UNIVERSIDAD DE BELGRANO

Las tesinas de Belgrano

Facultad de Tecnología Informática
Licenciatura en Sistemas de Información

Transmisión de voz, video y datos en Redes Privadas Virtuales VPN/MPLS

Nº 259 **Damián Rodríguez**

Tutor: Alberto David Airala

Departamento de Investigaciones
Noviembre 2008

Resumen

Un trabajo final de carrera presentado sobre redes privadas virtuales utilizando la tecnología VPN/MPLS, tiene como objetivo definir un modelo para la implementación para la transmisión de voz, video y datos; permitiendo a los Carriers y ISPs entender la complejidad, ventajas y desventajas de su implementación; y a los clientes comprender el beneficio de utilizar esta nueva tecnología para obtener conectividad entre sucursales, acceso a Internet y la posibilidad de transmitir voz y video sobre el mismo transporte de red.

Agradecimientos

A mi novia especialmente por haberme apoyado durante el desarrollo del documento y a lo largo de mi carrera. Por haber leído varias veces el documento y hacer las veces de editora.

A mi familia por el punta pie inicial y por inculcarme el estudio como herramienta de trabajo.

Al Licenciado David Airala, por haber confiado en mi trabajo y cederme su valioso tiempo para ayudarme a conformar este documento.

A mis profesores y compañeros de la UB por acompañarme durante estos años de carrera.

.

Tabla de Contenido

Tabla de Ilustraciones

Objetivo del documento

El presente documento tiene como objetivo ***definir un modelo para la implementación de redes privadas virtuales con la tecnología VPN/MPLS para la transmisión de voz y datos***, que permita a los Carriers y ISPs entender la complejidad, ventajas y desventajas de sus implementación, y a los clientes comprender el beneficio de utilizar esta nueva tecnología para obtener conectividad entre sucursales, acceso a Internet y la posibilidad de transmitir voz sobre el mismo transporte de red.

El modelo se desarrolla identificando las ***claves de diseño*** de redes privadas virtuales y aplicando dicho modelo a un caso real.

Planteamiento y contexto del problema

El ***crecimiento de las redes Internet Protocol (IP)****, en conjunto con:*

- *la necesidad de los Carriers de unificar sus estructuras de redes de telefonía, datos y servicio para reducir costos operativos y de capacidad, acelerando así* ***la implementación de redes de próxima generación (NGN: Next Generation Network)****;*
- *las necesidades de los clientes que además de acceso a Internet buscan* ***conectividad entre sus redes de sucursales o puntos de presencia en forma privada*** *a menor costo, con servicios de valor agregado, desligándose de la operación de estas y acordando niveles de servicios* ***(Service Level Agredment SLA)****;*

Son el motivo del desarrollo de este documento, que brinda herramientas para la decisión en el momento de implementar VPNs más eficientes sobre sus redes proveedoras (Backbones), con menor costo y con visión de futuro.

En base al contexto planteado y a lo largo de este documento trataremos de ***comprender que tecnología adoptar*** *y cuales serán las ventajas y desventajas* ***teniendo en cuenta la evolución de las VPNs*** *y las tecnologías existentes para implementarlas.*

Justificación

Existen estándares variados de VPNs, papers y foros que discuten las diferentes tecnologías, muestran graficas teóricas e inducen al uso de la nueva tecnología en VPNs “VPN/MPLS”, por lo que es necesario realizar un estudio de esta tecnología y analizar el impacto de su implementación, medir los beneficios y desventajas de esta evolución.

El modelo de diseño de redes VPN/MPLS es necesario para comprender como esta tecnología puede ser implementada sobre casos reales de transmisión de voz y datos.

El desarrollo del modelo de diseño de redes VPN/MPLS, se realizará en base a ***pruebas de laboratorio*** y podrá utilizarse como base para el diseño de implementaciones en campo.

Limitaciones

El análisis de las tecnologías estudiadas y el modelo de diseño teórico para la implementación de VPN/MPLS, contiene:

- Comparación entre distintas tecnologías para soluciones de VPN y su evolución.
- Estudio profundo de MPLS/VPN.
- Estudio general de IPSec, Frame Relay y ATM.
- Seguridad sobre redes privadas virtuales.
- Calidad de servicio sobre VPN/MPLS (QoS VPN/MPLS).
- Estudio de Voz sobre IP.

El desarrollo del documento pretende:

- Generar un modelo de red y servicio general, el cual será flexible para poder extrapolarse a otros servicios particulares.
- Describir los resultados de las pruebas realizadas en laboratorio sobre tecnología Cisco System, que permitan avalar el caso teórico.
- Analizar el impacto de implementación se una red MPLS y la posibilidad de brindar VPNs sobre dicha red.

Para el trabajo de tesina se utilizarán RFCs, papers, draft y libros referidos a las tecnologías estudiadas.

Organización del documento

El documento se organiza en cuatro grandes capítulos y anexos:

- Capitulo I - Introducción a las redes privadas virtuales, un detalle de las nuevas necesidades de los clientes y un marco teórico que proporcionan un conocimiento a las VPNs/MPLS.
- Capitulo II - Comparación de los diferentes modelos de tecnologías para implementar VPNs, el cual permite identificar las ventajas y desventajas de MPLS.
- Capitulo III – Identificación de claves para migrar a la tecnología VPN/MPLS, tomando como base la migración desde una red tradicional del tipo Frame-Relay/ATM.
- Capitulo IV - Caso de estudio, sobre una red de un cliente que contiene la propuesta de migración de una red tradicional a una red VPN/MPLS.
- Capitulo V – Demostración de una red VPN/MPLS diseñada para tráfico de voz, vídeo y datos.
- Capitulo VI - Resumen
- Anexo I -Funcionamiento de MPLS. Este anexo fue confeccionado en base a teoría y su aplicación en un entorno de laboratorio.

Capitulo I – Introducción a las Redes Privadas Virtuales

Definición de red Privada virtual

Actualmente el termino VPN o red privada virtual puede aplicarse a varios conceptos, ya que dependiendo del contexto, una VPN puede ser entendida como una red empresarial o una simple conexión entre PCs. Si bien este termino entonces puede ser utilizado con diversos significados, este documento utiliza el termino VPN definiéndolo como una ***"red privada"*** que utiliza ***"virtualmente"*** los ***"recursos compartidos o públicos"*** de los proveedores de servicios.

Entonces una red privada (red dedicada, accedida y administrada por sus propietarios), esta constituida por recursos compartidos o públicos (enlaces dedicados, circuitos virtuales y VPNs IP) de los proveedores de servicios, por lo que estos últimos entienden a esa red privada como virtual por utilizar recursos compartidos.

Los proveedores de servicios (Service Providers) han brindado sus productos de redes privadas virtuales (VPN: Virtual Private Network) a sus empresas clientes desde la introducción de redes basadas en TDM y redes de conmutación de paquetes de datos X.25. Más recientemente, las redes basadas en Frame Relay y ATM con múltiples clases de servicios han remplazado al X.25 y líneas dedicadas como TDM. Los proveedores de servicios contaban entonces con productos de VPN con redes fijas o basadas en la tasa de utilización de sus vínculos.

El término de VPN ha sido utilizado por los proveedores de servicios para identificar circuitos virtuales de un grupo de usuarios desde la creación y desarrollo de los servicios por X.25, Frame-Relay y ATM. Recientemente, el término comenzó a utilizarse por administradores de redes de empresas para identificar un grupo cerrado de usuarios con IP privadas.

Por otro lado los clientes buscan unificar sus servicios de datos, voz y video. Ellos quieren servicios de administración de IP con servicios de nivel agregado (SLAs: Service-Level Agreements) y una calidad de servicio garantizada (QoS: Quality of Service).

La VPN basada en IP es rápidamente adoptada por la facilidad de consolidar servicios de datos, voz y video. Muchos proveedores de servicios están ofreciendo aplicaciones de valor agregado sobre la base del transporte de sus redes VPNs.

Servicios emergentes como e-commerce, hosting, Voz sobre IP y aplicaciones de multimedia podrían permitir a los proveedores de servicios generar nuevas ganancias y mantener una ventaja competitiva por un largo tiempo. Solamente dos arquitecturas de VPNs han evolucionado IP Security (IPSec) y Multiprotocol Label Switching (MPLS), estas tecnologías son diferentes pero complementarias.

La VPN IP es la base que las compañías pueden utilizar para desarrollar o administrar servicios de valor agregado, incluyendo aplicaciones y almacenamiento de datos de redes comerciales y servicios de telefonía.

En redes empresariales, las redes internas basadas en IP (Intranets) han cambiado fundamentalmente la forma en que las compañías conducen sus negocios. Las compañías están cambiando sus aplicaciones de negocio a sus Intranets para extenderse sobre redes de mayor alcance (WAN: Wide-Area Network). Las compañías están también adoptando la necesidad de sus clientes, proveedores, y socios utilizando Extranets (una Intranet que agrupa múltiples negocios). Con las Extranets, las compañías reducen los costos de de los procesos de negocios facilitando la automatización de los procesos. Para tomar ventaja

de sus oportunidades de negocio, los proveedores de servicios deben contar con una infraestructura de IP VPN que permita ofrecer servicios de redes privadas sobre una infraestructura compartida.

Este documento desarrolla el último concepto en redes privadas virtuales utilizadas por los proveedores de servicios ***VPN/MPLS,*** la tecnología en constante evolución que permite desarrollar redes privadas virtuales sobre redes IP en forma sencilla, con la ventaja de integrar todos los servicios IP y asegurar niveles de acuerdo de servicios con los clientes.

Necesidades de servicio

Servicios existentes

Los métodos para soportar los requerimientos de redes de datos privadas, consistieron por un largo tiempo de tecnologías como líneas privadas y frame relay. Los servicios brindados por estas tecnologías tienen sus ventajas y desventajas, detalladas en la siguiente tabla:

Tecnología	Ventajas	Desventajas
Líneas privadas	Los circuitos dedicados generan un alto grado de control, calidad de servicio, y un alto grado de seguridad para las empresas.	Mayores costos alternativos. Dificultad para crecer en volumen, requiere de circuitos dedicados desde cada sitio de la empresa hasta el resto de los demás sitios. Difícil administración, especialmente para redes complejas y grandes.
Frame Relay	Las empresas eligieron la naturaleza de "virtual" de Frame Relay para provisionar sus redes mas fácilmente y a un costo menor que las redes de líneas privadas. Por medio de una infraestructura pública, el tráfico es aislado. Las empresas perciben esto como seguro y rentable.	Son menos costosas que las líneas privadas, pero más costosas que las redes IP. No son muy escalables en redes grandes y se dificulta el manejo de circuitos virtuales permanente (PVCs). No es flexible para conectar entre Extranets o accesos básicos a Internet.

Tabla 1 – Redes tradicionales

Las empresas que mantienen sus redes de datos basadas en estos tipos de tecnologías, encuentran que estas desventajas señaladas en el cuadro anterior, pueden realmente estancar su crecimiento, debido a que las actuales tendencias impactan directamente a sus negocios:

- Presión sobre los costos: Reducción de costos de capacidad y operación; mejorando la eficiencia e incrementando la performance.
- Utilización de ancho de banda a bajo costo: Creciente demanda de banda a bajo precio, como son acceso a Internet por banda ancha utilizando tecnología DSL o cable.
- Incremento del desarrollo de aplicaciones de software basadas en IP: Crecimiento en aplicaciones basadas en IP, como aplicaciones de negocio, Web, e-mail y aquellas que permiten la implementación de voz y video sobre IP.
- Incremento en la interconexión de empresas: La necesidad de intercambiar información y aplicativos de software, que permiten el negocio entre empresas "business-to-business" y además utilizar esta posibilidad como una estrategia de diferenciación.

Estas tendencias son algunas de las tantas que abren un nuevo paradigma en la implementación de las redes privadas y por las cuales los proveedores de servicios están trabajando en ofrecer nuevos servicios.

Nuevos servicios

Actualmente, los proveedores de servicios de red están trabajando en soportar los nuevos requerimientos de sus clientes. Estos no solo requieren performance para los datos que ellos consideran críticos para su negocio, sino que también quieren soportar aplicaciones de tiempo real como lo son la voz y el video. La red además debe proveer de seguridad para la conectividad de todos los empleados, socios y

proveedores. Actualmente los clientes quieren todo esto y además reducir costos manteniendo el mismo nivel de seguridad.

Las redes del tipo MPLS le permitió a los Carriers y proveedores de servicios ofrecer a sus clientes, el transporte de sus redes de datos, ya no utilizando redes tradicionales de líneas privadas y Frame Relay/ATM, sino evolucionando a redes VPN-IP y permitiéndoles a estas empresas algunos de los siguientes beneficios:

- Conectividad any-to-any: La expresión any-to-any indica la facilidad de que los clientes interconecten cualquier de sus sitios entre ellos. Las empresas pueden interconectar centrales, sucursales y sitios remotos por medio de una VPN-IP.
- Nuevas aplicaciones: El protocolo IP habilita la evolución de las aplicaciones de software para transmitir datos, como lo son el e-mail, mensajería instantánea y Web. Pero adicionalmente IP provee un mecanismo para aplicaciones multimedia, como ser comunicaciones de voz, streaming de video, y entrega/distribución de contenido.
- Flexibilidad en el diseño de la red: Las empresas pueden cambiar sus tradicionales diseños de redes centralizadas “hub-and-spoke” hacia un diseño de todos los sitios interconectados en forma de maya “full-mesh”, para aplicaciones punto a punto “peer-to-peer“.
- Acceso remoto: Evita la utilización de llamadas del tipo internacional o del tipo 0800 para realizar conexiones dialup remotas y permitiendo realizar llamadas locales o arrendar acceso a Internet local para luego después ser parte de la VPN-IP.
- Interconexión con otras empresas: La conectividad entre empresas con relaciones del tipo sociedades o cliente-proveedor pueden ser conectadas en menor tiempo y con mayor flexibilidad conectando múltiples sitios utilizando una VPN IP que con una red tradicional. Adicionalmente, en las redes Frame-Relay/ATM esto podría requerir que ambas empresas estén subscriptas al mismo Carrier o proveedor de servicio. Utilizando VPN IP, cada empresa puede elegir su propio Carrier o proveedor de servicio.
- Seguridad: Los niveles de seguridad otorgados por una red tradicional, pueden ser iguales a los de una red del tipo VPN IP y con la ventaja que esta ultima esta en constante evolución permitirá nuevas herramientas para superarlas.

Marco Teórico

Antecedentes

En los últimos años Internet ha evolucionado en una gran red, inspirando además el desarrollo de una variedad de aplicaciones en negocios y mercados de consumo. Estas nuevas aplicaciones han conducido al incremento de la demanda de ancho de banda garantizado en el área principal de las redes (backbone) de los proveedores de servicios (Carriers y services providers).

El desarrollo inicial de Internet esta basado en el transporte de datos a través de la red; adicionalmente a los servicios tradicionales de datos provistos por Internet, nuevos servicios de voz y multimedia están siendo desarrollados y puestos en producción, e Internet ha emergido como la red de elección para proveer dichos servicios.

Por el contrario, las demandas aplicadas a la red en términos de velocidad y ancho de banda debido a las nuevas aplicaciones y servicios, han disminuido abruptamente los recursos existentes de la infraestructura de Internet. Adicionalmente al problema de los recursos, se presenta otro desafió relativo al transporte de bits y bytes sobre un “backbone” para proveer clases de servicios diferenciadas a los usuarios (CoS); por otro lado el crecimiento exponencial en el numero de usuarios y el volumen de trafico añade otra dimensión al problema.

En el esquema de las redes convencionales IP (IP packet forwarding), los routers analizan la dirección IP destino contenida en el encabezado de red de cada paquete a medida que el mismo atraviesa la red desde su origen hasta su destino final. Cada router analiza la dirección IP destino independientemente en cada sitio de la red. Los protocolos de ruteo dinámicos o las configuraciones estáticas dentro de los routers construyen la base de datos (tabla de ruteo o “routing table”) necesaria para determinar la dirección destino y consecuentemente su próximo destino o acción a tomar. El proceso implementado en el ruteo IP tradicional también se llama ruteo “unicast” salto por salto basado en destino (hop-by-hop destination-based unicast routing).

A pesar de ser exitoso y ampliamente desarrollado, ciertas restricciones que han sido detectadas tiempo atrás prevalecen en este método de envío de paquetes (forwarding packet) que disminuye la flexibilidad de la red. Por lo tanto nuevas técnicas son requeridas para contrarrestar los inconvenientes presentados y al mismo tiempo expandir las funcionalidades de la infraestructura de una red basada en protocolo IP.

Debido a los aspectos expuestos resulta evidente la necesidad de contar con redes basadas en tecnologías capaces de afrontar los aspectos mencionados y proporcionar resultados ventajosos.

Los aspectos económicos siempre presentan un papel importante en la selección e implementación de las redes de nueva generación. Los "Carriers" y "services providers" que poseen redes ATM (Asynchronous Transfer Mode) o Frame-Relay no están dispuestos a remplazar por completo su infraestructura, como consecuencia de esto, cualquier implementación de una tecnología de nueva generación deberá tener en cuenta la utilización de equipamiento y tecnologías existentes tales como ATM, Frame-Relay e IP.

MPLS (Multiprotocol Label Switching) o conmutación de etiquetas de múltiples protocolos es una tecnología emergente apuntando a solucionar las limitaciones presentes en las redes actuales bajo técnicas de "packet forwarding" (redes IP) tales como velocidad, escalabilidad, manejo de calidad de servicio (QoS), y manejo de trafico para mejora del rendimiento de la prestación de la red. MPLS proporciona manejo de ancho de banda y servicios requeridos para las futuras redes "backbone" (núcleos principales) basadas en Protocolo IP (Internet Protocol).

MPLS afronta asuntos referentes a la escalabilidad (habilidad para crecer en determinadas proporciones), ruteo basado en QoS y métricas de calidad de servicio; además posee la particularidad de soportar redes de enlaces (Capa 2 del modelo OSI) existentes tales como Modelo de Transferencia Asincrónica (ATM: Asynchronous Transfer Mode) y Frame-relay.

Evolución de las redes privadas virtuales

Los proveedores de servicios han estado ofreciendo servicios de VPN (Virtual Private Network) a sus clientes corporativos desde la concepción de las redes TDM (líneas dedicadas punto-a-punto) y las redes de paquetes X.25. Mas recientemente, dichas redes fueron reemplazadas por redes Frame-Relay y ATM con múltiples clases de servicio. El término de VPN ha sido empleado por los proveedores de servicios para identificar a los grupos cerrados de circuitos virtuales de usuario desde la creación de las redes X.25, Frame-Relay, etc.; y más recientemente, el término ha sido usado para identificar grupos de usuarios IP privados.

Los clientes corporativos han reconocido las ventajas que proporciona la tercierización del servicio "outsourcing" de sus redes de servicios IP y la consolidación de los servicios de voz, datos y video.

Al mismo tiempo, solicitan la administración de dichos servicios IP con acuerdos de nivel de servicio extremo a extremo (SLA: service-level agreements) y calidad de servicio garantizado (QoS).

La VPN IP ha estado convirtiéndose en la base de la provisión de servicios de voz, datos y video. Muchos proveedores de servicios se encuentran ofreciendo aplicaciones de valor agregado sobre sus redes VPN de transporte. Los servicios emergentes, tales como e-commerce, aplicaciones de hosting (almacenamiento), y aplicaciones de multimedia, permitirán a los proveedores de servicios generar una nueva ganancia incremental y mantener una ventaja competitiva a largo plazo. Dos tecnologías únicas y complementarias de arquitecturas de VPN tales como IPSec (IP Security) y MPLS (Multiprotocol Level Switching) forman la base predominante para la provisión de servicios consolidados.

La característica de VPN IP para MPLS permite desarrollar redes backbone de servicios escalables mediante VPNs de capa de red IPv4. Mediante una VPN IP una compañía puede desarrollar y administrar servicios de valor agregado, incluyendo aplicaciones de datos y servicios de telefonía para negocios.

En las redes corporativas las "Intranets" basadas en IP han cambiado la manera de conducir los negocios empresariales, las compañías están migrando sus aplicaciones comerciales hacia su Intranet para luego extender la misma hacia redes extendidas (WAN). Al mismo tiempo, las compañías unifican las necesidades de sus clientes, proveedores y socios por medio de la implementación de "Extranets", mediante las cuales, las compañías facilitan la reducción de costos de procesos de negocios, proporcionando cadenas de automatización, intercambio electrónico de la información (EDI), etc. Para tomar ventaja de esta oportunidad de negocio, los proveedores de servicios deberán poseer una infraestructura de VPN IP capaz de proporcionar servicios a redes probadas sobre una red compartida.

Introducción a las VPNS / MPLS

Esta sección detalla la tecnología de redes privadas virtuales basada en MPLS, apoyándose sobre la base de los conceptos específicos de la tecnología MPLS en el "Anexo I" del presente documento.

MPLS

Para comprender el funcionamiento de las VPNs MPLS, es necesario comprender MPLS. Si bien el detalle de funcionamiento es desarrollado en el *Anexo I* incluido en este documento, una breve introducción ayudará a comprender los principales conceptos.

El funcionamiento de MPLS se basa principalmente en el switcheo de etiquetas, un método mejorado

para el envió de paquetes o forwarding packets a través de una red empleando información contenida en las etiquetas adosadas a los paquetes IP. Dichas etiquetas son insertadas entre los encabezados de capa 3 (red) y los encabezados de capa 2 (enlace).

Básicamente MPLS identifica una dirección IP destino y le asigna una etiqueta en el primer router de la red, luego cada equipo dentro de la red se independiza de la dirección IP y solo se limita a conmutar las etiquetas hacia el ultimo router de la red, donde en este ultimo se conoce la dirección IP destino.

De esta forma MPLS se independiza de las largas tablas de rutas que los routers manejan en una red IP nativa y mejora la performance limitándose a conmutar etiquetas.

MPLS provee capacidades de ingeniería de trafico “Traffic Engineering” que permite direccionar el trafico en forma inteligente, VPNs (Redes Privadas Virtuales) y simultáneamente ofrece Calidad de Servicio (QoS) mediante la cual es posible asegurar envió de trafico critico sin perdida de paquetes y mínima latencia.

VPNs MPLS

Una red privada virtual (VPN: Virtual Private Network) consiste para todos los propósitos en un conjunto de sitios compartiendo en común información de ruteo de Capa 3. A pesar de que las VPNs MPLS son no-orientadas a la conexión, se combinan para construir las mismas, los beneficios de la Capa 2 con el paradigma de no-orientado a la conexión de Capa 3. Además, las VPNs MPLS ofrecen comunicaciones seguras permitiendo solo el intercambio de información entre los sitios que pertenecen a una VPN en común. Esto permite a los proveedores de servicios construir intranets y extranets, y brindar conectividad de Internet publica a estas VPNs por medio de una infraestructura en común que al mismo tiempo podría ofrecer servicios de ISP (Internet Service Provider), Frame-Relay o ATM.

La funcionalidad de VPN para el protocolo MPLS (Multiprotocol Label Switching) permite que la red del proveedor desarrolle servicios de backbone de VPNs en IPv4 escalables.

Las VPNs de nivel 3 brindan tres beneficios claves para las empresas: conectividad “any-to-any” utilizando tablas de ruteo, la posibilidad de utilizar el mismo plan de direccionamiento IP, y una gran escalabilidad entre sitios de las empresas y sus datacenters.

Operación de las VPNs MPLS

La Figura 1 detalla un ejemplo de una VPN desarrollada por un proveedor de servicios:

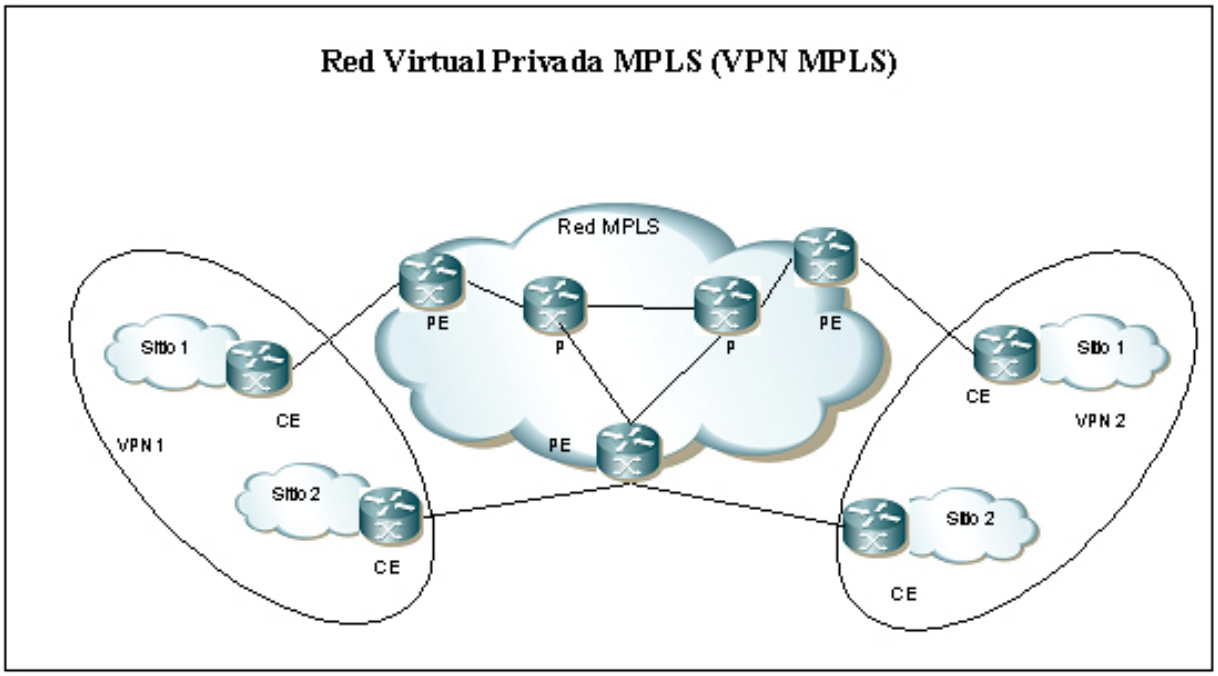


Figura 1 – Esquema de red VPN/MPLS

Los componentes de una red MPLS necesarios para construir una VPN resultan:

- MPLS core routers (P): también conocidos como (P: Provider router), se encuentran conectados en topología malla parcial o completa con otros LSRs P, y se conectan con interfaces al los routers de borde (PE: Provider edge); no contienen VPNs ni tampoco los clientes se conectan directamente a ellos.

- MPLS edge router (PE): también conocidos como (PE: Provider edge router), se pueden conectar con los P u otros PE. A ellos se conectan los clientes (CE) y son los que mantienen las rutas de las VPNs.
- Customer-Premises edge router (CPE): no necesitan emplear MPLS, con lo cual emplean métodos de ruteo convencionales, se conectan a los PE del proveedor, y son propiedad del mismo. Generalmente, los proveedores de servicios colocan dicho equipos en lugar de conectarse directo al CE con el PE para aprovechar la gestión sobre el enlace de acceso al PE.
- Customer edge router (CE): No necesitan emplear MPLS, con lo cual emplean métodos de ruteo convencional, y son propiedad del cliente.

La VPN contiene a los dispositivos conectados a los routers CPE (o CE), y estos a su vez pueden conectarse en cualquiera de los routers PE de la red del proveedor, ya que todos los PE se conectan entre si a través de una red (core) de routers P.

Instancia virtual de envió y ruteo

Cada VPN es asociada a una o varias instancias virtuales de envío y ruteo de VPN (VRF: Virtual Routing and Forwarding). Una VRF define a cual de las VPNs pertenecerá un cliente conectado a un router PE.

Una VRF consiste en una tabla de ruteo, un conjunto de interfaces que emplean la tabla de envío, y de un conjunto de reglas y parámetros de protocolos de ruteo que controlan la información de la tabla de ruteo anteriormente mencionada. No es necesaria una relación uno a uno entre un sitio y una VPN, sino que un sitio puede pertenecer a múltiples VPNs, como indica la Figura 2.

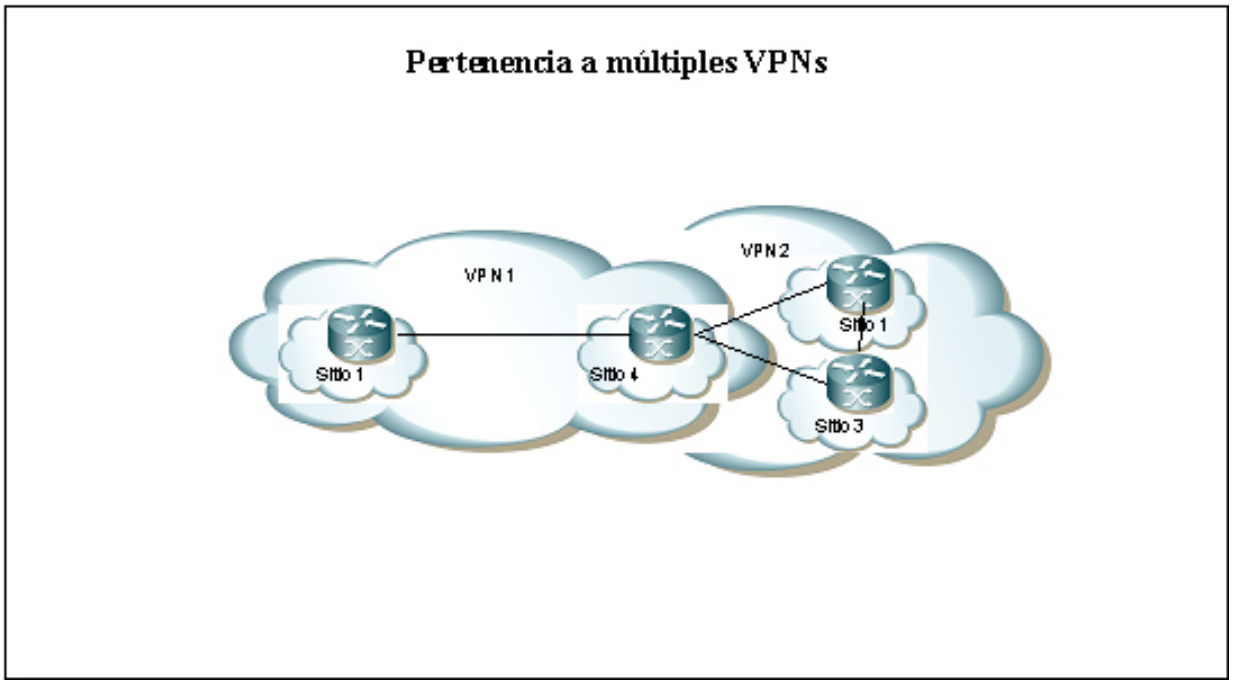


Figura 2 – Múltiples VPNs

La información de ruteo de paquetes se almacena en la tabla de ruteo IP de cada VRF, con lo cual, un conjunto de tablas de ruteo separadas es mantenido para cada VRF. Dichas tablas previenen, en primera instancia, que la información sea enviada fuera de la VPN. Por otro lado, las VRFs son empleadas para enviar información dentro de una VPN, y cada combinación de VRFs contiene rutas que pertenecen a una o varias VPNs.

Resulta necesario que cada cliente dentro de una VPN mantenga la unicidad del espacio de direcciones, y para el caso en el cual dos clientes de VPNs que deciden combinarse para formar una extranet por medio de la importación y exportación de rutas, deberán también conservar la unicidad, o de existir solapamiento de direcciones deberá emplear NAT en el punto de contacto entre ambas.

Las interfaces de los routers PE son asociadas con VRFs individuales; la información de ruteo aprendida a través de dichas interfaces es asociada a las VRFs configuradas y es conocida como el contexto de ruteo.

Distribución de rutas de VPNs

Los routers PE emplean el protocolo de ruteo BGP para distribuir las rutas de las VPNs entre cada router. Un router con BGP puede instalar y distribuir una ruta a un solo prefijo por defecto.

Queda claro que necesitamos permitir que BGP instale y distribuya múltiples rutas a un solo prefijo IP, y además necesitamos asegurar una política que determine que sitios pueden emplear que ruta. Todas estas metas se alcanzan por medio del empleo de una familia de direcciones.

Las extensiones del Multiprotocolo BGP (MBGP) permiten al protocolo BGP convencional transportar rutas desde múltiples familias de direcciones. Se introduce aquí la noción de VPN-IPv4 address family, donde una VPN-IPv4 consiste en un valor de 12 bytes, donde los 8 primeros bytes corresponden al Route Distinguisher (RD), y siguen 4 bytes de una dirección IPv4.

En el caso de que dos VPNs empleen el mismo prefijo IP, los PEs trasladan estos prefijos a una unívoca dirección VPN-IPv4, asegurando que si un mismo espacio de direcciones es empleado en dos VPNs distintas, cada una de ellas mantenga su unicidad intacta y en forma independiente de la otra.

BGP propaga información de conectividad de prefijos VPN-IPV4 para cada VPN mediante extensiones del Multiprotocolo BPG (MB-iBGP), los cuales definen el soporte adicional de familias de direcciones que sean IPv4. Esto asegura que las rutas de una VPN dada sean aprendidas solo por los miembros de la misma, permitiendo así la comunicación entre ellos.

VPNs nivel 3 basadas en MPLS están definidas en el RFC 2547bis, publicado por el Internet Engineering Task Force (IETF) L3VPN working group. Este RFC define VPNs basadas en el uso del protocolo de ruteo BGP para distribuir etiquetas de VPN (ver próxima figura). Los routers de borde (PE) activan sesiones BGP entre ellos, en el caso de la figura se ejemplifican dos routers de bordes. El Label Distribution Protocol (LDP) será el encargado de distribuir las etiquetas en el núcleo de la red (core). También en el core, el envío y ruteo de VPN llamada “tablas VRF” son derivadas de las tablas globales de ruteo las cuales residen en cada router.

Con este método una VRF es asignada a cada cliente; por ende cada router de borde (PE) contendrá una tabla de ruteo global y varias tablas VRF, por lo que en una misma conexión el proveedor de servicios o Carrier puede ofrecer Internet y servicios de VPN.

Cuando el trafico arriba sobre una VPN, la decisión de envió se realiza acorde a la VRF asociada. El tráfico de Internet podría permanecer siendo ruteado usando la tabla de ruteo global.

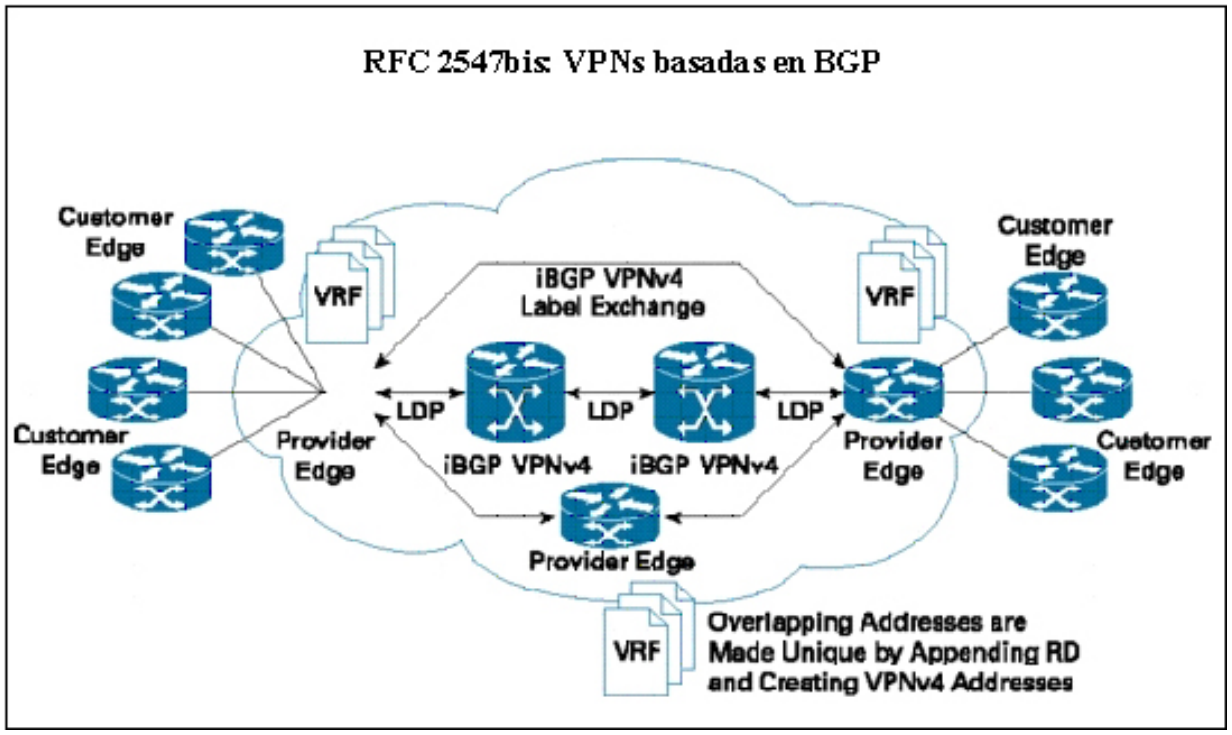


Figura 3 – Esquema VRF

Comunidades para las rutas objetivo de VPNs

La distribución de información de ruteo de una VPN es controlada a través de comunidades para las rutas objetivo de VPNs (VPN route target communities), implementado por medio de las comunidades de BGP extendido. La distribución de información de ruteo funciona de la siguiente manera:

Cuando una ruta aprendida desde un CE es inyectada dentro del MP-iBGP, asociándole una lista de atributos de comunidad extendida para las rutas objetivo de la VPN, y el atributo para dicha ruta es transportado en MP-iBGP hacia otros routers PEs. Típicamente, dicha lista de los valores de comunidad de ruta objetivo (route target community values) es configurada de una lista de exportación de rutas objetivo asociada con la VRF de donde la ruta provino.

Cada VRF, a su vez, es asociada a una lista de importación de comunidades extendida para rutas objetivo. La lista de importación define los atributos de comunidad extendida que una ruta debe tener para poder ser importada dentro de dicha VRF desde MP-iBGP en un router PE, por ejemplo, la lista de importación de una VRF particular incluye las comunidades objetivo de rutas A, B, y C, y cualquier ruta de una VPN que transporte dicho atributo de comunidad extendida A, B o C será importada dentro de la VRF.

Distribución de información de rutas de una VPN

Las posibles técnicas de distribución de información de rutas entre dispositivos PE y CPE (o CE) son enumeradas a continuación:

- Ruteo estático: realizado por configuración, y muy empleado en VPNs con un único punto de salida.
- Ruteo RIP: El router CPE (o CE) y PE establecen una vecindad RIP, y el CPE (o CE) emplea RIP para publicar al router PE el conjunto de prefijos que son alcanzables desde el sitio donde se encuentra.
- Ruteo OSPF: El router CPE (o CE) y PE establecen una vecindad OSFP, y el CPE (o CE) emplea OSPF para publicar al router PE el conjunto de prefijos que son alcanzables desde el sitio donde se encuentra. Esta técnica solo deberá emplearse para VPNS con un único punto de salida.
- Ruteo BGP: El router CPE (O CE) y Pe establecen una vecindad BGP, y el CPE (O CE) emplea eBGP (external BGP) para publicarle al router PE el conjunto de prefijos que son alcanzables a través de el. Esta técnica es empleada tanto para VPNs con un único punto de salida como para VPNS de transito.

Desde la perspectiva técnica, el método de distribución mediante BGP resulta el más apropiado debido a:

- No requiere que el PE corra múltiples instancias de algoritmo de protocolo de ruteo para comunicarse con el CPE (o CE), como es requerido en los protocolos IGP (Interior Gateway Protocol).
- BGP fue explícitamente diseñado para la función de transporte de información de ruteo entre sistemas manejados por distintos administradores.
- Si el sitio contiene otra conexión BGP hacia otro router que no sea el PE (BGP backdoors), el correcto ruteo funcionará en cualquier circunstancia. Los demás métodos pueden no funcionar dependiendo de las circunstancias.
- El empleo de BGP facilita al CPE (O CE) pasarle al PE atributos de rutas, como por ejemplo, sugerir un objetivo particular para cada ruta dentro del rango de atributos autorizados en el PE vecino.

El empleo de CPE como salida de la red de routers del cliente (CEs) hacia el PE evita que el cliente deba interiorizarse con el protocolo de ruteo BGP (salvo que el cliente sea un ISP); el cliente solo deberá preocuparse por enviar las rutas que le interese ser transportadas a través del backbone MPLS.

BGP es un protocolo extremadamente escalable que soporta la provisión de un gran número de VPNs.

El protocolo BGP también soporta el intercambio de información de rutas entre routers que no se encuentren directamente conectados (la conectividad entre dispositivos es provista en ese caso por IGP).

Envío MPLS

Basándose en la información de ruteo almacenada en la tabla de ruteo IP VRF, los paquetes son enviados hacia su destino empleando MPLS.

El router PE vincula una etiqueta con cada prefijo aprendido desde el router CPE (o CE) e incluye la etiqueta en la información de conectividad de red (información de vinculación) para los prefijos que son advertidos a otros routers PE. Cuando un router PE envía un paquete recibido desde un router CPE a través de la red, marca al mismo con la etiqueta que recibe del router de destino (en realidad el próximo salto hacia la red destino). Cuando el routers PE destino recibe el paquete etiquetado, remueve la etiqueta y la emplea para determinar el router CPE (o CE) correcto al cual enviar dicho paquete.

Nota: Los routers P no son parte del proceso MP-iBGP, y no transportan información de las VPNs. Los routers P envían paquetes basándose en los valores de las etiquetas adosadas a los paquetes IP. A pesar de que los routers P participan en el intercambio de etiquetas, no terminan VPNs MPLS.

