UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

COMO IMPLEMENTAR UNA RED PRIVADA VIRTUAL
UTILIZANDO TECNOLOGÍA MPLS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JORGE ALAN PEZO PEZO

PROMOCIÓN
1985 - I

LIMA – PERÚ
2006

COMO IMPLEMENTAR UNA RED PRIVADA VIRTUAL UTILIZANDO TECNOLOGÍA MPLS

Dedico este Trabajo a:

María Elena, por ser una gran compañera y esposa.
César Alan y Elena de Jesús; mis hijos, inspiración y esperanza de superación
A mis padres, quienes siempre han sido ejemplo en mi vida.
A mi suegro Licurgo que siempre me respaldó en todo.

A mis cuñados Lidia y Juan por su invalorable apoyo.

SUMARIO

Las Redes Privadas Virtuales (VPNs) son una alternativa práctica, segura y eficiente de los enlaces privados que en la actualidad son usados para interconectar redes corporativas y brindar acceso con seguridad a usuarios y a sitios remotos.

El propósito de este informe consiste en analizar, modelar e implemantar una VPN usando tecnología MPLS. La tecnología *Multi-Protocol Label Switching* (MPLS), ha sido identificada como una importante herramienta para confrontar las necesidades de los proveedores de servicios de Internet. El MPLS implementa mejoras a los protocolos de ruteo IP con el fin de orientarlos a la conexión. Es por esto que el MPLS se considera la evolución natural requerida para que las redes de comunicaciones soporten servicios de IP óptimos y predecibles.

Los siguientes capítulos componen el siguiente trabajo:

El capitulo I ofrece una introducción con una visión general del crecimiento de Internet con un incremento en la demanda de nuevos y más sofisticados servicios. Una de estas nuevas tecnologías para confrontar las necesidades de los servicios de los proveedores de Internet es Multiprotocol Label Switching (MPLS). El capitulo II se refiere a los enlaces privados antes de la aparición de las redes privadas virtuales. El capitulo III trata sobre las Redes Privadas Virtuales. El capitulo IV describe la arquitectura operación y aplicaciones de la tecnología MPLS. El capitulo V describe la implementación de una red VPN usando la tecnología MPLS.

ÍNDICE

CAPÍTULO III

REDES PRIVADAS VIRTUALES

CAPÍTULO IV

INTRODUCCION MPLS

PRÓLOGO

Hace unos años no era tan importante conectarse a Internet por motivos laborables, pero a medida que ha pasado el tiempo las corporaciones han requerido que las redes de área local (Local Area Network, LAN) trasciendan más allá del ámbito local para incluir personal y centros de información de otros edificios, ciudades, estados e incluso otros países. En contrapartida, era necesario invertir en hardware, software y en servicios de telecomunicaciones costosos para crear redes amplias de servicio (Wide Area Network, WAN). Sin embargo, con Internet, las corporaciones tienen la posibilidad de crear una red privada virtual (VPN) que demanda una inversión relativamente baja utilizando Internet para la conexión entre diferentes localidades o puntos.

Las redes privadas virtuales (VPN) deben su creciente popularidad al hecho que las empresas, han buscado la forma de utilizar una red pública, ampliamente extendida y de bajo costo cómo Internet para aumentar la movilidad, mejorar la productividad de los empleados y contribuir al desarrollo. Y las VPN han demostrado que lo pueden lograr, cuando les permiten a los trabajadores remotos que desarrollan sus actividades en la calle, en el hogar o en otras oficinas, tener acceso a una única red privada de la compañía desde cualquier parte del mundo utilizando su computadora portátil, hogareña o de oficina y el Internet público.

Básicamente, una VPN es una red privada que utiliza una red pública (generalmente Internet) para conectar varios lugares o usuarios remotos entre ellos. En vez de utilizar una conexión dedicada o líneas alquiladas, una VPN usa una "conexión virtual" a través de Internet desde la red privada de la compañía hasta el sitio o empleado remoto. En este artículo intentaremos llegar a un entendimiento más acabado sobre las redes privadas virtuales y sus diferentes usos.

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentas con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia.

Las Redes Privadas Virtuales (VPNs) son una alternativa práctica, segura y eficiente de los enlaces privados que en la actualidad son usados para interconectar redes corporativas.

Tradicionalmente, IP (Internet Protocol) ha sido ruteado sobre ATM (Asynchronnous *Transfer Mode) por medio de circuitos virtuales (VCs) o multiprotocolos sobre ATM*(MPOA). Estos métodos probaron ser complicados para implementar, por lo que se sintió la necesidad por un método de ruteo más simple.

Todas estas necesidades pueden ser cubiertas por el MPLS, ya que integra las más importantes características de las capas 2 y 3 del modelo ISO/OSI.

La tecnología MPLS (Multiprotocol Label Switching) integra el ancho de banda y la utilización de Capa 2 en la Capa3 para mejorar y simplificar el intercambio de paquetes. Es decir, es una técnica que utiliza la inteligencia del ruteo y el desempeño del switcheo para disminuir el tráfico de rutas, la congestión, las fallas de conexión y los cuellos de botella.

El propósito de este informe consiste en el análisis, modelado e implementación de una red VPN usando tecnología MPLS, siendo un tema de actualidad y de gran futuro. Se pretende realizar esquemas y casos en los que se demuestre que la implementación de dicha tecnología en VPNs mejora el rendimiento, tanto de rapidez como de seguridad.

CAPITULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Planteamiento del Problema

Durante los últimos años, el crecimiento de Internet ha seguido un curso que se torna imparable y de crecimiento exponencial; al mismo tiempo se incrementa la demanda de nuevos y más sofisticados servicios, la tecnología ha tenido que sufrir cambios fundamentales con respecto a las prácticas habituales desarrolladas a mitad de los años 90.

En este ambiente de supercrecimiento, los proveedores de servicio Internet (ISP's[1]) deben encontrar una manera de ajustar el dramático crecimiento del tráfico en las redes y el número de usuarios.

Hay muchos factores que han contribuido a la demanda por un ancho de banda más grande. Cada vez se realizan más transacciones de negocios por Internet, ya que la gran mayoría de las empresas están buscando las mejores formas de mejorar sus procesos de ventas y de reducir los costos para hacer tratos con sus socios. El número de usuarios alrededor del mundo está creciendo también muy rápido.

En los últimos años también las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado que las redes reducen, en tiempo y dinero, los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, por eso que escuchamos hablar tanto de los famosos *firewalls* y las VPN.

---

[1] ISP, Internet Services Provider

Las Redes Privadas Virtuales (VPNs) son una alternativa práctica, segura y eficiente de los enlaces privados que en la actualidad son usados para interconectar redes corporativas.

Tradicionalmente, IP (*Internet Protocol*) ha sido ruteado sobre ATM (*Asynchronnous Transfer Mode*) por medio de circuitos virtuales (VCs) o multiprotocolos sobre ATM (MPOA). Estos métodos son complicados para implementar, por lo que se tuvo la necesidad de emplear un método de ruteo más simple.

Todas estas necesidades pueden ser cubiertas por el MPLS, ya que integra las más importantes características de las capas 2 y 3 del modelo ISO/OSI.

El propósito de este informe consiste en analizar, modelar e implemantar una red VPN usando tecnología MPLS, esto es, encontrar las principales características de este nuevo estándar y así demostrar su mayor eficiencia en el manejo del tráfico en redes de comunicaciones.

La tecnología *Multi-Protocol Label Switching* (MPLS), ha sido identificada como una importante herramienta para confrontar las necesidades de los proveedores de servicios de Internet. El MPLS combina una variedad de funciones tanto de IP, como de ATM.

Específicamente, el MPLS implementa mejoras a los protocolos de ruteo IP con el fin de orientarlos a la conexión. Es por esto que el MPLS se considera la evolución natural requerida para que las redes de comunicaciones soporten servicios de IP óptimos y predecibles. El MPLS sigue los preceptos de los SLAs(*Service Level Agreements*), al incorporar las mejores características de las Capas 2 y 3 de OSI.

1.2 Justificación e Importancia del tema

La importancia del tema se hace visible cuando se quiere conocer, dentro de las tecnologías actuales, la mejor opción con que se cuenta para implementar redes basadas en IP. Si bien el modelo IP sobre ATM ha sido una solución que ofrece grandes ventajas sobre otros protocolos, ha quedado claro que ya ha sido superado por el crecimiento exponencial de la demanda por mejores servicios de red.

El MPLS surge como la mejor opción que se puede encontrar, por sus características, sus ventajas, su ingeniería de tráfico, su bajo costo de implementación y, sobre todo, por el gran futuro que le espera en la adecuación y desarrollo de nuevas redes.

CAPITULO II
ENLACES

2.1 Los enlaces Privados antes de las Redes Privadas Virtuales

En las redes de comunicaciones, en especial en el sector corporativo, siempre se ha requerido la implementación de enlaces privados para transportar de forma segura toda la información confidencial.

Este capítulo trata sobre la manera en que se realizan los enlaces privados y las diferentes tecnologías que los soportan.

Los enlaces privados se caracterizan por brindar seguridad en la transmisión de datos de extremo a extremo. Se valen siempre de una red de transmisión (en algunos casos también existe una red de conmutación) para conectar las partes. Estos enlaces pueden ir desde los 9600 bps (en el caso de una conexión conmutada usando un modem análogo de 9600 bps) hasta el orden de los Gigabps (usando redes ópticas, con equipos de transporte de última generación o multiplexores DWDM).

Las redes de computadores se han valido de los enlaces privados para interconectarse a través de grandes distancias geográficas. Antes de la aparición de las VPN existían sólo dos tecnologías de enlaces WAN, los enlaces dedicados y los enlaces conmutados.

Dentro de los enlaces dedicados mencionamos topologías tales como *Clear Channel*, *Frame Relay* y ATM. Aunque se sabe que *Frame Relay* usa conmutación de paquetes y ATM la conmutación de celdas, aquí se clasifican como enlaces dedicados, porque para el usuario la conmutación es transparente.

Dentro de los enlaces conmutados existen los análogos que van desde 2400bit/s hasta los 56 kbits/s y los digitales RDSI[2] de 64 kbits/s y 128 kbits/s.

[2] RDSI, Red Digital de servicios Integrados

2.2 Los enlaces Dedicados

Los enlaces dedicados, como su nombre lo indica, son conexiones permanentes punto-punto o punto-multipunto, que se valen de una infraestructura de transporte (Capa 1) o de transporte y conmutación (Capa 1 y 2). Los primeros son comúnmente llamados enlaces *Clear Channel* y los segundos son enlaces *Frame Relay* o ATM.

2.2.1 Clear Channel

Son enlaces donde solo interviene la red de transporte del proveedor de servicios. Para el mercado corporativo comúnmente van desde los 64 kbits/s hasta los 2048 kbits /s, en pasos nx64. Para el mercado de proveedores de servicio van desde tasa E1 hasta OC-3 y superiores inclusive. En la tabla 2.1 se observan las tasas de transmisión desde OC-1 hasta OC-768 así como su correspondencia entre redes SONET y SDH.

Tabla 2.1 Equivalencia entre sistemas SONET y SDH

SONET	SDH	Mbps
OC-1	---	51.84
OC-3	STM-1	155.52
OC-12	STM-4	622.08
OC-48	STM-16	2455.32 (≈2.5 Gbps)
OC-192	STM-64	9953.28 (≈10 Gbps)
OC-768	STM-256	39813.12 (≈40 Gbps)

Los enlaces *Clear Channel* ofrecen un *throughput* efectivo casi del 100% ya que no usan ningún tipo de encapsulación de nivel 2, es decir, no hay presentes cabeceras de ningún tipo. Por lo general estos enlaces son entregados en interfaz E1 balanceada o desbalanceada con trama G.703, o en interfaz serial de datos V.35. Por lo general, la compañía (o cliente en general) debe tener un puerto disponible DTE que cumpla con las especificaciones técnicas del equipo de comunicaciones entregado por el proveedor. Típicamente la mayoría de los equipos que se usan para recibir los enlaces *Clear Channel* por parte del cliente son enrutadores o switches de nivel 3. Y son estos, los que se encargan de manejar los niveles 2 y3[3]

[3] En la actualidad existen enrutadores y switches que manejan incluso protocolos a nivel 4. Estos equipos se usan para balancear tráfico entre varios servidores, redireccionamiento de tráfico, políticas de calidad de servicio y *accounting* (toda aquella información que sirve para tarifar transacciones o servicios).

En general, las topologías de los enlaces *Clear Channel* son robustas pero a su vez estáticas. Esto significa que para aumentar o disminuir la tasa del enlace es necesario cambiar equipos o manipularlos localmente. Lo que se transfiere al cliente en indisponibilidades del servicio no deseadas.

Vale la pena aclarar, que los enlaces *Clear Channel* fueron la primera tecnología WAN que se adoptó usando la infraestructura de voz PCM(*Pulse Code Modulation*) de los distintos operadores de telefonía locales, nacionales e internacionales. Como era de esperarse, por provenir de una tecnología que no había sido pensada para transmitir datos fue superada rápidamente por otros tipos de tecnologías como *Frame Relay* y ATM, aunque aun muchas empresas siguen teniendo enlaces *Clear Channel*. La figura 2.1 muestra un esquema básico, donde se observa la transparencia para una organización del enlace *Clear Channel* contratado.

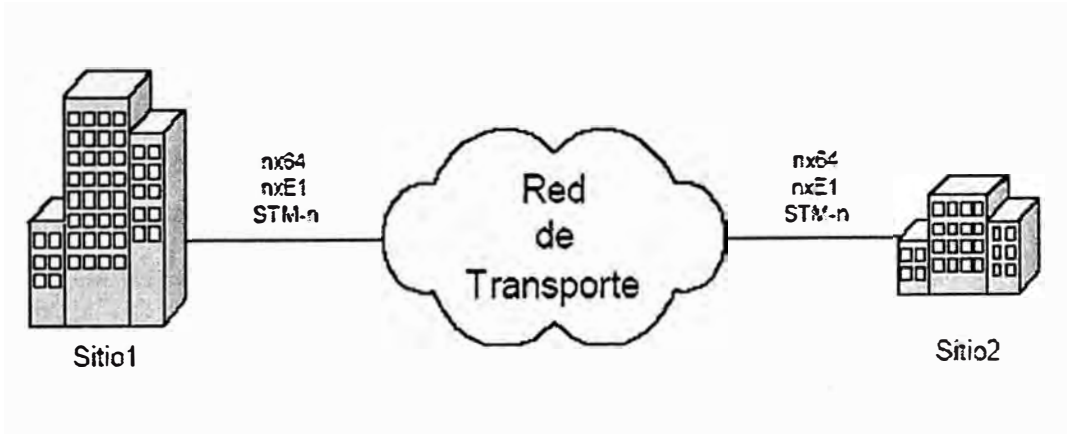


Figura 2.1 Enlace típico Clear Channel. Esquema Básico

La figura 2.2 muestra un esquema detallado de los equipos usados en una topología de transporte de datos *Clear Channel*. También muestra los límites de la última milla y del *backbone* que se usa para transporte, estos tramos son generalmente responsabilidad del proveedor del servicio. Los equipos que se muestran pueden variar dependiendo del medio físico a utilizar: cobre, fibra óptica o espectro electromagnético.

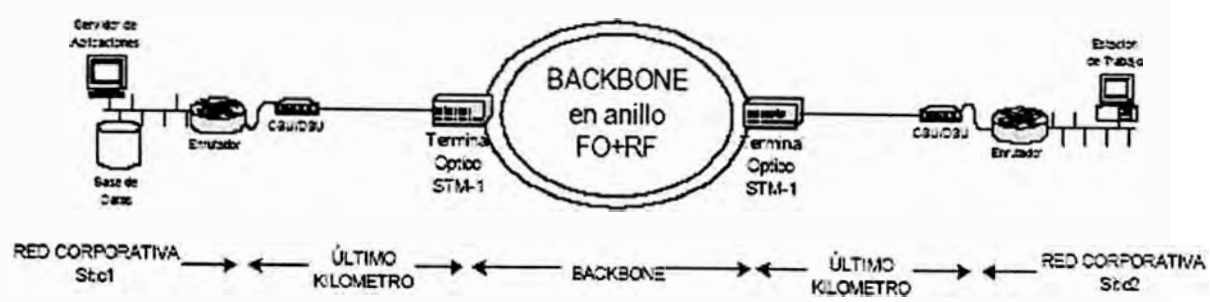


Figura 2.2 Enlace típico Clear Channel. Esquema detallado

2.2.2 Frame Relay

Frame Relay es un protocolo WAN de alto rendimiento que trabaja en la capa física y de enlace de datos del modelo de referencia OSI.

Frame Relay fue diseñado originalmente para trabajar con redes ISDN.

Frame Relay es una tecnología de conmutación de paquetes, que permite compartir dinámicamente el medio y, por ende, el ancho de banda disponible. La longitud de los paquetes es variable para hacer más eficiente y flexible las transferencias de datos. Estos paquetes son conmutados por varios segmentos de la red hasta que llegan hasta el destino final. Todo el acceso al medio en una red de conmutación de paquetes es controlado usando técnicas de multiplexación estadística, por medio de las cuales se minimizan la cantidad de demoras y/o colisiones para acceder al medio.

Ethernet y *Token Ring*, los protocolos de redes LAN más usados, también usan conmutación de paquetes y técnicas de difusión.

Frame Relay es una evolución de las redes X.25, no hace retransmisión de paquetes perdidos ni *windowing*[4], características que si ofrecía su antecesor ya que en los años 70 (época en la que aparece X.25) los medios físicos no eran tan confiables como los de hoy día, y por tanto se necesitaba mayor robustez. Todas las ventajas que ofrecen los medios de hoy día, han posibilitado a *Frame Relay* ofrecer un alto desempeño y una gran eficiencia de transmisión. (1)

Los propósitos iniciales para estandarizar *Frame Relay* fueron presentados al Comité Consultivo Internacional para la Telefonía y la Telegrafía (CCITT) pero no tuvieron mucha acogida. Solo hasta 1990 cuando Cisco, Digital Equipment, Nortel Networks (en ese tiempo todavía Northern Telecom) y SttasaCom conformaron un forum y desarrollaron un conjunto de normas llamadas LMI (*Local Management Interface*) que fueron adicionadas a

[4] Windowing es un esquema de control de flujo en el cual el dispositivo fuente requiere un reconocimiento del destino después que un cierto número de paquetes han sido transmitidos

la propuesta original que tenia la CCITT, fue que esta última organización junto con la americana ANSI se interesaran de nuevo en *Frame Relay* y finalmente se publicara un estándar, que fue apoyado por la ITU-T.

Esta estandarización le dio tal fuerza a *Frame Relay* que prácticamente todos los fabricantes de equipos de comunicaciones de datos desarrollaron dispositivos que soportaron la creciente tecnología.

Los equipos que se usan en una red *Frame Relay* se pueden dividir en dos categorías: Equipos Terminales de Datos (DTEs) y Equipos Terminales de circuitos de Datos (DCEs). La figura 2.3 ilustra la ubicación de los DTEs y los DCEs en una red *Frame Relay*.

Los DTEs son generalmente considerados equipos terminales de una red especifica y típicamente son enrutadores, computadores personales, terminales o *bridges*. Estos equipos se localizan en las premisas del cliente y en la mayoría de los casos son propiedad de los mismos.

Los DCEs son dispositivos normalmente propiedad del *carrier*. El propósito de los equipos DCEs es proveer o generar señales de reloj y conmutar los paquetes de la red. Por lo general, son llamados *packet switchs* o conmutadores de paquetes.

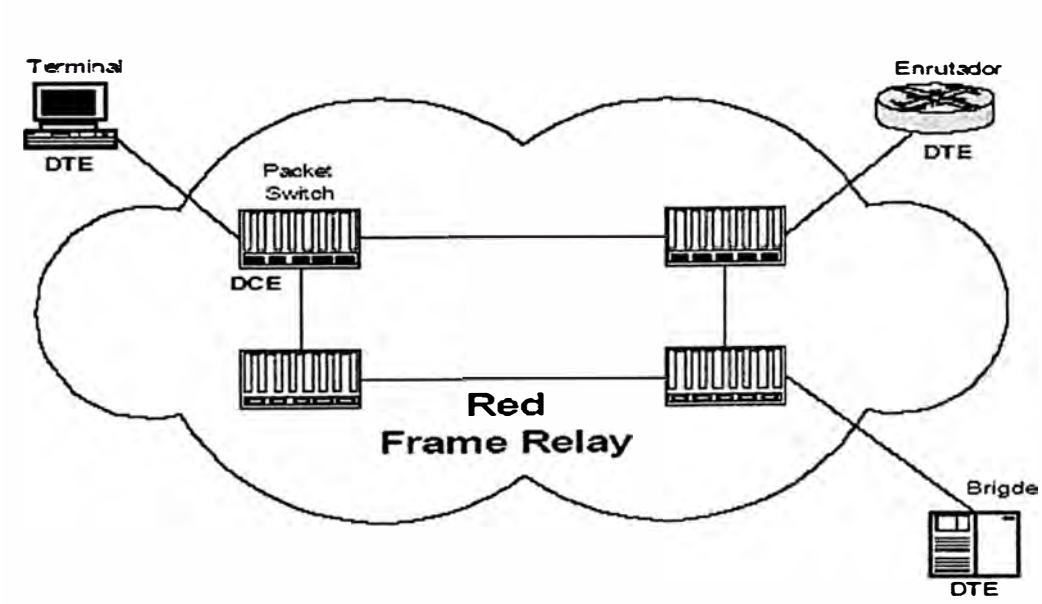


Figura 2.3 Diferentes dispositivos que intervienen en una red Frame Relay. Esquema básico.

En la conexión entre los dispositivos DCE y DTE intervienen dos componentes, uno de nivel físico y otro de nivel de enlace de datos. En el nivel físico se definen todas las características físicas, eléctricas y mecánicas entre los dos, y el nivel de enlace de datos define todas las especificaciones *Frame Relay* o *Frame Relay* LMI según sea el caso.

a). Circuitos virtuales *Frame Relay*

Frame Relay es una tecnología WAN que usa enlaces orientados a conexión, esto significa que una comunicación se define entre un par de dispositivos y que cada una de las conexiones existentes en la red tiene un identificador asociado particular. Este servicio es implementado usando circuitos virtuales, los cuales son conexiones lógicas creadas entre dos dispositivos DTE a través de la red conmutada de paquetes *Frame Relay*. Sobra decir que este circuito es bidireccional.

