

## 5. Capítulo 5: Implementación de redes conmutadas (Frame Relay, ATM y MPLS)

El desarrollo y la evolución de los conceptos de multiplexión y conmutación han permitido la implementación de soluciones eficientes para la interconexión de redes a nivel global. De esta forma han surgido distintas tecnologías de comunicación que permitieron el extraordinario crecimiento de internet, y por lo tanto favoreció a la revolución del comercio electrónico y las redes sociales. A continuación, se describirá en un orden cronológico de aparición las tres de las tecnologías más importantes: Frame Relay, una técnica de retransmisión de tramas que mejoró la eficiencia y la velocidad de transmisión en las redes WAN, luego se desarrollará ATM (Asynchronous Transfer Mode), la cual permitió el despliegue de redes de datos y voz integrados, y por último MPLS (Multi-Protocol Label Switching), un protocolo de conmutación de paquetes orientado a la conexión de capa 2 que, como su nombre indica, puede proporcionar un servicio de conmutación para una variedad de protocolos y aplicaciones, incluyendo IP, voz y video.

### 5.1. Frame Relay (Retransmisión de Tramas)

La técnica de retransmisión de tramas (Frame Relay) se diseñó para proporcionar un esquema de transmisión más eficiente que el proporcionado por X.25. Tanto las normalizaciones como los productos comerciales relacionados con la retransmisión de tramas aparecieron antes que los correspondientes a ATM, por lo que existe una amplia base de productos de retransmisión de tramas instalados.

Esta técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual fue introducida por la ITU-T a partir de la recomendación I.122 de 1988 y opera en la capa Enlace de Datos del modelo OSI. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos (“frames”) para datos, y que por sus características aplica la transmisión de grandes cantidades de datos. Su popularidad (años atrás, actualmente está siendo reemplazada por MPLS) se debe a que es relativamente más económico que alquilar una línea dedicada ya que sólo se paga por la cantidad de ancho de banda que se requiere. Ofrece anchos de banda en el rango de 56 Kbps a 2,048 Mbps (en EEUU hasta 1,544 Mbps).

Esta tecnología utiliza un subconjunto del Protocolo de Control de Enlace de Datos de Alto Nivel (HDLC) llamado Procedimiento de Acceso a Enlaces para Frame Relay (LAPF, Link Access Procedure for Frame-Relay). El tamaño de la trama es variable, normalmente hasta 4096 octetos (aunque también puede llegar hasta 8192 octetos).

La técnica de retransmisión de tramas puede utilizarse tanto como protocolo de transporte, como de acceso a redes públicas o privadas, proporcionando servicios de comunicaciones, aunque ha prevalecido el uso como protocolo de acceso. Especifica el método mediante el cual un dispositivo de usuario (router, bridges y hosts) puede interactuar con la red Frame Relay (nodos de conmutación FR).

Los dispositivos de usuario se conocen como equipos terminales de datos (DTE), mientras que los equipos de la red que hacen de interfaz con los DTEs, se conocen como equipos de terminación del circuito de datos (DCE). A esta interfaz se le denomina FRI (Frame Relay Interface) y está basado en la estructura de la trama LAP-D del canal de señalización de la RDSI. Las tramas se envían y entregan desde un DTE a otro DTE utilizando la red de Frame Relay que consiste, en general, de muchos conmutadores Frame Relay esparcidos geográficamente, los cuales se interconectan mediante líneas troncales (Figura 5.1.1). Esto quiere decir que todos los clientes de la compañía que provee el servicio de Frame Relay comparten la misma infraestructura.

Frame Relay no tiene mecanismos de recuperación de errores, porque fue diseñada para operar en canales digitales de alta calidad. Esto implica que protocolos en capas más altas sean responsables de la recuperación de errores.

Estas múltiples ventajas hacen de Frame Relay una buena tecnología para las necesidades de comunicaciones de datos y voz por sus bajos costos de operación, altas velocidades de transmisión y utilización eficiente del ancho de banda.

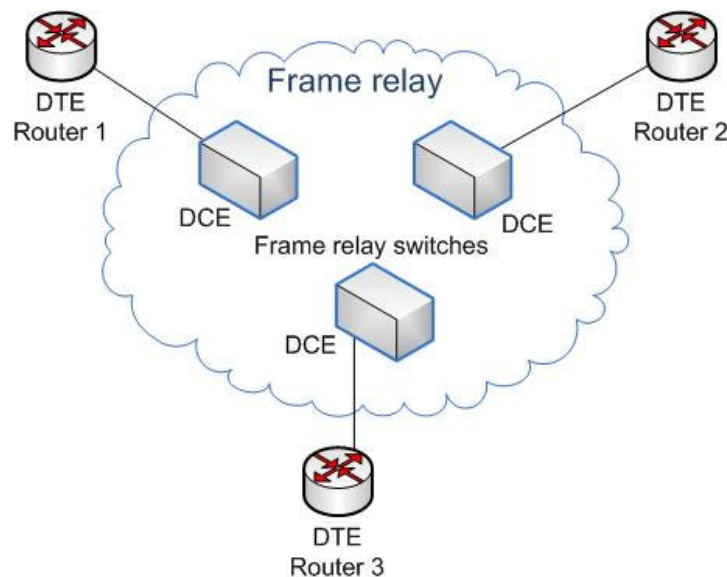


Figura 5.1.1: Componentes de una red Frame Relay

### 5.2.1. Terminología

Como toda tecnología de transmisión de datos, la retransmisión de tramas cuenta con terminología específica. A continuación, se describen cada uno de los términos:

#### Velocidad de acceso

La velocidad medida por reloj (velocidad de puerto) de la conexión (loop local) a la nube Frame Relay. Es equivalente a la velocidad a la que los datos viajan hacia dentro o fuera de la red.

#### Circuito Virtual (VC)

La conexión a través de la red Frame Relay entre dos DTE se denomina circuito virtual (VC). Estos conectan un DTE en una red con un DTE de otra red mediante la infraestructura de la red Frame Relay. Los circuitos virtuales pueden ser de dos tipos:

- Circuitos virtuales conmutados (SVC, Switches Virtual Circuits). Son aquellos que se establecen cuando los nodos necesitan comunicarse y se terminan cuando se completa la transmisión. Se establecen dinámicamente mediante el envío de mensajes de señalización a la red.
- Circuitos virtuales permanentes (PVC, Permanent Virtual Circuits). Son aquellos previamente configurados por la compañía de servicios.

El uso de PVC no significa que se cree un enlace dedicado ya que en el contrato con la compañía de servicios se especifican los extremos del circuito y la cantidad de ancho de banda que se requiere, pero no se especifica cómo llegar a los extremos y varios circuitos pueden compartir enlaces entre conmutadores Frame Relay. Los diversos circuitos virtuales en la línea de acceso única se diferencian mediante un Identificador de Canal de Enlace de Datos (DLCI, Data Link Circuit Identifier) para cada circuito. En la figura 5.2.1.1, el Router A tiene un PVC hacia el Router C, a través del DLCI 103, a su vez el Router C tiene un PVC hacia el Router B a través del DLCI 302.

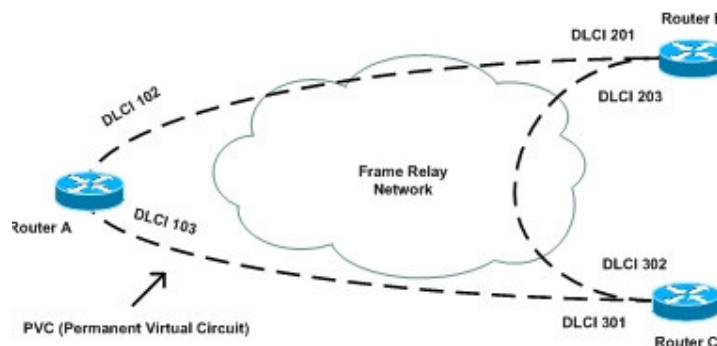


Figura 5.2.1.1: Circuito Virtual Permanente

### Identificador de conexión de enlace de datos (DLCI)

Es un número que identifica el extremo final en una red Frame Relay. Este número sólo tiene importancia para la red local. El switch Frame Relay asigna los DLCI entre un par de routers para crear un circuito virtual permanente.

Los DLCI sólo tienen significado local ya que son usados internamente por el proveedor de servicios para la conmutación de tramas entre los conmutadores Frame Relay. En la siguiente Figura 5.2.1.2 se pueden observar que en las oficinas ubicadas en Tucumán se cuenta con un acceso mediante una línea E1 y las sucursales de Córdoba y Santa Fé a través de enlaces de 512 Kbps. En este ejemplo se observa que Tucumán tiene configurado un enlace activo con el DLCI 400 (Santa Fé) y el DLCI 500 (Córdoba).

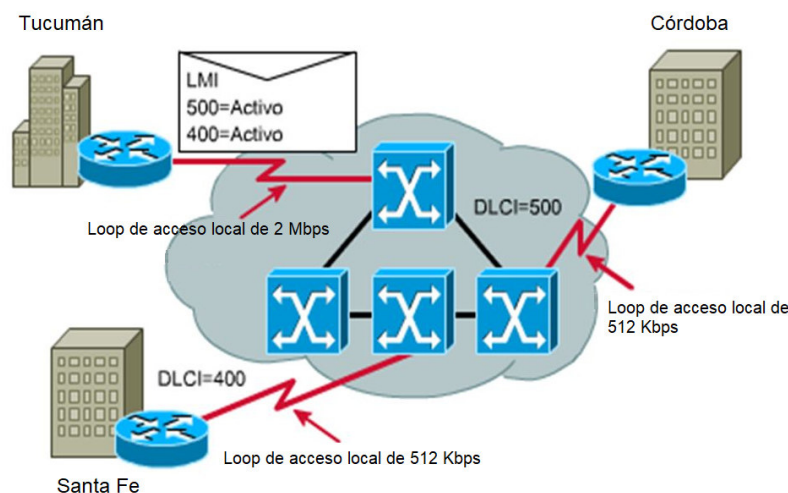


Figura 5.2.1.2: Enlaces activos desde Tucumán hacia Córdoba y Santa Fé

### Interfaz de Administración Local (LMI)

La Interfaz de Administración Local (LMI, Local Management Interface) permite transferir la información del estado de la red de forma dinámica entre el enrutador de una LAN (el DTE) y su conmutador Frame Relay más cercano (el DCE). La trama de Frame Relay tiene un campo de 10 bits para el DLCI usado para identificar el VC. Esto permite de 0 a 1023 valores. LMI utiliza algunos de estos valores para intercambiar información entre los DTE y los DCE. Del 16 al 1007 pueden ser usados para identificar los VC's (Circuitos Virtuales).

Existen varios tipos de LMI (Local Management Interface), todos incompatibles entre ellos. El tipo de LMI configurado en el enrutador debe coincidir con

el utilizado por el proveedor de servicios. En el caso de los enrutadores Cisco, estos soportan tres tipos de LMI:

- a. Cisco
- b. ANSI
- c. Q933A

Los mensajes LMI se envían a través de una variante de las tramas LAPF, pero el campo de dirección lleva uno de los DLCI reservados y hay un campo que indica el tipo de mensaje LMI. Los mensajes LMI comunican información acerca de lo siguiente:

- a. Keepalive (para verificar que los datos fluyen).
- b. Multicasting (para la distribución eficiente de la información por la red Frame Relay).
- c. Direccionamiento Global (para proveer significado global a los DLCI).
- d. Estado de los circuitos virtuales.

### **Velocidad de información suscrita (CIR)**

CIR es la velocidad garantizada, en bits por segundo, que el proveedor del servicio se compromete a proporcionar.

### **Ráfaga suscrita (BC)**

BC (Burst Committed), es la cantidad máxima de bits que la red se compromete a enviar, en condiciones normales, durante un intervalo de tiempo T. Estos datos pueden estar o no contiguos (pueden formar una o varias tramas).

### **Ráfaga excesiva (BE)**

BE (Burst Excess), es la cantidad máxima de bits no suscritos que el switch Frame Relay intenta transferir más allá de la CIR. La ráfaga excesiva depende de las ofertas de servicio que el distribuidor coloca a disposición, pero se limita generalmente a la velocidad de puerto del loop de acceso local.

## **5.2.2. Arquitectura del protocolo**

En la Figura 5.2.2.1 se muestra la arquitectura de protocolos para proveer servicios de transporte en modo trama. Se consideran dos planos diferentes de operación: plano de control (C), relacionado con el establecimiento y liberación de conexiones lógicas, y plano de usuario (U), responsable de la transferencia de los datos de usuario entre abonados. Así, los protocolos del plano C se implementan entre el usuario y la red, mientras que los del plano U proveen de funcionalidad extremo a extremo.

