiten la máxima flexibilidad en la utilización de recursos, estén estos en la computadora central, en el procesador departamental o la estación de trabajo; facilitando, por tanto, la optimización del coeficiente prestaciones/precio del sistema.

Las Redes de Area Local se clasifican en función a la topología en:

- Anillo(*Token Ring*)
- Bus
- Estrella

Y la clasificación en función a la velocidad de transmisión es en:

- Redes Ethernet hasta 10Mbps
- Redes Token Ring hasta 16 Mbps
- Redes Fast Ethernet hasta 100Mbps

- Redes Giga Ethernet hasta 1000Mbps

Método de acceso

Los métodos de acceso se refieren a las reglas que deben seguir las estaciones de trabajo para acceder al medio y transmitir su información en forma ordenada, evitando así colisiones con la consecuente pérdida de datos. Permiten también el direccionamiento de la comunicación entre estaciones. El método de acceso más utilizado es CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*).

Es un método en el que la estación de trabajo censa el medio antes de hacer una transmisión; si el medio está ocupado espera un tiempo determinado antes de volver a censar. Cuando detecta que ninguna estación está transmitiendo comienza su envío. Es posible que dos estaciones transmitan al mismo tiempo por hacer la detección simultáneamente, por lo tanto habrá una colisión. Cuando ocurre esto, ambas máquinas vuelven a esperar un tiempo aleatorio para iniciar el proceso. Se usa principalmente en redes con topología bus.

Detallamos características técnicas de las redes Fast Ethernet y Giga Ethernet las vigentes en mayor porcentaje en la actualidad.

2.2.1 Arquitectura de redes de área local Fast Ethernet

Mantener el protocolo de control de acceso al medio CSMA/CD y conservando la compatibilidad con las redes ethernet pero a mayor velocidad, dio lugar a Fast Ethernet.

Fast Ethernet sigue la norma 802.3u. Es compatible y puede coexistir con redes Ethernet tradicionales ya que se mantienen todos los elementos de la norma 802.3 en cuanto a interfaces, estructura y longitud de tramas, detección de errores, método de acceso, etc. Lo único que se modifica es el nivel físico, reduciendo el tiempo de *bit* en un factor de 10 (10ns), permitiendo un ancho de banda de 100Mbps. El cableado que se emplea es par trenzado (de categoría 3,4 ó 5) y fibra óptica.

En Fast Ethernet también se dispone de una nomenclatura para designar el medio físico empleado:

- **100BaseT4:** emplea UTP de categoría 3. De los 4 pares (*8 hilos*) emplea 3 para transmisión a 100Mbps (recordemos que Ethernet es *semiduplex*) y 1 para detección de colisiones. Se emplea una codificación 8B6T. La longitud máxima es de 100m.

- **100BaseTX:** usa UTP de categoría 5. Utiliza 2 pares, uno para fordwarding y otro para recepción (100Mbps). La codificación que emplea es 4B5B (compatible con FDDI). La longitud máxima también es de 100m.
- **100BaseFX:** Emplea fibra óptica a una velocidad de 100Mbps *(full duplex)*. La longitud máxima es de 2000m.

Mantener la técnica de acceso CSMA/ CD le conlleva una serie de ventajas:

- Ethernet es conocida y aceptada por el mercado.
- Conlleva un bajo costo de implementación.
- Es compatible con componentes actuales y redes ya instaladas.

Pero también existen una serie de inconvenientes:

- La interrelación entre el tamaño mínimo de trama, velocidad de transmisión y retardo de propagación.
- El retardo variable de CSMA/CD hace que Ethernet no sea adecuado para aplicaciones sensibles al retardo.
- El ancho de banda es inversamente proporcional al número de usuarios en la red.

2.2.2 Arquitectura de redes de área local Giga Ethernet

En Mayo de 1996 se formó la alianza Gigabit Ethernet conformada por 11 compañías, poco después la IEEE anuncia la formación del 802.3z, proyecto del estándar Gigabit Ethernet.

El nuevo estándar Gigabit Ethernet es compatible completamente con las instalaciones existentes de redes ethernet reteniendo el mismo método de acceso CSMA/CD, soporta modos de operaciones como *full-Duplex* y *half-Duplex*. También soporta fibra mono-modo, multi-modo y cable coaxial *short-haul* (dos centros conductores rodeados por una capa espaciadora aislante)

La capa física de Gigabit Ethernet esta formada por un híbrido entre las tecnología Ethernet y la especificación de canales por fibra ANSI X3T11. Gigabit Ethernet acepta finalmente 4 tipos de medios físicos, los cuales son definidos en 802.3z (1000Base-X) y 802.3ab (1000Base-T):

- 1000Base-X

En el estándar 1000Base-X la capa física es el canal de fibra, dicho canal de fibra es una tecnología de interconexión entre estaciones, supercomputadoras, dispositivos de almacenamiento de información y periféricos. El canal de fibra

tiene una arquitectura de 4 capas. La más baja tiene 2 capas FC-0 (Interfaz y Medio) y FC-1 (Codificador y Decodificador), estas son usadas en Gigabit Ethernet.

Hay 3 tipos de medios de trasmisión que son incluidos en el estándar 1000Base-X:

1000Base-SX: usa una fibra multi-modo

1000Base-LX: puede ser usada tanto mono-modo y multi-modo.

1000Base-CX: usa un cable par trenzado de cobre (STP).

- 1000Base-T

El estándar 1000Base-T de Gigabit Ethernet emplea como medio de trasmisión un cable UTP, usando 4 pares de líneas de categoría 5 UTP.

La capa MAC de Gigabit Ethernet usa el mismo protocolo de Ethernet CSMA/CD. La máxima longitud del cable usada para interconectar las estaciones está limitado por el protocolo CSMA/CD. Si dos estaciones detectan el medio desocupado y comienzan la trasmisión ocurrirá una colisión.

Ethernet tiene una trama mínima de 64 *bytes*, la razón de tener un tamaño mínimo en la trama es para prever que las estaciones completen la trasmisión de una trama antes de que el primer *bit* sea detectado al final del cable, donde este puede chocar con otra trama. Sin embargo, el tiempo mínimo de detección de colisión es el tiempo que toma una señal en propagarse desde un extremo a otro del cable. Este tiempo mínimo es llamado *slot time*.

La longitud máxima de un cable en Ethernet es de 2.5 Km (con un máximo de 4 repetidores). Como la tasa de *bit* se incrementa hace que aumente la velocidad de transmisión. Como resultado, si el mismo tamaño de la trama y la longitud del cable se mantienen, entonces la estación puede también trasmitir una trama a gran velocidad y no detectar una colisión al final del otro cable. Entonces, una de las siguientes cosas se deben hacer:

Mantener una longitud máxima del cable e incrementar el *time slot* (y por eso, un tamaño mínimo en la trama) o mantener un mismo *time slot* y decrementar la longitud del cable o ambos. En Fast Ethernet la longitud máxima del cable es reducida a 100 metros, dejando el tamaño de la trama en mínimo y el *time slot* intacto.

Gigabit Ethernet mantiene los tamaños mínimos y máximos de las tramas de Ethernet. Desde que Gigabit Ethernet es 10 veces más rápida que Fast Ethernet mantiene el mismo tamaño del *slot*, máxima longitud del cable deberá ser reducida a 10 metros, el cual no es muy usado. En lugar de ello, *Gigabit Ethernet* usa un gran tamaño del *slot*, siendo de 510 *bytes*. Para mantener la compatibilidad con Ethernet, el mínima tamaño de la trama no es incrementado, pero el "*carrier event*" es extendido. Si la trama es más corta que 512 *bytes*, entonces agregamos símbolos de extensiones.

2.3 Redes de área extensa (WAN)

Son redes que cubren una amplia región geográfica, a menudo un país o un continente. Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas *hosts* o sistemas finales (*end system*). Los sistemas finales están conectados a una subred de comunicaciones.

La función de la subred es transportar los mensajes de un *host* a otro.

En la mayoría de las redes de amplia cobertura se pueden distinguir dos componentes: Las líneas de transmisión y los elementos de intercambio (conmutación). Las líneas de transmisión se conocen como circuitos, canales o troncales. Los elementos de intercambio son computadores especializados utilizados para conectar dos o más líneas de transmisión.

Las redes de área local son diseñadas de tal forma que tienen topologías simétricas, mientras que las redes de amplia cobertura tienen topología irregular. Otra forma de lograr una red de área extensa es a través de satélite o sistemas de radio.

Ejemplo de redes de amplia cobertura: X.25, RTC, ISDN, FRAME RELAY, ATM, MPLS etc.

Cuando se llega a un cierto punto critico deja de ser práctico seguir ampliando una LAN a veces esto viene impuesto por limitaciones físicas (distancia), aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras; dos de los componentes importantes de cualquier red son la red de teléfono y la de datos. Casi todos los operadores de redes nacionales (como *DBP Telekom* en Alemania o *British Telecom* en Inglaterra) ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de

telefonía hasta los complejos servicios de alta velocidad (como Frame Relay y SMDS-*Synchronous Multimegabit Data Service*) adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Buscándose que proporcionen los enlaces necesarios entre LANs para hacer posible lo que han dado a llamarse autopistas de la información.

Como parte de la evolución de las redes de área extensa describiremos las arquitecturas:

- Red Digital de Servicios Integrados(RDSI)
- Redes de conmutación de paquetes X.25
- Redes de transmisión de tramas Frame Relay
- Redes ATM (Asynchronous Transfer Mode)
- Redes MPLS (*Multiprotocol Label Switching*)

2.3.1 Red digital de servicios integrados (RDSI)

La RDSI (Red Digital de Servicios Integrados, en ingles *ISDN*) presta conexiones extremo a extremo a nivel digital y es capaz de brindar diferentes servicios.

Se denomina servicios integrados porque utiliza la misma infraestructura para muchos servicios que tradicionalmente requerían interfaces distintas (télex, voz, conmutación de circuitos, conmutación de paquetes); es digital porque se basa en la transmisión digital, integrando las señales analógicas mediante la transformación Analógico - Digital, ofreciendo una capacidad básica de comunicación de 64 Kbps.

Como podemos observar, en el caso del teléfono se efectúa la conversión Analógico Digital. En el caso de equipos digitales, Ordenador, se transforma el código original a otro más adecuado a la comunicación (transformación de código). Ventajas de la RDSI:

- Velocidad

Supera el límite de velocidad en las comunicaciones a través de una línea telefónicas empleando señales analógicas entre central y usuario mediante el uso de módems que era alrededor de los 56Kbps.

La RDSI ofrece múltiples canales digitales que pueden operar simultáneamente a través de la misma conexión telefónica entre central y usuario; la tecnología digital

está en la central del proveedor y en los equipos del usuario, que se comunican ahora con señales digitales.

Este esquema permite una transferencia de datos a velocidad mucho mayor. Así, con un servicio de acceso básico, y empleando un protocolo de agregación de canales, se puede alcanzar una velocidad de datos, sin comprimir, de unos 128 Kbps.

Además, el tiempo necesario para establecer una comunicación en RDSI es cerca de la mitad del tiempo empleado con una línea con señal analógica.

- Conexión de múltiples dispositivos

Con líneas analógicas resulta necesario disponer de una línea por cada dispositivo del usuario, si estos se quieren emplear simultáneamente. Resulta muy caro enviar datos (archivos o vídeo) mientras se mantiene una conversación hablada. Por otra parte, se requieren diferentes interfaces para emplear diferentes dispositivos al no existir estándares al respecto.

Con la RDSI es posible combinar diferentes fuentes de datos digitales y hacer que la información llegue al destino correcto.

Como la línea es digital, es fácil controlar el ruido y las interferencias producidas al combinar las señales. Además, las normas de la RDSI especifican un conjunto de servicios proporcionados a través de interfaces normalizadas.

- Señalización

La forma de realizar un llamada a través de una línea analógica es enviando una señal de tensión que hace sonar la "campana" en el teléfono destino. Esta señal se envía por el mismo canal que las señales analógicas de sonido. Establecer la llamada de esta manera requiere bastante tiempo. Por ejemplo, entre 30 y 60 segundos con la norma V.34 para módems.

En una conexión RDSI, la llamada se establece enviando un paquete de datos especial a través de un canal independiente de los canales para datos. Este método de llamada se engloba dentro de una serie de opciones de control de la RDSI conocidas como señalización y permite establecer la llamada en un par de segundos. Además, informa al destinatario del tipo de conexión (voz o datos) y desde que número se ha llamado y puede ser gestionado fácilmente por equipos inteligentes como un ordenador.

- Servicios

La RDSI no se limita a ofrecer comunicaciones de voz. Ofrece otros muchos servicios, como transmisión de datos informáticos (servicios portadores), télex, facsímil, videoconferencia, conexión a Internet, etc, y opciones como llamada en espera, identidad del origen, entre otras.

Los servicios portadores permiten enviar datos mediante conmutación de circuitos (con un procedimiento de llamada se establece un camino fijo y exclusivo para transmitir los datos en la red, al estilo de las redes telefónicas clásicas) o mediante conmutación de paquetes (la información a enviar se divide en paquetes de tamaño máximo que son enviados individualmente por la red).

Canales y Servicios.

- Canales de transmisión.

La RDSI dispone de distintos tipos de canales para el envío de datos de voz e información y datos de control: los canales tipo B, tipo D y tipo H:

- Canal B.- Los canales tipo B transmiten información a 64Kbps, y se emplean para transportar cualquier tipo de información de los usuarios, bien sean datos de voz o datos informáticos. Estos canales no transportan información de control de la RDSI.

Este tipo de canales sirve además como base para cualquier otro tipo de canales de datos de mayor capacidad, que se obtienen por combinación de canales tipo B.

- Canal D.- Los canales tipo D se utilizan principalmente para enviar información de control de la RDSI, como es el caso de los datos necesarios para establecer una llamada o para colgar. Por ello, también se conoce un canal D como "canal de señalización". Los canales D también pueden transportar datos cuando no se utilizan para control. Estos canales trabajan a 16Kbps o 64kbps según el tipo de servicio contratado.

- Canales H.- Combinando varios canales B se obtienen canales tipo H, que también son canales para transportar solo datos de usuario, pero a velocidades mucho mayores. Por ello se emplean para información como audio de alta calidad o vídeo.

Hay varios tipos de canales H:

Canales H0, que trabajan a 384Kbps (6 canales B).

Canales H10, que trabajan a 1472Kbps (23 canales B).

Canales H11, que trabajan a 1536Kbps (24 canales B).

Canales H12, que trabajan a 1920Kbps (30 canales B).

2.3.2 Redes de Conmutación de Paquetes X.25

Es el protocolo de acceso a redes públicas de conmutación de paquetes definido por el ITU-T, anteriormente CCITT (especificación ITU-T X.25) [1]. Este protocolo garantiza la retransmisión libre de errores de información en forma de datos entre terminales conectados a una misma red de conmutación de paquetes o a redes diferentes adecuadamente interconectadas.

Ofrece múltiples facilidades y/u opciones de uso que permiten un adecuado control sobre aspectos tales como seguridad, distribución del tráfico, etc.

- Descripción

X.25 es un servicio de transmisión de datos apropiado para el intercambio de tráfico transaccional, transferencias de fondos, consultas a bases de datos, teleproceso, etc. Es extremadamente fiable, garantizando la transmisión libre de errores entre terminales conectados a una misma red de conmutación de paquetes o a redes diferentes adecuadamente interconectadas. Ofrece múltiples facilidades y opciones de uso que permiten un adecuado control sobre aspectos tales como seguridad, distribución del tráfico, etc.

El acceso al servicio se suministra a través de líneas dedicadas que van desde las dependencias del cliente hasta el nodo de acceso al servicio más próximo, con la posibilidad de incluir, como parte del servicio, equipamiento adicional en casa del cliente encaminado a:

- Establecer conexiones de respaldo de las líneas dedicadas.
- Concentrar tráfico sobre el acceso al Servicio.
- Permitir al cliente la gestión de sus propias conexiones.

- Aplicaciones

Las aplicaciones típicas de X.25 son:

Intercambio de tráfico de tipo transaccional (Gestión de pedidos, Consulta de Costos, Plazos de Entrega y Almacén), transferencias electrónicas de fondos, consultas en bases de datos, etc.

Conexión de terminales a un ordenador central en un sistema de teleproceso. Mediante el uso de equipos concentradores y/o multiprotocolo, el usuario puede

concentrar en una sola línea el tráfico de comunicaciones procedente de todos los ordenadores o terminales de un mismo emplazamiento.

Correo electrónico y EDI también pueden operarse satisfactoriamente sobre X.25.

- **Ventajas**

Calidad: el compromiso de calidad del servicio se basa en la disponibilidad de los accesos de cliente al servicio y se garantiza mediante:

La infraestructura de red sobre la que se soporta el servicio y que se traduce en una fiabilidad y una capacidad de transmisión muy elevadas mediante la utilización de nodos de red de alta tecnología, la construcción del núcleo de red (*backbone*) sobre enlaces de alta velocidad (34 Mbps), una arquitectura de red completamente redundante, tanto en nodos como en enlaces

En la posibilidad de contratar nodos de Red instalados en casa de cliente a través del servicio nodo de red.

En la existencia de un centro de gestión con amplias capacidades de supervisión, operación y control, y en funcionamiento 24 horas/día, 365 días/año

Economía: aplicación de tarifa por uso del servicio para todas las comunicaciones establecidas entre los diferentes accesos del cliente integrados al servicio.

Disponibilidad del servicio a nivel nacional independiente de la ubicación geográfica.

Posibilidad de concentrar tráfico en el domicilio de cliente.

Normalización: libertad en la elección de equipos de cliente, al tratarse de un servicio basado en un protocolo estándar soportado por la práctica totalidad de los fabricantes

Seguridad: en el acceso al servicio, mediante la posibilidad de respaldo RTB/ RDSI, y la contratación de accesos multienlace.

En el transporte, ya que las técnicas de conmutación de paquetes y de protección de errores garantizan el transporte y entrega de información con total fiabilidad y seguridad.

Conexiones de la Empresa Cliente mediante la creación de grupo cerrado de usuarios, y la posibilidad de cifrar los datos que viajan por la red.

Ventajas que ofrecen los servicios basados en X.25:

Coste independiente de la distancia.

Transmisión libre de errores.

Posibilidad multidestino en modo simultáneo.

2.3.3 Redes de transmisión de tramas FRAME RELAY

Frame Relay comenzó como un movimiento a partir del mismo grupo de normalización que dio lugar a X.25 y RDSI. Sus especificaciones fueron definidas por ANSI, fundamentalmente como medida para superar la lentitud de X.25, eliminando la función de los conmutadores, en cada "salto" de la red. X.25 tiene el grave inconveniente de su importante "overhead" producido por los mecanismos de control de errores y de flujo.

Anteriormente, X.25 se vino utilizando como medio de comunicación para datos a través de redes telefónicas con infraestructuras analógicas, en las que la norma ha sido la baja calidad de los medios de transmisión, con una alta tasa de errores. Esto justificaba los abundantes controles de errores y sus redundantes mecanismos para el control de flujo, junto al pequeño tamaño de los paquetes. En resumen, se trataba de facilitar las retransmisiones para obtener una comunicación segura.

Frame Relay, por el contrario, maximiza la eficacia, aprovechándose para ello de las modernas infraestructuras, de mucha mayor calidad y con muy bajos índices de error, y además permite mayores flujos de información.

Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2,048 Mbps, aunque nada le impide superarlas.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red.

- **Tecnología:**

Las redes Frame Relay fueron construidas partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporaron los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red.

Este equipo conmutador se denomina FRAD o "Ensamblador/Desensamblador Frame Relay" (*Frame Relay Assembler/Disassembler*) y el nodo de red se denomina FRND o "Dispositivo de Red Frame Relay" (*Frame Relay Network Device*).

Figura 2.1 Muestra la red Frame Relay operando en la subcapa del nivel de enlace (nivel 2) del modelo OSI, el nivel físico es representado por HSSI (*High-Speed Serial Interface*).

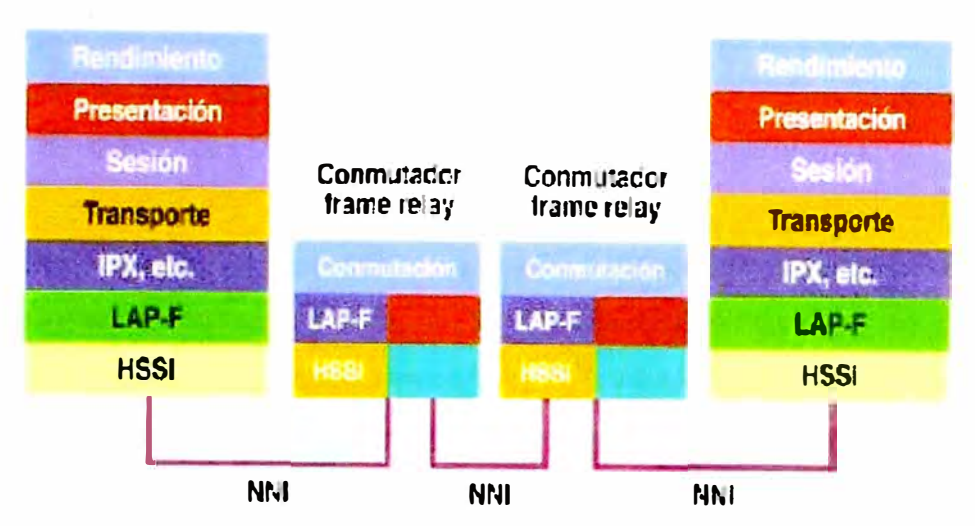

Fig 2.1: Estructura OSI de la red Frame Relay

Las tramas y cabeceras de Frame Relay pueden tener diferentes longitudes, ya que hay una gran variedad de opciones disponibles en la implementación, conocidos como anexos a las definiciones del estándar básico.