El protocolo LDP de MPLS asegura que todos los routers PE reciban las etiquetas asociadas a las diferentes rutas contenidas dentro de cada router PE, y una red MPLS se encuentra lista para transmitir paquetes cuando el router *PE de ingreso* recibe una etiqueta para el router *PE de salida*.

El envío basado en etiquetas dentro de la red backbone del proveedor se sustenta en la conmutación dinámica de etiquetas. Un paquete de datos de un cliente entonces transporta dos niveles de etiquetas; el primer nivel se emplea para enviar el paquete al próximo salto (hop) correcto, y la segunda etiqueta indica la VRF asociada con la internase de salida hacia el CPE (o CE) destino. El mecanismo de dos niveles de etiquetas es comúnmente llamado conmutación jerárquica de etiquetas (hierarchical label switching).

Cuando un paquete IP es recibido a través de una interfase particular desde el CPE (o CE), el PE lo asocia a una VRF y obtiene una etiqueta relacionada con el router PE de salida (el cual identifica la VRF objetivo y la interfaz saliente en el router PE destino: etiquetado de fondo de pila). El router Pe obtiene de la tabla de ruteo global otra etiqueta (tope de pila) que apunta al próximo salto (generalmente un router P), y combina ambas etiquetas en una pila de etiquetas MPLS. Dicha pila es asociada al paquete de la VPN y enviada hacia el próximo salto. Los routers P en la red MPLS examinan la etiqueta de tope y envía el paquete correctamente a través de la red hacia el próximo salto.

El router PE de salida es el encargado de quitar la etiqueta de tope y examinar el fondo de la pila (segunda etiqueta), que identifica la VRF objetivo y la interfaz de salida. La etiqueta del fondo de la pila es extraída y el paquete IP es enviado hacia el correcto router CPE (o CE).

Esquema de VPN/MPLS – Comprendiendo el funcionamiento

Este apartado trata de describir y detallar como un proveedor de servicios o Carrier maneja el tráfico de diferentes VPNs sobre un backbone MPLS. En principio se debe tener en cuenta que dicho backbone brinda servicios de Internet y al mismo tiempo servicio a múltiples VPNs. Las descripciones y figuras siguientes ayudarán a comprender como es el esquema de VPN/MPLS y como esta tecnología separa, envía y rutea el trafico de cada VPN.

Las siguientes políticas describen el diseño de conectividad entre los sitios:

- Cualquier host en el Sitio 1 puede comunicarse con cualquier host en el Sitio 4.
- Cualquier host en el Sitio 2 puede comunicarse con cualquier host en el Sitio 5.
- Cualquier host en el Sitio 3 puede comunicarse con cualquier host en el Sitio 6 y 7.
- Cualquier host en el Sitio 4 puede comunicarse con cualquier host en el Sitio 1.
- Cualquier host en el Sitio 5 puede comunicarse con cualquier host en el Sitio 2.
- Cualquier host en el Sitio 6 puede comunicarse con cualquier host en el Sitio 3 y 7.
- Cualquier host en el Sitio 7 puede comunicarse con cualquier host en el Sitio 3 y 6.

Asumiendo que la red de Carrier es MPLS y por lo tanto utiliza LDP dentro del backbone y entonces establece caminos LSPs para comunicarse entre PE. La etiqueta que se muestra en el ingreso de cada router PE, es la asociada con la ruta que este usa para enviar tráfico a los routers PE remotos.

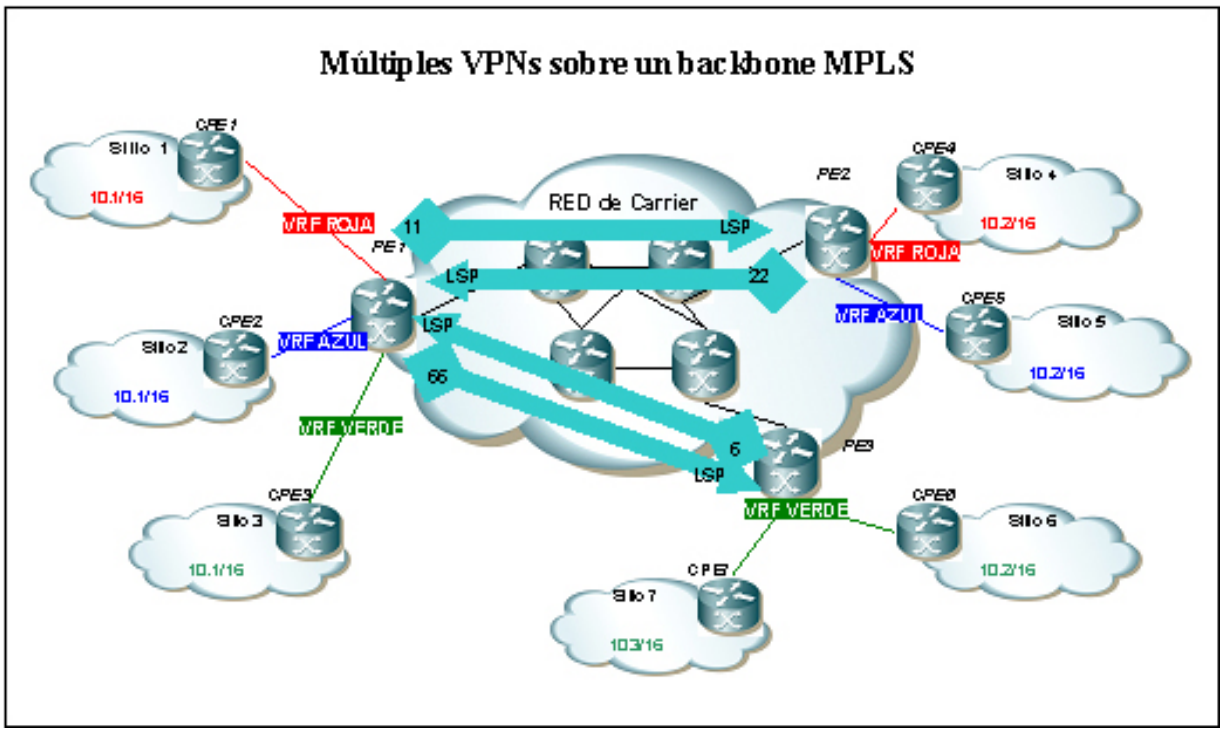


Figura 4 – Detalles de etiquetas

- Asumiendo que el PE1 asigna la etiqueta 1001 para las rutas aprendidas desde el Sitio 1, la etiqueta 1002 para las rutas aprendidas desde el Sitio 2, y la etiqueta 1003 para las rutas aprendidas desde el Sitio 3. Entonces PE1 instala tres rutas MPLS tales que cuando un paquete con la etiqueta 1001, 1002, o 1003 son recibidas desde el backbone, este puede simplemente quitar la etiqueta y enviar el paquete de IPv4 directamente al CE1, CE2, o CE3 basándose en la etiqueta del paquete.
- Asumiendo que el PE2 asigna la etiqueta 1004 para las rutas aprendidas desde el Sitio 4 y la etiqueta 1005 para las rutas aprendidas desde el Sitio 5. Entonces PE2 instala dos rutas MPLS tales que cuando un paquete con la etiqueta 1004, o 1005 son recibidas desde el backbone, este puede simplemente quitar la etiqueta y enviar el paquete de IPv4 directamente al CE4, o CE5 basándose en la etiqueta del paquete.
- Asumiendo que el PE3 asigna la etiqueta 1006 para las rutas aprendidas desde el Sitio 6 y la etiqueta 1007 para las rutas aprendidas desde el Sitio 7. Entonces PE3 instala dos rutas MPLS tales que cuando un paquete con la etiqueta 1006, o 1007 son recibidas desde el backbone, este puede simplemente quitar la etiqueta y enviar el paquete de IPv4 directamente al CE6, o CE7 basándose en la etiqueta del paquete.

Teniendo en cuenta entonces que cada router PE aprende y envía al resto de los router PE las tablas asociadas a cada VRF. En la figura siguiente se muestra un ejemplo de las tablas de ruteo del PE1.

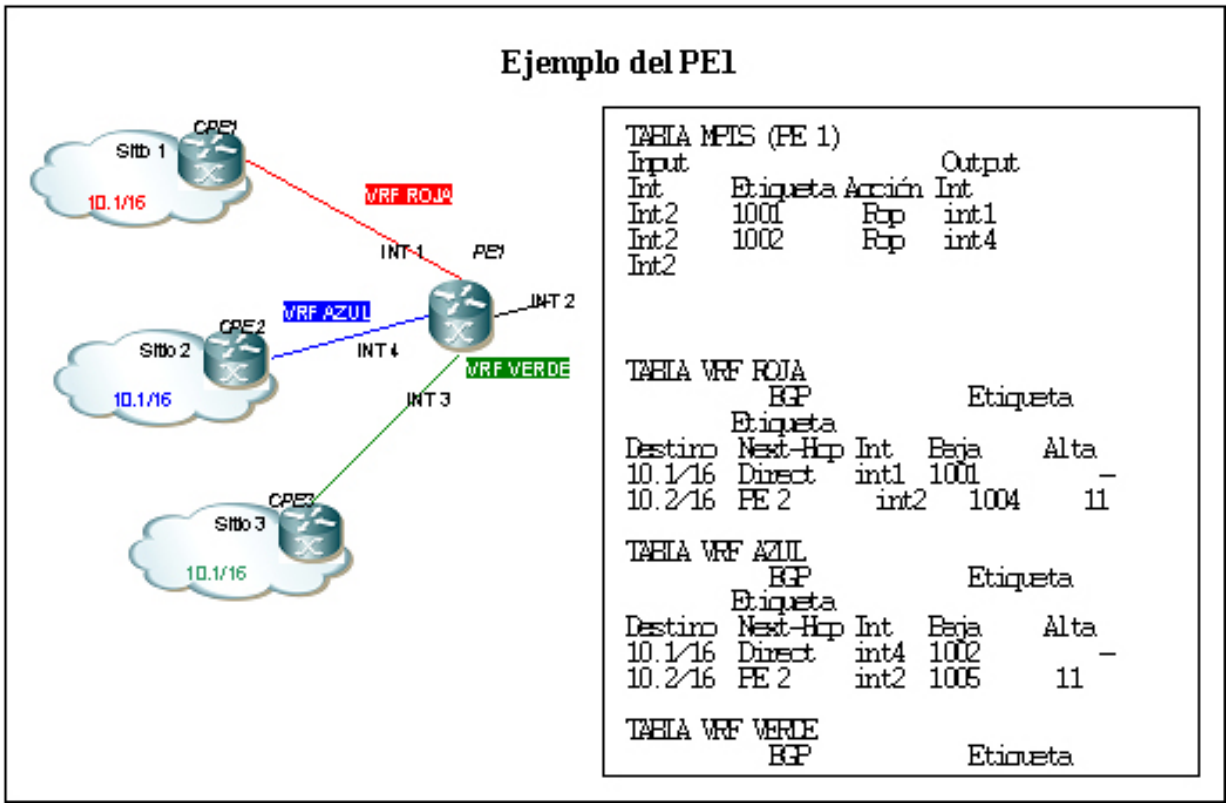


Figura 5 – Tablas de enrutamiento

Para comprender entonces como el router PE1 envía y recibe tráfico por una VPN, el siguiente ejemplo detalla el manejo de etiquetas dentro del backbone MPLS y en cada sitio extremo de la red de la VPN.

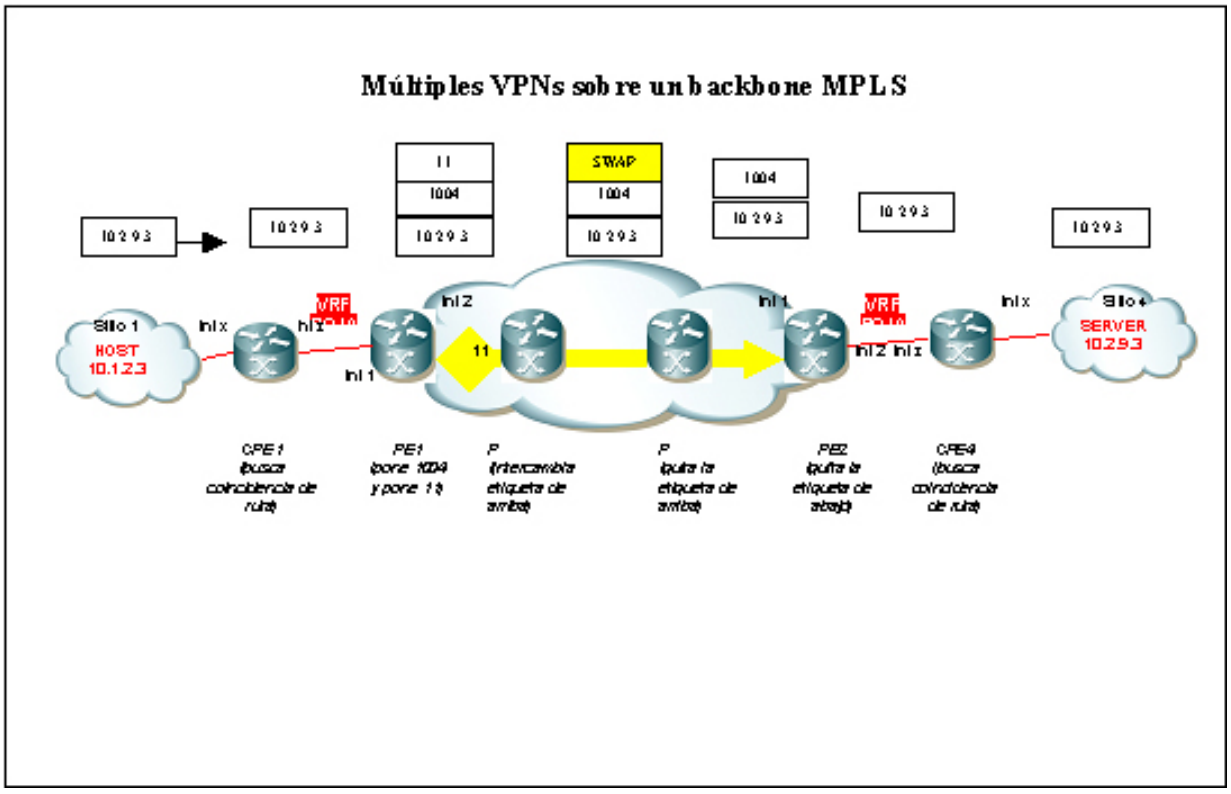


Figura 6 – Intercambio de etiquetas

Cuando el paquete nativo IPv4 llega al CPE1, este realiza una búsqueda en la tabla de ruteo en su tabla de envíos. La mejor coincidencia dentro de la tabla de envíos es la siguiente.

Destino	Next-Hop	Interface
10.2/16	PE 1	intz

Como resultado de esta coincidencia, CPE1 envía el paquete IPv4 nativo sobre la interface intz al PE1. PE1 recibe el paquete IPv4 nativo sobre la interface int1. Todos los paquetes que arriban a la interface int1 son asociados con la VRF ROJA, entonces PE1 ejecuta una búsqueda en la tabla de ruteo de la VRF ROJA. La entrada de la tabla de la VRF ROJA que mejor coincide es

BGP Destino	Next-Hop	Interface	Etiqueta Baja	Etiqueta Alta
10.2/16	PE 2	int2	1004	11

Como los paquetes de salida por la interface int2 no están asociados con la VRF local, el paquete debe viajar al menos por un salto (hop) a través del backbone MPLS. Entonces PE1 crea una cabecera para el paquete y entonces agrega la etiqueta (1004)- asignada por el PE2 cuando este originalmente envió su ruta 10.2/16 - sobre la etiqueta baja. PE1 agrega la etiqueta de arriba (11) para el LSP desde PE1 hasta PE2.

El paquete es entonces enviado hacia el primer router de transito P. El backbone MPLS conmuta los paquetes etiquetados a lo largo del LSP, intercambiando la etiqueta de arriba en cada salto, hasta llegar al penúltimo router hacia PE2. En el penúltimo router, se quita la etiqueta de arriba y el paquete con una sola etiqueta (1004) es enviada a PE2.

Cuando PE2 recibe el paquete etiquetado sobre la interface int1, este hace una búsqueda sobre la tabla de ruteo de MPLS, La entrada de la tabla de ruteo de MPLS coincide con.

Input			Output
Interface	Label	Action	Interface
Int1	1004	Pop	int2

Como resultado de esta búsqueda, PE2 quita la etiqueta (Proceso POP) y envía el paquete IPv4 nativo sobre la interface int2 hacia el CPE4.

Cuando el paquete IPv4 nativo llega al CPE4, este realiza una búsqueda en su tabla de envíos. La entrada que tiene mayor coincidencia es la siguiente.

Destino	Next-Hop	Interface
10.2/16	Direct	intx

Como resultado de esta búsqueda, el CPE4 envía el paquete sobre la interface intx al servidor 10.2.9.3 en el Sitio 4.

Convergencia de datos y voz

En la actualidad los servicios de voz son soportados en su mayoría sobre redes de telefonía basadas en la conmutación de circuitos (circuit-switched), al mismo tiempo los servicios de datos son soportados sobre redes basadas en la conmutación de paquetes (packet-switched). Al mismo tiempo los Carriers mantiene en servicio ambas redes duplicando costos de mantenimiento, ampliaciones y costos operativos.

Si bien los servicios de telefonía tradicional están desplegados en forma masiva, este tipo de servicio no puede ofrecer servicios de valor agregado por el tipo de redes (redes antiguas y pensadas para el servicio de telefonía básica) donde se encuentran desplegados. Sumándole a esto los altos costos que requiere una actualización de este tipo de redes, los Carriers se ven limitados a pensar en un cambio.

Como contrapartida las redes de datos, permiten adaptarse para crear servicios de valor agregado y dejando de lado los costos, que sobre este tipo de redes son menores debido a la simplificación de la tecnología y la gran cantidad de proveedores.

Los Carriers comenzaron a pensar en la integración de servicios de telefonía y datos sobre una misma red permitiendo sobre todo la creación de una nueva cartera de productos como:

- Mensajería integrada (e-mail/voice mail),
- Call Centres basados en Web,
- integración de la telefonía mediante la PC,
- telefonía mediante intranet e internet,
- fax.

Los beneficios de una única infraestructura de red:

- Reducir los costos de WAN,
- Eliminación de PBX,
- Simplificar la operación,
- Budget compartido,

Todos los Carriers tienen el mismo objetivo, unificar sus redes para diversificar los servicios, pero existen diferentes tecnologías para lograr la unificación y es necesario comprender como migrar el servicio de voz tradicional a un servicio de voz sobre redes de datos. En los siguientes puntos dentro de esta sección se desarrollaran los conceptos básicos para comprender el impacto de la migración.

Hacia la convergencia

Es preciso comprender que las redes de telefonía tradicionales contaban con circuitos dedicados (TDM). Con este tipo de redes el servicio es garantizado end-to-end, pero los recursos de red no son utilizados constantemente por lo que el manejo de ancho de banda es ineficiente.

Las redes basadas en paquetes permiten multiplexar estadísticamente haciendo más eficiente la utilización de ancho de banda.

Convirtiendo la voz en datos

El proceso de convertir la voz (analógica) como una señal de datos (digital), se realiza utilizando CO-DEC (codificador-decodificador) que convierte la señal de analógica a paquetes de datos digitales para ser transportados sobre una red de datos.

El chip Digital Signal Processing (DSP) comprime el paquete para ser transmitido sobre una red de datos. El mismo procedimiento pero descomprimiendo se realiza en el camino inverso.

Figura 7 – Voz a Datos

Existen diversos CODEC que pueden utilizarse, el más utilizado es el G.729 debido a su relación ancho de banda/ calidad.

Voz paquetizada

La paquetizacíon de voz (transmitir la voz en paquetes) fue posible desde el momento que las redes de comunicaciones comenzaron a ser más rentables, con la introducción de circuitos digitales que ofrecieron buena performance libre de errores. Además de la incorporación de equipamiento que permitió disminuir el delay (retardo), recuperar y retransmitir datos perdidos.

La paquetización permite cursar tráfico de voz sobre redes preparadas para transportar datos, permitiendo con la codificación digital de señales analógicas un uso más eficiente del ancho de banda.

Para cursar tráfico de voz sobre redes de datos se deben tener en cuenta los siguientes puntos:

- Delay (retardo): Tiempo que insume un paquete en ser transportado por la red hasta el destino. La recomendación G.114 de la ITU considera los siguientes rangos de delay sobre una red para aplicaciones de voz, según tabla siguiente:

Rango en milisegundos	Descripción
0 – 150	Aceptable para las aplicaciones de voz
150 – 400	Aceptable teniendo en cuenta que los administradores son consientes del tiempo de transmisión y el impacto que este tiene sobre la calidad de las transmisiones de aplicaciones de voz
Mayor a 400	Inaceptable

Tabla 2 – Delay aceptable para VoIP

Nota: Estas recomendaciones están orientadas a administradores de redes utilizadas para transito de voz nacional e internacional. Para redes privadas 200ms es un delay aceptado y con un límite superior de 250ms.

- Jitter (variación): La variación del delay (retardo) en la recepción de paquetes. Es decir, la fuente emisora generará un stream continuo de paquetes, espaciados entre sí por un intervalo de tiempo constante. Luego, por congestión en la red, por algún mal diseño de las colas de los elementos de red o por velocidades de los enlaces, esta continuidad en el espaciado de los paquetes se ve alterada. A esta variación en el retardo se la denomina Jitter.
- Packet Loss: Es la pérdida de paquetes de voz a lo largo del transito por la red. Esta perdida de paquetes degrada severamente la calidad de la voz. Cuando se pierdan algunos paquetes, los equipos de voz interpolarán entre los últimos paquetes recibidos y crearán un paquete de voz que hace que el stream de audio sea constante. Cuando la pérdida de paquetes excede un umbral esto ya no es posible y la calidad de la voz sufre una degradación importante. Según recomendaciones de diseño la perdida de paquetes sobre una red para aplicaciones voz debe ser menor al 1 por ciento $P \leq 1\%$. En la siguiente figura esquematiza los tres parámetros de calidad de voz:

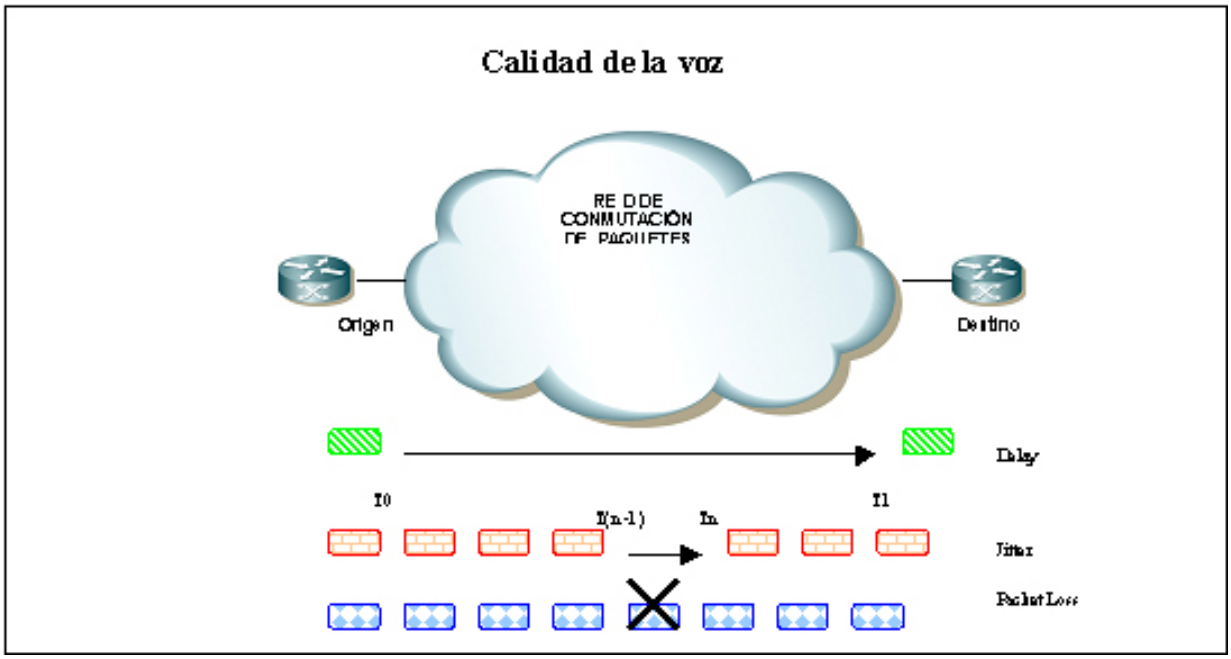


Figura 8 – Calidad de VoIP

Priorización de paquetes de voz

Teniendo en cuenta las premisas básicas para mantener una buena calidad de voz, las redes de datos necesitan de un manejo especial para este tipo de paquetes. En particular MPLS maneja una arquitectura de calidad de servicio que le permite identificar, marcar y encolar el trafico de voz en forma prioritaria; de esta forma los paquetes de voz será despachados con bajo delay y sin perdida de paquetes.

Calidad de servicio (quality of service)

En orden de manejar las diferentes aplicaciones y servicios como ser streaming de video, voice over IP, e-commerce y otras; una red requerirá de Calidad de Servicio (QoS). Las diferentes aplicaciones tienen necesidades de delay, variación de delay (jitter), bandwidth, packet loss y disponibilidad. Estos parámetros son la base de QoS.

Así como las redes IP, MPLS permite manejar calidad de servicio y si bien existen varias alternativas de implementación en este documento, se elegirá el modelo conocido como DiffServ.

Para comprender rápidamente la diferencia con el otro modelo IntServ, este requiere de señalización punta a punta (end-to-end) para reservar el ancho de banda y asegurar la calidad de servicio. De esta forma los hots (PCs, dispositivos, teléfonos IP, etc) necesariamente deben soportar este mecanismo de reserva de QoS. El mecanismo de reserva es RSVP (Resource Reservation Protocolo).

Entre los problemas de implementación de IntServ se encuentran:

- Todos los dispositivos, incluidos los host, requieren de la utilización de RSVP.
- La actualización de cada reserva se realiza mediante “soft”, por lo que debe refrescarse constantemente y agrega tráfico a la red.
- Mantener el estado de reservación en cada router y cada control de admisión, incrementa la utilización de memoria y suma complejidad a la red.
- Cada flujo de tráfico debe tener una reservación, mantener estas reservaciones en gran escala (cientos de millones de flujos) genera un gran costo de red.

Cuando nos referimos al modelo DiffServ no requiere la implementación de una señalización, y simplemente se limita a categorizar trafico en diferentes clases - llamadas Clases de Servicios (CoS) - aplicándole parámetros de QoS a estas clases. El proceso de QoS en DiffServ pasa por las siguientes etapas:

- Clasificación

Se eligen los paquetes por determinado patrón (protocolo de transporte, port, IP, etc.) y se los clasifica para luego ser marcados. Por ejemplo los paquetes con el puerto UDP 2021 pueden ser clasificados como puertos de VoIP.

- Marcado

Una vez clasificados los paquetes son marcados, para realizar esto los paquetes son en principio divididos en clases marcando el byte de Type of Service (ToS) sobre el encabezado de IP. En este docu-

mento elegimos el marcado por DSCP (Differentiated Services Code Point), utilizando los primeros 6 bits del campo ToS de IP. El marcado se realiza según la siguiente tabla.

Clase	DSCP
Reserved for control plane traffic	Class Selector 7
Reserved for control plane traffic	Class Selector 6
Class 1 (real-time traffic)	EF
Class 2	Class Selector 4
Class 3 (conforming traffic)	AF31
Class 3 (exceeding traffic)	AF32
Class 3 (violating traffic)	AF33
Class 4 (best effort)	Default

- Encolado

A cada marcado se le asignará una cola de despacho de paquetes, en el case de DiffServ se definen:

  - Low Latency Queue (LLQ): Esta cola es de lata prioridad y despacha los paquetes con la mínima latencia y asegura el despacho de todos los paquetes reservando un ancho de banda mínimo preestablecido para ese tipo de tráfico. Posee mecanismos para no superar un máximo ancho de banda, de esta forma se evita la canivalización de este tipo de tráfico.
  - CBFQ: Esta cola permite tomar ancho de banda sobre varias clases definidas. El ancho de banda puede ser reservado para cada clase. En caso de excedente de tráfico sobre la cola comienza a poner los paquetes en buffer hasta descartar paquetes.
  - Default Queue: Esta cola recibe todos los paquetes marcados con el DSCP en “000000” y es la cola de menor prioridad. Habitualmente esta cola se utiliza para tráfico de Internet. En caso de excedente de tráfico descarta paquetes.

Comprendido el concepto de DiffServ solo resta comprender que hace MPLS con la calidad de servicio. Como el marcado de los bits de clasificación se realiza en los bordes de la red, en donde no hay MPLS, a nivel IP el campo DSCP es marcado y encolado desde un router CE hacia el router PE de MPLS. Cuando el router primer router PE MPLS toma el paquete IP, este mapea el campo DSCP al campo EXP de MPLS. Un simple mapeo mantiene la calidad de servicio dentro de la red MPLS y manteniendo todos los conceptos de DiffServ.

La siguiente tabla detalla el mapeo entre DSCP y EXP en MPLS.

DSCP	EXP
Class Selector 7	7
Class Selector 6	6
EF	5
Class Selector 4	4
AF31	3
AF32	2
AF33	1
Default	0

Para comprender los conceptos se adjunta un esquema de Calidad de Servicio, en el cual se ejemplifican tres clases de trafico y como cada elemento de la red trata los paquetes IP/etiquetes MPLS.

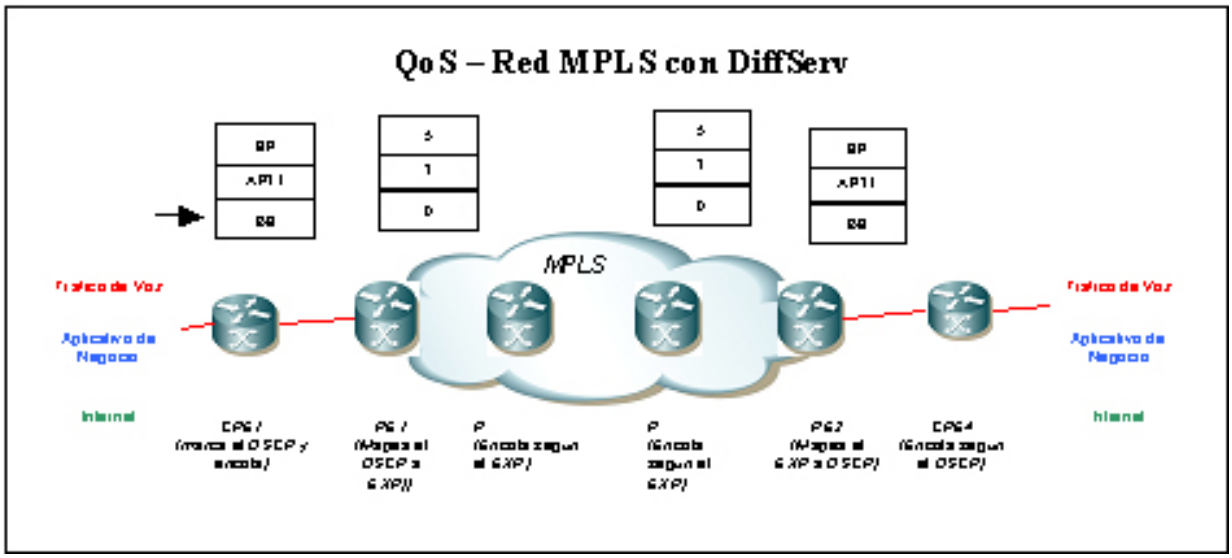


Figura 9 – QoS con DiffServ

La fácil implementación de mecanismos de calidad de servicio sobre una red MPLS, facilita la implementación de diferenciación de tráfico y la implementación de servicio de datos, voz y video.

Capitulo II – Comparación de Redes Privadas Virtuales

Modelo de redes privadas virtuales

Existen diferentes modelos de redes privadas virtuales dependiendo del tipo de red de transporte, estos diferentes modelos limitan o amplían las posibilidades de generar nuevos esquemas de servicios. A continuación se detallan los diferentes modelos que permitirá un mayor entendimiento de los diferentes modelos.

VPNS orientadas a la conexión

Las VPNs orientadas a la conexión pueden ser constituidas sobre infraestructuras de Capa 2 o 3. Ejemplos de redes VPNs orientadas a la conexión de Capa 2 son las redes punto a punto en modelo overlay, como lo es Frame-Relay y las conexiones virtuales de ATM. Por otro lado, las VPNs construidas mediante túneles IPSec (con encripción para garantizar privacidad) de malla completa o parcial corresponden a ejemplos de redes de Capa 3 orientadas a la conexión.

Las VPNs de acceso son orientadas a la conexión mediante circuitos conmutados que proveen una conexión segura para el acceso remoto entre individuos (usuarios móviles y viajeros) y una red extranet o intranet corporativa a través de la red compartida de un proveedor de servicios.

Las deficiencias de las VPNs orientadas a la conexión radican en su escalabilidad, específicamente dichas VPNs en caso de no contar con conexiones de malla entre sus sitios ocasionan ruteo deficiente.

VPNs orientadas a la conexión de Capa 2

Dichas redes están formadas sobre la base de una modelo VPN overlay. En dicho modelo, el proveedor de servicios proporciona los circuitos virtuales y la información de ruteo es intercambiada directamente entre los routers del cliente “CPE”.

Para las redes basadas en TDM los proveedores de circuitos ofrecen a sus clientes corporativos redes de líneas privadas mediante líneas punto a punto dedicadas. Este proceso involucra el multiplexado digital, en donde dos o más ráfagas de bits aparentemente simultáneas son derivadas en sucesivos canales inter-espaciados (circuitos E1 o E3), y transportadas en forma hacia su destino. Tal como muestra la Figura 7, los clientes A y B comparten la misma infraestructura física del proveedor o Carrier, aunque se encuentran lógicamente separados entre si mediante mapeos de puertos y conexiones electrónicas cruzadas realizadas por el proveedor.

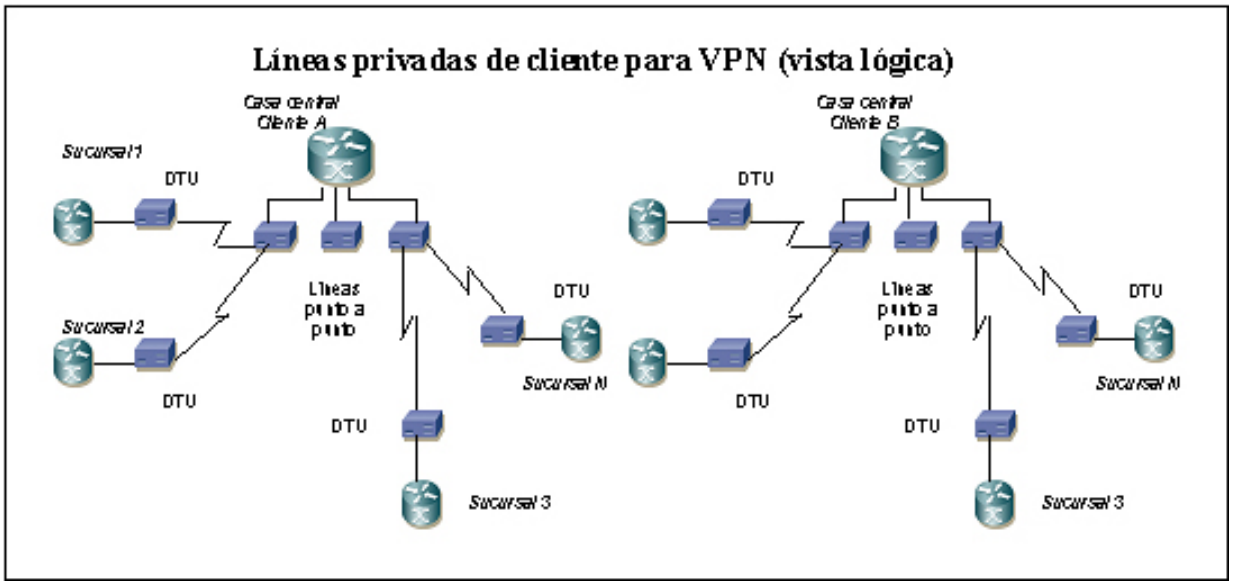


Figura 10 – VPN orientada a la conexión (VL)

La Figura 8 muestra la conectividad física entre el cliente A, el cliente B y la red del proveedor de servicios.

Nota: Las redes TDM componen las formas más simples de redes privadas virtuales VPNs que aseguran alta calidad de ancho de banda fijo a los clientes.

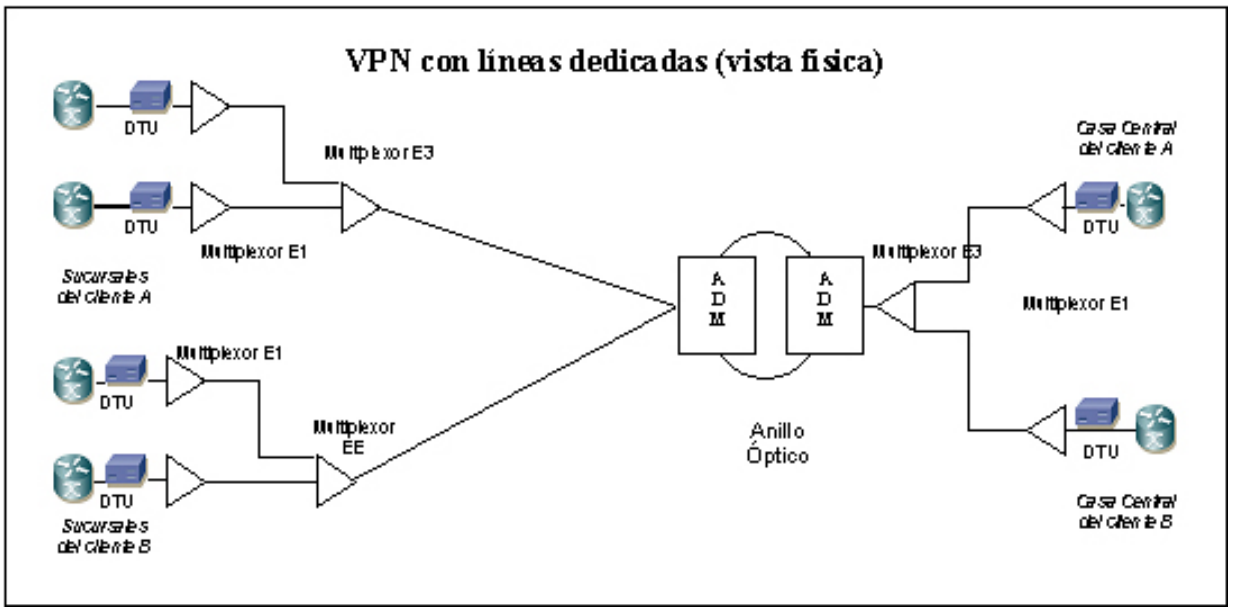


Figura 11 – VPN orientada a la conexión (VF)

Las VPNs basadas en tramas, tales como Frame-Relay y X.25 emplean caminos lógicos definidos por circuitos lógicos “DLCI”. En la Figura 9, se muestran múltiples grupos cerrados de usuarios o clientes compartiendo la infraestructura de conmutación del proveedor de servicios. Los clientes perciben que los circuitos virtuales son aprovisionados exclusivamente para su uso privado.

Para tales DLCIs se establece un contrato de tráfico, en el cual se especifica cuanto tráfico de red se compromete a transportar. Esto se realiza configurando un Commited Information Rate “CIR”, el cual establece una tasa de información que fija el ancho de banda determinado en el puerto de acceso (local loop).

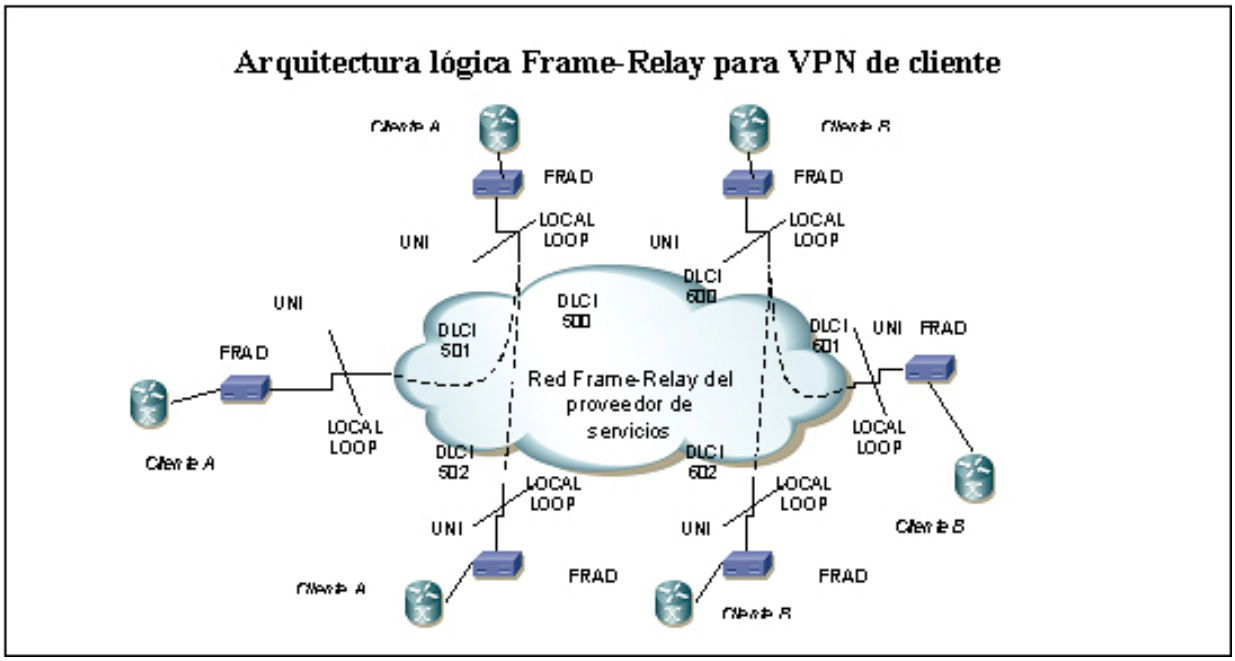


Figura 12 – VPN Frame-Relay

Las VPNs basadas en celdas ATM emplean caminos lógicos definidos por circuitos virtuales conmutados “SVC” y circuitos virtuales permanentes “PVC”. Como indica la Figura 10, múltiples grupos de usuarios cerrados o clientes comparten la infraestructura conmutada del proveedor de servicios. Los clientes perciben que los circuitos virtuales son aprovisionados exclusivamente para su uso privado. Tales PVCs o SVCs pueden ser aprovisionados mediante una clase de servicio tal como CBR, VBR-RT, VBR-NRT, ABR, o UBR.