Un circuito lógico puede crearse a través de múltiples dispositivos intermediarios DCE dentro de la red *Frame Relay*.

Los circuitos virtuales Frame Relay se pueden dividir en dos categorías: circuitos virtuales conmutados (SVCs) y circuitos virtuales permanentes (PVCs).

a1). Circuitos Virtuales Conmutados (SVCs)

Los SVCs son conexiones temporales y que se usan en situaciones donde la transferencia de datos entre un par de dispositivos DTE es esporádica a través de la red *Frame Relay*. Los SVCs tienen 4 estados operacionales:

- *Call Setup*: Cuando se realiza la negociación y el establecimiento de un circuito virtual entre dos DTEs.
- *Data Transfer*: Cuando los datos entre los dos DTEs son transmitidos sobre el circuito virtual.
- Idle: Cuando la conexión entre los dos DTEs está todavía activa, pero no hay tráfico de datos. Si por cierto periodo de tiempo el circuito se encuentra en este estado, se procede a terminar la conexión.
- *Call Termination*: Cuando el circuito virtual entre los dos DTEs es terminado. Si después de terminado el circuito los dispositivos DTEs necesitan transmitir más datos, se deberá establecer un nuevo SVC, y así sucesivamente.

Este tipo de circuitos virtuales no es muy usado, de hecho muchos fabricantes no incluyen esta característica dentro de sus equipos *Frame Relay*.

a2). Circuitos Virtuales Permanentes (PVCs)

Los PVCs son conexiones establecidas permanentemente y que se usan en donde la transferencia de datos es continua entre dos dispositivos DTE. Este tipo de conexiones no

requieren hacer una llamada de configuración ni de terminación como en los SVCs. De hecho los PVCs siempre operan en uno de los siguientes dos estados:

- *Data transfer*: Cuando los DTEs están intercambiando tráfico.
- Idle: Cuando no hay transferencia de datos, pero la conexión sigue activa.

A diferencia de los SVCs, un PVC puede estar indefinidamente en este estado y el enlace no es terminado.

b). Identificadores de conexión de enlace de datos (DLCI)

Los circuitos virtuales *Frame Relay* son identificados por DLCIs. Los valores de los DLCIs son asignados por el proveedor de servicio y tienen solo significado a nivel local, esto quiere decir que en una red *Frame Relay* pueden existir varios DLCIs con el mismo valor, pero no puede haber varios DTEs con un mismo DLCI conectados al mismo *Packet Switch*. Nótese que en la figura 2.4 existen valores repetidos de DLCIs pero no en un mismo DCE.

Además, los dos extremos del PVC pueden tener valores diferentes.

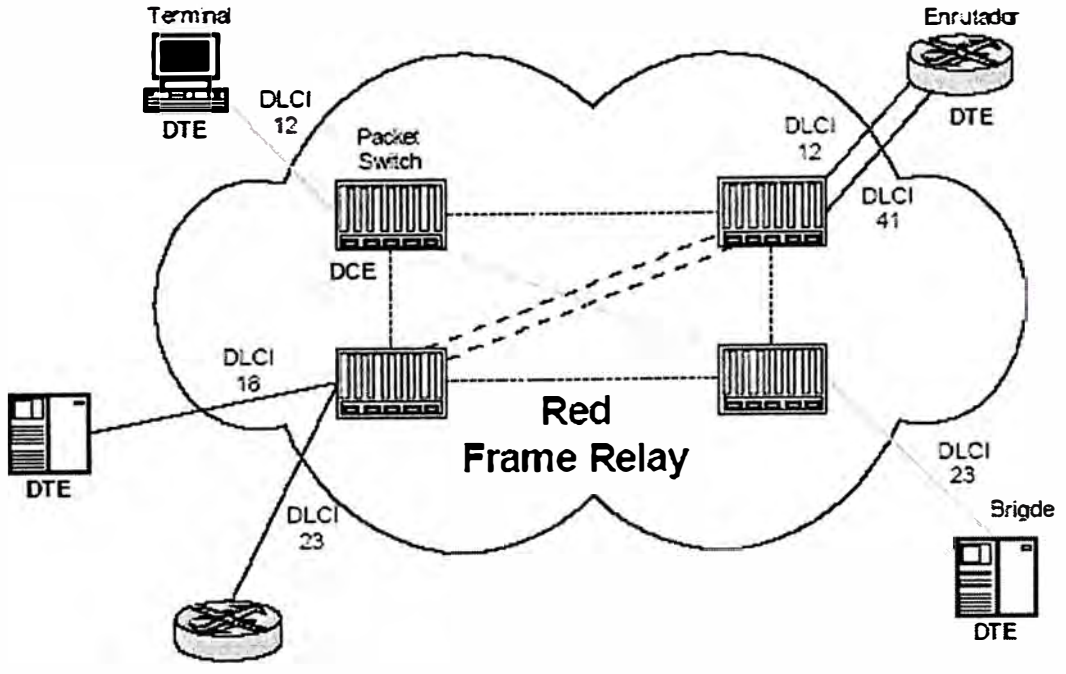


Figura 2.4 Ejemplo de asignación de valores DLCI en una red *Frame Relay*.

2.2.3 ATM (*Asynchronous Transfer Mode*)

El Modo de Transferencia Asíncrono (ATM) es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (ITU-T) para transmitir múltiples tipos de servicios, tales como voz, video y datos usando técnicas de conmutación de celdas pequeñas de tamaño fijo.

Las redes ATM son, al igual que las redes *Frame Relay*, orientadas a conexión. (2)

a). Estandarización

ATM está basado en esfuerzos hechos por el grupo de trabajo BISDN (*Broadband Integrated Services Digital Network*) de la ITUT. Fue originalmente concebido como una tecnología de transferencia de voz, video y datos de alta velocidad sobre redes públicas. Luego el Foro ATM extendió la visión pública de la ITU-T a redes privadas.

El foro ATM ha trabajo en el desarrollo de las siguientes especificaciones, que hacen parte de ATM:

- *User-to-Network Interface* (UNI) 2.0
- UNI 3.0
- UNI 3.1
- **Public-Network Node Interface** (P-NNI)
- *LAN Emulation* (LANE)

b). Funcionamiento de las redes ATM

ATM es una tecnología de multiplexación y de conmutación de celdas que combina los beneficios de una red de conmutación de circuitos (capacidad garantizada, retardos constantes) y de una red de conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente). Permite transmisiones desde unos pocos megabits por segundo hasta cientos de gigabits por segundo.

Su naturaleza asíncrona, hace del ATM una tecnología más eficiente que las síncronas tales como TDM. En TDM a los usuarios se les asigna un *timeslot*, y ningún otro cliente puede transmitir en ese *timeslot* así el propietario no este transmitiendo. Esto hace que la red no sea muy eficiente. En ATM los *timeslots* siempre están disponibles y se asignan por demanda basándose en la información que está contenida en las cabeceras de cada celda.

c). Formato de una celda ATM

ATM transmite información en unidades de tamaño fijo llamadas celdas. Cada celda contiene 53 octetos o bytes. Los primeros 5 bytes conforman la cabecera y los restantes 48 contiene la información del usuario o *payload* tal como se ve en la figura 2.5. El tamaño pequeño de cada celda hace que las transmisiones de voz y video gocen de una buena calidad ya que esta clase de tráfico no tolera retardos producidos por esperar paquetes de gran tamaño.

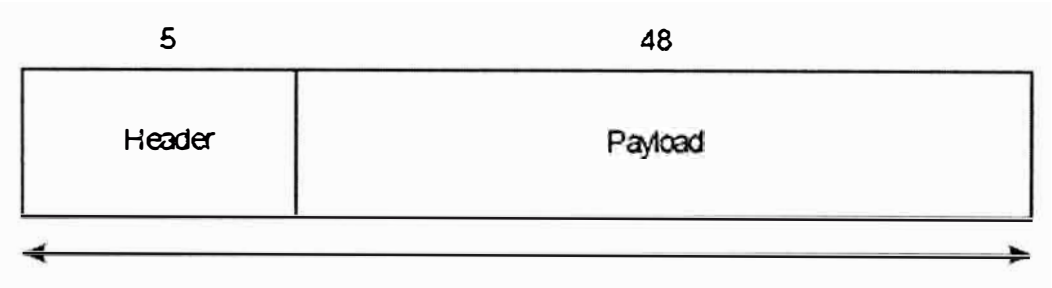


Figura 2.5 Formato básico de una celda ATM

d). Dispositivos ATM

Una red ATM está compuesta de dos tipos de dispositivos: los *switches* ATM y los terminadores ATM. Un *switch* ATM es el encargado de recibir las celdas entrantes provenientes de otro *switch* ATM, leer y actualizar las cabeceras de cada celda y direccionar la celda hasta que llegue a su destino final.

Los terminadores ATM (o sistemas finales) son dispositivos que están provistos de un adaptador de interfaz de red ATM, por lo general están en las premisas del cliente. Ejemplos de terminadores ATM, como los que aparecen en la figura 2.6 son estaciones de trabajo, enrutadores, *switches* LAN, video CODECs (*coder-decoders*).

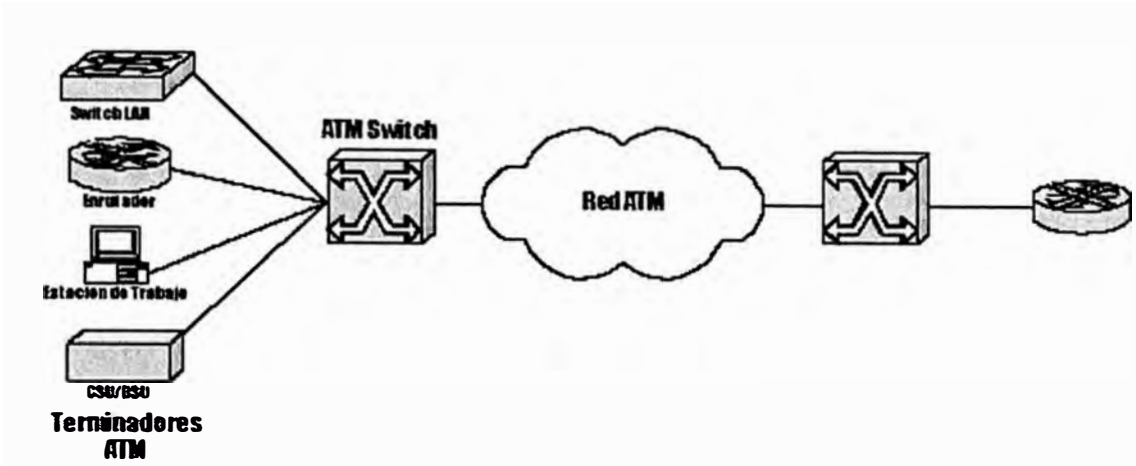


Figura 2.6 Dispositivos que intervienen en una red ATM

En ATM se distingue dos tipos de interfaces: la UNI (*user-network interface*) que se conecta un a terminador con un *switch* ATM y la NNI (*network-node interface*) que conecta dos switches ATM.

e) Formato de una cabecera ATM

Una cabecera de una celda ATM puede tener dos tipos de formatos, dependiendo si se usa en interfaces UNI o NNI. La estructura de cada uno de estos formatos se detalla en la figura 2.7. La diferencia principal radica en que el campo VPI de una cabecera NNI ocupa los primeros 12 bits ya que tiene que manejar un gran numero de identificadores debido a que se usan para comunicación entre *switches* ATM y en una red pueden haber muchos de ellos.

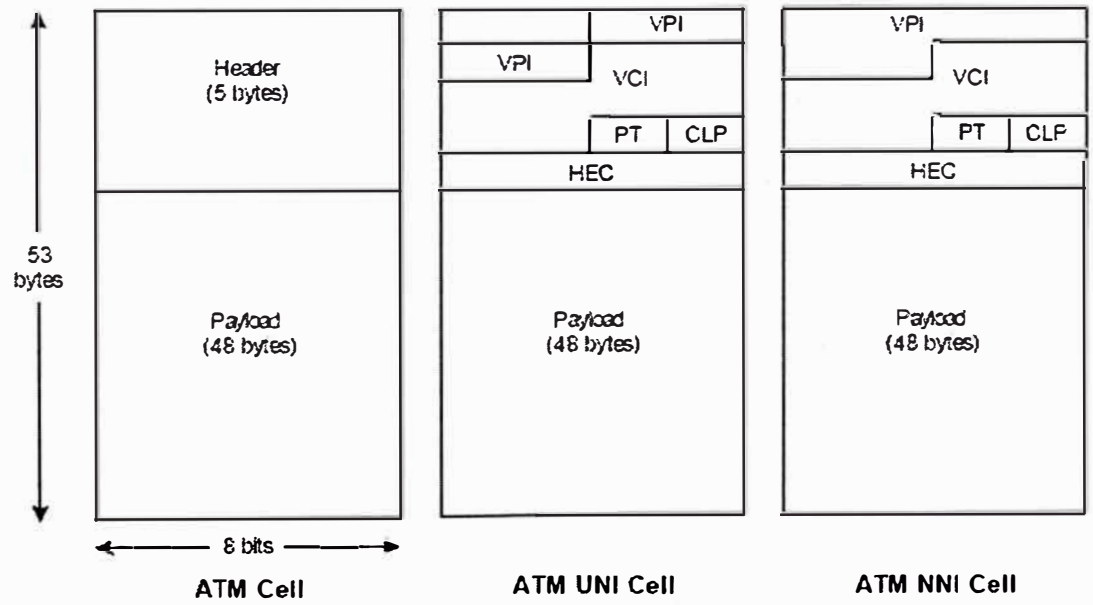


Figura 2.7 Formato de las diferentes cabeceras de una celda ATM. A la izquierda el formato general, en el centro una celda UNI, y a la derecha una celda NNI

- Control de flujo genérico (GFC): Contiene funciones locales, tales como identificadores para múltiples estaciones que usan una misma interfaz ATM compartida. Casi no se usa, y siempre tiene un valor por defecto.
- Identificador de camino virtual (VPI): Conjuntamente con el VCI, identifica el siguiente destino de una celda a través de una red de switches ATM.
- Identificador de canal virtual (VCI): Tiene la misma función que un VPI pero a nivel más bajo. Un VP (*Virtual Path*) es la suma de varios VC (*Virtual Channel*).
- Tipo de carga útil (PT): Indica si la carga útil de la celda contiene información de datos del usuario o de control.
- Prioridad para evitar congestión (CLP): Indica si la celda debe ser descartada o no. Si el bit CLP tiene como valor 1, la celda deberá ser descartada prefiriendo así las celdas con el bit CLP en cero.
- Control de error para la cabecera (HEC): Sirve para realizar *checksum*, pero solamente para la cabecera misma.

f). Conexiones Virtuales ATM

Las redes ATM son básicamente redes orientadas a conexión, esto significa que se tienen que configurar canales virtuales (VC) a través de la red para la adecuada transferencia de datos. Haciendo la analogía con *Frame Relay*, un canal virtual equivale a un circuito virtual.

En ATM existen dos tipos de conexiones: los caminos virtuales (*Virtual Paths* - VPs), los cuales son identificados por medio de VPIs (*Virtual Path - Identifiers*), y los canales virtuales, los cuales son identificados con una combinación de VPIs y de VCIs (*Virtual Channel Identifier*).

Un camino virtual es una suma de canales virtuales, cada uno de los cuales es conmutado transparentemente sobre la red ATM. La figura 2.8 muestra esta relación entre VCs y VPs.

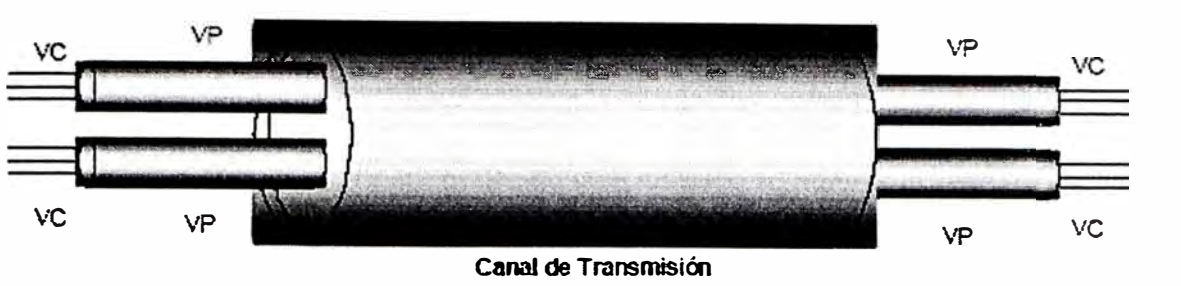


Figura 2.8 Canales Virtuales (VC) dentro de caminos virtuales (VP)

g). Conmutación ATM

La función básica de un *switch* ATM es la de reenviar. Una celda es recibida a través de un enlace con un valor conocido VCI o VPI. El *switch* mira en su tabla local de traslación para determinar el puerto (o puertos) de salida para este tráfico y les coloca un nuevo VPI o VCI, y así se repite este esquema hasta que el tráfico es recibido por el punto terminal ATM. Como se puede ver, cada vez que una celda es retransmitida se le asigna un nuevo VPI o VCI, por esto se dice que estos valores solo tienen significado local y que se pueden reutilizar en otros puntos de la red cuando así se necesite.

2.3 Enlaces Conmutados

Los enlaces conmutados se dividen en dos tipos: los análogos y los digitales. Los primeros llegan hasta tasa de 53 kbits/s para el *downlink* y hasta de 48 kbits/s para el *uplink* (3), los segundos transmiten y reciben a 64 kbits/s o 128 kbits/s. Estos últimos son conocidos como enlaces RDSI (o ISDN, en inglés) que son las siglas de Red Digital de Servicios Integrados.

2.3.1 Enlaces Conmutados Análogos

Fue quizá la primera tecnología de transmisión de datos que usó el hombre para construir redes privadas entre dos sitios remotos. Esto lo hizo aprovechando la Red de Telefonía Pública Conmutada – RTPC (PSTN, en inglés), dicha red ha tenido muchos desarrollos en los últimos 20 años. El servicio tradicional que la RTPC ha prestado ha sido comunicación de voz, y solo recientemente se empezó a usar para soportar un creciente mercado de transferencia de datos.

El rango de frecuencia de la voz humana va desde los 20Hz hasta los 20Khz, pero casi toda la energía espectral se encuentra entre los 300Hz y 3.4Khz, por ende, la ITU ha definido un canal de voz (*speech channel*) para telefonía en esta banda. (4)

Por cuestiones prácticas, y para evitar efectos *aliasing* se maneja el canal desde los 0Hz hasta los 4KHz, dejando unos pocos Hz como bandas de guarda.
La figura 2.9 representa lo dicho anteriormente.

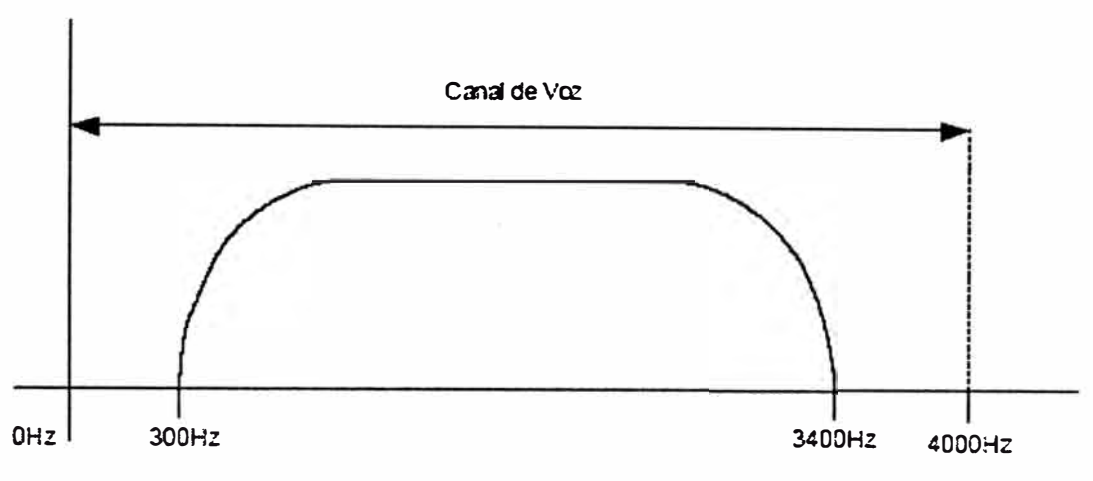


Figura 2.9. Ancho de banda de un canal convencional de voz humana

De este criterio partió todo el desarrollo que se ha hecho sobre las redes de telefonía, todos los equipos fueron diseñados para transmitir señales en este rango. Las investigaciones que se hicieron en el campo de las comunicaciones han demostrado que transportar cualquier señal, incluso la voz, en formato digital tiene inmensas ventajas comparado con una transmisión análoga, de allí que nuestra voz sea convertida en una señal digital en las centrales telefónicas y transportada de la misma manera entre ellas.

Apoyándose en la teoría, el criterio de muestreo de Nyquist (5) dice que para recuperar una señal análoga partiendo de ella misma pero digitalizada, se tiene que muestrear al doble de la frecuencia máxima, es decir que para la voz humana la tasa de muestreo debe ser 8Khz. Si se usan conversores A/D – D/A de 8 bits se necesita un canal de transporte de 64 kbits/s, de allí proviene la tasa básica de transmisión de voz, y que hoy prácticamente ha sido una limitante para las comunicaciones de datos sobre redes telefónicas, que se pensaron inicialmente solo para voz. (6)

En un enlace conmutado de datos, intervienen varios equipos desde el usuario inicial hasta el punto o equipo destino. La figura 2.10 muestra los componentes de un enlace

típico de datos sobre la red telefónica pública, se puede notar la necesidad de realizar una conversión A/D y otra D/A. La inercia que resulta de todo este proceso electrónico es la que en últimas limita a 56 kbits/s[5] una comunicación análoga, que incluso puede llegar a 33.6 kbits/s cuando aparece una tercera y cuarta conversión entre la Central Telefonica 2 y el terminador de la llamada.