La información transmitida en una trama Frame Relay puede oscilar entre 1 y 8.250 *bytes*, aunque por defecto es de 1.600 *bytes*.

Lo más increíble de todo es que a pesar del gran número de formas y tamaños, Frame Relay funciona perfectamente y ha demostrado un muy alto grado de interoperatibilidad entre diferentes fabricantes de equipos y redes. Ello es debido a que, sean las que sean las opciones empleadas por una determinada implementación de red o equipamiento, siempre existe la posibilidad de "convertir" los formatos de Frame Relay a uno común, intercambiando así las tramas en dicho formato.

En Frame Relay, por tanto, los dispositivos del usuario se interrelacionan con la red de comunicaciones, haciendo que sean aquellos mismos los responsables del

control de flujo y de errores. La red sólo se encarga de la transmisión y conmutación de los datos, así como de indicar cual es el estado de sus recursos. En el caso de errores o de saturación de los nodos de la red, los equipos del usuario solicitarán el reenvío (al otro extremo) de las tramas incorrectas y si es preciso reducirán la velocidad de transmisión, para evitar la congestión.

Las redes Frame Relay son orientadas a conexión, como X.25, SNA e incluso ATM. El identificador de conexión es la concatenación de dos campos HDLC (*High-level Data Link Control*), en cuyas especificaciones originales de unidad de datos (protocolo de la capa 2), se basa Frame Relay. Entre los dos campos HDLC que forman el "identificador de conexión de enlace de datos" o DLCI (*Data Link Connection Identifier*) se insertan algunos bits de control (CR y EA).

A continuación se añaden otros campos que tienen funciones muy especiales en las redes Frame Relay. Ello se debe a que los nodos conmutadores Frame Relay carecen de una estructura de paquetes en la capa 3, que por lo general es empleada para implementar funciones como el control de flujo y de la congestión de la red y que estas funciones son imprescindibles para el adecuado funcionamiento de cualquier red.

Los tres más esenciales son DE o "elegible para ser rechazada" (*Discard Eligibility*), FECN o "notificación de congestión explícita de envío" (*Forward Explicit Congestion Notification*) y BECN o "notificación de congestión explícita de reenvío" (*Backward Explicit Congestion Notification*). El *bit* DE es usado para identificar tramas que pueden ser rechazadas en la red en caso de congestión. FECN es usado con protocolos de sistema final que controlan el flujo de datos entre el emisor y el receptor, como el mecanismo "windowing" de TCP/IP; en teoría, el receptor puede ajustar su tamaño de "ventana" en respuesta a las tramas que llegan con el bit FECN activado. BECN, como es lógico, puede ser usado con protocolos que controlan el flujo de los datos extremo a extremo en el propio emisor.

Según esto, la red es capaz de detectar errores, pero no de corregirlos (en algunos casos podría llegar tan solo a eliminar tramas).

No se ha normalizado la implementación de las acciones de los nodos de la red ni del emisor / receptor, para generar y/o interpretar estos tres *bits.* Por ejemplo, TCP/IP no tiene ningún mecanismo que le permita ser alertado de que la red

Frame Relay esta generando *bits* FECN ni de como actuar para responder a dicha situación. Las acciones y funcionamiento de las redes empleando estos bits son temas de altísimo interés y actividad en el "*Frame Relay Forum*" (equivalente en su misión).

Frame Relay también fue denominado "tecnología de paquetes rápidos" (*fast packet technology*) o el "X.25 de los 90".

El protocolo X.25 opera en la capa 3 e inferior del modelo OSI, y mediante la conmutación de paquetes, a través de una red de conmutadores, entre identificadores de conexión. En cada salto de la red X.25 se verifica la integridad de los paquetes y cada conmutador proporciona una función de control de flujo. La función de control de flujo impide que un conmutador X.25 no envíe paquetes a mayor velocidad de la que el receptor de los mismos sea capaz de procesarlos. Para ello, el conmutador X.25 receptor no envía inmediatamente la señal de reconocimiento de los datos remitidos, con lo que el emisor de los mismos no envía más que un determinado número de paquetes a la red en un momento dado.

Frame Relay realiza la misma función, pero partiendo de la capa 2 e inferiores. Para ello, descarta todas las funciones de la capa 3 que realizaría un conmutador de paquetes X.25 y las combina con las funciones de trama. La trama contiene así al identificador de conexión y es transmitida a través de los nodos de la red en lugar de realizar una "conmutación de paquetes".

Lógicamente, todo el control de errores en el contenido de la trama, y el control de flujo, debe de ser realizado en los extremos de la comunicación (nodo origen y nodo destino). La conmutación de paquetes en X.25, un proceso de 10 pasos, se convierte en uno de 2 pasos, a través de la transmisión de tramas.

2.3.4 Redes ATM (*Asynchronous Transfer Mode*)

Las nuevas necesidades de comunicaciones aparecidas en la década de los 80 orientaron las comunicaciones hacia la conmutación de paquetes en alta velocidad para contar simultáneamente con las ventajas de las redes de circuitos y las redes de paquetes. La nueva tecnología debería ser capaz de proporcionar anchos de banda variables, ser transparente a los protocolos utilizados y soportar una gama amplia de servicios con soluciones específicas de velocidad, sincronización y latencia. Con éstas especificaciones aparecieron dos tecnologías

de acceso en la interfase usuario / red: Frame Relay y C*ell Relay*, la primera para transmitir datos especialmente y la segunda para transmitir cualquier tipo de tráfico. Las dos reclaman para sí lo mejor de ambos mundos, esto es, la predictibilidad de las redes de circuitos y la flexibilidad de las redes de paquetes.
ATM proporciona las mejores características de las redes de paquetes y de las redes de circuitos conmutados.

- ***Cell Relay* (ATM).** Envía unos paquetes de 53 *bytes* denominados células. El pequeño tamaño de los paquetes garantiza un mínimo retardo aunque supone un incremento del *overhead*: cuanto más pequeño es el paquete, más proporción hay de cabeceras y más pérdida de ancho de banda. Las ventajas obtenidas son una baja latencia que permite transportar datos isocrónicos y una eficiente conmutación de hardware gracias al tamaño constante de los paquetes.
ATM soporta cualquier tipo de tráfico proporcionando calidad de servicio específica para cada uno de ellos.

- **Breve historia de ATM.** La primera referencia del ATM (*Asynchronous Transfer Mode*) tiene lugar en los años 60 cuando un norteamericano de origen oriental perteneciente a los laboratorios *Bell* describió y patentó un modo de transferencia no síncrono. Sin embargo el ATM no se hizo popular hasta 1988 cuando el CCITT decidió que sería la tecnología de conmutación de la futura red ISDN en banda ancha. En aquellas históricas fechas los valedores del ATM tuvieron primero que persuadir a algunos representantes de las redes de comunicaciones que hubieran preferido una simple ampliación de las capacidades de la ISDN en banda estrecha. Conseguido este primer objetivo y desechando los esquemas de transmisión síncronos, se empezaron a discutir aspectos tales como el tamaño de las células. Por un lado los representantes de EEUU y algún otro país proponían un tamaño de células grande de unos 128 *bytes*: `cuanto mayor es el tamaño de las células menor es el *overhead*, parámetro muy importante cuando se desean transmitir datos era el argumento. Sin embargo, los representantes de los países europeos decían que el tamaño ideal de las células eran de 16 *bytes* y señalaron que un tamaño de célula de 128 *bytes* provocaría retardos inaceptables de hasta 85 miliseg. Este retardo no permitiría la transmisión de voz con cierto nivel de calidad a la vez que obligaba a instalar canceladores de eco.

Después de muchas discusiones ambas partes habían hecho una concesión: el lobby norteamericano proponía 64 *bytes* y el lobby europeo 32 *bytes* que básicamente coincidían con los representantes de las redes de datos y las redes de voz respectivamente. Ante la falta de acuerdo en la reunión del CCITT celebrada en Ginebra en Junio de 1989 se tomó una decisión salomónica: "Ni para unos ni para otros 48 *bytes* será el tamaño de la célula". Para la cabecera hubo posicionamientos similares, y el definitivo tamaño de 5 *bytes* también fue un compromiso.

Un extraño número primo 53 (48+5) sería el tamaño definitivo, en octetos, de las células ATM. Un número que tuvo la virtud de no satisfacer a nadie pero que suponía un compromiso de todos los grupos de interés y evitaba una ruptura de consecuencias imprevisibles.

- Arquitectura de un nodo ATM.

El ATM puede ser considerado como una tecnología de conmutación de paquetes en alta velocidad con unas características particulares:

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

Simplificando al máximo podemos ver que una red ATM está compuesta por nodos de conmutación, elementos de transmisión y equipos terminales de usuarios. Los nodos son 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 *hardware* mientras que el establecimiento de conexiones y el empaquetamiento/desempaquetamiento de las células son procesos *software*.

- Jerarquía de transmisión.

Bajo un punto de vista basado exclusivamente en la transmisión, el ATM se puede dividir en tres niveles que se combinan de forma jerárquica de modo que cada capa superior puede tener uno o varios de los elementos inferiores.

- **Canal Virtual (VC)** Así es llamada la conexión unidireccional entre usuarios. E importante resaltar la unidireccionalidad: si dos usuarios

quisieran estar conectados *en full duplex* deberán utilizar dos canales. Los VCs, además de transportar datos entre usuarios, también son utilizados para transportar la señalización y la gestión de la red.

- Trayecto Virtual (VP). Se entiende al conjunto de canales virtuales que atraviesan multiplexadamente un tramo de la red ATM. Los VP facilitan la conmutación de los canales virtuales, pues conectan tramos enteros de la red ATM. De no existir por cada conexión entre usuarios obligaría a reelaborar todas las tablas de *routing* de los nodos atravesados, lo cual supondría un incremento del tiempo necesario para establecer una conexión.

- Sección Física (PS). Conecta y proporciona continuidad digital entre los diferentes elementos que componen la red controlando el flujo de bits. Debe mantener en óptimas condiciones las señales físicas, eléctricas u ópticas regenerándolas cuando resultan afectadas por atenuaciones, ruido o distorsiones.

- Modelo de referencia ATM.

Bajo una perspectiva arquitectónica el ATM se divide en tres niveles que ocupan las capas 1 y parte de la capa 2 del modelo de referencia OSI:

- Nivel de adaptación ATM (AAL)

Se encarga de las relaciones con el mundo externo. Acepta todo tipo de información heterogénea y la segmenta en paquetes de 48 *bytes* a la velocidad que fue generada por los usuarios. Sólo se encuentra en los puntos terminales de la red. Según el modelo OSI maneja, en el nivel 2, las conexiones entre la red ATM y los recursos no ATM pertenecientes a los usuarios finales.

- Nivel Modo de Transferencia Asíncrona (ATM)

encargado de construir las cabeceras de las células ATM, responsable del *routing* y el multiplexado de las células a través de los Canales y Rutas Virtuales. También es misión suya el control del flujo de datos y la detección de errores ocurridos en la cabecera aunque no en los datos.

- Nivel físico (PL)

Es el nivel inferior encargado de controlar las señales físicas, ya sean ópticas o eléctricas e independizarlas de los niveles superiores de

protocolo adaptándolas al medio de transmisión y codificación utilizado. Puede soportar diversas configuraciones punto-a-punto y punto-a-multipunto. En una red ATM se distinguen dos tipos de nodos: los terminales que proporcionan los puntos de acceso a los usuarios finales y los nodos de conmutación responsables dentro de la red del *routing* de las células.

Ampliamos conceptos de cada uno de ellos es así como tenemos a:

- Nivel de Adaptación ATM (AAL)

Responsable de las relaciones con el mundo externo, por esta razón el nivel AAL sólo se encuentra en los nodos terminales de la red. Su misión es la de aceptar la información adaptando los niveles superiores de comunicación no ATM a los formatos ATM. Son funciones del nivel AAL:

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

- Estructura de la Capa AAL

Internamente el AAL se divide en dos partes:

- El subnivel de convergencia (CS): Es la capa más externa y ejecuta funciones como la detección y demultiplexión de datos, detección de células perdidas y mantenimiento del sincronismo de la conexión.

- El subnivel segmentación y reensamblado (SAR): Esta capa segmenta los datos en células y las envía al nivel ATM para que les ponga la cabecera. El proceso inverso se verifica al lado opuesto cuando recibe células y reconstruye la información original.

- Calidad de servicio (QoS).

La información que llega a un nodo terminal ATM es captada, segmentada y dispuesta en células con las cabeceras adecuadas para cada tipo de tráfico. Este servicio proporcionado por el nivel AAL se denomina QoS que queda definido por tres parámetros:

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

- **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.

- La Capa ATM

Este nivel es el auténtico núcleo sobre el que se soporta la tecnología del *cell relay*. Sus funciones, fundamentales y comunes a cualquier nodo, se encargan de la manipulación de células ejecutándose los siguientes procesos:

- Construcción / extracción de cabeceras
- *Routing* entre los nodos
- Multiplexión y demultiplexión de células

- Formato de las Células ATM

Son estructuras de datos de 53 *bytes* compuestas por dos campos principales:

- ***Header***, sus 5 *bytes* tienen tres funciones principales: identificación del canal, información para la detección de errores y si la célula es o no utilizada. Eventualmente puede contener también corrección de errores, número de secuencia, etc.
- ***Payload***, tiene 48 *bytes* fundamentalmente con datos del usuario y protocolos AAL que también son considerados como datos del usuario.

Dos de los conceptos más significativos del ATM, canales virtuales y rutas virtuales, están materializados en dos identificadores en el *header* de cada célula (VCI y VPI) ambos determinan el *routing* entre nodos. Existen dos formatos de células: la UNI (*User to Network Interfase*) utilizado en el

interfaz red/usuario y la NNI (*Network to Network Interfase*) cuando circulan por la red.

- Conexiones y *routing*

Los conmutadores de VP modifican los identificadores VPI para redirigir las rutas de entrada hacia una salida específica. Un conmutador de VP no analiza ni modifica el campo VCI, ya que al operar en un nivel inferior conmuta todos los canales asociados a dicha ruta. Los conmutadores de VC aplican un mayor nivel de complejidad ya que manejan atributos como nivel de errores, calidad servicio, ancho de banda o servicios relacionados con la tarificación. Las tablas de *routing* de cada nodo pueden estar ya predefinidas, o bien deben construirse dinámicamente en el tiempo del establecimiento de las conexiones realizadas mediante el protocolo Q.2931 similar al Q.931 utilizado en el ISDN para banda estrecha.

Una ruta virtual puede ser permanente (PVP) o conmutada (SVP). Si es conmutada, es decir si se ha establecido explícitamente para una comunicación, todos sus canales virtuales (VCs) asociados son dirigidos a través de ese camino y no será necesario conmutarlos. Si el VP es permanente es probable que sólo conecte troncales de la red por lo que los VCs deberán ser conmutados en algún nodo de la red. El *routing* de canales y rutas virtuales es realizado mediante etiquetas, nunca con direcciones explícitas. Por ejemplo, un nodo de conmutación debe leer el identificador VCI = i de cada célula que entra por el puerto K y de acuerdo con su tabla de *routing*, la envía por el puerto Q modificando el *header* al escribir VCI = j.

La capa ATM es el núcleo real de la tecnología. Se ocupa de añadir y extraer las cabeceras, mantener los identificadores de conexión para realizar el encaminamiento entre nodos, y de multiplexar y demultiplexar las celdas a través del medio físico, manteniendo un secuenciamiento correcto de las celdas.

- El Nivel Físico

El nivel físico realiza dos funciones fundamentales: el transporte de células válidas y la entrega de la información de sincronismo

La estructura del nivel físico se divide en dos capas:

- **El subnivel convergencia de la transmisión (TC).** Encargado de adaptar la velocidad y de crear el *datastream* para su posterior transmisión al medio físico. El proceso inverso se realiza en el otro extremo de la red donde el TC destino debe extraer las células del *datastream* recibido, comprobar su corrección y entregarlas finalmente al nivel superior ATM. Las células incorrectas o vacías se desechan.
- **El subnivel medio físico (PM).** Es el encargado de la transmisión de bits y de la sincronización de señales.

Dos velocidades estandarizadas por el ITU son 155,52 Mbps y 622,08 Mbps; mientras que el ATM Forum ha estandarizado interfaces con velocidades a 25 Mbit/s, 44,736 Mbit/s, 100 Mbit/s y 155,52 Mbit/s.

El nivel físico debe adaptar la secuencia de celdas a la estructura y a la velocidad del canal de transmisión utilizado.

- Datastream del medio de transmisión

El servicio portador de la red encargado de transportar la información hasta los usuarios puede ser de los modelos:

- Basado en células.

Es la forma nativa utilizada en redes locales. Consiste en la transmisión directa de la secuencia de células ATM sobre el medio de transmisión que puede ser fibra y cable de diversas categorías. Dependiendo del estándar utilizado deben ser insertadas señales de delineación, sincronismo de las células.

- Basados en tramas plesiócronas o PDH,

Las células se agrupan en una trama plesiócrona que incluye funciones de mantenimiento. El estándar utilizado se deriva del IEEE 802.6 utilizado por el DQDB en redes metropolitanas.

- Basados en tramas síncronas o SDH,

En este caso las células son empaquetadas en *frames* síncronos denominados STM transmitidos a velocidades ópticas múltiplos de 155,52 Mbps. Estas estructuras transportan también información de sincronismo y el *overhead* necesario para el transporte. La ventaja de los *frames* STM es que ofrecen un mecanismo estandarizado para realizar la multiplexión de

los canales a medida que los enlaces aumentan o disminuyen su capacidad de transporte.

El ITU-T seleccionó la SDH como una de las bases para el B-ISDN para el transporte y multiplexión de señales a través de una red óptica. Es importante señalar que el SDH no es en sí mismo una red de comunicaciones, ni forma parte del ATM, sino el más bajo nivel de transporte de la red también utilizable por otras redes de transmisión como Frame Relay o SMDS.

Estructura e interrelación de las PDUs (*Protocol Data Units*).

- B-ISDN Y ATM

Existe cierta confusión entre ATM y B-ISDN, y a menudo se usa incorrectamente un término por el otro. La diferencia es clara:

- El ATM es una tecnología para la conmutación de células en alta velocidad, utilizable en múltiples entornos, LAN, MAN y WAN.

- El B-ISDN es una red de área extensa (WAN) que utiliza el N-ISDN como modelo de referencia y señalización; el ATM como tecnología de conmutación y el SDH como estándar de transporte dentro de la red.

Es decir, otros tipos de redes como por ejemplo una LAN puede también utilizar la tecnología ATM pero no han de utilizar necesariamente ni el SDH, ni el modelo de referencia ISDN.

Por tanto, se puede concluir respecto a ATM que tal y como reza el más extendido tópico de las redes digitales, el ATM dará soporte tanto a los servicios tradicionales en datos como para las más modernas aplicaciones multimedia en audio y vídeo. Inicialmente especificado para las grandes redes públicas ya ha ampliado su radio a entornos metropolitanos y locales.

Si con una sola palabra quisiéramos resumir el impacto que puede provocar el ATM esa palabra sería integración. Se trata de una tecnología altamente escalable capaz de manejar desde una WAN de grandes dimensiones, hasta de controlar el tráfico LAN de ordenadores. Una tecnología que puede simultáneamente transportar una videoconferencia y distribuir un paquete de software a escala mundial.

2.4 Calidad de servicio en Redes IP

Las redes IP fueron diseñadas para el transporte óptimo del tráfico de datos, por lo que la calidad de servicio (QoS) requerida en las mismas se basó únicamente en la integridad de los datos, esto es, no pérdida de contenido y ni secuencialidad de los mismos. En este sentido IP fue concebido, es decir, para (mover) por la red, de forma óptima y segura, tráfico sin requerimientos de tiempo real. Para esto el servicio que brinda IPv4 es del tipo *Best-Effort*.

Por otra parte, el tráfico de audio y vídeo no solo requiere ser transferido por las redes IP de forma íntegra, sino que además requiere ser transferido en el tiempo adecuado, al (ritmo) adecuado, en correspondencia con la cadencia que es generado. En consecuencia, la QoS en relación con el tráfico que tiene requerimientos de tiempo real necesita considerar otros parámetros de calidad, tales como la latencia (retardo y *jitter*) y el ancho de banda.