- CBR: Constant Bit Rate: Utilizado para emulación de circuitos.
- VBR-RT: Real Time Variable Bit Rate: Utilizado para aplicaciones de tiempo real como por ejemplo la voz o el video comprimido.
- VBR-NRT: No Real Time Variable Bit Rate: Aplicaciones que requieran una determinada calidad de servicio y no necesariamente en tiempo real.
- ABR: Available Bit Rate: Utilizado para aplicaciones de datos.
- UBR: Unspecified Bit Rate: Es utilizado para aplicaciones que no necesitan ninguna calidad de servicio “Best Effort”.

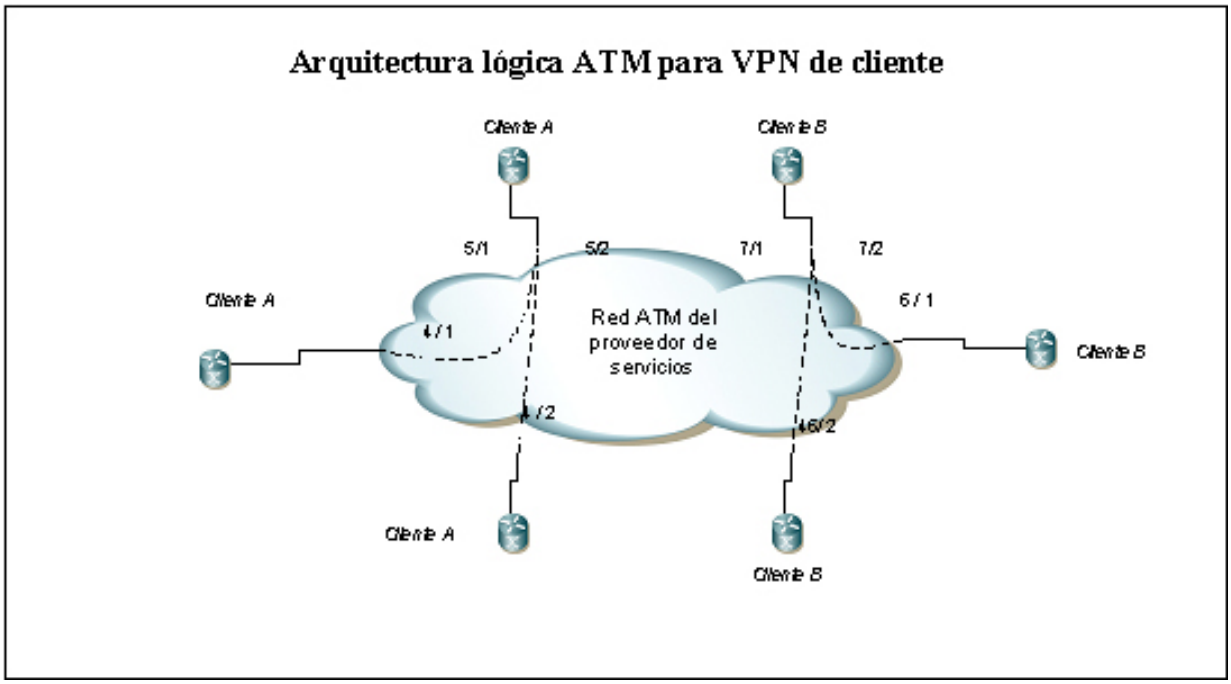


Figura 13 – VPN ATM

VPNs orientadas a la conexión de Capa 3

Las redes orientadas a la conexión de Capa 3 se forman en base de modelos de VPNs con túneles. El modelo IPSec (IP Security) provee un modelo de túneles punto a punto sobre una red IP intranet o Internet, mientras que las redes privadas de discado (VPDNs) proveen una combinación híbrida de discado a través de una conexión segura sobre Internet hacia un punto de entrada (gateway) de la red corporativa.

IPSec es una tecnología altamente segura que emplea una combinación de encripción y un mecanismo de túnel, que protege los paquetes en transito en una red IP. Generalmente IPSec se utiliza sobre redes IP públicas no confiables, como ser Internet. Es posible construir una VPN sobre una red IP pública mediante la combinación de túneles IPSec punto a punto.

La mayoría de las arquitecturas IPSec se emplean en el dispositivo CPE (customer Premises equipment) o equipo de casa de cliente, como se indica en la Figura 11.

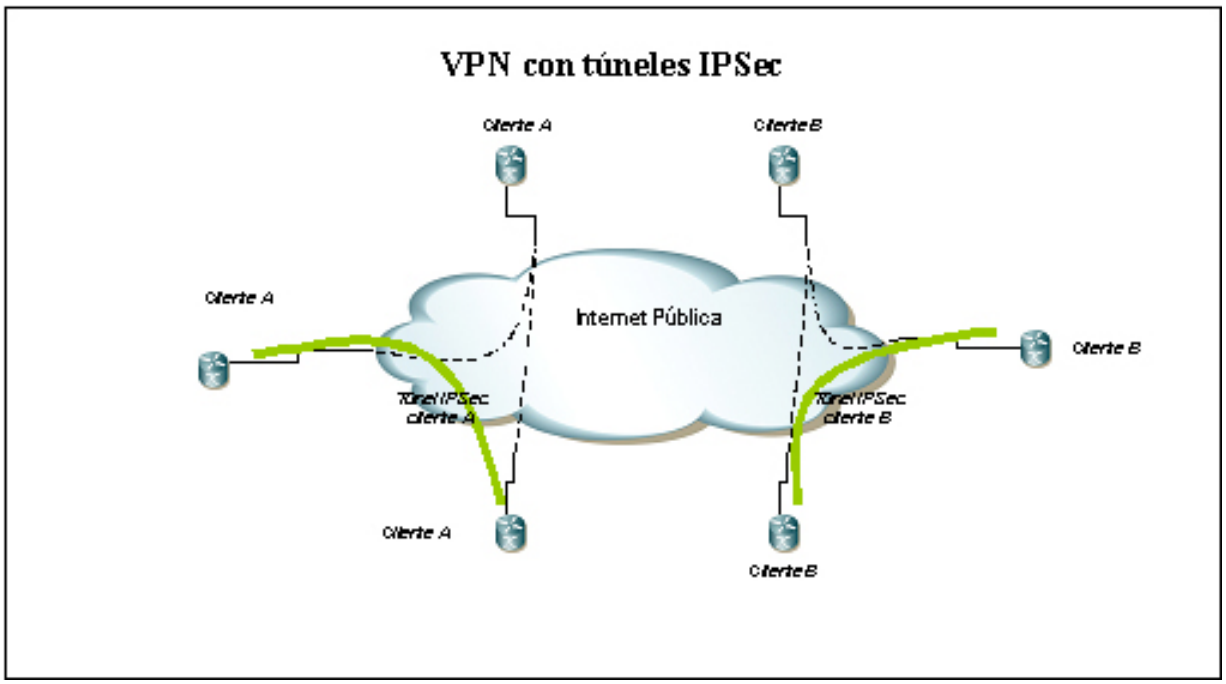


Figura 14 – VPN IPSec

Una opción práctica al día de hoy para aquellos usuarios móviles o viajeros que requieran un acceso remoto seguro hacia su empresa consiste en emplear IPSec. Los usuarios acceden remotamente a la corporación a través de la red pública conmutada de telefonía (PSTN: Public Switched Telephone Network). La Figura 12 detalla un servicio de VPDN (Virtual Private Dial-up Network) implementada sobre la red privada IP backbone del proveedor de servicios. Los protocolos empleados para implementar el servicio VPDN sobre una red IP incluyen Layer 2 Forwarding (L2F) o Layer 2 Tunneling Protocol (L2TP). Los usuarios remotos inician una conexión discada hacia el servidor de acceso remoto (NAS: Network Access Server) empleando el protocolo PPP. El NAS a su vez autentica la llamada y envía la misma a través de L2F o L2TP hacia el punto de entrada (gateway) de la red del cliente. El gateway acepta la llamada y realiza el proceso de autenticación, autorización y facturación, terminando la sesión PPP del usuario.

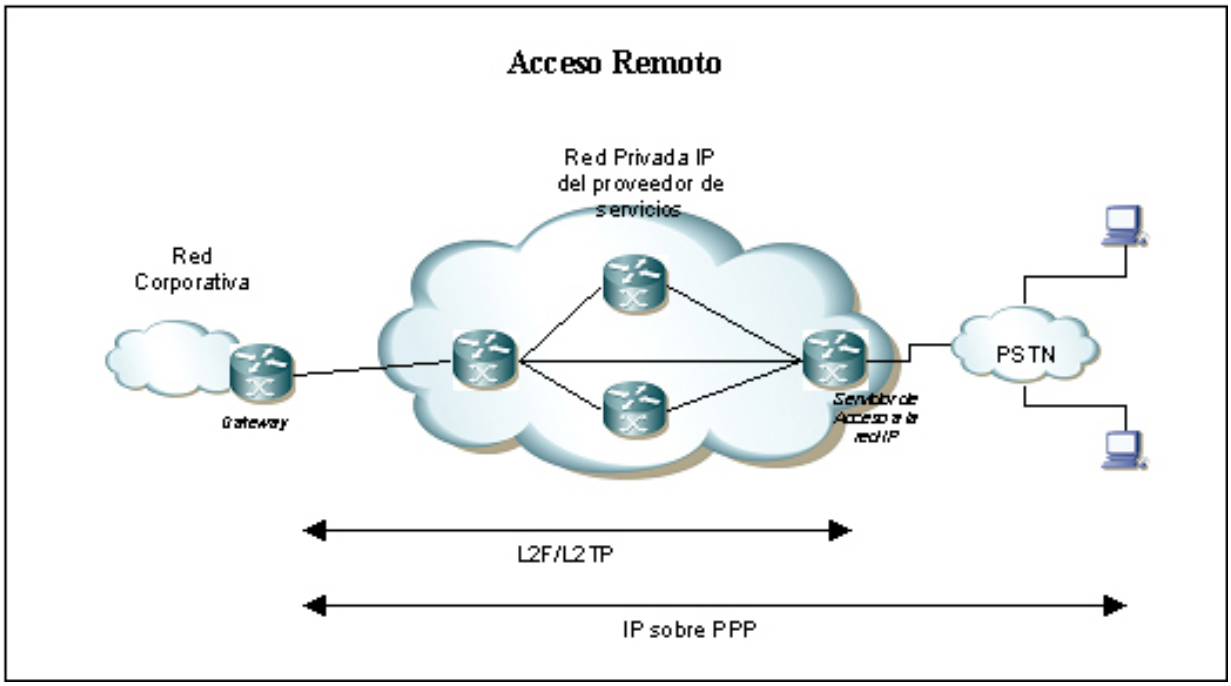


Figura 15 – Acceso Remoto

VPNS no orientadas a la conexión

Las VPNs no-orientadas a la conexión no requieren de un conexionado lógico predefinido o de la provisión de circuitos virtuales entre dos extremos para establecer la conexión de los mismos.

VPNs IP convencionales

Varios proveedores de servicios o Carriers proveen manejo de servicios IP (manager IP servicies) ofreciendo básicamente la conexión de los routers CPE de los clientes a la red backbone del proveedor de servicios. Los proveedores de servicios IP poseen una red IP sobre una infraestructura de Capa 2 como puede ser una red ATM o Frame-Relay. Un ejemplo de VPN IP convencional se detalla en la Figura 13.

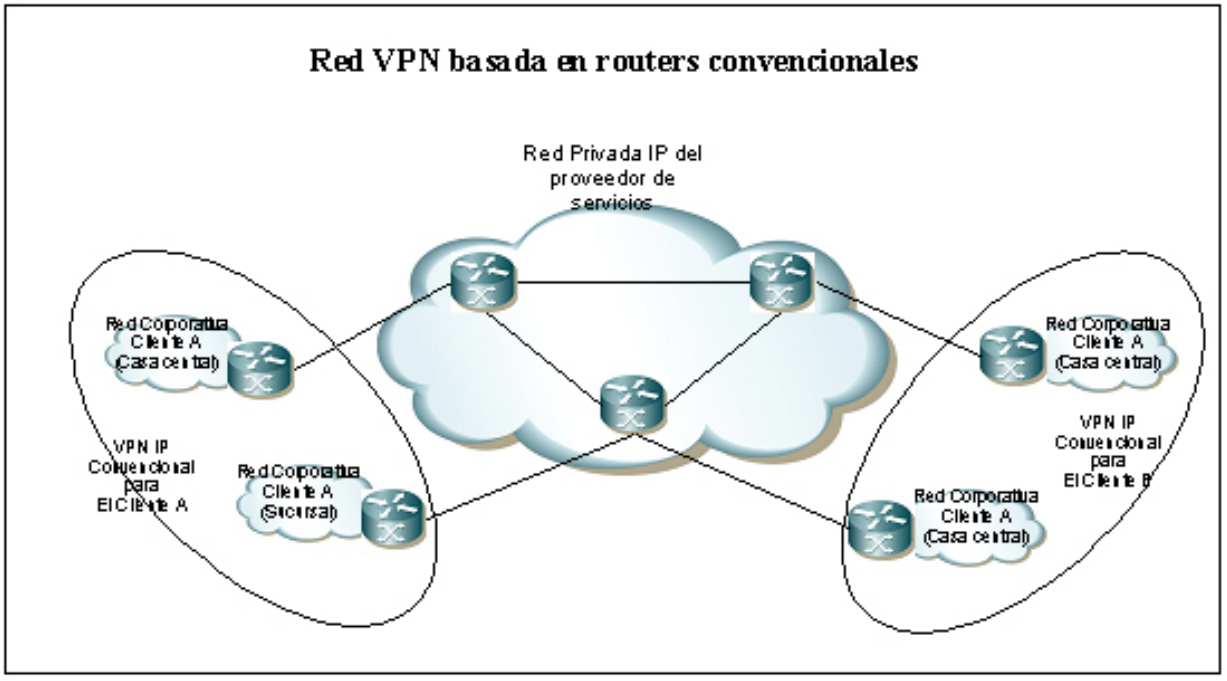


Figura 16 – VPN basada en routers

El proveedor de servicios IP configura típicamente múltiples protocolos dinámicos de ruteo corriendo además múltiples procesos de ruteo en sus routers de backbone para el servicio de sus clientes. Los

clientes perciben una red VPN IP privada por virtud de la combinación de listas de acceso, y procesos y protocolos de ruteo.

Los mayores inconvenientes que se presentan a los proveedores de manejo de servicios IP son la escalabilidad y la complejidad de implementación. El numero disponible de protocolos y procesos de ruteo soportados por las plataformas de cada router obliga a los proveedores a implementar routers separados por cada VPN de cliente en el punto de presencia del proveedor (POP: Point of Presence).

VPNs MPLS

Las VPNs MPLS son no-orientadas a la conexión. El protocolo MPLS separa trafico y provee privacidad sin la necesidad de encripción o protocolos de túneles de Capa 2, con lo cual, simplifica enormemente el proceso de provisión. MPLS resuelve los problemas de escalabilidad encontrados en los desarrollos de Frame-Relay y ATM ya que permite a los proveedores de servicios aprovisionar múltiples VPNs para diversos clientes sin la necesidad de configurar decenas de cientos de circuitos virtuales para cada uno de los grupos cerrados de usuarios. En la Figura 14 se detalla un ejemplo de red MPLS, donde los clientes A y B comparten la misma infraestructura del proveedor de servicios mientras poseen sus propios grupos cerrados de usuarios mediante una probada seguridad. Además, permite que el cliente corra sus propios protocolos de ruteo.

El modelo MPLS requiere que los routers CPE intercambien información de ruteo directamente con los routers de borde del proveedor, en lugar de que cada CPE debe intercambiar la información con cada uno de los restantes CPE. Los miembros de una VPN son identificados como pertenecientes a un grupo cerrado por medio de etiquetas. Dichas etiquetas transportan información del próximo salto, los atributos de los servicios, y un identificador de VPN, que mantiene la comunicación dentro de un ámbito privado (VPN).

Los paquetes que ingresan en la red del proveedor desde un router CPE son procesados, y las etiquetas son asignadas al mismo basándose en la interface física por la cual dicho paquete provino. Las etiquetas son aplicadas empleando la funcionalidad de las tablas VRF (Virtual Router Forwarding). Las tablas de envío son predeterminadas, y los paquetes son analizados en el LSR de ingreso o (PE: Provider Edge). Los dispositivos de core o (P: Provider) tienen la función solamente de conmutar paquetes etiquetados.

MPLS hace que las redes backbone de ruteo de los proveedores provean capacidad de VPN y visibilidad de Capa 3 aun sobre infraestructuras de Capa 2. Esto último permite crear grupos cerrados de usuarios y asociar servicios con ellos.

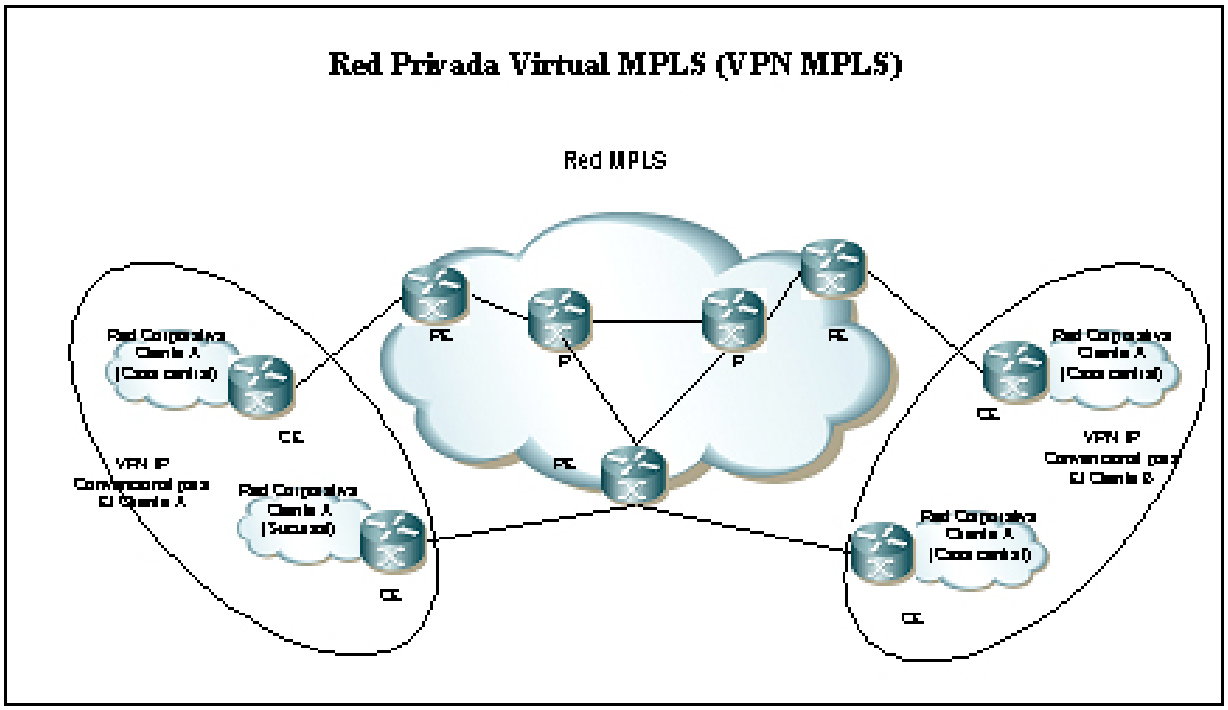


Figura 17 – VPN MPLS

Comparación de las tecnologías VPN

Los proveedores de servicios deberán decidir entre las diferentes tecnologías de VPNs disponibles en el mercado, con el objetivo de satisfacer las necesidades de sus clientes y con el objetivo de reducir sus costos operativos y de infraestructura de red.

En este apartado se realizará un análisis de las variables más representativas que los proveedores de servicios necesitan a la hora de realizar una toma de decisión sobre la tecnología de VPNs a implementar.

El siguiente análisis fue realizado en base a un estudio de redes, sistemas de gestión, tecnologías de VPNs y sobre la experiencia de migración de una red ATM a una red VPN/MPLS.

Para cada una de las variables a analizar, se realizo una comparativa entre VPNs de capa 2 (implementadas con circuitos virtuales) del tipo ATM o Frame Relay, VPNs basadas en túneles de capa 3 del tipo IPSec y VPNs/MPLS.

Configuración y operación

La tarea de configuración y operación de una red con soporte de VPNs, es una tarea muy compleja para el proveedor de servicios, debido a la necesidad de mantener la provisión de varias redes de clientes sobre una infraestructura de red publica.

Los mecanismos de configuración y operación difieren dependiendo de la tecnología de VPNs a implementar; y pueden basarse en sistemas de provisión enlatados, en sistemas desarrollados ad-hoc, o en forma manual. Esta ultima modalidad parece no ser la mas conveniente pero debido a la esencia de los operadores de las redes, la modalidad de configuración y operación manual es muy utilizada por eso también será tenida en cuenta en el análisis.

- VPNs del tipo ATM o Frame Relay

La configuración inicial de una red VPN sobre una red ATM o Frame Relay consiste en la generación de circuitos virtuales sobre una red publica, con la complejidad que estos circuitos deben configurarse “nodo a nodo” desde el equipo en casa de cliente pasando por todos los equipos que compongan la red hasta el otro extremo del cliente. Como ya hemos visto en los capítulos anteriores una red típica de cliente esta compuesta por una topología “hub-and-spoke” con una casa central y N sucursales; por lo cual esta cantidad de circuitos virtuales multiplicada por varios clientes la hacen una red difícil de configurar y operar.

Una ventaja de este tipo de redes es el know-How (conocimiento) de los operadores sobre esta tecnología, debido a la gran cantidad de tiempo que esta lleva implementada y sumada a los sistemas de gestión asociadas a esta tecnología facilitan la configuración y operación diaria.

- VPNs del túnel IPSec

La configuración inicial de una red VPN sobre una red IPSec, es simple desde el punto de vista de la provisión de una red VPN para un cliente, teniendo en cuenta que este tipo de redes también son topologías “hub-and-spoke”. Entonces el proveedor de servicio solo deberá configurar los equipos de casa de cliente apuntando el túnel IPSec hacia la casa centra y resolver la autenticación de los túneles y los usuarios en forma local o incluyendo un servidor de claves.

La desventaja de este modelo es la operación cuando existen varios clientes configurados, ya que no existen sistemas de gestión para esta tecnología y mayormente la configuración y operación se realiza en forma manual o con sistemas ad-hoc.

- VPNs MPLS

La configuración inicial de VPNs con esta tecnología es sencilla, ya que al no ser orientada a la conexión se pueden generar topologías hub-and-spoke o full-meshed solo haciendo que el equipo de casa de cliente sea parte de la VPN, esto significa que solo configurando el CPE y sin realizar modificaciones en la red es posible que este nuevo equipo sea parte de la VPN.

La desventaja de este modelo que como toda nueva tecnología, los sistemas de gestión asociados recién comienzan a integrarse al mercado y muchos de esto no satisfacen las necesidades de los proveedores de servicios, por lo que actualmente se realizan en Argentina en forma manual o con sistemas ad-hoc. Además el Know-How es menor comparándolo con el resto de las tecnologías, lo que hace más difícil la operación de este tipo de redes.

Escalabilidad

Entendamos la escalabilidad como la capacidad que tienen las tecnologías en adaptarse, flexibilizarse y crecer en cantidad de clientes. Teniendo en cuenta esto se realizó un análisis comparativo de cómo cada tecnología puede afrontar estos desafíos.

- VPNs del tipo ATM o Frame Relay

La escalabilidad de la tecnología ATM o Frame Relay para la implementación de VPNs no encuentra límites en la cantidad de clientes o la necesidad de ancho de banda que la red proveedora necesita para afrontar las necesidades de los clientes. Pero actualmente las necesidades de integración de los servicios hacen que los clientes necesiten una tecnología que permita integrar todos sus servicios sobre un mismo

transporte de red para ahorrar costos y simplificar la operación. Esto último hace que ATM o Frame-Relay comience a ser reemplazado por otro tipo de tecnología que permita flexibilidad y adaptación.

- VPNs del túnel IPSec

La escalabilidad de este tipo de redes a nivel de volumen no es muy grande, ya que la operación y configuración comienza a complicarse a medida que los clientes requieren más mayor capacidad de ancho de banda y mayor cantidad de sucursales. Si bien esta tecnología cumple un papel muy importante para los accesos remotos permitiendo flexibilidad de acceso, pierde importancia cuando es desplegada a nivel de core de una red VPN ya que no cumple con los requisitos de calidad de servicio QoS que los clientes requieren para sus servicios.

- VPNs MPLS

Sin dudas esta tecnología es muy escalable por la capacidad de adaptarse a las necesidades de los clientes, permitiendo integrar los servicios en una misma red e implementando la calidad de servicio QoS, para que estos servicios cumplan con las necesidades de los clientes.

Un punto a tener en cuenta es que al ser una tecnología nueva, la maduración de esta implica riesgos mayores para los proveedores de servicios, los cuales deberán sopesarse contra todas sus ventajas.

Calidad de Servicio QoS

Cuando hablamos de calidad de servicio, pedimos que la tecnología sea capaz de asignar prioridades a los distintos tipos de tráfico y manejar la congestión a lo largo de toda la red por donde el tráfico fluye.

El análisis de calidad de servicio se realizó sobre un esquema de servicio en donde los clientes generan y reciben tráfico de datos, voz y video sobre un mismo vínculo que es parte de la VPN.

- VPNs del tipo ATM o Frame Relay

Las redes ATM o Frame Relay pueden asignar distintas calidades de servicio a nivel de capa 2, manejando la congestión de manera muy eficiente. ATM por ejemplo nativamente soporta clases de servicio que permite por ejemplo asignar al tráfico de datos una calidad del tipo UBR, al trafico de voz una calidad del tipo VBR-RT y al de video una calidad del tipo VBR-NRT.

El tipo UBR no asigna ningún tipo de calidad por lo tanto el trafico de datos transitará la red sin ningún tipo de calidad.

El tipo VBR-RT asigna una calidad que permite que el trafico transite en real time, especial para el trafico de voz en donde es necesario poca perdida de paquetes, poco delay y poco jitter.

El tipo VBR-NRT asigna una calidad que permite que el tráfico de video transite la red, sin perdida de paquetes aunque con mayor delay y jitter. Recordemos que las aplicaciones de video trabajan con buffers por lo que la latencia y el jitter no degradan el servicio.

- VPNs del túnel IPSec

La calidad de servicio sobre esta tecnología no esta asegurada ya que no cuenta con ningún mecanismo en forma nativa. Todo lo correspondiente a calidad de servicio podrá realizarse a nivel de equipos de cliente, pero dentro de la red del proveedor no existe ningún mecanismo que permita asegurar que el tráfico llegue a destino con las calidades asignadas en los extremos de las redes.

Además otra desventaja de esta tecnología es el overhead (sumatoria de cabeceras por la utilización de protocolos) que generan los túneles IPSec, haciendo esto que el ancho de banda utilizado sea mayor comparado con el resto de las tecnologías.

- VPNs MPLS

Esta tecnología fue pensada para trabajar con calidad de servicio, por lo que todos los mecanismos ya fueron construidos desde la generación de la tecnología. Es posible asignar calidad de servicio a nivel de capa 2 y capa 3; permitiendo diferenciar el tipo de tráfico y asignar un ancho de banda especifico a cada uno.

La única desventaja de este modelo, es nuevamente la dificultad de operación y gestión debido a la falta de sistemas de gestión y Know-How.

Seguridad

Entendamos la seguridad de una red VPN, como la posibilidad que brinda una tecnología de proteger las redes de clientes ante posibles ataques que afecten la disponibilidad de sus servicios y la posibilidad de resguardar sus datos para que estos nos puedan ser modificados y visualizados.

- VPNs del tipo ATM o Frame Relay

Las redes VPN del tipo ATM o Frame Relay por estar constituidas por circuitos virtuales de nivel 2, poseen un alto grado de seguridad ante ataques del tipo DoS (denegación de servicio), ya que todos los

equipos componentes de la red solo pueden ser alcanzados por un equipo adyacente. Solo los equipos de clientes del tipo routers, podrán ser alcanzados por el resto de los equipos routers de la red VPN, por lo que la seguridad ante ataques DoS quedará circunscripta a nivel del cliente.

Naturalmente el tráfico entre los diferentes puntos de un cliente no fluye encriptada, por lo cual cualquier intromisión en la red del cliente o proveedor podría modificar o visualizar los datos de los clientes.

- VPNs del túnel IPSec

En cuanto a la posibilidad de ataques DoS, esta tecnología esta igualmente expuesta mas expuesta a la anterior, ya que tanto los equipos de clientes y los equipos del proveedor son equipos del tipo router que al mismo tiempo brindan servicio de Internet, por lo que la exposición a ataques del tipo DoS es más alto.

La gran ventaja de esta tecnología ante el resto, es la posibilidad de encriptar el tráfico entre los diferentes puertos del cliente, haciendo que la intromisión en los datos de los clientes sea casi nula.

- VPNs MPLS

El nivel de seguridad que brinda esta tecnología puede compararse con la de ATM o Frame Relay ya que aunque el tráfico fluye a nivel de capa 3, lo hace emulando una capa de nivel 2 implementando la metodología de etiquetas. Esto permite aislar el trafico entre clientes, pero debemos tener en cuenta que en algunos casos los proveedores de servicio despliegan estas redes sobre redes IP y al mismo tiempo brindan servicios de Internet por lo que hace que los equipos del proveedor tengan un grado de exposición a los ataques de DoS mayor que en le caso de ATM o Frame Relay.

Resumen comparativo

La matriz de la Tabla 2 presenta una comparación entre varias tecnologías VPN y la recomendación de las mismas teniendo en cuenta la seguridad, escalabilidad, y otros factores que impactan directamente en los recursos de las redes de los proveedores de servicios.

	Comentario	Circuitos Virtuales Capa 2	Túneles Capa 3	VPNs MPLS
Grado de facilidad para configurar y operar la red.	Debe poseer un monitoreo avanzado y automatizado para rápidamente agregar nuevos servicios y operar los existentes.	Alto	Bajo	Medio
Nivel de seguridad	Debe estar diseñado para prevenir ataques del tipo DoS y conservar los datos del los clientes.	Medio	Alto	Medio
Grado de escalabilidad	Debe poder escalar en las nuevas necesidades de los clientes y adaptarse a sus requerimientos.	Medio	Bajo	Alto
Grado de implementación de QoS	Debe ser capaz de asignar prioridad al tráfico crítico o sensitivo y manejar congestión a lo largo de diferentes anchos de banda.	Alto	Bajo	Alto

Tabla 3 – Seguridad en VPN

Ventajas de VPNS MPLS

Se presentan a continuación las ventajas de las VPNs MPLS:

- Escalabilidad.
- Seguridad.
- Fácil de aprovisionar.
- Direccionamiento de cliente flexible.
- Basada en estándares.
- Servicios con prioridad extremo a extremo.
- Consolidación.
- Ingeniería de tráfico.
- Servicio centralizado.

- Soporte integrado de clase de servicio.
- Mecanismos de migración hacia MPLS.
- Escalabilidad (Scalability)

El protocolo MPLS fue específicamente diseñado para soluciones altamente escalables (gran capacidad de crecimiento), permitiendo grandes cantidades de VPNs sobre una misma red. Las VPNs basadas en el protocolo MPLS emplean el modelo de vecino y la arquitectura no-orientada a la conexión de Capa 3 para acentuar su naturaleza de solución escalable. El modelo de vecindad (peer model) permite agregar un nuevo CPE en forma sencilla conectando lo a un router PE y agregándolo como miembro de la VPN donde otros CPEs ya se encuentran vinculados; el modelo de Capa 3 evita la necesidad de emplear túneles o circuitos virtuales.

- Seguridad (Security)

Las VPNs MPLS ofrecen el mismo nivel de seguridad que las VPNs orientadas a la conexión como Frame-Relay o ATM. Los paquetes de una VPN no ingresan involuntariamente a otra, ya que la seguridad es provista en el borde del proveedor asegurando que los paquetes recibidos de un cliente son colocados en la VPN correspondiente. Dentro del backbone MPLS el tráfico VPN se mantiene separado por medio de los niveles de etiquetas. La técnica de ataque spoofing (intento de ganar acceso a una determinada red haciéndose pasar por miembro de ella) es prácticamente imposible, porque los paquetes IP de un cliente deben ser recibidos en una interface, o sub-interface unívocamente identificada por una etiqueta VPN, con lo cual reduce al máximo dicha posibilidad.

- Fácil de aprovisionar

En las redes VPN MPLS ningún mapeo de conexión punto-a-punto es requerido, posibilitando adicionar un sitio a una VPN de intranet o extranet para formar un grupo cerrado de usuarios. Cuando las VPNs son administradas de esta manera permite agregar a un sitio en múltiples VPNs, maximizando la flexibilidad para construir intranet y extranet. Además, la funcionalidad MPLS yace solo en la red del proveedor de servicios, siendo mínima la configuración de los routers CPE, y transparente para los routers CE del cliente.

- Direccionamiento flexible

Para que un servicio de VPN pueda ser más flexible, los clientes de los proveedores de servicios deben poder determinar su propio plan de direccionamiento, independientemente del plan de direccionamiento de otros clientes. Muchos clientes emplean el direccionamiento privado definido en el RFC 1918, y no desean invertir tiempo y dinero en convertir todas sus direcciones privadas a IP publicas (además carecería de algunos privilegios de seguridad para redes privadas) solo para presentar a externos la conectividad de parte de su red (intranet). Las VPNs MPLS permiten a sus clientes conservar sus direcciones privadas sin necesidad de utilizar NAT (Network Address Translation); solo se requerirá NAT en caso de que dos VPNs con solapamiento de direcciones deseen interconectarse. Esta particularidad de las VPNs MPLS permite que los clientes empleen sus direcciones no registradas (privadas) y que se comuniquen libremente entre si a través de una red IP publica.

- Basada en estándares

El protocolo MPLS se encuentra disponible para todos los fabricantes de equipos de comunicaciones para de esta manera asegurar redes con interoperabilidad entre las distintas marcas.

- Servicios con prioridad extremo a extremo

Por medio de los mecanismos de QoS presentes en la industria de soluciones de calidad de servicio (QoS) extremo a extremo, los proveedores de servicios pueden garantizar compatibilidad con los SLAs (servicie level agreements).

- Consolidación

Las capacidades de consolidación de los tráficos de voz, datos y video permiten a los proveedores reducir los costos operativos y sus grandes inversiones gracias a las VPNs.

- Ingeniería de trafico (Traffic Engineering)

El empleo del ruteo con funcionalidad de reserva de recursos (RRR: Routing with Resource Reservation) con utilización de extensiones al protocolo RSVP provee a los Carriers máximo aprovechamiento de los recursos de red y la posibilidad de operar sus redes los mas eficientemente posible. La funciona-

lidad RRR permite a los operadores de red aplicar y forzar ruteo explicito, modificando las técnicas de ruteo convencional, brindando rápida convergencia y mecanismos de protección frente a determinadas situaciones, como por ejemplo, forzar la derivación de tráfico por vínculos sub-utilizados en momentos de altos volúmenes de datos en la red.

- Servicio centralizado

Una VPN debe brindarle al proveedor mas funcionalidad que un mecanismo para conectar usuarios a intranets en forma privada, debe también proveer una manera para aprovisionar valor agregado a ciertos clientes en forma flexible. Debido a que las VPNs MPLS son vistas como intranets privadas, es posible agregarles nuevos servicios como: Multicast, Calidad de Servicio (QoS), soporte de telefonía dentro de la VPN (VoIP o IP telephony), contenidos de almacenado (DataCenter), y conectividad múltiple. Es posible combinar varios de estos servicios para en un cliente en particular, como por ejemplo la combinación de IP Multicast y una calidad de servicio de bajo retardo permiten videoconferencia dentro de una intranet.

- Mecanismos de migración hacia MPLS

La migración de un cliente que posee otras tecnologías hacia el empleo de las VPNs MPLS para el desarrollo de su intranet o extranet resulta mínima, ya que el cliente no se ve involucrado en la necesidad de implementar MPLS en sus routers de borde (CE), y además no necesita realizar ninguna modificación a su intranet.

Capitulo III – Identificación de claves

Claves para migrar de una red tradicional a una red VPN IP

Si bien todo los detallado hasta el momento posee un alto grado de subjetividad, teniendo en cuenta que cada caso deberá analizarse en forma individual, a lo largo de este apartado desarrollaremos las claves que deben tenerse en cuenta para que las empresas tomen la decisión de migrar sus redes basadas en redes tradicionales hacia redes del tipo VPN IP.

Alcance del análisis

La elección de las claves se basa en identificar todas las variables que una empresa debe analizar antes de tomar la decisión de migrar su actual red de datos basada en una red Frame-Relay/ATM hacia una red de datos basada en una VPN/MPLS.

La elección de las claves parte de la suposición de que la empresa posee actualmente una red de datos sobre una red Frame-Relay/ATM y durante este apartado se le brindarán las herramientas necesarias para el análisis de conveniencia de migrar o no hacia una red del tipo VPN/MPLS.

Identificación de las claves

La experiencia implementando y diseñanando redes de Carriers, los requerimientos de los clientes y la experiencia ganada durante el desarrollo de este documento; me permitió identificar

puntos comparativos entre diferentes tipo de redes privadas virtuales a las que llame “claves”. Durante esta sección seleccioné las claves principales que los Carriers deberán tener en cuenta, en el momento de decidir el tipo de red a utilizar y los servicios que pretende comercializar.

Entre las principales claves se encuentran:

- Dimensión de la red de datos.
  - Diseño de red.
  - Anchos de banda.
  - Cantidad de sitios.
  - Crecimiento proyectado.
  - Equipamiento utilizado.
- Requerimientos adicionales.
  - Accesos remotos.
  - Interconexión con redes externas.
- Otras redes.
  - Red telefonía interna.
  - Voz sobre Frame-Relay.
  - Voz sobre Frame-Relay.

- Voz sobre IP.
- Comparativa de VoFR/VoATM/VoIP.
- Seguridad.
- Tipo de seguridad requerida.
- Administración de los equipos de red.
- Costos.
- Costos de dimensión de red.
- Costos de operación.
- Costos de instalación.
- Evolución.
- Integración de redes.
- Integración de servicios.

Clave - Dimensión de la red de datos

Para el análisis de las claves de la dimensión de la red de datos, tendremos en cuenta el diseño de red de la empresa, los anchos de banda utilizados, la cantidad de sitios, el equipamiento utilizado y el crecimiento proyectado.

Diseño de red

El diseño de red se refiere a la topología utilizada por la empresa, esto puede ser una red del tipo “full-meshed” o del tipo “hub-and-spoke”.

El tipo “full-meshed” indica que todos los sitios están interconectados con el resto de los sitios que son parte de la red, esto nos indica que el patrón de tráfico es del tipo “peer-to-peer” o sea punto a punto.

La tecnología VPN/MPLS permite diseñar la red del cliente en full-meshed al mismo costo que el diseño en hub-and-spoke. Solo dependerá de la empresa la elección del mismo.

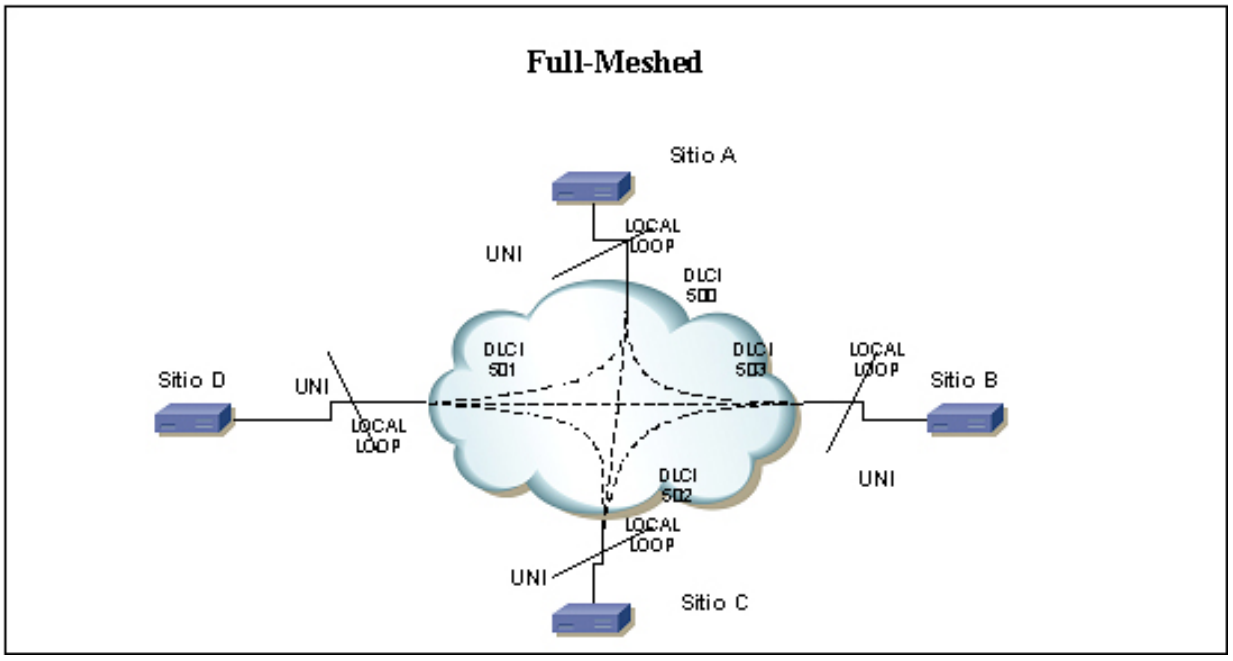


Figura 18 – Topología Full-Meshed

El tipo “hub.-and-spoke” pretende tener uno o dos sitios que podemos llamar casa central, en donde convergen todo el resto de los sitios que podemos llamar sucursales.