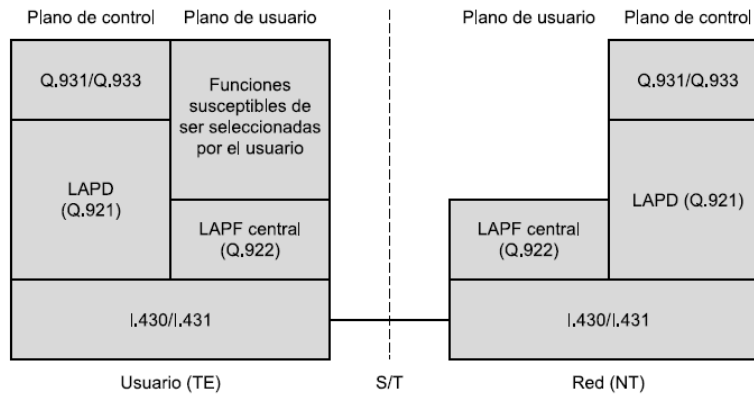


Figura 5.2.2.1: Arquitectura de protocolos para la retransmisión de tramas interface usuario - red

### Plano de control

El plano de control para servicios en modo trama es similar al de señalización por canal común para servicios de conmutación de circuitos por cuanto que se utiliza un canal lógico diferente para la información de control. En la capa de enlace se utiliza el protocolo LAPD (Q.921) para proporcionar un servicio de control del enlace de datos fiable, con control de errores y de flujo, entre el usuario (TE) y la red (NT) sobre el canal D. Este servicio de enlace de datos se usa para el intercambio de mensajes de señalización de control Q.933.

### Plano de usuario

Definido en Q.922, LAPF (procedimiento de acceso al enlace para servicios en modo trama, Link Access Procedure for Frame Mode Bearer Services) es el protocolo del plano de usuario para la transferencia real de información entre usuarios finales. En retransmisión de tramas sólo se usan las funciones básicas de LAPF:

- ✓ Delimitación de tramas, alineamiento y transparencia.
- ✓ Multiplexación/demultiplexación de tramas utilizando el campo de dirección.
- ✓ Inspección de las tramas para asegurar que éstas constan de un número entero de octetos, antes de llevar a cabo la inserción de bits cero o tras una extracción de bits cero.
- ✓ Inspección de la trama para comprobar que no es demasiado larga ni demasiado corta.
- ✓ Detección de errores de transmisión.
- ✓ Funciones de control de congestión.

La última función es nueva en LAPF, siendo el resto funciones también presentes en LAPD.

Las funciones básicas de LAPF en el plano de usuario constituyen una subcapa de la capa del enlace de datos. Esto proporciona el servicio de transferencia de tramas del enlace de datos entre abonados sin control de flujo ni de errores. Además de este hecho, el usuario puede seleccionar funciones extremo a extremo adicionales de la

capa de enlace o de la de red, las cuales no forman parte del servicio de retransmisión de tramas. De acuerdo con las funciones básicas, una red ofrece retransmisión de tramas como un servicio orientado a conexión de la capa de enlace con las siguientes propiedades:

- ✓ Se preserva el orden de la transferencia de tramas entre el origen y el destino.
- ✓ Existe una probabilidad pequeña de pérdida de tramas.

### 5.2.3. Transferencia de datos de usuario

El funcionamiento de la técnica de retransmisión de tramas, por lo que respecta a la transferencia de datos de usuario, se explica mejor considerando el formato de trama, mostrado en la Figura 5.2.3.1(a).

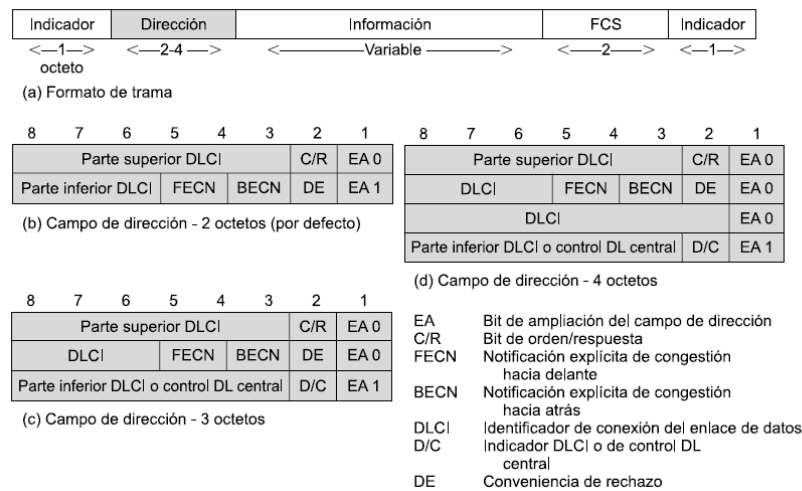


Figura 5.2.3.1: Formatos del protocolo central LAPF

Éste es el formato definido para el protocolo LAPF de funcionalidad mínima (conocido como protocolo LAPF central), el cual es similar al de LAPD y LAPB con una salvedad obvia: no existe campo de control. Esto tiene las siguientes implicaciones:

- ✓ Existe un único tipo de trama, usada para el transporte de datos de usuario, y no existen tramas de control.
- ✓ No es posible el uso de señalización en banda; una conexión lógica sólo puede transmitir datos de usuario.
- ✓ No es posible llevar a cabo control de flujo ni de errores, dado que no existen números de secuencia.

Los campos, indicador (delimitador de trama) y secuencia de comprobación de trama (FCS) funcionan como en HDLC. El campo de información contiene datos de capas superiores, de modo que, si el usuario decide implementar funciones adicionales de control del enlace de datos extremo a extremo, se puede incluir

una trama de datos en este campo. En particular, una opción usual es el empleo del protocolo LAPF completo (conocido como protocolo LAPF de control) para llevar a cabo funciones por encima de las funciones centrales de LAPF. Obsérvese que el protocolo así implementado es estrictamente entre los abonados finales y resulta transparente para la red de retransmisión de tramas.

El campo de dirección tiene una longitud, por defecto, de 2 octetos, pudiéndose ampliar hasta 3 o 4 octetos. Este campo contiene un identificador de conexión del enlace de datos (DLCI, Data Link Connection Identifier) de 10, 16 o 23 bits. DLCI realiza la misma función que el número de circuito virtual en X.25: permite la multiplexación de varias conexiones lógicas de retransmisión de tramas a través de un único canal. Como ya se aclaró, el identificador de conexión tiene sólo significado local: cada extremo de la conexión lógica asigna su propio DLCI de acuerdo con los números libres, debiendo realizar la red la conversión correspondiente entre ellos.

La longitud del campo de dirección, y por tanto del DLCI, se determina mediante los bits de ampliación del campo de dirección (EA). El bit C/R es específico de la aplicación y no se usa en el protocolo de retransmisión de tramas estándar. Los bits restantes del campo de dirección están relacionados con el control de congestión y se discutirán más adelante.

#### 5.2.4. Funcionamiento de la red

Para comprender el funcionamiento de la red Frame Relay vamos a utilizar la figura 5.2.4.1. Se supone que se definieron cuatro conmutadores en la red FR que nos alquila el proveedor de telecomunicaciones. Tanto A, como B, C y D desempeñan aquí un papel equivalente a los routers en una red IP, dado que cada uno cuenta con una tabla de circuitos virtuales. Además, se dispone de cuatro routers, X, Y, Z y W (generalmente en las instalaciones de los clientes), que en la red Frame Relay desempeñan el papel de hosts. Este es un ejemplo bastante habitual, ya que permite aprovechar una única conexión Frame Relay para vincular cada una de las redes LAN conectadas a los routers en cada una de las localidades, provincias o países, permitiendo así el tráfico de datos a través de toda la empresa, como si fuera una única gran red.

En primer lugar, el host X va a establecer un circuito virtual con el host Y. Para ello genera una conexión con el conmutador A empleando el DLCI 16, pues es el primero que está libre (los DLCI inferiores están reservados para funciones de servicio de la red, tales como señalización). Para constituir el circuito, el conmutador A establece una conexión con el conmutador B usando también el DLCI 16, por último, lo mismo hace el conmutador B con el host Y, usando un DLCI 16. El conjunto de las tres conexiones establece un circuito virtual, que se llamará el circuito ‘rojo’, entre el host X el host Y.

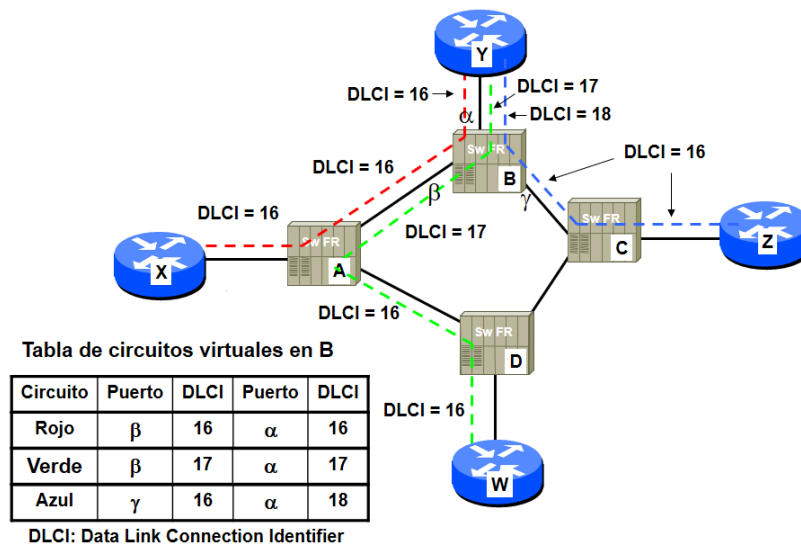
Ahora se va a establecer un segundo circuito, pero esta vez entre el conmutador W y el conmutador Y, y se decidió establecer el circuito usando la ruta D-A-B. Se procede como se hizo anteriormente, usando el DLCI 16 en el tramo W-D y D-A



(recuerde que el valor del DLCI es sólo local), pero al establecer la conexión A-B no podemos utilizar este DLCI 16 pues ya está ocupado por el circuito creado en el paso anterior, por lo que empleamos el DLCI 17. La misma situación ocurre en el tramo B-Y, por lo que se decide también crear el DLCI 17.

Así pues, el segundo circuito (verde) utiliza el número de DLCI 16 en algunos tramos y el número de DLCI 17 en otros. Esto no supone ningún problema pues cada conmutador sabrá gracias a los valores configurados en sus tablas de circuitos virtuales, la pertenencia de cada uno de los DLCI's, tal como se muestra en la figura para el caso de la tabla generada en el conmutador B.

Por último, el conmutador Z va a establecer un circuito con Y, para lo cual emplea se decide emplear la ruta Z-C-B-Y. Como puede verse en la figura este circuito coincide con los otros únicamente en el enlace B-Y, por lo tanto, en este tramo deberá utilizar un número de DLCI diferente a los otros dos. En cambio, en los tramos z-C y C-B, donde está solo, puede utilizar el DLCI 16 sin problemas (se insiste que el valor del DLCI es sólo local).



• Figura 5.2.4.1: Cuatro sitios conectados a través de una red Frame Relay

### 5.2.5. Ventajas y Desventajas de Frame Relay

Para comprender en forma resumida cuáles son las mejoras obtenidas gracias al desarrollo de esta tecnología, como así también cuales son los aspectos a mejorar, se detalla a continuación las ventajas y desventajas de la misma.

#### Ventajas

- ✓ La multiplexación y conmutación de conexiones lógicas tiene lugar en la capa 2 en lugar de la 3 eliminando una capa entera de proceso.
- ✓ No hay control de flujo ni control de error de salto. Este control se realiza extremo a extremo es responsabilidad de una capa más alta, si es que se emplea.

- ✓ Tiene la característica de implementar una multiplexación estadística de muchas conversaciones lógicas de datos sobre un simple enlace de transmisión físico. Esto permite un uso más flexible del ancho de banda disponible.
- ✓ Acelera el proceso de enrutamiento de paquetes a través de una serie de conmutadores a una localización remota, eliminando la necesidad de que cada conmutador chequee cada paquete que recibe antes de retransmitirlo al siguiente conmutador. Con esto se destaca que el chequeo de errores y control de flujo solamente se realiza en la estación destino, no en los nodos intermedios.
- ✓ Soporta mecanismos de notificación de congestión muy simples para permitir a una red informar a un dispositivo de usuario que los errores de la red están agotados cuando se alcanza el estado de congestión.
- ✓ Proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red pública con circuitos punto a punto. Es decir que permite reemplazar las líneas privadas por un sólo enlace de red.
- ✓ Permite poner en servicio varios circuitos virtuales sobre una misma interfaz física.
- ✓ Existe una independencia entre el coste y la distancia.
- ✓ Se adapta perfectamente al tráfico en ráfagas, propio de las aplicaciones cliente/servidor o de interconexión de redes locales.
- ✓ Con la integración de servicios se puede gestionar una única red en lugar de varias, además, el ancho de banda contratado se pone a disposición en cada momento de quien lo necesite.
- ✓ Transporte integrado de distintos protocolos de voz y datos.

### **Desventajas**

- ✓ Dado que Frame Relay está orientado a conexión, todas las tramas siguen la misma ruta a través de la red, basadas en un identificador de conexión. Pero las redes orientadas a conexión son susceptibles de perderla si el enlace entre el nodo conmutador de dos redes falla. Aun cuando la red intente recuperar la conexión, deberá ser a través de una ruta diferente, lo que cambia el retardo extremo a extremo y puede no ser lo suficientemente rápido como para ser transparente a las aplicaciones.
- ✓ Frame Relay no fue diseñada originalmente para aplicaciones de tráfico de tasa de bits constante como voz y video y no tiene la capacidad de asegurar que las tramas perdidas no superen un umbral.
- ✓ Pérdida de la calidad del sonido como resultado de la compresión de la voz

## 5.2. ATM (Asynchronous Transfer Mode – Modo de Transferencia Asíncrono)

El modo de transferencia asincrónica es una tecnología de conmutación y multiplexación que emplea paquetes pequeños de longitud fija llamados celdas (Figura 5.1.1). Se eligió un paquete de tamaño fijo para garantizar que la función de conmutación y multiplexación se pueda llevar a cabo de manera eficiente, con poca variación de retardo. El tamaño de “celda” pequeño permite soportar servicio de voz interactivo, intolerante al retardo que se produce en la conmutación de paquetes.