Dados estos requerimientos de QoS impuestos por el tráfico con características de tiempo real, como son el audio y el vídeo, se necesitan mecanismos de señalización que propicien tener bajo control dichos parámetros de calidad y dar garantía de QoS.

2.4.1 Arquitectura TCP/IP

TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes, con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que es en realidad es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (*Transmission Control Protocol*) y el IP (*Internet Protocol*), que son los que dan nombre al conjunto. La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- **Aplicación:** Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (*Hypertext Transfer Protocol*). Mencionamos a:

  - **FTP (*File Transfer Protocol*).** Se utiliza para transferencia de archivos.

  - **SMTP (Simple Mail Transfer Protocol).** Es una aplicación para el correo electrónico.

  - **TELNET**: Un protocolo Internet para la conexión a máquinas remotas y procesar los datos localmente.

  - **RPC (*Remote Procedure Call*)**. Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.

  - **SNMP (*Simple Network Management Protocol*).** Se trata de una aplicación para el control de la red.

- **Transporte**: Coincide con el nivel de transporte del modelo OSI. Este nivel proporciona una comunicación extremo a extremo entre programas de aplicación. La maquina remota recibe exactamente lo mismo que le envió la maquina origen. En este nivel el emisor divide la información que recibe del nivel de aplicación en paquetes, le añade los datos necesarios para el control de flujo y control de errores y se los pasa al nivel de red junto con la dirección de destino.

En el receptor este nivel se encarga de ordenar y unir las tramas para generar de nuevo la información original.

Para implementar el nivel de transporte se utilizan dos protocolos :

  - **UDP**: proporciona un nivel de transporte no fiable de datagramas, ya que apenas añade información al paquete que envía al nivel inferior, solo la necesaria para la comunicación extremo a extremo. Lo utilizan aplicaciones como NFS y RPC, pero sobre todo se emplea en tareas de control.

  - **TCP (*Transport Control Protocolo*):** es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones. Esta pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de aplicaciones de la dificultad de gestionar la fiabilidad de la conexión (retransmisiones, perdidas de paquete, orden en que llegan los

paquetes ,duplicados de paquetes, etc) que gestiona el propio protocolo. Pero la complejidad de la gestión de la fiabilidad tiene un coste en eficiencia, ya que para llevar a cabo las gestiones anteriores se tiene que añadir bastante información a los paquetes a enviar. Debido a que los paquetes a enviar tienen un tamaño máximo, como más información añada el protocolo para su gestión, menos información que proviene de la aplicación podrá contener ese paquete. Por eso, cuando es más importante la velocidad que la fiabilidad, se utiliza UDP, en cambio TCP asegura la recepción en destino de la información a transmitir.

- **Internet**: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Coloca la información que le pasa el nivel de transporte en datagramas IP, le añade cabeceras necesaria para su nivel y lo envía al nivel inferior. Es en este nivel donde se emplea el algoritmo de encaminamiento, al recibir un datagrama del nivel inferior decide, en función de su dirección, si debe procesarlo y pasarlo al nivel superior, o bien encaminarlo hacia otra maquina. Para implementar este nivel se utilizan los siguientes protocolos:

  - **IP *(Internet Protocol)***: es un protocolo no orientado a la conexión, con mensajes de un tamaño máximo. Cada datagrama se gestiona de forma independiente, por lo que dos datagramas pueden utilizar diferentes caminos para llegar al mismo destino, provocando que lleguen en diferente orden o bien duplicados. Es un protocolo no fiable, eso quiere decir que no corrige los anteriores problemas, ni tampoco informa de ellos. Este protocolo recibe información del nivel superior y le añade la información necesaria para su gestión (direcciones IP, *checksum*)

  - **ICMP *(Internet Control Message Protocol)***: Proporciona un mecanismo de comunicación de información de control y de errores entre maquinas intermedias por las que viajaran los paquetes de datos. Esto datagramas los suelen emplear las maquinas (gateways, host, etc) para informarse de condiciones especiales en la red, como la existencia de una congestión, la existencia de errores y las posibles peticiones de cambios de ruta. Los mensajes de ICMP están encapsulados en datagramas IP.

- **IGMP (*Internet Group Management Protocol*):** Este protocolo esta íntimamente ligado a IP. Se emplea en maquinas que emplean IP multicast. El IP multicast es una variante de IP que permite emplear datagramas con múltiples destinatarios.

También en este nivel tenemos una serie de protocolos que se encargan de la resolución de direcciones:

- **ARP (*Address Resolution Protocol*):** Cuando una maquina desea ponerse en contacto con otra conoce su dirección IP, entonces necesita un mecanismo dinámico que permite conocer su dirección física. Entonces envía una petición ARP por broadcast (o sea a todas las maquinas). El protocolo establece que solo contestará a la petición, sí esta lleva su dirección IP. Por lo tanto solo contestara la maquina que corresponde a la dirección IP buscada, con un mensaje que incluya la dirección física. El software de comunicaciones debe mantener una cache con los pares IP-dirección física. De este modo la siguiente vez que hay que hacer una transmisión a esa dirección IP, ya conoceremos la dirección física.
- **RARP (*Reverse Address Resolution Protocol*):** A veces el problema es al revés, o sea, una máquina solo conoce su dirección física, y desea conocer su dirección lógica. Esto ocurre, por ejemplo, cuando se accede a Internet con una dirección diferente, en el caso de PC que acceden por módem a Internet, y se le asigna una dirección diferente de las que tiene el proveedor sin utilizar. Para solucionar esto se envía por *broadcast* una petición RARP con su dirección física, para que un servidor pueda darle su correspondencia IP.
- **BOOTP (*Bootstrap Protocol*):** El protocolo RARP resuelve el problema de la resolución inversa de direcciones, pero para que pueda ser más eficiente, enviando más información que meramente la dirección IP, se ha creado el protocolo BOOTP. Este además de la dirección IP del solicitante, proporciona información adicional, facilitando la movilidad y el mantenimiento de las maquinas.

- **Acceso a la Red (Incluye al nivel de Enlace OSI)**: Es la interfaz de la red real. TCP/IP no especifica ningún protocolo concreto, así es que corre por las interfaces conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc.

Este nivel se limita a recibir datagramas del nivel superior (nivel de red) y transmitirlo al hardware de la red. Pueden usarse diversos protocolos: DLC(IEEE 802.2), Frame Relay, X.25, etc.

La interconexión de diferentes redes genera una red virtual en la que las maquinas se identifican mediante una dirección de red lógica. Sin embargo a la hora de transmitir información por un medio físico se envía y se recibe información de direcciones físicas. Un diseño eficiente implica que una dirección lógica sea independiente de una dirección física, por lo tanto es necesario un mecanismo que relacione las direcciones lógicas con las direcciones físicas. De esta forma podremos cambiar nuestra dirección lógica IP conservando el mismo hardware, del mismo modo podremos cambiar una tarjeta de red, la cual contiene una dirección física, sin tener que cambiar nuestra dirección lógica IP.

- **Físico**: Análogo al nivel físico del OSI.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de "datagrama" (*datagram*), y son conjuntos de datos que se envían como mensajes independientes.

2.4.2 Servicios Integrados

Esta basado en el protocolo RSVP (*Resource ReSerVation Protocol*, RFC 1633), implica una reserva de recursos en la red para cada flujo de información de usuario, así como el mantenimiento en la red (en los *routers*) de un estado para cada flujo, esto es, mantenimiento de la reserva (tablas de estados de reserva). Esto conduce a un considerable tráfico de señalización y ocupación de recursos

en cada *router* para cada flujo, con la consiguiente complejidad en el hardware, al margen del aporte que esta señalización hace a la congestión de la red. No es una solución escalable, no es una solución adecuada para grandes entornos como Internet, aunque si lo es para entornos más limitados y también para redes de acceso al *backbone*.

RSVP es un protocolo de señalización de QoS y posibilita: dar a las aplicaciones un modo uniforme para solicitar determinado nivel de QoS, encontrar una forma de garantizar cierto nivel de QoS, y proveer autentificación.

RSVP es un protocolo que se desarrolla entre los usuarios y la red, y entre los diferentes nodos (*routers*) de la red que soportan este protocolo. Consiste en hacer «reservas» de recursos en dichos nodos para cada flujo de información de usuario, con la consecuente ocupación de los mismos. Esto requiere, lógicamente, intercambio de mensajes RSVP entre dichos entes funcionales, así como mantener estados de reserva en cada nodo RSVP. De manera que tanto la solicitud de las reservas, como el mantenimiento de éstas durante la comunicación, y la posterior cancelación, implica el intercambio de mensajes de señalización, lo que representa un tráfico considerable cuando de entornos como Internet se trata.

RSVP ofrece dos tipos de servicios, a saber: servicio de carga controlada y servicio garantizado.

Servicio de carga controlada: aunque no está muy bien definido, se entiende en general que la pérdida de paquetes debe ser muy baja o nula.

Servicio garantizado: se basa en solicitar determinado ancho de banda y cierta demora de tránsito máxima.

De los dos tipos de servicios que RSVP soporta, el más adecuado para aplicaciones con requerimientos de tiempo real es el servicio garantizado, aunque es más complejo de implementar que el servicio de carga controlada.

- *Classic* RSVP

RSVP define dos sentidos para la transferencia de sus mensajes de señalización, *downstream* y *upstream*. El flujo *downstream* se efectúa desde la fuente al receptor o receptores, y el flujo *upstream* en sentido contrario.

PATH y RESV son dos mensajes básicos del protocolo RSVP y son en definitiva los mensajes a través de los cuales se lleva a cabo la reserva de recursos en la

red previa a la comunicación. Los mensajes PAHT son generados por la fuente de mensajes de usuario necesitados de garantía de QoS e indica las características de éstos en cuanto a recursos que necesita. La ruta que deben seguir estos mensajes es la misma que siguen los datos de usuario, para lo cual se requiere previamente un «diálogo» entre el proceso RSVP y el proceso de *routing*, pues dicha ruta quien la determina es el protocolo de *routing*, de lo contrario para nada serviría RSVP.

En su paso por cada *router* RSVP los mensajes PATH se actualizan y se retransmiten, consiste esto en poner la dirección IP del router que lo actualiza y reenvía. Cada *router* RSVP también almacena la dirección del *router* anterior. Así, con los mensajes PATH se posibilita indicar al receptor, o receptores, no solo las características del tráfico de usuario, sino también la ruta por donde debe solicitar las correspondientes reservas de recursos. Los *routers* que no soporten RSVP transfieren transparentemente los mensajes PATH.

Los mensajes RESV son producidos por el receptor (o receptores) de los flujos de información de usuario, como «respuesta» a los mensajes PATH y solicitan a la red (a los *routers* RSVP) las correspondientes reservas de recursos para soportar la comunicación con cierta QoS, fluyendo hasta la fuente del flujo de datos de usuario, es decir, en sentido *upstream.* Con la información de ruta que suministran previamente los mensajes PATH, los mensajes RESV dirigen las solicitudes de reservas a los *routers* RSVP apropiados, esto es, por donde fluirán los streams de datos.

Los mensajes RESV´s especifican el ancho de banda mínimo que se requiere para obtener determinada demora en un flujo de datos específico. Vale decir además, que es posible efectuar reservas compartidas, esto es, una misma reserva aplicable a varios flujos de datos de usuario.

Estas reservas de recursos en los routers RSVP de la red se materializan mediante *soft-states* en dichos *routers*, estados que requieren para mantenerse de «refrescamientos» periódicos, por lo que durante toda la comunicación se necesita «señalizar» para mantener las reservas previamente efectuadas. En consecuencia, esto conlleva a cierta señalización «permanente» durante la fase de transferencia de información de usuario, con la consiguiente carga de tráfico que implica.

Vale decir también que la reserva de recursos extremo a extremo que posibilita RSVP será válida si, y solo si, la congestión y demora que introduzcan los *routers* no RSVP no es significativas.

Otros mensajes del protocolo RSVP son:

PATHTEAR: son mensajes generados por la fuente de datos de usuario para eliminar los estados *path* en todos los *routers* RSVP. Siguen la misma ruta que los mensajes PATH. También puede ser originados por cualquier nodo cuando se agota el *timeout* del estado *path*.

RESVTEAR: son generados por los receptores para borrar los estados de reserva en los *routers* RSVP, por tanto viajan en el sentido *upstream*. Pueden ser también originados por nodos RSVP al agotarse el *timeout* del estado de reserva de los mismos.

PATHERR: viajan en sentido *upstream* hacia el emisor siguiendo la misma ruta que los mensajes *PATH*, notifican errores en el procesamiento de mensajes *PATH* pero no modifican el estado del nodo por donde ellos pasan en su «viaje» hacia la aplicación emisora.

RESVERR: notifican errores en el procesamiento de mensajes RESV, o notifican la interrupción de una reserva. Se transfieren en la dirección *downstream* hacia el receptor o receptores apropiados.

- Protocolo básico

En la figura 2.2. se muestra de forma muy simplificada el intercambio de mensajes RSVP, específicamente mensajes PATH y RESV entre un emisor y dos receptores (A y B), indicándose que la reserva representada por el mensaje RESV_2 prevalece sobre la reserva representada por el mensaje RESV1, de manera que esto sugiere que la reserva solicitada por el receptor A es mayor que la solicitada por el receptor B. Esto es, la reserva «mayor» prevalece sobre la reserva «menor», así el *router* B sólo solicita al *router* A la mayor de las dos solicitudes de reservas a él llegadas desde el *router* C (originada por el receptor A) y desde el receptor B. Esto es una característica de RSVP.

Estas solicitudes de reserva conducen a que en cada *router* RSVP se establezca un estado soft (*Soft-State*), es decir, una reserva en cada *router* es un estado *Soft* con un determinado *timeout*, que debe ser refrescado periódicamente por los

receptores, de lo contrario vence el *timeout* y se deshace la correspondiente reserva, con la consecuente generación de un mensaje RESVTEAR.

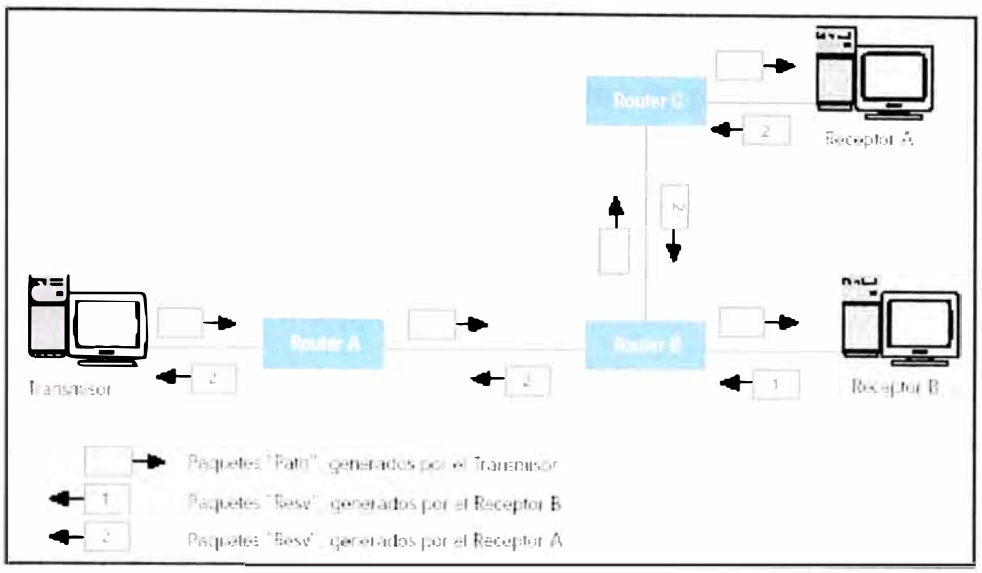

Figura 2.2 Intercambio básico de mensajes RSVP.

La liberación de recursos reservados mediante RSVP se puede materializar de diferentes maneras, así la solicitud para dar baja a determinada reserva puede ser originada:

- Por el emisor,
- Por el receptor, o
- Por un nodo de la red.

Por parte del emisor o de un receptor acontece cuando así lo decide la aplicación correspondiente, en cuyo caso esto se produce mediante la generación de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente.

Por parte de un nodo se lleva a cabo cuando vence el *timeout* correspondiente del estado *path* o del estado de reserva, lo que origina la emisión de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente.

2.4.3 Servicios Diferenciados

Se basa en «marcar» los paquetes IP, y luego la red (los *routers*) los tratarán en base a esa marca, esto es, se desarrolla un tratamiento diferenciado de los paquetes IP marcados en los *routers*. Define y utiliza diferentes tipos de *routers*. Esta diferenciación no es la misma en los diferentes nodos, sino depende de si se trata de un nodo interior o un nodo frontera. En consecuencia, y a diferencia de la

solución Servicios Integrados (basada en RSVP RFC 1633 [2]), la red con nodos Diff-Serv no establece ni mantiene estados de las conexiones por flujos de paquetes. Es una solución escalable, más apropiada para grandes entornos como Internet. Puede ser «fácilmente» implementada en las redes IP existentes.

La versión seis de IP contempla este «marcado» de paquetes, mediante el campo DS (*Differentiated Service*), byte DS de la cabecera IP. En la Figura 2.3 se muestra el formato del paquete IPv6. Como se puede observar, el *byte* de clase de servicio se puede utilizar como *byte* de servicios diferenciados, teniendo el mismo significado que en IPv4.

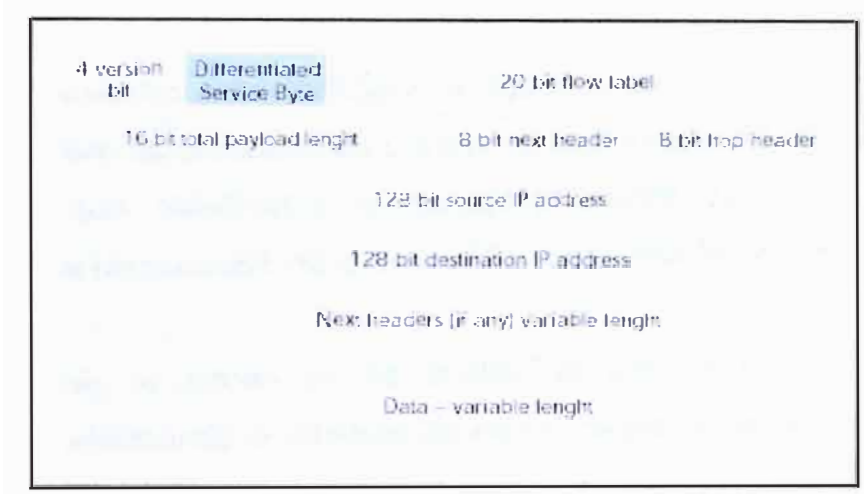

Figura 2.3 Formato del paquete Ipv6

También IPv4 permite dicho «marcado» de paquetes, a través del *byte* ToS (*Type of Service*), y en tal caso se utiliza éste como *byte* DS.

Se han definido dos tipos de Diff-Serv con garantía de QoS

- *Assured Forwarding Service* (AFS),
- *Expedited Forwarding Service* (EFS).

EFS equivale a una línea arrendada virtual, por lo que se garantiza cierto ancho de banda y reducida demora de cola. Emula un circuito.

Con el AFS los paquetes se etiquetan con «alta prioridad», aunque no se garantiza un ancho de banda. Se posibilita una QoS superior al servicio tradicional *best-effort* de Internet. Brinda cuatro clases de servicios, cada una con tres niveles diferentes de «*dropping*». Un nodo DS es, en principio, una combinación

de cinco módulos funcionales, aunque no todo *router* DS tiene que contener la totalidad de éstos:

- Clasificador de tráfico: clasifica los paquetes en base a uno o varios campos de su cabecera.
- Medidor de tráfico (*Traffic Meter*): mide las propiedades temporales de los paquetes.
- Marcador de paquetes (*Packet Markers*): establece un *codepoint* en el campo DS del paquete
- Conformador (*Shapers*): establece cierta demora para uno o más paquetes de un flujo.
- *Droppers*: descarta algunos o todos los paquetes de un flujo de tráfico.

Los tipos de *routers* en redes Diff-Serv se clasifican así:

First Hop Router: es el *router* más próximo al *host* emisor de paquetes. Los flujos de paquetes son clasificados y marcados acorde al SLA (*Service Level Agreement*). Es responsable de que el tráfico esté acorde con el ancho de banda del perfil.

Ingrees Router: se sitúan en los puntos de entrada al *backbone Diff-Serv* (dominio DS), efectuando la clasificación de los paquetes sobre la base del campo DS o sobre la base de múltiples campos de la cabecera de éstos.

Egress Router: se ubican en los puntos de salida de redes *Diff-Serv* (dominio DS), controlando el tráfico. Efectúan la clasificación de paquetes en base solo al campo DS de las cabeceras.

Interior router: Tienen la misión de «sumar» flujos, realizar la clasificación DS y reenvío de paquetes. Se sitúan dentro del backbone DS (dominio DS).