Aquí el patrón de difiere al anterior ya que todo el trafico deberá pasar por los sitios centrales aunque tengan como destino cualquier otra sucursal.

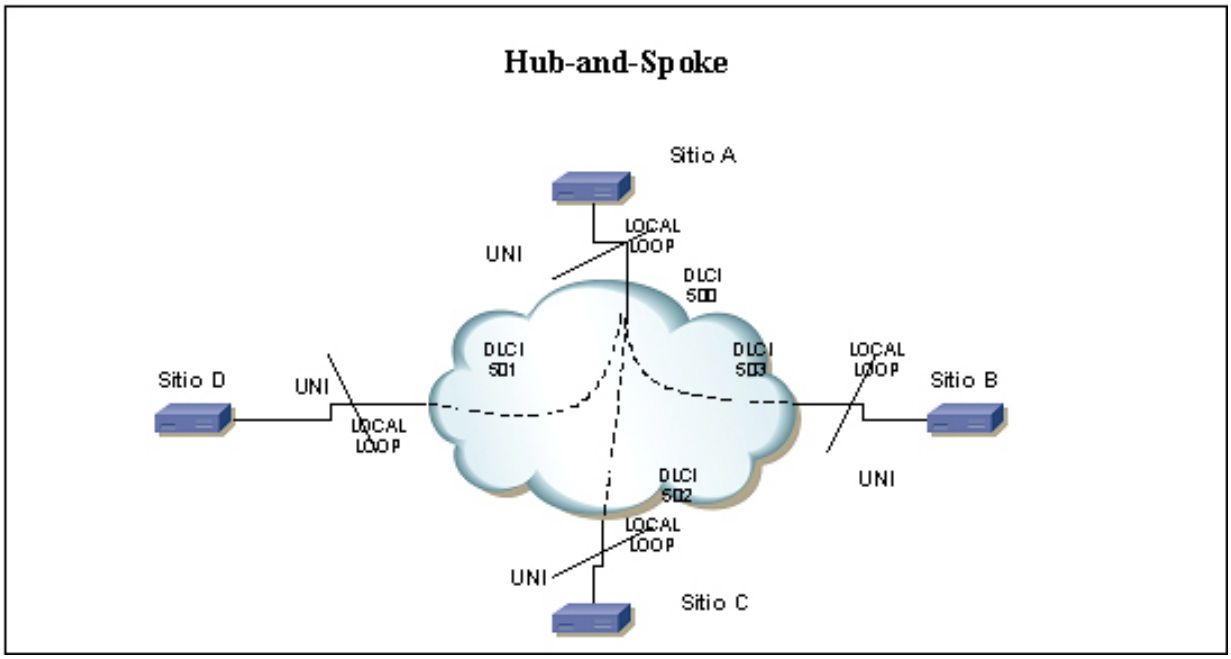


Figura 19 – Topología Hub-and-Spoke

Además el diseño de red elegida tendrá un impacto directo con el la cantidad de vínculos y anchos de banda utilizados, ya que sobre un diseño full-meshed tendremos una mayor cantidad de vínculos con menor ancho de banda y en un diseño hub-and-spoke menor cantidad de vínculos con mayor ancho de banda (aumentando el ancho de banda en los sitios centrales).

En algunos casos existen topologías mixtas, pero para el estudio solo tomaremos los dos diseños anteriores dejando la topología mixta para un estudio particular.

En muchos casos la elección del diseño de red de una empresa, sobre redes Frame-Relay/ATM, solo depende del costo asociado, por lo que eligen redes del tipo hub-and-spoke pero terminan siendo ineficientes y poco flexibles.

Anchos de banda

La red debe dimensionarse teniendo en cuenta los requerimientos de servicios, aplicativos, cantidad de usuarios y la topología a utilizar. Si bien estas variables son difíciles de medir en el momento de diseñar las redes, se desarrolla un modelo que permitirá estimar el ancho de banda a utilizar teniendo en cuenta estas variables. El análisis se realizará comparando las diferentes topologías utilizadas.

Siguiendo con el ejemplo anterior, la red cuenta con cinco sitios los cuales representan Sitio A “Casa Central” y los sitios B, C, D y E “Sucursales” de una empresa.

Los usuarios de la red utilizan diferentes servicios y aplicaciones:

- Correo electrónico interno y externo vía Internet, los servidores de correo se encuentran centralizados en la casa central y desde este lugar se distribuyen en el resto de las sucursales los correos internos y los externos son enviadas hacia fuera de la empresa.
- Servicio de telefonía, todas las sucursales se comunican entre si y con casa central utilizando la tecnología Voz sobre Frame-Relay “VoFR”, luego todo conmuta a una PABX mediante la cual se conecta a la red de telefonía publica.
- Aplicativos internos, estos aplicativos son software de negocio y poseen un servidor en cada sucursal y casa central, estos servidores replican la información de cada sitio al resto para mantenerse actualizados.
- Aplicativos de red, mediante las facilidades del sistema operativo Windows en casa central se cuenta con servidores para backup de información, compartir archivos y además compartir los recursos de impresión.
- Internet, la empresa tiene una política de Internet limitada por lo tanto necesita autorizar los usuarios permitidos y filtrar contenido.

Las topologías de red a analizar son hub-and-spoke y full-meshed; se encuentran graficadas de tal forma de poder identificar los sitios (A, B, C, D, y E) y vínculos de red (v1, v2, v3, v4 y v5):

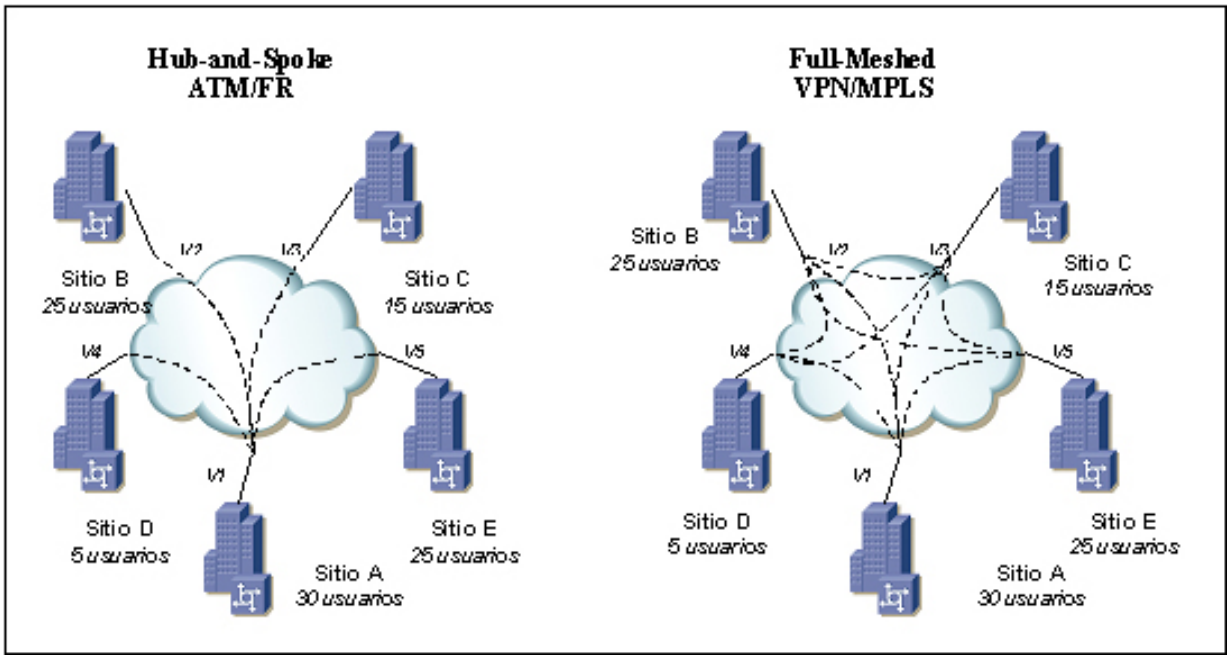


Figura 20 – Comparativa de topologías

Tomando como promedio de utilización de ancho de banda por usuario 25Kbps para tráfico de datos comprendido entre las diferentes aplicaciones, programas y servicios; y otros 25Kbps promedio de VoFR/ VoIP (calculo estimativo de 1 llamada promedio por sucursal).

Según los anchos de bandas descriptos podemos inferir que cada usuario utiliza 50Kbps de ancho de banda en forma entrante “input” y en forma saliente “output”.

Si suponemos que la casa central “A” concentra la mayoría de los servidores y es utilizada como gateway de acceso a Internet, la distribución de trafico no será uniforma entre las diferentes sucursales y ya no solo dependerá de la cantidad de usuarios por sucursal sino también porque gran parte del trafico de datos deberá pasar en forma obligada por la casa central debido a la centralización de servidores.

Con el objetivo de realizar una comparativa entre diferentes tipos de topología, se realiza un cálculo de utilización de ancho de banda entre las diferentes sucursales, utilizando las siguientes premisas.

Para el tráfico de datos:

- Se suponen 25Kbps de tráfico bidireccional de datos por usuario.
- Debido a la centralización de servidores y el acceso a Internet, la casa central concentra un 60% del tráfico de datos.
- El resto del 40% del tráfico se distribuye entre las diferentes sucursales dependiendo de la cantidad de usuarios por sucursal.

Para el tráfico de voz:

- Se suponen 25Kbps de tráfico bidireccional de VoFR/VoIP por usuario.

Las siguientes tablas detallan la distribución de ancho de banda por sucursal. Los cálculos realizados en las tablas permiten realizar una comparativa del consumo de ancho de banda entre la topología Hub-and-Spoke utilizada en ATM/FR y la topología Full-Meshed utilizada en VPN/MPLS.

Para el caso de una topología Hub-and-Spoke, los cálculos de ancho de banda son los siguientes:

Trafico de Datos	**Porcentaje de Trafico**	0,6	0,15	0,07	0,03	0,15	
Total de trafico/sucursal	**Sucursal**	A	B	C	D	E	**Output**
750	A		281,25	148,75	71,25	281,25	782,5
625	B	531,25					531,25
375	C	348,75					348,75
125	D	121,25					121,25
625	E	531,25					531,25
	Input	1532,5	281,25	148,75	71,25	281,25	

Trafico de Voz	Porcentaje de Trafico	0,3	0,25	0,15	0,05	0,25	
Total de trafico/sucursal	Sucursal	A	B	C	D	E	Output
750	A		468,75	318,75	118,75	468,75	1375
625	B	468,75					468,75
375	C	318,75					318,75
125	D	118,75					118,75
625	E	468,75					468,75
	Input	1375	468,75	318,75	118,75	468,75	

Basado en las tablas de cálculo de ancho de banda, el dimensionamiento de los vínculos en una topología Hub-and-spoke se distribuye de la siguiente forma:

Vínculos	V1	V2	V3	V4	V5
Output	2157,5	1000	667,5	240	1000
Input	2907,5	750	467,5	190	750

Para el caso de una topología Full-Meshed, los cálculos de ancho de banda son los siguientes:

Trafico de Datos	Porcentaje de Trafico	0,6	0,15	0,07	0,03	0,15	
Total de trafico/sucursal	Sucursal	A	B	C	D	E	Output
750	A		112,5	52,5	22,5	112,5	300
625	B	375		43,75	18,75	93,75	531,25
375	C	225	56,25		11,25	56,25	348,75
125	D	75	18,75	8,75		18,75	121,25
625	E	375	93,75	43,75	18,75		531,25
	Input	1050	281,25	148,75	71,25	281,25	

Trafico de Voz	Porcentaje de Trafico	0,3	0,25	0,15	0,05	0,25	
Total de trafico/sucursal	Sucursal	A	B	C	D	E	Output
750	A		187,5	112,5	37,5	187,5	525
625	B	187,5		93,75	31,25	156,25	468,75
375	C	112,5	93,75		18,75	93,75	318,75
125	D	37,5	31,25	18,75		31,25	118,75
625	E	187,5	156,25	93,75	31,25		468,75
	Input	525	468,75	318,75	118,75	468,75	

Basado en las tablas de cálculo de ancho de banda, el dimensionamiento de los vínculos en una topología Full-Meshed se distribuye de la siguiente forma:

Vínculos	V1	V2	V3	V4	V5
Output	825	1000	667,5	240	1000
Input	1575	750	467,5	190	750

Como conclusión de este análisis podemos abordar a que la topología hub-and-spoke es conveniente cuando la red posee un sitio que agrupa la mayor cantidad de servicios y aplicativos de toda la red. De esta forma para el sitio central deberá tenerse en cuenta además del tráfico que posee su origen o destino, el tráfico entre sitios que necesariamente deberá hacer transito a través del sitio central.

Para el caso contrario en donde prevalecen los servicios del tipo punto a punto - servicios de voz, aplicaciones peer-to-peer - la topología del tipo full-meshed ahorra ancho de banda, permite una descentralización de servicios y aplicativos simplificando el diseño de la red.

El hecho de migrar una red basada en ATM/Frame-Relay a VPN/MPLS, permite un ahorro de ancho de banda, teniendo en cuenta que esta tecnología permite diseñar una red full-meshed al mismo costo que una hub-and-spoke.

Cantidad de sitios

La cantidad de sitios de la red es otra variable a analizar, ya que de esta variable dependen la cantidad de vínculos según la topología utilizada.

Siendo “n” la cantidad de sitios y “V” la cantidad de vínculos:

Para el caso de ATM/Frame-Relay con $n \geq 2$

$V = n - 1$ (Para un diseño hub-and-spoke)

$V = \frac{(n-1) * n}{2}$ (Para un diseño full-meshed)

Para el caso de VPN/MPLS con $n \geq 2$

$V = n - 1$ (Para un diseño full-meshed)

La tecnología de las VPN/MPLS tiene una gran ventaja sobre la ATM/Frame-Relay, ya que la flexibilidad de esta tecnología permite incluir un sitio de la red dentro de una topología full-meshed sin la necesidad de definir vínculos entre los restantes sitios. Por ende la cantidad de vínculos no es una variable de dimensionamiento de red en VPN/MPLS.

Crecimiento proyectado

Para el diseño de una red debe tenerse en cuenta el crecimiento proyectado, en cantidad de sitios, anchos de banda y expansión geográfica. En la actualidad muchas empresas tienen la necesidad de expandir sus redes fuera del país; como puede ser conectar algunas de sus sucursales e interconectarse con proveedores o socios que residen en otros países.

Las redes ATM/Frame-Relay de Argentino no se expanden fuera del territorio nacional, para lo cual la interconexión de sitios fuera de ese ámbito no es posible.

Muchas empresas hasta el día de hoy realizan estas conexiones utilizando soluciones punto a punto o VPNs nivel 3 del tipo IPSec utilizando la conectividad de Internet.

La tecnología VPN/MPLS permite la interconexión de redes de Carriers o proveedores de servicios, permitiendo así que la interconexión que la empresa necesita fuera del país pueda realizarse en forma transparente, solamente requiriendo un nuevo punto de conexión a su VPN. Para esto es necesario que el Carrier o proveedor de servicio posea un convenio con otras redes MPLS para realizar la interconexión.

Equipamiento utilizado

En las redes de empresas basadas en ATM/Frame-Relay el equipamiento utilizado en las sucursales y casa central son del tipo routers (equipos que permiten interconectar diferentes interfaces y enrutar el trafico a nivel 3 entre ellas). Si bien las redes ATM/Frame-Relay realizan conmutación de celdas/conmutación de circuitos a nivel 2; en los extremos como ser sucursales y casa central las redes se administran a nivel 3, utilizando el protocolo IP que les permite asociar en forma directa los servicios y aplicativos de las empresas, para luego transportar los datos en ATM/Frame-Relay.

La figura describe como pueden reutilizarse los equipos de la empresa en una migración a redes VPN/MPLS:

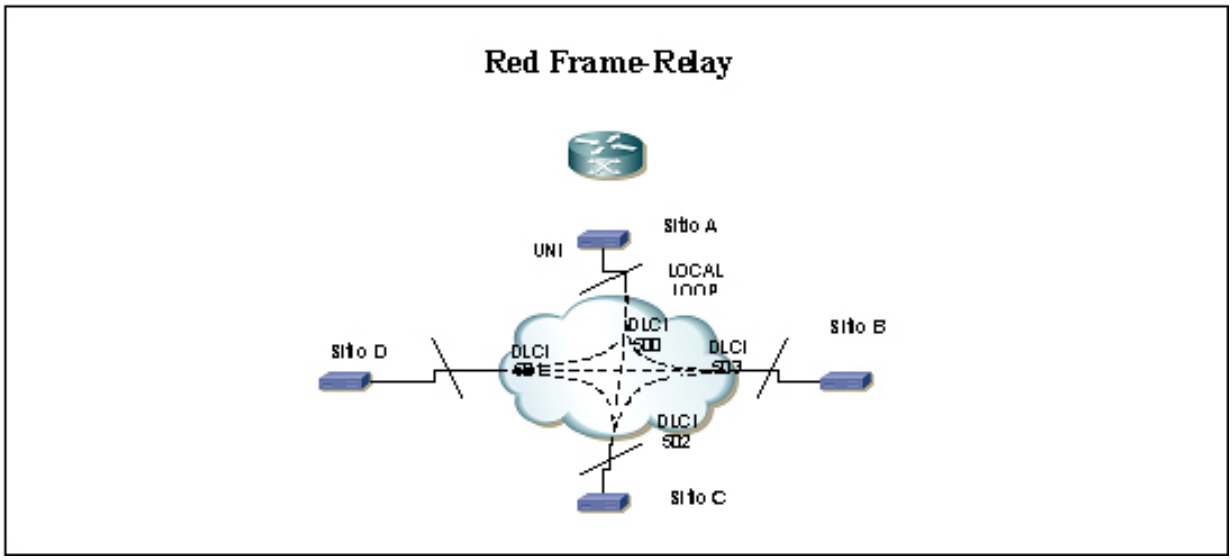


Figura 21 – Equipamiento en Frame-Relay

En muchos casos estos equipos routers pueden ser utilizados como equipos CPE dentro de la arquitectura de red VPN/MPLS. De esta forma la migración es más sencilla y menos costosa que cambiar todo el equipamiento.

Cada caso deberá estudiarse en detalle y de esta forma analizar la reutilización de equipamiento.

Clave – Requerimientos adicionales

Adicionalmente a los requerimientos de conectividad entre sucursales y casa central, las empresas requieren soluciones de valor agregado tales como acceso remoto e interconexión con clientes, proveedores y socios.

Acceso remoto

El acceso remoto es utilizado por las empresas por diversos motivos como ser el acceso remoto de:

- Personal ejecutivo: Este tipo de usuarios necesitan conectarse en forma remota por motivos de viajes, requiriendo la posibilidad de conexiones desde diversas provincias e inclusive desde otros países.
- Usuarios móviles: Es muy común que las empresas posean personal móvil, por ejemplo vendedores, que requieran conectividad a los sistemas de la empresa para tomar y volcar datos de sus ventas.
- Tele trabajadores: Aunque esta modalidad no es muy común en Argentina, algunas empresas lo requieren para el caso de enfermedad, trabajo en horarios extra laboral, etc. Para esto requieren que los usuarios posean el mismo nivel de conectividad que desde sus oficinas.

Actualmente la solución técnica para este tipo de accesos se realiza utilizando dial-up, accesos ADLS, cable MODEM, o accesos satelitales. Si bien esta tecnología es muy utilizada para el acceso a Internet, debe adecuarse para acceder a un ámbito privado como la empresa. Para esto la empresa suele hacerlo de las siguientes formas:

- Acceso dial-up con servidores propios: Las empresas habilitan una numeración del tipo 0800 e instalan servidores que permiten terminar sesiones dial-up en su empresa (NAS: Networks Access Servers), de esta forma los usuarios acceden directamente a la red de la empresa. ***Esta opción es segura pero muy costosa, por la inclusión de equipos NAS en la red de la empresa.***
- Accesos no seguros: Utilizan los accesos convencionales a Internet y se conectan hacia un gateway de la empresa que permite el ingreso del personal habilitado. ***Esta opción no es segura, debido a que la empresa queda muy expuesta a ataques en este tipo de arquitecturas.***
- Accesos seguros: Utilizan los accesos convencionales a Internet, agregando una conexión IPSec desde la PC del usuario hacia un servidor IPSec dentro de la empresa. ***Es el más seguro de todos pero implica un costo para la empresa por la inclusión de un servidor de IPSec.***

En la figura siguiente se detallan algunas formas de conexión remota de usuarios sobre redes ATM/ Frame-Relay, existen variantes de conexión pero el problema es integrar todos los tipos de accesos sobre la red de la empresa de una forma segura:

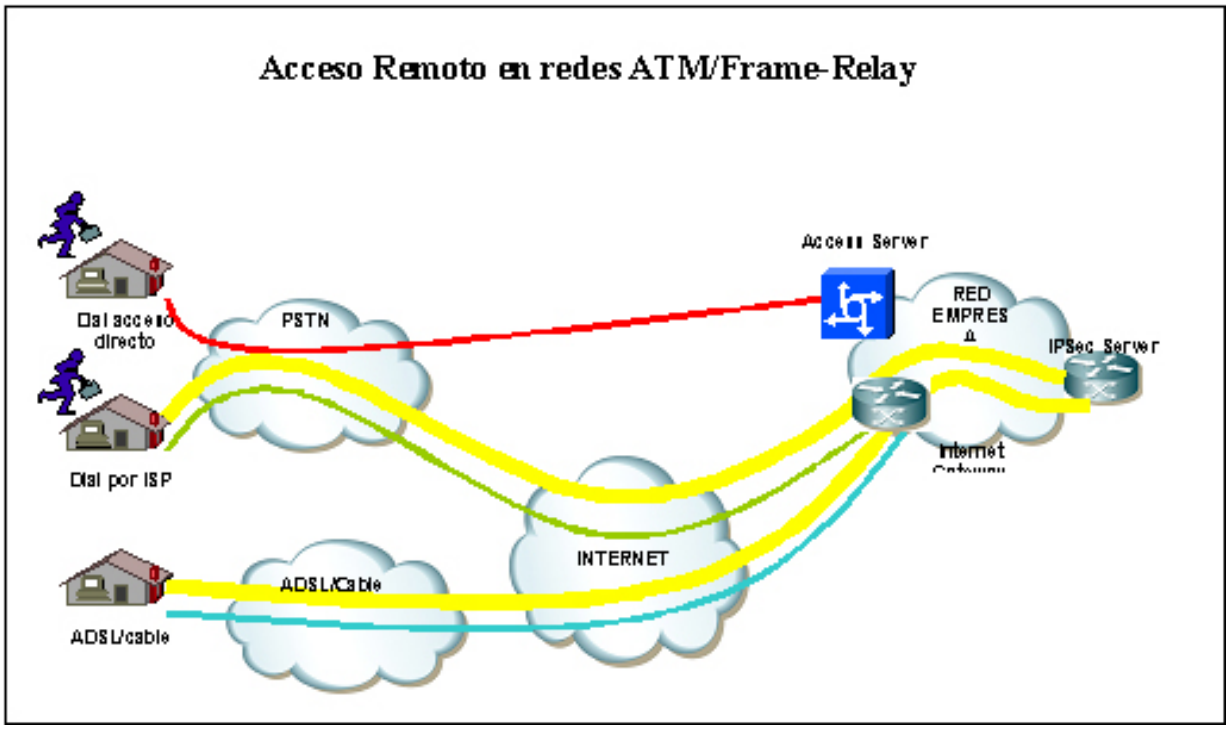


Figura 22 – Topología de Acceso Remoto

En la figura siguiente se detallan algunas formas de conexión remota de usuarios sobre redes VPN/MPLS, mostrando la flexibilidad de esta arquitectura con la ventaja de que al mismo Carrier o proveedor de servicio, la empresa puede contratar no solo los vínculos punto a punto para su red, sino también accesos DIAL, ADSL o IPSec que ingresan directamente a la VPN/MPLS de la empresa, permitiendo de esta forma accesos remotos seguros:

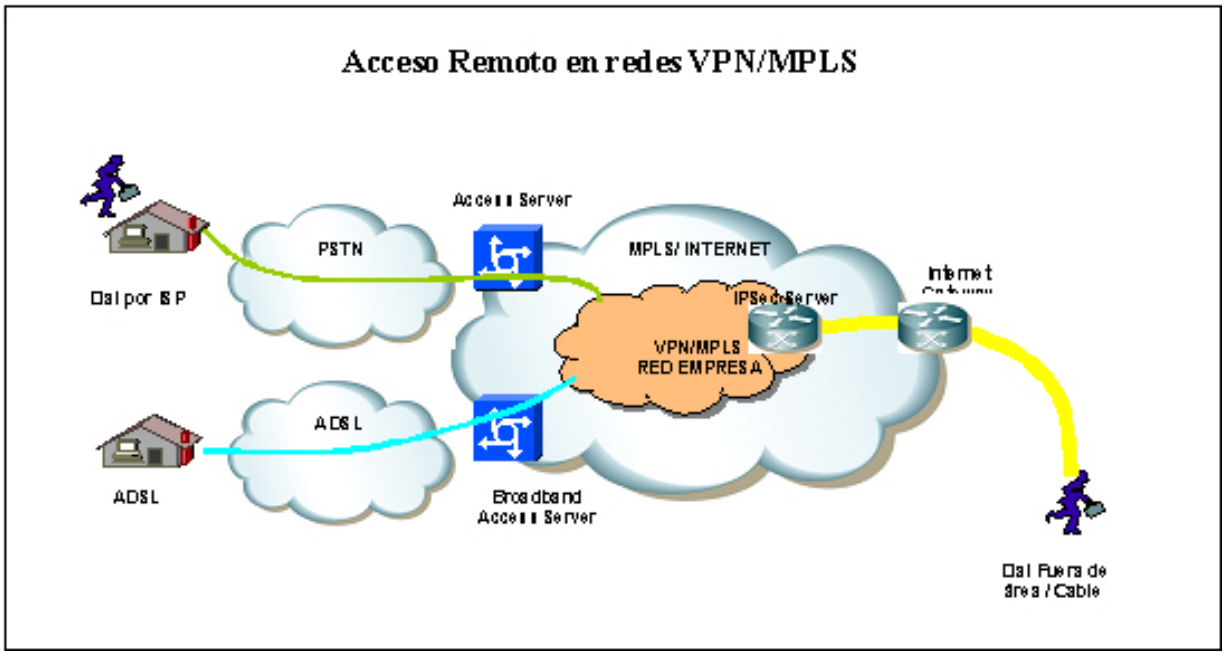


Figura 23 – Acceso Remoto sobre VPN/MPLS

Las redes VPN/MPLS permiten utilizar los mismos accesos dial-up y/o ADSL que se utilizan para acceder a Internet, utilizarlos para acceder a la VPN de la empresa. La particularidad de las redes MPLS es que integran es su arquitectura a los equipos NAS (NAS: Network Access Server) y BAS (Broadband Access Server) utilizados para conexiones dial-up y ADLS sucesivamente.

De esta forma si el Carrier o proveedor de servicio que ofrece la VPN, ofrece también este tipo de accesos remotos, con un costo adicional podrían integrarse las soluciones.

Interconexión con redes externas

Las empresas tienen una necesidad muy común de interconectar las redes para intercambiar datos con sus clientes, proveedores y socios. Esta interconexión de redes es comúnmente conocida como Extranet (redes administradas por diferentes dominios, con la necesidad de intercambiar datos). Entre las necesidades de intercambio de datos pueden encontrarse archivos con información relativas al negocio, conectividad de aplicaciones de negocio, acceso a paginas Web, y muchas otras; sobre estas aplicaciones existe un gran predominio de aplicativos que trabajan basados en IP.

En las redes basadas en ATM/Frame-Relay la interconexión entre estas se realiza a nivel de circuitos virtuales (nivel 2) y luego basados en este nivel se conectan dispositivos que administran el protocolo IP (nivel 3) posibilitando el ruteo entre redes. Esta es una ventaja para las redes basadas en VPN/MPLS, porque en forma nativa permite la interconexión con otras redes nivel 3 y hasta la interconexión con otras redes basadas en VPN/MPLS, por lo que la interconexión se simplifica y abarata los costos.

Entre las necesidades para la interconexión entre redes ATM/Frame-Relay se destaca, la de arrendar y mantener uno o varios circuitos virtuales necesarios para la interconexión. Inclusive si las redes a interconectar pertenecen al mismo Carrier o proveedor de servicios.

En la siguiente figura se detalla un ejemplo de una Extranet sobre una red VPN/MPLS, considerando la posibilidad de extender la VPN sobre diferentes dominios. Para identificar que una VPN se extiende sobre varios dominios (administración de red) MPLS, se denomina a este modelo como “Inter-dominio” como lo muestra la figura siguiente:

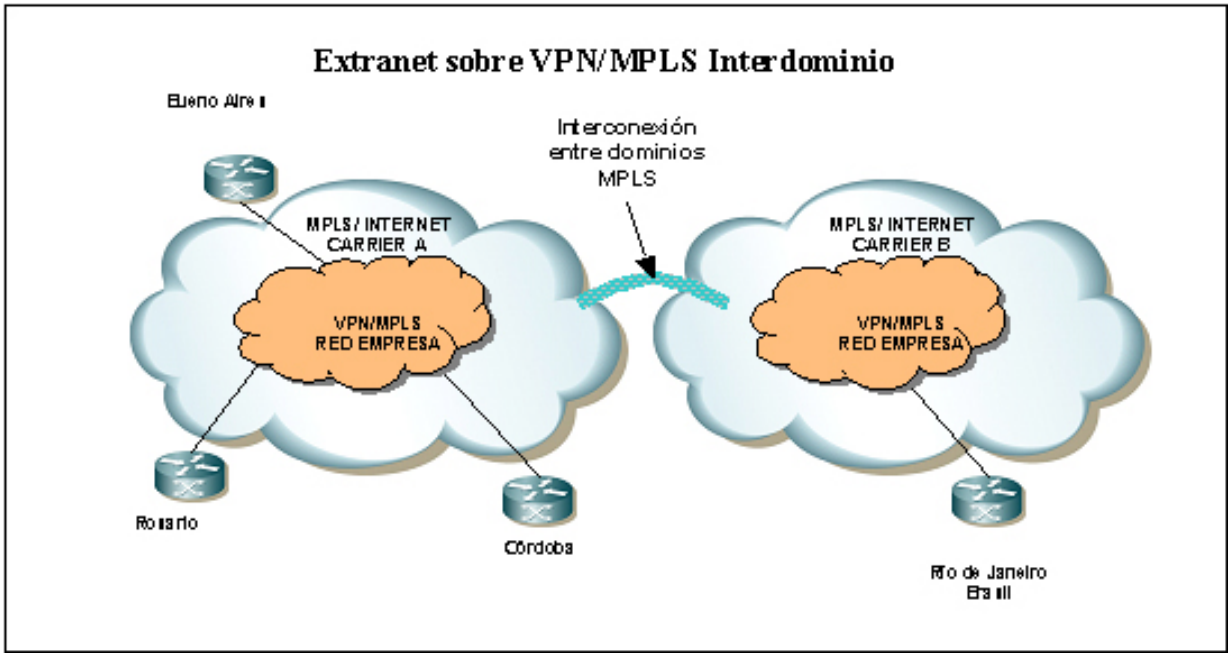


Figura 24 – VPN/MPLS entre dominios

Para redes basadas en VPN/MPLS solo una con una simple interconexión lógica de configuración, en la red del Carrier o proveedor del servicio, las redes pueden interconectarse sin necesidad de arrendar un nuevo vínculo entre ellas.

Además la flexibilidad de MPLS brinda la opción de extender la VPN sobre diferentes dominios de red MPLS, ya sea que la VPN se extienda sobre diferentes regiones o países, independientemente de si el Carrier o proveedor de servicio posean presencia territorial y solo será necesario un acuerdo entre dominios MPLS.

Clave – Otras redes

Las redes de empresa además de estar conformadas por redes para transmitir datos, cuentan con redes de telefonía interna PABX. Las distintas sucursales se comunican entre si utilizando numeración de internos y utilizan la PABX como interfaz a la red de telefonía publica PSTN. Esta modalidad esta siendo remplazada la opción de telefonía sobre redes de datos, ya que les permite ahorrar ancho de banda y constituir una sinergia de redes bajando los costos de instalación, mantenimiento de las redes.

Red de telefonía interna

Las redes de telefonía interna de las empresas están constituidas por un conjunto de PABX, una pequeña central telefónica en donde convergen todos los internos de un edificio. Las PABX a su vez están interconectadas entre si, por medio de vínculos E1 (1024Kbps = 32 canales de 64Kbps), de los cuales solo 30 canales son utilizados para la voz y dos canales reservados para la señalización (Ejemplos: R2 Argentina, SS7).

Una de las PABX es la encargada de conectarse a PSTN, con el fin de enviar y recibir llamadas de la empresa hacia y desde la red de telefonía pública.

En la siguiente figura se muestra una red de telefonía interna de una empresa y su interconexión con la PSTN.

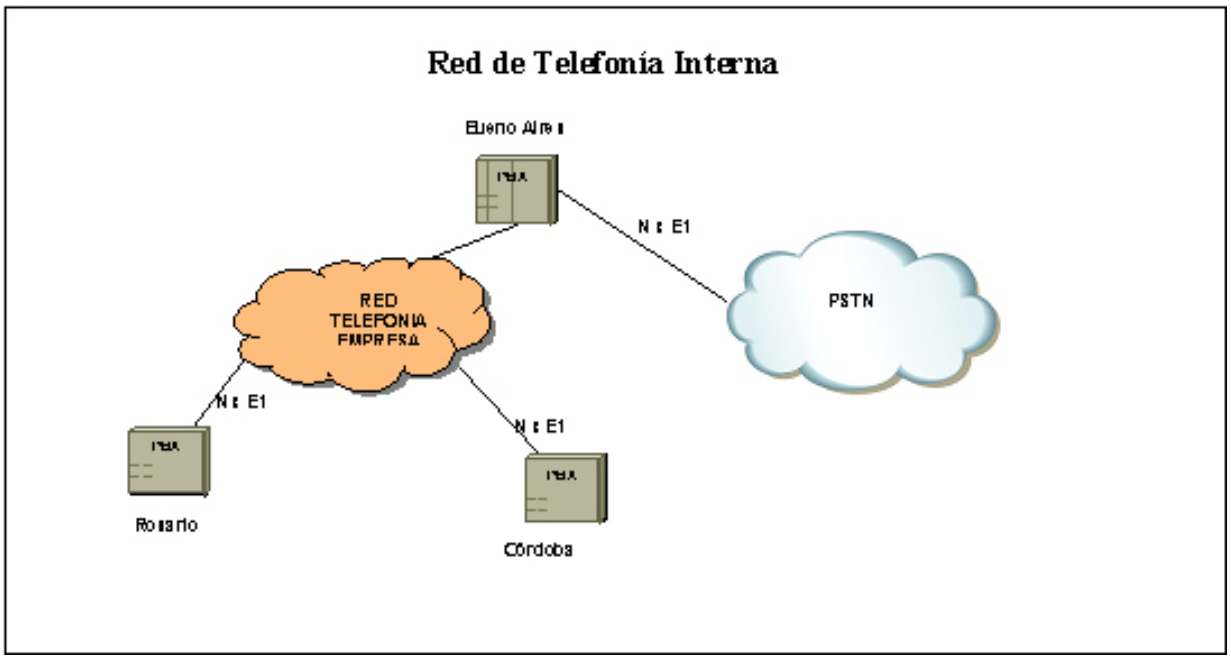


Figura 25 – Red de telefonía interna

La unidad mínima de capacidad de transmisión disponible en los circuitos digitales alquilados es de 64Kbps, esta unidad de capacidad esta dada por la conversión de las señales analógicas a digitales, producida al cuantificar cada pulso a su forma binaria equivalente. Cada señal modulada por amplitud de pulso (PAM: Pulse Amplitude Modulated) se cuantifica con ocho dígitos binarios (bits), de los cuales un bit indica el signo de la señal (positivo o negativo). Esto significa que se usan 256 niveles discretos: desde ocho bits en 0 hasta ocho bits en 1. A la señal digital resultante se la conoce como señal modulada por codificación en pulsos (PCM: Pulse Code Modulated) y tiene una tasa de bits de 64Kbps – 8000 muestras por segundo, cada una de 8 bits-.

Para transportar múltiples llamadas al mismo tiempo en forma digital, los circuitos que enlazan centrales cuentan con múltiplexion por división de tiempo (TDM). Puesto que cada señal analógica se muestra 8000 veces cada segundo, esto produce una señal de 8 bits cada 125 microsegundos.

En el sistema recomendado por la ITU-T se reservan dos ranuras de tiempo 0 (cero) para la sincronización de trama y el canal de tiempo 16 para la señalización, el resto de los 30 canales se utilizan para transmitir voz, lo que genera un total de $32 \times 8bits / 125\mu s = 2.048Mbps$.

Voz sobre Frame Relay VoFR

La red Frame-Relay es la red de datos mas implementadas actualmente para la utilización de redes de datos de empresas debido a su flexibilidad en el ancho de banda y el soporte de diversos tráficos. El servicio de Frame-Relay se basa sobre PVCs, por ende VoFR constituye una opción tecnológica para cursar voz sobre la red de datos de las empresas con este tipo de redes. Las principales características de VoFR son:

- Permite configurar múltiples circuitos lógicos (DLCI´s) sobre un único enlace físico.
- Integra aplicaciones de Datos con servicios de Voz y vides.
- Utiliza multiplexado estadístico de tráfico.
- Frame-Relay es un protocolo usado masivamente.

- El servicio de VoFR puede llegar a ser muy económico.
- Frame Relay nos brinda QoS.
- Los estándares de VoFR permiten interoperabilidad entre diferentes marcas de equipos.
- Standard de Frame-Relay Forum - Voice over Frame-Relay y Frame-Relay Fragmentation.

La siguiente grafica muestra el cálculo de ancho de banda para canales de VoFR:

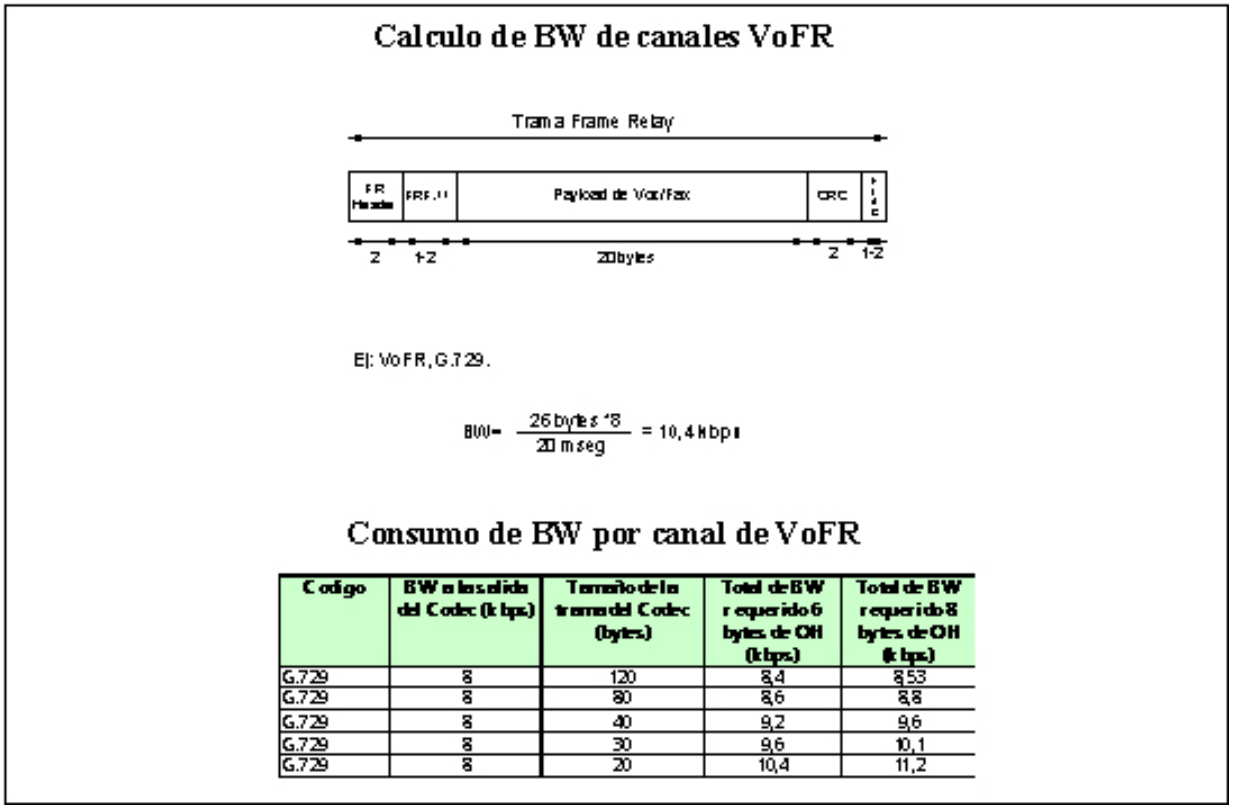


Figura 26 – Ancho de banda en VoFR

El transito de voz sobre redes Frame-Relay es el mas utilizado actualmente para redes privadas y permite por su diseño una calidad de voz aceptable y fácil de asegurar.