ATM es una tecnología de conmutación de paquetes orientada a la conexión que fue diseñada para proporcionar el rendimiento de una red de conmutación de circuitos y la flexibilidad y eficiencia de una red de conmutación de paquetes. Uno de los principales objetivos del esfuerzo de normalización de ATM fue proporcionar un poderoso conjunto de herramientas para respaldar una rica capacidad de QoS y una poderosa capacidad de gestión del tráfico. ATM fue destinada a proporcionar una red unificada estándar para tráfico de conmutación de circuitos y de paquetes, y para admitir datos, voz y video con mecanismos de QoS apropiados. Con ATM, el usuario puede seleccionar el nivel de servicio deseado y obtener una calidad de servicio garantizada. Internamente, la red hace reservas y planifica rutas para que la asignación de transmisión se base en las características de prioridad y QoS.

ATM fue destinada a ser una tecnología de red universal, con gran parte de la capacidad de conmutación y enrutamiento implementada en hardware, y con la capacidad de admitir redes basadas en IP y redes de conmutación de circuitos. También se anticipó que ATM se utilizaría para implementar redes de área local, aunque por los costos nunca logró desplegarse en este tipo de redes. Sin embargo, ATM sigue siendo una tecnología importante.

Los proveedores de telecomunicaciones utilizan habitualmente ATM para implementar redes. Muchas implementaciones de DSL utilizan ATM sobre el hardware DSL básico para multiplexación y conmutación, y ATM se utiliza como tecnología de red troncal en numerosas redes IP y partes de Internet.

Es oportuno señalar que en los últimos años varios factores han llevado a que el crecimiento de ATM fuera ingresando en una meseta. IP, con sus muchos protocolos asociados, proporciona una tecnología integradora que es más escalable y menos compleja que ATM. Además, la necesidad de utilizar pequeñas celdas de tamaño fijo para reducir el retardo ha desaparecido a medida que aumenta la velocidad de transporte. El desarrollo de voz y video sobre protocolos IP ha proporcionado una capacidad de integración a nivel de IP.

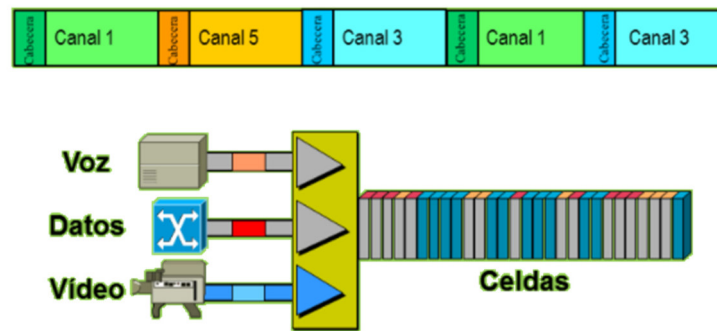


Figura 5.1.1: Modo de Transferencia Asincrónico

### 5.2.6. Capas ATM

En la Figura 5.2.1.1 se muestra la arquitectura de capas básica para una interfaz entre un usuario y la red.

- ✓ Capa Física. Especifica un medio de transmisión y un esquema de codificación de señal. Las velocidades de transmisión especificadas van desde 25,6 Mbps hasta 622,08 Mbps, siendo posibles velocidades superiores e inferiores.

Las funciones propias de ATM se implementan mediante dos capas relacionadas que son la capa ATM y una capa de adaptación ATM (AAL):

- ✓ Capa ATM. Es común a todos los servicios de transferencia de paquetes. Define la transmisión de datos en celdas de tamaño fijo y, además, establece el uso de conexiones lógicas.
- ✓ Capa AAL. Esta capa de adaptación ATM o AAL (ATM Adaptation Layer) depende de cada servicio particular. Esta capa es necesaria para dar soporte a protocolos de transferencia de información no basados en ATM. En ese sentido, AAL convierte la información procedente de capas superiores en celdas ATM para enviarlas a través de la red. Al mismo tiempo, extrae la información contenida en las celdas ATM que vienen de la red y la transmite hacia las capas superiores.

Además de la división en capas, la gestión de la comunicación en ATM está repartida en planos, asignándose a cada plano una tarea específica. El modelo de referencia de protocolos involucra tres planos independientes:

- ✓ Plano de usuario. Permite la transferencia de información de usuario, así como de controles asociados a esa transferencia, por ejemplo, control de flujo y de errores.
- ✓ Plano de control. Realiza funciones de control de llamada y de control de conexión.
- ✓ Plano de gestión. Comprende la gestión de plano; esto implica la realización de funciones de gestión relacionadas con un sistema como un todo y proporciona la

coordinación entre todos los planos. Además, comprende la gestión de capa; es decir, realiza funciones de gestión relativa a los recursos y a los parámetros residentes en las entidades de protocolo como, por ejemplo, gestionar prioridades ante la red para una aplicación determinada.

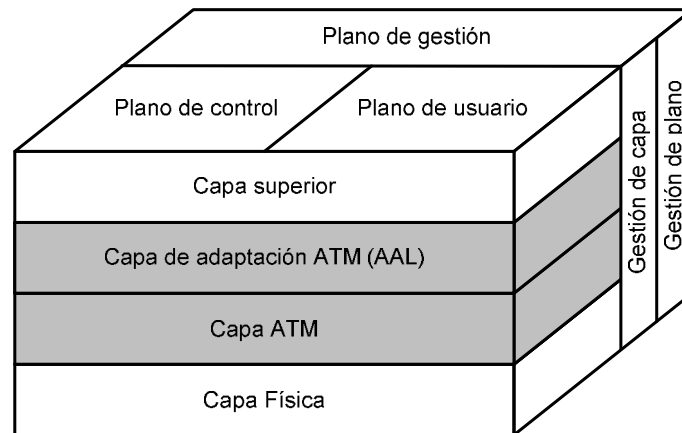


Figura 5.2.1.1: Arquitectura de capas ATM

### 5.2.7. Conexiones Lógicas ATM

Las conexiones lógicas en ATM, cuya relación se muestra en la Figura 5.2.2.1, son:

- ✓ Conexión de Canal Virtual o VCC (Virtual Channel Connection). Una VCC es similar a un circuito virtual y constituye la unidad básica de conmutación en una red ATM. Una VCC se establece a través de la red entre dos usuarios finales, intercambiándose sobre la conexión celdas en modo full duplex de velocidad variable. Las VCC se utilizan también para intercambio de señalización de control entre usuario-red; además, para la gestión interna de la red, y de ruteo entre red y red.
- ✓ Conexión de Camino Virtual o VPC (Virtual Path Connection). Una VPC es un conjunto de VCC's con los mismos extremos, de manera que todas las celdas transmitidas a través de todas las VCC de una misma VPC se conmutan conjuntamente.

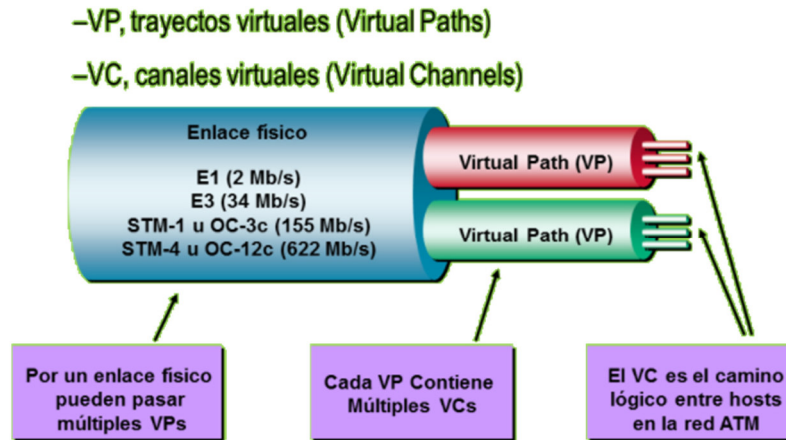


Figura 5.2.2.1: Tipos de conexiones ATM

### Concepto de Camino Virtual

La conexión entre dos dispositivos de usuario puede requerir de varias conexiones independientes entre distintas aplicaciones que corren en ellos. El concepto de camino virtual (VPC) se desarrolló en respuesta a que el costo de control estaba alcanzando una proporción cada vez mayor respecto al costo total de gestión en las redes de voz, datos y video. La técnica de camino virtual ayuda a contener el costo asociado al control mediante la agrupación en una misma unidad de aquellas conexiones que comparten rutas comunes a través de la red. De esa forma, las acciones de gestión de red se aplican a un reducido número de grupos (VPC), en lugar de aplicarlas a un elevado número de conexiones individuales (VCC) con la consiguiente reducción de procesamiento y costo.

### Ventajas de Usar Caminos Virtuales

Además de la importante ventaja señalada anteriormente, el uso de caminos virtuales presenta, además, varias ventajas adicionales:

- ✓ Arquitectura de red simplificada. Las funciones de transporte de red se pueden separar en dos grupos: aquellas relacionadas con una conexión lógica individual (canal virtual) y las relativas a un grupo de conexiones lógicas (camino virtual).
- ✓ Incremento de eficiencia y confiabilidad. La red maneja entidades totales menores.
- ✓ Reducción en el procesamiento y bajo tiempo de establecimiento de conexión. Gran parte del trabajo se realiza cuando se establece el camino virtual. Esto significa que la reserva previa de capacidad en la VPC permite luego establecer nuevos canales virtuales de forma simple en los extremos del camino virtual puesto que no se necesita procesamiento en el establecimiento de llamadas en los

nodos intermedios de la red. Esto hace que la incorporación de nuevos canales (VCC) a un camino virtual (VPC) ya existente requiera un procesamiento mínimo.

- ✓ Servicios de red mejorados. El camino virtual se usa internamente a la red, aunque también es visible para el usuario final. Así, el usuario puede definir grupos de usuarios fijos o conjunto de redes fijas (canales virtuales).

### **Establecimiento de VPC y VCC**

El proceso de establecimiento de un camino virtual se encuentra desvinculado del proceso de establecimiento de un canal virtual porque:

- ✓ Entre los mecanismos de control de un camino virtual se encuentra la definición una ruta, extremo a extremo, la reserva de capacidad y el almacenamiento de información de estado de la conexión.
- ✓ En cambio, el establecimiento de un canal virtual precisa la existencia previa de un camino virtual hacia el nodo del destino deseado con suficiente capacidad disponible para soportar dicho canal virtual y con la calidad de servicio adecuada. El establecimiento se lleva a cabo mediante el almacenamiento de la información necesaria que consiste en asociar el canal virtual a un camino virtual.

La terminología relativa a caminos virtuales y a canales virtuales se resume en la Tabla 5.2.2.3:

Tabla 5.2.2.3: Terminología ATM

<b>Canal virtual (VC)</b>	Término genérico usado para describir el transporte unidireccional de celdas ATM asociadas a un valor identificador único común (VCI).
<b>Enlace de canal virtual</b>	Medio de transporte unidireccional de celdas ATM entre un punto al que se asigna un valor de VCI y el punto en que este valor se traduce o termina.
<b>Identificador de canal virtual (VCI)</b>	Marca numérica única que identifica un enlace VC particular de una VPC dada.
<b>Conexión de canal virtual (VCC)</b>	Concatenación de enlaces VC que se extiende entre dos puntos extremos donde los usuarios del servicio ATM acceden a la capa ATM. Las VCC se utilizan con fines de transferencia de información usuario-usuario, usuario-red o red-red. Se preserva la integridad de la secuencia de celdas para aquellas pertenecientes a la misma VCC.
<b>Camino virtual (VP)</b>	Término genérico usado para describir el transporte unidireccional de celdas ATM pertenecientes a canales virtuales asociados a un valor de identificación único común (VPI).
<b>Enlace de camino virtual</b>	Grupo de enlaces VC, identificado por un valor común de VPI, entre un punto al que se asigna un valor de VPI y el punto en que este valor se traduce o termina.
<b>Identificador de camino virtual (VPI)</b>	Identifica un enlace VP particular.

<b>Conexión de camino virtual (VPC)</b>	Concatenación de enlaces VP que se extiende entre el punto en que se asignan los valores de VCI y el punto en que estos valores se traducen o eliminan (es decir, amplía la longitud de un haz de enlaces VC que comparten el mismo VPI). Las VPC se emplean con el objeto de transferir información usuario-usuario o red-red.
---	---

## Uso de Canales y Caminos Virtuales

Los extremos de una VCC pueden ser usuarios finales, entidades de red, o un usuario final y una entidad de red. En todos los casos se preserva la integridad de la secuencia de celdas dentro de una VCC; es decir, las celdas se entregan en el mismo orden en fueron enviadas. A continuación, se describen ejemplos de los tres usos de una VCC:

- ✓ Entre usuarios finales. Una VCC se puede utilizar para el transporte de datos entre aplicaciones de usuario en los extremos y, como se verá más adelante, para la transmisión de señalización de control entre usuarios finales. La existencia de una VPC entre usuarios finales les concede a éstos una capacidad total para organizar las VPC en varias VCC, siempre que el conjunto de las VCC no supere la capacidad de la VPC.
- ✓ Entre un usuario final y una entidad de red. Una VCC se usa para señalización de control desde el usuario hacia la red como se verá posteriormente. Una VPC del usuario a la red se puede emplear para el tráfico total desde un usuario final, por ejemplo, un servidor a un nodo conmutador ATM de red.
- ✓ Entre dos entidades de red. Una VCC se utiliza para la gestión del tráfico interno de red y con funciones de ruteo entre red y red. Una VPC red-a-red puede ser usada para definir una ruta común para el intercambio de información de gestión de red.