En la versión 4 de IP (IPv4) se emplea, como ya antes se dijo, el campo ToS (*Type of Service*) en la cabecera, que posibilita «marcar» cada paquete en base a cuatro tipos de servicios, a saber:

- Mínimo costo económico.
- Máxima fiabilidad.
- Máximo *throughput*.
- Mínimo retardo.

Sin embargo, este *byte* prácticamente no ha sido utilizado, pues los *routers* no procesaban esta información, además, con igual resultado se empleaban los bits

de prioridad. No obstante, es una posibilidad de obtener diferentes grados de QoS en IPv4, y puede emplearse como *byte* DS en redes Diff-Serv.

Ambas soluciones están basadas en modelos opuestos, en Diff-Serv la QoS es controlada por el emisor y en Int-Serv la QoS se controla por el receptor. Ahora bien, dadas las mejores características en cuanto a escalabilidad y grado de generación de tráfico de señalización que presenta la solución *Diff-Serv*, ésta se vislumbra como la mejor oferta para cubrir el sector *backbone*.

2.5 Redes MPLS (*Multiprotocol Label Switching*)

El crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y más sofisticados servicios, supone cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas a mitad de los años 90. Nuevas tecnologías de transmisión sobre fibra óptica, tales como *Dense Wavelength Division Multiplexing* (DWDM), proporcionan una eficaz alternativa al ATM para multiplexar múltiples servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM son desplazados por una nueva generación de *routers* con funciones especializadas en el transporte de paquetes en el núcleo de las redes. Esta situación se complementa con una nueva arquitectura de red conocida como *Multi-Prototocol Label Switching* (MPLS). MPLS se considera fundamental en la construcción de los nuevos cimientos para la interconexión de redes

El aspecto fundamental del MPLS, consiste en la clara separación entre las funciones de *routing* (es decir el control de la información sobre la topología y tráfico en la red), de las funciones de encaminamiento (es decir el envío en sí de datos entre elementos de la red).

MPLS es un estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También, como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "*tunneling*"). O como una técnica para acelerar el encaminamiento de paquetes. MPLS integra sin discontinuidades los niveles 2 (enlace) y 3 (red), combinando eficazmente las funciones de control del *routing* con la simplicidad y rapidez de la conmutación de nivel 2.

MPLS es el avance en la evolución de las tecnologías de *routing* y *forwarding* en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes. Los problemas que presentan las soluciones de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del *routing* con la rapidez del *switching*), MPLS ofrece nuevas posibilidades en la gestión de *backbones*, así como en la provisión de nuevos servicios de valor añadido.

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin discontinuidades. 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). Figura 2.4 Se representa la separación funcional de esos dos componentes, uno de control y el otro de envío.

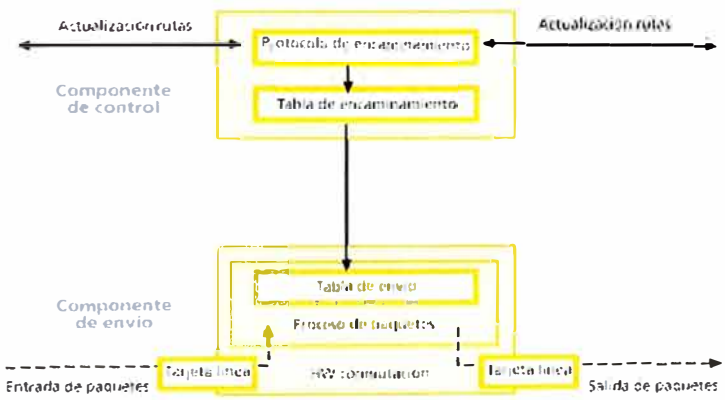

Figura 2.4 Componente de control y envío en MPLS.

El 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, el 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 el componente de control (encaminamiento) del componente de envío, cada uno de ellos se puede implementar y modificar independientemente. El único requisito es que el componente de encaminamiento mantenga la comunicación con el 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 la funcionalidad para ATM. La diferencia está en que ahora lo que se envía por el interfaz físico de salida son paquetes "etiquetados". De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento.

En cuanto a la etiqueta que marca cada paquete, se puede 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 FECs.

El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (*Label-Switched Paths*), funcionalmente equivalentes a los PVCs de ATM y Frame Relay. En el fondo, lo que hace es

imponer una conectividad entre extremos a una red no conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la diferencia básica con el modelo IP/ATM. Al hablar de MPLS con más detalle se entenderán mejor estas peculiaridades.

2.5.1 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 1997 se propuso como objetivo la adopción de un estándar unificado e interoperativo.

Ideas preconcebidas sobre MPLS

Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas inexactas sobre el alcance y objetivos de MPLS. Hay quien piensa que MPLS se ha desarrollado para ofrecer un estándar a los vendedores que les permitiese evolucionar los conmutadores ATM a *routers* de *backbone* de altas prestaciones. Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel, los recientes avances en tecnologías de silicio ASIC 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 RSVP

- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP

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

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

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

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

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

2.5.2 Descripción funcional del MPLS

La operación del MPLS se basa en los componentes funcionales de envío y control, aludidos anteriormente, y que actúan ligados íntimamente entre sí. Detallamos las tres componentes.

a) 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); 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.

En la figura 2.5 se puede ver la funcionalidad del MPLS aplicado a un paquete IP, aplicándosele el control y envío en su dominio. 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). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos a base de celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

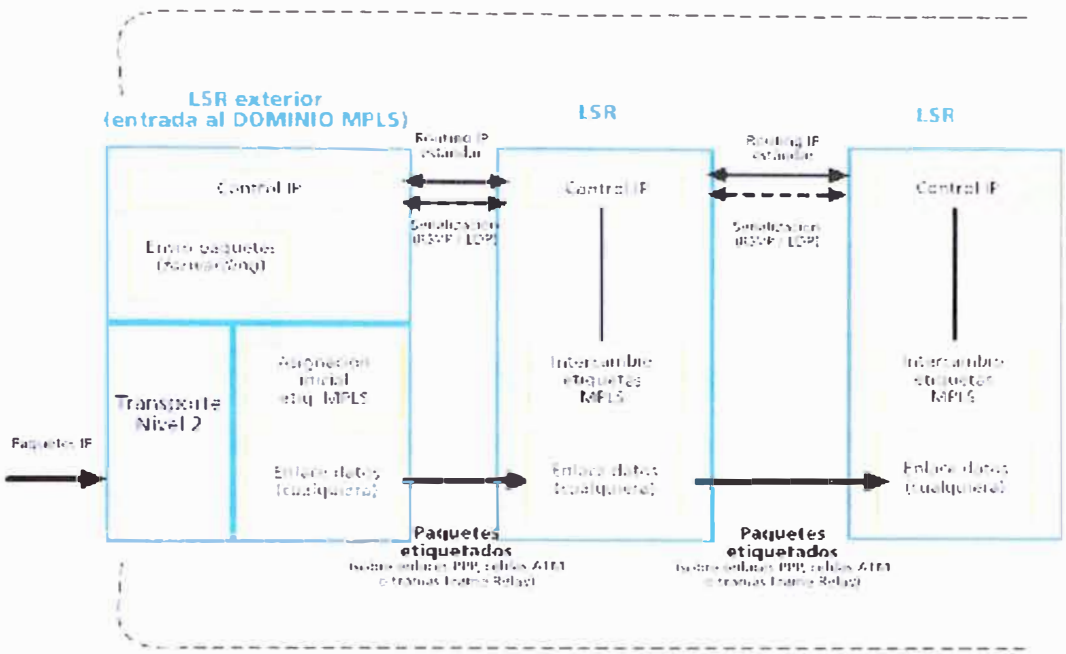

Figura 2.5 *Backbone* (dominio) MPLS

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 el componente de control (recuérdese el esquema de la figura 2.4), según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada / salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la figura 2.6 se ilustra un ejemplo del funcionamiento de un LSR del núcleo MPLS. A un paquete que llega al LSR por la interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por la interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

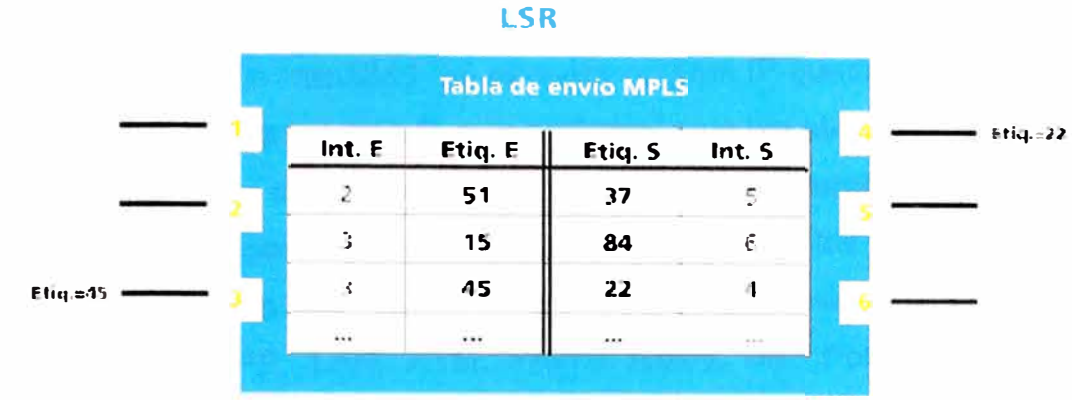

Figura 2.6 Ejemplo de operación de LSR.

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 2.7 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.

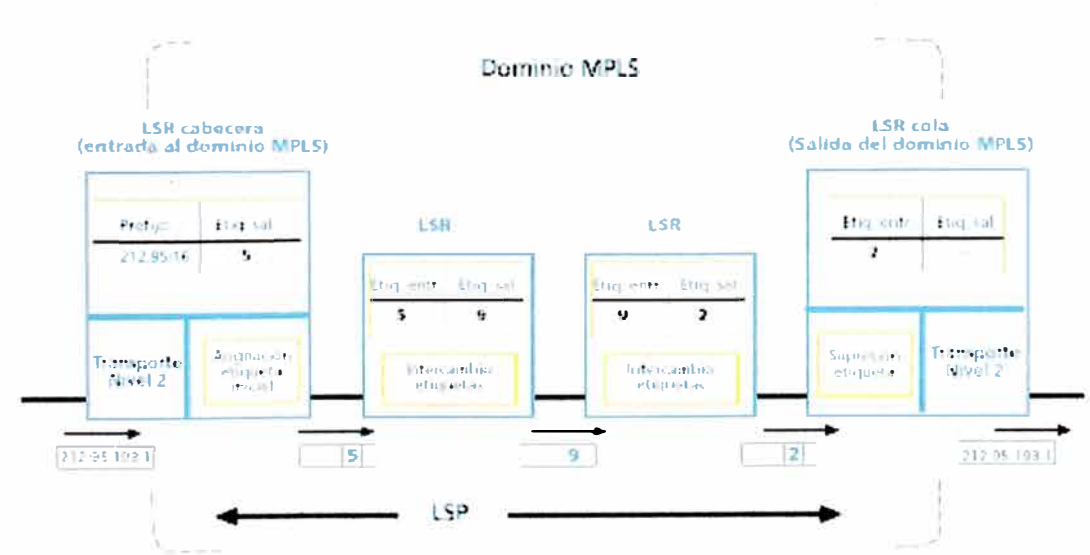

Figura 2.7 Ejemplo de funcionamiento de LSR en el dominio MPLS

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

En la figura 2.8 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.

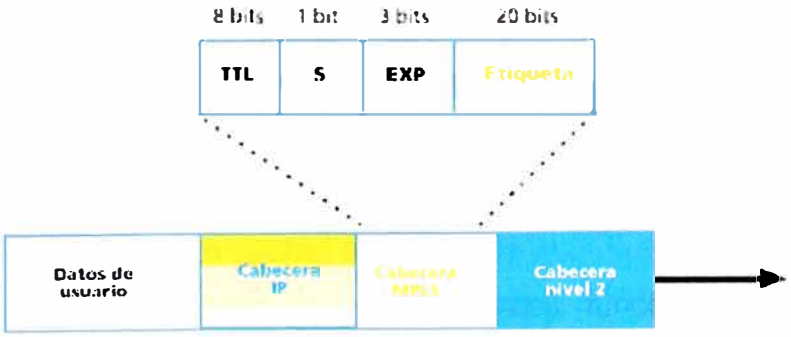

Figura 2.8 campos de la cabecera genérica MPLS

b) Control de la información en MPLS

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

¿Cómo se generan las tablas de envío que establecen los LSPs?

¿Cómo se distribuye la información sobre las etiquetas a los LSRs?

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

El segundo aspecto se refiere a la información de "señalización" (las comillas se ponen por el impacto que puede suponer este término para los puristas del mundo IP, de naturaleza no conectiva). Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; uno 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).

c) Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura 2.9, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red

convencional de *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.

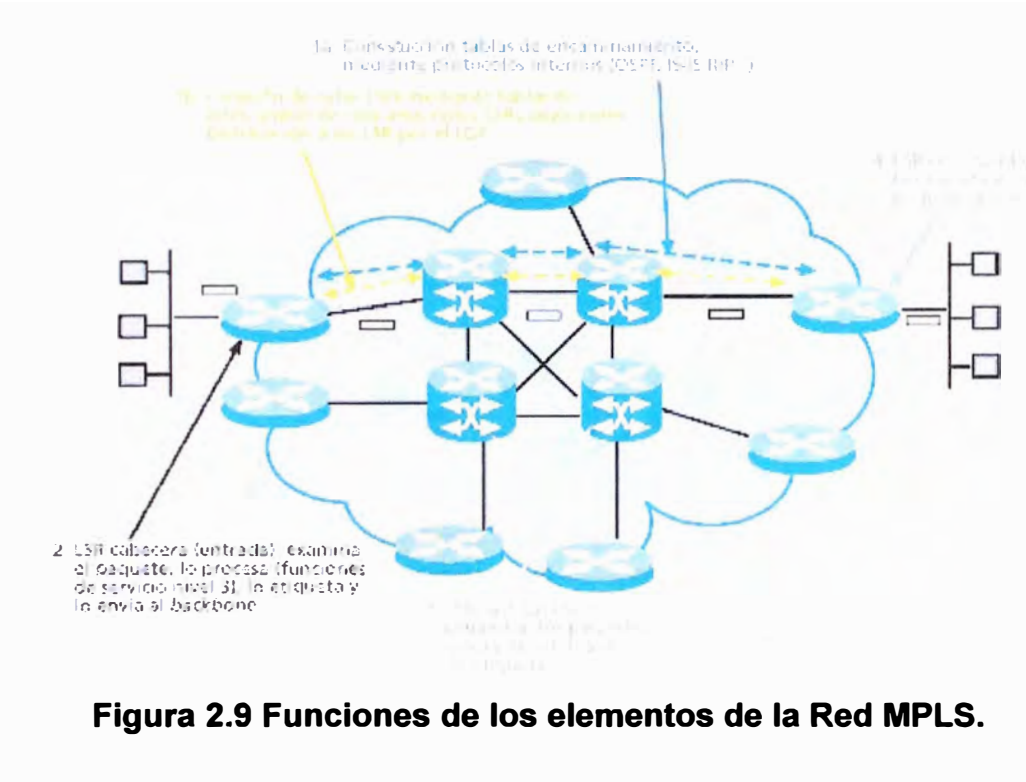

Figura 2.9 Funciones de los elementos de la Red MPLS.

2.5.3 Aplicaciones de MPLS

Las principales aplicaciones de MPLS en la actualidad son:

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

Describimos cada una, con las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

a) Ingeniería de Tráfico.

La persigue ingeniería de tráfico adaptar flujos de tráfico a recursos físicos de la red, de tal forma que exista un equilibrio entre dichos recursos. De esta forma se conseguirá que no haya recursos excesivamente utilizados, con cuellos de botella, mientras existan recursos poco utilizados.

Uno de los mayores problemas de las redes IP actuales es la dificultad de ajustar el tráfico IP para hacer un mejor uso del ancho de banda, así como mandar flujos específicos por caminos específicos. En las redes IP convencionales los paquetes suelen seguir el camino más corto. Por ejemplo, los protocolos IGP siguen este criterio. Esto suele provocar que algunos enlaces se saturen mientras otros están infrautilizados. Este problema se ha venido resolviendo añadiendo más capacidad a los enlaces. Como vemos en la figura 2.10.

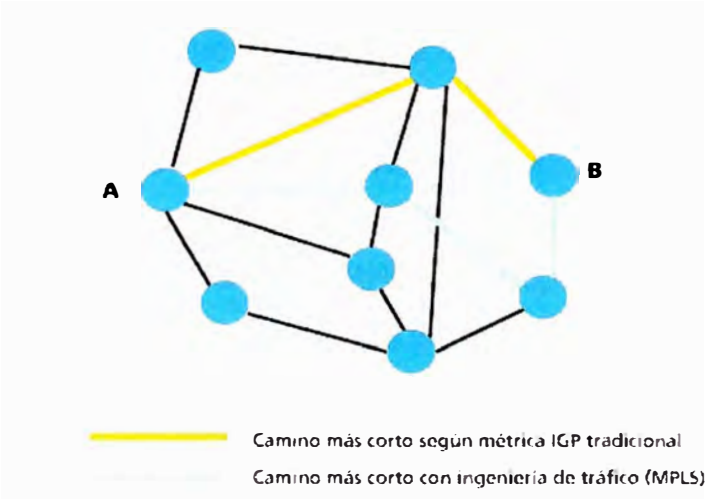

Figura 2.10 Aplicación de la ingeniería de tráfico.

El camino más corto entre A y C según la métrica normal IGP (protocolo de ruteo) es el que tiene dos saltos (A-B-C), pero puede que el exceso de tráfico sobre estos enlaces o la carga de los encaminadores hagan aconsejable la utilización de un camino que requiera saltos adicionales, como por ejemplo A-D-E-C.

MPLS es una herramienta efectiva para la ingeniería de tráfico:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso de un LSP.
- Permite usar el encaminamiento basado en restricciones de modo que el administrador de la red pueda seleccionar determinadas rutas para

servicios especiales con distintos niveles de calidad (por ejemplo, con garantías de ancho de banda, etc.).

b) Diferenciación de niveles de servicio mediante clases (CoS). MPLS soporta diferentes clases de servicio para cada LSP. Como caso particular, puede soportar servicios diferenciados en el mismo LSP.

Históricamente, La trasmisión de datos (caso Internet) ha ofrecido un solo nivel de servicio: "*Best effort*". Con la aparición de aplicaciones multimedia y aplicaciones en tiempo real, surgieron la necesidad de la diferenciación de servicios. De esta forma se podrán diferenciar servicios como el correo electrónico de otros que dependen mucho más del retardo y de la variación del mismo como el video y la voz interactiva.

El modelo de los servicios diferenciados define los mecanismos para poder clasificar el tráfico en clases de servicio con diferentes prioridades. Para clasificar el tráfico se emplea el campo ToS. A este campo se le llama DS en DiffServ. Una vez clasificados los paquetes en la frontera de la red, los paquetes se reenvían basándose en el campo DS. El reenvío se realiza por salto, es decir, el nodo decide por sí solo como se deberá realizar el reenvío. A este concepto se le denomina comportamiento por salto (PHB: *Per-Hop Behavior*).

MPLS se adapta bien a este modelo, ya que las etiquetas MPLS tienen el campo Exp para poder propagar la clase de servicio CoS en el correspondiente LSP. Por tanto, una red MPLS puede transportar distintas clases de tráfico. Entre cada par de LSRs exteriores se pueden tener distintos LSPs con distintas prestaciones y distintos anchos de banda.

c) Servicio de redes privadas virtuales (VPN).

Una de las principales razones del despliegue de MPLS en proveedores de servicios y redes empresariales son los servicios de VPNs (*Virtual Private Network*).

Inicialmente una red privada virtual no operaba necesariamente sobre MPLS es así que se define a una VPN como una red en la que la conectividad entre múltiples lugares se realiza a través de una infraestructura compartida con las mismas políticas de acceso y seguridad que en una red privada. Una compañía en la que su intranet corra encima de un servicio de VPN tendrá la misma seguridad, fiabilidad, etc, que el resto de sus redes privadas. Por tanto, el objetivo

de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables.

Las dos características más importantes de una VPN desde el punto de vista del usuario son la seguridad y la privacidad.

Las primeras WANs usaban líneas dedicadas para realizar sus conexiones. Estas redes tienen el inconveniente de ser caras, debido a la necesidad del alquiler de las líneas.

Posteriormente, con la introducción de las VPNs, se hace posible conectar múltiples sitios usando el *backbone* de un proveedor de servicios. Dicho proveedor ofrecerá servicios VPN a un precio inferior que con líneas dedicadas ya que el proveedor de servicios podrá utilizar los recursos de su *backbone* de forma compartida para múltiples clientes. Estas tecnologías de VPN se basaban fundamentalmente en protocolos de capa de red, típicamente Frame Relay, si bien también X.25.