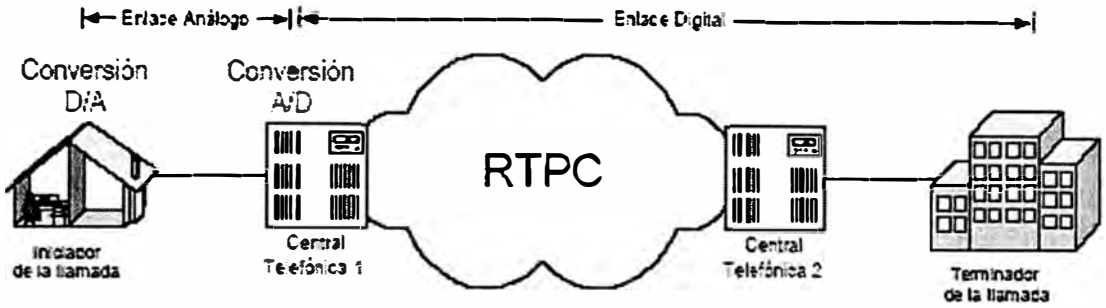


Figura 2.10 Escenario típico de una conexión análoga de datos sobre la RTPC.

Se puede notar que la conexión entre el iniciador de la llamada y la central telefónica es análoga, y se lleva a cabo usando el mismo par de cobre de la línea telefónica, para esto se usa un modem análogo.

Mientras que en el lado del sitio remoto la conexión es digital, y para esto se usan enlaces RDSI PRI o BRI. Por lo general los equipos que intervienen en este lado son servidores de acceso remoto (*Remote Access Server* – RAS). Cuando este enlace es también análogo, entonces se puede notar que en el proceso total de la conexión intervienen cuatro conversiones, dos A/D y dos D/A, esto hace que la tasa de transmisión y de recepción máximas sean apenas de 33.6 kbits/s. La figura 2.11 ilustra este escenario.

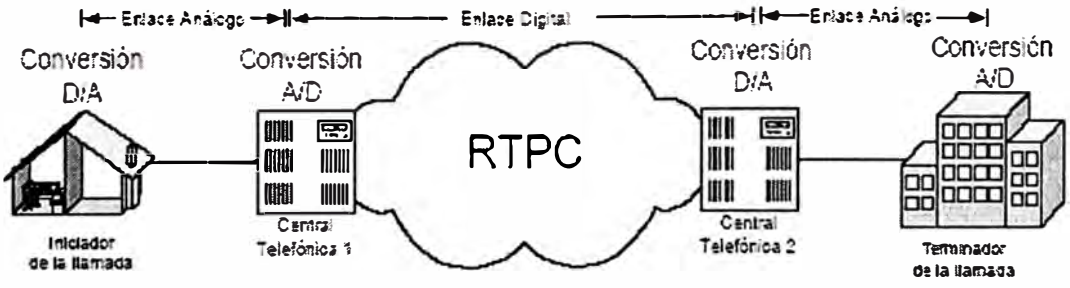


Figura 2.11 Escenario típico de una conexión análoga donde los enlaces de último kilómetro en ambos lados son análogos.

[5] Este valor es teórico, en la práctica no se obtienen tasa superiores de 53 kbits/s para el downstream y de 48 kbits/s para el upstream.

2.3.2 Enlaces Conmutados Digitales – RDSI

RDSI o Red Digital de Servicios Integrados, es un sistema de telefonía digital que se desarrolló hace más de una década. Este sistema permite transmitir voz y datos simultáneamente a nivel global usando 100% conectividad digital.

En RDSI, la voz y los datos son transportados sobre canales B (del inglés *Bearer*) que poseen una velocidad de transmisión de datos de 64 kbits/s, aunque algunos switches ISDN limitan esta capacidad a solo 56 kbits/s. Los canales D (o canales de datos) se usan para señalización y tiene tasa de 16 kbits/s o 64 kbits/s dependiendo del tipo de servicio.

Los dos tipos básicos de servicio RDSI son: BRI (del inglés *Basic Rate Interface*) y PRI (del inglés *Primary Rate Interface*). Un enlace BRI consiste de dos canales B de 64 kbits/s y un canal D de 16 kbits/s para un total de 144 kbits/s. Este servicio está orientado a brindar capacidad de conexión para usuarios residenciales.

Un enlace PRI está orientado a usuarios que requieren un mayor ancho de banda. En Estados Unidos la estructura básica de canales es 23 canales B y 1 canal D, todos de 64 kbits/s, para un total de 1536 kbits/s. En Colombia donde se ha adoptado el estándar internacional de la ITU-T, y que además es el estándar ETSI europeo, un PRI consiste de 30 canales B y 2 canales D, todos de 64 kbits/s, para un total de 2048 kbits/s.

Para accesar a un servicio BRI, es necesario tener una línea RDSI. Si solo se desean comunicaciones de voz es necesario tener teléfonos digitales RDSI, y para transmitir datos es necesario contar con un adaptador de Terminal – TA (del inglés *Terminal Adapter*) o un enrutador RDSI. La norma RDSI trabaja con interfaces BRI S/T, a diferencia de la americana que entrega en las premisas del usuario en interfaz BRI U. La figura 2.12 ilustra los diferentes tipos de interfaz y equipos terminales RDSI.

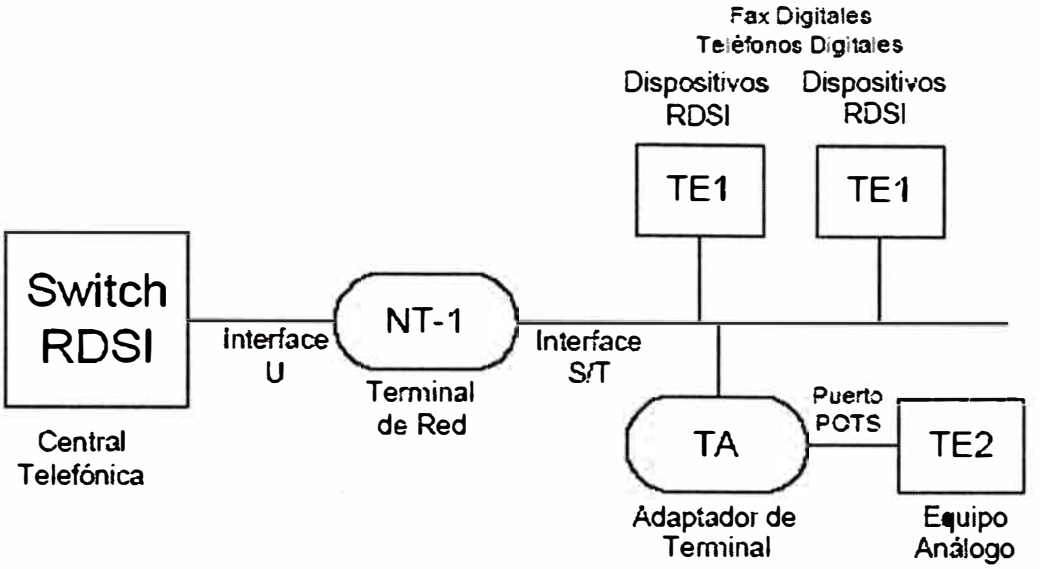


Figura 2.12 Diagrama de Interfaces y equipos en una conexión RDSI BRI.

A diferencia de las conexiones conmutadas análogas en una conexión RDSI el camino es 100% digital desde la central hasta el sitio del abonado, por lo cual no existe ningún tipo de conversiones A/D o viceversa, lo que facilita la obtención de tasa de 64 kbits/s o 128 kbits/s, lo cual se logra convirtiendo los dos canales B de 64 kbits/s o en un canal lógico de 128 kbits/s. Esta característica es usada solo en transmisión de datos y depende de la facilidad que tenga el equipo terminal de realizar esto. Típicamente esta característica tiene el nombre de Multilink.

CAPITULO III
REDES PRIVADAS VIRTUALES

3.1 Descripción de la tecnología

La tecnología de redes es desde hace años base importante para la comunicación dentro de las empresas, sin embargo, las empresas pueden contar con oficinas remotas las cuales tiene la misma necesidad de información que sus oficinas locales para trabajar como si estuvieran situadas en un mismo lugar geográfico. Una respuesta a esta necesidad es interconectar los nodos remotos mediante líneas dedicadas o mediante accesos con líneas de telefonía, lo cual es una solución costosa ya sea por el equipo necesario para la conexión o por el costo de las llamadas para el acceso telefónico.

Una solución mas novedosa es la implementación de Redes Privadas Virtuales, que además de resultar relativamente menos costosas proveen una comunicación segura y están siendo ampliamente utilizadas especialmente por su flexibilidad para establecer comunicaciones globales.

Una Red Privada Virtual, también conocida como VPN *(Virtual Private Network)*, es una solución específica de red que conecta a usuarios remotos a su red privada por medio de una infraestructura pública, de manera segura proporcionando iguales beneficios y recursos que una red de área local típica. Constituye una asociación lógica de líneas y terminales que pertenecen a un usuario particular e incluye proporciones de red que no son dedicados a dicho usuario.

En otras palabras, las Redes Privadas Virtuales permiten a los usuarios que trabajan en casa o a los usuarios móviles conectarse de modo seguro a un servidor corporativo remoto utilizando la infraestructura de routing provista por una red pública.

Desde el punto de vista del usuario, la red privada virtual es una conexión punto a punto entre el PC del usuario y un servidor corporativo. La naturaleza de la red intermedia es irrelevante para el usuario porque para él es como si los datos fuesen enviados sobre un enlace privado dedicado.

La tecnología VPN también permite a una corporación conectarse a oficinas filiales o a otras empresas a través de una red pública (como Internet), a la vez que mantiene las comunicaciones seguras. La conexión VPN a través de Internet opera lógicamente como una Red de Área Extensa (WAN) entre las sedes. En ambos casos, la conexión segura a través de la red intermedia tiene el aspecto para el usuario de una comunicación de red privada, a pesar de que dicha comunicación ocurra sobre una red pública; de ahí el nombre de Red Privada Virtual.

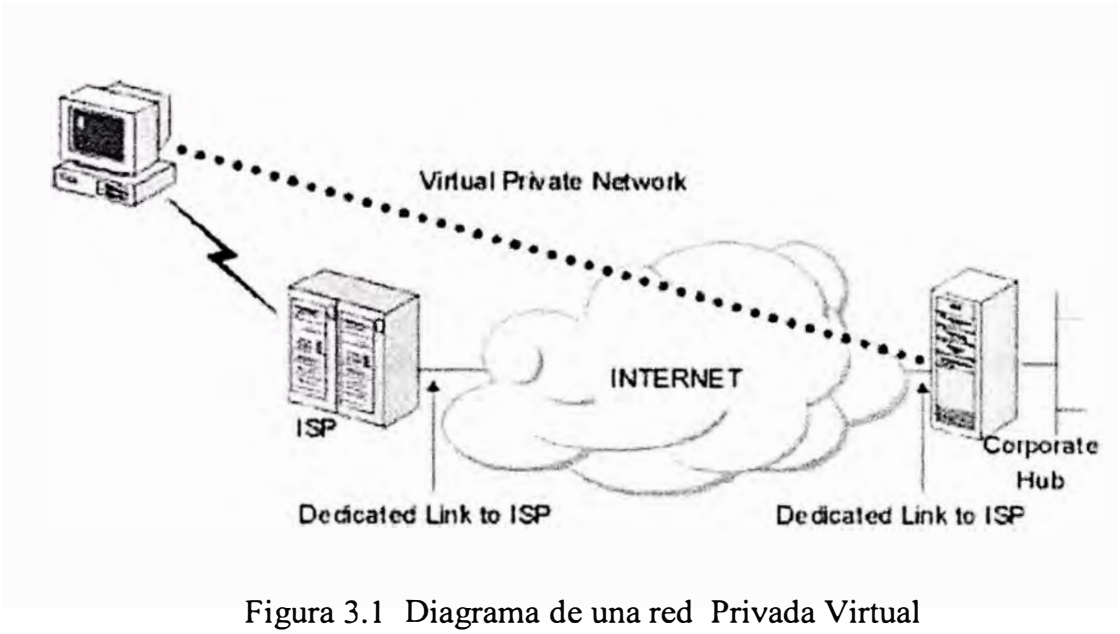


Figura 3.1 Diagrama de una red Privada Virtual

Las redes privadas virtuales surgen como una alternativa a los servicios de comunicaciones tradicionales de red amplia (WAN) de enlaces dedicados.

Este tipo de comunicaciones presentan múltiples ventajas y beneficios para los usuarios:

Bajo costo. Reduce el coste del servicio de comunicación o del ancho de banda de transporte, y también el de la infraestructura y operación de las comunicaciones.

Flexibilidad. Se puede optar por múltiples tecnologías o proveedores de servicio. Esa independencia posibilita que la red se adapte a los requerimientos de los negocios, y se pueda elegir el medio de acceso más adecuado. Por ejemplo, si se trata de una pequeña oficina remota, se puede utilizar acceso discado, ISDN, xDSL o cable módem.

Escalabilidad. El desarrollo masivo de redes como Internet permite que la empresa tenga puntos de presencia en todo tipo de lugares. Por otro lado, la independencia con respecto a la tecnología de acceso posibilita escalar el ancho de banda de la red de acuerdo con los requerimientos del usuario. Además, la escalabilidad de la red no incide en la operatoria y

gestión de ésta, dado que la infraestructura de la WAN es responsabilidad del proveedor del servicio.

Internet.

Pero recientemente, con el auge que ha tenido Internet, por el cada vez menor costo que la gente tiene que pagar para acceder a esta gran red y con el significado que esta ha adquirido como el principal medio mundial de comunicación, las redes privadas virtuales han hecho su aparición con más fuerza que nunca y se han ganado un espacio dentro del tan cambiante mundo de las redes de información. (7)

Las VPN utilizan, generalmente, Internet como su medio de transporte. Es un medio propicio tanto para clientes comerciales como privados. La conductividad de Internet es extremadamente eficiente en el mercado actual. La tecnología base de las VPN es el conjunto de protocolos TCP/IP de Internet, lo que la hace más fácil de comprender e implementar.

Una VPN es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado pero trabaja sobre una red pública. Para este propósito usa una técnica llamada entunelamiento (*tunneling*), los paquetes de datos son enrutados por la red pública, tal como Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura. También hace universales para su transporte los diferentes protocolos LAN entre los que se encuentran IP, IPX, Appletalk y Netbeui, de allí la característica de multiprotocolo que hace sumamente universal la tecnología de las redes virtuales privadas. La figura 3.2 muestra los distintos escenarios que se pueden manejar con la tecnología de Redes Privadas Virtuales (Dial-Up, Intranet VPN y Extranet VPN). (8)

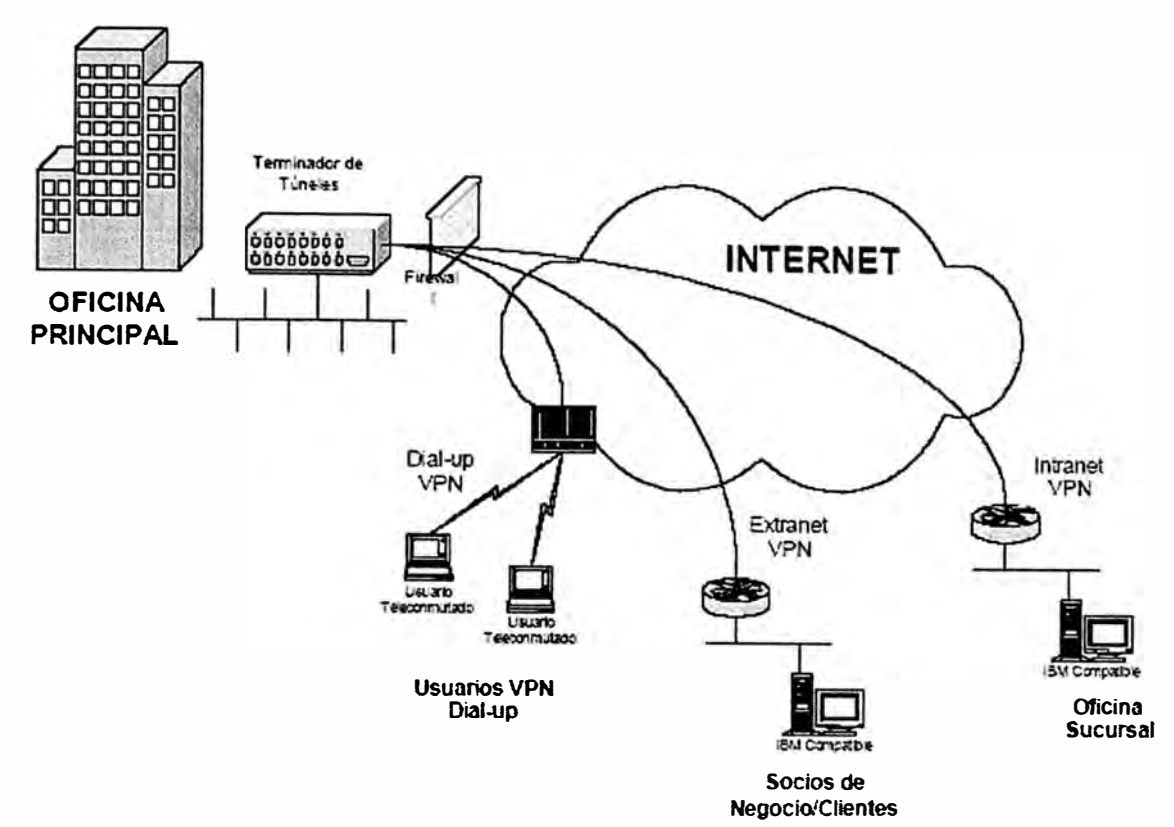


Figura 3.2 Distintas maneras de crear una VPN

Las técnicas de entunelamiento consiste en encapsular los paquetes de datos que salen de una LAN o del equipo del usuario remoto dentro de protocolos que trabajan a Nivel 2 de la torre OSI.

Los componentes básicos de un túnel, y que se muestran en la figura 3.3. son:

- Un iniciador del túnel
- Uno o varios dispositivos de enrutamiento
- Un conmutador de túneles (opcional)
- Uno o varios terminadores de túneles

El inicio y término del túnel pueden ser hechos por una amplia variedad de equipos o software. Un túnel puede ser empezado, por ejemplo, por un usuario remoto con un computador portátil equipado con un modem análogo y un software de conexión telefónica para hacer una VPN, también puede haber un enrutador de una extranet en una oficina remota o en una LAN pequeña. Un túnel puede ser terminado por otro enrutador habilitado para tal fin, por un switch con esta característica o por un software que haga tal fin.

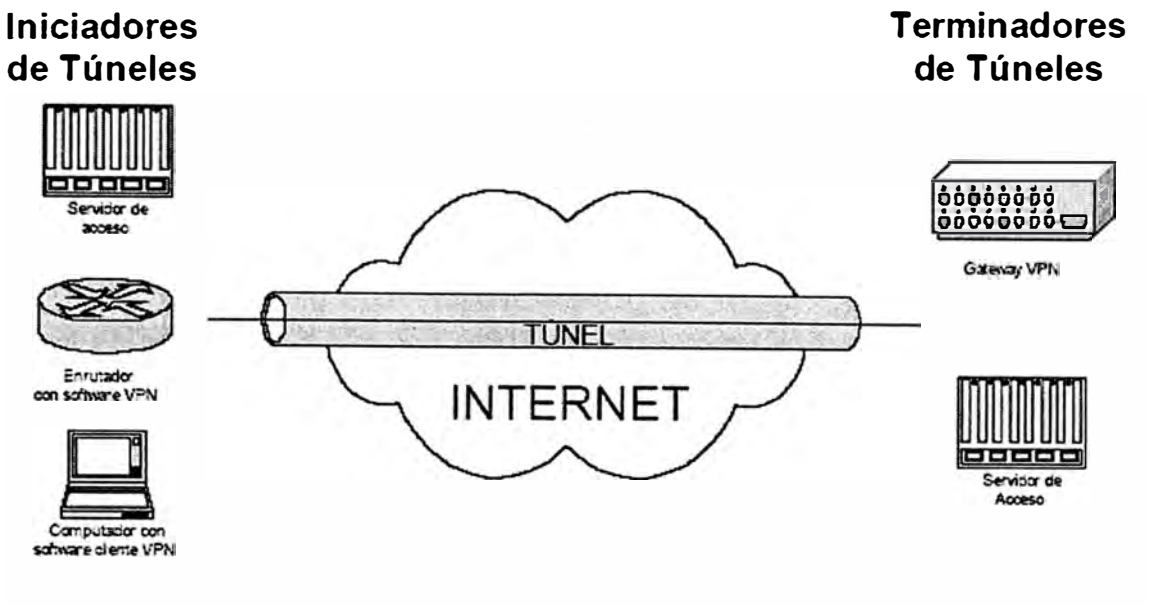


Figura 3.3 Elementos básicos de un túnel VPN

3.2 Requerimientos Básicos de una VPN

Una Red Privada Virtual ha de proveer de los siguientes mecanismos básicos.

- Autentificación de usuarios, verificar la identidad de los usuarios, para poder restringir el acceso a la VPN solo a los usuarios autorizados.
- Administración de direcciones, debe asignar una dirección del cliente sobre la red privada, y asegurar que las direcciones privadas se mantienen privadas.
- Encriptación de datos, los datos que viajan por la red publica, deben ser transformados para que sean ilegibles para los usuarios no autorizados.
- Administración de claves, debe mantener un mantenimiento de claves de encriptación para los clientes y los servidores.
- Soporte multiprotocolo, ha de ser capaz de manejar protocolos comunes, usando las red publica, por ejemplo IPX, IP, etc.
- Tunneling, Como mecanismo de intercambio de información

3.3 Como funciona, encriptación y rendimiento en una VPN

La tecnología de VPN se centra en el medio que hay entre las redes privadas y las redes públicas. El dispositivo intermediario, ya sea orientado a software, orientado a hardware o la combinación de ambos, actúa como una red privada como a la que protege. Cuando un *host* local manda un paquete a una red remota, primero los datos pasan de la red privada por el *gateway* protegido, viajando a través de la red publica, y entonces los datos pasan por el *gateway* que esta protegiendo el host destino de la red remota. Una VPN protege los

datos encriptandolos automáticamente antes de enviarlos de una red privada a otra, encapsulando los datos dentro de un paquete IP.