### 5.2.8. Servicios ATM al Usuario

El Modo de Transferencia Asíncrono define servicios al usuario, tanto a nivel Canal Virtual, como así también a nivel Camino Virtual.

#### Servicios de Canal Virtual

- ✓ Calidad de servicio. A un usuario de una VCC dada se le provee una calidad de servicio que está especificada por parámetros tales como:
  - Tasa de pérdida de celdas: relación entre celdas perdidas y transmitidas.
  - Variación de retardo de celdas.
- ✓ Tipos de conexiones. Existen dos tipos de conexiones de canal virtual:
  - VCC conmutada. Es una conexión bajo demanda que necesita señalización de control de llamada para su establecimiento y terminación.



- VCC semipermanente. Es de larga duración y se gestiona con el proveedor del servicio. Es similar a la gestión de una línea telefónica; la línea está activa mientras está activo el servicio.
- ✓ Integridad de la secuencia de celdas. Se preserva el orden de las celdas transmitidas en una VCC.
- ✓ Negociación de parámetros de tráfico y supervisión de su cumplimiento. Cuando un usuario requiere contratar los servicios de una red ATM, además del tipo y costo de los mismos, debe acordar con el prestador los parámetros de tráfico para cada VCC. El ingreso de celdas desde el sistema de usuario a la VCC es supervisado por la red para asegurar que se cumplen los parámetros negociados. Entre los parámetros de tráfico que se pueden negociar se encuentran:
  - Velocidad media.
  - Velocidad de pico.
  - Tipo de ráfagas.
  - Duración del pico.
- ✓ Acciones ante congestiones en la Red. La red utiliza varias estrategias para abordar la congestión. En ese sentido, interviene teniendo en cuenta las VCC existentes y las solicitadas. Ante distintos estados de congestión la red puede tomar las siguientes medidas:
  - Para prevenir la congestión. En un estado de pre congestión y ante nuevas peticiones de VCC, la red puede directamente denegar su otorgamiento.
  - En estado de congestión media a importante. Como medida adicional a la anterior, la red puede descartar celdas.
  - Congestión extrema. Además de las medidas expuestas, la red puede llegar a liberar conexiones existentes con el fin de solucionar la congestión.

### Servicios de Camino Virtual

Las cuatro primeras características de las VPC son idénticas a las de las VCC; es decir, calidad de servicio, VPC conmutadas y semipermanentes, integridad de la secuencia de celdas, y negociación de los parámetros de tráfico y supervisión de su cumplimiento.

Hay varias razones para la existencia de esta duplicidad:

- ✓ Se provee así de cierta flexibilidad sobre cómo el servicio de red gestiona los requisitos que debe cumplir.
- ✓ La red debe ocuparse de las necesidades de una VPC y, dentro de una VPC, puede negociar el establecimiento de canales virtuales donde cada VCC tenga sus características particulares.

- ✓ Una vez que se ha establecido una VPC, los usuarios finales pueden negociar la creación de nuevas VCC. Las características de la VPC determinan la elección de las características de cada VCC que los usuarios pueden hacer.

Adicionalmente, existe una quinta característica para las VPC:

- ✓ Restricción de identificador de canal virtual en una VPC. Puede que no sea posible proporcionar al usuario de una VPC uno o más identificadores o números de canal virtual, pero sí se pueden reservar para el uso de la red. Por ejemplo, es el caso del uso de una VCC para la gestión de la red.

### 5.2.9. Celdas ATM

El modo de transferencia asincrónico hace uso de celdas de tamaño fijo que constan de 5 bytes de cabecera y de un campo de información de 48 bytes. El empleo de celdas pequeñas de tamaño fijo presenta varias ventajas:

- ✓ Permite reducir el retardo de cola para celdas de alta prioridad, ya que la espera es menor si se reciben ligeramente después de que una celda de baja prioridad haya conseguido el acceso a un recurso, por ejemplo, el transmisor.
- ✓ Al tener las celdas tamaño fijo permite simplificar el hardware y software necesario para la conmutación, por lo que ésta se realiza en forma más eficiente lo que es importante para las altas velocidades.

#### Formato de Cabecera

En la Figura 5.2.4.1(a) se muestra el formato de cabecera de una celda en la interfaz “usuario-red”, mientras que en la Figura 5.2.4.1(b) se muestra el formato de una celda interna de la red ATM. A continuación, se describen los campos:

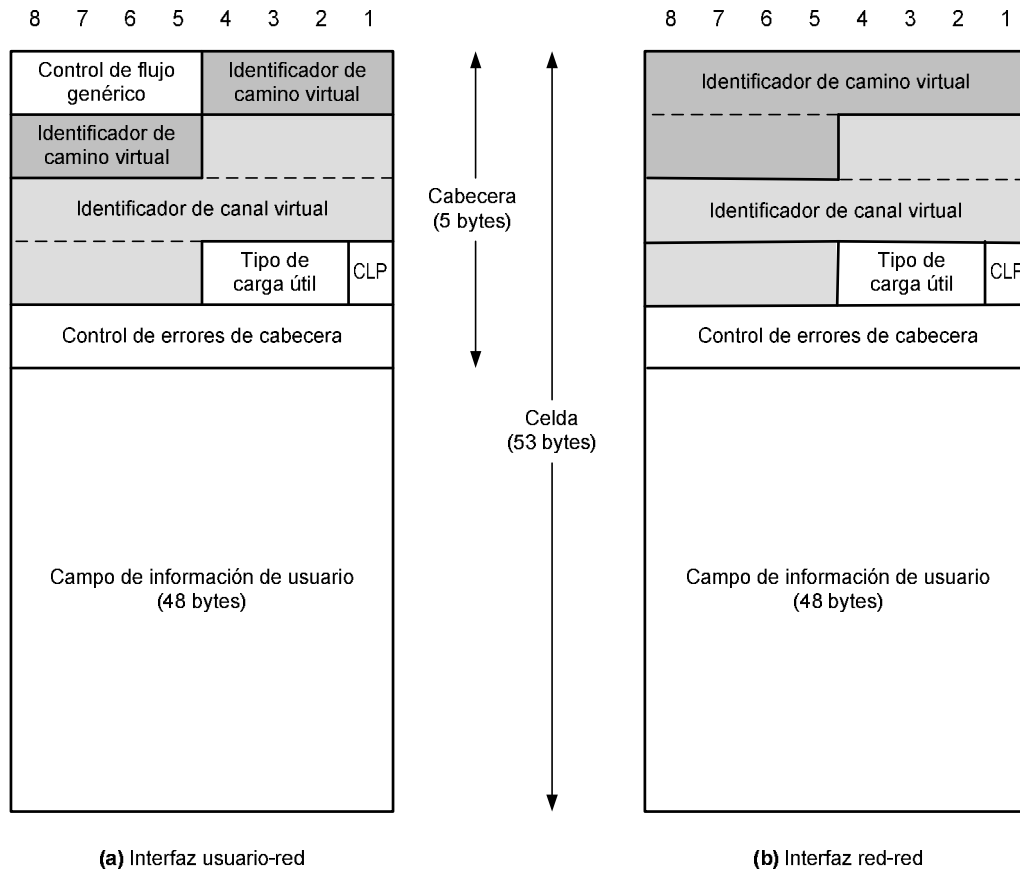


Figura 5.2.4.1: Formato celda ATM

- ✓ **Control de Flujo Genérico o GFC (Generic Flow Control).** Este campo no se incluye en la cabecera de las celdas internas a la red, sino sólo en la interfaz “usuario-red”, por lo que únicamente se puede usar para llevar a cabo el control de flujo de celdas en la interfaz local entre usuario y la red. Este campo podría utilizarse para ayudar al usuario en el control de flujo de tráfico para diferentes calidades de servicio. En cualquier caso, el mecanismo GFC se usa con el fin de aliviar la aparición esporádica de sobrecarga en la red.
- ✓ **Identificador de Camino Virtual (VPI).** Es un campo de ruteo para la red, de 8 bits para la interfaz “usuario-red” y de 12 bits para la interfaz red-red. Este último caso permite un número superior de VPC internas a la red, tanto para dar servicio a abonados como las necesarias para la gestión de red.
- ✓ **Identificador de Canal Virtual (VCI).** Se emplea para enrutar hacia y desde el usuario final.
- ✓ **Tipo de Carga Útil o PT (Payload Type).** Este campo indica el tipo de información contenida en el campo de información. En la tabla 5.2.4.2 se muestra la interpretación de los bits PT.

- Un valor 0 en el primer bit indica información de usuario; es decir, información procedente de la capa inmediata superior. En este caso, el segundo bit indica si se ha producido congestión o no. El tercer bit, llamado tipo de unidad de datos de servicio (SDU), es un campo de 1 bit que se puede usar para discriminar dos tipos de SDU ATM asociadas a una conexión dada. El termino SDU se refiere a la carga útil de 48 bytes de la celda.
  - Un valor de 1 en el primer bit del campo PT indica que la celda transporta información de gestión de red o de mantenimiento. Esto permite la inserción de celdas de gestión de red en una VCC de usuario sin afectar a los datos de usuario; de este modo el campo PT puede proporcionar información de control intrabanda.
- ✓ **Prioridad de Pérdidas de Celdas o CLP (Cell Loss Priority).** Este campo de un bit se emplea para ayudar a la red ante la aparición de congestión. Un valor 0 indica que la celda tiene prioridad relativamente alta, no debiendo ser descartada a menos que no queda otra opción. Un valor 1 indica, por el contrario, que la celda puede descartarse en la red. El usuario puede utilizar este campo para insertar celdas extra (una vez negociada la velocidad) con CLP igual a 1, y transmitir las a destino si la red no está congestionada. La red puede poner este campo en 1 en aquellas celdas que violen los parámetros de tráfico acordados entre el usuario y la red. En este caso, el conmutador que lo activa se percata de que la celda excede los parámetros de tráfico establecidos, pero que ésta puede ser procesada. Posteriormente, si se encuentra congestión en la red, esta celda se marcará para su rechazo antes que aquellas que se encuentran dentro de los límites de tráfico fijados.
- ✓ **Control de Errores de Cabecera.** Este campo se usa tanto para el control de errores como para sincronización.

Tabla 5.2.4.2: Codificación del campo de carga útil

Codificación PT	Interpretación		
000	Celda de datos de usuario	No se ha producido congestión	tipo SDU = 0
001	Celda de datos de usuario	No se ha producido congestión	tipo SDU = 1
010	Celda de datos de usuario	Se ha producido congestión	tipo SDU = 0
011	Celda de datos de usuario	Se ha producido congestión	tipo SDU = 1
100	Celda asociada a segmento OAM		

101	Celda asociada a OAM extremo a extremo
110	Celda de gestión de recursos
111	Reservada para funciones futuras

SDU: Unidad de Datos de Servicio.

OAM: Funcionamiento, Administración y Mantenimiento.

### Control de Flujo Genérico

El campo GFC se usa para llevar a cabo el control del flujo del tráfico en la interfaz “usuario-red” o UNI (User-Network Interface) con objeto de solucionar la aparición esporádica de sobrecarga. El control de flujo CFG forma parte de un mecanismo de transferencia controlada de celdas o CCT (Controlled Cell Transfer) propuesto, que está pensado para satisfacer los requisitos de las redes LAN no ATM conectadas a una red ATM de área extensa. En particular, el mecanismo CCT está ideado para ofrecer un buen servicio para un elevado tráfico de ráfagas con mensajes de longitud variable.

### Control de Errores de Cabecera

Cada celda ATM incluye un campo de control de errores de cabecera o HEC (Header Error Control) que se calcula en base a los restantes 32 bits de la cabecera. El polinomio usado para generar el código es  $X^8 + X^2 + X + 1$ . En la mayor parte de los protocolos existentes que incluyen un campo de control de errores, como HDLC, la cantidad de datos de entrada para el cálculo del código de error es generalmente mayor que el tamaño del código de error resultante, lo que permite la detección de errores. En el caso de ATM la entrada para el cálculo es solo de 32 bits, frente a los 8 bits del código. El hecho de que la entrada sea relativamente pequeña permite el uso del código no sólo para la detección de errores, sino que, es posible la corrección de éstos. Esto se debe a que hay suficiente redundancia en el código para recuperar ciertos patrones de error.

#### 5.2.10. Clases de Servicios ATM

Una red ATM se diseña para poder transmitir simultáneamente diferentes tipos de tráfico, entre los que se encuentra la transmisión en tiempo real con voz, video y tráfico TCP a ráfagas. Aunque cada uno de estos flujos de tráfico se gestiona como una secuencia de celdas de 53 bytes a través de un canal virtual, la forma en que se gestiona cada uno de ellos en la red depende de las características del flujo en cuestión y de los requisitos que impone la aplicación particular. Por ejemplo, el tráfico de video en tiempo real se debe transmitir con variaciones mínimas de retardo.

A continuación, se presentan las clases de servicios ATM usados por un sistema final para identificar el tipo de servicio requerido. En el foro ATM se han definido las siguientes clases de servicios:

- ✓ Servicio en tiempo real.