Debido a que las soluciones existentes de aquel entonces no eran compatibles surgió un gran interés por las redes privadas virtuales basadas en IP que funcionarán en la red de redes (Internet) y que utilizarán estándares que funcionarán a través de múltiles proveedores de servicios. De esta forma se consigue una mayor flexibilidad en el diseño e implantación con unos menores costes de gestión y provisión del servicio. La forma de conseguir VPNs IP es construyendo túneles IP de diversos modos. El objetivo de un túnel IP es crear una asociación permanente entre dos extremos de modo que funcionalmente parezcan conectados. Se utiliza una estructura no orientada a conexión para simular dichas conexiones.

El inconveniente de este tipo de soluciones es que está basadas en conexiones virtuales punto a punto.

La configuración es manual, la provisión y gestión es complicada pues para una nueva conexión supone alterar todas las configuraciones anteriores, por ello plantean problemas de crecimiento.

La gestión de la 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 las VPNs IP es que están basadas en el modelo superpuesto, por lo que el número de adyacencias es elevado y la escalabilidad limitada.

Con una arquitectura MPLS se solucionan 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 2.11 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, a base de LSPs, y no de extremo a extremo a través de la red.

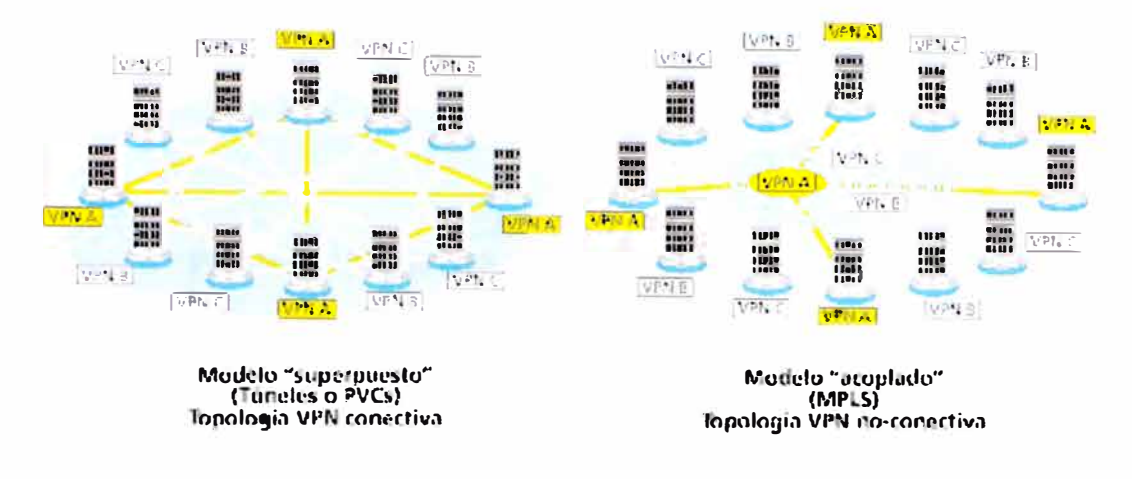

Figura 2.11 Modelo de VPNs convencionales y VPNs MPLS

En resumen las ventajas que ofrece MPLS para VPNs IP son las siguientes:

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

CAPÍTULO III
PLANTEAMIENTOS TECNICOS DE INGENIERIA

3.1 Características de diseño de redes

El diseño, instalación y operación de redes de datos es vital para el funcionamiento de las organizaciones modernas.

Si bien la implementación se lleva a cabo del nivel físico hacia arriba (respecto a OSI), el diseño se debe hacer del nivel aplicativo hacia abajo.

No se diseñan redes para ver que se puede poner a correr sobre ellas, más bien su diseño esta determinado por los requerimientos de los servicios que se tendrán: correo, voz, emulación de terminal, etc.

Dependiendo de las necesidades del usuario en cuanto al área a cubrir, la industria de telecomunicaciones ha diseñado tres tipos de redes, las cuales, hoy por hoy, ofrecen solución a cualquier demanda de los usuarios. Así, existen redes destinadas a dar cobertura a entornos locales, es decir, a diferentes departamentos de una misma compañía, un edificio o conjunto de estos, son las redes de área local (LAN).

Por otra parte, existen organizaciones e incluso conjuntos de ellas que necesitan mantener contacto permanente con otras o con ellas mismas si están dispersas geográficamente. Pensando en ellas, la industria ha desarrollado las denominadas redes de área amplia (WAN, *Wide Área Network*) y, como paso intermedio o nexo de unión entre las dos anteriores, se han comercializado las redes de área metropolitana (MAN, *Metropolitan Área Network*), las cuales unen edificios dentro de una misma área urbana.

Una empresa se plantea con el uso de una red de área amplia una serie de objetivos, entre ellos:

- Multiservicio (convergencia): soporte de datos, audio y video. Es decir servicios integrados a la medida de sus necesidades (integración de voz, datos e imagen, servicios de valor añadido)

- Calidad de servicio: priorización por tipo de aplicación ,administración y Monitoreo: soporte de protocolos como SNMP.
- Escalable, alta disponibilidad: redundancia en enlaces y componentes como fuentes de energía.
- Integración virtual de todos los entornos y dependencias, sin importar donde se encuentren geográficamente situados.
- Optimización de los costos de los servicios de telecomunicación.
- Flexibilidad en cuanto a disponibilidad de herramientas y métodos de explotación que le permitan ajustar la configuración de la red, así como variar el perfil y administración de sus servicios.
- Mínimo coste de la inversión en equipos, servicios y gestión de la red.
- Alta disponibilidad y calidad de la red (soporte de los servicios).
- Garantía de evolución tecnológica.
- Los diseños son raramente repetitivos.
- Combinación de reglas teóricas y experiencias practicas.
- Evaluación y selección de tecnologías de red
- Se aplica conocimiento de tecnologías, servicios, protocolos, experiencias implementaciones anteriores.

Las redes WAN sobre *backbone* MPLS, se plantean el reto de cubrir dichos requerimientos de las empresas.

3.2 Enfoques de diseño de Red

3.2.1 Recomendaciones generales para LAN

Todo diseño de Red corpotativa WAN debe tener un buen respaldo a nivel LAN, es así que se resume un conjunto de recomendaciones, que la empresa cliente debe garantizar para una funcionalidad óptima cuando el tráfico atraviese a nivel WAN se tiene:

- En redes muy grandes y de alto tráfico *broadcast* crear dominios de *broadcast* mediante VLAN´s y/o *routers*.
- Enrutar entre VLAN utilizando *swiches* nivel 3 o *router* de alta velocidad.
- Manejar 1 subnet IP por cada VLAN.
- Utilizar plataformas que permitan: priorización, monitoreo, administración de tráfico.

- Evitar desde el diseño los *loop* ya que al algoritmo *Spanning Tree* le toma de 30 a 50 segundos converger.

El diseño debe tener en cuenta el superar el enfoque tradicional en la cual se planificaba la capacidades determinadas de anchos de banda y ante problemas de congestión se incrementa el ancho de banda.

Las nuevas consideraciones, que se aplican tiene que ver con variables tales como: tiempos de transporte, fiabilidad, disponibilidad del servicio hacia los usuarios.

Durante el diseño se debe realizar un análisis, que permita absolver la inquietud: ¿Qué es lo que quieren los usuarios finales?, asimismo encontrar cual es el objetivo de diseño, frecuentemente: maximizar rendimiento, minimizar costes, etc.

Figura 3.1 Muestra un diseño LAN optimo dividido en capas de acceso, distribución y *backbone*, aplicable a redes LAN de gran tamaño.

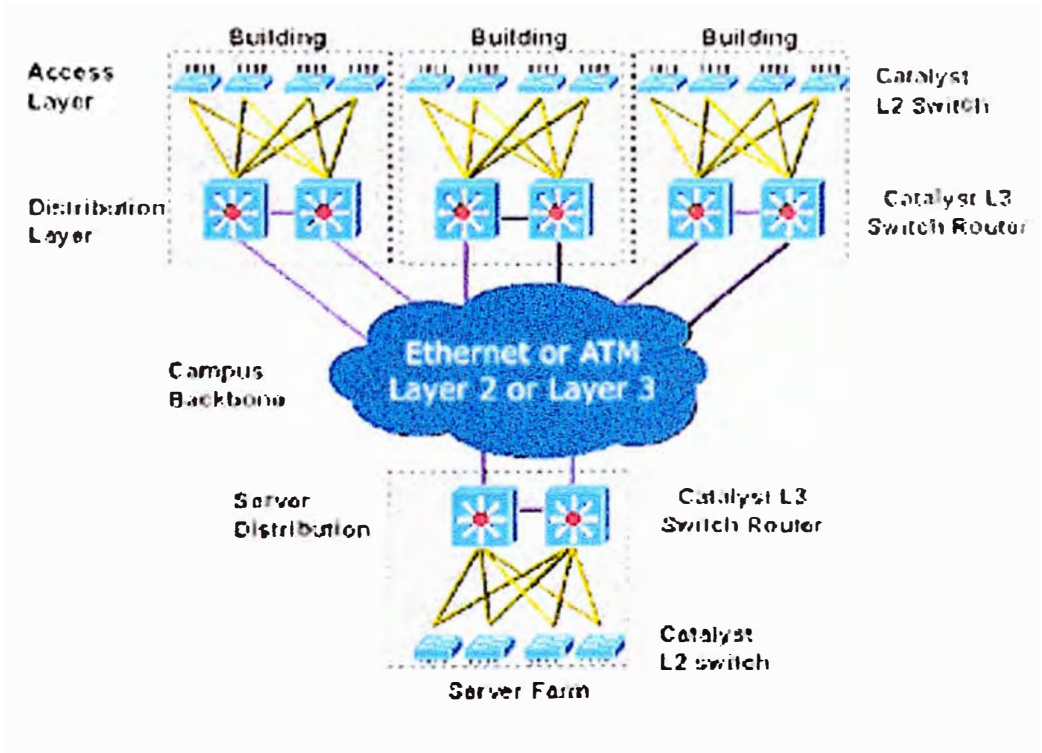

Figura 3.1 Diseño de una LAN de gran tamaño.

Asimismo es necesario tener presente que si desea integrarse e tráfico de voz y datos en un solo servicio, estamos en el ámbito de la voz sobre IP o sí fuera más

avanzado la Telefonía IP. Esto parte desde la red LAN donde se integrara el tráfico para transmitir a nivel WAN, por tanto es necesario. contar con:

- Centrales telefónicas con interfaces de red, TCP/IP y sistemas operativos convencionales.
- Teléfonos IP/Teléfonos Ethernet.
- Suministro de energía para los teléfonos, Alimentación Externa:

Requiere que cada toma donde se enchufe un teléfono tenga UPS.

3.2.2 Carácter de los servicios WAN

Es frecuente que los servicios WAN están asociados a ciertas premisas que deben tenerse en cuenta previo al diseño:

- Baja velocidad.
- Altos costos.
- Mayores retardos.
- Menor disponibilidad (más susceptible de fallas).
- Menor control (generalmente intervienen uno o más proveedores).
- Involucra generalmente varias tecnologías.

Factores fundamentales a tener en cuenta durante el diseño de la red WAN:

- Tiempo de conexión (permanente o temporal)
- Costos.
- Requerimientos de ancho de banda.
- Naturaleza del aplicativo y servicios que se implementaran.
- Sensibilidad a los retardos: Interactivo, transaccional, sensible a los retardos, ráfagas, etc.
- Requerimientos de calidad de servicio.

En este contexto surge un conjunto de recomendaciones generales, para encaminar un diseño WAN óptimo, tales como:

- Implementar una oficina piloto para obtener datos precisos de requerimientos (velocidades, retardos, etc).
- Utilizar tecnologías flexibles en crecimiento. Ejemplo: MPLS.
- Proveer un espacio físico para equipos en cada Oficina con acondicionamiento eléctrico (tierras, UPS, etc), ambientales (temperatura y humedad), seguridad y acceso.
- Escoger tecnologías sincrónicas sobre las asincrónicas.

- Implementar por lo menos una alternativa de contingencia (generalmente el servicio RDSI).
- Identificar equipos para facilitar diagnostico y solución de problemas.
- Capacitar por lo menos 2 personas en cada Oficina remota para facilitar el soporte remoto.
- Evitar al máximo el tráfico *broadcast*

Sustentado en ello es viable el establecimiento de las soluciones a nivel WAN. Se plantea el enfoque del diseño desde el Cliente y desde la empresa proveedora de servicios de telecomunicaciones, pero ello debe converger hacia una solución técnica única en beneficio del usuario final.

Como cliente (usuario de una empresa proveedora (*carrier*)): Implementa generalmente con tecnologías como: RDSI, Frame Relay y líneas telefónicas tradicionales. Generalmente utiliza un servicio de uno o más *carrier*.

Como proveedor (el *carrier*): Generalmente implementa con tecnologías como SDH, ATM, MPLS, hasta el equipo de capa 3 *router* e incluyendo como solución adicional *swiches*, y centrales.

El diseño tradicional de redes WAN utiliza modelos jerárquicos.

Donde se tiene modelos o arquitecturas de una capa (*one layer*), dos capas (*two layer*), tres capas (*three layer*) para el caso de esta ultima se tiene: *core*, distribución, acceso

- Una capa (*one layer*), Solo se tiene un nivel de *router*, típica de conexiones punto a punto, es el modelo más tradicional.
- Dos capas (*two layer*), generalmente implementado por empresas con oficinas en provincias o muchas oficinas en una ciudad, como ejemplo desde el equipo *router* de una provincia puede establecerse nuevas conexiones punto a punto con provincias mas alejadas con esto se reduce los costos del canal de larga distancia nacional o internacional.
- Tres capas (*three layer*), generalmente implementado por multinacionales, la conexión es en cascada donde una oficina remota debe atravesar mediante enlaces dos routers (de similar numero de Oficinas) antes de llegar al backbone del proveedor, caso típico de provincia alejada hacia capital departamental y de acá a capital de país, para recién establecer un canal de comunicación internacional, con lo que se obtiene el ahorro de

costos de la larga distancia nacional e internacional, ejemplo: caso de comunicaciones de voz.

En los nuevos diseños la arquitectura debe ser abierta y plana no necesariamente centralizada hacia determinada Oficina o nodo central de la empresa y es aquí donde se impone con fuerza las empresas proveedoras que cuentan con tecnología MPLS en el *backbone* y accesos de ultima milla por distintos medios de comunicación asociado a distintas tecnologías(TDM, ADSL, WiFi, microondas, VSAT).

Si finalmente todo va a ser datos: voz, video, etc. el *backbone* debe ser optimizado para este tipo de tráfico.

TCP/IP es el protocolo que se ha impuesto, por tanto el *backbone* debe ser optimizado para este tipo de tráfico.

El tráfico IP es el de más crecimiento más con los nuevos servicios y esquemas como VPN.

Figura 3.2 Muestra el esquema del *backbone* MPLS de una empresa proveedora de servicios de telecomunicaciones, atendiendo conexiones de voz y datos de extremo a extremo de una empresa cliente.

Figura 3.3 Muestra la operación de *routing* y conmutación del paquete de datos más la etiqueta al atravesar el *backbone* MPLS del proveedor.

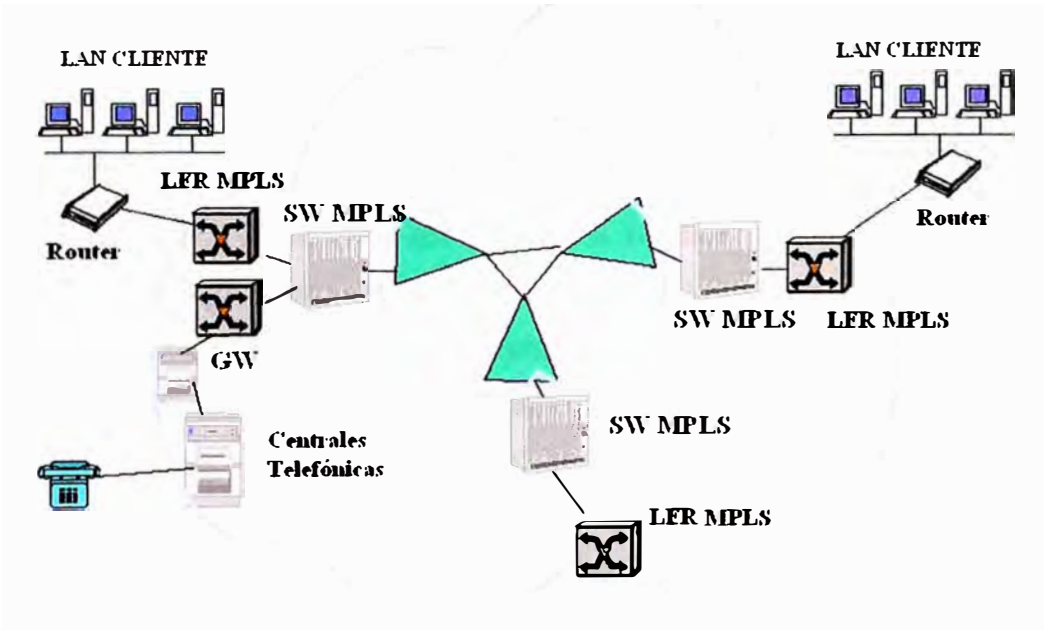

Figura 3.2 *Backbone* de carrier MPLS puro con IP

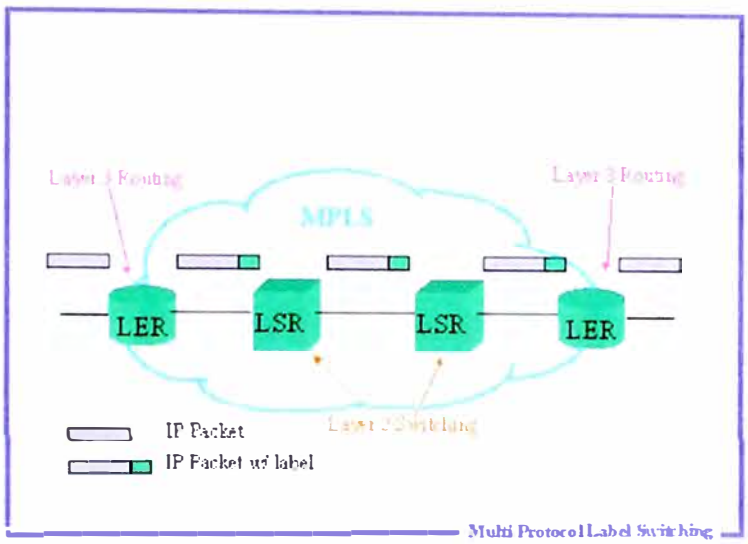

Figura 3.3 Esquema general de paquetes IP en MPLS

3.3 Recopilación de Información

El equipo diseñador, además de contar con propios conocimientos y experiencia, debe recopilar la información para desarrollar el Proyecto eficiente y esta debe abarcar todas las áreas de la empresa, tales como:

- La Alta dirección: Tener referencias de estrategias del negocio, presupuesto con que estimado para el Proyecto, fechas tentativas de contar con el servicio.
- Usuarios: Encuesta a cerca de funcionalidad actual de aplicaciones, necesidades futuras,
- Tecnologías: Tendencias en cuando a nuevas aplicaciones de: software base, manejadores de base de datos, plataformas de gestión administrativa, incorporación de telefónica IP, etc.
- Entorno del mercado: comportamiento en el ámbito financiero.
- Gestores de la red: Personal encargado de la administración y mantenimiento de la Red.
- Suministradores: empresas encargadas de dar soporte a los equipos de comunicaciones.
- Estándares: Internacionales, de mercado, de la empresa.

También debemos tener en cuenta el concepto de flujos es: decir del conjunto de información de aplicación y protocolo con atributos comunes tales como: Origen y destino de los datos, tipo de información.

Por lo cual se debe analizar el flujos de tráfico, con ello estimar el ancho de banda del enlace. Existen tipos de flujos individuales, compuestos y troncales.-

Flujos individuales: Con características específicas e identificables.

- Flujo compuestos: Con características de mejor esfuerzo, comparten el enlace
- Flujo troncal: De toda la red interna de la empresa

3.4 Aplicación al diseño de Red Corporativa

Se enfoca la aplicación de conceptos desarrollados, hacia interconexión de oficinas de las empresas para formar redes WAN de ultima generación, con el *backbone* MPLS del proveedor como soporte tecnológico.

3.4.1 Caso de estudio Red WAN con *backbone* MPLS

A continuación planteamos el caso de estudio de una entidad financiera para ilustrar la aplicación especifica en las plataformas de comunicaciones.

Se tiene una entidad financiera con 2 oficinas centrales (una es respaldo de la otra y están unidas por una fibra oscura propia) el cual debe interconectarse a 305 agencias remotas a nivel nacional y 200 cajeros automáticos.