Cuando estos llegan al destino, los datos son desencriptados. El proceso es el siguiente:

1- Un ordenador cliente llama a un ISP local y conecta a Internet.
2- Un software especial cliente reconoce un destino especificado y negocia una sesión de VPN encriptada
3- Los paquetes encriptados son envueltos en paquetes IP para crear el túnel y mandarlos a través de Internet.
4- El servidor de VPN negocia la sesión de VPN y desencripta los paquetes.
5- El tráfico no encriptado fluye a otros servidores y recursos con normalidad.

El fuerte de los componentes en VPN es la encriptación. El objetivo es restringir el acceso a los usuarios y *hosts* apropiados, y asegurar que los datos transmitidos por Internet sean encriptados para que solo estos usuarios y los hosts sean capaces de ver los datos. La técnica usada es envolver los datos de carga encriptados, con cabeceras que puedes ser leídas. Esto es lo que se llama Túnel. Una vez conectado, una VPN abre un Túnel seguro, en el cual el contenido será encapsulado y encriptado y los usuarios son autentificados.

Todos estos mecanismos empleados, aumenta la seguridad en el intercambio de datos pero no añade una reducción en el rendimiento de la comunicación por las sobrecargas. Muchas VPN, ya sean basadas en hardware o en software, deberían ser capaces de procesar la encriptación en conexiones hasta al menos una velocidad de 10BaseT.

A tasa superiores, el consumo de CPU necesaria en las VPN basadas en software es tan elevada que el rendimiento decrece. En los sistema orientados a hardware, que usan maquinas dedicadas, estas tasa aumentan. En conexiones como módems, el procesamiento en las VPN es mucho mas rápido que los retardos introducidos por el ancho de banda disponible. Las perdidas de paquetes y la demora en conexiones a Internet de baja calidad afecta mas al rendimiento, que a la carga añadida por la encriptación.

3.4 Que es Tunneling

Tunneling es una técnica que usa una infraestructura entre redes para transferir datos de una red a otra. Los datos o la carga pueden ser transferidas como tramas de otro protocolo. El protocolo de *tunneling* encapsula las tramas con una cabecera adicional, en vez de enviarla como la produjo en el nodo original. La cabecera adicional proporciona información de *routing* para hacer capaz a la carga de atravesar la red intermedia. Las

tramas encapsuladas son enrutadas a través de un túnel que tiene como puntos finales los dos puntos entre la red intermedia. El túnel en una camino lógico a través del cual se encapsulan paquetes que viajan entre la red intermedia.

Cuando un trama encapsulada llega a su destino en la red intermedia, se desencapsula y se envía a su destino final dentro de la red. *Tunneling* incluye todo el proceso de encapsulado, desencapsulado transmisión de las tramas.

Las tecnologías de *Tunneling* son:

- DLSW- Data Link Switching
- IPX for Novell Netware over IP
- GRE – Generic Routing Encapsulation
- ATMP – Ascend Tunnel Management Protocol
- Mobile IP – For mobile users
- IPSec – Internet Protocol Security Tunnel Mode
- PPTP - Point-to-Point Tunneling Protocol
- L2F – Layer 2 Forwarding
- L2TP – Layer 2 Tunneling Protocol

3.5 Que es el PPTP *(Point to Point Tunneling Protocol)*

El protocolo fue originalmente designado como un mecanismo de encapsulamiento, para permitir el transporte de protocolos diferentes del TCP/IP, como por ejemplo IPX sobre la red Internet. La especificación es bastante genérica, y permite una variedad de mecanismos de autentificación y algoritmos de encriptación.

El Protocolo de Túnel Punto-a-Punto (*Point to Point Tunneling Protocol*) es un protocolo que permite establecer conexiones con túneles PPP, a través de una red IP, creando una VPN. La compañía Microsoft, ha implementado sus propios algoritmos y protocolos con soporte PPTP, el Microsoft PPTP, y este es uno de los mas ampliamente extendidos, por la popularidad de los productos Microsft (Windows 98/ME, NT4, 2000) los cuales llevan incluidos de serie estos protocolos.

Fue desarrollado por el Forum PPTP que esta constituido por la siguientes organizaciones: Ascend Communications, Microsoft Corporation, 3 Com/Primary Access, ECI Telematics, and U.S. Robotics.

3.5.1 PPTP and VPN

Generalmente hay tres ordenadores involucrados en el uso del PPTP. Hay un cliente PPTP, un servidor de acceso a la red y un servidor de PPTP. En el caso de una LAN, el

servidor de acceso a la red no es necesario, porque ya esta en la misma red. La comunicación segura creada usando el protocolo PPTP conlleva tres fases, cada una de los cuales requiere la finalización correcta de las anteriores. Estas son: PPP conexión y comunicación, PPTP control de conexión, PPTP data tunneling.

3.5.2 PPP conexión y comunicación

Primero el cliente necesita una conexión a Internet, conectando con un Servidor de Acceso a Red (NAS *Network Access Server*) vía un Proveedor de Servicios de Internet (ISP). Un cliente PPTP usa el PPP para establecer esta conexión. La conexión requerida por un cliente consiste en unas credenciales de acceso (usuario, password) y un protocolo de autentificación para que el servidor de PPTP pueda autentificar al cliente. Una vez conectado el cliente puede enviar y recibir paquetes sobre Internet.

3.5.3 PPTP control de conexión

Cuando el cliente tiene establecida la conexión PPP con el ISP, se realiza un segundo establecimiento de llamada, sobre la conexión PPP existente. Esto crea la conexión VPN (conexión de control) a un servidor PPTP de una LAN privada a una empresa y actúa como un túnel a través de la cual fluyen los paquetes de red. Un set de ocho mensajes de control establecerán, mantendrán y finalizaran el túnel PPTP. Los mensajes son los siguientes:

- PPTP_START_SESSION_REQUEST Starts Session
- PPTP_START_SESSION_REPLY Replies to Start Session Request
- PPTP_ECHO_REQUEST Maintains Session
- PPTP_ECHO_REPLY Replies to Maintain Session Request
- PPTP_WAN_ERROR_NOTIFY Reports an error in the PPP connection
- PPTP_SET_LINK_INFO Configures PPTP Client/Server Connection
- PPTP_STOP_SESSION_REQUEST Ends Session
- PPTP_STOP_SESSION_REPLY Replies to End Session Request
- PPTP Data Tunneling

Después de establecer el túnel PPTP, los datos son transmitidos entre el cliente y el servidor PPTP. Los datos son enviados en formato de datagramas IP que contienen paquetes PPP, a los que referimos normalmente como paquetes PPP encapsulados.

Los datagramas IP contienen paquetes IPX, NetBEUI, o TCP/IP y tiene el siguiente formato:

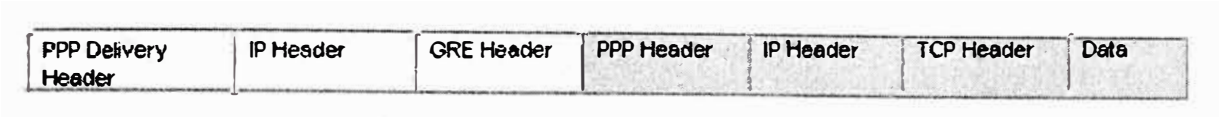


Figura 3.4 Datagrama IP conteniendo paquetes encriptados PPP creados por PPTP

La cabecera IP de entrega proporciona la información necesaria para que el datagrama atraviese la red Internet. La cabecera GRE se usa para encapsular el paquete PPP dentro de un datagrama IP. La zona ensombrecida representa los datos encriptados.

Después de que la conexión VPN esta establecida, el usuario remoto (cliente) puede realizar cualquier operación como si fuera un usuario local.

3.5.4 La seguridad en PPTP

Una de las características de este protocolo es la característica disponibles de seguridad. Hay tres áreas en la seguridad PPTP que lo hace más atrayente. Son la autentificación, encriptación de datos y filtrado de paquetes PPTP.

a). Autentificación

La autentificación de un cliente PPTP remoto se hacen de la misma manera que la autentificación PPP usado por cualquier cliente RAS (*Remote Access Service*). Las cuentas de usuarios son configuradas para que solo los usuarios específicos tengan acceso a la red a través del dominio de confianza. El uso de passwords seguras es uno de las mejores formas de utilización exitosa del PPTP.

b). Encriptación de Datos

Los datos enviados por el túnel PPTP en los dos sentidos son encriptados. Los paquetes de red son encriptados en la fuente (cliente o servidor), viajan a través del túnel, y son desencriptados en el destino. Como todos los datos en una conexión PPTP fluyen dentro del túnel, los datos son invisibles al resto del mundo. La encriptación de datos dentro del túnel da un nivel adicional de seguridad.

c). Filtrado de Paquetes PPTP

Esta opción incrementa el rendimiento y fiabilidad de la seguridad de red si está activada en el servidor PPTP. Cuando está activa acepta sólo los paquetes PPTP de los usuarios autorizados. Esto prevé que el resto de paquetes entren en la red privada y en el servidor de PPTP.

3.6 L2TP, Layer 2 Tunneling Protocol

El protocolo de túneles L2TP, ha nacido de la combinación de las características del protocolo PPTP y L2F (*Layer 2 Forwarding*). L2TP es un protocolo de red que facilita la creación de túneles para enviar tramas PPP. Encapsula las tramas PPP para que puedan ser enviadas sobre redes IP, X.25, *Frame Relay* o ATM. La carga útil de las tramas PPP, puede ser encriptada y/o comprimida. Se puede usar L2TP directamente sobre diferentes tipos de WAN, por ejemplo, *Frame Relay*, sin una capa de transporte IP. L2TP usa UDP y una serie de mensajes de L2TP para los mantenimientos de túneles sobre redes IP. L2TP permite múltiples túneles entre los dos puntos finales.

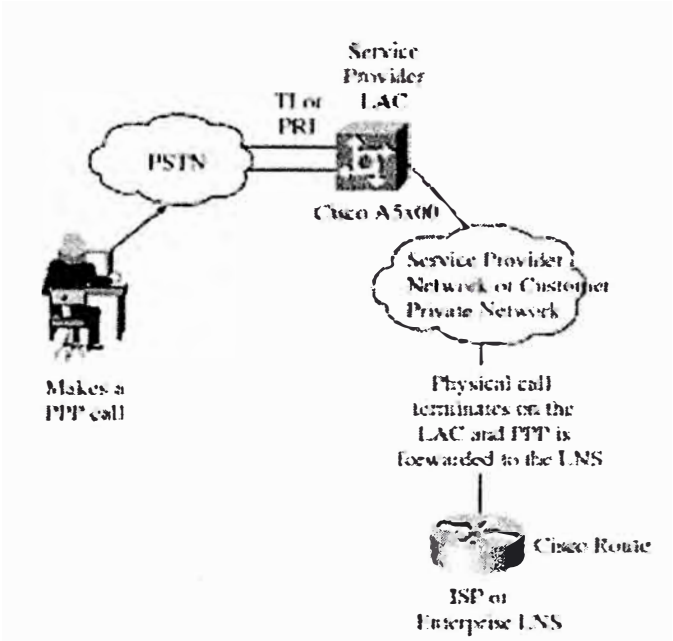


Figura 3.5 trafico utilizando protocolo L2TP

3.7 Que es IPSec

IPSec es un protocolo de seguridad para Internet. IPSec proporciona confidencialidad y/o integridad de los paquetes IP. Los paquetes normales de IPv4 están compuestos de una cabecera y carga, y ambas partes contienen información útil para el atacante. La cabecera contiene la dirección IP, la cual es utilizada para el routing, y puede ser aprehendida para ser usada mas tarde con técnicas de *spoofing*[1]. La parte de la carga esta compuesta de la información que se supone confidencial para una empresa o una organización. Ni que decir tiene, que esta información es la más valiosa. IPSEC proporciona seguridad mediante dos protocolos ESP, *Encapsulating Security Payload*, o AH, *Authentication Header*.

[1] Por **spoofing** se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada

Básicamente ESP cifra los datos y los autentica, mientras que AH sólo los autentifica. La diferencia entre ESP sólo autenticando y AH es que AH autentica también la cabecera IP del paquete. AH, firma digitalmente el paquete, verificando la identidad del emisor y del receptor del paquete. La manera en que se autentican los paquetes es mediante funciones HMAC (funciones HASH con clave), mientras que la manera de proporcionar confidencialidad es cifrando los paquetes con uno de los algoritmos de cifrado definidos.

IPSec es una buena solución para mantener la confidencialidad de los datos. Ofrece una comunicación segura host a host. Tiene dos modos de funcionamiento, modo transporte y modo túnel. En el modo transporte la encriptación se realiza extremo a extremo, del host origen al host destino, por lo tanto todos los hosts han de tener IPSec. En el modo túnel el encriptado se efectúa únicamente entre lo enrutadores de acceso a los hosts implicados. Con el modo túnel la encriptación se integra de manera elegante, los mismos dispositivos que se encargan que crean los túneles se encargan de integrar el encriptamiento.

La figura 3.6 muestra un diagrama más detallado de una VPN *dial-up* usando como protocolo de entunelamiento a PPTP. Se notan los trayectos en los cuales el protocolo que encapsula los datos es PPP y la parte del recorrido que es tunelizada usando PPTP.

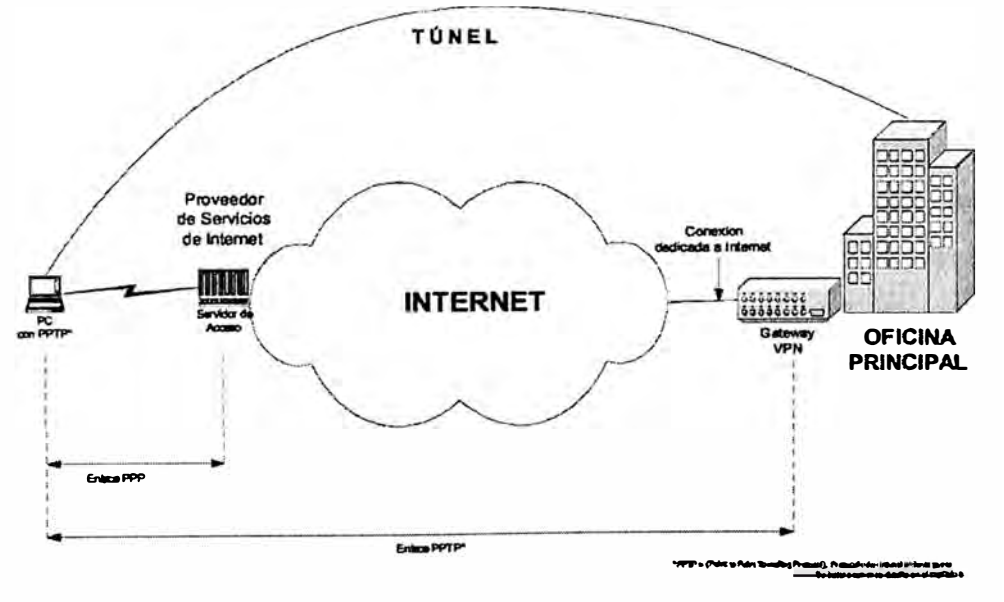


Figura 3.6 Una topología más compleja y detallada de una VPN

En muchos casos las características que le permiten a los dispositivos ser iniciadores o terminadores del túnel se pueden adicionar con una simple actualización del sistema operativo o de sus tarjetas.

Una buena solución VPN requiere la combinación de tres componentes tecnológicos críticos: seguridad, control de tráfico y manejo empresarial.

Seguridad: Dentro de este punto se destacan: el control de acceso para garantizar la seguridad de las conexiones de la red, el cifrado para proteger la privacidad de los datos y la autenticación para poder verificar acertadamente tanto la identidad de los usuarios como la integridad misma de la información.

Control de tráfico: el segundo componente crítico en la implementación de una efectiva VPN es el control de tráfico que garantice solidez, calidad del servicio y un desempeño veloz. Las comunicaciones en Internet pueden llegar a ser excesivamente lentas, lo que las convertirían en soluciones inadecuadas en aplicaciones de negocios donde la rapidez es casi un imperativo. Aquí es donde entra a jugar parámetros como la prioridad de los datos y la garantización de ancho de banda.

Manejo empresarial: El componente final crítico en una VPN es el manejo empresarial que esta tenga. Esto se mide en una adecuada integración con la política de seguridad de la empresa, un manejo centralizado desde el punto inicial hasta el final, y la escalabilidad de la tecnología.

Las VPNs se caracterizan también por su flexibilidad. Pueden ser conexiones punto-punto o punto-multipunto. Reemplazando una red privada con muchos y costosos enlaces dedicados, por un solo enlace a una ISP que brinde un punto de presencia en la red (POP por sus siglas en inglés), una compañía puede tener fácilmente toda una infraestructura de acceso remoto, sin la necesidad de tener una gran cantidad de líneas telefónicas análogas o digitales, y de tener costosos pools de módems o servidores de acceso, o de pagar costosas facturas por llamadas de larga distancia. En algunos casos las ISP se hacen cargo del costo que les genera a los usuarios remotos su conexión a Internet local, pues ven en este tipo de negocio un mayor interés por los dividendos del acceso.

El objetivo final de una VPN es brindarle una conexión al usuario remoto como si este estuviera disfrutando directamente de su red privada y de los beneficios y servicios que dentro de ella dispone, aunque esta conexión se realice sobre una infraestructura pública.

3.8 Características de las VPNs

Características que deben garantizar todas las VPN:

- **Confidencialidad**: previene que los datos que viajan por la red sean leídos correctamente.
- **Integridad**: asegura que los datos de origen corresponden a los de destino.
- **Autentificación**: asegura que quien solicita la información exista.

- **Control de acceso**: restringe el acceso a usuarios no autorizados que quieran infiltrarse en la red.

Estas características son ofrecidas gracias a tecnologías y protocolos de seguridad y encriptación que proporcionan seguridad en la transmisión de los datos independientemente de las redes involucradas y de sus medidas de seguridad:

- La privacidad de los datos debe ser garantizada mediante la encriptación de los mismos. La encriptación usa complejas transformaciones matemáticas en la cual los datos se combinan con una llave lógica y luego son desencriptados por la persona que los recibe usando la misma clave. Administrar estas claves es el aspecto más crucial para la encriptación, cualquier solución de VPDN deberá poseer un mecanismo de negociación de llaves dinámicas.
- Aplicar transformaciones matemáticas en los datos para crear una marca digital y evitar que no sea alterada ni modificada en el transporte.
- La autenticación de los usuarios evita que un usuario pueda ser confundido por algún otro y de esta manera le otorgue privilegios sobre la red que no le corresponden. La habilidad de realizar una Autenticación positiva de un usuario es vital para la seguridad de las VPDN. La protección mediante password es fácilmente violable y por lo tanto insegura.

3.9 Tipos de VPN

Las VPN se dividen en cuatro categorías de acuerdo con el servicio de conectividad que proporcionen:

3.9.1. Intranet.

Una VPN de intranet se crea entre la oficina central y oficinas independientes. Vincula la oficina remota o sucursal a la red corporativa, a través de una red pública, mediante enlace dedicado al proveedor de servicio. La VPN goza de las mismas cualidades que la red privada: seguridad, calidad de servicio y disponibilidad, entre otras características:

- Extiende el modelo IP a través de la WAN compartida.

3.9.2. Acceso remoto.

(*Remote Access* VPNs). Provee acceso remoto a la intranet o extranet corporativa a través de una infraestructura pública, conservando las mismas políticas, como seguridad y calidad de servicio, que en la red privada. Permite el uso de múltiples tecnologías como discado, ISDN, xDSL, cable o IP para la conexión segura de usuarios móviles, *telecommuters* o sucursales remotas a los recursos corporativos.

Características:

- *Outsourcing* de acceso remoto
- Llamadas locales o gratuitas (0800)
- Ubicuidad del acceso
- Instalación y soporte del PS (Proveedor de servicio)
- Acceso único al nodo central (elimina la competencia por puertos)
- Tecnologías de acceso RTC, ISDN, Xdsl
- Movilidad IP

3.9.3. Extranet.

Permite la conexión de clientes, proveedores, distribuidores o demás comunidades de interés a la intranet corporativa a través de una red pública.

Características:

- Extiende la conectividad a proveedores y clientes:
- Sobre una infraestructura compartida.
- Usando conexiones virtuales dedicadas.

3.9.4. VPN interna.

Diversos estudios demuestran que la mayoría de los ataques son lanzados por los empleados internos de la empresa. Con una VPN interna, es posible que dentro de los límites de la empresa se pueda crear un túnel, de modo que todo el tráfico que una compañía considere crítico puede pasar por un cable cifrado y almacenarse de manera segura sin que sea manipulado indebidamente.