Voz sobre ATM VoATM

La red ATM, Asynchronous Transfer Mode, es una red multiservicio, de alta velocidad y tecnología escalable preparada para transmitir distintas aplicaciones como ser datos, voz y video; adaptándose fácilmente a cada una de ellas.

La característica de estar diseñada sobre las bases de conmutación de celdas de tamaño fijo lo hace más eficiente para transmitir voz. Las principales características de VoATM son:

- Usa celdas cortas y de tamaño fijo (53 bytes).
- Protocolo orientado a la conexión.
- Soporta múltiples tipos de servicios.
- Soporta 5 calidades de servicio.
- Emula circuitos TDM.
- Minimiza el Delay y el Jitter.

Existen distintas formas de implementar VoATM:

- VoATM utilizando AAL5: Se utiliza para transportar tanto Voz comprimida (G.729, G723) como Voz sin Comprimir (G.711).
- VoATM utilizando AAL1: Se utiliza para transportar circuitos TDM (nx64) utilizando la funcionalidad de Circuit Emulation Services CES.

El cálculo de ancho de banda de los canales de VoATM debe realizarse según el siguiente esquema:

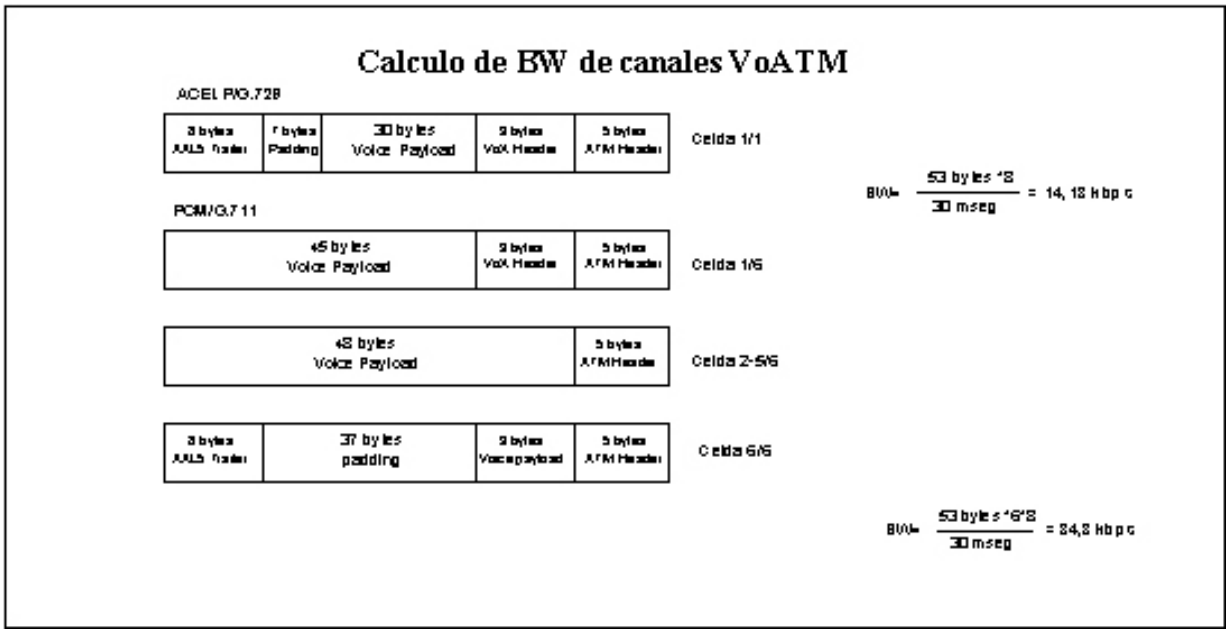


Figura 27 – Ancho de banda en VoATM

El transito de voz sobre redes ATM permite por su diseño proveer la mejor calidad de voz sobre redes de datos, pero no es la mas utilizadas por ser mas costosa que las soluciones de Frame-Relay para redes privadas.

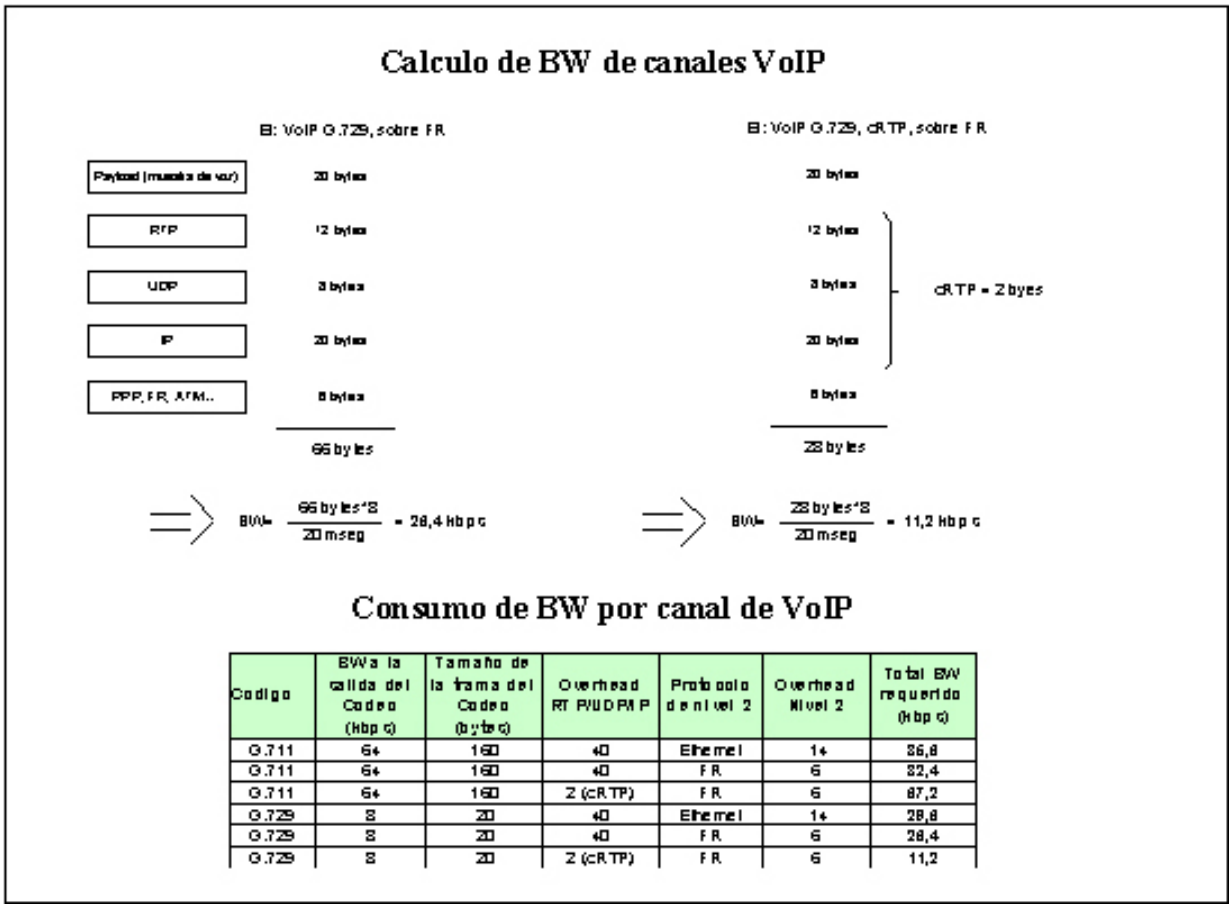
Voz sobre IP VoIP

El IP es un protocolo que permite que lo paquetes puedan tomar diferentes caminos entre los equipos de borde y todos los caminos son compartidos por paquetes de diferentes transmisiones.

Esto permite un eficiente uso de los recursos de red, por lo que los paquetes son ruteados sobre los caminos con menor congestión. El header (encabezado) de IP es mas largo (20 bytes) comparado con los header de Frame-Relay (2 bytes) y los de las celdas ATM (5 bytes), esto genera mayor overhead. Las principales características de VoIP son:

- Priorización de tráfico con técnicas de IP QoS.
- Fragmentación IP.
- Compresión de voz.
- Buffer jitter.
- Supresión de silencio.
- Cancelación de eco.
- Permite remotizar nodos de voz flexiblemente.
- Habilita fácilmente aplicativos de voz para usuarios finales.
- Permite realizar transito de voz vía Internet.

El cálculo de ancho de banda de los canales de VoIP debe realizarse según el siguiente esquema:



Codigo	BW a la salida del Codec (kbps)	Tamaño de la trama del Codec (bytes)	Overhead RTP/UDP/IP	Protocolo de nivel 2	Overhead Nivel 2	Total BW requerido (kbps)
G.711	64	160	40	Ethernet	14	86,8
G.711	64	160	40	FR	6	82,4
G.711	64	160	2 (cRTP)	FR	6	67,2
G.729	8	20	40	Ethernet	14	28,8
G.729	8	20	40	FR	6	26,4
G.729	8	20	2 (cRTP)	FR	6	11,2

Figura 28 – Ancho de banda en VoIP

El transito de voz sobre redes IP es el mas utilizado actualmente para redes publicas permitiendo realizar transito de voz a nivel de Carriers de VoIP (trunking de voz), aplicativos de usuarios de voz sobre Internet y telefonía IP. Para redes privadas comienza a utilizarse recientemente suplantando a Frame-Relay, por la flexibilidad del protocolo e integración con los servicios de voz sobre Internet, aunque comparado con el resto de las tecnologías de voz sobre redes de datos en redes IP es mas difícil asegurar la calidad de la voz.

Comparativa entre VoFR/VoATM/VoIP

Tanto las redes de datos Frame-Relay, ATM e IP poseen sus ventajas y desventajas para cursar tráfico de voz. La siguiente tabla compara las variables más significativas entre las diferentes tecnologías:

	Utilización de ancho de banda	Delay	Jitter	Calidad de servicio	Trunking de voz	Redes privadas	Telefonia IP	Remotización	Evolución	Costos
VoIP	11,2Kbps	Medio	Alto	Medio	Si	Si	Si	Si	Si	Medio
VoFR	10,4Kbps	Medio	Medio	Medio	No	Si	No	No	No	Bajo
VoATM	14,3Kbps	Bajo	Bajo	Alto	No	Si	No	No	No	Alto

Tabla 4 – Comparativa de voz

Utilización de ancho de banda: Ver tabla de cálculo de anchos de banda.

Delay: Se establece la medida ***bajo*** por ser ATM la red con menor delay por el diseño de conmutación de celdas del mismo tamaño. Se establece el indicador ***medio*** indicando que este tipo de redes posen un delay mayor que ATM, pero puede controlarse dentro de los parámetros recomendaos por la ITU.

Jitter: Se establece la medida ***bajo*** por ser ATM la red con menor delay por el diseño de conmutación de celdas del mismo tamaño. Se establece ***medio*** indicando que este tipo de redes posen un jitter mayor que ATM y las propiedades de priorización permiten mantenerlo en valores mejores que los indicados con el indicador de ***alto***, en donde este ultimo indica el tipo de redes que posee el mayor jitter teniendo que aplicar técnicas de cancelación de eco y priorización de trafico para mantenerlo en los valores aceptables.

Trunking de voz: Indica la posibilidad de realizar transito de voz entre Carriers, mayormente se realiza mediante Internet conectando a nivel IP gateways de voz encargados de paquetizar la voz para ser transmitida por redes de datos y suplantar a los enlaces dedicados del tipo NxE1 o NxT1 utilizados como canales de voz.

Redes privadas: Indica la posibilidad de utilizar las redes de datos privadas para cursar tráfico de voz.

Telefonía IP: Indica la posibilidad de brindar el servicio de telefonía IP, en donde las terminales telefónicas convencionales se remplazan por terminales IP.

Remotivación: Indica la posibilidad de extender la red de datos que transporta voz, a puntos remotos fuera del alcance de la red de datos que proveen el servicio localmente. La flexibilidad de IP por medio de Internet o VPNs IP, permite extender el dominio de transito de voz sobre redes de datos sobre cualquier punto remoto que sea alcanzable por el protocolo IP.

Evolución: Indica el estado de evolución de las tecnologías, en donde actualmente la telefonía IP, el trunking de voz y el éxito de las VPNs IP generan una continua evolución para mejorado las técnicas de calidad de voz e integración de soluciones.

Costos de transito en redes privadas: El indicador utilizado limita el alcance a comparar los costos de transito de voz sobre las diferentes redes de datos. El indicador ***bajo*** referencia a que las redes Frame-Relay son las más desplegadas para este tipo de soluciones y el costo es simplemente configurar un DLCI exclusivo para voz. El indicador ***alto*** referencia el costo del transito sobre redes ATM, la utilización de mayor ancho de banda que el resto de las redes. El indicador ***medio*** referencia que sobre un vinculo IP será necesario aplicar técnicas de QoS que elevaran el costo sobre Frame-Relay.

Como conclusión entre las variantes de voz paquetizada se destaca la VoIP por la flexibilidad que posee para adaptarse a los nuevos servicios. Nativamente la calidad de servicio sobre IP es menor a la de Frame-Relay o ATM, pero utilizando técnicas de calidad de servicio QoS pueden lograrse valores similares. Para esto MPLS brinda un soporte de QoS que logra equiparar la calidad de servicio con redes del tipo orientadas a la conexión.

Clave – Seguridad

Si bien la seguridad es una clave fundamental para el diseño de las redes, no muchas empresas conocen en detalles cuales son los problemas de seguridad que las redes pueden sufrir y mucho menos como combatirlos. Partiendo de este punto, es donde nace el prejuicio en cuanto a la seguridad de las VPNs basadas en IP y su comparación con redes tradicionales punto a punto o ATM/Frame-Relay.

Una de las trabas comerciales más importante para los ejecutivos de venta de los Carrier o proveedores de servicios, es hacer comprender a sus clientes de redes basadas en VPN/MPLS que sus redes son tan seguras como las redes tradicionales. En este apartado identificaremos las claves que ayudaran a comparar los niveles de seguridad de cada tipo de red.

Clasificación de ataques

Los clientes de los Carriers y proveedores de servicios hacen foco no solo en la seguridad de sus elementos de red, sino en la seguridad que la red transporte del Carrier o proveedor de servicio les brinda. A continuación se clasifican los ataques a la red transporte dependiendo si se basan en redes ATM/Frame-Relay o VPN/MPLS:

- Los ataques de nivel 2 (capa de enlace), no son muy sencillos de realizar, ya que para poder hacerlo el atacante debería estar conectado directamente a la red, por ende las redes de Carriers o proveedores de servicios del tipo ATM/Frame-Relay, solo pueden ser atacadas desde un cliente.
- Las VPNs/MPLS se despliegan sobre redes IP y este protocolo por ser el más difundido dentro de los dominios de redes, es el más vulnerable de los protocolos. Muchas personas conocen el protocolo y para los hackers es más sencillo realizar ataques a nivel 3, ya que no necesitan una adyacencia a la red, por que las direcciones IP son alcanzadas desde cualquier otro punto, dirección IP, que tenga conectividad mediante el protocolo IP. Por ende, una red basada en VPN/MPLS podría ser atacada si posee conectividad IP con otras redes por ejemplo Internet.
- La tecnología VPN/MPLS necesita de protocolos de ruteo y habilitar servicios que se basan en protocolos TCP, UDP e ICMP. Estos protocolos también son utilizados para realizar ataques.

Clasificación del nivel de seguridad

Comprender los requisitos de seguridad de las empresas es muy importante para comprender su diseño de red. Los requerimientos de seguridad varían dependiendo del tipo de empresa, como ser bancos, universidades, Pymes u otras.

Con el objetivo de simplificar la clasificación de seguridad de una red de transporte, se proponen tres niveles que identifican los requerimientos de seguridad:

- Nivel aceptable: En este nivel la red de transporte del Carrier o proveedor de servicios, brinda una separación física o lógica entre los vínculos de las distintas VPNs. De esta manera cada VPN posee sus propios vínculos, los cuales son independientes por clientes.
- Nivel deseable: En este nivel la red de transporte del Carrier o proveedor de servicios, permite asegurar que los elementos de la red de transporte brindan un alto nivel de seguridad ante vulnerabilidad de tipo Denial Of Services “DoS” y seguridad de gestión de los equipos. Entre los ataques mas comunes dentro de estas modalidades se encuentran el flood routing (inundación de ruteo), en donde se generan una gran cantidad de actualizaciones sobre los protocolos de ruteo de las VPNs; y el flood ICMP traffic (inundación de trafico ICMP), en donde se generan ráfagas indeseadas de trafico ICMP con destino a los diferentes equipos de red.
- Nivel requerido: En este nivel la red de transporte del Carrier o proveedor de servicios, esta preparada para que los datos transportados por las VPNs viajen encriptados entre los diferentes puntos de las VPNs. De esta forma si el tráfico es interceptado en cualquier punto de las VPNs, los datos están encriptados.

La siguiente Tabla resume como los diferentes tipos de redes de transportes se relacionan con los diferentes niveles de seguridad:

	Nivel aceptable	Nivel deseable	Nivel requerido
Red de transporte punto a punto	Los vínculos se construyen a nivel físico, cada VPN posee sus propios vínculos físicos que la componen.	La red de transporte esta compuesta por equipos de transmisión, los que están exentos de sufrir ataques lógicos de nivel 2 o nivel 3.	No poseen nivel de encripción. Es posible requerir líneas físicas encriptadas por hardware.
Red de transporte ATM/ Frame-Relay	Los vínculos se construyen a nivel de la capa de enlace (nivel 2). El identificador de cada vinculo esta compuesto por un PCV de Frame-Relay o ATM. Los PVC son definidos punto a punto entre los diferentes sitios de las VPNs.	Los ataques sobre equipos de redes ATM o Frame-Relay, deben realizarse desde un sitio adyacente, lo que condiciona a que solo desde los equipos de clientes conectados a la red de transporte podría sufrirse algún tipo de ataque.	No poseen nivel de encripción. Es posible encriptar a un nivel superior sobre los enlaces de nivel2, utilizando IPSec en la capa de red (nivel 3) entre los equipos de cliente.
Red de transporte VPN/ MPLS	Los vínculos se construyen a nivel de capa de red (nivel 3). El identificador de VRF dentro del paquete MPLS, identifica cada VPN. Los paquetes MPLS son direccionados entre los diferentes sitios de las VPNs utilizando una tabla de ruteo independiente para cada VPN.	Los ataques sobre equipos de redes IP, son los más comunes. Teniendo en cuenta que el protocolo IP es alcanzable desde cualquier punto, siempre y cuando exista una ruta que los comunique, los equipos de red pueden ser alcanzados por ejemplo desde Internet y por ende sufrir diversos ataques.	La integración de las VPN/MPLS con IPSec permite fácilmente que la red de transporte integre la encripción a los vínculos de las VPNs.

Tabla 5 – Comparativa de redes x seguridad

Seguridad de VPNs/MPLS vs. Frame-Relay y ATM

Para analizar la seguridad de cada red queda claro que deberá realizarse un análisis individual, realizando una prueba integral con los diferentes tipos de ataques posibles, de esta forma los clientes que requieran una VPN sobre redes de datos podrán asegurar y medir el nivel de seguridad ofrecido por los Carriers y proveedores de servicios.

Pero teniendo en cuenta que las redes IP poseen un riesgo mayor al resto de las tecnologías que soportan VPN como ser Frame-Relay o ATM, los Carriers y proveedores que brindan VPN/MPLS necesitan equiparar su nivel de seguridad contra las redes privadas sobre Frame-Relay y ATM.

Existe un mayor escepticismo por parte de los clientes sobre redes VPN basadas en IP, por lo que los Carriers deberán mostrar a sus clientes como esta nueva tecnología basada en dispositivos IP puede ser tan segura como las redes VPNs tradicionales.

Para esto basándome en las RFCs y draft realice una análisis de los puntos claves para mantener la seguridad en redes VPN/MPLS. Si bien las “RFCs RFC 2547 (rfc2547) - BGP-MPLS VPNs” y “RFC 2917 (rfc2917) - A Core MPLS IP VPN Architecture” realizan una aproximación sobre los aspectos mas importantes de la seguridad, tomando como referencia los puntos del draft “draft-behringer-mpls-security-10” realice el siguiente análisis.

- Separación de direccionamiento IP, ruteo y tráfico.

La tecnología VPN/MPLS naturalmente realiza una separación de direccionamiento IP, ruteo y trafico; logrando esto con la utilización de etiquetas permite contener sobre una misma red varias VPNs con la posibilidad que estas posean solapamiento de direccionamiento IP. Recordemos que con la utilización de etiquetas los routers se independizan de las direcciones IP, logrando una separación de ruteo y trafico.

- Ocultamiento de la infraestructura de la red de core.

Es imprescindible que los equipos de core de la red del proveedor de servicio se oculte de las redes de clientes y de la red Internet. De la misma forma que las redes ATM o Frame-Relay simulan una conexión punto a punto entre los sitios de cliente, las redes IP deben simular esta situación haciendo “invisibles” ante los sitios de clientes; además deberán ocultarse de la red Internet por posibles ataques.

Para lograr el ocultamiento se establece direccionamiento IP privado o direccionamiento publico (no publicado a Internet) sobre el core de la red, sobre los equipos P y las interfaces hacia los routers PE. De esta forma estos equipos se ocultan de Internet permitiendo aislar los posibles ataques con este origen.

- Resistencia a los ataques.

Tomando como medición de resistencia, la posibilidad que desde una VPN se acceda a otra VPN o que desde otro punto pueda vulnerarse la seguridad de un equipo router., se identifican tres posibles ataques:

  - Ataque DoS entre VPNs: Debido a la separación de tráfico no es posible realizar DoS desde una VPN hacia otra VPN. La única posibilidad de ataque DoS puede ser así misma.
  - Ataque a un routers de Carrier desde una VPN: Debido al ocultamiento de los equipo P del core, desde un equipo CE podrá solo atacarse a los equipos PE que formen parte de la VPN. Para evitar estos ataques los equipos PE deberán instalar medidas de seguridad que permitan contrarrestar posibles ataques DoS. Entre las medidas de seguridad se encuentran listas de acceso, autenticación MD-5 y la posibilidad de configurar parámetros que restrinjan el ruteo entre PE-CE.
  - Ataques a un router de Carrier desde Internet: Nuevamente es imposible atacar directamente los equipos P, pero los equipos PE son alcanzables desde Internet por lo tanto podrían sufrir ataques DoS. Para combatir esto nuevamente es necesario proteger los equipos con listas de acceso que restrinjan el acceso no autorizado, parámetros que inhabiliten o minimicen los ataques DoS.

Constantemente surgen nuevos parámetros, draft y RFCs que mejoran la seguridad en un entorno VPN/MPLS, los proveedores de equipamiento se preocupan en hacer que sus dispositivos routers se asemejen, en lo que a seguridad respecta, a dispositivos de nivel 2 como switches ATM o Frame-Relay.

- Spoofing de etiquetas

El spoofing de etiquetas consiste teóricamente que desde un equipo CE o desde Internet se falsifiquen las etiquetas MPLS y por ende se pueda ingresar a una VPN de forma no autorizada. En principio los equipos en Internet y los equipos CE no manejan etiquetas MPLS, simplemente direccionamiento IP, por lo que los equipos PE deben no permitir que ingresen etiquetas desde el exterior. Esta técnica permite que los routers PE solo acepten etiquetas desde adentro del core MPLS, pero no así desde equipos CE o desde Internet, por lo que limita ataques de spoofing de etiquetas.

Igualmente debido al escepticismo de los clientes, los proveedores de servicios y compañías proveedoras de equipamiento contratan a consultoras de seguridad para que realicen test de seguridad sobre sus redes MPLS, y de esta forma tener una constancia emitida por un ente independiente que asegure que sus redes son tan seguras como redes del tipo ATM/Frame-Relay.

Para citar un ejemplo Cisco Systems, proveedora de equipos de red y uno de los principales propulsores de MPLS, contrato a la empresa Miercom con el fin de realizar un reporte de seguridad de las VPN/MPLS. Este reporte tuvo como conclusión que las redes VPN/MPLS son tan seguras como las redes privadas sobre Frame-relay y ATM.

Aunque existe un alto escepticismo de los clientes sobre la seguridad brindada por redes del tipo IP. Las redes VPN/MPLS tienen herramientas para equiparar la seguridad con redes del tipo ATM o Frame-Relay.

Clave – Costos

Desde el punto de vista del cliente (empresa que contrata una VPN/MPLS) se deberán tener en cuenta algunas variables que se pondrán en juego a la hora de decidir la migración. Entre los costos que genera instalar y mantener una red tradicional contra una red del tipo VPN, se deben tener en cuenta:

Equipo de cliente en redes tradicionales

Es el equipo de comunicaciones encargado de enviar y recibir la información de la red Frame Relay o ATM. El CPE tiene como función traducir el protocolo de entorno LAN al protocolo de entorno WAN.

Mayormente los proveedores de servicios ofrecen el servicio Frame-Relay/ATM en dos modalidades:

Con equipo de cliente (con CPE): En donde se le provee al cliente el vínculo asociado con un equipo de cliente. En este caso el CPE es entregado en la modalidad de comodato, permitiendo que el cliente solo pague un plus como garantía del equipo, pero permaneciendo la titularidad del equipo a nombre del proveedor del servicio.

Sin equipo de cliente (sin CPE): En caso que el cliente decida instalar su propio equipamiento, el proveedor puede realizar la gestión del mismo siempre y cuando corresponda a algún modelo anteriormente probado por la compañía proveedora del servicio.

Los costos de estos equipos dependerán de las velocidades de conexión requerida y la capacidad de procesamiento asociada al protocolo de ruteo elegido. A continuación se indican algunos modelos de equipos CPE y su costo asociado.

http://www.purebyte.co.uk/	Equipos Nuevos	
CPE Cisco	**USD**	**Partners**
1800	955,68	764,54
2600	1212,70	970,16
2611	1520,40	1216,32
2620	1502,30	1201,84
2800	1312,25	1049,80
2811	1665,20	1332,16
2821	2678,80	2143,04
http://www15.serrahost.com	Equipos Usados	
CPE Cisco	**USD**	
2500	300,00	

Tabla 6 – Costos CPEs

Nota: Los precios indicados son indicativos, tomados de las fuentes indicadas en septiembre de 2005. Solo se tiene en cuenta el valor del equipo entregado en el país de origen, para lo cual la importación, gastos de envió y otros deberán adjuntase al costo indicado.

Para el caso de ser comprados por medio de partners (son ejemplos en Argentina las empresas Italtel, Sofnet, etc), estos equipos pueden llegar a tener una reducción en sus costos de hasta un 20%.

Equipo de cliente en redes VPN

El equipo de cliente router “CPE”, es el encargado de interconectar el sitio del cliente (sucursal, casa central, etc) con la red VPN/MPLS. Mayormente esta conexión se realiza con líneas punto a punto desde la casa del cliente hasta el punto de la red más cercano y puede utilizarse la red de transporte de SDH, ATM o Frame/Relay dependiendo del caso y las velocidades de conexión. Hacia el lado del cliente mayormente se conecta a un entorno LAN por medio de interfaces FastEthernet o Ethernet.

Las modalidades de servicio son idénticas a las descriptas anteriormente y los equipos CPE utilizados pueden ser los mismos a los utilizados en redes Frame-Relay/ATM o de mayor porte cuando se desean implementar los servicios de valor agregado que las VPN/MPLS facilitan.

Interconexión de sitios tradicionales

La interconexión entre sitios de cliente en una red ATM o Frame-Relay debe tener en cuenta la topología a utilizar. Recordemos que una red del tipo hub-and-spoke todas las sucursales apuntan a un sitio central, se utiliza esta tecnología para abaratar costos de interconexión de vínculos, pero deben incrementar el ancho de banda de la casa central para soportar el trafico entre sucursales.

Los costos para la interconexión dependen de los siguientes parámetros:

Línea de acceso: es el medio a través del cual se enlaza el equipo de conectividad del cliente con el nodo de red del proveedor más cercano a su domicilio.

Se trata de la línea digital de la del proveedor de servicios en todos los puntos donde hay cobertura de este servicio o de vínculos satelitales, radio, línea digital de otro operador.

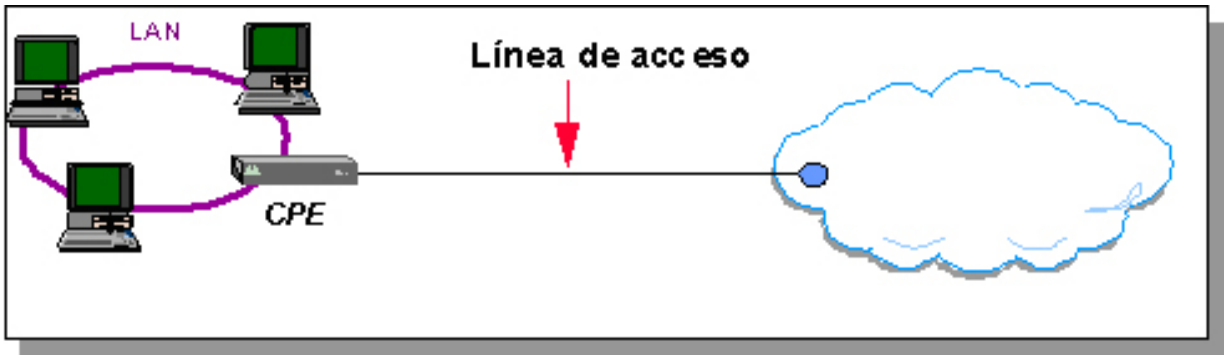


Figura 29 – Línea de acceso

Los parámetros que determinan el precio son:

- Velocidad de acceso: desde 64 kbps hasta 2048 kbps. Esta velocidad determina la capacidad máxima que puede alcanzar el servicio Frame Relay (access rate).
- Tipo de vínculo: terrestre o satelital.
- Área: Lugar geográfico donde se encuentra el sitio a interconectar.

Puerto: es la interfase que permite ingresar a la red del proveedor de servicios a una determinada velocidad la cual puede soportar múltiples PVC.

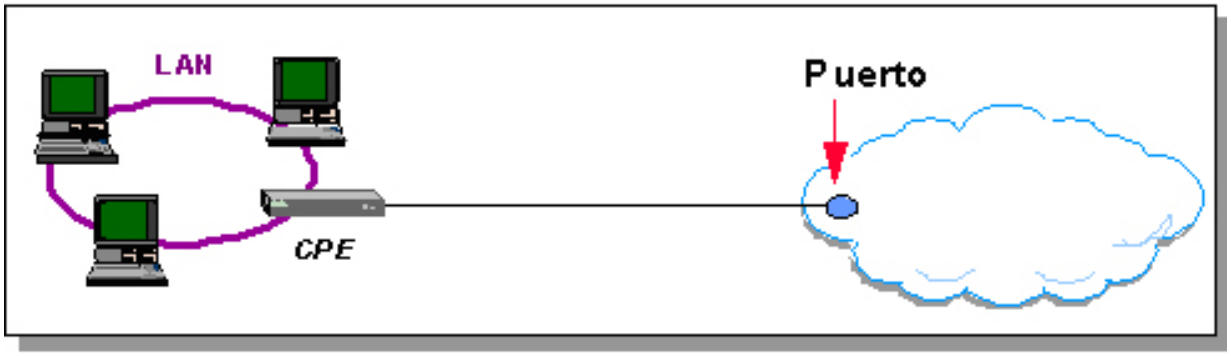


Figura 30 – Puerto de acceso

Circuito virtual permanente (PVC): es una conexión lógica identificada por ambos extremos que establece el proveedor de servicios. Cuando se configura el servicio, el PVC queda establecido en forma permanente.

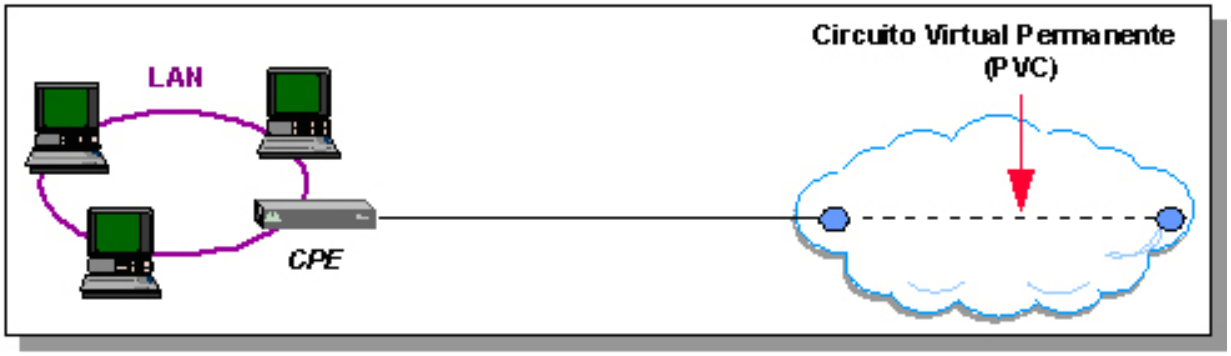


Figura 31 – Circuito virtual permanente

El PVC es full-duplex. Los parámetros que determinan el precio son:

- CoS, clase de servicio: se dispone de cuatro clases de servicio de acuerdo a lo definido en el protocolo frame relay. Estas clases son:

- Tiempo real (real time) para aplicaciones de voz y video.
- Bajo retardo (low delay) para aplicaciones SNA (protocolo propietario de IBM) e IPX.
- Caudal garantizado (committed throughput) para aplicaciones LAN to LAN.
- Mejor esfuerzo (best effort) para aplicaciones TCP/IP como intranets/extranets o acceso a Internet.

- Longitud del PVC: Depende de las distancias en Kilómetros.

Velocidad de acceso CIR + EIR (access rate): es la tasa de bits por segundo que el circuito tiene disponible para la transmisión de tramas en la modalidad de ráfagas. Si esta tasa supera el valor comprometido CIR, las tramas pueden ser descartadas en función de la disponibilidad de recursos de la red. Por encima de la velocidad de acceso, todas las tramas son descartadas. El servicio está disponible para las siguientes velocidades de acceso:

Velocidad de acceso
64 kbps
128 kbps
256 kbps
384 kbps
512 kbps
768 kbps
1024 kbps
1536 kbps
1920 kbps

Tabla 7 – Velocidades de acceso

Tasa de información comprometida CIR (committed information rate): es la tasa de bits por segundo que siempre está disponible para este circuito. Este valor se especifica en kbps aunque suele también indicarse en forma porcentual en relación a la capacidad máxima del circuito (access rate). El servicio está disponible para los siguientes valores de CIR:

CIR
2, 4, 6, 8, 10, 12, 14, 16kbps
24, 32, 40, 48, 56, 64 kbps
96, 128, 160, 192, 224, 256 kbps
320, 384, 448, 512 kbps
640, 768 kbps
896, 1024 kbps
1152, 1280, 1408, 1536 kbps
1664, 1792, 1920 kbps

Tabla 8 – Valores de CIR

Interconexión de sitios por VPN/MPLS

La utilización de la tecnología MPLS, permite realizar naturalmente una interconexión del tipo full-meshed, permitiendo aplicaciones peer-to-peer y ahorro de ancho de banda.

La interconexión de sitios de una VPN se realiza en última milla, mediante las redes SDH, Frame-Relay, ATM o MetroEthernet. Luego estas redes se interconectan a su vez a los equipos de la red MPLS. Teniendo en cuenta que la red MPLS no dedica recursos físicos a cada cliente, solo se estima un costo de utilización de ancho de banda sobre la red. Para lo que solo en el caso de la ultima milla se deberán tener en cuenta costos de vínculos dedicados.

Por lo explicado anteriormente el camino entre dos sitios de una VPN estará compuesto por el acceso a la red MPLS sumado a la conexión de última milla necesario para conectar al cliente a la red MPLS.

Los costos para la interconexión dependen de los siguientes parámetros:

Línea de acceso: similar a lo detallado para redes tradicionales, pero se agrega la posibilidad de también acceder mediante redes SDH y MetroEthernet.

Los parámetros que determinan el precio son:

- Velocidad de acceso: desde 64 kbps hasta 1 Gbps. Estas velocidades dependen de la red de acceso utilizada.
- Tipo de vínculo: terrestre o satelital.
- Área: Lugar geográfico donde se encuentra el sitio a interconectar.

Puerto: similar a lo detallado para redes tradicionales con la posibilidad de soportar múltiples PVC, VLANs o subinterfaces.

Acceso a la VPN: Una vez dentro de la red del proveedor, no se fija una velocidad como se hace en un PVC de las redes tradicionales. Se le asigna el ancho de banda total que la red del proveedor disponga (actualmente se implementan redes de hasta 10 Gbps) y la velocidad queda limitada a la velocidad configurada en el puerto de acceso.

Los parámetros que determinan el precio son:

- QoS, calidad de servicio: se dispone de tres clases de servicio de acuerdo a lo definido en MPLS. Estas clases son:
  - Tiempo real (real time) para aplicaciones de voz y video.
  - Misión Critica para aplicaciones LAN to LAN.
  - Mejor esfuerzo (best effort) para aplicaciones TCP/IP como intranets/extranets o acceso a Internet.

Mantenimiento de redes tradicionales

El mantenimiento de las redes tradicionales crece en complejidad a medida que la red crece debido al incremento de vínculos virtuales. Por otra parte el know-how del personal es mayor con respecto a este tipo de redes, los procedimientos y sistemas de gestión tienen un tiempo de maduración mayor al de las redes de tipo MPLS.

Mantenimiento de redes VPN/MPLS

La complejidad de mantenimiento para este tipo de redes no aumenta por el crecimiento de red, debido a que no sufre un incremento de vínculos a medida que la red crece. El personal que mantiene estas redes es mayormente el mismo que mantiene o mantenían las redes tradicionales por lo que su know-how sobre este tipo de redes es menor. Así mismo los procedimientos y sistemas de gestión no tienen un nivel de maduración acorde con el crecimiento de la tecnología.

Comparativa de costos entre VPN/MPLS y redes tradicionales

Las variables identificadas en esta sección nos permitirán realizar una comparativa de costos en conjunto con lo investigado en el mercado local e internacional.

- Equipos CPE

Los equipos CPE que son utilizados para redes tradicionales pueden utilizarse para redes VPN/MPLS, por lo que los costos para los equipos de clientes son independientes al tipo de red. Dependiendo de las necesidades de los clientes las VPN/MPLS pueden incorporar equipos más costosos para servicios de valor agregado.

- Línea de acceso

Se utilizan las mismas líneas de acceso, por lo tanto el tipo de red no varía el costo de la línea. Solo para velocidades mayores a 2Mbps la tecnología VPN/MPLS puede ofrecer servicios a mayor costo.

- Puerto y acceso

Los costos asociados al puerto y acceso están directamente relacionados al grado de amortización de los equipos de red del proveedor de servicio. Por lo tanto el costo de un PVC sobre una red tradicional es menor al costo de acceso a una VPN en redes MPLS.

- Topología

Si tomamos como base el mismo costo de un vínculo sobre la red tradicional que sobre la red MPLS, es significativa la ventaja de esta ultima tecnología por la posibilidad de brindar al mismo costo una red full-meshed que una red hub-and-spoke tradicional. En la próxima figura se puede ver una comparativa de costos entre una red tradicional hub-and-spoke y full-meshed contra una red VPN/MPLS.

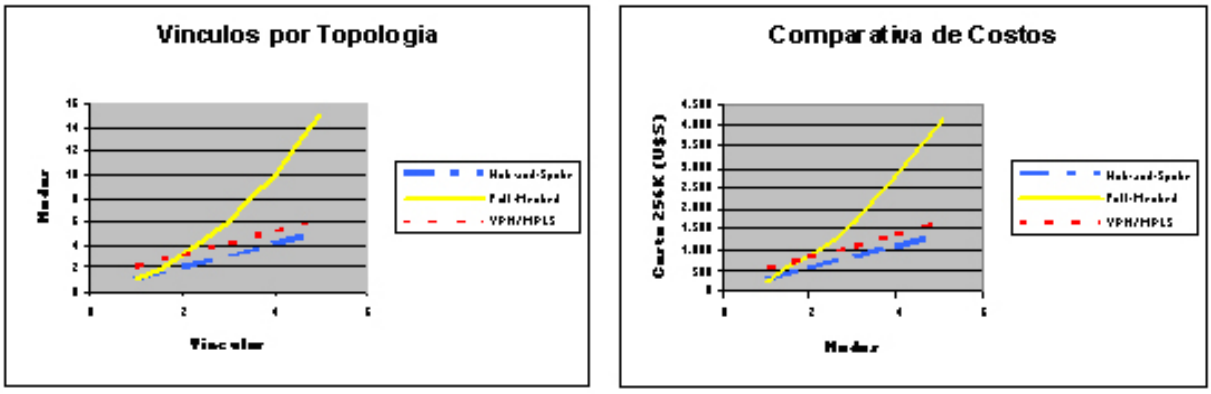


Figura 32 – Comparativa de costos x vinculo

Nota: Se tomo como base vínculos de 256Kbps, costo de alquiler mensual expresado en U$S a valor del mercado en Febrero del 2005.

- Know-How

Otra variable a tener en cuenta es el Know-How, que si bien no puede realizarse un cálculo exacto, sobre esta variable impactan costos de capacitación; costos relacionados al tiempo, sabemos que el tiempo es dinero, por lo que el costo asociado al tiempo invertido en implementar una tecnología no debe perderse de vista. En la siguiente figura se compara la variable know-how sobre las diferentes tecnologías.