Las Oficinas Centrales cuentan:

- Tráfico de datos: servidores *mainframe* marca IBM para agencias, servidores marca NCR para cajeros automáticos, arreglo de servidores *windows* XP *server* para aplicaciones administrativas, servidor *firewall* de seguridad.
- Tráfico de voz: central *Meridian* opción 61C con disponibilidad de 5 E1s PRI.
- Respaldo: se requiere alta disponibilidad de equipos de comunicaciones y enlaces en configuración de balanceo y redundancia.

Para las oficinas remotas se requiere:

- Tráfico de datos: Aplicación transaccional en protocolo TCP/IP para ventanillas en agencias, sistema administrativo cliente / servidor en Visual Basic, correo electrónico, Internet. (Se entiende por tráfico Internet la

navegación a paginas web de entidades financieras utilizando el protocolo HTML (*Hiper Text Markup language*) y descarga de archivos de servidores usando protocolo FTP (*File Transfer Protocol*).

- Tráfico de voz: encapsulación de voz sobre IP, con algoritmo de compresión G.729 y 2 canales de voz simultaneo.

Para los cajeros automáticos se requiere:

- Tráfico de datos: Aplicación transaccional en protocolo TCP/IP para cajeros automáticos.
- Respaldo: Se requiere que las líneas de comunicaciones tengan respaldo ante una eventual caída del enlace principal.

CAPÍTULO IV
SOLUCIÓN PROPUESTA

4.1 Alcances

Implantar una red WAN sobre la arquitectura MPLS contempla alcances técnicos y comerciales para una operatividad adecuada de la red. La herramienta de la ingeniería de tráfico que soporta una arquitectura MPLS, permite evaluar el funcionamiento global del tráfico de voz y datos requerido por las empresas clientes.

La red LAN remota accede al *backbone* MPLS mediante líneas de comunicaciones de ultima milla, por distintos medios y emplea diversos equipos de comunicaciones, todos ello formando la red WAN del cliente.

La implantación de una red VPN sobre *backbone* MPLS, no contempla los servidores, equipos LAN, centrales telefónicas que es equipamiento complementario a una plataforma de comunicaciones WAN y cuya responsabilidad de provisión y operatividad debe estar a cargo de la empresa cliente.

La meta de la conectividad de redes de las empresas clientes es facilitar procesamiento computaciónal corporativo, en la que los usuarios, de una organización, sean capaces de comunicarse entre sí y acceder a datos, servicios de procesamiento, aplicaciones y otros recursos, sin importar donde están localizados. El reto es proveer a la organización con facilidades de conectividad que cubran las necesidades de la arquitectura computaciónal empresarial sobretodo a un costo razonable. La compatibilidad es un factor clave en la provisión de conectividad entre todos los usuarios y recursos en la red empresarial.

La tarea de construir una red WAN de una empresa cliente consiste en interconectar diferentes redes individuales existentes de tal manera que constituyan un todo coherente. Estas redes generalmente usan tecnología de conectividad LAN, tecnología WAN o ambas.

En la mayoría de los casos se identifican las redes existentes de una organización dentro de dos categorías: redes departamentales y redes tradicionales. Las primeras usan tecnología LAN para interconectar sistemas y las redes tradicionales usan tecnología WAN para conectar mainframes o minicomputadoras a grupos de terminales. La mayoría de las redes empresariales deben incorporar la amplia variedad de LANs departamentales que han crecido en paralelo con las redes tradicionales WAN dentro de una organización.

4.1.1 Diseño de la Solución técnica del caso de estudio

En base al requerimiento mencionado en el capitulo III, se sigue una secuencia de diseño basado en:

- Ubicación de oficinas a interconectar
- Análisis del tráfico a cursar
- Planeamiento de la topología
- Planeamiento del ancho de banda
- Elección de la tecnología
- Costo y evaluación

Ubicación de oficinas a interconectar: Se identifica la necesidad de interconectar como:

Punto origen: La oficina principal 1 y su respaldo La oficina principal 2 ambas ubicadas en una ciudad principal que es cubierta por varios proveedores de comunicaciones.

Punto destino: Las oficinas remotas y los cajeros automáticos ubicados a nivel nacional (Lima y Provincias).

Análisis del tráfico a cursar: la clase de tráfico que se debe transportar es: Aplicativo transaccional para ventanillas de agencias, aplicativo transaccional para cajeros automáticos, canales de voz (voz sobre IP), correo electrónico corporativo y navegación a Internet.

La tabla 4.1 muestra que el tráfico con menor latencia será la voz y el de mayor latencia será el tráfico de datos (transaccional para cajeros automáticos, correo electrónico corporativo y navegación Internet).

Tabla 4.1 Clasificación de los tráficos por latencia y ancho de banda

Tráfico	Latencia	Ancho de banda
Aplicativo transaccional para Ventanillas de Agencias	medio	medio
Aplicativo transaccional para cajeros automáticos	alta	alta
Canales de voz	baja	baja
Correo electrónico corporativo	alta	alta
Navegación a Internet.	alta	alta

Planeamiento de la topología: En la figura 4.1 se esboza una topología de comunicaciones identificando la oficina principal 1, oficina principal 2 de respaldo, las oficinas remotas (agencias y cajeros automáticos), el *backbone* del proveedor, los enlaces de última milla de cada oficina, esquema referencia de equipos de comunicaciones de acceso y de enrutamiento. El objetivo es sintetizar la distribución de infraestructura y equipamiento que dan lugar a la plataforma de comunicaciones de una empresa. Lo que sintetizamos en la siguiente representación:

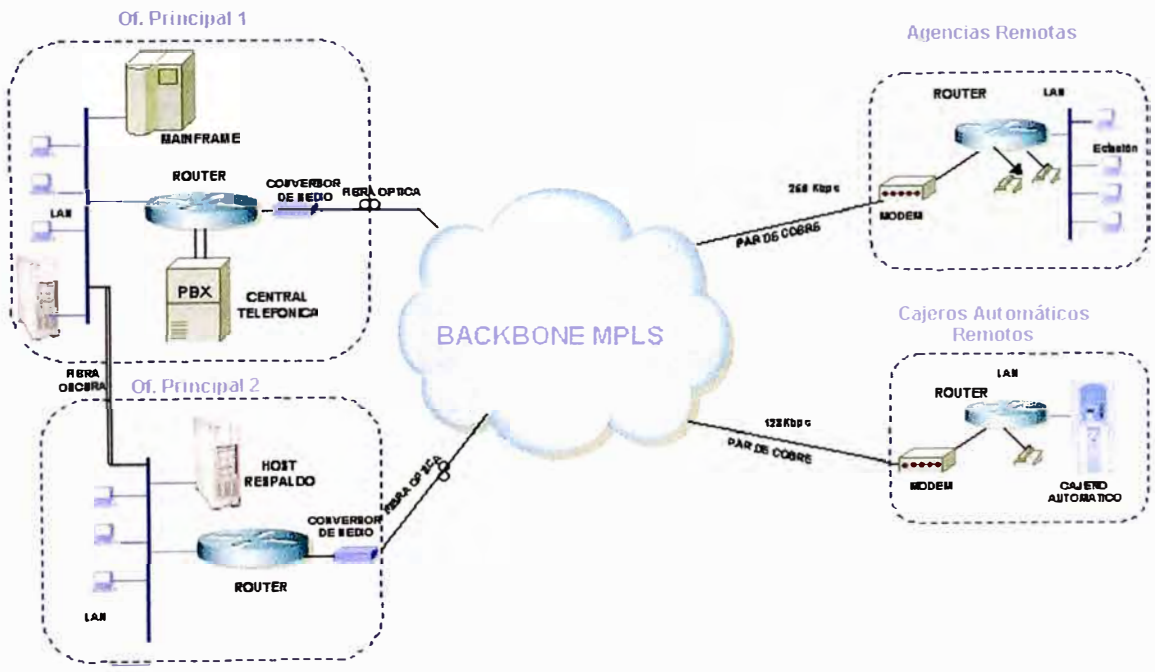

Figura 4.1 Red comunicaciones proyectada para la entidad financiera

Planeamiento del ancho de banda: El dimensionamiento del ancho de banda presenta la siguiente secuencia en las oficinas principales y las remotas.

El caso de estudio en mención tiene 02 oficinas principales (Oficina principal 1 y oficina principal 2 (respaldo)), 305 agencias remotas y 200 cajeros automáticos. La solución será atender a las 02 oficinas principales con enlaces de similar magnitud, configurando equipos y enlaces de tal modo que operan uno como respaldo del otro.

Para dimensionar el ancho de banda consideramos que cada agencia remota en promedio puede cursar tráfico a 256Kbps y cada cajero automático a 128Kbps cuyo sustento detallamos más adelante.

Basado en que se requiere conectividad de todas las agencias y cajeros remotos a la oficina principal nos encontramos ante una arquitectura centralizada de los servidores de datos así como de la central telefónica de voz de la entidad financiera, por tanto en caso de concurrencia total la velocidad necesaria seria 305x256 + 200x128 es decir 103680 Kbps o 103Mbps; esto implica que el procesamiento completo estaría en el nodo central, en aplicación de la regla 20/80, es decir, que el 80% de tráfico se trasladaría a nivel WAN hacia el nodo central y 20% de tráfico sería localmente en la oficina remota; se considera necesario que en la oficina principal se cuente con 80Mbps de ancho de banda.

Ahora identificamos los caudales a priorizar, encontramos que tenemos aplicativos para: transacciones financieras (soportadas en *mainframe*), aplicación para cajeros automáticos, tráfico de 2 canales de voz, correo electrónico e Internet, todos sobre el protocolo TCP/IP.

El tráfico más sensible es aquel en tiempo real con baja latencia y esto corresponde a la voz, que tendrá mayor prioridad en el diseño.

Considerando que las 305 oficinas remotas cursarán tráfico de 2 canales de voz en caso de comunicación simultanea serán necesarios en la oficina central 610 canales de voz. Considerando un factor de simultaneidad de 10%, serian necesarios 60 canales de voz. Para la compresión CODEC de voz se aplicará la norma G.729 para el cual reservamos 24Kbps por canal de voz en la WAN. Por tanto el caudal total necesario a priorizar seria 24x60 esto es 1440 Kbps

En consecuencia, el resto de caudal será asignado al tráfico de datos configurándose con una prioridad menor, ahora es aplicable la subdivisión en este tráfico de datos asignando mayor prioridad en el orden siguiente: tráfico transaccional de agencias, tráfico de cajeros automáticos, correo electrónico y navegación Internet.

Cada agencia remota cursará tráfico de dos (2) canales de voz, el ancho de banda necesario considerando la compresión de voz a un CODEC G.729 y adicionando tráfico cabecera se estima en 24Kbps por canal con lo que será necesario 48Kbps para ambos canales. Para el aplicativo transaccional de agencias reservamos 128Kbps, para tráfico de correo electrónico 32Kbps y navegación Internet 32Kbps.

Por lo que se ha estimado el ancho de banda de 256Kbps para cada Agencia remota siendo el valor comercial más próximo de las empresas proveedoras.

Cada cajero automático cursará el aplicativo transaccional propio para el cual reservamos 128Kbps, por lo que se ha estimado el ancho de banda de 128Kbps para cada uno de ellos coincidiendo con el valor comercial de las empresas proveedoras.

Elección de la tecnología: La conectividad de una Oficina en general tiene como elemento primordial al *backbone* de comunicaciones de la empresa proveedora de telecomunicaciones:

Siendo elemento primordial la tecnología del *backbone* a ser usada pues debe atender los requerimiento técnicos como:

- Conectividad completa de todas las oficinas remotas a las oficinas principales en protocolo no orientado a la conexión.
- Transporte íntegro de los datos en protocolo TCP/IP.
- Tolerancia a la latencia
- Tolerancia a la disponibilidad de la red
- Tolerancia al porcentaje de errores
- Priorización de tráfico
- Gestión completa de la red

Dado que nuestra red debe ser plana, abierta y escalable brindando conectividad de todos contra todos (caso especifico de tráfico de voz sobre protocolo TCP/IP), el *backbone* de la empresa proveedora soportara MPLS, proporcionando una red

VPN privada para la entidad financiera, cubriendo los requerimientos planteados. Siendo MPLS elegido para la solución técnica por las múltiples ventajas expuesta a lo largo de la sección 2.5.

Identificado el *backbone* la elección tecnológica de cada oficina se completa con el medio de acceso, equipo terminal de última milla, equipo de comunicaciones de capa 3.

En cuanto al medio de acceso que hará uso los enlaces de ultima milla para acceder al punto de presencia (nodo más cercano) del *backbone* del proveedor debe ser el de más alta confiabilidad; según sea el caso se elige la fibra óptica o par de cobre, asociado a la velocidad del enlace.

De igual modo se identifica el equipo terminal de datos de ultima milla a nivel de la capa de enlace OSI, el que será instalado en la oficina del cliente.

Posteriormente se dimensiona el equipo terminal (CPE: *Customer Premise Equipment*) a nivel de la capa 3 OSI, esto es el *router* con los distintos accesorios que cumplan con el requerimiento para cada oficina. Por ejemplo, en una oficina que utiliza canales de voz, se dimensionará el equipo con los módulos de voz necesarios.

Es preciso mencionar que debe considerarse desde un inicio el fabricante de equipos de comunicaciones en los que se soportará el diseño de la red. En particular mencionamos que el mayor fabricante de equipos de comunicaciones es *Cisco Systems* de USA, el cual es dominante en cuanto a arquitecturas con *backbone* MPLS así como en equipamiento de extremo LAN/WAN de la empresa cliente.

Nuestro diseño se sostiene en la arquitectura en hardware y sofware que proporciona dicho fabricante a sus equipos de comunicaciones.

A continuación se detalla el medio de acceso al *backbone* y equipamiento que harán uso por oficinas principales, agencias remotas y cajeros automáticos.

Las Oficinas principales, hacen uso del medio de acceso vía fibra óptica monomodo para acceder desde ambas ubicaciones (oficina principal 1 y oficina principal 2) hasta el nodo más cercano del proveedor, el equipo terminal de datos es un conversor óptico / eléctrico (MODEM óptico) que es conectado al equipo de capa 3. Este equipo de capa 3 será de marca Cisco, con características de procesamiento de CPU, memorias internas y módulos que soporte la cantidad de

oficinas remotas y los requerimientos de interfases. Es así como se considera un router Cisco modelo 7206 cuya capacidad de procesamiento es 400Kpps, con una capacidad de memoria: 48Mb Flash y 256Mb DRAM, así mismo se contempla 2 módulos PRI de datos por donde ingresarán llamadas de las oficinas remotas. Cabe mencionar que este modulo se conectará a la línea RDSI PRI de la red PSTN del proveedor.

El equipo que soportará el tráfico completo de voz de la WAN y hará de pasarela con la central telefónica (PBX) será el equipo de capa 3 Cisco AS 5350 con capacidad de procesamiento de 48.6, memoria flash de 64Mb, memoria DRAM de 256Mb y con 2 módulos E1s PRI los que serán conectados a interfases similares en la central telefónica (PBX) de la oficina principal 1.

Para obtener un respaldo completo de equipos y enlaces de acceso se duplican los mismos con determinadas consideraciones, el segundo enlace de acceso debe tener como destino un nodo distinto del proveedor, por una ruta alterna, y en referencia a equipos se considera uno similar al primero, pero estando en producción la red, este equipo debe mantenerse en *stand by* salvo avería del equipo principal. El fabricante Cisco desarrolló un Protocolo que permite dicha funcionalidad, dicho protocolo es el HSRP (H*ot Stand By Protocol*), que una vez aplicado a ambos *routers*, crea un tercer *router* virtual al cual apuntarán como *gateway* todos los servidores y estaciones en la oficina principal, ese tercer *router* nunca quedará inoperativo pues físicamente en todo momento puede ser cualquiera de los 2 *routers* reales: principal o el de *backup*.

Toda esta solución es aplicable bajo la arquitectura MPLS del *Service provider*, sobre la cual fluye tráfico TCP/IP y donde se forma la VPN privada para la entidad Financiera.

Para las agencias remotas, el medio de acceso en la ultima milla será vía par de cobre y el equipo terminal de datos de capa física es un MODEM digital que soporta la velocidad de acceso de 256Kbps En cuanto a la priorizacion de tráfico la voz es la que tiene la mayor prioridad, considerando 2 canales de voz para cada uno reservado 24Kbps. Por tanto, el ancho de banda reservado para el tráfico de mayor prioridad será 48Kbps, por lo cual tendremos el resto como tráfico para datos, dentro de ellos se subdividirá: el transaccional para ventanillas, Correo electrónico, Internet.

El equipo capa 3 considerado será un *router* marca Cisco modelo 2610XM con una capacidad de procesamiento de 20 Kpps, capacidad de memorias de 32Mb FLASH y 96 Mbps de DRAM, los accesorios serán: 1 puerta serial V.35 para conectar al MODEM, 1 puerta BRI para enlace de respaldo, 1 tarjeta FXS con 2 interfaces RJ48 para 2 canales de voz. A las interfases mencionadas se conectan 2 teléfonos analógicos y si la agencia cuenta con une centralita telefónica(PBX) es factible que las interfases FXS del router se conecten a troncales libres en la PBX.

La agencia remota también cuenta con una línea RDSI de respaldo al enlace principal dicha línea es conectada al modulo BRI del router, siendo este configurado para efectuar la conmutación automática.

En los cajeros automáticos el medio de acceso en la ultima milla será vía par de cobre y el equipo terminal de datos de capa física es un MODEM digital que soporta la velocidad de acceso de 128Kbps.

En cuanto a la priorizacion de tráfico, los datos tienen la mayor prioridad y es el único presente. El equipo capa 3 considerado será un router marca Cisco modelo 2610XM con una capacidad de procesamiento de 20 Kbps, capacidad de memorias de 32Mb FLASH y 96Mb DRAM, los accesorios serán: 1 puerta serial V.35 para conectar al MODEM, 1 puerta BRI para enlace de respaldo.

La funcionalidad completa de la VPN de la entidad financiera se completa identificando la cantidad de tráfico de larga distancia nacional que cursarán las oficinas remotas, para ser aplicadas en el *backbone* MPLS.

En cuanto a la alta disponibilidad en la red de la oficina principal 1, esto se completa con habilitar un enlace similar en la segunda oficina principal, la funcionalidad estará dada por una configuración que permita enrutamiento automático de los enlaces remotos al *router* de la segunda oficina principal.

Mas adelante esbozamos la topología final de la solución técnica del caso de estudio para la entidad financiera, ver figura 4.3..

Costo y evaluación

La plataforma de comunicaciones presenta costos de alquiler de enlaces de acceso, equipos de comunicaciones, gestión de la red y consultoria por implantación.

Las empresas proveedoras de servicios de telecomunicaciones ofrecen los servicios de desarrollo y ejecución de la solución técnica requerida por la empresa

cliente. Los planes tarifarios son regulados por el ente supervisor estatal en nuestro país es OSIPTEL (Organismo Supervisor de Inversión Privada en Telecomunicaciones), en cuyo portal podemos ubicar las tarifas tope que podemos tomar como para un costeo, que permita comparar con la propuesta de algún proveedor.

Resumen Técnico:

Hemos observado en la solución técnica del caso de estudio los beneficios tecnológicos de la arquitectura MPLS, aplicaciones de esta arquitectura son:

- Encaminamiento explícito e ingeniería de tráfico.
- Soporte a las CoS (Clases de Servicio)
- Servicio de redes privadas virtuales (VPN: *Virtual Private Network*)
- Integración de IP con todo tipo de redes subyacentes: Frame Relay, ATM, SDH, DWDM, etc.

4.1.2 Alcances de la solución técnica sobre *backbone* MPLS

El diseño de una red WAN, sobre *backbone* MPLS, para una empresa determinada plantea un escenario particular no necesariamente repetitivo, donde son aplicables conceptos teóricos de diseño y criterios sustentados en la experiencia practica en dicha tecnología, obteniendo un dimensionamiento óptimo para la solución técnica, se toma en consideración entre otros temas: tener una arquitectura robusta, escalable y redundante, en nuestro caso soportado por el MPLS. Estos elementos necesarios para brindar la conectividad de extremo a extremo, son: los medios de acceso de los enlaces de última milla, anchos de banda requeridos, hardware y software del equipamiento de comunicaciones WAN extremo empresa cliente, plataforma para monitoreo de los enlaces y equipamiento para los enlaces de respaldo.

La implantación de MPLS fue concebida para lograr aplicar las últimas tecnologías en el *backbone* de los *service provider* y ser la arquitectura base para una red WAN, buscando la optimización de recursos ante la evolución permanente de las aplicaciones de datos a transmitir.

Una de las mayores características del *backbone* MPLS son los distintos sistemas de comunicaciones de última milla a los que se adaptarán tales como: microondas, vía satélite, fibra óptica, par de cobre, *wireless*, etc; Los que son tomados en cuenta en los diseños de la red WAN. En cuanto a equipamiento de

comunicaciones la arquitectura abierta del MPLS, hace capaz el integrar diferentes fabricantes.

El ámbito de aplicación de las redes WAN sobre *backbone* en protocolo MPLS en la actualidad es a nivel nacional dentro de un país, si bien los enlaces internacionales entre países ya cuentan con dicha tecnología, recién se promueve su expansión aplicando a grandes empresas multinacionales.