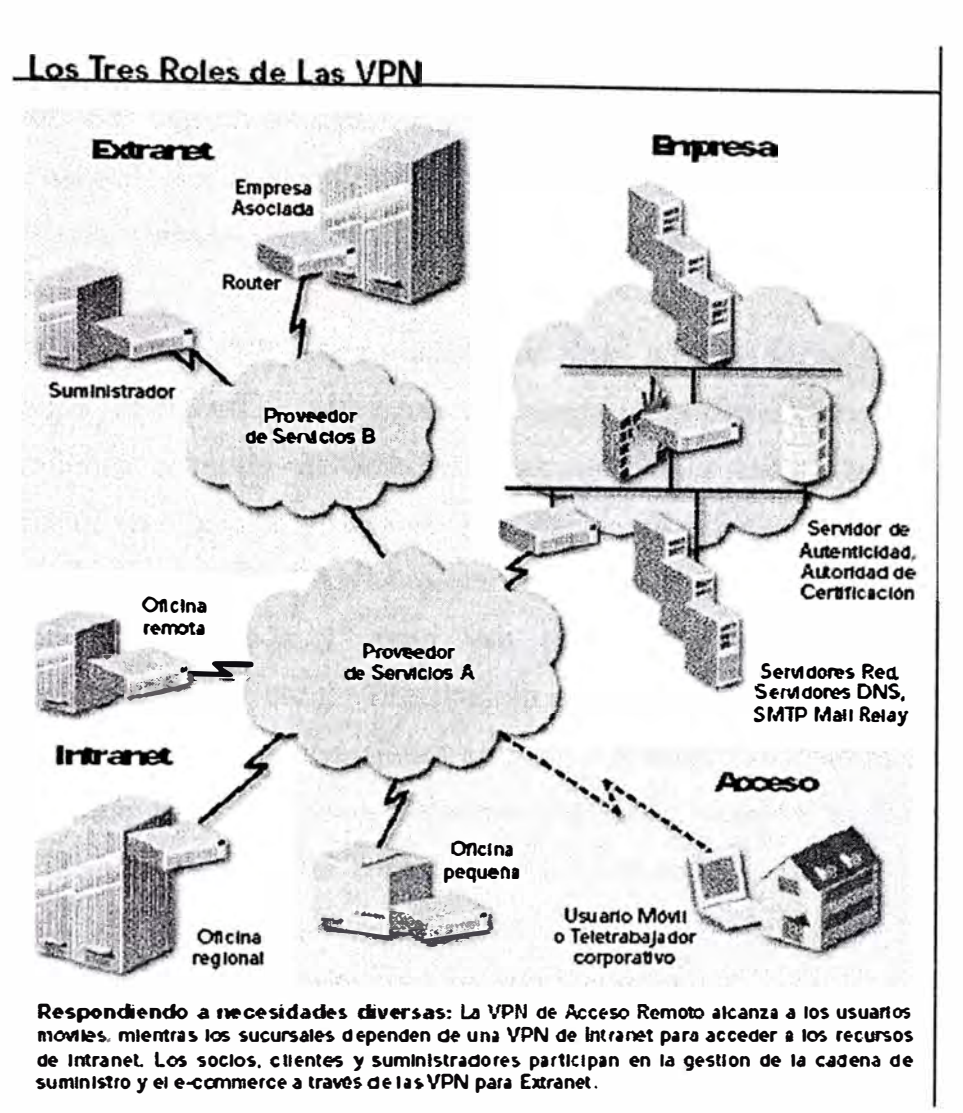


Figura 3.7 Tipos de VPN

3.10 Ventajas de las Redes Privadas Virtuales

La principal ventaja de usar una VPN es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de un terminal en esa red privada, pudiendo acceder a la información publicada para esa red privada: bases de datos, documentos internos, etc. a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a Internet desde el ordenador cliente VPN se realizarán usando los recursos y conexiones que tenga la red privada.

Reducen los costos frente a otras soluciones de conectividad como arriendo de líneas dedicadas u otros. Las VPN tienen un funcionamiento similar al de las redes tipo WAN pero su coste es muchísimo inferior ya que utiliza la red de Internet para comunicarse entre

si, permitiendo de esta manera tener comunicaciones rápidas y seguras entre sus oficinas o desde cualquier lugar exterior de ellas.

- La conexión WAN es posiblemente la solución más estable y segura para una red de cualquier tamaño. Las conexiones son totalmente privadas y usan tecnología estándar.
- La solidez de una VPN no es estable. Las redes privadas virtuales son una nueva tecnología, ejecutándose sobre una tecnología poco fiable (Internet). Realizando transacciones a través de Internet, comunicaciones entre varias plataformas, procesos de encriptación y similares se consigue un sistema menos fiable que en el caso de una conexión WAN. Sin embargo, el mundo se mueve más hacia una sociedad interconectada y como van apareciendo nuevos estándares reales (protocolos, hardware, etc.), VPNs tendrán una base estable sobre la que operar.
- No requiere de grandes inversiones en infraestructura. Los enlaces punto a punto implican que la organización debe realizar una cuantiosa inversión inicial en equipamiento para conectar cada una de las sucursales u oficina que posea. Sin embargo, con las VPN tanto la inversión inicial como las tareas de instalación, operación y mantenimiento son mucho más pequeñas.
- Extiende la conectividad geográfica. Una VPN conecta a empleados remotos a los recursos centrales.
- Crecimiento en productividad de empleados. Una solución VPN permite a los empleados remotos aumentar su productividad en un rango de 22% - 45% (Gallup Organization and Opinion Research) eliminando tiempo.
- Mejora la seguridad de Internet. Siempre en una conexión de banda ancha a Internet, hace a una red vulnerable a ataques de hacker´s. Muchas soluciones de VPN incluyen medidas de seguridad adicional, tales como dispositivos de seguridad ("firewall") y antivirus de chequeo para contrarrestar los diferentes tipos de amenazas a la seguridad de la red.
- Fácilmente escalable. Una VPN permite a las compañías utilizar la infraestructura de los accesos remotos dentro de los ISP´s. Por lo tanto, las compañías pueden agregar virtualmente una cantidad ilimitada de capacidad sin añadir infraestructura que sea significativa.
- Simplifica la topología de la Red. La eliminación de módems y una infraestructura de red privada, simplifica la administración de la red.

CAPITULO IV
INTRODUCCION MPLS

MPLS es un trabajo realizado y especificado por la *Internet Engineering Task Force* (IETF) que da los parámetros para la eficiente designación, ruteo, envío y conmutación de tráfico que fluye por la red. (9)

MPLS realiza las siguientes funciones:

- Especifica mecanismos para manejar flujos de tráfico de varias granularidades, como flujos entre diferente hardware, maquinas, o incluso flujos entre diferentes aplicaciones.
- Permanece independiente de los protocolos de capa 2 y de capa 3.
- Provee de medios para mapear direcciones IP, en etiquetas de longitud fija que son usadas por diferentes técnicas de envío y conmutación de paquetes.
- Tiene interfaces con protocolos de ruteo existentes como el Resource ReSerVation *Protocol (RSVP) y el Open Shortest Path First (OSPF).*
- Soporta protocolos de capa 2: IP, ATM, y frame-relay.

Se le llama "Multiprotocolo" porque sus técnicas son aplicables a cualquier protocolo de capa 3 (Red). Algunos de los siguientes conceptos ya han sido definidos, pero se recalcarán para adecuarse exactamente al contexto del MPLS.

En MPLS, la transmisión de datos ocurre sobre trayectorias "unidireccionales" definidas por etiquetas llamadas *label-switched paths* (LSPs). Una LSP es una secuencia de etiquetas en cada nodo a lo largo de la trayectoria, desde la fuente hasta el destino. Las LSPs pueden ser establecidas previamente a la transmisión de datos (*control-driven*), o al momento en que se detecta un cierto flujo de datos (*data-driven*).

Las etiquetas son distribuidas usando protocolos como el label distribution protocol (LDP) o el RSVP, o pueden ser sobrepuestas a protocolos de ruteo más comunes como el Border Gateway *Protocol (BGP) o el OSPF.* Cada paquete encapsula y acarrea las etiquetas a través de su paso por la trayectoria. La conmutación se efectúa a altas tasa, debido a que las etiquetas

son de una longitud fija, son insertadas al principio del paquete, y pueden ser manejadas por hardware para conmutar rápidamente
los paquetes entre los enlaces correspondientes.

4.1 LSRs y LERs.

Los dispositivos que participan en los mecanismos del protocolo MPLS, pueden ser clasificados en ruteadores de etiqueta de borde o *label edge enrutadores* (LERs), y en ruteadores de conmutación de etiquetas o label switching enrutadores (LSRs).

Un LSR es un dispositivo ruteador de alta velocidad, que dentro del núcleo de una red MPLS, participa en el establecimiento de los LSPs, usando el protocolo de señalización apropiado y una conmutación de alta velocidad aplicado al tráfico de datos, que se basa en las trayectorias establecidas.

Un LER es un dispositivo que opera en el borde de una red de acceso hacia una red MPLS. Un LER soporta múltiples puertos conectados a diferentes tipos de redes (*frame relay*, ATM, y Ethernet); y se encarga, en el ingreso de establecer una LSP para el tráfico en uso y de enviar este tráfico hacia la red MPLS, usando el protocolo de señalización de etiquetas, y en el egreso de distribuir de nuevo el tráfico hacia la red de acceso que corresponda. El LER juega un papel muy importante en la asignación y remoción de etiquetas que se aplica al tráfico que entra y sale de una red MPLS.

Un LSR puede tener dos tratamientos a un paquete que recibe. Cuando se encuentra con un paquete no etiquetado, el ruteo convencional usa un mapeo FEC-to-NHLFE (FTN) para enviar estos paquetes. Cuando se trata de un paquete etiquetado, el protocolo de distribución de etiquetas usa un mapeo Label-to-NHLFE (ILM) para enviar estos paquetes. Una NHLFE (*Next Hop Label Forwarding Entry*) es una entrada a una tabla de envío en la que se indica la etiqueta del siguiente hop. Ambos procesos serán explicados más adelante en este capítulo.

4.2 FEC

Una clase de envío equivalente o *forwarding equivalence class* (FEC), es una representación de un grupo de paquetes que comparten los mismos requerimientos para su transporte; todos los paquetes de este grupo tienen el mismo tratamiento en la ruta hacia su destino. Al contrario de lo que pasa en el tradicional envío de paquetes en IP, en MPLS, la asignación de un paquete a una FEC en particular se realiza solo una vez, en el momento en el que paquete entra a la red. La definición de una FEC se basa en los requerimientos de servicio que posea un conjunto de paquetes dado, o simplemente por el prefijo de una

dirección IP. Cada LSR construye una tabla para especificar que paquete debe ser enviado; esta tabla, llamada base de información de etiquetas (LIB), se construye con uniones FEC/etiqueta. En la Figura 4.1 podemos observar los principales componentes de una red MPLS que ya han sido descritos.

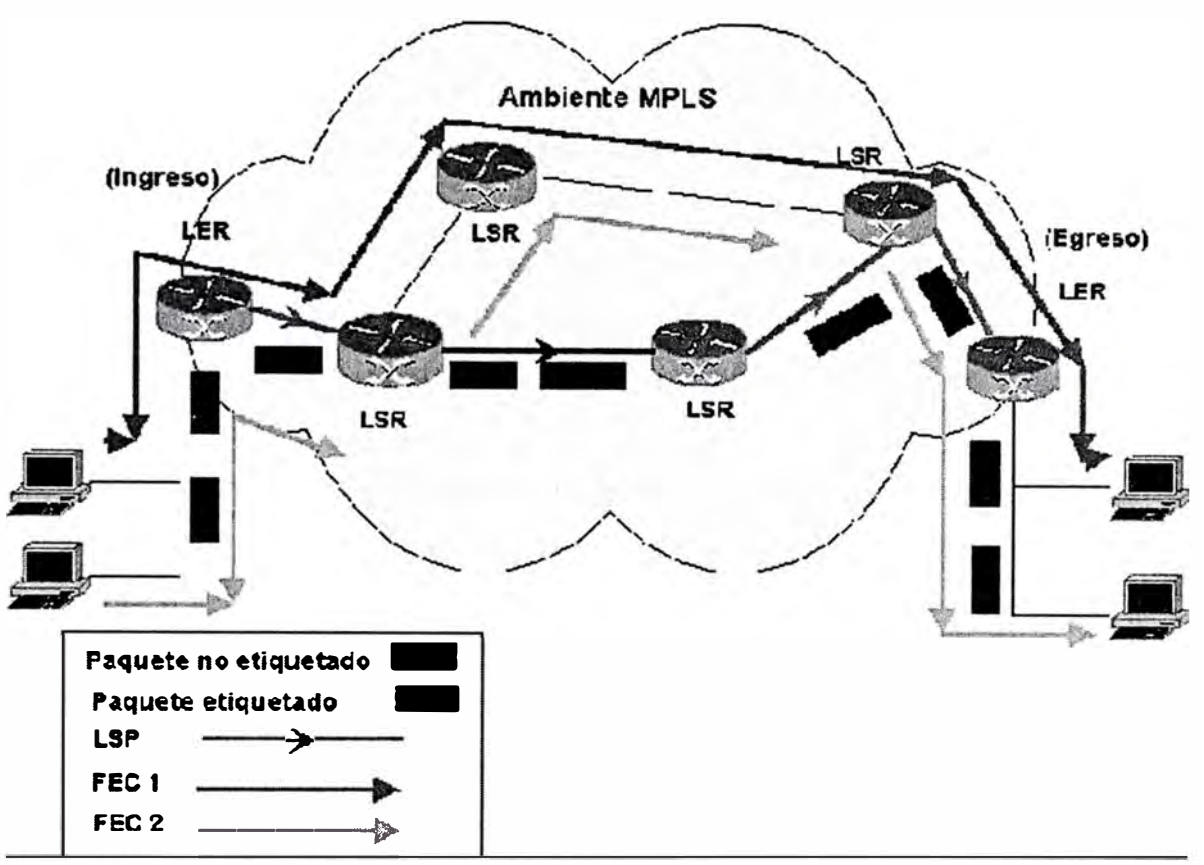


Figura 4.1 Componentes de una red MPLS.

Como se puede notar en la figura 4.1, las FECs representa a paquetes que pueden estar destinados a diferentes prefijos IP, pero pueden pasar a través de una misma LSP, como es el caso de FEC 1 y FEC 2.

4.3 Tipos de LSP

MPLS provee dos opciones para establecer una LSP:

Ruteo hop-by-hop: cada LSR selecciona independientemente el siguiente hop para una FEC dada. Esta metodología es similar a la que se usa en redes IP. El LSR usa cualquiera de los protocolos de ruteo disponibles, como OSPF, private network to network interface (PNNI), etc.

- Ruteo explícito: el LSR de ingreso especifica la lista de nodos por la cual viaja la trayectoria explícita. Sin embargo, la ruta especificada puede ser no óptima. A lo largo de la trayectoria, los recursos deben ser reservados para asegurar una calidad de servicio para el tráfico de datos (10). Este tipo de LSP facilita la ingeniería de tráfico.

4.4 Etiquetas

Una etiqueta, en su forma más simple, identifica la trayectoria que un paquete debe seguir. Una etiqueta es acarreada o encapsulada dentro de un encabezado de Capa 2 junto con el paquete. El ruteador que recibe el paquete, examina el contenido de la etiqueta para determinar el siguiente hop. Una vez que un paquete ha sido etiquetado, el resto del viaje del paquete a través de la red se basa en conmutación de etiquetas.

El valor de una etiqueta es estrictamente de significancia local, es decir que pertenecen únicamente a saltos entre LSRs.

El primer proceso al que se somete un paquete al ingresar a un ruteador MPLS, es el de ser clasificado como una FEC nueva o una ya existente, y es entonces cuando se le asigna una etiqueta al paquete. El valor de las etiquetas se deriva de valores entregados por los protocolos de Capa 2. Para protocolos de capa de enlace de datos (como frame relay y ATM), se pueden emplear los identificadores de capa 2 directamente como etiquetas, los DLCIs[7] en el caso de redes *frame-relay*, o los VPIs/VCIs en el caso de redes ATM.

Entonces el envío de los paquetes se basa en el valor de estas etiquetas. La figura 4.2 muestra el formato genérico de un encabezado MPLS o también llamado *shim header*, sus campos y como se interpone a los encabezados de las demás capas del modelo OSI. (11)

[7] DLCI. Data Link Connection Indentifier

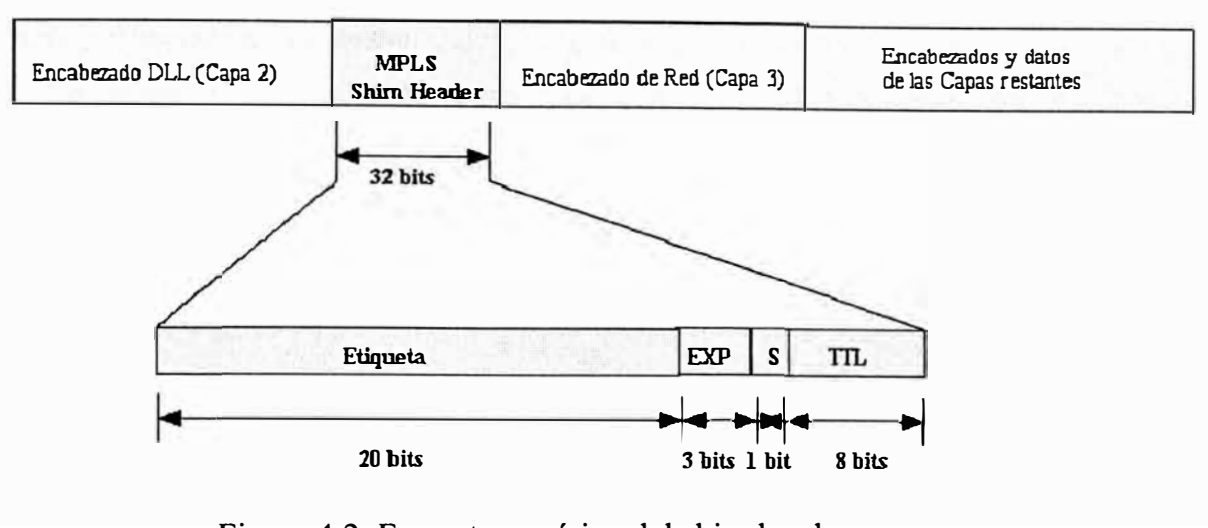


Figura 4.2 Formato genérico del shim header.

El *shim header* se interpone entre los encabezados de capa 2 y el encabezado IP (de capa 3), por eso su nombre: shim o calzado. El encabezado es de 32 bits y se divide en los siguientes campos:

- Etiqueta (20): campo de 20 bits que acarrea el valor de la etiqueta MPLS.
- EXP (3): Antes se llamaba CoS (Class of Service), ahora se considera un rango experimental. Este campo se considera para consideraciones QoS (*Quality of Service*).
- S (1): Se usa para indicar si esta presente una pila de etiquetas (*label stack*), entonces su valor será uno. Si la etiqueta es la única presente en la pila, entonces el valor será 0.
- TTL (8): el campo *Time To Live* provee funcionalidad IP TTL. Se usa para indicar el número de nodos MPLS por los que el paquete ha viajado hasta alcanzar su destino. El valor es copiado del encabezado del paquete cuando se ingresa a la LSP, y copiado de vuelta al encabezado del paquete IP cuando sale de la misma.

4.5 La Pila de etiquetas (*Label Stack*)

En un modelo más general, MPLS soporta la colocación de múltiples etiquetas a un solo paquete; en este caso, se soporta un diseño de ruteo jerárquico. Estas etiquetas se organizan en una pila o "*stack*" con una forma *last-in, first-out* (LIFO), y forma la llamada pila de etiquetas o *label stack*. El principal empleo de la pila de etiquetas se tiene cuando se emplea una operación MPLS llamada *Tunneling*, el cual será explicado más adelante en este capítulo.

4.6 Uniones a Etiquetas.

Las etiquetas son enlazadas a una FEC como resultado de algún evento o política que indica la necesidad por dicha etiqueta. Estos eventos de unión pueden ser divididos en dos categorías:

- Uniones *Data-Driven*: ocurre cuando el tráfico comienza a fluir, éste es sometido al LSR y es reconocido como un candidato a *label switching* (usa la recepción de un paquete para disparar el proceso de asignación y distribución de etiquetas). Las uniones a etiquetas son establecidas sólo cuando son necesitadas y son asignadas a flujos individuales de tráfico IP, y no a paquetes individuales.
- Uniones Control-Driven: se establecen como resultado de la actividad del plano de control y son independientes del flujo de datos. Las uniones pueden ser establecidas como respuesta a actualizaciones de ruteo (usa procesamiento de protocolos de ruteo como OSPF y BGP), o por la recepción de mensajes RSVP (usa procesamiento de control de tráfico basado en peticiones).

4.7 Distribución de etiquetas

En cuanto al proceso de distribución de etiquetas, se plantean conceptos que indican la dirección en que éste ocurre: *upstream* y *downstrem*. Por ejemplo: tenemos dos LSRs, R1 y R2, y estos concuerdan en atar la etiqueta L a la FEC Z, para paquetes mandados de R1 a R2. Entonces se dice que con respecto a esta unión, R1 es el LSR upstream y R2 es el LSR *downstream*. Cuando se dice que un nodo es *upstream* y otro es *downstream* con respecto a una unión, significa "únicamente" que etiqueta en particular representa a una FEC en paquetes que viajan del nodo upstream al nodo *downstream* (significancia local de la etiqueta). Esto "no" implica que todos los paquetes de tal FEC tienen que ser necesariamente ruteados del nodo *upstream* al nodo *downstream.(12)*

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por los cuales un LSR informa a otro de las uniones etiqueta/FEC que ha realizado. Dos LSRs que usan un protocolo de distribución de etiquetas para intercambiar información de las uniones, son conocidos como un par de distribución de etiquetas (*label distribution peer*) con respecto a la información que intercambian. Si se tiene un par de distribución de etiquetas, se puede hablar también de una adyacencia de distribución de etiquetas entre ellos. Un protocolo de distribución de etiquetas también se encarga de las negociaciones en la que se busca el enganche entre dos pares de distribución de etiquetas, con el objetivo de que cada uno aprenda sobre las capacidades MPLS del otro.

La arquitectura MPLS no reconoce solamente a un método de señalización para la distribución de etiquetas. Protocolos existentes han sido extendidos, de manera que la información de etiquetas pueda ser "cargada a cuestas" dentro de los contenidos de los protocolos (por ejemplo BGP, o túneles RSVP). El IETF ha definido en paralelo con la arquitectura MPLS, un nuevo protocolo conocido como el Protocolo de Distribución de Etiquetas (LDP), para un explícito manejo y señalización del espacio de etiquetas. También se han definido extensiones al protocolo LDP base, para soportar ruteo explícito basado en requerimientos QoS y CoS[8]; estas extensiones se concentran en el protocolo *Constraint-Based Label Distribution Protocol* (CR-LDP). Los principales protocolos existentes y sus principales características son LDP, RSVP, CR-LDP, *Protocol-Independent Multicast* (PIM) y BGP (en el caso de VPNs).