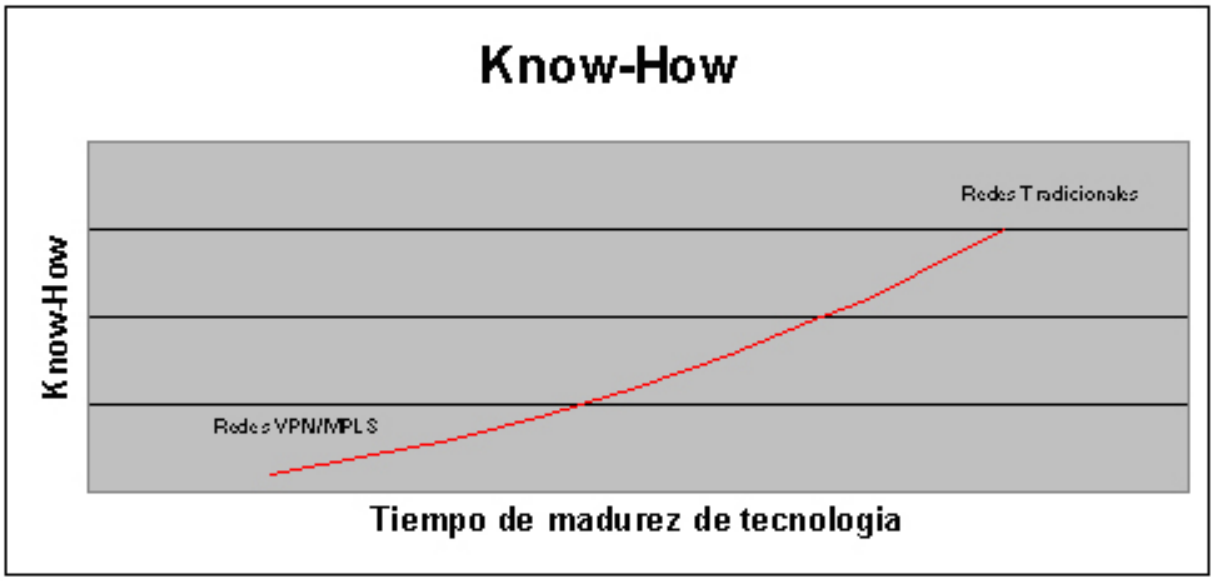


Figura 33 – Comparativa x Know-How

Clave - Evolución

La evolución de las redes es la clave que permite generar competencia, ya que la evolución sobre una red permite mantenerla fuera de la obsolescencia, incrementar el presupuesto para la inversión y generar nuevos servicios.

Integración de redes

Si bien la integración comenzó como una necesidad de bajar costos, hoy es la base principal para desarrollar nuevos servicios. La integración de redes necesita de una red robusta, rápida y que permita implementar servicios con diferentes calidades.

Se demostró que MPLS es la mejor opción para esta integración, por cumplir con todos los requerimientos de red y la posibilidad de aprovechar equipamiento existente de redes tradicionales.

Para el caso de las VPN, los clientes también necesitan una evolución, ahorrando costos de vínculos mediante la sinergia de las redes e integrando servicios bajo un mismo concepto de red. Para esto las VPNs basadas en MPLS son en la actualidad, la mejor forma de transportar servicios del tipo peer-to-

peer que requieren de una conectividad full-meshed. Además la adaptación y fácil integración con VPNs IPSec para las conexiones remotas hacen que este tipo de redes sean las más adecuadas para cubrir todas las necesidades de los clientes.

Integración de servicios

En este caso el transporte de voz fue el principal motor de integración, los altos costos y deficiente utilización del ancho de banda hicieron buscar la alternativa del transporte sobre redes de datos. Una vez en la misma red la integración la voz y los datos permitieron generar nuevos servicios como telefonía IP, PC teléfono, mensajería unificada de voz y datos entre otros.

Las VPNs basadas en MPLS hacen la integración y generación de servicios muy sencilla ya que permiten sobre un mismo vinculo físico y lógico transportar diferentes tipo de de servicios, simplificando la arquitectura de red del Carrier y del cliente.

En Argentina los proveedores de servicios están comenzando a ofrecer el servicio de VPN/MPLS a sus clientes, por ende la mayor cantidad de clientes se encuentran aun brindando sus servicios con redes de tecnología tradicional.

La principal estrategia de los Caries no es entonces atraer nuevos clientes sobre redes VPN/MPLS, sino la de convencer a los clientes existentes a utilizar esta nueva tecnología argumentando las posibilidades de integración y crecimiento a menor costo. Esta estrategia influye directamente en los precios hacia del servicio haciendo que el Carrier en cada caso proponga la migración mas adecuada al cliente y ofreciendo mejores precios sobre la red VPN/MPLS que sobre las redes tradicionales. Al mismo tiempo los Carriers comienzan a desmantelar sus redes tradicionales, ahorrando costos para ser invertidos en las nuevas redes.

La estrategia a implementar es ofrecer a sus clientes existentes que cualquier crecimiento de red ya sea un nuevo sitio o un incremento de ancho de banda se realice con la nueva tecnología, así entonces comienza el primer paso a la migración definitiva.

Las perspectivas comerciales crecen ya que las redes VPN/MPLS posibilitan ofrecer servicios de valor agregado como VoIP, video y aplicaciones peer-to-peer.

Capitulo IV – Caso de Estudio

Objetivo

El caso de estudio tiene como objetivo migrar hacia una VPN/MPLS la infraestructura de red de una gran empresa Argentina, proveedora de productos alimenticios, actualmente construida sobre enlaces Frame-Relay y ATM.

La evolución propuesta deberá contemplar los actúales servicios que el cliente posee, teniendo como dificultad seguir manteniendo las mismas prestaciones, el acuerdo de nivel de servicio “SLA” y disponibilidad brindados sobre la red Frame-Relay/ATM; y adicionalmente la propuesta deberá contener las oportunidades, desventajas y la evolución que las VPN-IP ofrecerán sobre el cliente.

Alcance

El alcance del caso de estudio estará dado por los siguientes parámetros:

- Migración de la topología actual sobre una red ATM/Frame-Relay a la topología VPN/MPLS sobre una red IP.
- Migración de los servicios actuales del cliente sobre la red propuesta.
- Posibilidad de evolución, oportunidades y desventajas.
- Estudio de impacto en la operación, supervisión de la red del cliente.
- Estudio de performance de la red propuesta vs. La red actual.
- Estudio de costos de la migración.

Necesidades del cliente

Para comprender las necesidades del cliente, comenzaremos detallando su red actual y los servicios existentes; de esta forma podremos comprender sus necesidades que luego utilizaremos para tomarlas como base de la red propuesta.

Dimensionamiento de la red actual

La red privada del cliente cuenta con treinta y tres (33) sitios remotos y tres (3) sitios principales, los cuales presentan acceso totalmente implementados sobre la red ATM y Frame-Relay sobre enlaces

arrendados al proveedor de telecomunicaciones (Carrier).

A continuación se adjunta el detalle de los accesos sobre la red ATM/Frame-Relay:

- 6 de 512Kbps, como accesos de contingencia.
- 3 de 64 Kbps, (1 de estos accesos es vía satelital).
- 8 de 128 Kbps, (1 de estos accesos es vía satelital para backup).
- 1 de 256 Kbps.
- 2 de 512 Kbps.
- 4 de 768 Kbps.
- 3 de 1024 Kbps.
- 3 de 1922 Kbps.
- 3 de 34 Mbps.

A continuación se detallan otros enlaces:

- 2 enlaces punto a punto de 100Mbps.
- 4 enlaces PABX-PABX.

Equipamiento de la red actual

Sitios Principales

En cada uno de los tres sitios principales A, B, y C poseen:

- 1 x Equipo ADM-1 para accesos de Fibra Óptica SDH.
- 1 x Equipo Alcatel modelo 7270 (Equipo de tecnología ATM).
- 1 x Equipo Cisco 7200 VXR (equipo de tecnología IP).

Los sitios A y B utilizan el siguiente equipamiento para la conexión de los canales de voz a la PABX:

- 2 x Equipos Cisco 3810 en sitio A.
- 3 x Equipos Cisco 3810 en sitio B.

Sitios Remotos

Los sitios remotos cuentan con accesos terrestres por par de cobre, radio enlace o fibra óptica. El equipamiento asociado esta compuesto en su mayoría por Cisco 3810, Cisco 2501 y Cisco 2610.

Data Center

La interconexión entre el cliente y el Data Center esta compuesta por 4 equipos Cisco 7200 VXR, equipados con placas STM-1 POS.

Conectividad lógica

Cada sitio remoto cuenta con:

- Un PVC de datos principal con un CIR definido. Este PVC tiene como concentrador el acceso del sitio A.
- Un PVC de respaldo con un CIR de 2Kbps. Este PVC tiene como concentrador el acceso del sitio B.
- Un PVC para la voz con un CIR de 10Kbps por cada canal de voz. Este PVC tiene como concentrador el acceso del sitio A o B según corresponda a cada sitio.

Sitio A

Cuenta con un PVC de datos con un CIR de 2Mbps contra el sitio B y de 4 Mbps contra el sitio C. Adicionalmente cuenta con un PVC (CBR) para establecer un enlace PABX-PABX contra el sitio B.

Sitio B

Cuenta con un PVC de datos con un CIR de 2 Mbps contra el sitio C. Adicionalmente cuenta con el enlace adicional PABX-PABX contra el sitio A.

Topología actual

La figura muestra el esquema de conexión lógico de la red actual del cliente y pretende describir los tipos de conexiones, equipamiento y distribución de ancho de banda.

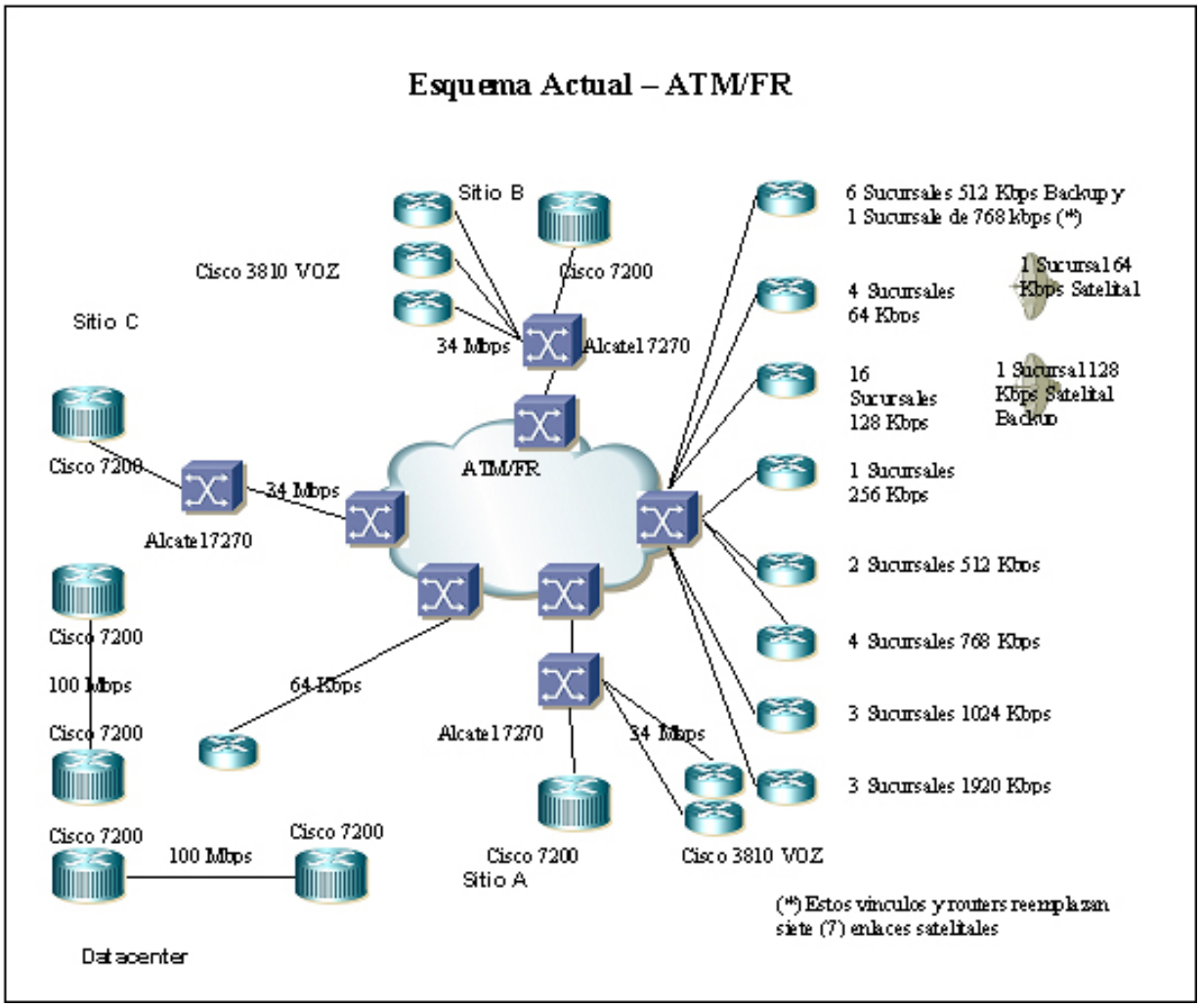


Figura 34 – Topología actual (caso de estudio)

Requerimientos del cliente para la propuesta

El proyecto de migración prevé las siguientes características complementarias, requeridas por el cliente:

- Servicio diferenciado por Calidad de Servicio (QoS), utilizando tres calidades capaces de manejar el tráfico de voz, video y datos.
- Garantizar un ancho de banda mínimo en los accesos de mayor ancho de banda para permitir la comunicación de todos los sitios aun en condiciones de saturación por tráfico.
- Mantener las capacidades actuales de segurización de la conectividad con el Datacenter, ante eventualidades en el sitio A.
- Esquema de backup discado.
- Ampliación y unificación de los enlaces en los sitios principales para permitir una optima integración de servicios.

Topología propuesta

La siguiente topología muestra la conectividad lógica de los distintos sitios del cliente, sobre una VPN/MPLS. La topología es a modo de ejemplo y solo intenta describir algunos los distintos anchos de bandas por sitios y la interconexión entre estos.

La definición de los anchos de bandas para los sitios A, B, y C serán explicados durante el desarrollo del documento.

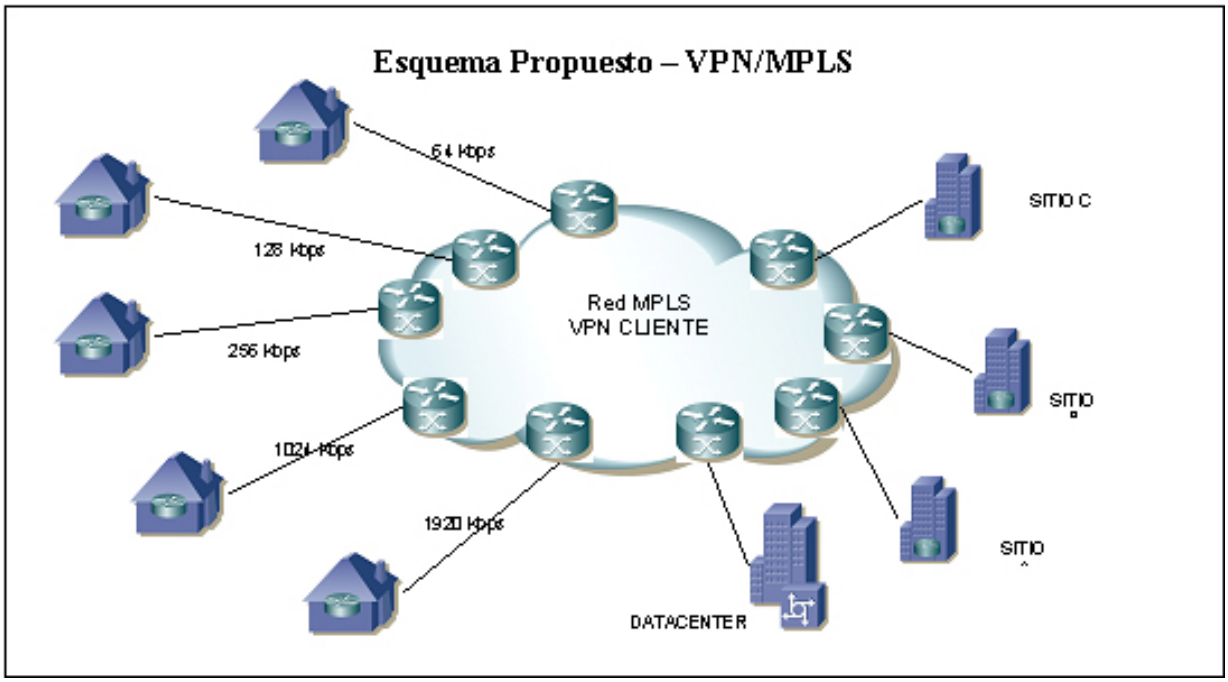


Figura 35 – Topología propuesta (caso de estudio)

Lineamientos de la propuesta para la migración

Los lineamientos para la propuesta pretenden ser la base del análisis y diseño de la migración de la red del cliente sobre la tecnología VPN-IP. A continuación se detallan los lineamientos:

- La arquitectura VPN-IP, se basará se el transporte sobre una red VPN/MPLS.
- El servicio de voz sobre Frame-Relay (VoFR) se migrará sobre voz sobre IP (VoIP).
- Se implementará un esquema de Calidad de Servicio en tres clases para diferenciar la voz, el video y los datos.
- Se implementará un sistema de backup discado.

Comparación de enlaces y ancho de banda

Teniendo en cuenta la topología actual (de enlaces punto a punto), la cantidad de enlaces es para brindar conectividad y contingencia se incrementa en forma exponencial, Además surge la necesidad de crear enlaces adicionales para diferenciar el trafico de voz sobre Frame-Relay en enlaces dedicados para esto y con una calidad de servicio diferenciado. En la siguiente figura se muestra la necesidad de enlaces.

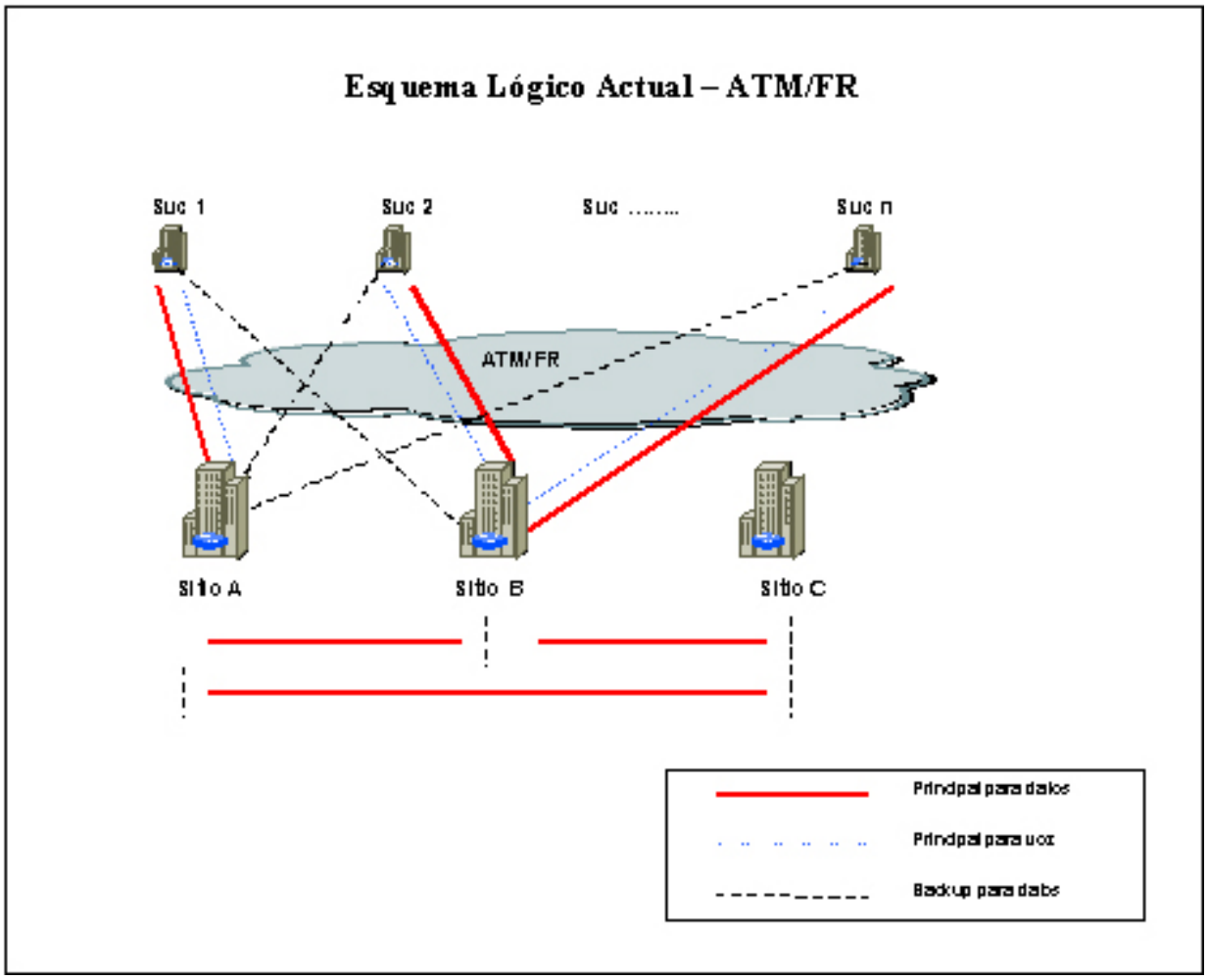


Figura 36 – Esquema lógico (red actual)

En la tabla siguiente se calculan la cantidad de enlaces lógicos y anchos de banda utilizados para la arquitectura de red actual.

	Sitios Principales			Cantidad de sucursales x ancho de banda									TOTAL	
	A	B	C	6	3	8	1	2	4	3	3	3	Ancho de banda	Enlaces
Enlaces de datos - A		2048	4056	512	64	128	256	512	768	1024	1922	34000	125582	35
Enlaces de datos - B			2048	2	2	2	2	2	2	2	2	2	2114	34
Enlaces de voz - A				10	10		10	10	10	10	10	10	250	25
Enlaces de voz - B						10							80	8
													128026	102

Tabla 9 – Dimensionamiento de red

Según la tabla de dimensionamiento para una cantidad de **33 sucursales y 3 sitios principales** se utilizan actualmente **102 enlaces** lógicos y un total de **ancho de banda de 128026Kbps**. Claramente la criticidad de la solución actual es la dependencia del costo por vínculo para establecer la topología de red.

Como alternativa a esta topología las VPN/MPLS brindan un esquema de conectividad mucho más simple, desligándose de la dependencia de la cantidad de enlaces por servicio o por redundancia. Así entonces la figura siguiente muestra como se simplifica la topología de red.

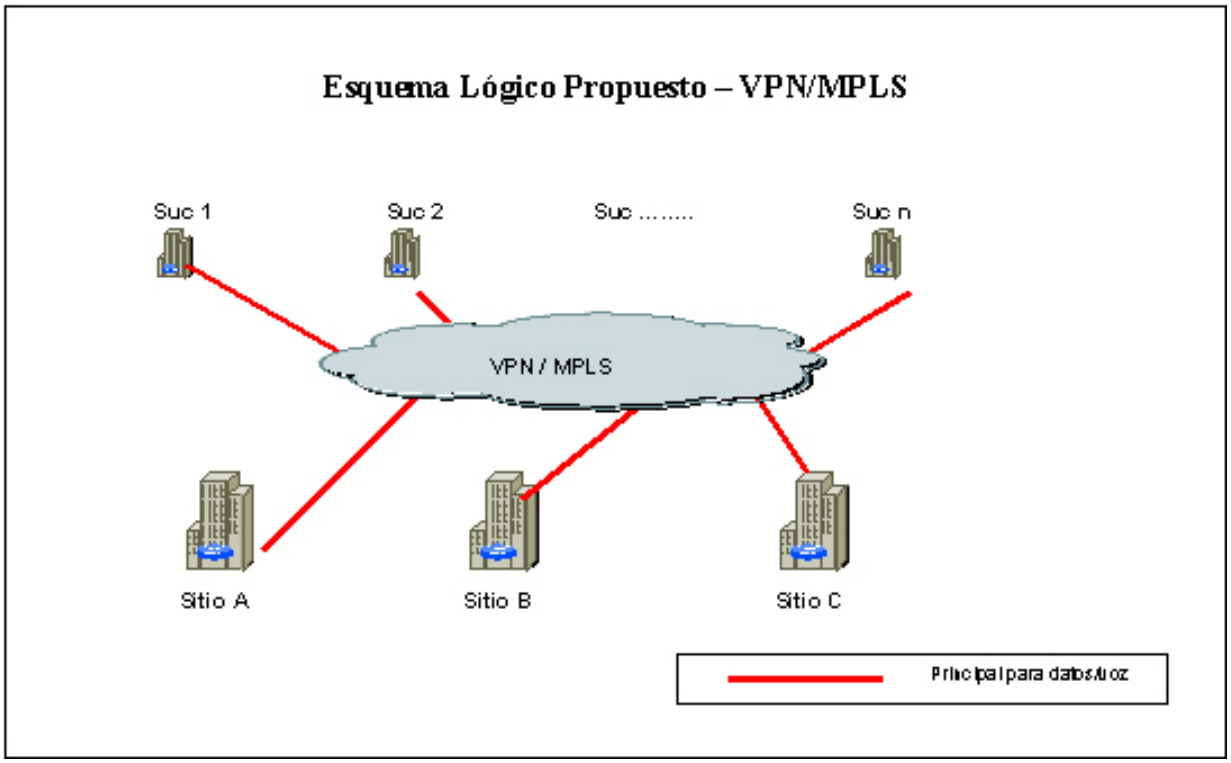


Figura 37 – Esquema lógico propuesto

En la tabla siguiente se calculan la cantidad de enlaces lógicos y anchos de banda utilizados para la arquitectura de red propuesta.

	Sitios Principales			Cantidad de sucursales x ancho de banda									TOTAL	
	A	B	C	6	3	8	1	2	4	3	3	3	Ancho de banda	Enlaces
Enlaces de datos/voz	6104	2048		532	84	148	276	532	788	1044	1942	34020	128290	36

Tabla 10 – Dimensionamiento propuesto

Según la tabla de dimensionamiento propuesta para una cantidad de **33 sucursales y 3 sitios principales** se utilizan actualmente **36 enlaces** lógicos y un total de **ancho de banda de 128290Kbps**. Claramente se denotan las ventajas de la solución propuesta marcando la independencia del volumen de sucursales del volumen de enlaces.

Supongamos ahora que la empresa decide incorporar 3 nuevas sucursales con enlaces de 512Kbps utilizando redundancia y un vinculo de voz; u otro ejemplo puede ser que la empresa decida incorporarle a cada sucursal 1 vinculo dedicado para transmitir video. La figura siguiente muestra la comparativa de cantidad de enlaces y ancho de banda utilizados en ambas soluciones.

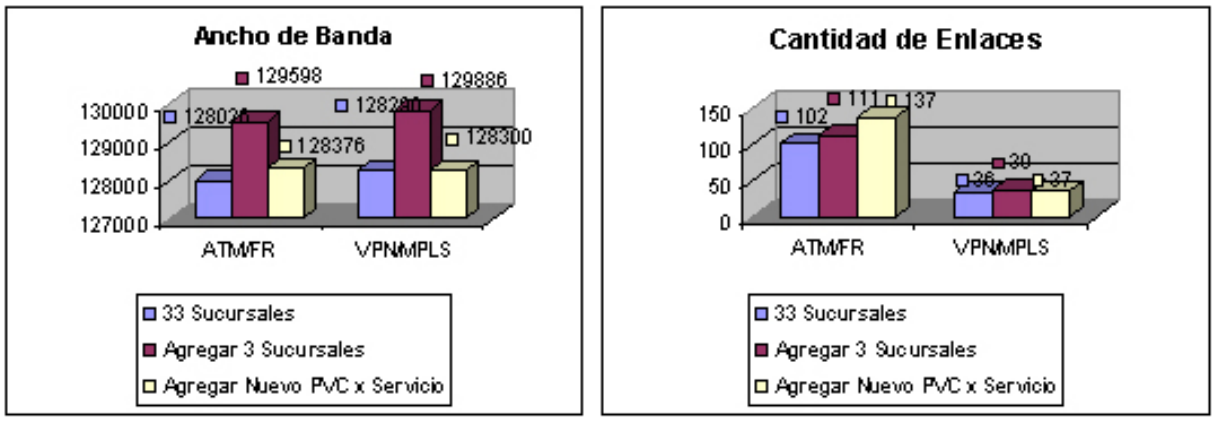


Figura 38 – Ahorro de enlaces y ancho de banda

Como conclusión de las figuras se destaca que con un mínimo incremento del ancho de banda total debido a la concentración de de trafico sobre los sitios principales, la cantidad de enlaces utilizados en la solución con redes VPN/MPLS es aproximadamente 3 veces menor a la cantidad de enlaces utilizadas en la solución ATM/Frame-Relay. De donde podemos aproximar la siguiente formula:

$$Cantidad\_enlaces\_VPNMPLS \cong \frac{(Cantidad\_enlaces\_ATMFR)}{3}$$

Pasos para la migración

Los pasos para lograr una exitosa migración sin afectar a los servicios brindados por la red del cliente, se acordaron mediante un documento detallado técnicamente y en conjunto con un cronograma de despliegue se establecieron los pasos a seguir.

Incorporación de sitios principales

La incorporación de los sitios principales - A, B y C - sobre la red VPN/MPLS, pero sin desconectarlos de la red actual ATM/Frame-Relay fue el primer hito para la migración. Esta nueva conexión de los sitios principales a la red VPN/MPLS permitiría entonces que el núcleo de la red del cliente tenga conectividad con la red sobre la que en el futuro próximo sus sucursales se interconectarían. Para esto el Carrier debería hacerse cargo de costos adicionales (placas para el equipamiento existente de los sitios A y B), estas placas permitirían conectar dichos sitios a una velocidad de acceso de 34Mbps . En la figura próxima se muestra la incorporación de los sitios a la red VPN/MPLS. Finalizada la migración el Carrier recupera las placas utilizadas como contingencia durante la migración.

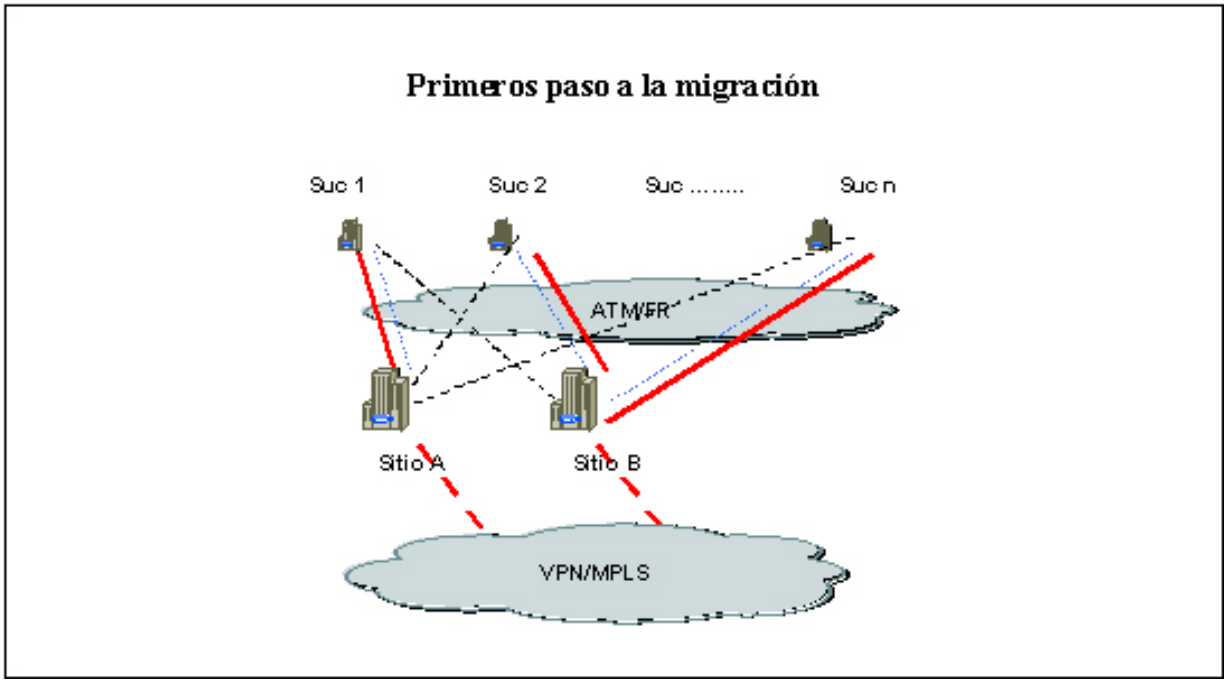


Figura 39 – Primeros pasos de la migración

Selección de una sucursal para la migración

Se selección en conjunto con el cliente la sucursal con menor trafico y la de menor impacto sobre el negocio. Además se acordó antes de la migración conectar una sucursal “piloto”, sucursal de prueba sobre la red VPN/MPLS que permitiría al cliente realizar todas las pruebas de interoperabilidad con sus sistemas de negocio y al grupo de operación del Carrier tomar experiencia en el vuelco de las futuras sucursales.

Luego se acordó la forma de separar los diferente tipo de tráficos (voz y datos), asignando los mecanismos de Calidad de Servicio QoS de la siguiente forma:

- El tráfico de datos se marcaría en la salida del router CPE, como trafico de baja prioridad (Best Effort). Este trafico entonces tiene como limite utilizar todo el enlace mientras este disponible y en caso de detectar tráfico de mayor prioridad comenzar a descartar paquetes hasta lograr acomodarse al ancho de banda disponible.

- El tráfico de voz se marcaría en la salida del router CPE, como trafico de alta prioridad (High Priority). A este tipo de trafico se le asigna un ancho de banda de 25Kbps (dependerá de las llamadas simultaneas que pretendan realizar) y tendrá una prioridad por encima de todas las demás.
- Se realiza una tercera selección del tráfico para los datos que el cliente necesite asignar mayor prioridad (Mision Critical). A este tráfico se le asignarían el 10% del total del ancho de banda total. Dentro de este tipo de trafico pueden estar aplicativos de negocio, vídeo, etc, (identificando puertos udp o tcp, direcciones ip origen y/o destino).
  En la siguiente figura se representa la conexión de la sucursal piloto.

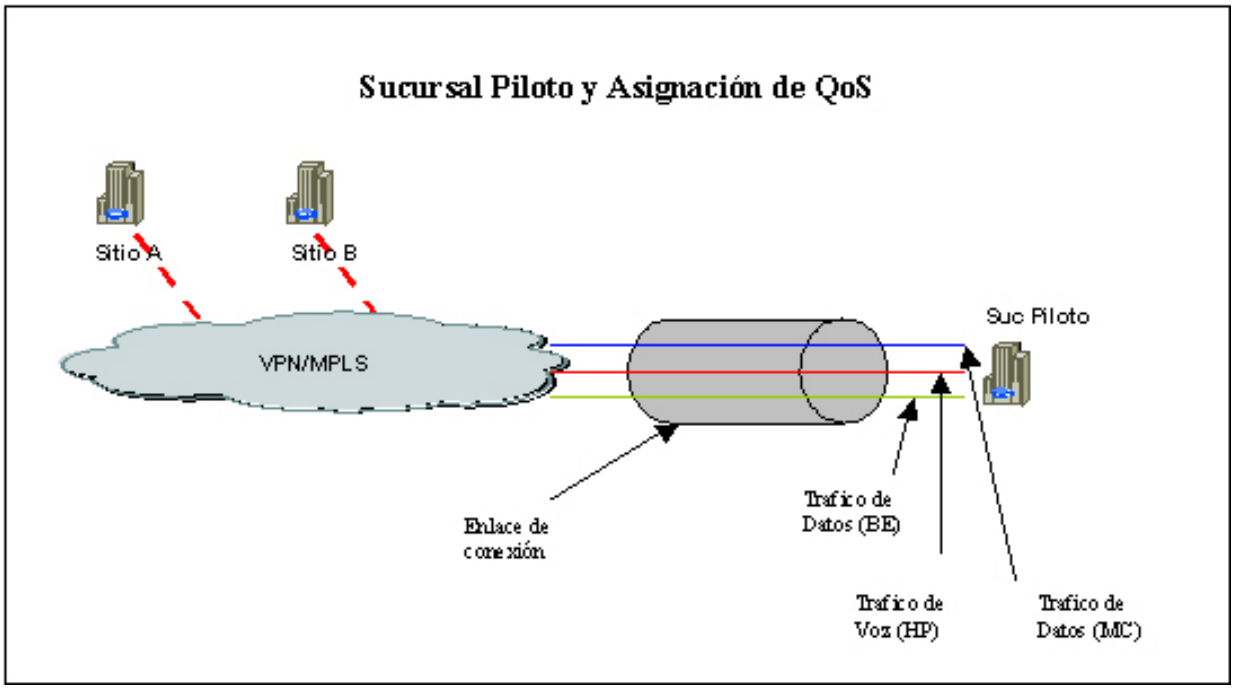


Figura 40 – Sucursal piloto

Pruebas de performance y seguridad sobre la sucursal piloto

Se acordó un conjunto de pruebas con el fin de testear la performance y seguridad de la sucursal piloto en relación a las sucursales tradicionales. Estas pruebas tienen como fin principal no solo medir los requerimientos pedidos por el cliente, sino también demostrar que esta nueva tecnología posee las mismas prestaciones. El conjunto de pruebas estuvo compuesto por:

Pruebas de troughput

Sobre un vínculo de 512Kbps esta prueba medio el throughput con ráfagas de tráfico generados por aplicativos de negocios – actualización de bases de datos, transferencias de archivos – que permitieron generar un tráfico superior a los 512Kbps. Luego se realizó la medición del vínculo en donde se constato la velocidad de acceso.

Pruebas de delay (latencia)

Sobre el mismo enlace se establecieron los mismos requerimientos de delay utilizados para las sucursales de ATM/FR contra los sitios principales:

- Promedio Delay sin Trafico <= 10ms
- Promedio Delay con Trafico <= 40ms

Debido a que la sucursal piloto posee un menor encapsulamiento que sobre ATM/FR, los delay medidos sobre la nueva tecnología lograron acordar un nuevo acuerdo de servicio sobre estas nueva tecnología:

- Promedio Delay sin Trafico <= 7ms
- Promedio Delay con Trafico <= 30ms

Pruebas de packet loss (perdida de paquetes)

Sobre el mismo enlace se establecieron los mismos requerimientos de packet loss utilizados para las sucursales de ATM/FR contra los sitios principales (Packet Loss <= 1). En las mediciones realizadas

sobre la nueva tecnología nunca se detecto un paquete perdido, pero por posibles problemas de red el acuerdo de servicio se estableció en le mismo valor.

Pruebas de calidad de servicio

Si bien para las pruebas de calidad de servicio no pudieron ser utilizados los mismos parámetros de medición, debido a que la tecnología actual dedica un enlace (PVC) por servicio de voz y video; se tomo como medida sobre el enlace de 512Kbps realizar las siguientes pruebas:

- Prueba de datos (Best Effort): Se realizó la prueba generando tráfico desde la sucursal a los sitios principales llenando en su totalidad el vínculo de 512Kbps. El tráfico generado era tráfico marcado como best effort por lo tanto ingresaba sobre la cola de baja prioridad, utilizando toda la capacidad del enlace debido a que no había tráfico de mayor prioridad.
- Prueba de voz (High Priority): Con el tráfico generado en la prueba anterior y sin ancho de banda disponible se genero una llamada telefónica entre la sucursal y el sitio principal A. Luego se midió el tráfico para constatar que el tráfico de voz ingreso por la cola de alta prioridad ocupando 25Kbps y la cola best effort comenzó a descartar paquetes por exceso de tráfico. Además el cliente probó en varias oportunidades la percepción al oído de las llamadas realizadas para constatar la calidad de la voz (microcortes, eco y retardos).
- Prueba de datos críticos (Mision Critical): Al mismo tiempo que el tráfico de datos de baja prioridad y la llamada de voz estaban en curso, se genero un tráfico de datos de alta criticidad para el negocio (actualizaciones de base de datos). Nuevamente se constato que al ingresar el trafico de datos a la cola de mision critical desplazó al trafico best effort detectando mayor cantidad de descarte de paquetes en este ultimo y sin variar la calidad de la voz.

Una vez establecidos los tres tipos de tráfico se midió el tráfico promedio ingresado a cada cola:

- Cola Best Effort → 435.8Kbps
- Cola Mision Critical → 51.2Kbps
- Cola High Priority → 25Kbps

Pruebas de seguridad

Las pruebas de seguridad tenían como base establecer si la sucursal piloto cumplía con los requerimientos de seguridad establecido para las sucursales ATM/FR. Se establecieron entonces las siguientes pruebas:

- Aislamiento del tráfico: La prueba constó en verificar si desde distintas sucursales de otros clientes era posible visualizar o acceder a la tabla de ruteo del cliente bajo prueba. Debido a que todos los clientes tienen sus sucursales en diferentes VPNs, cada tabla de rutas quedan aisladas bajo el dominio de cada VPN, por ende no fue posible acceder a las rutas del cliente bajo prueba desde un sitio no deseado.
- Solapamiento de direcciones IP: Se incorporo una sucursal de otro cliente, en diferente VPN, con el mismo rango de direccionamiento IP que la sucursal piloto. Se verificó que desde una sucursal con el mismo direccionamiento que el cliente bajo prueba no pudo establecerse conectividad IP con los sitios principales, nuevamente debido a permanecer a diferentes VPNs.
- Denegación de servicio de una sucursal (DoS): Se verificó la imposibilidad de atacar una sucursal piloto desde Internet y desde la sucursal de otro cliente. En primera instancia desde Internet no fue posible debido a que los rangos de direccionamiento utilizados para los clientes en VPNs no son publicados desde el Carrier hacia otros dominios de Internet por lo que fue imposible acceder. En segunda instancia desde una sucursal de otro cliente nuevamente por no poder acceder a la tabla de ruteo de otra VPN no fue posible el ataque.
- Denegación de servicio de un router PE: Recordemos que las sucursales están directamente conectadas a routers del Carrier (PE), los cuales además de interconectar las diferentes VPNs brindan servicios de Internet lo que los hace mas vulnerables que una sucursal. Se verifico entonces la imposibilidad de atacar un router PE desde Internet o desde una sucursal, pero en este caso si era posible tener conectividad desde Internet al router PE, por lo que en entro en juego las reglas de firewall – reglas activadas por comando que permiten denegar el tráfico no deseado o habilitar el trafico deseado - activadas en el router PE para denegar ataques de DoS.