El enfoque de la plataforma de comunicaciones a dimensionar es a nivel corporativo, empresas de distinto rubro, con volúmenes de tráfico diverso e independiente de la ubicación de sus oficinas.

En resumen en este informe profesional se da a conocer los beneficios del protocolo MPLS, mostrando el método de dimensionamiento para conectividad de las oficinas de una empresa cliente a través del *backbone* MPLS de una empresa proveedora.

4.2 Descripción de la solución técnica

En el marco de ofrecer un diseño de red WAN soportado en un *backbone* de última generación, la elección de la arquitectura MPLS es la alternativa tecnológica por la cual optan las empresas proveedoras.

El *backbone* de comunicaciones está compuesto por nodos distribuidos en todo el ámbito geográfico de cobertura de la red.

4.2.1 Topología de la Red de Comunicaciones

a) Descripcion de equipos de comunicaciones

La arquitectura de una plataforma de comunicaciones WAN sobre *backbone* MPLS, está formada por una variedad de dispositivos que permitan conectar sistemas de cómputo (redes) separados por grandes distancias a medios de transmisión públicos o privados para formar una WAN. Clasificamos como dispositivos de conectividad WAN los siguientes:

Módem

Es el elemento de acceso de ultima milla necesario para transmitir señales digitales, de las redes de cómputo, a distancias que impliquen ubicar el nodo más cercano del *backbone* de la empresa proveedora. El módem, es un dispositivo que convierte las señales provenientes de un equipo terminal de datos en señales adecuadas para que sean transmitidas por las redes telefónicas analógicas. Se utilizan en pares, uno por cada extremo de la línea.

Existen diferentes tipos de módems de acuerdo al medio seleccionado de transmisión:

- De línea conmutada.
- De radio.
- Vía microondas.
- Satelitales.
- De fibra óptica.
- Láser, entre otros.

Router

Un *router* (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de ordenadores / computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Los routers toman decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados. Los *routers* toman decisiones basándose en diversos parámetros, el más importante es la dirección de la red hacía la que va destinado el paquete (en el caso del protocolo IP esta sería la dirección IP), otro sería la carga de tráfico de red en las distintas interfaces de red del *router* y la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.

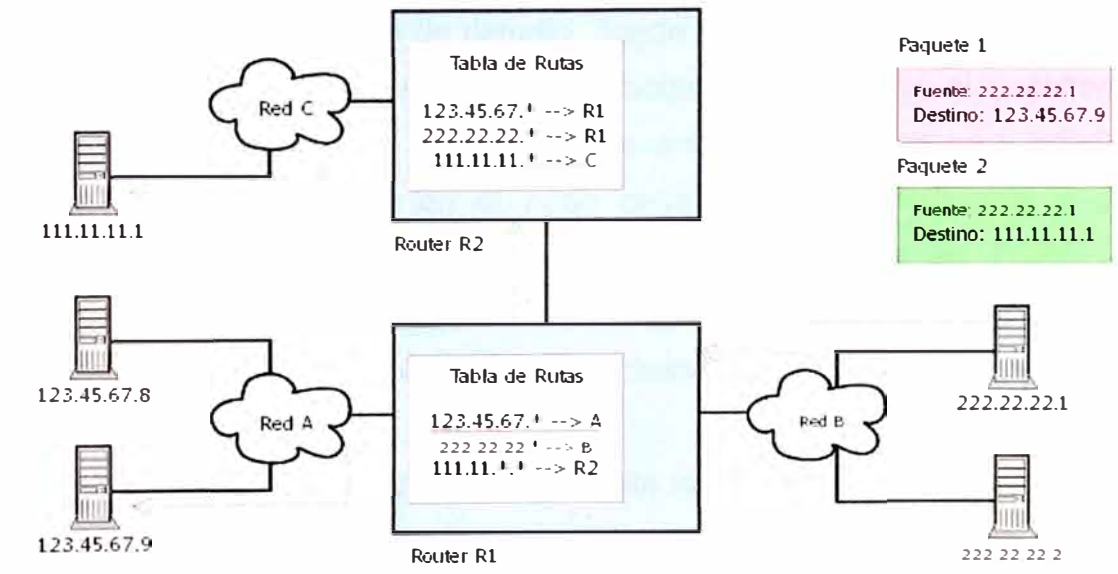

Figura 4.2 Operación de *routers* con sus tablas de rutas.

En la figura 4.2 se muestra como ejemplo 3 redes IP interconectadas por 2 *routers*. La computadora con el IP 222.22.22.1 envía 2 paquetes, uno para la computadora 123.45.67.9 y otro para 111.11.11.1 A través de sus tablas de enrutamiento configuradas previamente, los *routers* pasan los paquetes para la red o *router* con el rango de direcciones que corresponde al destino del paquete.
Nota: el contenido de las tablas de rutas está simplificado por motivos didácticos. En realidad se utilizan máscaras de red para definir las subredes interconectadas.
Los broadcast, o difusiones, se producen cuando una fuente envía datos a todos los dispositivos de una red. En el caso del protocolo IP, una dirección de *broadcast* es una dirección compuesta exclusivamente por números unos (1) en el campo del *host*.
Los protocolos de enrutamiento son aquellos protocolos que utilizan los *routers* o encaminadores para comunicarse entre sí y compartir información que les permita tomar la decisión de cual es la ruta más adecuada en cada momento para enviar un paquete. Los protocolos más usados son RIP (v1 y v2), OSPF (v1, v2 y v3), y BGP (v4), que se encargan de gestionar las rutas de una forma dinámica. Aunque no es estrictamente necesario que un *router* haga uso de estos protocolos, pudiéndosele indicar de forma estática las rutas (caminos a seguir) para las distintas subredes que estén conectadas al dispositivo.

b) Topología de la solución técnica del caso de estudio

Mediante la figura 4.3. se muestra la topología de comunicaciones de la entidad financiera presentada en el caso de estudio, donde se contempla la conectividad de las oficinas principales con las oficinas remotas, soportada en el *backbone* MPLS del s*ervice provider*, con distribución de enlaces y equipos para brindar redundancia, alta disponibilidad en el nodo central, enlaces dedicados y de respaldo en oficinas remotas, soporte a aplicaciones de datos en TCP/IP y encapsulando protocolos *legacy*. Se brinda conectividad de canales de voz sobre IP de todos contra todos. La VPN es de uso exclusivo por la red corporativa de la entidad financiera.
Las oficinas principales presentan enlaces de alta velocidad el medio es por fibra óptica aplicando tecnología *metro ethernet* para acceder al nodo MPLS, el equipo

de borde es un *router* Cisco 7206, también cuenta con un primario a la red publica RDSI para recibir llamadas de oficinas remotas.

Las Oficinas remotas agencias o cajeros automáticos usan el medio vía par de cobre el acceso hacia el nodo más próximo es por enlace dedicado TDM, el *router* de borde para ambos casos es un Cisco 2610XM, como respaldo al enlace principal usa el servicio RDSI que efectúa la conmutación automática, generando una llamada a la oficina principal.

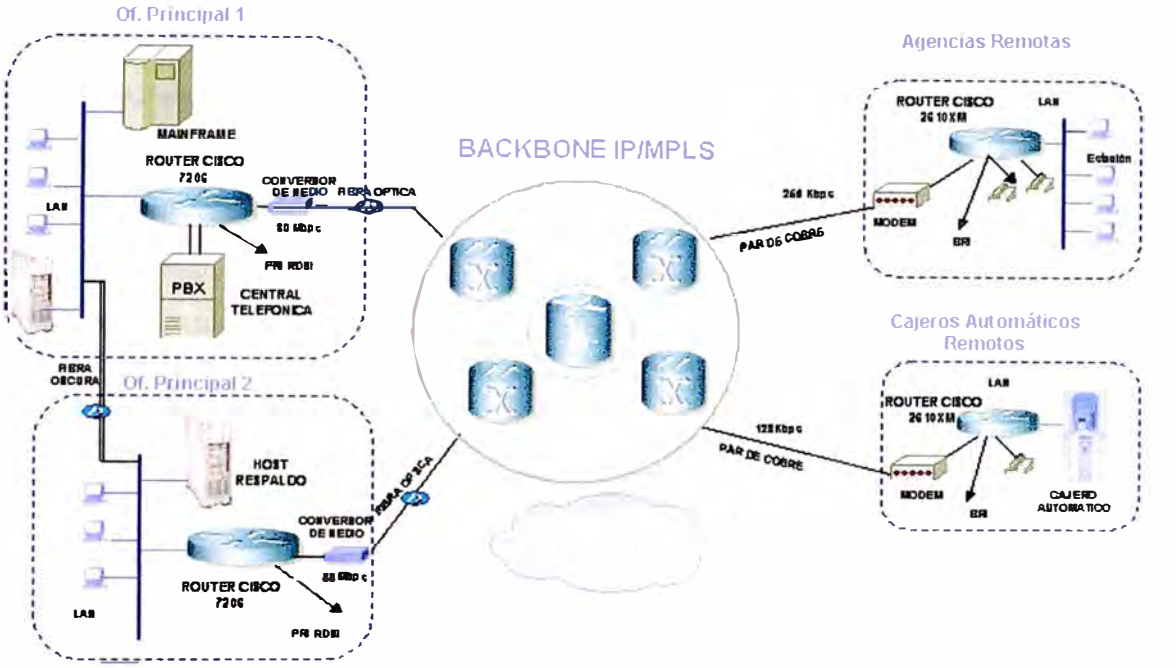

Figura 4.3 Red de comunicaciones sobre *backbone* MPLS

c) Operación interna de MPLS aplicado a la solución técnica.

La operación óptima de MPLS se mide cuando el usuario final percibe que es transparente al funcionamiento de sus aplicaciones. A continuación detallamos como MPLS establece enlaces no orientados a la conexión LSP, que trasportan paquetes IP etiquetados en el dominio MPLS hasta el equipo LSR de salida para ser nuevamente convertidos en paquetes IP normales y ser enviados mediante *routing* convencional al *router* destino CPE ubicado en el local remoto

En forma general vamos a definir la funcionalidad de conmutación de etiquetas entre LSR y formación de LSP para las oficinas principales, una oficina remota y un cajero automático en general.

Como se muestra en la figura 4.4, se inicia generando el tráfico (paquete IP normal de voz y datos) desde la oficina principal 1 con destino a la agencia remota, el LSR A es de entrada y recibe el paquete sin etiquetar consulta la tabla de encaminamiento y asigna el paquete a una clase asociada a la dirección IP destino (Agencia Remota), asimismo el LSR A asigna una etiqueta (por ejemplo de valor 6) y envía el paquete al LSR C que repetirá el mismo proceso hacia el LSR D. Es de notar que en el dominio MPLS los LSR no toman en cuenta la cabecera IP, solo se analiza la etiqueta de entrada y mediante el algoritmo de conmutación de etiquetas se reemplazará por otra. Volviendo a nuestro ejemplo, el LSR C asigna al paquete una etiqueta de salida de valor 5, finalmente dicho paquete llega al LSR D (que asigna una etiqueta de entrada con valor 8), dado que el siguiente salto será al equipo CPE de la agencia remota, por lo que el LSR D al consultar la tabla de conmutación de etiquetas quita ésta y envía el paquete IP normal, mediante *routing* convencional (ejemplo RIP versión 2) al CPE mencionado, llegando el paquete IP a su destino.

Los diferentes saltos desde el LSR A, LSR C y LSR D configuran el camino LSP 1 por el cual se transmitirá el tráfico desde la oficina principal 1 hacia la agencia remota.

De forma similar se configurarán caminos LSP para todos los escenarios, por tanto se tendrá:

- LSP 1: enlace entre oficina principal 1 con agencia remota, camino: LSR A, LSR C y LSR D
- LSP 2: enlace oficina principal 1 con cajero automático, camino: LSR A, LSR C y LSR E.
- LSP 3: enlace de redundancia entre oficina principal 2 con agencia remota, camino: LSR B, LSR C y LSR D
- LSP 4: enlace de redundancia entre oficina principal 2 con cajero automático, camino: LSR B, LSR C y LSR E.

Dado que existe una oficina principal 2, que opera como respaldo ante alguna posible avería de la oficina principal 1, se establecerían LSPs entre esta oficina,

las agencias remotas y cajeros automáticos respectivamente, en caso la oficina principal 1 sufra una incidencia.

Por tanto, se concluye que la VPN, que da lugar a la intranet privada tendrá como base los distintos caminos LSP a formarse entre las oficinas que requerirán transmitir tráfico y garantizándose la identidad del paquete original IP pues queda enmascarada durante su trasporte por la red MPLS.

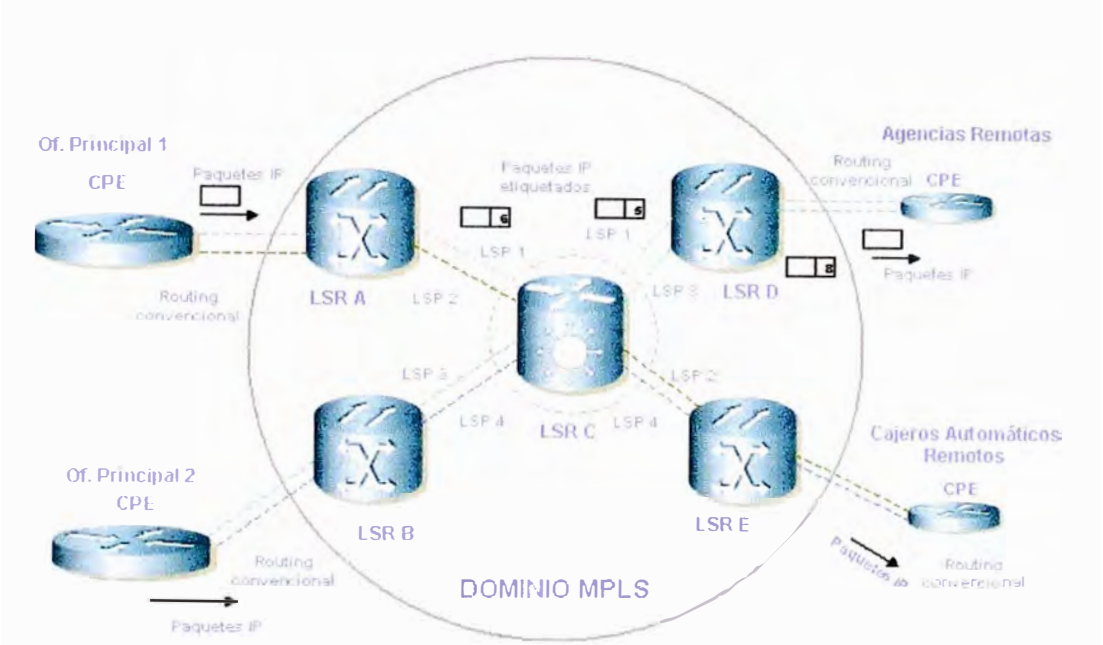

Figura 4.4 Operación de LSPs en el dominio MPLS

4.2.2 Cobertura

La solución técnica para una plataforma de comunicaciones WAN mediante un *backbone* MPLS del *carrier* contempla brindar el servicio durante las 24 horas del día, los 365 días del año, con el objetivo de garantizar un alto nivel de calidad y disponibilidad.

La calidad de la solución técnica se mide en función a parámetros tales como disponibilidad de la red, lo que operando en un *backbone* MPLS esta garantizado.

La disponibilidad del servicio debe cuantificarse en valores muy próximos al limite teórico 99.999%, cuantos más "nueves" de esos cinco se tengan de izquierda a

derecha, la calidad del servicio ofrecido será mayor. No obstante, en una red de un cierto volumen, ese "límite" será difícilmente alcanzable.

Los *carrier* para cubrir en su totalidad la interconexión de oficinas remotas de sus empresas clientes deben contemplar un plan de ubicación estratégica de sus nodos, basados en demanda de usuarios en la zona. Asimismo contar con diversas plataformas de acceso en la última milla, tales como par de cobre TDM, ADSL, SDH , VSAT, Metro *Ethernet.*

Deben conectar la oficina remota hacia el nodo MPLS más próximo mediante enlaces de elevada confiabilidad (sin interrupciones del servicio), ancho de banda escalable y bajo costo

Sin embargo ningún *carrier* puede cubrir con su infraestructura la ubicación de algunas de las oficinas remotas de sus empresas clientes, en esta situación se debe emplear mecanismos de ampliar la cobertura sustentado en un estudio de campo en la oficina remota del cliente.

Los estudios de campo pueden detallarse como visita de personal técnico especializado, que efectúa un levantamiento de información en la zona, ubicando la infraestructura actual y la faltante, definiendo que el medio de acceso a usar sea radio enlace para el cual debe ubicarse una línea de vista y lugar donde ubicar torres y antenas, en casos extremos se ve la necesidad de instalar un plato satelital, con los accesorios necesarios para garantizar su operatividad.

Culminada dicha labor el resultado reporta el medio de acceso más óptimo que será propuesto para la interconexión; dependiendo del soporte que pueda brindar un *carrier* podría emplear: par de cobre (dedicado, ADSL), fibra óptica (Ethernet, SONET, DWDM), radio enlace (microondas, *Wireless*), satélite (TDMA, VSAT), los que involucran un tiempo de implantación por encima de lo normal y costo diferente a lo convencional, debido al estudio para ampliar la cobertura y atender una oficina especifica.

4.3 Gestión de red

La gestión se está convirtiendo en un elemento esencial para asegurar la disponibilidad tanto física como lógica de las redes de área extensa. La complejidad de las actuales redes impone la necesidad de utilizar sistemas de gestión capaces de controlar, administrar y monitorizar redes locales,

metropolitanas y extensas, a la vez que dispositivos de interconexión, servidores y clientes.

En la actualidad existen diferentes niveles en la concepción de las herramientas de ayuda a la gestión; cada uno de estos niveles permite acometer una problemática particular del entorno de redes y en general no están integrados en un único sistema capaz de proporcionar una visión completa de los subsistemas que conforman las redes.

La tendencia en la evolución de la tecnología de gestión de redes se encamina hacia el desarrollo de productos integrados capaces de gestionar conjuntamente subsistemas de voz, datos e imagen en sus diferentes niveles: medio físico de transmisión, redes, aplicaciones, etc.

El *backbone* MPLS debe poseer en si su propio centro de gestión a cargo de un equipo humano de presencia permanente, para garantizar los niveles de servicio que asegura dicha arquitectura.

El otro frente son los equipos de borde ubicados en el local de las empresas clientes, hacia donde se enfoca un conjunto de mecanismos de gestión orientados a garantizar al usuario final la disponibilidad de la red y soporte en el tratamiento de averías que pudieran presentarse en los enlaces.

Esta parte también debe comprender la gestión administrativa del servicio que involucra ampliaciones del dimensionamiento, nuevas oficinas a interconectar y asesoria de primer nivel en temas comerciales.

El concepto de gestión en el local de la empresa cliente toma aplicación practica en un equipo y aplicaciones que permiten facilidades arriba mencionadas; para ello se hace uso de algunos de los equipos:

- Servidor Windows NT pentium IV
- Servidor Sun Solaris modelo Sunblade 150
- Servidor Linux.

En el cual se instalan productos ó aplicativos de gestión tales como:

- HP Openview
- Patrol
- Cisco Works

Este equipamiento permite a la empresa cliente

- Visualizar estadísticas (por ancho de banda, protocolos, etc)

- Obtener graficas de cada enlace y reportes en línea de operatividad.
- Estadísticas de utilización de servicio.
- Detección automático de equipo nuevos a nivel WAN
- Utiliza protocolos SNMP, ICMP cuya modalidad de trabajos es de ejecución de captura/ envío de datos y pruebas de conectividad respectivamente.

- Para nuestro caso práctico contaremos con un servidor SUN con sistema operativo Solaris y soportado en ello, el aplicativo de gestión HP-Openview.

Por ejemplo el servidor SUN modelo sunblade 150, al que se habilita como servidor TFTP, para almacenar backup de las configuraciones de *routers* de la red WAN, server NTP, utilizado para sincronizar la hora de los equipos de la red del cliente, para facilitar la secuencia de eventos en la detección de problemas y su rápida solución. Siendo factible implementar un server syslog de almacenamiento de incidencias capturando alarmas que envían los routers en red de la empresa cliente.

Se activa el servicio DNS Server para reconocimiento de los *routers* de la empresa cliente, siendo esto equipos identificados mediante una descripción para facilitar su presentación de las alarmas como la generación de gráficas.

El software de gestión HP *Open View*, se personaliza para displayar y organizar las alarmas de una manera adecuada, permitiendo: configuración, filtrado de alarmas y eventos, correlación de eventos, personalización de mapas por topología. La figura 4.5 se muestra la red de *routers* de una empresa cliente, personalizando la distribución de nodos.