4.7.1 Control de distribución de etiquetas

MPLS define dos modos de control para la distribución de etiquetas entre LSRs vecinos:

- Control independiente: en este modo, un LSR reconoce una FEC en particular y toma la decisión de unir una etiqueta a la FEC independientemente de distribuir la unión a sus LSR pares.
- Control Ordenado: en este modo, un LSR une una etiqueta a una FEC dada, si y solo si se trata de un LER. Es decir, que el LER o también llamado label manager, es responsable de la distribución de etiquetas.

4.7.2 Esquemas de distribución de etiquetas.

En la arquitectura MPLS, la decisión de unir una etiqueta en particular a una FEC en particular se realiza por el LSR que es downstream con respecto a dicha unión. Entonces el LSR *downstream* informa al LSR *upstream* de la unión. Por lo tanto las etiquetas son asignadas en tendencia *downstream*, y las uniones de etiquetas son distribuidas en dirección *downstream* a *upstream*. Con un control ordenado, la distribución de etiquetas puede ser disparada por el uso de dos posibles escenarios o esquemas:

- Distribución de etiquetas *Downstream* (no solicitada) -DOU: en este método se permite que un LSR distribuya las uniones de etiquetas a LSRs que no los han requerido.

[8] Es una manera de manejar tráfico dentro de una red, al agrupar tipos similares de tráfico en clases, y asignarles a cada clase una prioridad en el nivel de servicio

- Distribución de etiquetas Downstream-on-Demand (solicitada) -DOD: permite a un LSR requerir explícitamente, al siguiente hop de una FEC en particular, una unión de etiqueta para dicha FEC.

4.8 Mecanismos de Señalización

- Petición de Etiquetas (*label request*): usando este mecanismo, un LSR hace una petición de etiqueta a su vecino downstream, de manera que la pueda unir a una FEC específica. Este mecanismo puede ser empleado por toda la cadena de LSRs hasta el LER de egreso.
- Mapeo de Etiquetas (*label mapping*): En respuesta a una petición de etiqueta, un LSR downstream entonces manda (mapea) una etiqueta al LSR upstream correspondiente, usando este mecanismo de mapeo.

Los conceptos de señalización se representan gráficamente en la siguiente figura

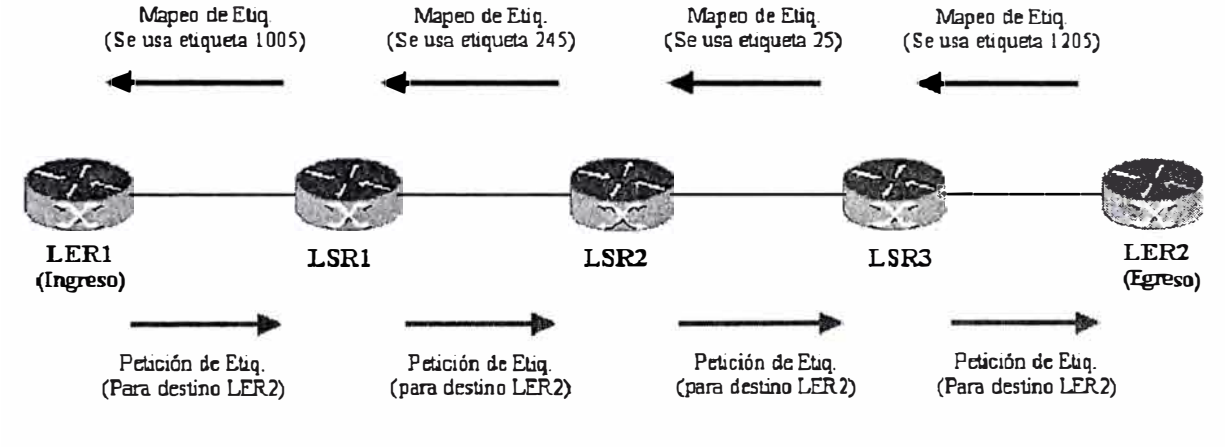


Figura 4.3 Mecanismos de señalización MPLS.

4.9 Proceso de envío en MPLS y tablas que lo asisten

Un ruteador MPLS tiene como primer obligación, procesar paquetes con etiquetas entrantes. A veces a esta información se le llama tabla *cross-connect* (de interconexión), o en términos más adecuados y usados se le llama tabla NHLFE (*Next Hop Label Forwarding Entry*). Una tabla de este tipo se utiliza para el envío de paquetes etiquetados. La principal ventaja al usar estas tablas, en vez del tradicional ruteo, es que la información puede ser procesada como datos de tipo Capa 2, donde el procesamiento es considerablemente más rápido que el ruteo.

La tabla NHFLE está formada principalmente por todas las etiquetas que pueden ser encapsuladas dentro de los paquetes. Cada NHLFE contiene: el siguiente hop (*next hop*) del paquete, y la operación que la pila de etiquetas debe ejecutar, que es la siguiente:

1. Reemplazar la etiqueta que se encuentra primera en la pila con una nueva etiqueta específica.
2. Ejecutar un *pop* en la pila.
3. Repite el paso 1, y después ejecuta un *push* de una o varias nuevas etiquetas en la pila.

Después de ejecutar el *pop* en la pila, la etiqueta obtenida se agrega al paquete, y es entonces cuando el paquete es enviado al siguiente *hop* por medio de la interfase de salida. Como la NHLFE se encuentra en la interfase de transmisión, la tabla no necesita almacenar información de la interfase de salida.

La estructura de datos (tabla) con la que un LSR interpreta etiquetas entrantes es llamada "mapa de etiquetas entrantes" o *incomig label map* (ILM). Una tabla ILM se forma de todas las etiquetas entrantes que un LSR o LER de egreso puede reconocer.

El contenido de cada entrada ILM es: etiqueta, código de operación, FEC y un campo opcional que contiene un enlace a la estructura de salida utilizada para el envío de los paquetes (NHLFE). Cada interfase lógica del LSR almacena su propia tabla ILM.

En el caso de un LER de ingreso, existe una estructura que tiene el propósito de ayudarle al ruteador a decidir qué etiquetas agregar a un paquete en particular. Esta estructura es llamada FEC-to-NHLFE (FTN), es decir un mapeo de cada FEC a un conjunto de NHLFEs. Se usa para enviar paquetes que llegan no etiquetados, y que van a serlo antes de ser enviados. Una entrada FTN esta formada por: una FEC y una entrada NHLFE. El procesamiento general que realiza esta tabla es la siguiente:

1. Decide a que FEC pertenece un paquete
2. Encuentra la FEC dentro de la tabla FTN
3. Envía el paquete a la entrada NHLFE que corresponde a la FTN

En resumen: un LSR usa el mapeo FTN para enviar paquetes no etiquetados, y usa mapeo ILM cuando se trata de enviar paquetes etiquetados.

En las figuras 4.4 y 4.5 se muestra un ejemplo gráfico de cómo un LSR usa la tabla NHLFE para enviar paquetes a través de la LSP que va de LER1 a LER2. En la Figura 4.4 se puede observar la dirección del mapeo, que como se ha dicho, se realiza por los LSPs *downstream* en dirección *upstream*. LER2 funciona como *label manager*, ya que se encarga de la requisición de etiquetas.

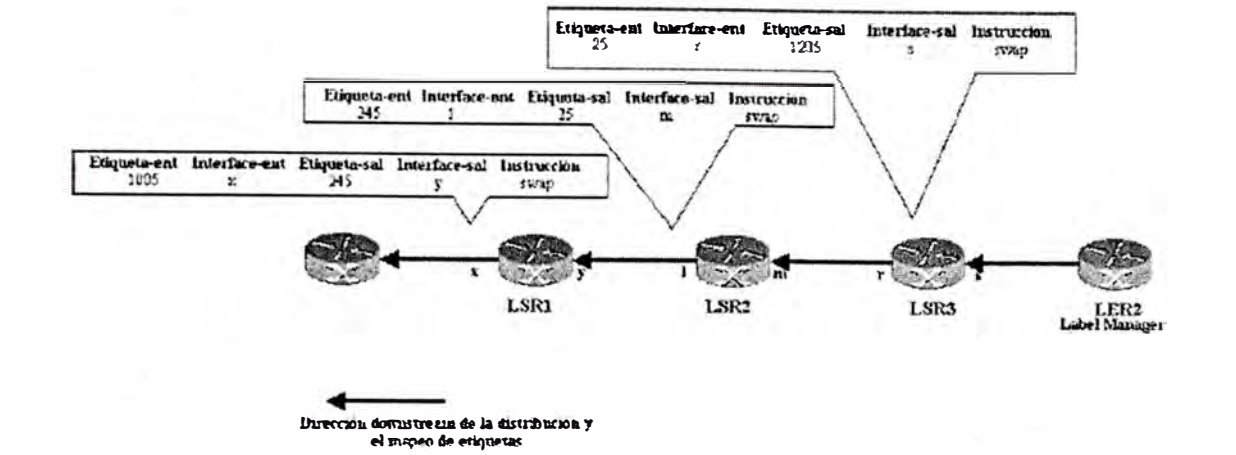


Figura 4.4: Trayectoria de LSRs con tablas NHLFE.

En la Figura 4.5 se puede observar el envío de paquetes una vez realizado el mapeo correspondiente. Los paquetes se desplazan del LER1 al LER2 intercambiando etiquetas en cada LSR.

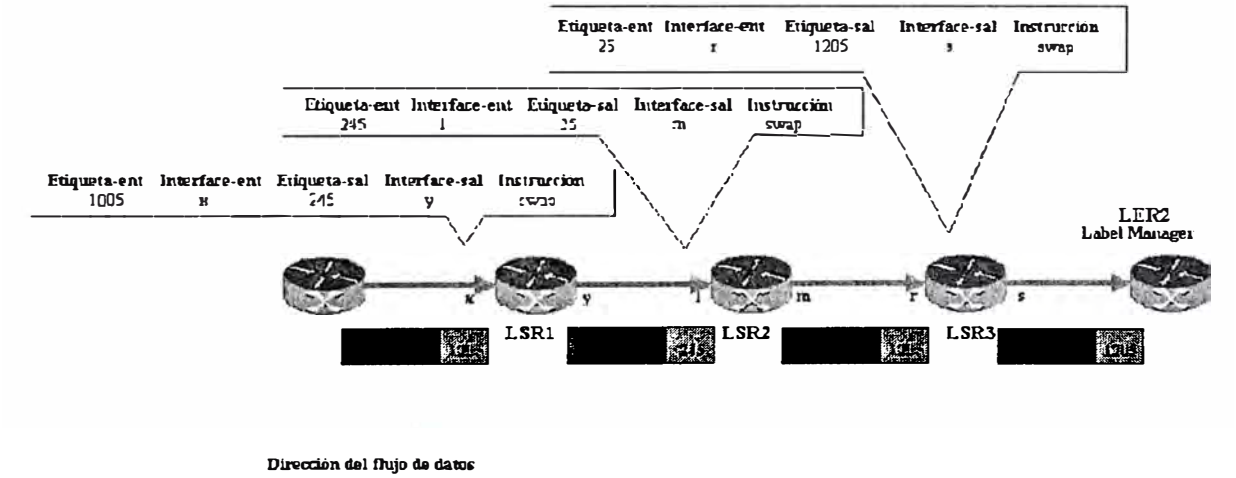


Figura 4.5 Flujo de datos en dirección del mecanismo de petición.

4.10 Fusión de etiquetas (*label merging*)

Los flujos de tráfico entrantes a un ruteador provenientes de diferentes interfaces, pueden ser fusionados y conmutados usando una etiqueta en común, si y sólo si están viajando rumbo a un mismo destino. Esto es conocido como una **fusión de flujos o agregación de flujos.**

4.11 Retención de etiquetas.

La arquitectura MPLS (13) define el tratamiento para uniones FEC/etiquetas en LSRs que no son el siguiente hop de una FEC en particular. Se definen dos modos:

- Conservativo: en este modo, las uniones FEC/etiqueta recibidas por LSRs que no son el siguiente hop dentro de una FEC en particular son descartadas.
- Liberal: en este modo, las uniones recibidas por LSRs que no son el siguiente hop de la FEC son retenidas.

4.12 Protocolo LDP (*label distribution protocol*)

El LDP es un protocolo creado específicamente para la distribución de información concerniente a uniones FEC/etiqueta, dentro de una red MPLS. Es usado para mapear FECs a etiquetas, lo cual consecuentemente creará LSPs. Las sesiones LDP son creadas entre pares LDP de una red MPLS (pares no necesariamente adyacentes).

Los pares intercambian los siguientes tipos de mensajes LSP:

- **Mensajes de descubrimiento (*discovery messages*):** Anuncian y mantienen la presencia de un LSR dentro de la red MPLS.
- **Mensajes de sesión (*session messages*):** Establecen, mantienen y terminan sesiones entre pares LDP.
- **Mensajes de advertencia (*advertisement messages*):** Crean, cambian y borran mapeos de etiquetas a FECs.
- **Mensajes de notificación (*notification messages*):** Proveen de información de aviso y de información de error en la señal.

4.13 Operación del MPLS

Los paquetes que viajan a través de una red MPLS, en general, deben seguir los siguientes pasos:

1. Creación y distribución de etiquetas
2. Creación de tablas en cada LSR
3. Creación de LSP
4. Inserción de etiquetas /chequeo de tablas
5. Envío de paquetes

En MPLS, no todo el tráfico es necesariamente transportado por la misma trayectoria. Dependiendo de las características de ingeniería de tráfico, se pueden crear diferentes LSPs para paquetes que tengan diferentes requerimientos de QoS. En la siguiente figura tenemos una red MPLS con 4 LERs y 3 LSRs, donde LER1 es el de ingreso y LER4 el de egreso.

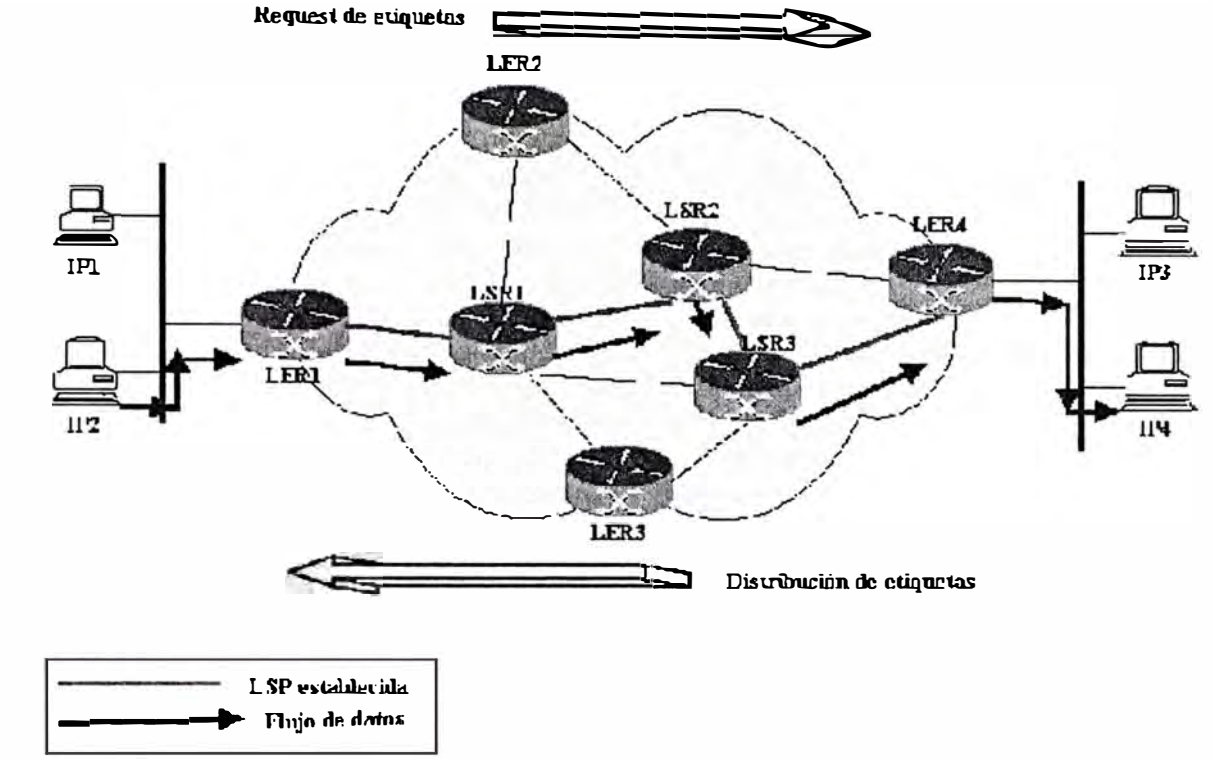


Figura 4.6 Creación de una LSP y envío de paquetes a través de ella.

La tabla 4.1 especifica paso a paso las operaciones MPLS, que se realizan con respecto a un paquete que entra al dominio MPLS (Figura 4.6).

Tabla 4.1: Descripción de las acciones MPLS.

Acciones MPLS	Descripción
Creación de etiquetas y distribución de etiquetas	Antes que el tráfico empiece a fluir, los LSRs toman decisiones para unir una etiqueta a una FEC, y contruir sus tablas. Con LDP, los enrutadores *downstream* inician la distribución de etiquetas y d e las uniones etiqueta/FEC. También LDP realiza las negociaciones de las características relacionadas con tráfico y de las capacidades MPLS. Se usa un protocolo de transporte ordenado y confiable como protocolo de señalización. El LDP usa TCP.
Creación de tablas	Cuando un LSR recibe las uniones a etiquetas crea entradas para la base de información de etiquetas (LIB). Los contenidos de la LIB especifican el mapeo entre una etiqueta y una FEC. El mapeo entre la tabla de puertos y etiquetas de entrada con la tabla de puentes y etiquetas de salida. Las entradas son actualizadas cada vez que se efectúa una renegociación de las uniones a etiquetas.
Creación de la LSP	Como se puede ver en la figura por la línea roja, las LSPs son creadas en sentido inverso de la creación de entradas LIB. El LER de ingreso usa la tabla LIB para encontrar el siguiente hop, y hace una petición de una etiqueta para una FEC en particular. Inserción de etiquetas / Chequeo de tablas Los LSRs subsecuentes solo usan la etiqueta para encontrar el siguiente hop. Una vez que un paquete llega al LER de egreso, la etiqueta es removida y el paquete es entregado a su destino
Envío de paquetes	Con referencia en la Figura 4.6 examinamos la trayectoria creada para los paquetes que viajan de LER1 a LER4, a través de LSR1, LSR2 y LSR3. LER1 puede que no tenga ninguna etiqueta disponible, ya que es el primer request que se realizará. Así que lo que tiene que hacer el nodo es econtrar el siguiente nodo usando el algoritmo *logest address match*. Entonces especifica que LSR1 es su siguiente hop. LER1 iniciará entonces el *request* de etiqueta hacia LSR1. Entonces el *request* se propagará por la trayectoria en dirección a LER4 (egreso), como se observa en la figura. LER4 que funciona como manager de etiquetas, distribuirá las etiquetas en dirección *upstream*, pasando por cada nodo de la trayectoria. Es así como el protocolo LDP (u otro de los ya vistos) realiza el establecimiento de trayectoria. LER1 insertará la etiqueta y enviará el paquete hacia LSR1. Cada LSR subsecuente realizará el envío de paquetes realizando un intercambio de etiquetas (*label swapping*). Cuando el paquete llega a LER4, entonces le será retirada la etiqueta (pop), ya que el paquete saldrá del dominio MPLS y será entregado a su destino. El camino que siguen los paquetes desde IP2 hasta IP4 se observa en la anterior figura 4.6

La siguiente Tabla 4.2 muestra un ejemplo de la base de información (LIB) que se crea en un LSR para ayudar a la distribución de etiquetas y envío de paquetes.

Tabla 4.2 Ejemplo de una tabla LIB

Puerto de Entrada	Etiqueta de Entrada	Puerto de Salida	Etiqueta de Salida
3	2005	5	23
5	125	7	1005
6	10	2	9

Si consideramos un ejemplo en particular, se comprende mejor la función de esta tabla. Tenemos tres tipos de flujos diferentes pasando por un LSR en particular, el primero se ttasa de una transferencia regular de información entre servidores (por ejemplo FTP), el segundo se tasa de datos de voz, y el tercero es un flujo de video (estos dos últimos tipos de flujos generalmente requieren de la implementación de ingeniería de tráfico para su mejor transmisión). Cada flujo es asignado a una FEC en particular, ya que cada uno debe ser tasado de una manera en especial (ancho de banda, QoS, etc).El mapeo asociado con cada flujo corresponde a las etiquetas 2005, 125 y 10, con sus correspondientes puertos de entrada 3, 5 y 6. El LSR ejecuta un intercambio de etiquetas, por lo que para paquetes de la FEC1 se cambia la etiqueta 2005 por 23, para paquetes correspondientes a FEC2 se cambia 125 por 1005, y para FEC3 se cambia 10 por 9. Las interfaces de salida correspondientes para las 3 FECs son 5, 7 y 2.

Una característica única que presenta MPLS, es que puede controlar la trayectoria de un paquete sin que sea necesario que se especifiquen los ruteadores intermedios.

Esto se realiza por la creación de túneles que pasen por ruteadores intermedios, los cuales pueden abarcar múltiples segmentos, se le llama *tunneling*.

En la figura 4.7 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura 4.7, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS), 1 bit de *stack* para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar

el TTL (*time-to-live*) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

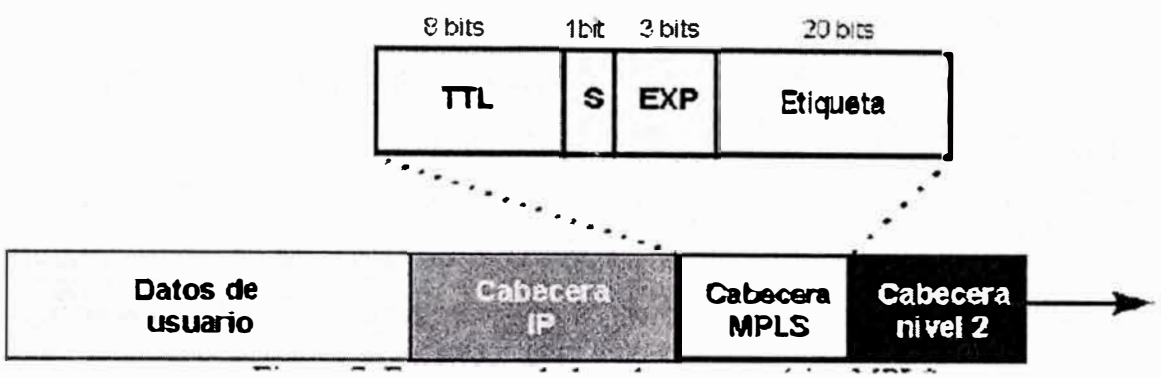


Figura 4.7 Estructura de la Cabecera genérica MPLS

Etiqueta: La etiqueta propiamente dicha que identifica una FEC (con significado local)

Exp: Bits para uso experimental; una propuesta es transmitir en ellos información de DiffServ.