- A velocidad constante o CBR (Constant Bit Rate).
- A velocidad variable en tiempo real o rt-VBR (real-time Variable Bit Rate)
- ✓ Servicio en no tiempo real.
  - A velocidad variable en no tiempo real o nrt-VBR (non-real-time Variable Bit Rate).
  - A velocidad disponible o ABR (Available Bit Rate).
  - A velocidad no especificada o UBR (Unspecified Bit Rate).

### **Servicios en Tiempo Real**

Existen servicios como la voz y el video que son altamente sensibles a la magnitud y a la variabilidad (fluctuación) del retardo de los datos cuando se transmiten desde la fuente al destino. Básicamente, las aplicaciones en tiempo real consisten en la generación de un flujo de información que debe llegar a destino con velocidad constante y en las mismas condiciones en que fue generado en la fuente. Por ejemplo, un usuario espera que la recepción de un flujo de información de audio o video tenga lugar de una forma continua (no variable) y homogénea. La falta de continuidad de los datos o pérdidas excesivas de éstos provoca una disminución importante en la calidad. Son más sensibles aquellas aplicaciones en la que hay interacción entre usuarios, resultando generalmente perjudicial cualquier retardo que supere unas pocas centenas de milisegundos. En consecuencia, en una red ATM y en cualquier red, son muy exigentes las demandas de conmutación y envíos de datos en tiempo real.

### **Velocidad Constante (CBR)**

El servicio CBR es quizás el más sencillo de definir. Se usan en aplicaciones que precisan una velocidad constante disponible durante toda la conexión y un retardo de transmisión máximo relativamente sin variación. CBR se usa comúnmente para información de audio y video sin comprimir. Algunos ejemplos de aplicaciones CBR son:

- ✓ Videoconferencia.
- ✓ Audio interactivo (por ejemplo, telefonía).
- ✓ Distribución de audio o video, por ejemplo, televisión, enseñanza a distancia, servicios de tipo pagar por ver (pay per view).
- ✓ Recuperación de audio o video (por ejemplo, video bajo demanda, audioteca).

### **Velocidad Variable en Tiempo Real (rt-VBR)**

La clase rt-VBR está pensada para aplicaciones sensibles al tiempo; es decir, aquellas que presentan fuertes restricciones en las magnitudes del retardo y de su variación. La principal diferencia entre aplicaciones adecuadas para rt-VBR y aquellas

indicadas para CBR es que en las primeras la transmisión se realiza a una velocidad que varía en el tiempo o, lo que es lo mismo, una fuente rt-VBR se puede caracterizar por su funcionamiento a ráfagas. Por ejemplo, cuando se transmiten datos de video comprimido éstos tienen tamaño variable, por lo que, dado que el video en tiempo real necesita una velocidad de transmisión de tramas uniforme, la velocidad real variará.

El servicio rt-VBR permite más flexibilidad a la red que al servicio CBR, ya que la red puede multiplexar estadísticamente varias conexiones sobre la misma capacidad dedicada y aun así proporcionar el servicio requerido para cada una de ellas.

### **Servicios en No Tiempo Real**

Los servicios que no son en tiempo real están pensados para aplicaciones que presentan características de tráfico a ráfagas y no presentan fuertes restricciones en lo que respecta al retardo y a la variación del mismo. Consecuentemente, la red dispone de mayor flexibilidad en la gestión de flujos de tráfico y puede hacer un mayor uso de la multiplexión estadística para aumentar su eficiencia.

### **Velocidad Variable en No Tiempo Real (nrt-VBR)**

Para algunas aplicaciones que no son en tiempo real es posible caracterizar el flujo de tráfico esperado de forma que la red pueda proporcionar una calidad de servicio o QoS (Quality of Service) sustancialmente mejorada desde el punto de vista de las pérdidas y el retardo. Estas aplicaciones pueden hacer uso del servicio nrt-VBR, en el que el usuario final especifica una velocidad de pico de celdas, una velocidad de celdas sostenible o promedio y una medida acerca de cómo de agrupadas o en ráfagas pueden estar las celdas. Con esta información, la red puede reservar recursos para ofrecer un retardo relativamente pequeño y una pérdida de celdas mínima.

El servicio nrt-VBR se puede utilizar para transmisiones de datos que presentan requisitos críticos en cuanto a la respuesta en el tiempo. Algunos ejemplos de ello son la reserva de vuelos, transacciones bancarias y supervisión de procesos.

### **Velocidad No Especificada (UBR)**

En cualquier instante de tiempo, una cierta cantidad de la capacidad de una red ATM se consume en el transporte de tráfico CBR y tráfico VBR de los dos tipos existentes. Una parte adicional de la capacidad se encuentra por alguna de las dos razones siguientes:

1. No todos los recursos se han destinado a tráfico CBR y VBR.

2. La naturaleza a ráfagas del tráfico VBR implica que a veces se usa menos capacidad de la reservada.

Toda esta capacidad sin usar se encuentra disponible para el servicio UBR. Este servicio es adecuado para aplicaciones que toleran retardos variables y cierta tasa de pérdida de celdas, lo que generalmente sucede en el tráfico TCP. En el servicio UBR, las celdas se transmiten según una cola FIFO (First-In-First-Out) haciendo uso de la capacidad no consumida por otros servicios, siendo posible la aparición de retardos y pérdidas variables. Debe señalarse que en el servicio UBR no se hacen reservas iniciales ni se proporciona realimentación relativa a la congestión, por lo que se conoce como servicio de mínimo esfuerzo. Algunos ejemplos de aplicaciones UBR son:

- ✓ Transferencia, mensajería, distribución, recuperación de texto, datos e imágenes.
- ✓ Terminal remoto (teletrabajo).

### **Velocidad Disponible (ABR)**

Las aplicaciones de transmisiones a ráfagas usando un protocolo confiable extremo a extremo como TCP pueden detectar congestión en una red a través del incremento en los retardos del viaje de ida y vuelta y en base al rechazo de paquetes. Sin embargo, TCP no dispone de ningún mecanismo para compartir los recursos internos a la red entre varias conexiones. TCP, además, no minimiza la congestión tan eficientemente como es posible mediante el uso de información explícita de los nodos de la red congestionados.

Para mejorar el servicio ofrecido a las fuentes de naturaleza a ráfagas, que deberían hacer uso del servicio UBR, se ha definido al servicio ABR. Una aplicación que haga uso de ABR especifica una velocidad de picos de celdas o PCR (Peak Cell Rate) a usar y una velocidad de celdas mínimas o MCR (Minimum Cell Rate) necesaria. La red reserva los recursos de forma que todas las aplicaciones ABR reciban al menos su capacidad MCR, compartiéndose la capacidad no usada de forma equitativa y controlada por todas las fuentes ABR. El mecanismo ABR hace uso explícito de realimentación hacia las fuentes para asegurar que la capacidad se ha reservado adecuadamente. La capacidad no usada por las fuentes ABR permanece disponible para tráfico UBR.

Un ejemplo de aplicación que usa ABR es la interconexión de redes LAN. En este caso, los sistemas finales conectados a la red ATM son routers.

### **Velocidad de Tramas Garantizada (GFR)**

El servicio GFR es el de más reciente adopción en ATM y está diseñado específicamente para dar servicio a subredes troncales IP. GFR proporciona mejor servicio que UBR para tráfico basado en tramas, incluyendo el tráfico de tipo IP y Ethernet. El principal objetivo de GFR es la optimización de la gestión de tráfico basado en tramas que va desde una LAN a una red troncal ATM a través de un router. El tipo de redes ATM mencionado está siendo usado de forma creciente en redes de grandes



empresas, de operadores y de proveedores de servicios de Internet con el objeto de consolidar y extender los servicios IP sobre redes de área extensa. Aunque ABR es también un servicio pensado para mejorar la transmisión de paquetes sobre redes ATM, resulta relativamente difícil de implementar entre routers en una red ATM. Debido al creciente uso de ATM para dar soporte de tráfico IP, en especial el originado en las LAN de tipo Ethernet, GFR puede resultar una alternativa más atractiva que ABR para proporcionar un servicio ATM.

Una de las técnicas empleadas por GFR para proporcionar mejores prestaciones que UBR consiste en hacer que los elementos de red conozcan las fronteras de las tramas o paquetes. De este modo, cuando la ocurrencia de congestión precisa el rechazo de celdas, los elementos de la red deben rechazar todas aquellas que componen la misma trama.

### 5.2.11. Conclusiones sobre ATM

El uso de la conmutación de celdas es un rompimiento drástico con la tradición centenaria de la conmutación de circuitos en la comunicación telefónica. Son muchas las razones por las que se escogió la conmutación de celdas, entre ellas están las siguientes:

- ✓ La conmutación de celdas es altamente flexible y puede manejar con facilidad tanto tráfico de velocidad constante como el audio, tráfico variable como el video, o tráfico que admite retardos, como los datos de archivos.
- ✓ A altas velocidades de transmisión (del orden de 1 Gigabps) la multiplexión de celdas es más fácil que el empleo de las técnicas tradicionales de multiplexión, en especial si se usa fibra óptica.
- ✓ Para la distribución de televisión es esencial la difusión; lo que puede proporcionar la conmutación de celdas, pero no la de circuitos.
- ✓ La tecnología ATM está orientada a conexión. No garantiza la entrega de celdas, pero sí el orden en que fueron enviadas. En esto es similar a Frame Relay.
- ✓ Las redes ATM se organizan como las WAN tradicionales, con líneas y nodos conmutadores.
- ✓ Las velocidades pretendidas para las redes ATM son de 155 Mbps y 622 Mbps. En la actualidad puede ofrecer velocidades de hasta 10 Gbps. La velocidad de 155 Mbps se escogió porque es cercana a lo que se necesita para transmitir televisión de alta definición. La velocidad de 622 Mbps se eligió para que se pudieran enviar por ella cuatro canales de 155 Mbps.

### 5.3. Multiprotocol Label Switching (MPLS – Conmutación de Etiquetas Multiprotocolo)

El protocolo IP (Internet Protocol) se ha convertido en el pilar donde se sustentan las actuales redes de telecomunicaciones, gracias al gran crecimiento de la red Internet. Actualmente cuenta con más de un 80% del tráfico cursado. La versión actual de IP, conocida como IPv4 y recogida en la RFC 791, lleva operativa desde 1980. Este protocolo está definido en la capa de red (Nivel 3 OSI), e implementa los mecanismos de la distribución o encaminamiento de paquetes. Lo hace de una manera no fiable y sin conexión, en redes heterogéneas, por lo que se suele utilizar junto con TCP (Transmission Control Protocol) en el Nivel 4 del modelo de referencia OSI, con el objetivo de garantizar la entrega de los paquetes.

Durante la década de los 90, se introdujo ATM (Asynchronous Transfer Mode) en la capa de enlace (Nivel 2 de OSI) de las redes a causa de la gran demanda por parte de los clientes de los ISP (Internet Service Providers) de aplicaciones multimedia con altas necesidades de ancho de banda y una calidad de servicio o QoS (Quality of Service) garantizada (se desarrolló en 5.2). Este nuevo modelo de IP sobre ATM satisfacía los requisitos de las nuevas aplicaciones, ya que utilizaba el encaminamiento inteligente de nivel 3 de los routers IP en la red de acceso, e incrementaba el ancho de banda y rendimiento con los switches ATM en la red central, basándose en la alta velocidad de los conmutadores de nivel 2 y los circuitos permanentes virtuales. Por otro lado, esta arquitectura, presentaba ciertas limitaciones, debido a:

- ✓ Elevada segmentación de los datos de nivel superior en celdas de sólo 53 bytes
- ✓ La dificultad de integrar y operar una red basándose en tecnologías muy distintas
- ✓ La mayor capacidad de transmisión ofrecida por SDH/SONET (Synchronous Digital Hierarchy / Synchronous Optical Network) y DWDM (Dense Wavelength Division Multiplexing) respecto a ATM.

En 1996, aparecieron soluciones de conmutación de nivel 2 propietarias diseñadas para la red troncal de Internet que integraban la conmutación ATM con el encaminamiento IP; como, por ejemplo, Tag Switching de Cisco o Aggregate Route-Based IP Switching de IBM. La parte común de estas tecnologías, era tomar el software de control de un router IP, integrarlo con el rendimiento de reenvío con cambio de etiqueta de un switch ATM y crear un router extremadamente rápido y eficiente en cuanto a coste.

Finalmente, en 1997, el IETF (Internet Engineering Task Force) estableció el grupo de trabajo MPLS (MultiProtocol Label Switching) para producir un nuevo estándar que unificase las soluciones propietarias de conmutación de nivel 2. Como resultado se obtuvo la definición en 1998 del estándar conocido por MPLS, recogido en la RFC 3031. MPLS proporciona las ventajas de la ingeniería de tráfico del modelo de IP sobre ATM, pero además proporciona los siguientes beneficios:

- ✓ Un modo de operación más sencillo y escalable

- ✓ Un modelo de conectividad que favorece claramente a la convergencia de las redes, reduciendo los costos asociados al mantenimiento de muchas redes con diferentes tecnologías, a un escenario de una única red que soporta varios tipos de servicios, como lo muestra la Figura 5.3.1.
- ✓ MPLS está diseñado para operar sobre cualquier tecnología en el nivel de enlace, facilitando así la migración a las redes ópticas de próxima generación, basadas en infraestructuras SDH/SONET y DWDM, a diferencia de las soluciones de conmutación de nivel 2 propietarias.