Migración de las sucursales

Se acordó un cronograma de migración por sucursal, realizando para todas ellas un subconjunto de pruebas reducido del anterior para constatar la aprobación del cliente de la migración. Hasta el momento el cliente lleva migrado el 30% de sus sucursales.

Problemas y oportunidades

Durante la migración de las sucursales se presento un único problema técnico al cursar voz sobre un enlace satelital. El problema se debió a que los enlaces satelitales poseen un delay natural mayor a los enlaces terrestres y que el interleave (paquetes de voz intercalados entre una x cantidad de paquetes de datos) tenia una valor no optimizado para este tipo de enlaces. Corregido este problema el cliente siguió adelante con la migración.

La migración a voz sobre IP le permitió a la empresa unificar su plataforma de voz, utilizada para llamadas dentro de la empresa, con una plataforma para realizar llamadas nacionales y al exterior sobre voz sobre IP.

Capitulo V – Demostración

Objetivo

La demostración tiene como objeto simular una red privada virtual (VPN/MPLS) para un cliente, dicha red esta preparada para soportar trafico de datos, voz y video.

Alcance

Durante la demostración se simularan dos sucursales de cliente, las cuales podrán transmitir datos, voz y video con diferentes calidades de servicio, permitiendo simular patrones de tráfico de las redes reales y el comportamiento de una VPN/MPLS al momento de congestión de los enlaces.

Entre las pruebas a realizar durante la demostración se destacan:

- Armado de una red VPN/MPLS para un cliente.
- Diseño de tres colas para Calidad de Servicio (datos, voz y video).
- Transmisión de datos y video; realización de llamadas utilizando VoIP.
- Medición de Calidad de servicio.
- Pruebas de seguridad de la VPN.

Esquema de la DEMO

La demostración se realizará utilizando el siguiente esquema y equipamiento. Este esquema permitirá simular una red MPLS y una VPN asociada a un cliente.

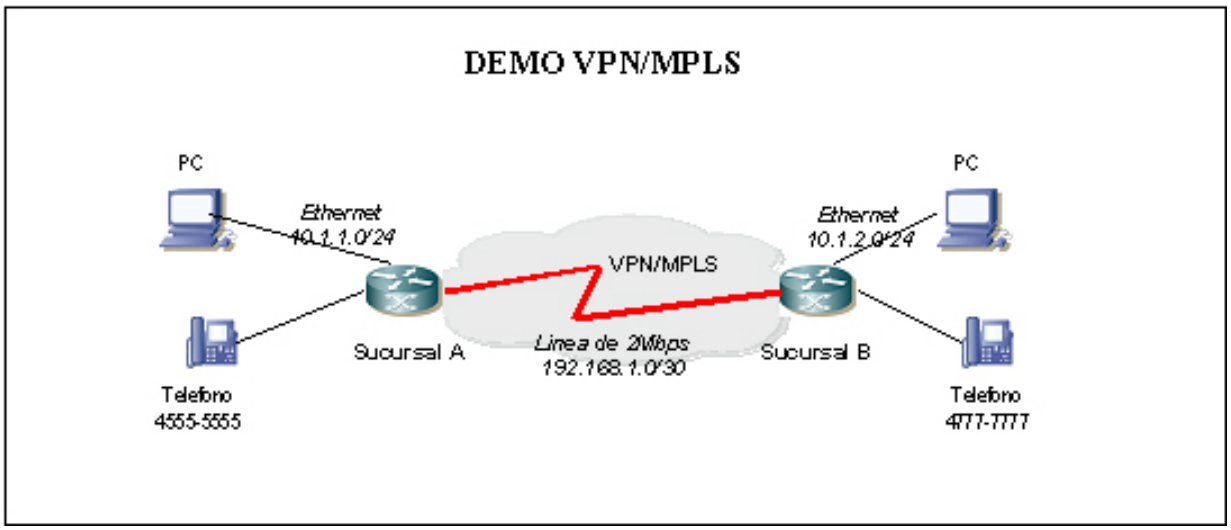


Figura 41 – Demo

Condiciones de Pruebas

Las pruebas se realizaran sobre las siguientes condiciones:

- Cada sucursal pertenecerá a una VPN/MPLS. En este caso se creo una VPN llamada DEMO en ambas sucursales.
- Sobre ambas sucursales se configuraron tres colas para calidad de servicio y en la entrada de cada sucursal (interfase Ethernet e interfase telefónica) se marca el trafico para diferenciarlo dentro de estas tres colas, siguiente el siguiente parámetro:

- Trafico de voz: Se marcó sobre la interfase de teléfono que el tráfico proveniente de esta interfase sea marcado como “alta prioridad”. Al mismo tiempo se asigna una cola de alta prioridad a la que se asoció un ancho de banda de 25Kbps.
- Trafico de video: Se marcó sobre la interfase ethernet que todo el tráfico de video (en este caso el tráfico de video se identifica como trafico UDP con destino al puerto 1234) sea marcado como tráfico “prioridad media”. Al mismo tiempo es asociado a una cola de prioridad media que tiene asignado un ancho de banda de 1.5Mbps.
- Trafico de datos: Se marcó el resto del tráfico que ingresa por la interfase ethernet como “baja prioridad”. En este caso el tráfico se asocia a una cola de baja prioridad la cual tiene asignado el resto del ancho de banda sobrante 463Kbps.

- Cada sucursal contiene un teléfono convencional y las sucursales están preparadas para recibir o generar llamadas.

Pruebas de DEMO

Pruebas de VoIP:

1. Desde la sucursal A se generará una llamada mediante el protocolo VoIP a la sucursal B. Se verificará la calidad de voz y el ancho de banda utilizado.
2. Con el teléfono de la sucursal B descolgado se verificará la presencia del tono ocupado cuando la sucursal A intente realizar una llamada.

Pruebas de Calidad de Servicio:

1. Generación de tráfico de datos utilizando todo el ancho de banda disponible más halla del configurado en la cola de baja prioridad. Se verificará el ancho de banda utilizado.
2. Generación de tráfico de video. Este tráfico utilizará un promedio de 1.5Mbps por lo que el tráfico de datos de menor prioridad deberá utilizar como máximo 512Kbps.
3. Generación de una llamada telefónica. La llamada de voz posee mayor prioridad por lo que el tráfico de datos quedará restringido a 463Kbps.

Pruebas de seguridad:

1. Se creará una nueva VPN llamada ESPIA, con el mismo direccionamiento que la sucursal B. Se verificará la imposibilidad de acceder a la sucursal A.
2. Se verificará la tabla de rutas separada para cada VPN.
3. Se verificará la imposibilidad de generar desde la VPN ESPIA un ataque Denial of Service a la VPN DEMO.

Resumen

A lo largo del documento, se puede comprender porque surge la necesidad de redes privadas virtuales generadas desde un nuevo concepto, debido a la necesidad de nuevos servicios y optimización de utilización de recursos de redes. Si bien existen diferentes alternativas para brindar una red privada virtual, elegí las redes VPNs basadas en MPLS con el objetivo de aportar mis conocimientos, de tal forma que desde el punto de vista del Carrier y los clientes puedan entenderse las ventajas y desventajas de una evolución hacia esta nueva tecnología.

En principio MPLS supliendo los problemas de las redes IP nativas, en cuanto a la mejora de velocidad de fowardeo de paquetes e implementando una nueva filosofía de conmutación de etiquetas comenzó a ser utilizada por los grandes Carriers para sus servicios de Internet. Al mimo tiempo enriqueció la oportunidad de implementar sobre la misma red de servicios de Internet, redes privadas virtuales VPN haciendo posible la integración de servicios corporativos sobre una misma infraestructura de red.

Sumándole a lo anterior la obsolescencia en las redes tradiciones de datos y voz, la tecnología MPLS puede hacerse cargo de la integración de servicios de telefonía y datos, posibilitada por las funcionalidad de calidad de servicios que puede implementarse tanto en los equipos de clientes como en el core de la red principal.

Con todas estas funcionalidades las redes privadas virtuales basadas en MPLS, pueden brindar transporte de diferentes tipos de servicios con diferentes SLA, desplegar una red full-meshed sin la necesidad de circuitos virtuales entre todos los sitios, permitiendo una implementación menos costosa y más eficiente que cualquier otra tecnología conocida hasta el momento.

La migración ha comenzado y es el primer desafió que los Caries deben enfrentar, ya que la atracción de nuevos clientes es inmediata por los beneficios que esta tecnología presenta. El miedo al cambio de

los clientes de redes tradicionales deberá contraponerse contra la evolución. Con el tiempo estos clientes necesitaran flexibilidad en sus redes, para integrarse a un nuevo modelo de negocios y solo podrá realizarse con una tecnología que permita construir intranets. Extranets, accesos remoto y bajar costos de telefonía corporativa y vínculos de red.

Anexo I – Conceptos de MPLS

IP Forwarding Vs MPLS

Escalabilidad y flexibilidad del sistema IP-based Forwarding

En pos de comprender todas las cuestiones que afectan la escalabilidad y flexibilidad de las redes tradicionales de “IP packet forwarding” debemos revisar los mecanismos básicos de “IP forwarding”y su interacción con las estructuras de red que lo soportan (redes de área local LAN o extendida WAN). Con dicha información podremos identificar sus inconvenientes y estudiar alternativas de mejora.

El paradigma de la capa de ruteo (Network Layer Routing Paradigm)

El tradicional envió de paquetes en la capa de red “network layer packet forwarding” (por ejemplo el envió de paquetes IP a través de Internet) se sustenta en la información provista por los protocolos de ruteo de la capa de red (Capa 3, OSPF: Open Shorter Path First; BGP: Border Gateway Protocol), o en ruteos estáticos para analizar una decisión de envió independiente en cada salto o “hop” (router) dentro de la red. La decisión de enviar o “forwarding decisión” esta basado solamente en la dirección de IP destino unicast. Todos los paquetes con el mismo destino siguen un mismo camino a través de la red si no es que existe otro camino de igual costo para el mismo destino. En caso de que el router tenga dos caminos de igual costo hacia un mismo destino, los paquetes podrán tomar uno o ambos, resultando este ultimo caso en algún tipo de balanceo de carga o “load sharing”.

Los routers realizan el proceso de decisión que selecciona que senda o camino tomara un paquete. Estos dispositivos de red participan en la colección y distribución de información de capa de red, y posteriormente realizan conmutación de capa 3 (capa de red) basado en los contenidos del encabezado de red de cada paquete. Los routers pueden conectarse directamente por enlaces punto-a-punto o por medio de redes de área local LAN (hub, MAU, switch, etc.), o pueden conectarse entre si a través de de switches de WAN (ATM o Frame-Relay).

Estos switches de capa de enlace (Capa 2: Lan o Wan) desafortunadamente no poseen capacidad de albergar información de ruteo de Capa 3 del paquete, por ello, los switches de capa de enlace (LAN o WAN) no pueden verse envueltos en el proceso de decisión de envió de la capa de red.

Los enlaces en los dispositivos de LAN son simples de establecer – todos los switches de LAN actúan de forma transparente a los dispositivos conectados a ellos.

El establecimiento de los caminos en el ambiente WAN (capa de enlace) resulta mas complejo; el diseñador de la red debe establecer manualmente dos caminos de capa de enlace a través de la WAN, y serán estos caminos quienes a su vez transporten los paquetes de capa de red entre los routers que se encuentran conectados físicamente a esta red de capa 2 (WAN).

Los caminos WAN usualmente se encuentran basados en parámetros punto-a-punto (por ejemplo circuitos virtuales “virtual circuits” en la mayoría de las redes WAN) y son establecidos en base a una solicitud de configuración manual. Cualquier dispositivo de entrada (router de ingreso) en la periferia de la WAN (capa 2) que desee enviar paquetes de capa 3 a algún otro dispositivo de ruteo (router de salida) necesitará por lo tanto establecer una conexión directa a través de la red WAN con el dispositivo de salida o deberá enviar sus datos a un dispositivo diferente para transmisión hacia el destino final.

Consideremos el ejemplo mostrado en la Figura 29.

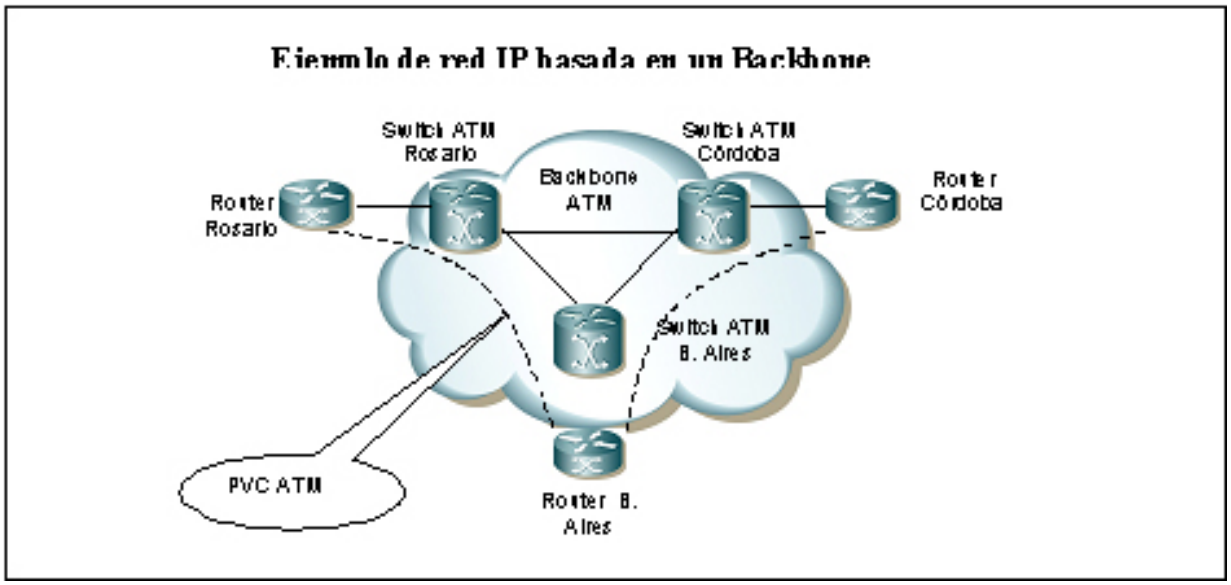


Figura 42 – Topología IP basada en ATM

La red ilustrada en la figura 29 esta basado en un “backbone” o “core” ATM rodeado de routers que realizan “network layer forwarding” (envió de paquetes de capa 3). Asumiendo que las únicas conexiones entre los routers son las mostradas en el esquema, todos los paquetes enviados desde Rosario hacia Córdoba deberán ser enviados al router de Buenos Aires, donde serán analizados y enviados nuevamente por la misma conexión de acceso ATM en B. Aires hacia el router de Córdoba. A pesar de parecer una solución trivial para redes pequeñas (pocos routers), se presenta un problema de escalabilidad en redes con varias decenas o centenas de routers conectados a la misma WAN.

Los siguientes ítems detallan los problemas de escalabilidad que pueden encontrarse:

- Cada vez que un nuevo router sea conectado al backbone de la red WAN deberá establecerse un circuito virtual entre este router y cualquier otro router dentro de la red, en caso de requerirse optimo ruteo (ej: se requieren N-1 circuito virtual en cada router para realizar una red mellada total “full-meshed” con rute y redundancia óptimos, con lo cual consumirá N*(N-1) circuitos de la red).
- En determinadas configuraciones de protocolos de ruteo, cada router conectado a la red WAN (construido con switches ATM o Frame-Relay) necesitara un circuito virtual dedicado a cada router conectado a la misma WAN. Para alcanzar la deseada redundancia de red, cada router además deberá establecer una adyacencia en el protocolo de ruteo con cada router conectado a la misma red. La resultante red mellada de routers con adyacencia provocará en cada uno de ellos un gran número de vecinos de ruteo, generando grandes cantidades de tráfico con información de ruteo. Por ejemplo, si la red emplea OSPF como protocolo de ruteo, cada router propagará cada cambio topológico en la red a los demás routers vecinos generando un tráfico de ruteo proporcional al cuadrado del número de routers involucrados.
- La provisión de los circuitos de virtuales entre los routers resulta compleja, ya que es difícil predecir a priori la cantidad exacta de tráfico entre dos routers específicos de la red. Para simplificar la tarea de provisión de algunos proveedores de servicio simplemente optan por la falta de garantía de servicio en la red – cero Tasa de Información Comprometida “Commited Information Rate” (CIR) en Frame-Relay, o en conexiones ATM de Tasa de Bits no especificada “Unspecified Bit Rate” (UBR).

La falta de intercambio de información entre los routers y los switches de WAN no fue un inconveniente para los tradicionales Proveedores de Servicios de Internet (ISP) que empleaban backbones con solo routers, o para los Proveedores de Servicios de Transporte WAN (Carriers) de circuitos virtuales de ATM o Frame-Relay. Sin embargo, existen algunos aspectos que llevan a juntar ambos grupos para el diseño de backbones mixtos:

- Los tradicionales Proveedores de Servicios son promovidos por sus clientes para ofrecer servicios IP. Desean replantear sus inversiones y basar estos nuevos servicios sobre su infraestructura WAN existente.
- Los Proveedores de Servicios de Internet son promovidos por sus clientes para ofrecer calidad de servicio (QoS) garantizada, fácil de alcanzar mediante switches ATM.
- El rápido incremento en los requerimientos de ancho de banda anterior a la introducción de interfaces ópticas en los routers, forzaba a los grandes proveedores de servicios a comenzar a basarse en

tecnología ATM ya que las interfaces de los routers en aquel entonces no eran capaces de proveer la velocidad ofrecida por los switches ATM.

Queda claro entonces, que un mecanismo distinto debe ser empleado para el intercambio de información de red en routers y switches de WAN, y deberán permitir a los switches participar en el proceso de decisión de envió de paquetes "forwarding packets" para de esta manera no resulten necesarias las conexiones directas entre routers de borde.

Servicios de paquete diferenciado

En el proceso tradicional de envió de paquetes IP solo se emplea la dirección IP destino contenida en el encabezado de capa 3 dentro del paquete para luego tomar la decisión del envió (forward). El paradigma del hop-by-hop destination-only (solo destino en cada salto) empleado actualmente limita la cantidad de métodos innovadores del diseño de red y la optimización del flujo de trafico. En la figura 30, por ejemplo, el enlace directo (8 Mbps) entre el router de core de Rosario y el router de core de Córdoba rutea el trafico entre la zona de litoral y zona centro, sin embargo dicho enlace puede encontrarse congestionado, mientras que los enlaces entre Rosario y B. Aires, Córdoba y B. Aires podrían estar poco utilizados.

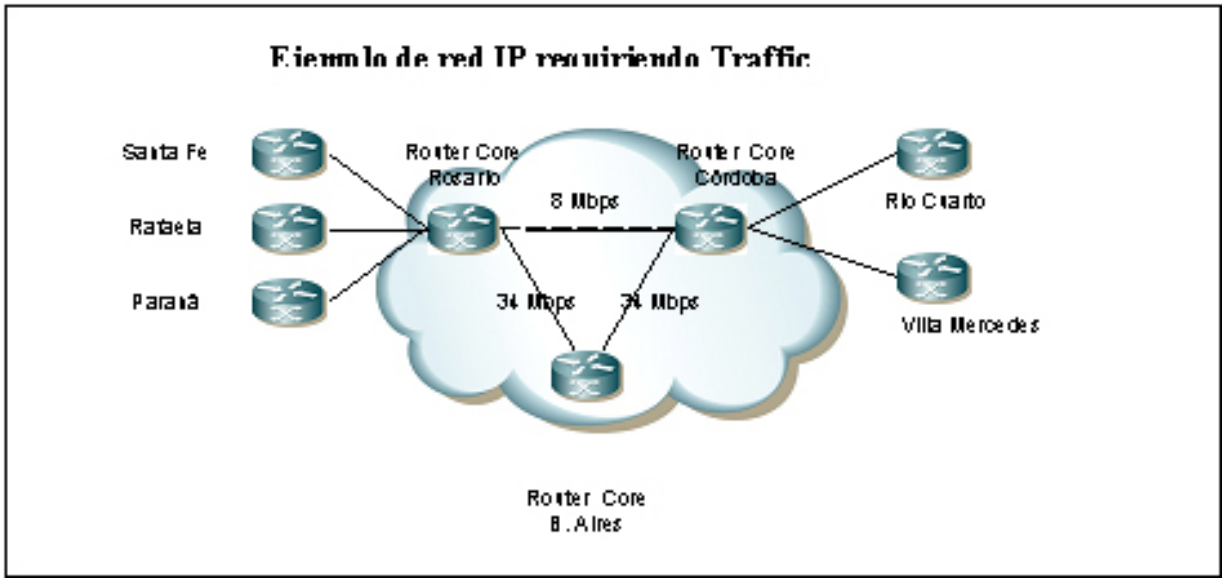


Figura 43 – Ingeniería de trafico

A partir de que existen ciertas técnicas que afectan el proceso de decisión, tales como Políticas Basada en Rute o Policy Based Routing (PBR), ninguna técnica escalable existente puede decidir el camino completo que un paquete debe tomar al atravesar una red hacia su destino final. En la red detallada en la figura 30, el policy based routing deberá desarrollarse en el router de core de Rosario para dirigir parte del trafico hacia Córdoba a través de Buenos Aires. Desarrollar estas características en los routers de core puede reducir severamente la performance de los mismos resultando además en un diseño sin escalabilidad (al crecer en cantidad de routers y enlaces de core resultará inmanejable su operación). Idealmente, los routers de borde (ejemplo Paraná) deberían especificar sobre que enlace el paquete debe transitar.

Gran parte de los proveedores de servicios desarrollan sus redes con caminos redundantes, con lo cual aflora un claro requerimiento para permitir que los dispositivos de ingreso sean capaces de decidir en el proceso de forwarding (envió), que afecta a su vez el camino del paquete a través de la red, y al mismo tiempo deberán aplicar una marca al mismo que indique a los demás dispositivos cual es el camino que el paquete debe tomar.

Paralelamente, este requerimiento debe además permitir que el flujo de paquetes que son destinados hacia una misma red IP, tomar caminos distintos en lugar de los determinados por los protocolos de ruteo (capa 3). Consecuentemente, la decisión deberá en otros factores distintos al destino IP del paquete, tales como desde cual puerto el paquete fue conocido, cual debe ser el nivel de calidad de servicio que el paquete requiere, etc.

Control y envió independientes

En el convencional proceso de IP packet forwarding cualquier cambio en la información que controla el envió de paquetes es comunicado a todos los dispositivos dentro del dominio de ruteo. Dicho cambio siempre requiere un periodo de convergencia dentro del algoritmo de forwarding (envió).

Por lo tanto, es deseable un mecanismo capaz de modificar como un paquetes es enviado sin afectar a los demás dispositivos dentro de la red. Para implementar tal mecanismo, los routers (forwarding devices) para enviar un paquete no deberán sustentarse sobre la información del encabezado IP del mismo; por lo tanto una etiqueta o marca adicional deberá agregarse al paquete enviado para indicar el comportamiento de envió esperado. Con un proceso de forwarding de paquetes desarrollado en base a etiquetas adosadas a los paquetes IP originales, cualquier cambio en el proceso de decisión puede ser comunicado a otros dispositivos a través de la distribución de nuevas etiquetas. Debido a que estos dispositivos solamente envían trafico basado en etiquetas adosadas, cualquier cambio podrá ocurrir sin impactar de ninguna manera en otro dispositivo que se encuentre realizando envió de paquetes (packet forwarding).

Propagación de la información de ruteo externa

El convencional proceso de IP packet forwarding dentro del core de una red IP requiere que la información de ruteo externa sea comunicada a todos los dispositivos de transito. Esto resulta necesario a modo que los paquetes puedan ser ruteados en base a la dirección destino contenida en el encabezado de la capa de red del paquete mismo. Volviendo al esquema de la Figura 30, y suponiendo que los routers de core deberían almacenar todas las rutas de Internet (actualmente comprenden aproximadamente 100.000 rutas o prefijos BGP) a modo de poder propagar un paquete originado en algún punto de la red interna y cuyo destino se encuentre en algún lugar de Internet. Este método tiene implicancia de escalabilidad (dificultad de expansión o crecimiento) en términos de propagación de rutas, utilización de memoria y CPU en los routers de core, y no resultan funcionalidades requeridas si lo deseado solamente en enviar trafico de un router de borde hacia otro router. Resulta entonces, como obvio requerimiento un mecanismo que permita a los routers internos conmutar los paquetes de un router de ingreso hacia un router de egreso a través de la red sin necesidad de analizar en cada salto la dirección de capa de red destino.

Introducción a Multiprotocol Label Switching

MPLS es un método mejorado para el envió de paquetes o forwarding packets a través de una red empleando información contenida en las etiquetas adosadas a los paquetes IP. Dichas etiquetas son insertadas entre los encabezados de capa 3 (red) y los encabezados de capa 2 (enlace) en el caso de la tecnologías de capa de enlace basadas en tramas o frames (Frame-Relay, HDLC, etc), y son contenidas dentro de los campos del virtual path identifier (VPI) y virtual channel Identifier (VCI) en el caso de las tecnologías basadas en celdas como lo es ATM.

MPLS combina tecnologías de switching de capa de enlace con tecnologías de ruteo de capa de red. El objetivo primario de MPLS es crear una malla de red flexible capaz de proveer performance y escalabilidad incrementales. Este hecho incluye proveer capacidades de Traffic Engineering y VPNs (Redes Privadas Virtuales), que simultáneamente ofrezcan Calidad de Servicio (QoS) mediante múltiples Clases de Servicio (CoS).

Nota importante: El termino Multiprotocolo indica que la técnica MPLS es aplicable a cualquier protocolo de capa de red. De todas maneras, pondremos foco en este documento sobre el empleo del protocolo de capa de red IPv4 (Internet Protocol versión 4).

En el ejemplo de red MPLS detallado en la Figura 31, a los paquetes entrantes se le asigna una etiqueta en el Edge Label-Switched Router (Edge LSR: router de borde conmutador de etiquetas). Los paquetes son enviados a lo largo de un LSP o camino conmutado de etiquetas (Label Switched Path), donde cada Label-Switched Router (LSR) realiza una decisión de envió (forwarding decisión) basada solamente en el contenido de la etiqueta. En cada salto (hop), el LSR remueve la etiqueta existente y aplica una nueva etiqueta, la cual indicará al próximo salto (hop) de que manera deberá pasar este paquete. Finalmente, en el Edge LSR de salida la etiqueta es removida y el paquete enviado a su destino.

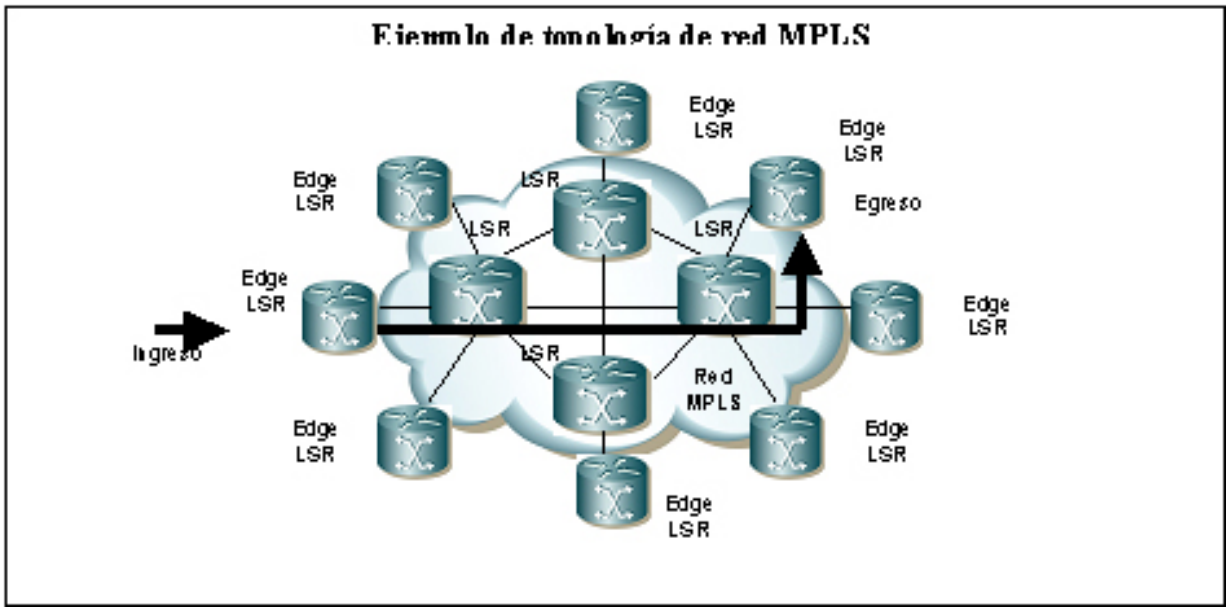


Figura 44 – Tipo de equipos en MPLS

MPLS es además un programa de desarrollo del Internet Engineering Task Force (IETF), quien ha desarrollado documentos descriptivos y al mismo tiempo estándares sobre los diferentes aspectos de la tecnología MPLS a emplearse sobre redes de proveedores de servicios.

La evolución del Multiprotocol Label Switching

La propuesta inicial de la técnica de conmutación basada en etiqueta (label-based switching) consistió en proporcionar velocidades de conmutación de capa 2 a la capa 3. Esta justificación inicial para las tecnologías como MPLS dejo de ser percibida como un beneficio, ya que los nuevos switches de capa 3 mediante aplicaciones especificas en los circuitos integrados (ASIC: application-specific integrated circuit) lograban búsquedas de rutasen tablas a suficiente velocidad como para soportar casi todos los tipos de interfaces disponibles.

En cierta forma, el interés general en MPLS para ampliar se desarrollo motivo de la formación del grupo de trabajo IETF MPLS en el año 1997. MPLS ha evolucionado desde numerosas tecnologías pioneras incluyendo versiones propietarias de implementaciones de conmutación de etiquetas (label switching) tales como Tag Switching de Cisco, Agrégate Route-Based IP Switching (ARIS) de IBM, Cell-Switched Router de Toshiba, IP Switching de IPSILON, y el IP Navigator de Lucent Technologies.

Los beneficios de MPLS

Los métodos de conmutación basados en etiquetas le permiten a los routers y a los switches de ATM con soporte para MPLS realizar decisiones de envió (forwarding decisions) basándose sobre los contenidos de una simple etiqueta, en lugar de realizar una búsqueda compleja de una ruta dentro de una tabla con las posibles direcciones IP de destino. Estas técnicas aportan grandes beneficios a las redes basadas en el protocolo IP:

- VPNs: Empleando MPLS, los proveedores de servicios pueden crear VPNs (redes privadas virtuales) de capa de red (capa 3) para múltiples clientes, dentro de su red de backbone empleando una infraestructura común, sin la necesidad de encripción.
- Traffic Engineering: Brinda la posibilidad de establecer en forma explicita un conjunto de posibles múltiples caminos que el tráfico podrá tomar al transitar a través de la red. Al mismo tiempo, provee un conjunto de facilidades con performance para clases de tráfico. Esta característica optimiza el empleo de caminos subutilizados.
- Quality of Service: Utilizando la calidad de servicio (QoS) de MPLS, los proveedores de servicios podrán proveer múltiples clases de servicio con buena garantía de QoS a sus clientes de VPNs.
- Integración de IP y ATM: La mayoría de las redes de Carriers emplean un modelo de cobertura en el cual ATM es utilizado en la capa de enlace (capa 2) e IP es empleado en la capa de red (capa 3). Tales implementaciones presentan dificultades de escalabilidad. Al emplear MPLS, los Carriers pueden migrar muchas de las funcionalidades del plano de control de ATM a la capa de red, consecuentemente simplificando la provisión de la red, el manejo, y la complejidad de la misma. Esta técnica provee in-

mensa escalabilidad y elimina la penalidad de ATM (cell tax) debido al encapsulamiento al transportar trafico IP.

MPLS combina la performance y capacidades de conmutación de nivel 2 (capa de enlace) con la probada escalabilidad de ruteo de nivel 3 (capa de red). Esto permite a los proveedores de servicios alcanzar los retos del crecimiento explosivo en la utilización de la red al mismo tiempo de proveer servicios diferenciados sin sacrificar la actual infraestructura de red. La arquitectura MPLS es flexible y puede ser desarrollada en combinación con tecnologías de capa de enlace.

Al incorporar MPLS los proveedores de servicios dentro de su arquitectura de red ya establecida obtienen como rédito la redundancia de costos, el incremento en la ganancia y en la productividad, la provisión de servicios diferenciados, y al mismo tiempo ganan una ventaja competitiva frente a otros proveedores que no poseen servicios de MPLS tales como VPNs IP o Ingeniería de Trafico (traffic engineering).

MPLS y la arquitectura de Internet

Desde los comienzos de ARPANET hasta la actualidad, la arquitectura de Internet ha cambiado constantemente. Ha evolucionado en respuesta a los avances en tecnología, en crecimiento y ofrecimiento de nuevos servicios. El cambio mas reciente en la arquitectura de Internet es la incorporación de MPLS. Cabe destacar que el mecanismo de envió de paquetes en Internet, el cual se basa en ruteo por destino, no ha cambiado desde los días de ARPANET.

MPLS ha impactado en el mecanismo de envió de paquetes IP y la determinación del camino (el camino que los paquetes deben tomar mientras transitan Internet). Esto ha resultado en una re-arquitectura de Internet. El beneficio de MPLS mas inmediato con respecto a una red backbone de un proveedor de servicios es la posibilidad de brindar ingeniería de trafico (traffic engineering). La ingeniería de tráfico permite a los proveedores descargar los vínculos saturados y dirigir dicho tráfico hacia vínculos subutilizados. Esto resulta en un mayor grado de utilización de los recursos que se trasladan en eficiencia y ahorro de costos.

Las redes privadas virtuales (VPNs: virtual private network) de Internet son actualmente implementadas mediante túneles de seguridad IP (IPSec) sobre trafico de Internet (publico). Tales VPNs, a pesar de funcionar correctamente, poseen una elevada sobrecarga de encapsulado (overhead) y resultan lentas para ciertas aplicaciones. Las VPNs MPLS sobre Internet permiten a los proveedores de servicios ofrecer a sus clientes VPNs basadas en Internet con anchos de bandas y niveles de servicios comparables con ATM y Frame-Relay.

Otra desventaja de los túneles IPSec es que no presentan escalabilidad, ya que proveen conexión del tipo acuerdo vecino-vecino (peer to peer, o uno a uno).

Las VPNs MPLS pueden ser implementadas para proveer redes IP privadas con mayor performance y escalabilidad que los túneles IPSec.

Los servicios VPN IP sobre redes backbone MPLS pueden ser ofrecidos a bajo costo para los clientes en comparación de los servicios VPN (circuitos) Frame-Relay o ATM tradicionales, debido a los bajos costos de provisión, operación y mantenimiento de los servicios VPN MPLS. La ingeniería de tráfico de MPLS puede optimizar el uso del ancho de banda de los caminos subutilizados, resultando en un ahorro de costo que puede ser transferido al cliente. El QoS de MPLS proporciona al proveedor de servicios la capacidad de ofrecer múltiples clases de servicio a sus clientes, y consecuentemente dichos servicios pueden ser cobrados de acuerdo al ancho de banda empleado y a otros parámetros.

Multiprotocol Label Switching

MPLS y las tecnologías WAN

Se presentará una introducción a las tecnologías empleadas en las redes de los Carriers y los proveedores de servicios, tales como TDM, Frame-Relay y ATM. Resulta importante comprender las arquitecturas y protocolos de capa de enlaces y sus interacciones con los protocolos de capa de red tales como IP, para luego comprender la tecnología MPLS.

Conmutación de Circuitos (Circuit Switching) y TDM

La tecnología TDM (time división multiplexing) combina y asigna a cada porción de ráfagas de datos una diferente ranura de tiempo (time spot) de un conjunto. TDM transmite repetidamente una secuencia fija de ranuras de tiempo sobre un único canal de transmisión. Dentro de los circuitos de los sistemas de los proveedores tales como E1/T1 o E3/T3., TDM combina ráfagas moduladas por código de pulso (PCM: pulse code modulated) para cada conversación o flujo de datos. Circuitos o líneas TDM E1/T1 o E3/T3 pueden ser usadas tanto para comunicaciones de voz como para datos.

En la Figura 32 se presenta un ejemplo de red de circuitos conmutados (circuit-switched network) desde la perspectiva de los clientes.

Esta topología también es referida como de líneas punto-apunto (point-to-point lines). Típicamente, dichas líneas son rentadas a un proveedor de comunicaciones mayorista (carrier), y se las denomina líneas privada o lease lines; en una topología tipo estrella, una línea privada es necesaria por sitio para conectarse con casa matriz.

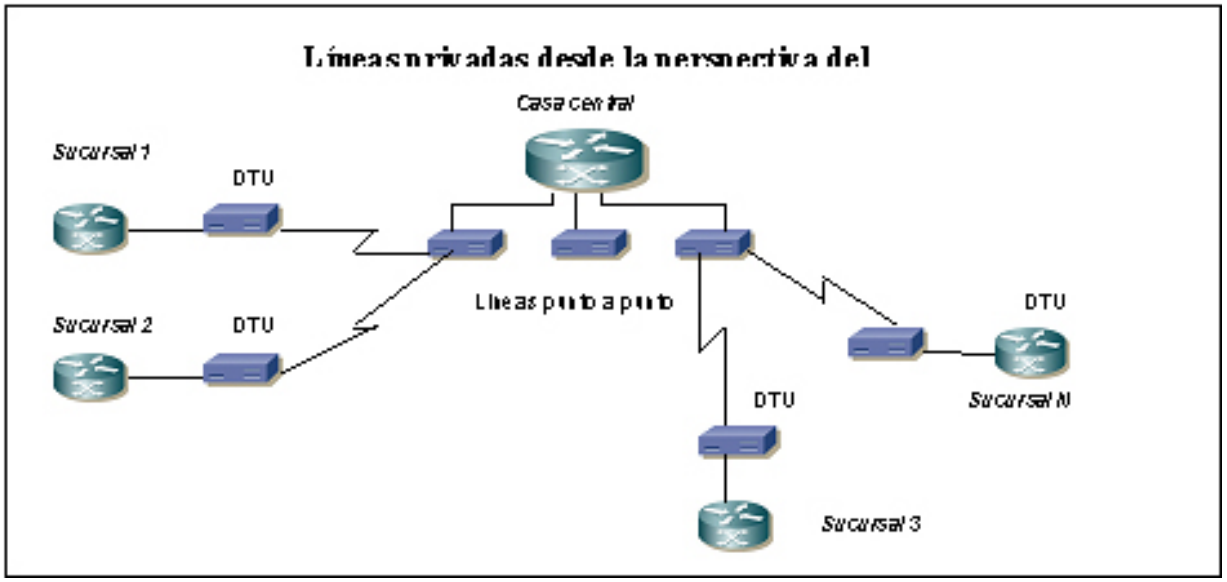


Figura 45 – Líneas privadas (Vista cliente)

La naturaleza privada de las redes de líneas punto-a-punto provee privacidad inherente y beneficios de control. Las líneas punto-a-punto son dedicadas, por lo tanto, no existen problemas estadísticos de disponibilidad como si existen en las redes publicas de conmutación de paquetes (public packet-switched networks). Esto presenta una fortaleza y una debilidad.

La fortaleza radica en que el circuito se encuentra disponible permanentemente y no requiere del establecimiento de una conexión anterior al paso del trafico, y la debilidad es que el ancho de banda siempre es abonado aunque no este siendo utilizado (típicamente entre un 30 al 60% del tiempo). En adición al uso ineficiente del ancho de banda, una desventaja mayor de las líneas punto-a-punto es debido a su naturaleza sensible con la distancia, que lo convierte en una alternativa sumamente costosa para redes que se expanden en grandes distancias, es decir, que requieran una conectividad extendida entre sitios.

Las líneas punto-a-punto también carecen de flexibilidad en términos de cambios en la red cuando se las compara con alternativas tales como Frame-Relay. Por ejemplo, agregar un nuevo sitio a una red requiere de un nuevo circuito aprovisionado extremo-a-extremo con cada sitio que el nuevo nodo deba comunicarse. Si existen ya algunos sitios, el costo puede aumentar rápidamente.

Las líneas punto-a-punto son valorizadas por los proveedores o Carriers en función de la distancia de recorrido de la misma, incurriendo los clientes en altos costos mensuales por tales circuitos dedicados.

En comparación con TDM, las redes publicas como Frame-relay, para agregar un sitio con el cual el cliente desee comunicarse simplemente requiere de una línea de acceso al nodo de red Frame-Relay mas próximo y la provisión de los circuitos virtuales (VCs: virtual circuits) necesarios. En la mayoría de los casos, los sitios existentes solo requieren de la definición de un circuito virtual extra para comunicarse con el nuevo sitio.