S: Vale 1 para la primera entrada en la pila (la más antigua), cero para el resto. Esta es la primera etiqueta introducida.

TTL: Contador del número de saltos. Este campo reemplaza al TTL de la cabecera IP durante el viaje del datagrama por la red MPLS.

4.14 Control de la información en MPLS

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

1. Cómo se generan las tablas de envío que establecen los LSP.
2. Cómo se distribuye la información sobre las etiquetas a los LSR.

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de *routing* para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información

de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP...) para construir las tablas de encaminamiento (recuérdese que los LSR son *enrutadores* con funcionalidad añadida). Esto es lo que hace MPLS precisamente para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

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

4.15 Funcionamiento global MPLS

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

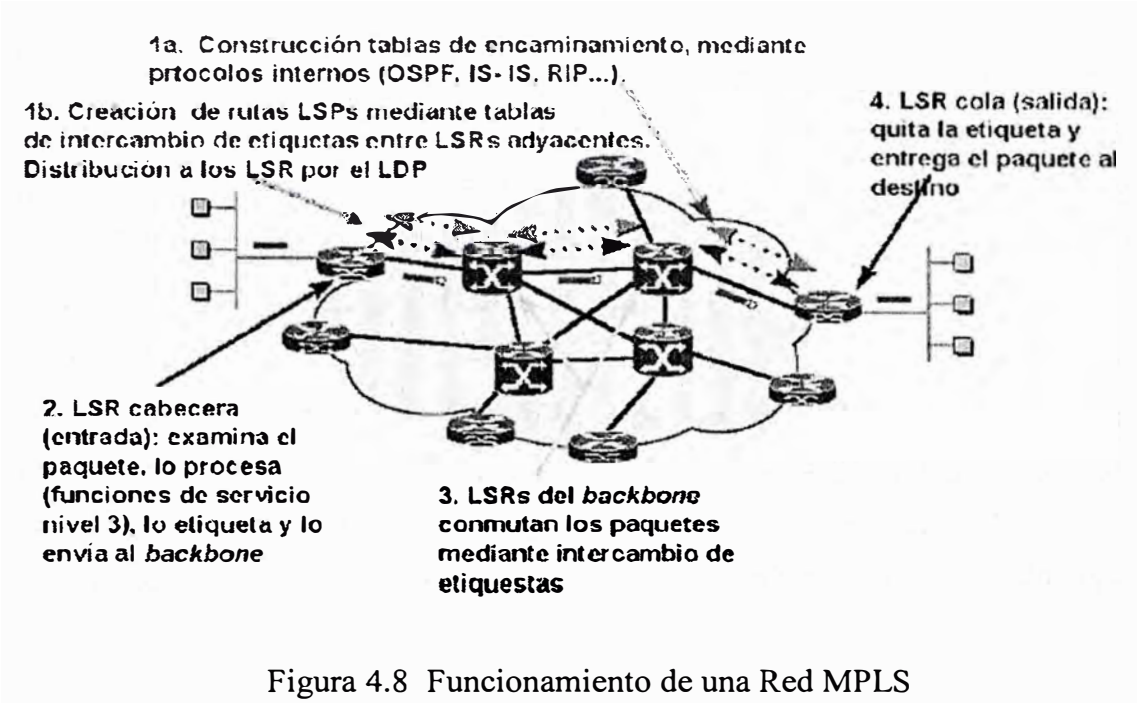


Figura 4.8 Funcionamiento de una Red MPLS

4.16 Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

- . Ingeniería de tráfico.
- . Diferenciación de niveles de servicio mediante clases (CoS).
- . Servicio de redes privadas virtuales (VPN).
- Aspectos de comparación ATM-MPLS

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

4.16.1 Ingeniería de tráfico

La ingeniería de tráfico es un proceso que optimiza la total utilización de la red, al tratar de crear una distribución de tráfico uniforme o diferenciada a través de la red.

Trata de adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no existan algunos que sean sobre utilizados, con posibles puntos con cuellos de botella, mientras otros estén siendo al mismo tiempo desperdiciados.

Es importante notar que la ingeniería de tráfico no selecciona necesariamente la trayectoria más corta entre dos dispositivos. Es posible que, para dos flujos de datos, los paquetes viajen por dos trayectorias completamente diferentes, aunque compartan los mismos nodos de fuente y de destino y que implique en una ruta larga.

En MPLS, la ingeniería de tráfico se provee inherentemente usando LSPs explícitas (como se vio en los tipos de LSPs). Los LSPs son creados independientemente, especificando diferentes trayectorias que se basan en políticas definidas por el usuario. Sin embargo se necesita la intervención de extensiones a los mecanismos de señalización.

Existen dos diferentes iniciativas para implementar la ingeniería de tráfico en MPLS: RSVP con ingeniería de tráfico y el CR-LDP.

a). TE-RSVP

El *Resource ReSerVation Protocol* (RSVP) o protocolo de reservación de recursos es un método diseñado por la IETF en 1997, que fue creado para adaptar el concepto de reservación de recursos antes de la transmisión de datos, antes utilizado en telefonía, y que está contemplado por los requerimientos de QoS. El protocolo fue diseñado para especificar requerimientos de ancho de banda y de condiciones de tráfico, para una trayectoria definida. Si el ancho de banda requerido está disponible, entonces se establece el enlace necesario para la transmisión.

MPLS propone extensiones a este protocolo para la implementación de la ingeniería de tráfico, a la que se llama TE-RSVP (*Traffic Engineering*-RSVP) o RSVP con ingeniería de tráfico, el cual es especificado en el RFC 2205. El usar esta extensión, no significa que deba ser totalmente implementado el protocolo RSVP por los LER y LSR con los que cuente la red MPLS. TE-RSVP es un protocolo de "estado suave" (*soft state*) que usa datagramas UDP o IP como mecanismo de señalización en el establecimiento de LSPs, incluyendo peticiones de etiquetas, descubrimiento y mapeo. La figura 4.9 siguiente muestra un ejemplo de la señalización en TE-RSVP.

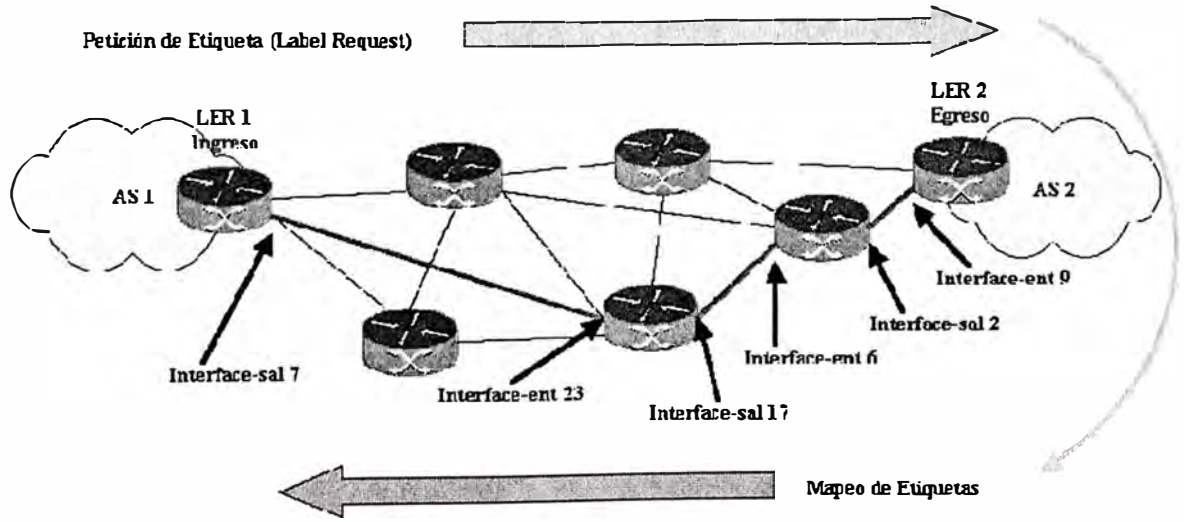


Figura 4.9 Ejemplo de una LSP estricta, ruteada por CR-LDP.

Como se puede observar, se usan los mismos mecanismos de señalización del protocolo LDP para establecer una LSP estricta limitada al paso por dos LSR específicos.

Se envía un *label request* en sentido *downstream* y un *label mapping* en sentido *upstream* para establecer la trayectoria. La trayectoria puede ser tan precisamente definida, como para especificar las direcciones IP de cada LER y LSR. Este sistema puede ser muy ventajoso para tráficos específicos, como voz o VPNs, ya que se puede definir la trayectoria óptima para satisfacer sus necesidades de ancho de banda y de prioritización.

4.16.2 Clases de servicio (CoS)

MPLS está diseñado para poder transmitir flujos de tráfico que necesitan ser diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades.

Según los requisitos de los usuarios, DiffServ permite diferenciar servicios adicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. Para ello se emplea el campo ToS (*Type of Service*), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP.

De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.
- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda.

Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico *best-effort*, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

4.16.3 Redes privadas virtuales (VPNs)

Una red privada virtual (VPN) se construye basado en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las VPNs son soluciones de comunicación VPN basadas en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR)[9]. Algo similar se puede hacer con ATM, con diversas clases de garantías. El inconveniente 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 costos asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CEs[10] del cliente y restablecer todos los PVCs.

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

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

---

[9] CIR: *Velocidad de información suscrita:* La velocidad a la que una red Frame Relay acepta transferir información bajo condiciones normales

[10] CE : *Consumer Edge Device*. Sitio del cliente

sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones.

Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:

- En el nivel 3, mediante el protocolo IPSec10 del IETF.
- En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un NSP.

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

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

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

- Están basadas en conexiones punto a punto (PVCs o túneles).
- La configuración es manual.
- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.
- Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.

- La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

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

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

4.16.4 Aspectos de comparación ATM – MPLS.

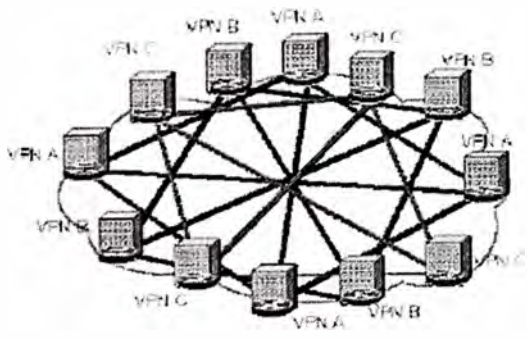
En el capítulo anterior se vieron las principales limitaciones que se tienen al implementar el modelo IP sobre ATM, y es este modelo el que se plantea como principal referente o antecesor a MPLS. Y ya teniendo claras las características que diferencian tanto al modelo IP/ATM como a MPLS, resulta interesante compararlas entre sí. La siguiente tabla presenta una comparación entre las características funcionales de IP, ATM y MPLS.

Tabla 4.3 Comparación entre IP, ATM y MPLS. (14)

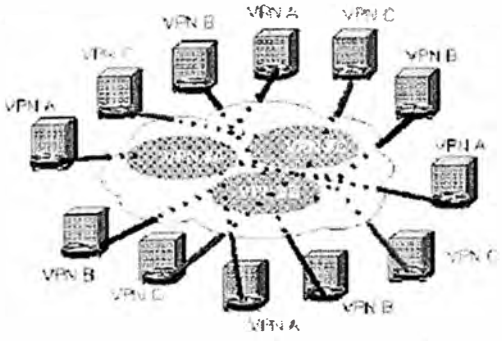
	IP	MPLS	ATM
Plano de Control de la Red			
Control de admisión	Ninguno	En desarrollo por el foro MPLS	UNI
Ruteo	OSPF, IS-IS, BGP4	OSPF-TE, IS-IS-TE, BGP4-TE	PNNI
Cómputo de trayectoria	Ninguno - Envío por hop	Punto a Punto, CBR, *Congestion-aware*	Punto a Punto, CBR, *Congestion-aware*
Señalización	Ninguno - Envío por hop	RSVP-TE, CR-LDP	PNNI
Nombre de la conexión	Ninguno	*Label Switched Path* (LSP)	*Virtual Connection*
Identificador de conexión	Ninguno	ID de la etiqueta	VPI, VCI
Ruteo Explícito	Ninguno	Objetos de ruteo explicito	Listas de tránsito designadas
Plano de datos de la red			
Unidad de transmisión	Paquetes (de longitud variable)	Paquetes y/o celdas	Celdas o paquetes (ATM forum FAST)
Políticas para imparcialidad	Ninguna	Ninguna	Si, para contratos de tráfico múltiple
Marcación	Ninguna	Ninguna	Las celdas están marcadas conforme o no conforme
Buffer Allocation	Limitado	En desarrollo por el foro MPLS	Reservaciones por flujo
Organización para priorización y frames	Limitado o ninguno, dependiendo de estándar del protocolo	En desarrollo por el foro MPLS	Por puerto, por flujo, por clase

Ventajas en una red centrada en IP	Flexibilidad, gran variedad de Protocolos de servicios de datos, integración con UNIX OS, multi-Vendor, implementación basada en estándares.	Provisionamiento eficiente; predecible y confiable; soporte a diferencias de servicios y SLA; utilización óptima del ancho de banda de la red, balanceo de carga punto a punto.	Predicción y confiabilidad de la red, orientado a conexión, partición de red entre capa 2/capa 3; utilización óptima del ancho de banda de la red, balanceo de carga punto a punto.
Limitaciones en una red centrada en IP	Soporte limitado para servicios diferenciados, predictibilidad limitada, redes menos optimizadas; como es un protocolo *conectionless*, el ruteo *hop-by-hop* crean congestión y suprautilización de los recursos de la red	Es un estándar emergente, se tiene poca experiencia en el campo; todavía no soporta ni multiservicio ni interoperabilidad, y entonces todavía no puede ser propuesto como un *back-bone* común para operadores de red que soportan multiservicios.	Se tiene que manejar un plano de control adicional; la integración de ATM en ruteadores resulta en un mayor número de adyacentes que manejar.

En la tabla se hacen evidentes las ventajas de MPLS sobre sus antecesores. De aquí surge la problemática que las grandes compañías proveedoras de servicios de red han tenido que superar, la migración de una infraestructura ATM a una MPLS. Para realizar esto, no hay algún método específico, simplemente es donde entra en acción la ingeniería de redes.



Modelo "superpuesto"
(Túneles o PVCs)
Topología VPN conectiva



Modelo "acoplado"
(MPLS)
Topología VPN no-conectiva

Figura 4.10 Modelo "superpuesto" (túneles/PVCs) vs. modelo "acoplado" (MPLS)

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

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

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

CAPITULO V
IMPLEMENTACION DE UNA RED IP-MPLS PARA LA UNIVERSIDAD SAN MARTÍN DE PORRES

Este capitulo trata sobre una posible implementación de una red privada virtual, basada en la tecnología MPLS, para la Universidad San Martín de Porres - USMP con el objetivo de mejorar la interconexión entre las redes.

5.1 Descripción de la Red Actual

Actualmente la red de la USMP se encuentra interconectada con líneas dedicadas permanentes entre las distintas Facultades, resultando estas conexiones muy costosas y operando en forma separadas. Cada Facultad tiene su propia red local, su propio dominio y por lo tanto tienen dificultades para compartir información instantánea. Esto se ve graficado en la figura 5.1.

DIAGRAMA DE LA RED USMP

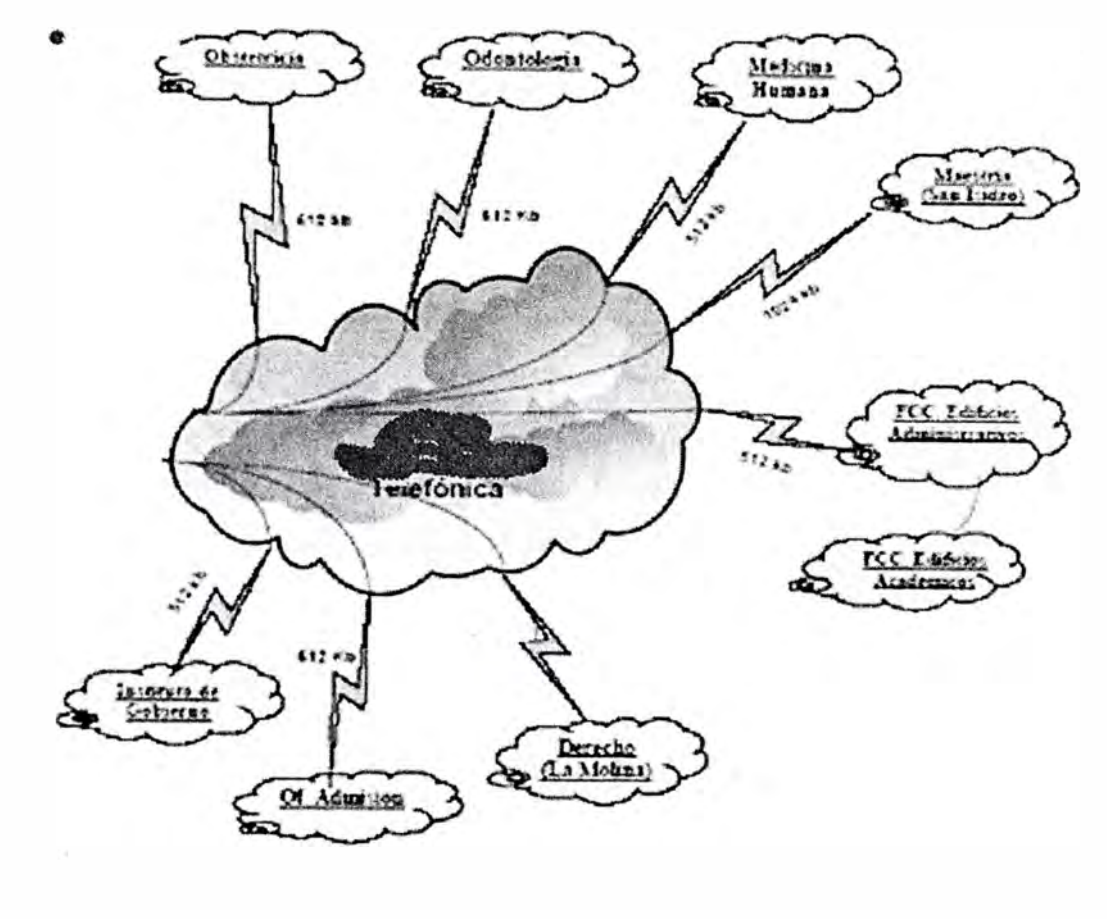


Figura 5.1 Interconexión de las facultades de la USMP.

5.2 Implementación de la VPN-MPLS para la Red USMP

Como se ha visto anteriormente, la Universidad San Martín de Porres no cuenta con el servicio de red privada virtual sobre MPLS para la transmisión de información, en esta sección describiremos una posible configuración de la red de la universidad a través de VPNs configuradas para interconectar las subredes de las Facultades por medio de la tecnología MPLS.

5.3 Descripción de la Red Planteada

La red que se va implementar tiene la siguiente topología

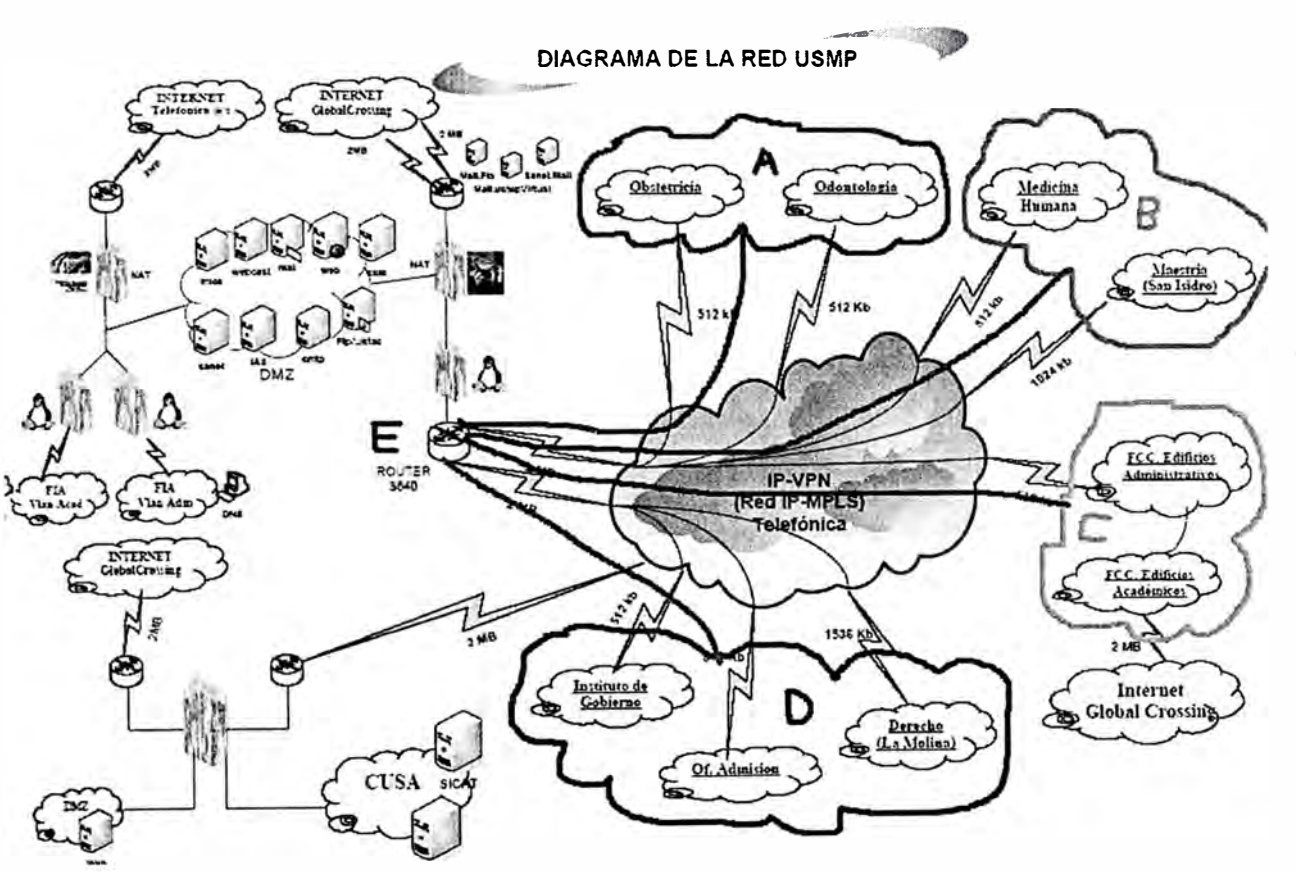


Figura 5.2 Interconexión de las Facultades de la USMP con VPN MPLS

5.3.1 Nodo Central

El nodo central es el Router 3640 que optimiza el ancho de banda, tiene el servicio corporativo para los proveedores de servicio. Esto es que permite el ruteo de los datos de las redes LAN de las facultades de la Universidad USMP, como también permite el ruteo de los datos del Servidor hacia la subred DMZ (zona desmitarilizada) y la salida hacia Internet. Estas funcionalidades de gestión de tráfico del router 3640 evolucionan con la inclusión de la tecnología MPLS.