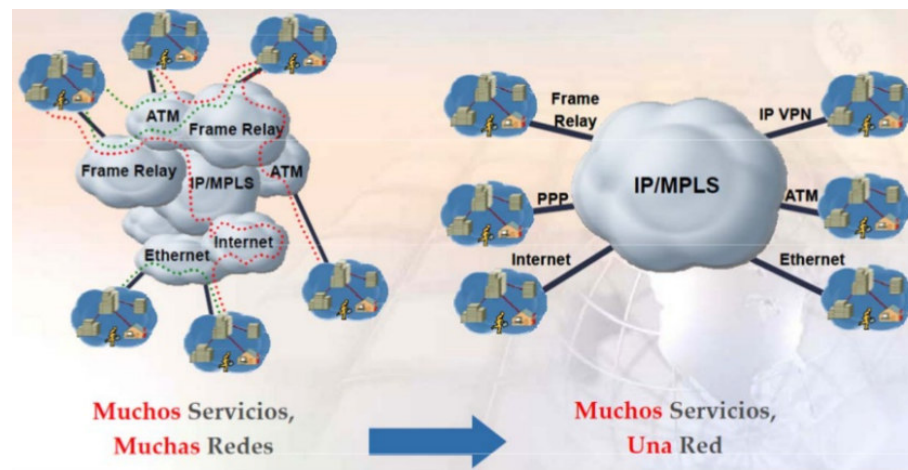


Figura 5.3.1: MPLS, un modelo de red convergente

### 5.3.1. ¿Qué es MPLS?

Como se comentó anteriormente, la necesidad de las operadoras de que sus redes tuviesen una cierta calidad de servicio, ha llevado a la búsqueda de una tecnología que ofreciese ese QoS por sí misma. Las tecnologías como ATM o SDH tienen una complejidad importante a la hora de aplicar calidad de servicio.

MPLS es una tecnología orientada a paquetes muy flexible. Si la situásemos en el modelo ISO/OSI (International Standard Organization / Open System Interconnection) se encontraría en la capa 2.5 (Figura 5.3.1.1), entre la capa de enlace y de red, o sea, entre la capa 2 y 3. El hecho de que se encuentre entre dos capas, le proporciona el nombre de “Multi Protocol”. Este hecho le da la ventaja de poder usar las características de los protocolos de las capas adyacentes sin ninguna restricción. Además de esto, MPLS ofrece adaptación total a IP. Esto es de gran importancia porque actualmente el mundo se mueve con este protocolo.

Con MPLS se gana en muchos aspectos en los que ATM presentaba carencias. Gracias al “Label Switching”, técnica usada en MPLS para enrutar paquetes, se consigue hacer este enrutado a más velocidad, a la vez que se disminuye el retardo y el jitter. Estas características son de especial interés en las redes troncales, donde uno de

sus principales objetivos es enviar paquetes de una localización a otra en el mínimo tiempo posible.

Pero MPLS va más allá que la velocidad y ofrece otras grandes ventajas, como la posibilidad de tener el control de la ruta, asignar distintos anchos de banda a los enlaces o crear prioridades para la utilización de un enlace. Todas estas ventajas y otras adicionales constituyen lo que se llama “Ingeniería de Tráfico” (TE - Traffic-Engineering) y que suele designarse como MPLS-TE.

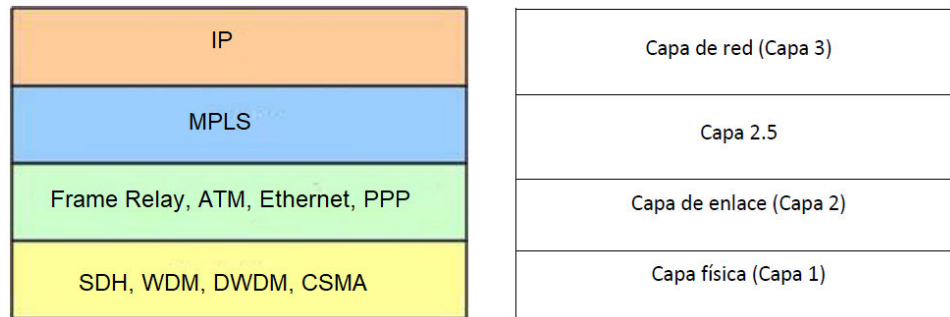


Figura 5.3.1.1: Ubicación de MPLS en el modelo de comunicación

A partir de las definiciones del RFC 3031, se describe a continuación las prestaciones del mismo:

### Soporte de QoS orientado a conexión

Los administradores y usuarios de red requieren un soporte de QoS cada vez más sofisticado para un número de razones. Algunas de ellas son las siguientes:

- ✓ Garantizar una cantidad fija de capacidad para aplicaciones específicas, como audio /video conferencia.
- ✓ Controlar la latencia<sup>1</sup> y el jitter<sup>2</sup> para garantizar la capacidad de voz.
- ✓ Proporcionar acuerdos de nivel de servicio muy específicos, garantizados y cuantificables, o contratos de tráfico.
- ✓ Configure diversos grados de QoS para múltiples clientes de red.

Una red sin conexión, como en Internet basada en IP, no puede proporcionar Compromisos de QoS verdaderamente firmes. Un marco de servicio diferenciado (DS) funciona sólo de forma general y sobre agregados de tráfico de diversas fuentes. Un marco de servicios integrado (IS), utilizando RSVP (Protocolo de Reserva de

<sup>1</sup> Es el tiempo que tarda en transmitirse un paquete dentro de la red

<sup>2</sup> El jitter se define técnicamente como la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino

Recursos), tiene algo del sabor de un enfoque orientado a conexión, pero sin embargo es limitado en términos de su flexibilidad y escalabilidad.

Para servicios como voz y video que requieren una red con alta previsibilidad, los enfoques DS e IS, por sí mismos, pueden resultar inadecuados en una red muy cargada. Por el contrario, una red orientada a la conexión, como que hemos visto con ATM, tiene una potente gestión de tráfico y capacidades de QoS.

MPLS impone un marco orientado a la conexión en una Internet basada en IP y, por lo tanto, proporciona la base para contratos de tráfico QoS sofisticados y confiables.

### **Ingeniería de Tráfico**

MPLS facilita la asignación de recursos de red de tal manera que equilibre la carga frente a una demanda determinada y comprometerse con niveles diferenciales de apoyo para satisfacer diversos requisitos de tráfico de usuarios. La capacidad de definir rutas de forma dinámica, planificar los compromisos de recursos sobre la base de la demanda conocida y optimizar la utilización de la red se conoce como ingeniería de tráfico. Antes de la llegada de MPLS, una tecnología de red que proporcionó sólidas capacidades de ingeniería de tráfico fue ATM.

Con el mecanismo de IP básico, existe una forma primitiva de Ingeniería de tráfico. Específicamente, los protocolos de enrutamiento como OSPF permiten a los enrutadores cambiar la ruta a un destino dado, paquete por paquete, para así mantener el equilibrio de carga. Pero este enrutamiento dinámico reacciona de una manera muy simple a la congestión y no proporciona una forma de admitir QoS. Todo el tráfico entre dos puntos finales sigue la misma ruta, que puede cambiar cuando se produce una congestión.

MPLS, es consciente no sólo de que existen paquetes, sino que, existen también flujos de paquetes en los que cada flujo tiene requisitos de QoS y una demanda de tráfico predecible. Con esta tecnología, es posible configurar rutas sobre la base de estos flujos individuales, con dos flujos diferentes entre los mismos puntos finales, tal vez siguiendo diferentes enrutadores. Además, cuando la congestión amenaza, las rutas MPLS se pueden desviar de forma inteligente. Esto significa que en lugar de simplemente cambiar la ruta paquete por paquete, con MPLS, las rutas se cambian flujo por flujo, aprovechando la conocida demanda de tráfico de cada flujo. El uso efectivo de la ingeniería de tráfico puede aumentar sustancialmente capacidad de red utilizable.

### **Configuración de Redes Privadas Virtuales (VPN - Virtual Private Networks)**

MPLS proporciona un mecanismo eficaz para admitir VPN. Con una VPN, el tráfico de una empresa o grupo dado pasa a través de Internet de una manera que efectivamente diferencia ese tráfico de otros paquetes en Internet, siendo un tráfico que tiene garantía de rendimiento y la implementación de esquemas de seguridad.

## **Soporte Multi – Protocolo**

MPLS se puede utilizar en varias tecnologías de red. Puede trabajar con internet basado en IP, de hecho, es muy utilizado, y su uso mejora sustancialmente la eficiencia de una red que opera con IP sin conexión. También está diseñado para funcionar en redes ATM y Frame Relay. Además, MPLS se puede utilizar de forma pura.

### **5.3.2. Componentes Básicos**

A continuación, se detallan los principales componentes que forman parte de una red MPLS.

#### **Label (Etiqueta)**

La etiqueta MPLS es un identificador de 20 bits encapsulado dentro de la cabecera MPLS de 32 bits. Esta contiene la información necesaria para enrutar un paquete hasta su destino.

Las etiquetas se utilizan en los routers para diferenciar entre los distintos FEC's (Forward Equivalence Class) y por lo tanto determinar el siguiente salto donde el paquete debe ser enviado. Generalmente el valor de la etiqueta se asigna a partir de la dirección IP destino y es meramente local, ya que solo tiene validez entre dos routers vecinos. Por otro lado, un mismo paquete puede ser etiquetado con un valor distinto dependiendo de cuál sea su router de entrada a la red MPLS (LSR). También cabe añadir que un paquete puede disponer de múltiples etiquetas (pila de etiquetas).

Como puede observarse en la Figura 5.3.2.1, la cabecera MPLS se incluye entre las cabeceras de nivel 2 y 3 y contiene los siguientes campos:

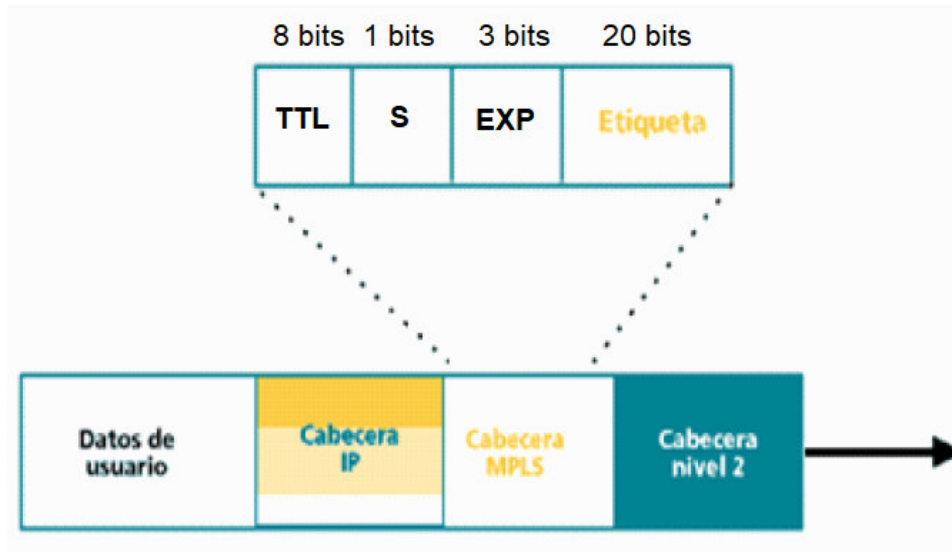


Figura 5.3.2.1: Cabecera de MPLS

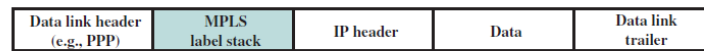
- ✓ TTL (Time to Live): es un valor que se decrementa cada vez que el paquete es reenviado por un router de la red MPLS (LSR). Cuando el valor es 0, el paquete se descarta. Su función es evitar que un paquete viaje indefinidamente por la red, provocando tráfico innecesario.
- ✓ S (Bottom of stack): Si su valor es 1 indica que el paquete solo contiene una etiqueta. Si por el contrario vale 0, significa que el paquete posee una pila de etiquetas.
- ✓ EXP (Experimental): Anteriormente era denominado CoS (Class of Service) pero ahora se considera un campo experimental. Se suele usar para proporcionar QoS.
- ✓ Etiqueta (Label): Valor local que usa el router para identificar un FEC en el proceso de forwarding, para determinar el próximo salto del paquete o su encapsulación.

La etiqueta MPLS (o la pila de etiquetas, si hubiera más de una) se ubican después de los encabezados de la capa de enlace de datos, pero antes encabezados de capa de red.

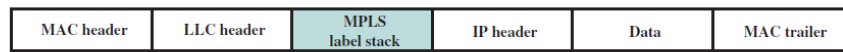
El paquete de la capa de red comienza inmediatamente después a la etiqueta MPLS que tiene el bit S=1. En las tramas de enlace de datos, como PPP (protocolo punto a punto), la pila de etiquetas aparece entre el encabezado IP y el encabezado de enlace de datos, como muestra la Figura 5.3.2.2(a).

Para una trama IEEE 802, la etiqueta MPLS (o la pila de etiquetas) se ubica entre el encabezado IP y el encabezado LLC (control de enlace lógico), como la Figura 5.3.2.2(b). En el caso de que la trama transportara un paquete IP v6, la etiqueta MPLS viaja en la cabecera del paquete IP, en el campo “Flow Label” (en el módulo 6 se verá en detalle los campos que forman la cabecera de un paquete IP v6).