Servicios adicionales de monitoreo en línea como información de tráfico asociado a sus enlaces de acceso al *backbone* MPLS. La figura 4.6 muestra gráficas de tráfico total en línea y en la figura 4.7 se muestra gráficas por protocolos en línea

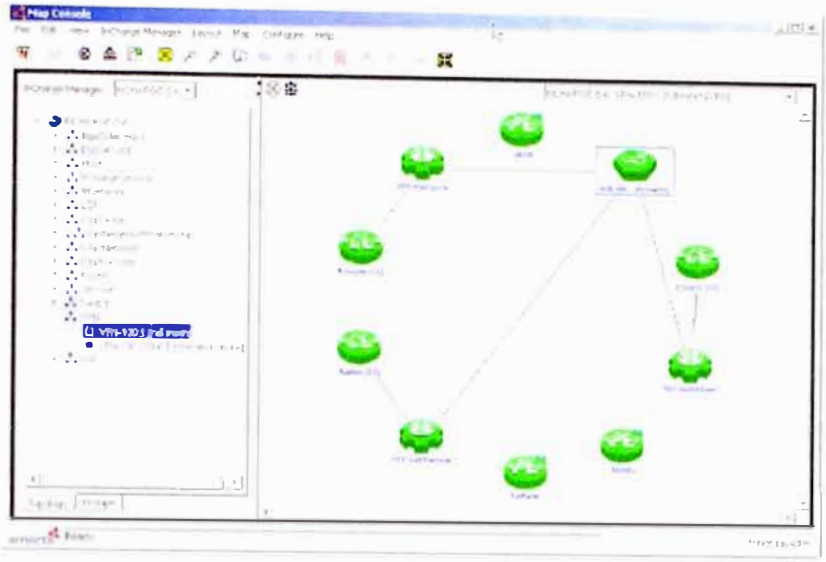

Figura 4.5 Personalización de mapa de red

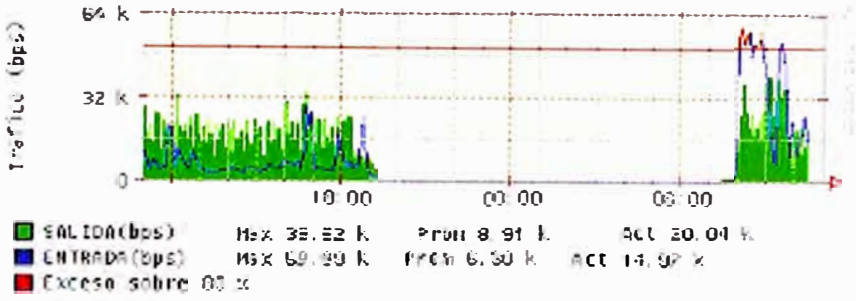

Figura 4.6 Tráfico total en línea

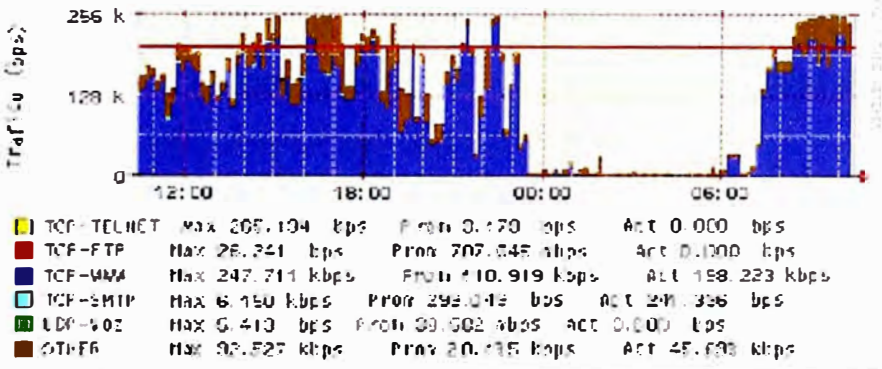

Figura 4.7 Gráficas por Protocolos

Las facilidades mostradas en las figuras 4.6 y 4.7 permite a la empresa cliente verificar su tráfico total y por protocolos en sus enlaces que tienen acceso al *backbone* MPLS, según los tipos de tráfico indicados en esquema.

4.4.1 Cronograma de actividades

La ejecución de una solución técnica va asociada a un conjunto de tareas a realizar de manera secuencial o paralela teniendo como meta la implantación total de la solución técnica culminando en la aceptación del servicio, teniendo claras las premisas comerciales asociadas del *carrier* hacia la empresa cliente que pueden identificarse como:

- Los precios del servicio deben ser cotizados en moneda nacional.
- Precio del puerto de VPN es de acuerdo al ancho de banda solicitado, servicio asociado y plazo de contratación elegido.
- El servicio a proporcionar requiere de un acceso local entre la oficina de la empresa cliente y el nodo más cercano de la red de c*arrier*.
- El acceso local esta sujeto a disponibilidad y cobertura del *carrier*.
- Cualquier equipo o servicio no frecuentemente relacionado con la implantación del servicio y que no se incluye en la cotización del *carrier* debe ser asumido por la empresa cliente o ser materia de cotización aparte.
- Los plazos de contratación varían partiendo desde contratación independiente del tiempo a plazos de 1, 2,3,etc años los normados por el ente regulador para los *carriers*.

Un cronograma de trabajo tiene representación grafica de tareas a las que se efectuaran seguimiento en función al avance del Proyecto, vericando tiempos, costos, uso de recursos (personas, equipos, etc).

Como se muestra en la tabla 4.2 podemos mediante un cronograma controlar tiempos de ejecución del Proyecto.

Tabla 4.2 Cronograma genérico de control de tiempos

Hito No	Descripción de actividades	Fecha relativa de duración
1	Aprobación del proyecto de comunicaciones	To
2	Reunión empresa cliente y carrier	To + 3 días
4	Inicio de los trabajos de infraestructura física	To + 5 días
5	Finalización trabajos infraestructura	To + 27 días
6	Instalación y configuración de equipos	To + 30 días
7	Habilitación de conectividad WAN	To + 35 días
8	Pruebas de conectividad y aplicativos	To + 40 días
9	Aceptación y fin de proyecto	To + 45 días

4.4.2 Plan de trabajo

La secuencia de tareas a ejecutar en la implantación del proyecto se plasma en un plan de trabajo del equipo de trabajo que implanta la solución técnica.

Plan del Proyecto:

- Selección de dispositivos piloto
- Conexión de *routers* a la red LAN de cada localidad
- Instalación y programación de líneas de comunicaciones, nodos locales y remotos
- Configuración de *routers* de extremo a extremo.
- Evaluación de desempeño de los enlaces pilotos
- Medición de resultados

Una vez que el plan se lleve a cabo, viene la parte de la operación que en este caso es otra actividad a considerar, debido a que los procedimientos en la atención y reportes de fallas se ven modificados, la forma en que los problemas serán atendidos cambiará. Entonces es conveniente firmar un acuerdo de nivel de servicio entre el proveedor que ofrece el servicio y el cliente, de tal forma que ambas partes entiendan cuales serán los procesos a seguir y los compromisos de cada parte a fin de poder resolver de una manera más expedita algún problema.

4.5.1 Equipo de trabajo

El equipo humano involucrado en la implantación de la solución técnica a nivel WAN sobre un *backbone* MPLS debe tener presente:

Convertir el plan de acción del proyecto para lograr el alcance: tiempo, costo y calidad establecida.

Este itinerario será utilizado como una base para controlar el proyecto.

Dicho equipo de trabajo es un conjunto de profesionales con alta especialización en plataformas de comunicaciones de datos, ellos deben cooperar para lograr un solo resultado general, esto es, la implantación satisfactoria del proyecto. La división del esfuerzo se enlaza en un solo resultado coordinado, donde el total es más y diferente, que la suma de sus partes individuales.

El rol de liderazgo del equipo de trabajo es fundamentalmente diferente de lo que con frecuencia se describe como el rol gerencial de planeación, organización, dirección y control. Los líderes del equipo están enfocados en el desarrollo continuo de capacidades de su equipo tanto que muchas de las responsabilidades asociadas con la administración y supervisión del grupo son gerenciadas por el grupo mismo. Como el grupo asimila más de estas responsabilidades de "supervisión", el líder del equipo está en una posición para trabajar en la expansión de su propio rol lo que facilita encaminar el cumplimiento oportuno de las tareas del cronograma del Proyecto.

4.5.2 Responsabilidades del proyecto

En esta sección del informe detallamos que responsabilidades incumben al *carrier* que proporciona la solución técnica de una red WAN sobre *backbone* MPLS y a la empresa cliente que contrata los servicios de comunicaciones.

Especificamos como responsabilidades directas del *carrier* el proporcionar desde su centro de gestión de la red:

- *Help Desk* (ayuda) a inquietudes técnicas de operatividad
- Mantener la Operación del Servicio
- Soporte técnico durante ampliaciones de servicio, nuevas instalaciones o averías de enlaces.
- Mantener el inventario de los equipos de comunicaciones en operación y un *stock* de respaldo a los mismos.
- Bases de datos de configuraciones de equipos, identificación de enlaces, dimensionamiento actual de cada enlace, líneas de respaldo y parámetros asociados.
- Garantizar el máximo de seguridad a las comunicaciones del cliente enfocando ello arquitectura técnica del Protocolo MPLS así como estándares para la gestión de equipos.

Como actividades de Soporte del Carrier se toma en cuenta:

- Análisis de la operación de la red de comunicaciones, para proporcionar a la empresa cliente futuras propuestas de ampliación del servicio u optimización de enlaces actuales.
- Desarrollo de procedimientos periódicos de revisión de totalidad de enlaces, y pruebas de enlaces de respaldo.
- El suministro de las piezas de repuesto necesarias para la reparación de los equipos en operación

Por otro lado las responsabilidades también alcanzan a la empresa cliente, esto se puede resumir en:

- Proveer en forma continua un medio ambiente adecuado para los equipos de comunicaciones de acuerdo a las especificaciones técnicas de cada uno de ellos.
- Proporcionar el suministro de energía eléctrica conforme a las especificaciones proporcionadas por cada equipo de comunicaciones.
- Respetar las especificaciones de utilización del equipo.
- Proveer al *carrier* acceso total, libre y seguro a sus instalaciones a fin que cumpla con sus obligaciones de mantener la operatividad del Servicio.
- Notificar al *carrier* de cualquier cambio en la ubicación física del equipo.
- No realizar mantenimiento o reparación del equipo proporcionado para operatividad del servicio.
- Designar a una persona responsable, la que será la autorizada a solicitar los servicios del *carrier* y/o ampliación del servicio,etc.

CONCLUSIONES Y RECOMENDACIONES

1. En el momento actual, todos los proveedores de servicios tienen ante sí el enorme reto de gestionar redes cada vez más complejas y extensas, con una mayor gama de servicios y con creciente demanda de ancho de banda, calidad y garantías. Para los *backbones*, las posibilidades que ofrecen la extensión de infraestructuras de fibra óptica y las nuevas tecnologías de transmisión son enormes. En este contexto, la evolución natural hacia redes IP y aplicaciones TCP/IP han llevado a desarrollar la arquitectura MPLS como una de las opciones más prometedoras para proporcionar los nuevos servicios del siglo XXI.

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel (o conmutación IP). La idea básica de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles dos y tres, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura.

Por otro lado, el hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte, no sólo sobre infraestructuras ATM, va a facilitar de modo significativo la migración para la próxima generación de la Internet óptica, en la que se acortará la distancia entre el nivel de red IP y la fibra.

MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas anteriores de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino). Además de poder hacer ingeniería de tráfico IP, MPLS permite mantener clases de servicio y soporta con gran eficacia la creación de VPNs. Por todo ello, MPLS aparece ahora como la gran promesa y esperanza para poder mantener el ritmo actual de crecimiento de las redes corporativas empresariales y la Internet.

2. Como conclusión fundamental puede decirse que el proporcionar redes de última generación tecnológica donde las aplicaciones evolucionan

permanentemente, viéndose la necesidad de proyectarse hacia redes de banda ancha que ya están ingresando al mercado local, se soporta el continuo crecimiento del tráfico del usuario final.

La integración en un solo medio de la voz, datos y video hace que estas nuevas redes sean respaldadas por otro medio de trasmisión y servicio distinto, para el caso de contingencia ante eventuales caídas del enlace principal.

La distribución del tráfico representado con el balanceo en los equipos de comunicaciones, encargados de trasmitir el tráfico, requiere de la misma disposición de líneas de comunicaciones a la misma velocidad de acceso.

3. La Ingeniería involucrada en el diseño de redes se ve reforzada con la presencia de un *backbone* de comunicaciones de última generación a través del protocolo MPLS que utiliza la inteligencia del *ruteo* y el desempeño del *switcheo* para disminuir el tráfico de rutas, la congestión, las fallas de conexión y los cuellos de botella.

Dado que en los últimos años el tráfico de redes ha aumentado considerablemente, al igual que la necesidad de transmitir cada vez más información en menos tiempo, como video y audio en tiempo real o *streaming* media, la solución no es solo aumentar el ancho de banda cada vez más, ya que en la mayoría de los casos esto no es posible y el ancho de banda es limitado, es aquí donde la administración efectiva de recursos que provee la calidad de servicio soportada por MPLS entra a relucir.

4. La tecnología MPLS es de aplicación masiva en nuestro país, los *carriers* han optado por esta tecnología de avanzada beneficiando la operatividad de las empresas, es así como desde entidades financieras, de servicios y manufactureras han implantado dicha tecnología ó migrado de alguna arquitectura *legacy*, beneficiándose con una red multiservicio que aplica calidad de servicio y reconoce todas las aplicaciones IP del cliente, priorizandolos y con posibilidad de seguir innovando aplicaciones para sus usuarios finales soportados en las funcionalidades de la nueva red.

5. Enmarcado en el contexto de una evolución tecnológica mayor de aplicaciones de Cliente, emerge los *backbones* MPLS de las empresas proveedoras a brindar el soporte tecnológico para el flujo del tráfico con la más alta eficiencia, es por ello que recomendamos la tecnología MPLS como la

integradora de las distintas tecnologías heredadas, que conviven y posibilitan su migración a una red multiservicio integrando los nivel 2 y 3 OSI mediante el encaminamiento y control de los paquetes de datos.

6. En el presente informe se trata de mostrar que la tecnología de VPN sobre MPLS permitirá a una empresa mejorar sus procesos internos para poder contar con esquemas de alta disponibilidad, balanceo de carga y ahorro; A fin de poder incrementar el nivel de utilidades, al reducir costos de operación mejorando los servicios a sus usuarios finales y en conjunto a la sociedad. Con el uso de éstas tecnologías se deben romper con paradigmas que muchas organizaciones tienen ideas poco claras por falta de información.

7. En las empresas que poseen redes *legacy* y van a migrar a tecnología MPLS, se debe ejecutar de manera ordenada, cautelosa, planeada y siempre pensar en respaldos durante la transición para poder regresar a las redes antiguas si fuera necesario, mientras se realizan ajustes y afinamientos de la nueva tecnología para la solución técnica particular de la empresa.

8. Con el objeto de obtener mayor seguridad y rapidez de transmisión de información en redes se recomienda aplicar las VPNs privadas sobre *backbone* MPLS, que son muy distintas a los túneles IP Sec convencionales, debido a que MPLS se encarga de reenviar paquetes a través de túneles privados utilizando etiquetas que actúan como códigos postales, dicha etiqueta tiene un identificador que la aísla a esa VPN.

ANEXO

Notas:

[1] Especificación ITU-T X.25, Red de conmutación de paquetes conforme con la recomendación UIT-T X.25 (Referencia X.412 (99))

[2] RFC 1633 – Servicios diferenciados para soporte de tráfico en tiempo real. Detallado en documento http://www.faqs.org/rfcs/rfc1633.html

Glosario de Términos:

AAA: Authentication, authorization, and accounting.

AAL: ATM adaptation layer.

AFS: Assured Forwarding Service

ANSI: American National Standards Institute.

ARIS: Aggregate Route-Base IP Switching

ARP: Address Resolution Protocol

ATM: Asynchronous Transfer Mode.

B channel: bearer channel.

Backbone: Serie de nodos de conexión que forman el eje principal de la red

Bc: Committed Burst.

Be: Excess Burst.

BECN: Backward Explicit Congestion Notification

BER: bit error rate

BERT: bit error rate tester

BGP: Border Gateway Protocol..

BGP4: BGP Version 4.

BOOTP: Bootstrap Protocol

BRI: Basic Rate Interface

CBR: constant bit rate.

CCITT: Consultative Committee for International Telegraph and Telephone.

CE: Customer Edge

CG: Centro de Gestión

CGI: Common Gateway Interface

CIDR: Classless Interdomain Routing

CIR: Committed information rate.

CoS: Class of Service

CPE: Customer Premise Equipment

CSMA/CD: Carrier Sense Multiple Access with Collision Detection

D channel: Canal D.

DCE. Data Communications Equipment

DE: Discard Eligibilit

DLCI: Data Link Connection Identifier

DS: Differentiated Service

DTE: Data Terminal Equipment

EFS: Expedited Forwarding Service

FCC: Federal Communications Commission.

FDDI: Fiber Distributed Data Interface.

FEC: Forwarding Equivalence Class

FECN: Forward Explicit Congestion Notification

FTP: File Transfer Protocol

HSRP: Hot Stand By Protocol

HSSI: High-Speed Serial Interface

HTTP: Hypertext Transfer Protocol

ICMP: Internet Control Message Protocol

IEEE: Institute of Electrical and Electronics Engineers.

IETF: Internet Engineering Task Force.

IGMP: Internet Group Management Protocol

IP: Internet Protocol

ISDN: Integrated Services Digital Network.

ITU-T: International Telecommunication Union Telecommunication

Kpps: Kilo packets per second

LAN: Local Area Network

LDP: Label Distribution Protocol

LSP: Label-Switch Paths

LSR: Label-Switch Router

MAN: Metropolitan Área Network

MPLS: Multi-Protocol Label Switching.

MTU: maximum transmission unit..

NNI: Network to Network Interfase

OSPF: Open Shortest Path First.

PABX: Private Automatic Branch Exchange.

PDU: protocol data unit.

PE: Provider Edge.

PHB: Per-Hop Behavior

POP: Point Of Presence

POTS: plain old telephone service.

QoS: Quality of Service

RFC: Request For Comments

RSVP: Resource ReSerVation Protocol

SLA: Service Level Agreement

SMDS: Synchronous Multimegabit Data Service

SMTP: Simple Mail Transfer Protocol

SNA: Systems Network Architecture.

SONET: Synchronous Optical Network.

STM-1: Synchronous Transport Module level 1

TCP: Transmission Control Protocol

TELNET: Conexión Remota

ToS: Type of Service

UNI: User to Network Interfase

VPN: Virtual Private Network

WAN: Wide Area Network

BIBLIOGRAFÍA

[1] B.T Doshi, S. Dravida, and P. Harshavardhana "Overview of INDT- a New Tool for next generation Network Design," IEEE GLOBECOM, Nov 13-17, 1995

[2] Halsall, "Comunicación de datos, Redes de Computadoras y Sistemas abiertos" Fred Halsall. Addison – Wesley Iberoamericana cuarta edición 1996.

[3] Jordi Palet, "Tutorial: Frame Relay" Autor: Jordi Palet, publicado por: Global Communications (Mayo 1997)

[4] J. García Tomás. Francisco Herrera Gálvez. Luis Merayo Fernández "La arquitectura de la RDSI-BA. Capa de Adaptación AAL".. Mundo Electrónico.Núm 275. Marzo 1997

[5] R.Andel, Manfred N. Huber, Stefan Shroder, "ATM Network Concepts, Protocols and Aplications". Addison – Wesley.

[6] ANDERSSON L. et al., "LDP Specification", Internet Draft, <draft-ietf-mpls-ldp-05.txt>, junio 1999

[7] AWDUCHE D.O. et al., "Requirements for Traffic Engineering Over MPLS", Internet Draft, <draft-ietf-mpls-traffic-eng-01.txt>, junio 1999

[8] CALLON R. et al., "A Framework for Multiprotocol Label Switching", Internet Draft, <draft-ietf-mpls-framework-04.txt>, julio 1999

[9] BLAKE S. et al., "An Architecture for Differentiated Services", RFC 2475, diciembre 1998

[10] LI T., REKHTER Y., "A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)", RFC 2430, octubre 1998

[11] NICHOLS K. et al., "Differentiated Services Operational Model and Definitions", Internet Draft, <draft-nicholsdsopdef-00.txt>, febrero 1998

[12] REDFORD R., "Enabling Business IP Services with Multiprotocol Label SWitching", Cisco Systems, Inc., White Paper, 1999 http://www.cisco.com/warp/public/cc/cisco/mkt/wan/ipatm/tech/mpls_wp.htm

[13] "Intranet and Extranet Virtual Private Networking", Cisco Systems, Inc., Technical Service Description,

[14] "Delivering New World Virtual Private Networks with MPLS", Cisco Systems, Inc., White Paper, http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/mpls_wi.htm

[15] Organismo Supervisor de Telecomunicaciones (OSIPTEL) http://www.osipetel.gob.pe/