5.3.2 Creación de los LSP (Label Switched Path)

Como podemos ver en la figura 5.2 se crean LSPs entre el nodo central y las subredes de las Facultades. Se crean desde el Nodo Central hasta las VPN A (Obstetricia y Odontología), VPN B (Medicina Humana y Maestría), VPN C (FCC. Edif.. Académicos y FCC. Edif.. Administrativos) y VPN D (Instituto de Gobierno, Oficina de Admisión y Derecho). El ancho de banda de los enlaces van desde 512 Kbps a 2 Mbps.

En la figura 5.2 se tiene la interconexión completa de la red VPN MPLS , donde los proveedores de servicios son Telefónica y Global Crossing.

Las distintas Facultades están interconectadas para facilitar el flujo de información entre las mismas. Tales como el Sistema SAP. Ingreso al SAP de los requerimientos de Activos Fijos, Bienes y Servicios solicitados por las diferentes oficinas de todas las facultades de la USMP. También el Aplicativo SICAT, que es el Sistema Integrado de cuentas corrientes Académicas y de Tesorería.

Tenemos Firewall en la VPN, el cual establece una barrera entre la red pública y la privada. Controla y monitorea el tráfico a través de este límite.

Aplicación Gateway. Sistema altamente seguro y dedicado a soportar el software del gateway.

DMZ. Una DMZ se crea cuando las empresas quieren compartir algo de su información. Está delineada por dos firewall, uno entre la red pública y la DMZ y el otro entre la red privada y la DMZ.

En el diagrama también se nota que en la Facultad de la FIA(Ingeniería) tiene 2 VLAN, una académica y otra administrativa.

5.3.3 Configuración de VPNS de la USMP

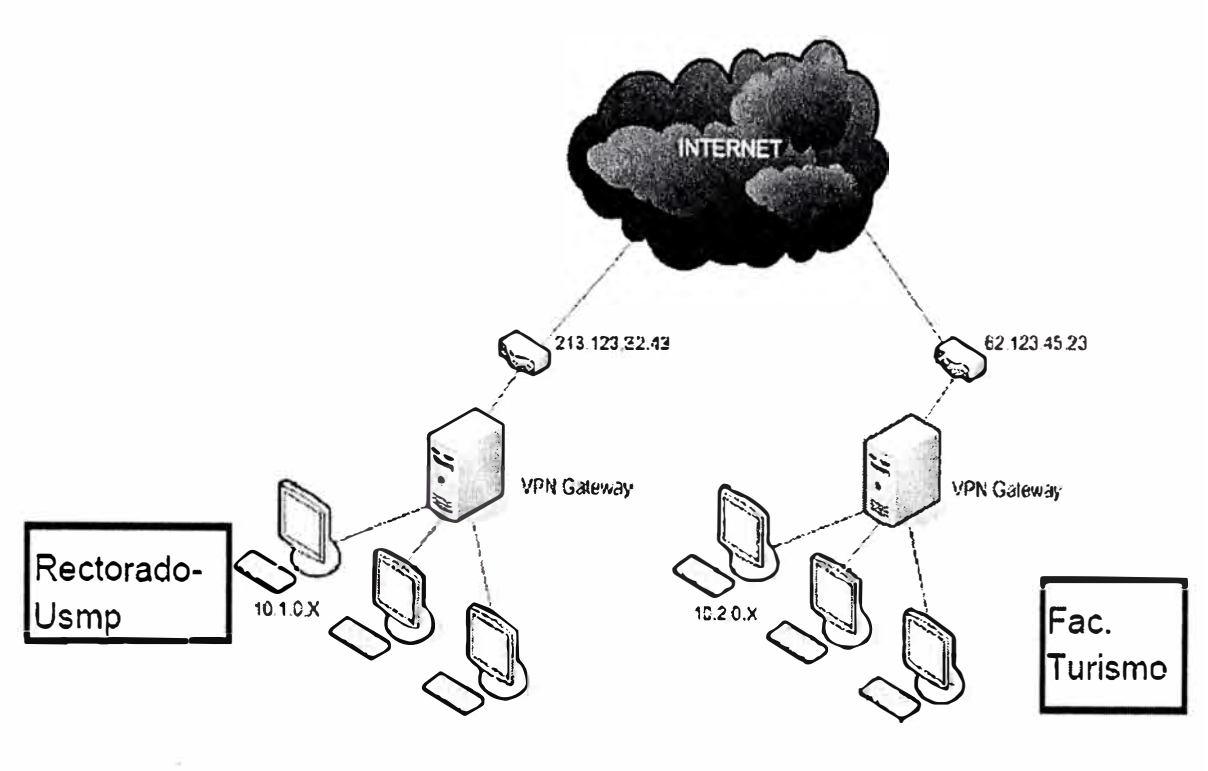


Figura 5.3 red VPN de dos nodos

Esta es una conexión de dos Facultades de la Universidad de San Martín de Porres.

Se establece una VPN entre dos gateways, cada uno de una red privada. Los equipos de las redes utilizan esos gateways como routers.

Cuando un gateway recibe un paquete dirigido a la red privada del otro extremo, lo envía a través de la VPN de modo seguro.

Las VPNs basadas en MPLS ofrecen un servicio múltiple y garantizado sobre una única infraestructura de red.

MPLS es una técnica que permite crear trayectos virtuales sobre una red enrutada, de un modo similar al funcionamiento de las redes ATM y Frame relay

Comparadas con las redes IP puras, que requieren largos periodos de tiempo para reconfigurar y reconstruir tablas de enrutamiento, los trayectos conmutados por etiquetas (LSPs, *Label Switched Paths*) de MPLS pueden configurarse por adelantado para desviar el tráfico en caso de que se produzcan problemas en un trayecto primario, y ofrecer así una recuperación rápida.

5.4 Hardware y Software a Utilizar

5.4.1 Hardware

Se utilizará el hardware disponible en el laboratorio de redes de la Universidad. El hardware es el siguiente:

CISCO CATALYST 2950 24PORT 10/100 SWITCH

CISCO 3640 – ROUTER

Cables UTP CAT 5: Straight, Cross over

Cables de Consola

Computadora Personal o de Escritorio

5.4.2 Software

El software precargado en el Switch y en el Router es Cisco IOS.

Los nuevos routers de Cisco están basados en el software Cisco IOS, el estándar "defacto" para las operaciones de Internet. El software Cisco IOS ofrece un número de elementos avanzados de seguridad, incluyendo firewall de inspección, IPSec para redes privadas virtuales, VPN, y un sistema de detección de intrusos (IDS) para mantener la red y la información segura. Muchas de las plataformas ofrecen también aceleración de hardware para entregar desempeño 3DES VPN. El software Cisco IOS permite configuración remota, ayudando a los administradores de red a evitar amenazas potenciales antes de que se perturbe el desempeño de la red. Además, el software Cisco IOS permite a los administradores determinar la calidad de servicio al priorizar el tráfico por aplicación o usuario, asegurando que las aplicaciones estratégicas y sensibles al tiempo obtengan una alta prioridad.

HyperTerminal. Es un sistema básico de comunicación para conectarse a otros sistemas. Es un emulador de terminal tipo texto y sólo se puede utilizar para conectarnos con un sistema multipuesto y multitarea (ej. UNIX). También se pueden transferir ficheros de una máquina a otra.

5.5 Requerimientos para Implementar una VPN

Para el correcto armado de una VPN, es necesario cumplir con una serie de elementos y conceptos que a continuación se detallan:

- ***Tener una conexión a Internet:*** *Se tiene* una conexión IP dedicada.
- ***Servidor VPN:*** básicamente es una PC conectada a Internet esperando por conexiones de usuarios VPN y si estos cumplen con el proceso de autenticación, el servidor aceptara la conexión y dará acceso a los recursos de la red interna.
- ***Cliente VPN:*** este puede ser un usuario remoto o un enrutador de otra LAN.
- ***Asegurarse que la VPN sea capaz de:***

- Encapsular los datos

-Autentificar usuarios.

-Encriptar los datos.

-Asignar direcciones IP de manera estática y/o dinámica.

CONCLUSIONES

1.- El uso de Internet por parte de las empresas ha llevado a la creación de nuevas formas de comunicación y de integración de sistemas de información, tanto en el uso de la tecnología dentro de la empresa, como en el uso de la tecnología Internet en la comunicación y colaboración con los clientes y proveedores de la empresa.

2.- Las Redes Privadas Virtuales permiten la interconexión e integración de servicios de información de diferentes sucursales dispersas geográficamente de forma segura.

3.- Aprovechan la infraestructura de comunicaciones de Internet, siendo una alternativa de interconexión de puntos remotos rentable y eficaz.

4.- Para el siguiente informe se ha tomado el ejemplo de configuración de la Universidad San Martín de Porres interconectada con sus 12 facultades. Se realiza una posible implementación de la red privada virtual, basada en la tecnología MPLS, con el objetivo de mejorar la interconexión entre las distintas sedes. Se crean LSPs entre el nodo central y las subredes de las Facultades. Se crean desde el Nodo Central hasta las VPN A (Obstetricia y Odontología), VPN B (Medicina Humana y Maestría), VPN C (FCC. Edif.. Académicos y FCC. Edif.. Administrativos) y VPN D (Instituto de Gobierno, Oficina de Admisión y Derecho). El ancho de banda de los enlaces va desde 512 Kbps a 2 Mbps. Siendo los proveedores de servicios Telefónica y Global Crossing.

Se ha modelado como se indica líneas arriba el ejemplo de la Universidad San Martín De Porres interconectándose el local central (Rectorado-Santa Anita) con las distintas Facultades que se encuentran en distintas áreas geográficas, donde los proveedores de servicios son Telefónica y Global Crossing.

Las distintas Facultades están interconectadas para facilitar el flujo de información entre las mismas. Tales como el Sistema SAP. Ingreso al SAP de los requerimientos de Activos Fijos, Bienes y Servicios solicitados por las diferentes oficinas de todas las facultades de la USMP. También el Aplicativo SICAT, que es el Sistema Integrado de cuentas corrientes Académicas y de Tesorería.

Tenemos Firewall en la VPN, el cual establece una barrera entre la red pública y la privada.Controla y monitorea el tráfico a través de este límite.

Aplicación Gateway. Sistema altamente seguro y dedicado a soportar el software del gateway.

DMZ. Una DMZ se crea cuando las empresas quieren compartir algo de su información. Está delineada por dos firewall, uno entre la red pública y la DMZ y el otro entre la red privada y la DMZ.

5.- El principal motivo de la utilización de las redes privadas virtuales es su rentabilidad. Los canales de comunicación públicos con recursos compartidos por muchos usuarios son más asequibles que las líneas dedicadas.

Para muchos casos, una red privada virtual en cualquiera de sus modalidades presenta un excelente ratio precio / prestaciones y son de gran eficacia al soportar infinidad de aplicaciones complejas.

6.- Estos sistemas son capaces de ofrecer la misma seguridad que cualquier otro medio.

En la transmisión de datos se usan medidas estándares de seguridad como la encriptación y autenticación de los elementos que intervienen. Cifra y autentica el tráfico entre delegaciones a nivel de IP. El tráfico entre delegaciones se realiza mediante un encapsulado de IP en IP que va con clave de cifrado de datos, por lo que la información viaja con absoluta seguridad por la red.

7.- También se ha realizado la descripción del MPLS, y la presentación de los argumentos que han llevado a los desarrolladores de redes de comunicaciones a señalar a esta tecnología, como la más adecuada para confrontar los problemas en las redes actuales.

8.- El MPLS usa un método de reenvío de paquetes basado en etiquetas. Estas pueden corresponder a los destinos IP en las redes, como en el reenvío IP tradicional, pero también puede representar otros parámetros, como fuentes de direcciones, calidad de servicio (QoS) y otros protocolos. MPLS implementa intercambio de etiquetas entre diferentes módulos de las redes.

El hecho de simplemente intercambiar etiquetas, en vez de la interpretación y el procesamiento de todo un encabezado IP en cada *hop*, provee una mejor manera de enviar paquetes, lo que al mismo tiempo ofrece la oportunidad de enviar flujos de tráfico a una mayor velocidad.

9.- MPLS es la evolución natural de las redes existentes que quieren converger en sistemas de comunicaciones que puedan soportar las capacidades necesarias, el impresionante crecimiento de Internet implica; y al mismo tiempo, que permitan a los administradores de redes controlar el tráfico en un nivel mucho más granular o específico.

10.- El éxito de MPLS tiene que ver directamente con la solución a problemas que se presentaban en técnicas anteriores como IP sobre ATM. Termina con los problemas de escalabilidad y manejo de múltiples planos de control, que el modelo IP/ATM presentaba.

Al ser MPLS un multiprotocolo, permite flexibilidad de arquitectura con respecto al medio que se usa como transporte (tecnología de Capa 2), como ATM, *frame-relay*, Ethernet Gigabit, o paquetes sobre SONET (PoS). Es por esta característica que se pueden plantear esquemas de transición o migración de tecnologías como las mencionadas, a una arquitectura MPLS.

11.- Como MPLS es una integración de las tecnologías de Capa 2 y de Capa 3, permite la aplicación de ingeniería de tráfico, cuyo objetivo básico es adaptar los flujos de tráfico a los recursos físicos de la red. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP que trabaja sobre enlaces congestionados, a otros enlaces más descargados, aunque no cumplan con el algoritmo de la ruta más corta.

En general, se puede concluir que MPLS, por sus características, resulta ser la mejor opción para funcionar como núcleo o *backbone* de cualquier tipo de red (incluyendo IP, ATM, *frame-relay*, Ethernet, etc.). MPLS ofrece una mayor estabilidad en lo que respecta al ancho de banda, una mayor confiabilidad para la entrega de información (pérdida de paquetes), mejores mecanismos de señalización, un envío de paquetes mucho más rápido, y la capacidad de adecuación a las necesidades del usuario (administrador de red) como consecuencia del uso de aplicaciones de ingeniería de tráfico.

12.- Una importante ventaja de una red única es la simplificación en cuanto a administración de una sola red, sobre la que se pueden crear tantas redes virtuales como sea necesario. Esto facilitará enormemente la labor a los proveedores de servicio al tiempo que les permitirá ofrecer servicios de valor añadido, pues es lo que en definitiva acabará marcando la diferencia entre ellos. Hoy en día hay operadores que migran a esta solución, por ejemplo: Cable & Wireless, Equant, Genuity y MCI World-Com, Telefonica.

Los fabricantes también se han volcado a desarrollar software necesario para la migración y del equipamiento propio de MPLS. Tanto CISCO como Nortel Networks, Juniper Networks o Nokia (entre otros) disponen de grupos de trabajo especializados

desarrollando este nuevo estándar. Este es el punto clave para que los proveedores de servicio puedan comprobar la aceptación de MPLS en el mercado, dando así el primer paso hacia una nueva etapa para las redes de comunicaciones. Una etapa, si todo evoluciona siguiendo la trayectoria actual, será muy prometedora.

ANEXO A ACRÓNIMOS

ATM—*Asynchronous Transfer Mode*

BGP—*Border Gateway Protocol*

CBR — *Constant Bit Rate*

CoS—*Class of Service*

CR-LDP—*Constraint-based RoutingLabel Distribution Protocol*

DLCI—*Data Link Connection Identifier*

DOD — *Downsream on Demand*

DOU — *Downstream unsolicited*

EGP—*Exterior Gateway Protocol*

ERB — *Explicit Route Information Base*

FEC—*Forwarding Equivalence Class*

FTN—*FEC to NHLFE Map*

FTP — *File Transfer Protocol*

GMPLS—*Generalized Multiprotocol Label Switching*

GRE—*Generic Route Encapsulation*

IETF—*Internet Engineering Task Force*

IGP—*Interior Gateway Protocol*

ILM—*Incoming Label Map*

IP—*Internet Protocol*

ISP—*Internet Service Provider*

LAN—*Local Area Network*

LDP—*Label Distribution Protocol*

LER—*Label Edge Router*

LIB—*Label Information Base*

LS — *Label Swapping*

LSP—*Label Switch Path*

LSR—*Label Switch Router*

MAN—*Metropolitan Area Network*

MPE—*Multiprotocol Extension*

MPLambdaS—*Multiprotocol Lambda Switching*

MPLS—*Multiprotocol Label Switching*

MPOA—*Multiprotocol over ATM*

NHLFE—*Next Hop Label Forwarding Entry*

OSI—*Open Systems Interconnection*

OSPF—*Open Shortest Path First*

PFT — *Partial Forwarding Table*

PHB — *Per Hob Behavior*

PNNI—*Private Network-to-NetworkInterface*

PoS—*Packet over SONET*

PSTN—*Public Switched TelephoneNetwork*

PVC—*Permanent Virtual Circuit*

QoS—*Quality of Service*

RIP—*Routing Information Protocol*

RSVP—*Resource Reservation Protocol*

SLA — *Service Level Agreements*

SVC—*Switched Virtual Circuit*

SVP—*Switched Virtual Path*

TCP—*Transmission Control Protocol*

TE—*Traffic Engineering*

TE-RSVP — *Traffic Engineering Resource Reservation Protocol*

TTL—*Time-To-Live*

UBR—*Unspecified Bit Rate*

UDP—*User Datagram Protocol*

VC—*Virtual Circuit*

VCI—*Virtual Circuit Identifier*

VoIP—*Voice over IP*

VP—*Virtual Path*

VPI—*Virtual Path Identifier*

VPN—*Virtual Private Network*

WAN—*Wide Area Network*

BIBLIOGRAFÍA

[1] [2] Internetworking Technologies Handbook, Cisco Press. Ford, Kim Lew, Spanier and Stevenson. 1997.

[3] http://www.v90.com

[4] Recomendación G.100, Definitions used in Recommendations on general characteristics of internacional telephone connections and circuits, ITU-T, 1993

[5] Digital Communications, Pag. 63. Bernard Sklar, 1998, Second Edition

[6] Recomendación G.711, Pulse Code Modulation (PCM) of voice frecuencies, ITU-T, 1988

[7] Revista Data Communications, Artículo Next-Gen VPNs: The Design Challenge, Pag. 83, Vol. 28, No. 12, Septiembre de 1999.

[8] Virtual Private Networking, An Overview, Microsoft, Septiembre de 2001.

[9] IETF. "Charter IETF sobre MPLS."

[10] International Engineering Consortsium. "MPLS Tutorial."

[11] Gallaher, R. "An introduction to MPLS."

[12] Rosen E. "Multiprotocol Label Switching Architecture," RFC 3031.Enero 2001.

[13] Gallaher, R. "Advanced MPLS Signaling."

[14] Semeria, Chuck. "RFC 2547bis: BGP/MPLS VPN Fundamentals". Juniper Networks, March 2001.

[15] Ford, M., Lew, K., Spanier, S. y Stevenson, T.. Internetworking Technologies Handbook. Indianapolis: Cisco Press, 1997.

[16] Sklar, Bernard. Digital Communications, Fundamentals and Applications, Second Edition. New Jersey: Prentice Hall PTR, 2000.

[17] Pepelnjak, Ivan y Guichard, Jim. MPLS and VPN Architectures. Indianapolis: Cisco Press, 2001

[18] Brown Steven. Implementación de redes privadas virtuales, Mexico:McGgraw-Hill, 2000

SITIOS WEB

http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/vpnoverview.asp

http://www.ietf.org/html.charters/mpls-charter.html

http://www.convergedigest.com/Bandwidth/archive/010910TUTORIAL-rgallaher1.htm. 1999.

http://www.iec.org/online/ tutorials/mpls/. 2003.

http://www.juniper.net/techcenter/techpapers/200012.html
http://www.convergedigest.com/tutorials/. 1999.

http://www.microsoft.com

Pagina web oficial de Microsoft Corporation. Fuente de información sobre losprotocolos PPTP y L2TP sobre computadores instalados con sistemas operativos Windows NT, Windows 2000 server, Windows XP y Windows 2003 Server.

http://www.cisco.com

Pagina web oficial de Cisco Systems. Compañía mundial líder en la fabricación de equipos para Internetworking. Dentro de sus productos cuenta con equipos concentradores de túneles L2F, L2TP y IPSec. Desarrolla sistemas operativos (IOS) para sus enrutadores y switches que capacitan a los mismos para crear y terminar túneles.

http://www.v90.com

Pagina desarrollada por Copper Pair Communications Inc. que discute los antecedentes, y beneficios del estandar V.90 para transmisión de datos sobre líneas análogas conmutadas. Además ilustra de manera breve las características de una red telefónica tradicional.