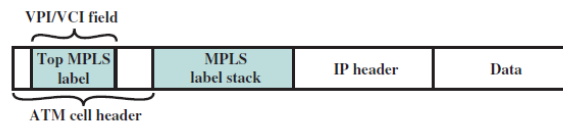
Si se utiliza MPLS sobre un servicio de red orientado a la conexión, se puede observar la ubicación de la o las etiquetas en la Figura 5.3.2.2 (c) y (d). Para las celdas ATM, el valor de la etiqueta MPLS o el valor de la etiqueta superior (en el caso de una pila de etiquetas), se ubica dentro de los campos VPI/VCI del encabezado ATM. Toda la etiqueta superior permanece en la parte superior de la pila de etiquetas, que se inserta entre el encabezado de la celda y el encabezado IP. De esta forma, colocando el valor de la etiqueta en la cabecera de la celda ATM, se facilita la conmutación mediante un conmutador ATM, que, como de costumbre, solo necesitaría mirar el encabezado de la celda. Del mismo modo, el valor de etiqueta superior se puede colocar en el campo DLCI (identificador de conexión de enlace de datos) de un encabezado de Frame Relay.



(a) Data link frame



(b) IEEE 802 MAC frame



(c) ATM cell

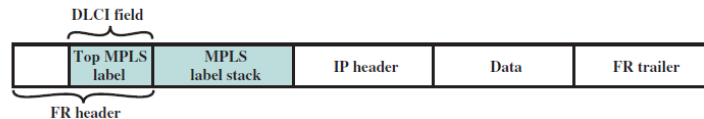


Figura 5.3.2.2: Ubicación de la etiqueta MPLS

### FEC (Forwarding Equivalence Class)

El FEC es la agrupación de etiquetas que permite la asociación de un conjunto de paquetes sobre el mismo camino y con un destino común. Un FEC tiende a corresponder con un único LSP. Un LSP puede y (usualmente es) usado por múltiples FEC's.

Un FEC no es un paquete, no es un label. Un FEC es una entidad lógica creada por el router para representar una clase (categoría) de paquetes

Todos los paquetes de un mismo FEC se tratan de la misma forma hacia su destino, y cuantos más FEC's se tenga, mayor granularidad para diferenciar entre distintos tipos de flujos. Se debe contemplar que el hecho de tener más FEC's afecta en la escalabilidad de la red, por lo tanto, es necesario llegar a un compromiso entre el número de FEC's y la eficiencia de la red.

Cada FEC tiene un camino específico a seguir a través de la red MPLS y es independiente en cada router. Puede darse el caso que para una misma dirección IP haya



más de un FEC a través del mismo LSP (Label Switched Path), lo que significa que paquetes con un mismo destino pueden y deben pertenecer a FEC's distintos si se tienen que tratar de forma distinta.

Así, la etiqueta de un determinado paquete representa al FEC al cual pertenece. Los LSR de entrada, que son los que etiquetan a los paquetes, son los encargados de asociar cada paquete a un FEC y se basan principalmente en la dirección destino para hacerlo, aunque también puede depender de otros factores como de la dirección de origen, los puertos de origen y destino, el protocolo o los requerimientos de servicio.

La asignación de un paquete particular a un FEC es hecha sólo una vez (cuando el paquete entra a la red).

A pesar de que los FEC's están pensados para agrupar a un conjunto de etiquetas, en la práctica lo normal cada FEC esté asociado a una única etiqueta.

### **LSR (Label Switched Router)**

Los LSR son todos aquellos routers que son capaces de usar MPLS. A diferencia de un router convencional, estos routers reenvían los paquetes en función de las etiquetas de los paquetes recibidos, y no en función de la dirección IP de destino. En una red MPLS se puede encontrar dos tipos de LSR:

- ✓ **Label Edge Router (LER):** Los LER son los routers frontera que operan en los bordes de una red MPLS. Estos routers son los encargados de convertir los paquetes IP en paquetes MPLS, o viceversa. Dependiendo de esta función, se puede diferenciar entre los tipos Ingress Edge Router (router de ingreso) y los Egress Edge Router (router de salida). Los primeros se sitúan en la entrada de la red y se encargan de asignar un FEC a los paquetes que reciben y de etiquetarlos para que lleguen a su destino. Los routers de salida son los encargados de hacer la acción contraria, eliminar la etiqueta (operación label pop). Estos se sitúan al final de la red. Además de la interface MPLS, estos routers soportan interfaces Frame Relay, ATM y Ethernet.
- ✓ **Core Router:** Estos son los routers que forman el núcleo de la red y permiten el tránsito de los paquetes hacia su destino. Estos routers están capacitados para hacer un label swapping (intercambio de etiquetas), label push (agregar etiqueta) y label pop (retirar etiqueta). Son routers de alta velocidad que forman parte del core de la red MPLS.

### **LSP (Label Switched Path)**

El LSP es el camino compuesto por uno o varios LSR a través del cual se transmiten todos los paquetes pertenecientes a un determinado FEC.

Estos caminos son unidireccionales (simplex) y solo transmiten hacia un sentido de tráfico. Si se quiere que la red sea dúplex, se deben establecer dos LSP's, uno para cada sentido.

Los LSP's se pueden diseñar para minimizar el número de saltos de los paquetes, para evitar congestiones en puntos críticos de la red, para tener un cierto ancho de banda o simplemente para forzar que el tráfico pase a través de un cierto nodo.

MPLS proporciona dos opciones para crear un LSP:

- ✓ Ruteo explícito: Desde el LSR de origen, se especifica punto a punto los saltos que tiene que dar el paquete. No suele ser el LSP más óptimo, pero es el más fácil de gestionar ya que el administrador controla por donde pasa el tráfico.
- ✓ Acoplados (merging): El camino escogido por los paquetes es determinado por el protocolo de enrutamiento interno (IGP)<sup>3</sup>, normalmente OSPF<sup>4</sup> o IS-IS<sup>5</sup>. Este camino puede ir variando si las condiciones de la red cambian.

### Label Stack (Pila de Etiquetas)

Una de las características del protocolo MPLS es que nos permite apilar diversas etiquetas unas sobre las otras. Esto se denomina “Pila de Etiquetas” y consigue anidar un LSP dentro de otro. El objetivo de esta técnica es el de crear túneles dentro de los otros LSPs, como se puede observar en la siguiente Figura 5.3.2.1:

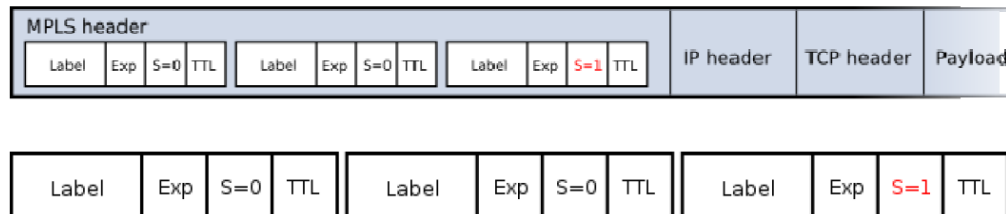


Figura 5.3.2.1: Ejemplo de “Label Stack”

Para conseguirlo, un LSR en vez de intercambiar las etiquetas lo que hace es añadir una etiqueta nueva arriba en la pila. Las etiquetas se añaden siguiendo un sistema LIFO (Last-in, First-out) y no altera el funcionamiento de enrutado, simplemente el router lee la etiqueta más externa y actúa únicamente en función de ese valor.

<sup>3</sup> El Interior Gateway Protocol (IGP), Protocolo de Pasarela Interna o Protocolo de Pasarela Interior, hace referencia a los protocolos usados dentro de un sistema autónomo.

<sup>4</sup> Open Shortest Path First (OSPF), Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP)

<sup>5</sup> IS-IS (del inglés Intermediate System to Intermediate System) es un protocolo de estado de enlace, o SPF (Shortest Path First), que básicamente maneja un mapa para enrutar paquetes mediante la convergencia de la red. Es también un protocolo IGP

## LDP (Label Distribution Protocol)

EL LDP es el protocolo más extendido para la distribución de etiquetas y comunicación de ellas a los LSR's, aunque existen otros como RSVP, PIM o TDP. Está definido en el RFC 3036, funciona sobre TCP y usa las tablas de enrutamiento IP existentes creadas por el protocolo de enrutamiento, como OSPF, para propagarse.

El LDP, por un lado, asocia un FEC con cada camino LSP que se crea, y por el otro, intercambia y distribuye esta información de asociación de las etiquetas entre dos LSR vecinos. Esta asociación es bidireccional y permite que un LSR aprenda del otro.

La distribución de las etiquetas usa uno de los dos siguientes métodos:

- ✓ Unsolicited Downstream: En este método, el LSR distribuye su información sobre las etiquetas cuando las tiene disponibles, aunque no se la hayan solicitado.
- ✓ Downstream on Demand: Solo se envía información sobre las etiquetas cuando el LSR vecino pide información sobre ella.

### 5.3.3. Funcionamiento del protocolo

Con el enrutamiento IP los paquetes avanzan de “salto en salto” a través de la red, es decir que en cada router se encamina el paquete hacia el siguiente salto en función de su dirección IP destino y de la tabla de enrutamiento. En MPLS, los LSR también encaminan los paquetes “salto a salto” pero simplemente basándose en la etiqueta de longitud fija, lo que significa que no usan la información de la cabecera IP. Para explicar el funcionamiento del protocolo se hará referencia al modelo de la Figura 5.3.3.1.

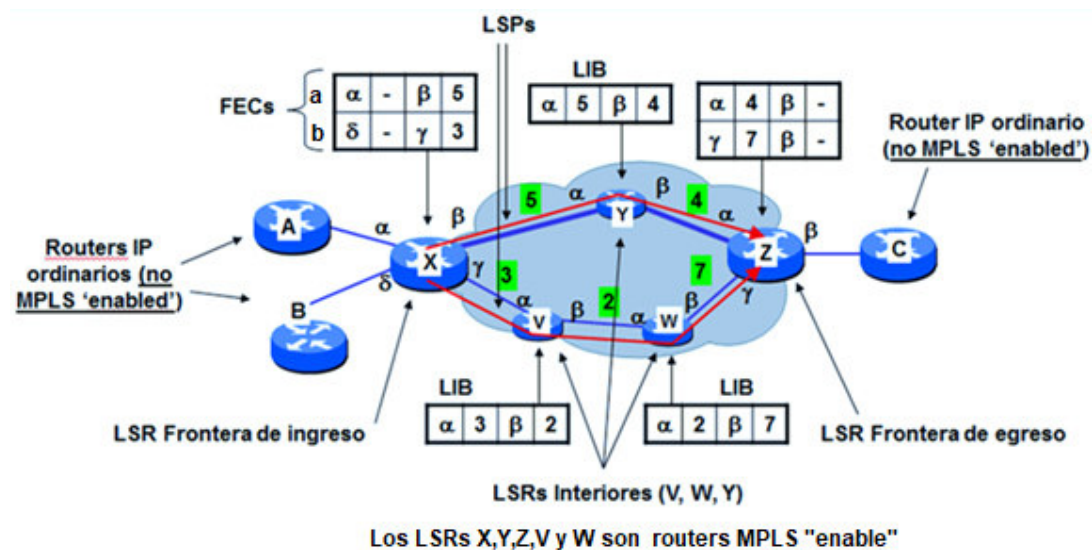


Figura 5.3.3.1: Red MPLS

## Creación y distribución de etiquetas

Antes de que se inicie el tráfico de datos, cada router de ingreso (LER) une ciertas etiquetas con determinados FEC's. La FEC de un paquete se puede determinar mediante uno o más de varios parámetros, según lo que sea especificado por el administrador de red. Algunos de los posibles parámetros son los siguientes:

- ✓ Direcciones IP de origen y / o destino o direcciones de red IP
- ✓ Números de puerto de origen y / o destino
- ✓ ID de protocolo IP
- ✓ Código de servicios diferenciados (valor que se le asigna a un campo del datagrama IP para diferenciar servicios)
- ✓ Etiqueta de flujo IPv6 U

Una vez completado este proceso, se distribuyen estas uniones usando el protocolo LDP entre los distintos LSR's.

En el caso de la Figura 5.3.3.1, el router "X" tiene definido dos FEC's (a y b). Luego el protocolo LDP ha distribuido la información correspondiente a cada uno de los FEC's hacia los LSR's.

## Protocolo LDP (Label Distribution Protocol)

LDP es un protocolo de capa de aplicación para distribuir la asociación de Label's a LSR's. Son usados para mapear FEC's a Label's y a su vez, éstos a LSP's. Las sesiones LDP son establecidas entre LDP pares en la red MPLS (no necesariamente adyacentes).

El protocolo LDP usa TCP para comunicar las etiquetas, ya que aporta fiabilidad a la red. Un error en la distribución de las etiquetas resultaría fatal para el funcionamiento de la red.

## Creación de la tabla LIB en cada LSR

Cada LSR construye una tabla de etiquetas LIB (Label Information Base) a medida que va recibiendo las etiquetas por parte del protocolo LDP. Las tablas LIB es donde se especifica el mapeo de cada etiqueta con un interfaz, tanto de entrada como de salida. Esta tabla se actualiza cada vez que se efectúa una renegociación de las uniones de etiquetas.

Esta tabla (LIB), guía al LSR cuando tiene que realizar un swap de etiquetas, indicándole a que interfaz tiene que dirigir el paquete. En el ejemplo de la figura 5.3.3.1, la tabla del router "Y" está indicando que un paquete que arribe por la interfaz 2

con  $\alpha$  con etiqueta 5, debe ser enviado a la interfaz  $\beta$  con una etiqueta 4 (debe ser extraída la etiqueta 5 y agregada la etiqueta 4).

### Creación de los LSPs

El siguiente paso es la creación de los LSP, los cuales se crean en orden inverso a la trayectoria del paquete. Lo que significa que el LSP se crea en el Nodo Destino hacia el Nodo Origen.

El Nodo Origen, al recibir un paquete del cual no tiene etiqueta en la tabla LIB, solicita mediante un paquete “request” la ruta que necesita. Este paquete “request” se irá propagando hasta llegar al nodo LER de salida. Una vez recibido este paquete, el LER enviará un paquete de “mapping” en dirección upstream. Este paquete, al pasar por los nodos hacia el Nodo Origen, irá completando la tabla LIB relacionada con el LSP que se está creando.

En el caso de la figura 5.3.3.1, el FEC “a” tiene como LSP el siguiente camino: routers “X”, luego el “Y” y por último el router “Z”.

### Cómo fluye un paquete en la red MPLS

Una vez ya tenemos definidos los FEC’s, y las etiquetas, solo nos queda analizar el proceso que sigue un paquete al entrar en una red MPLS.

Primero, llega un paquete sin etiquetar a un router LER de ingreso. El router entonces decide a que FEC pertenece y le asigna las etiquetas correspondientes (push). El proceso de asignar un paquete a un FEC solo se hace una vez, a diferencia de lo que ocurriría con un paquete IP tradicional, que se evalúa en cada nodo.

Una vez el paquete ya está etiquetado, se envía al siguiente salto LSR usando la tabla LIB.

Este paquete va saltando de LSR en LSR basándose en la tabla LIB de cada router. Normalmente lo que hacen estos routers es hacer un swap de la etiqueta.

Finalmente, el paquete llega al router LER de salida, el cual es el encargado de quitar la última etiqueta (pop) y enviar el paquete hacia su destino por routing convencional. En este punto, el paquete ya no es del tipo MPLS porque ya no tiene etiquetas. Este último paso suele realizarlo en penúltimo router de la red (Penultimate Hop Popping). La razón de esto es para liberar al último router del trabajo, ya que este tiene que enrutar un paquete IP y si además tuviera que eliminar la etiqueta, tendría dos trabajos. De esta forma, el penúltimo router de la red MPLS hace un pop en el momento de enviar el paquete al interfaz que le indica la tabla LIB y el último router ya recibe un paquete IP convencional.

### Fast Reroute

Existen muchos factores que pueden provocar un fallo en la red, pero a grandes rasgos y a nivel del router se pueden resumir en fallos en los enlaces o en los nodos. Estos fallos pueden repercutir en la pérdida de paquetes por parte de la red.

MPLS introduce el mecanismo de Fast Reroute para redirigir el tráfico por nuevas rutas no definidas por el protocolo IGP y minimizar el número de paquetes perdidos.

Normalmente, cuando se produce un fallo en un enlace o un nodo, se señala en las cabeceras de los LSP's que usan ese enlace o nodo. En ese momento el protocolo IGP recalcula la ruta para redirigir los paquetes. En este tiempo se pueden producir las pérdidas de paquetes, las cuales pueden ser significativas en aplicaciones en tiempo real como la voz o el video.

El mecanismo, aunque no asegura no tener pérdidas de paquetes, sí que las minimiza. Para poder usar este mecanismo eficientemente, se tiene que configurar un camino principal por donde se enrutará el tráfico, y simultáneamente implementar un camino de backup para dotar al enlace, o nodo de redundancia. Cuando se detecte un fallo en el enlace principal, Fast Reroute desviará el tráfico hacia el camino de backup, que cómo ya estaba configurado, no perderá tiempo en recalcular la ruta.

#### 5.3.4. Calidad de Servicio (QoS) y Clases de Servicios (CoS)

Una de las características clave de MPLS, comparado con redes tradicionales como Frame Relay y ATM, es que está diseñado para proveer servicios garantizados. Es decir, que, según los requisitos de los usuarios, permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva.

QoS y clases de servicios, factores fundamentales de esta tecnología pueden ser implementados a través de ingeniería de tráfico. Esta capacidad permite proveer a los distintos usuarios; un servicio de nivel estable (Service Level Agreements, SLAs) en aspectos como: ancho de banda, tiempo de demora, y variación del mismo.

En los últimos años el tráfico de redes ha aumentado considerablemente, la necesidad de transmitir cada vez más información en menos tiempo, como video y audio en tiempo real (streaming media). La solución no es solo aumentar el ancho de banda (bandwidth) cada vez más, ya que en la mayoría de los casos esto no es posible y además es limitado. Es aquí donde la administración efectiva de recursos que provee QoS es clave en la operación eficiente de la red.

QoS trabaja a lo largo de la red y se encarga de asignar recursos a las aplicaciones que lo requieran, dichos recursos se refieren principalmente al ancho de banda. Para asignar estos recursos QoS se basa en prioridades, algunas aplicaciones podrán tener más prioridades que otras, sin embargo, se garantiza que todas las

aplicaciones tendrán los recursos necesarios para completar sus transacciones en un periodo de tiempo aceptable.

QoS otorga mayor control a los administradores sobre sus redes, mejora la interacción del usuario con el sistema y reduce costos al asignar recursos con mayor eficiencia (bandwidth). Mejora el control sobre la latencia (Latency y jitter) para asegurar la capacidad de transmisión de voz sin interrupciones y por ultimo disminuye el porcentaje de paquetes desechados por los enrutadores: confiabilidad (Reliability).

La Figura 5.3.4.1 muestra un camino para el tráfico QoS en rojo, otro camino para el tráfico normal en azul, y como complemento del ejemplo, muestra cual sería el camino más corto en color verde. Éste último no es elegido para el tráfico de voz, porque tal vez esté muy congestionado, y tenga demoras inaceptables para la voz.

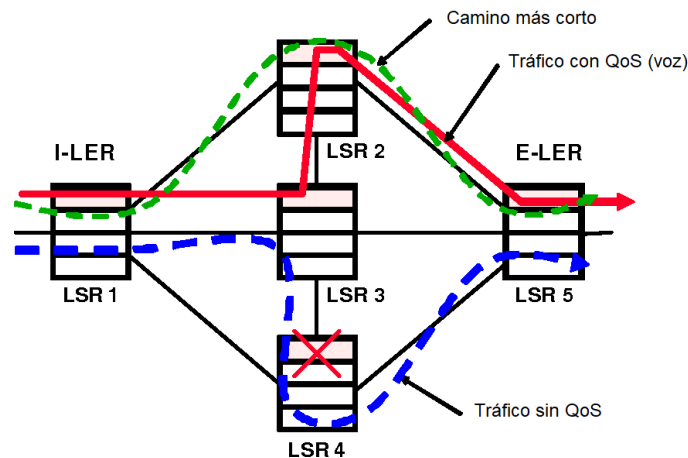


Figura 5.3.4.1: Caminos alternativos para cada tipo de tráfico

### InterServ y DiffServ

Varios mecanismos son los que utiliza MPLS para dar estabilidad de QoS y CoS dentro de su red. En el modelo InterServ (Integrated Services), RSVP obtiene los requerimientos para establecer un flujo de tráfico con QoS, permitiendo a los distintos LSR las negociaciones necesarias para generar un tráfico garantizado y otros parámetros o recursos como ancho de banda y latencia end to end.

El modelo DiffServ (Differentiated Services) del IETF, define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio (CoS), otorgando un servicio no necesariamente garantizado para el curso del tráfico con diferentes prioridades. Para ello se emplea el campo ToS (Type of Service), en la cabecera de paquete IP para proveer esta clasificación.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP (3 bits) para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- ✓ El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.
- ✓ Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio: premium, normal y turista, que, lógicamente, tendrán distintos costos.
- ✓ Mientras que InterServ ofrece ancho de banda garantizado para el tráfico, no provee escalabilidad u operabilidad en grandes redes, por otro lado, la arquitectura DiffServ, es una alternativa escalable pero no provee de una garantía total.
- ✓ Recientemente la IETF workgroup se ha enfocado en la combinación de elementos de DiffServ e ingeniería de tráfico, para dar servicios garantizados de flujos de datos MPLS dentro de la red. La información DiffServ en la cabecera IP es mapeada e introducida dentro de la etiqueta de información de los paquetes MPLS.
- ✓ Qos puede ser y es generalmente implementado en el borde de la red MPLS donde el usuario comienza con la transmisión de los paquetes que requieren un tráfico en tiempo real.

### 5.3.5. MPLS y VPN (Virtual Private Networks)

Cómo ya fue desarrollado en 1.9.5, una VPN (Virtual Private Network) es una tecnología en la que se establecen canales seguros de comunicación que ofrecen protección a los datos transmitidos mediante el uso de algoritmos de encriptación y/o autenticación criptográfica.

Una VPN es virtual porque es físicamente una red distinta, es privada porque la información que transita por los túneles es encriptada para brindar confidencialidad, y es una red porque consiste en enlaces de comunicación, pudiendo incluir enrutadores, switches y gateways de seguridad.

VPN es una tecnología punto a punto, ampliamente adoptada en redes que requieren confidencialidad permanente, tanto en redes privadas como entre proveedores de Servicio de Internet y sus clientes. En el mercado existe una gran variedad de soluciones VPN, sin embargo, ahora solo se hará referencia a VPN MPLS.

Las redes VPN pueden ser organizadas en dos categorías:



- ✓ Basadas en Clientes: La VPN es configurada en equipos exclusivamente localizados en el cliente y usando protocolos de túneles para el curso de tráfico sobre redes públicas. IPSec agrega seguridad y capacidad de encriptación para IP. Este es típicamente manejado desde el cliente, es decir, fuera del proveedor de servicio.
- ✓ Basadas en redes: Aquí la VPN es configurada en equipos de los proveedores de servicios y manejadas por los mismos. MPLS VPN es un ejemplo de estas redes.

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

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

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN.

Sin embargo, el problema real que plantean estas IP VPN's, es que están basadas en un modelo topológico superpuesto sobre la topología física existente, es decir, basado en túneles extremos a extremo (o circuitos virtuales permanentes) entre cada par de routers de clientes en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes.

MPLS VPN es mantenida y manejada por el proveedor de servicio, con lo cual puede proveer al consumidor ahorros muy significativos, además de una gran escalabilidad de crecimiento comparado con otras tecnologías VPN. MPLS VPN lleva diferentes tipos de tráfico del cliente, de forma única y separada para el envío de flujo de datos por cada VPN establecida. Este método de funcionamiento evita la necesidad de establecer y mantener circuitos virtuales permanentes, algo que, junto con la aplicación de técnicas de priorización de tráfico, hace de MPLS una solución ideal para crear redes VPN IP completamente malladas.

Estos mecanismos además de proveen la separación del tráfico y es totalmente transparente en el usuario final, que pertenece a un grupo VPN. MPLS VPN provee seguridad inherente, llevando tráfico IP seguro, como Frame Relay o ATM reduciendo la necesidad de encriptación.

MPLS VPN se clasifica en dos categorías, aquellas que operan sobre capa 3 y las que operan sobre capa 2.

La siguiente Figura 5.3.5.1 muestra ejemplos de MPLS VPN de capa 2 y de capa 3. Se observa que se utilizan LSP's, nombre genérico de un camino MPLS, y en todos los casos se observan que se necesita un camino en cada dirección.

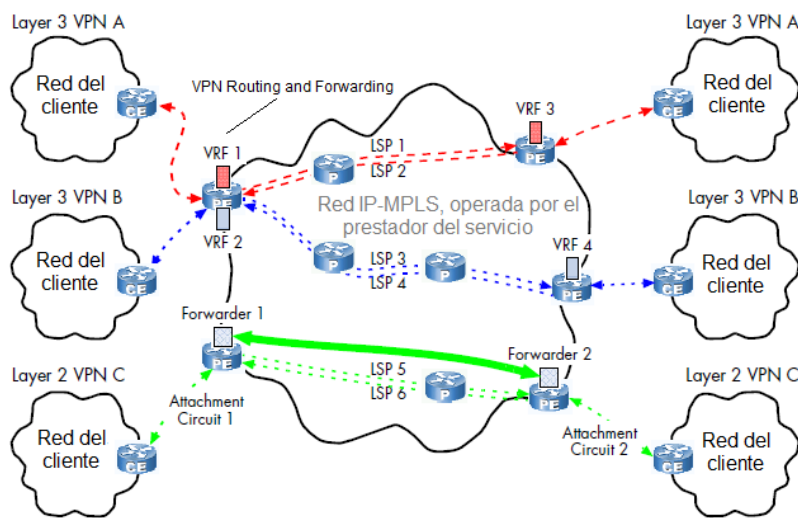


Figura 5.3.5.1: VPN MPLS de capa 2 y 3

En el caso de las VPN's de capa 3 (A y B), se puede observar que en LER de ingreso/egreso (aquí lo llaman PE, Provider Edge) se deben definir instancias de ruteo (VRF, VPN Routing and Forwarding), de forma tal que el mismo pueda realizar de la tarea de enrutar los datagramas en función del Label (etiqueta) que tengan. Es oportuno aclarar que, en el gráfico, al router que se encuentra en las instalaciones del cliente le llama CE (Client Edge).

Por último, la VPN C, la cual es de capa 2, no necesita una definición de una instancia de VRF. En este caso, sólo con la definición de los LSP's (en color verde) se puede activar la misma. Cabe acotar en este caso, que las redes definidas en los clientes de ambas puntas, pueden pertenecer al mismo espacio de direcciones IP, con lo cual, los usuarios van a percibir una única red virtual, como si todos estuvieran conectados a un único conmutador (switch).