Desde la perspectiva del carrier, el circuito asignado al cliente (conocido también como lazo local o local loop) es aprovisionado en los DACs o banco de canal. Los circuitos individuales E1 son multiplexados en una E3 y troncalizado en un enlace terrestre, de microondas o satelital hacia el destino, donde es demultiplexado y enviado sobre las líneas E1 individuales. En la figura 33 se detalla un ejemplo de dicho esquema, donde FE1 significa E1 fraccional. Los E1 fraccionales son aprovisionados en múltiplo de 64Kbps representando fracciones del ancho de banda de la E1 o E3.

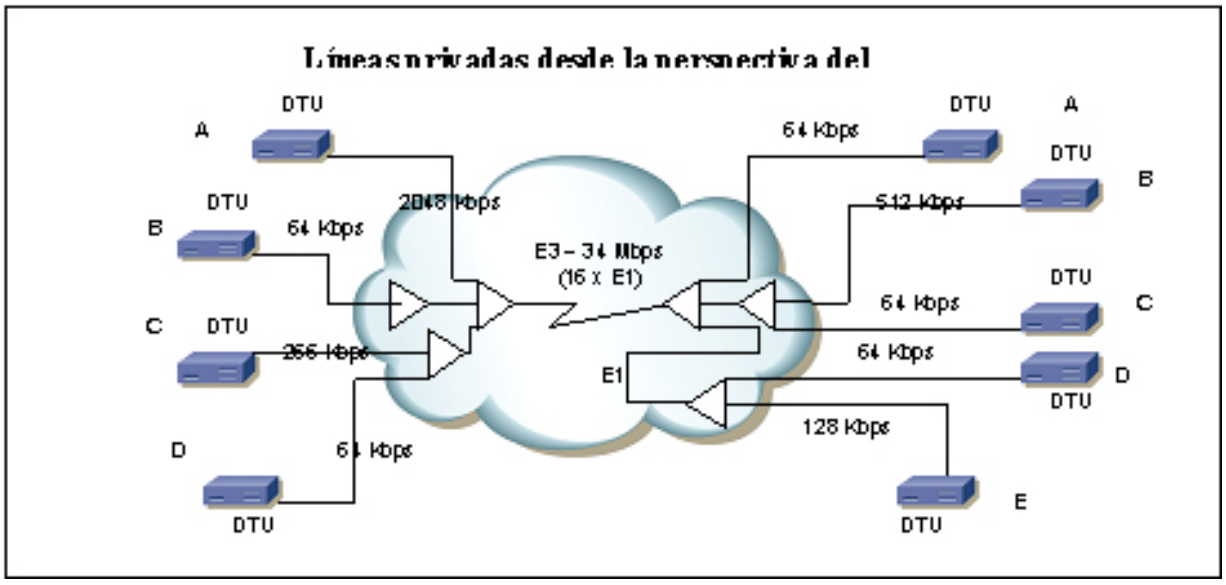


Figura 46 – Líneas privadas (vista proveedor)

Red Óptica Sincrónica (SONET)

La jerarquía SONET (Synchronous Optical Network) es la extensión óptica de la jerarquía TDM y emplea niveles de trasporte ópticos. SONET es el estándar del American Nacional Standards Institute (ANSI) para América del Norte, y SDH (synchronous Digital Hierarchy o jerarquía Digital sincrónica) para el resto del mundo.

Los sistemas SONET ofrecen manejo de red, protección, y manejo de ancho de banda. Los mismos pueden ser implementados empleando diversas topologías, incluyendo anillos, punto-a-punto, malla completa (full-meshed), y mall parcial (partial-meshed). Las redes de SONET son construidas normalmente empleando topología de anillo, La figura 34 muestra un típico esquema de topología SONET

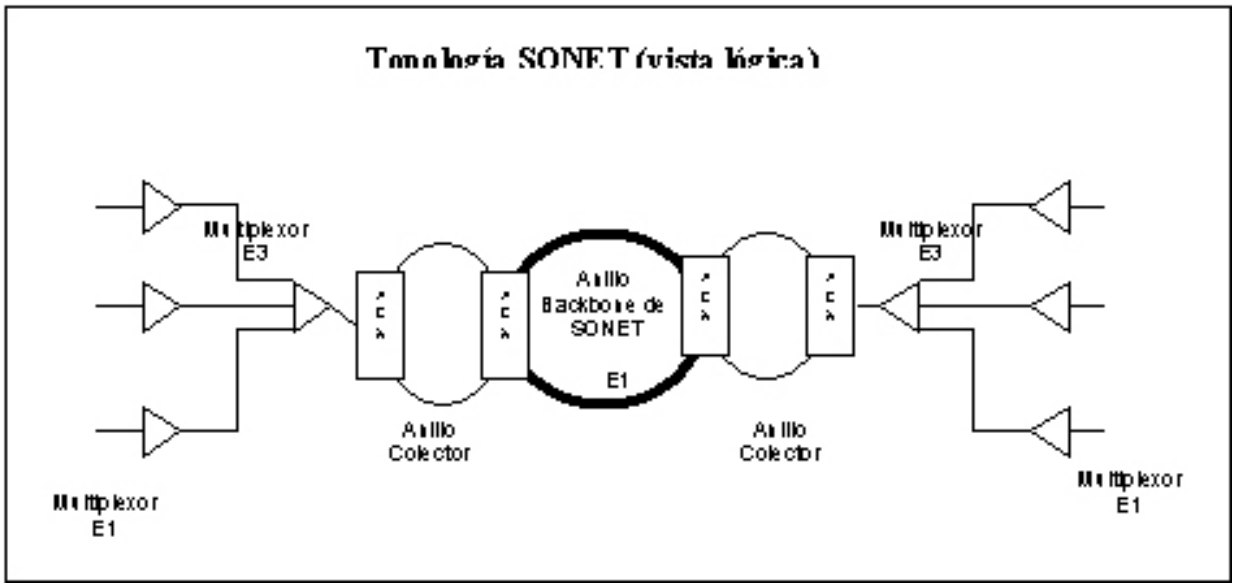


Figura 47 – Topología SONET

Conmutación de celdas y paquetes (Packet & Cell Switching)

Algunas de las tecnologías ampliamente usadas y empleadas por las redes corporativas son Frame-relay, X.25, SMDS, y ATM. Frame-Relay es una tecnología de conmutación de paquetes (packet-switched). X.25, es un protocolo mas antiguo, también emplea técnicas de conmutación de paquetes y es similar a Frame-Relay en muchos aspectos. ATM y Switched Multimegabit Data Service (SMDS) son tecnologías de conmutación de celdas (cell-switched).

Frame-Relay

Frame-Relay es un protocolo y un estándar derivado del protocolo ISDN de banda ancha y fue desarrollado por ANSI y el Internacional Telecommunication Union Telecommunication Standardization Sector (ITU-T), anteriormente el Consultative Comité for Internacional Telegraph and Telephone (CCITT).

El foro Frame-Relay (FRF) se ocupa de varios temas de implementación, asegurando que las redes puedan operar en modo multivendor (multimarca). El protocolo Frame-Relay opera solamente en la capa de enlace y no incluye ninguna función de capa de red o superior. Como resultado, el overhead del protocolo es mucho menor a comparación de la tecnología de conmutación de paquetes como X.25, la cual opera en capa 2 y 3. La reducción de overhead del protocolo es dependiente de la suposición de que la capa física se encuentra relativamente libre de errores y en caso de que ocurriera un error, capa superiores tales como TCP o dispositivos finales, podrán recuperar de dichos errores. Como tal, Frame-relay no provee integridad de datos, ni tampoco provee ningún tipo de control de flujo. Frame-Relay emplea un mecanismo de chequeo de error (error-checking) basado en un polinomio CRC de 16 bits; este polinomio provee detección de error en tramas de hasta 4096 bytes de largo.

En el caso de Frame-Relay, los proveedores (Carriers) aprovisionan a los clientes circuitos virtuales permanentes (PVCs: permanent virtual circuits). Dichos circuitos son canales lógicos entre el dispositivo de acceso Frame-Relay (FRAD) y el switch que son aprovisionados a lo largo de la red Frame-Relay. Un router con capacidad Frame-Relay es un excelente ejemplo de FRAD.

Un identificador de conexión de enlace (DLCI: data-link connection identifier) identifica el PVC Frame-Relay en el acceso. Las tramas son ruteadas a través de uno o más circuitos virtuales identificados por DLCIs. Cada DLCI posee una configuración permanente de camino hacia un destino determinado. Además si el sistema posee una configuración permanente de camino hacia un destino determinado. Además si el sistema posee varios DLCIs configurados puede comunicarse simultáneamente con diferentes sitios al mismo tiempo. La interface usuario-red (UNI: User-Network interface) provee demarcación entre el FRAD y la red Fram-Relay. La combinación de un UNI y un DLCI especifica el punto final para un circuito virtual particular. El DLCI posee significación local y la numeración es decidida por el operador y asignada por el proveedor de servicios Frame-Relay. El número del DLCI puede ser mayor o igual a 1 o menor o igual a 1022 dentro de un mismo UNI. La Figura 35 se detalla un ejemplo de Fram-Relay desde la perspectiva del cliente.

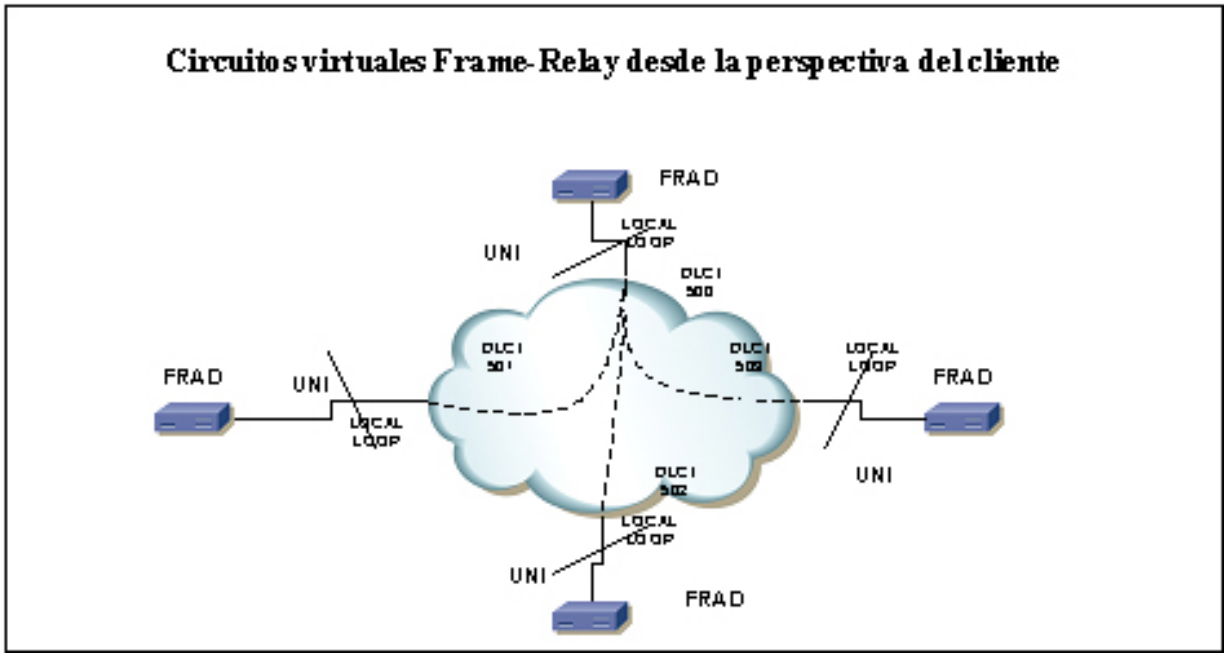


Figura 48 – Frame-Relay (vista cliente)

Los PVCs de Frame-Relay han pasado a ser tan populares que las mayorías de las migraciones de circuitos de las empresas se presentan de líneas dedicadas punto-a-punto a PVCs de Fram-Relay.

Otro parámetro llamado Tasa de Información Comprometida (CIR: Commited Information Rate), define un acuerdo entre el proveedor y el cliente en referencia para la entrega de datos de un circuito virtual particular, y su unidad es bits por segundo (bps). El CIR mide la cantidad promedio de datos sobre un periodo específico de tiempo (generalmente un segundo) en que la red intentará los mismos con prioridad normal.

En el caso de congestión, las ráfagas de datos que excedan el CIR serán marcadas como elegidas para descartar (DE: discard eligible) y serán entregadas con prioridad menor o posiblemente descartadas.

El protocolo de soporte operacional para la UNI se llama manejo de interface local (LMI: Local Managemet Interface). Los estándares de LMI empleados son ANSI T1.617 Annex D y Q.933 Annex A. El LMI define el protocolo de poleo entre el FRAD y el switch Frame-Relay. El FRAD genera periódicamente un mensaje status enquiry, y el Switch Frame-Relay debe responder con un mensaje status. El LMI verifica la integridad del enlace, el estado de los PVCs, y las condiciones de error que existen en la señalización de enlace, o podría también indicar problemas internos de la red. A fin de poder compartir dicha información entre los dispositivos de acceso (FRAD y Switch), el LMI emplea un DLCI para la comunicación entre los dispositivos, y el DLCI 0 que el LMI Annex A y Annex D emplean para señalización.

Las redes Frame-Relay poseen además dos métodos de control de congestión para manejar el trafico: explicit congestion notification (notificación explicita de congestión) e implicit congestion notification (notificación implícita de congestión).

La notificación explícita de congestión emplea los bits FECN (forward o hacia delante) y BECN (backward o hacia atrás) incluidos en el campo de dirección T1.618, y a su vez, el empleo de estos bits es determinado por la dirección del flujo de trafico. El bit FECN es enviado al próximo switch Frame-Relay en la dirección del flujo de datos, y el bit BECN es enviado en la dirección opuesta del sentido del tráfico de los datos.

La notificación implícita de congestión se realiza en los protocolos superiores del FRAD o de algún dispositivo terminal que controle la cantidad de datos que ingresan en la red en cada extremo.

ATM (Asynchronous Transfer Mode)

El protocolo Modo de Transferencia Asincrónica (ATM: Asynchronous Transfer Mode) es un protocolo derivado de los estándares desarrollados por la ITU-T basados en la tecnología BISDN (Broadband ISDN o Red Digital de Servicios Integrados de Banda Ancha).

ATM es un servicio orientado a la conexión (connection-oriented) en el cual los datos transmitidos son organizados dentro de una celda de largo fijo. Los protocolos superiores y datos de usuarios tales como un paquete IP son segmentados en unidades de datos de protocolo de 48 bytes (PDUs: Protocolo Data Units). A dichos PDUs se le agrega un encabezado ATM de 5 bytes y la resultante celda de 53 bytes es colocada dentro de un switch ATM y a su vez multiplexada con otras celdas. Posteriormente las celdas compiten por ranuras vacantes (slots) en las ráfagas de celdas ATM salientes. Cada encabezado de celda ATM contiene un identificador de camino virtual (VPI: virtual path identifier) y un identificador de de circuito virtual (VCI: virtual channel identifier), que juntos definen el circuito virtual ATM que la celda necesita para continuar en el trayecto hacia su destino. La tasa de arribo, o el retardo, de una ráfaga particular de celdas resulta no periódica, por lo tanto, la transferencia de celdas se denomina como Modo de Transferencia Asincrónica, en contraste con el trasporte sincrónico de TDM, que emplea periodos de tiempos fijos para la transmisión y recepción de tramas.

ATM fue pensada como una tecnología extremo a extremo para expandir redes LANs y WANs en forma global. La naturaleza de la tecnología del circuito virtual orientada a la conexión hizo que ATM sea adecuada para implementaciones de WANs multi-servicios, dando a las redes de los Carriers la posibilidad de transportar datos, voz y video. De todas maneras, la emulación de ambientes broadcast encontrados en las LANs, lleva al desarrollo de complejos protocolos de emulación de LAN tales como LANE (LAN emulation), que han encontrado éxito limitado mayoritariamente como una red de puentes para segmentos de tecnologías LAN totalmente colapsadas. El protocolo ATM como tecnología de alta velocidad dentro de las redes LAN ha sido superado por tecnologías FastEthernet y GigabitEthernet. Dichos protocolos son simples y fáciles de implementar en redes de área local, y más importante resulta el hecho de que el protocolo Ethernet es más familiar para los usuarios corporativos y al mismo tiempo existe una gran base instalada de esta tecnología.

Para el caso de las redes de servicio ATM, los Carriers aprovisionan PVCs a sus clientes (como harían en el caso de Frame-Relay). Dichos circuitos son identificados mediante el para identificados de camino virtual / identificador de circuito virtual (VPI/VCI).

El protocolo ATM se encuentra basado en le modelo de arquitectura de protocolo ISDN de Banda Ancha (Broadband ISDN). Este modelo varia del modelo OSI de referencia ya que hace uso de un modelo de tres dimensiones, en lugar de dos como el OSI. La arquitectura ATM emplea un modelo lógico para describir las funciones soportadas por el protocolo tal, como se muestra en la figura 36.

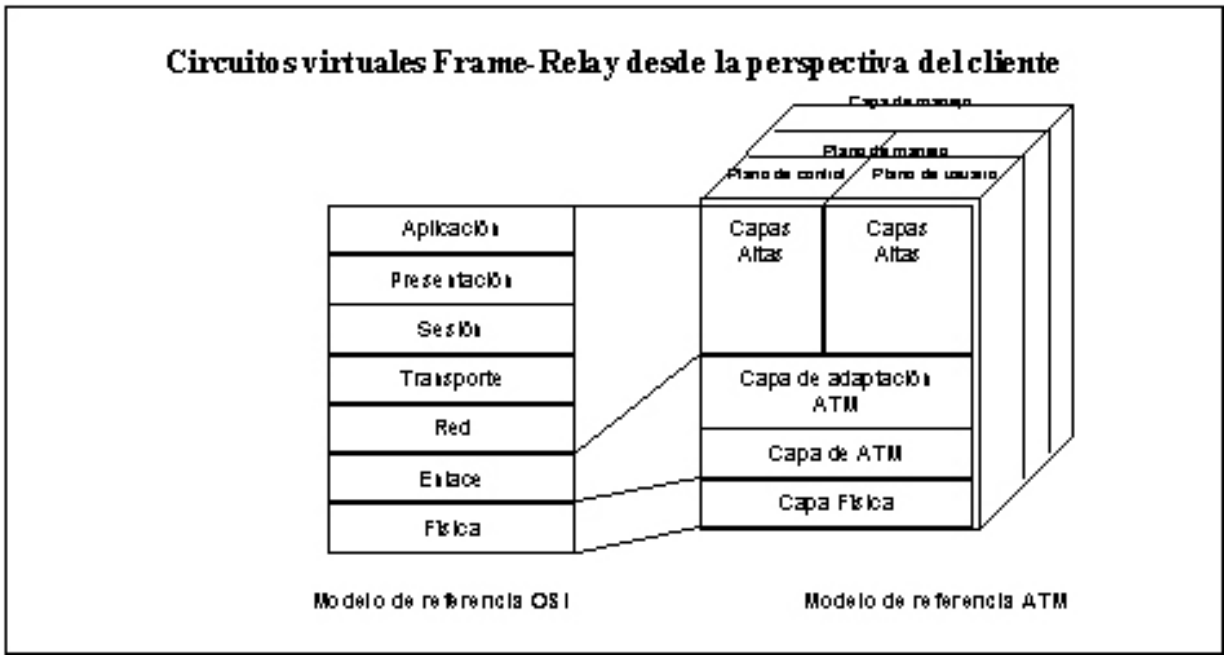


Figura 49 – VC Frame-Relay (vista cliente)

Existen tres planos en el modelo de referencia ATM, los cuales son responsables de la señalización, transferencia de datos del usuario y del manejo (managment).

- Plano de control (Control Plane): este plano es responsable de generar y manejar las solicitudes de señalización. El plano de control soporta llamadas y funciones de conexión de control tales como señalización (establecimiento, supervisión y liberación de llamadas y conexiones).
- Plano del usuario: contiene dos componentes, la capa de manejo y el plano de manejo. La capa de manejo supervisa funciones específicas de capa tales como la detección de fallas y problemas en el protocolo. El flujo de información de operación, administración, y mantenimiento (OAM) es un ejemplo de función de capa de manejo. El plano de manejo coordina y administra funciones relacionadas con el sistema completo, es decir, interviene en la coordinación entre planos.

Las capas de protocolo ATM presentan el flujo de datos hacia y desde protocolos de capa superior tales como TCP/IP. Dichas capas se dividen en:

- Capa Física: es análoga a la capa física del modelo OSI, manejando la transmisión a través del medio.
- Capa ATM: en combinación con la capa de adaptación ATM (AAL), esta capa es análoga a la capa de enlace del modelo OSI, y es la responsable del establecimiento de las conexiones y pasaje de celdas a través de la red ATM.
- Capa de adaptación ATM (AAL): la capa AAL es responsable del aislamiento de los protocolos de capa superior del detalle de los procesos ATM. Aquí se realiza la segmentación y re-ensamblado de los PDUs. Existen tres capas de adaptación: AAL1 (servicio orientado a la conexión adecuado para el manejo de voz y video conferencia), AAL3/4 (soporta servicios orientados y no orientados a la conexión, y es empleado para transmitir paquetes SMDS sobre redes ATM), y AAL5 (es la adaptación para los datos ya que soporta servicios orientados y no orientados a la conexión y es empleado para el transporte de IP clásico sobre ATM).

La generación de celdas ATM responde a la siguiente secuencia: la información de usuario como el trafico de voz, datos y video es enviado desde las capas superiores hacia las porción de subcapa de convergencia (CS) de la capa de adaptación ATM que esta siendo empleada. En dicha subcapa es agregada información en el encabezado y en la cola, y luego enviada a la subcapa de segmentación y re-ensamblado (SAR). Una vez generado el PDU de 48 octetos pasa por la capa ATM donde se le agrega el encabezado apropiado (UNI o NNI), resultando en una celda de 53 octetos. Posteriormente la celda se transmite sobre el medio físico hacia un switch de destino, y luego despachada hacia el dispositivo del usuario final.

Una red ATM puede incluir distintas interfaces. La interfaz UNI conectada a la red ATM con los equipos en casa de cliente, tales como un switch ATM o un router. El termino NNI (Network Node Interface) se emplea para describir diversos modos de interconexión de redes entre distintos Carriers.

Cuando un dispositivo final en ATM requiere establecer una conexión con otro dispositivo final, este envía un paquete de solicitud de señalización hacia el switch ATM directamente conectado. Dicha solicitud contiene la dirección ATM del punto final con el que se desea conectar, como así también cualquier parámetro de calidad (QoS) requerido para la conexión. La señalización del protocolo ATM puede variar de acuerdo a la naturaleza del enlace ATM UNI o NNI.

Cada celda enviada a una interfaz UNI o NNI contiene información que identifica la conexión virtual a la que pertenece. La identificación posee dos partes: un identificado de canal virtual y otro de camino virtual, ambos empleados en la capa ATM. La figura 37 muestra circuitos virtuales de ATM desde la perspectiva del cliente.

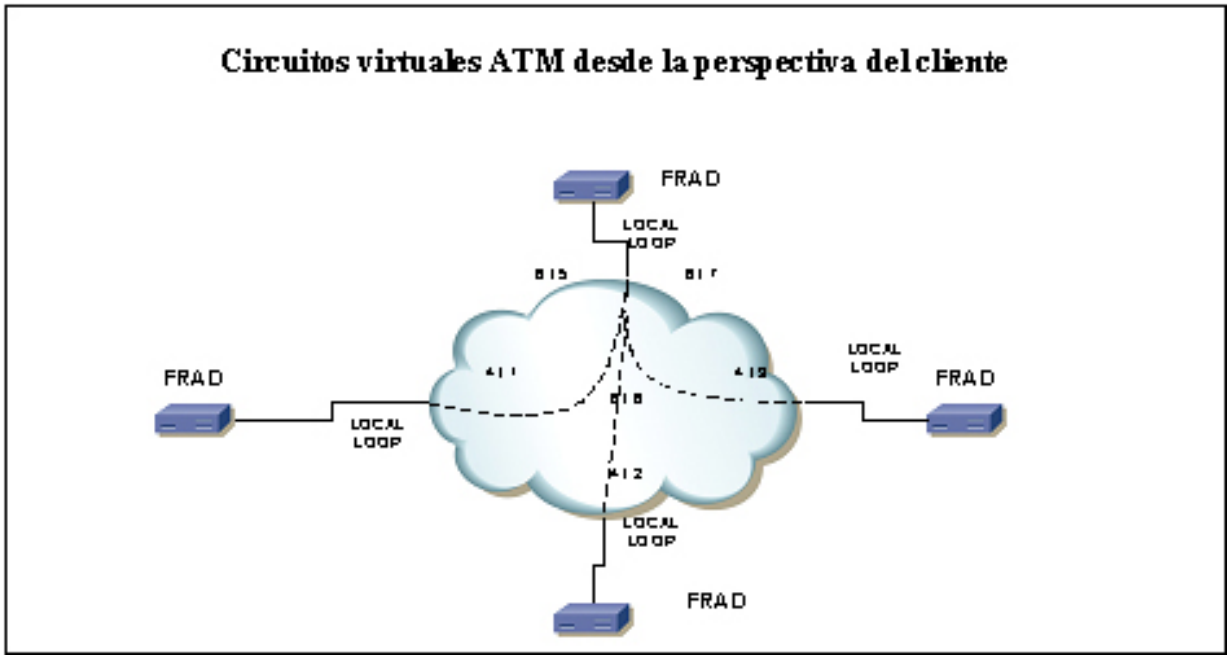


Figura 50 – VC ATM (vista cliente)

El manejo de tráfico es una de las claves del protocolo ATM que los distingue de los actuales protocolos de red (networking protocols), y que lo hace adecuado para el desarrollo de redes de alta velocidad y la provisión de performance garantizada en un ambiente integrado. El soporte garantizado de QoS (Quality of Service) dentro del protocolo ATM se compone de contratos de trafico, trafico moldeado (traffic shaping) y políticas de trafico. El foro ATM ha definido cuatro clases de servicio para la capa ATM, cada uno de ellos con niveles de escalabilidad:

- Clase A: Tasa Constante de Bits (CBR: constant bit rate). El trafico CBR es caracterizado por una ráfaga continua de bits a una tasa constante, como lo es el trafico TDM.
- Clase B: Tasa de Bits Variable en Tiempo Real (VBR-RT: variable bit rate, real time). El trafico VBR-RT posee una naturaleza de ráfagas donde el retardo extremo a extremo resulta critico (aplicación de voz y video).
- Clase C: Tasa de Bit Variable en Tiempo No Real (VBR-RNT: variable bit rate, non real time). El trafico VBR-NRT posee una naturaleza de ráfagas en el cual es retraso extremo a extremo no resulta critico (programas de entrenamiento grabados, y mensajes de correo en video).
- Clase D:
  - Tasa de Bit Disponible (ABR: available bit rate). El tráfico ABR puede ser representado por tráfico de LAN en ráfagas y por datos más tolerantes a los retardos y a la perdida de celdas.
  - Tasa de Bit sin especificar (UBR: unespecified bit rate). El tráfico UBR es un servicio con pocas garantías donde no se especifica tasa de transmisión, ni posee garantía de QoS.

Ruteo de Capa 3

El ruteo de capa de red esta basado en el intercambio de información de alcance dentro de una red. Al tiempo que un paquete atraviesa la red, cada router extrae del encabezado de capa 3toda la información relevante para realizar el proceso de envió (forwarding). Dicha información es empleada como índice para la búsqueda dentro de la tabla de ruteo y así determinar el próximo salto (nodo) del paquete. Dicho proceso se repite en cada router a lo largo de la red, por lo cual, la decisión del optimo envión de un paquete debe realizarse nuevamente.

La información dentro de los paquetes IP tales como la información de calidad de servicio (IP QoS), generalmente no es considerada, obteniendo así máxima performance en el proceso de envió de paquetes (forwarding). Típicamente, solo se considera la dirección de destino, a pesar de que el campo de IP QoS convierte otros campos tales como T0S (Type of Service) en relevantes dentro del encabezado. De esta manera, un análisis complejo del encabezado debería realizarse en cada router que el paquete encuentre en su camino hacia la red de destino.

Las funciones de ruteo poseen dos componentes separados: el componente del envió (forwarding), y el componente de control.

Componente de envió (forwarding)

El componente de envió utiliza información contenida en la tabla de envió y en el encabezado de capa 3. Al mismo tiempo, emplea un conjunto de algoritmos que definen el tipo de información extraída del encabezado del paquete y el procedimiento que el router utilizará encontrar la entrada asociada dentro de la tabla de envió (forwarding table). El router luego envía los paquetes basándose en dicha información. El envió de paquetes responde a:

- Unicast forwarding: El router emplea la dirección de destino del encabezado de capa 3 y el algoritmo que determine la mayor coincidencia con dicha dirección para encontrar una entrada en la tabla de envió o forwarding.
- Unicast forwarding con ToS: el router emplea la dirección de destino y el valor del campo ToS del encabezado de Capa 3, y el algoritmo que determine la mayor coincidencia con dicha dirección, como así también con el mapeo exacto de ToS para encontrar una entrada en la tabla de envió o forwarding.
- Multicast forwarding: el router emplea las direcciones de origen y destino del encabezado de capa 3 como así también la interface de ingreso del paquete al router. Luego, el router emplea un algoritmo que determine la mayor coincidencia con la dirección de origen y destino, como así también el mapeo exacto sobre la interface de entrada para encontrar una entrada asociada en la tabla de envió o forwarding.

Componente de Control

El componente de control es responsable de la construcción y mantenimiento de la tabla de envió (forwarding table). Dicho proceso se implementa mediante protocolos dinámicos de ruteo tales como OSPF (Open Shortest Path First), IS-IS (Intermediate System – Intermediate System), RIP v1y2 (Routing Information Protocol), BGP (Border Gateway Protocol), y PIM (Protocol Independent Multicast), que intercambian información de ruteo entre routers, como así también el algoritmo de Dijkstra o el algoritmo de difusión que el router emplee para convertir las tablas de topología de red en tablas de ruteo (forwarding table).

Forwarding Equivalency Class

La clase de equivalencia de envió (FEC: Forwarding Equivalency Class) consiste en un conjunto de paquetes de Capa 3 que son enviados de una misma manera sobre un mismo camino y con el mismo tratamiento de envió (forwarding). Mientras se asigna un paquete a una FEC, el router podrá observar el encabezado IP y también alguna información, como por ejemplo, la interface por la cual arribo dicho paquete, Las FECs pueden proveer un envió (forwarding) granular basado en la cantidad de información requerida para configurar la equivalencia. A continuación se muestran algunos ejemplos de FECs:

- Un conjunto de paquetes unicast cuya dirección destino de Capa 3 coincide con un cierto prefijo de dirección.
- Un conjunto de paquetes unicast cuya dirección destino coincide con un prefijo de dirección IP particular y similar valor de campo tipo de servicio.
- Un conjunto de paquetes unicast cuya dirección destino coincide con un prefijo de dirección IP particular y poseen el mismo puerto TCP destino.
- Un conjunto de paquetes multicast con la misma dirección origen y destino de Capa 3.
- Un conjunto de paquetes multicast con similar dirección origen y destino de Capa 3 y la misma interface de ingreso al router.

Por ejemplo, como se muestra en la Figura 38, la dirección IP 200.15.45.9 y la IP 200.15.45.126 se encuentran dentro de la misma FEC con un prefijo de dirección 200.15.45.0/24 y puerto destino 23 de TCP.

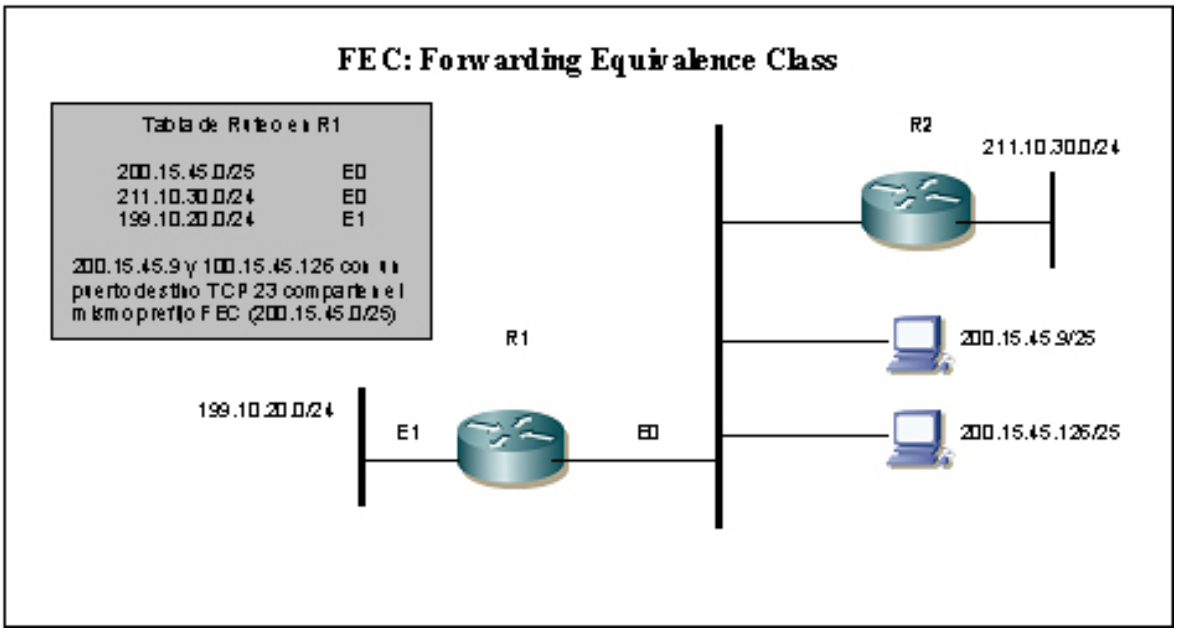


Figura 51 – Detalle de FEC

Conmutación de etiquetas

Los dispositivos de conmutación de etiquetas (Babel-switching) asignan etiquetas pequeñas y fijas en tamaño en los paquetes y celdas. Las entidades de conmutación realizan búsquedas en las tablas basándose en estas simples etiquetas para determinar donde debe ser enviado el tráfico.

La etiqueta contienen en forma resumid información esencial acerca del proceso de envió del paquete o celda. Esta información incluye el destino, la prioridad (precedente), la pertenecía a una VPN (Virtual Private Network), información de QoS, y la ruta con ingeniería del trafico (traffic engineering) para el paquete en cuestión.

Mediante la conmutación de etiquetas, el análisis completo del encabezado de la Capa 3 es realizado solamente una vez: al ingreso de la red conmutada de etiquetas. En dicho punto, el encabezado de la Capa 3 es mapeado con una etiqueta de tamaño fijo.

En cada entidad conmutadora de etiquetas o router a lo largo de la red, solo necesitaran examinar la etiqueta del paquete o celda entrante para enviar los mismos en su camino a través de la red.

En el egreso de la red, una entidad de borde conmutadora de etiquetas (edge Babel switching) o un router quitará la etiqueta para el apropiado encabezado de Capa 3 ligado con dicha etiqueta. El protocolo MPLS integra la performance y las capacidades del manejo de tráfico de la Capa 2 (capa de enlace) con la escalabilidad y flexibilidad de una red de Capa 3. Esta integración puede ser aplicable a cualquier red que emplee conmutación de Capa 2, aunque presente mayores ventajas al aplicarse sobre redes ATM. MPLS integra el ruteo IP con la conmutación ATM para ofrecer redes escalables de IP sobre ATM.

La técnica de conmutación de etiquetas integra funciones de conmutación y ruteo, combinando la propiedad de alcance de la información provista por la función del router, más los beneficios alcanzados por la ingeniería de tráfico mediante la optimización de las capacidades de los switches.

Ruteo convencional de Capa 3 versus MPLS

El ruteo convencional, al momento en que los paquetes de Capa 3 son enviados de un router al siguiente, cada uno de ellos realiza una decisión de envió (forwarding) independiente para dicho paquete. Cada router analiza la dirección de destino de Capa 3 dentro del encabezado del paquete, y ejecuta un algoritmo de capa de ruteo, y elige en forma independiente el próximo salto para dicho paquete basándose en estos análisis. Las decisiones de envió (forwarding) son el resultado de dos funciones:

La clasificación de paquetes de Capa 3 dentro de las FECs basándose en la mayor igualación de prefijo de dirección.

Igualación de FECs en el próximo salto.

Todos aquellos paquetes que pertenezcan a una FEC particular y que provienen desde un mismo nodo siguen el mismo camino. En caso de que existan múltiples caminos similares hacia el mismo destino, los

paquetes seguirán algún camino del conjunto asociado a dicha FEC. A medida que el paquete atraviesa la red, cada salto a su vez reexaminará el paquete y lo asignará a una FEC.

En MPLS la asignación de un paquete particular es realizado una sola vez cuando el paquete ingresa en la red. La FEC al cual el paquete es asignado se encuentra codificada en un valor pequeño y de tamaño fijo conocido como etiqueta. Cuando el paquete es enviado hacia el próximo salto, la etiqueta lo acompaña a lo largo de de este trayecto; esto significa que la etiqueta se coloca antes de enviarlo. En los subsiguientes saltos, no se continúan realizando mas análisis sobre el encabezado de la capa de red, en su lugar se emplea la etiqueta como índice dentro de una tabla que especifica el próximo salto y una nueva etiqueta. La vieja etiqueta entrante es remplazada por la nueva, y el paquete es enviado hacia el nuevo salto.

En el paradigma de envió MPLS, tan rápido como un paquete sea asignado en una FEC, no mas análisis se realiza sobre su encabezado de Capa 3 en los subsiguientes routers. Todo el manejo de envió se realiza mediante las etiquetas; esto presenta una nueva ventaja sobre el proceso de envió del ruteo convencional.

Los routers con protocolo MPLS pueden asignar paquetes arribando en diferentes puertos a diferentes FECs. Esto forma la base para la construcción de las redes privadas virtuales (Virtual Private Networks) de MPLS. Por el contrario, el envió convencional puede considerar solamente la información que viaja en el paquete dentro de su encabezado de Capa 3.

La ingeniería de trafico fuerza a los paquetes a seguir rutas particulares para de esta manera, optimizar y balancear el trafico en enlaces subutilizados. En el protocolo MPLS una etiqueta puede ser usada para representar una ruta, entonces la identidad de la ruta explícita la necesita ser transportada con el paquete. En el envió convencional, esto requiere que el paquete lleve consigo su ruta codificada (source routing).

Los routers convencionales analizan el encabezado de capa de red del paquete no solamente para determinar el próximo salto, sino también para determinar la prioridad o la clase de servicio del paquete. Ellos entonces podrían aplicar diferentes umbrales de descarte para diferentes paquetes.

El protocolo MPLS permite determinar, en forma total o parcial, por medio de la etiqueta el QoS en términos de la prioridad o de la clase de servicio. En dicho caso, la etiqueta representa la combinación de una FEC y una prioridad o clase de servicio.

Integración de los protocolos IP y ATM

EL concepto de “IP sobre cualquier protocolo” ha tomado ventaja sobre el enfoque de forzar el protocolo ATM a comportarse como un protocolo LAN. El protocolo LAN, IP clásico sobre ATM y MPOA (multiprotocol over ATM) ha tenido crecimiento limitado y fueron aventajados por el protocolo FastEhernet (100Mbps) y GigabitEthernet (1000Mbps). Sin embargo, ATM ha tenido un crecimiento masivo en el ámbito WAN ya que el QoS ha proporcionado al protocolo la capacidad multiservicio para ofrecer clases de servicios separados por voz, video y datos.

IP y ATM corresponden a tecnologías completamente distintas. ATM es un protocolo orientado a la conexión y establece circuitos (PVCs) antes de enviar tráfico sobre un camino predeterminado y emplea celdas de tamaño fijo y QoS predefinido. El protocolo IP, en cambio, es una tecnología no orientada a la conexión. Su gran aceptación radica en su habilidad para adaptarse a cualquier protocolo de capa de enlace y de transporte.

Generalmente, IP y sus protocolos de ruteo asociados corren sobre ATM o Frame-Relay con pequeña integración. Los proveedores de servicio de Internet (ISP), por ejemplo construyen sus redes principales con ATM o Frame-Relay dentro de sus redes IP, y estas redes son utilizadas para armar (PVCs) entre sus routers de borde. Esto genera un modelo overlay o sobrecargado que no es escalable ni tampoco fácil de operar (Figura 39 A), básicamente porque todos los routers de la red se convierten en vecinos a nivel IP.

El modelo overlay requiere que cada router tenga una adyacencia con cada otro de los routers de la red, y debido a que las mismas deben establecerse utilizando los circuitos virtuales ATM, la red requiere de una malla completa (full-Meshed network) de PVCs para conectar los routers. A medida que el numero de routers crece, el numero de PVCs de la malla crece a N*(N-1)/2, donde n es el numero de routers dentro de la red. Cualquier red menor implica que exista más de un salto para alcanzar otro router. El resultado final es una red ATM con una gran cantidad de PVCs con problemas de escalabilidad. Además, la provisión y des-provisión (en caso de baja de algún router) se convierten en una tarea ardua para los operadores de red.

Otro problema que presentan lasa redes tradicionales resulta de los protocolos de ruteo, tales como OSPF, que no trabajan bien sobre grandes redes, totalmente mayadas, debido a los duplicados de es-

tado de los enlaces, y al gran numero de maquinas de estado vecinas (otros routers con OSPF) a ser mantenido. La oscilación de rutas causadas por fallas en los enlaces puede exceder el uso de la CPU del dispositivo y causar inestabilidades en la red.

El protocolo MPLS soluciona le problema de la sobrecarga de mallas eliminando la noción de red ATM o Frame-Relay. Mediante MPLS, los switches ATM se enteran del protocolo IP, y consecuentemente los enlaces ATM son tratados como vínculos IP. De esta manera, cada switch ATM se transforma en vecino IP, tal cual se encuentra ilustrado en la (Figura 39 B), en donde el router forma solo tres vecindades o adyacencias, cada una de ellas con R3, R4 y LSR2.

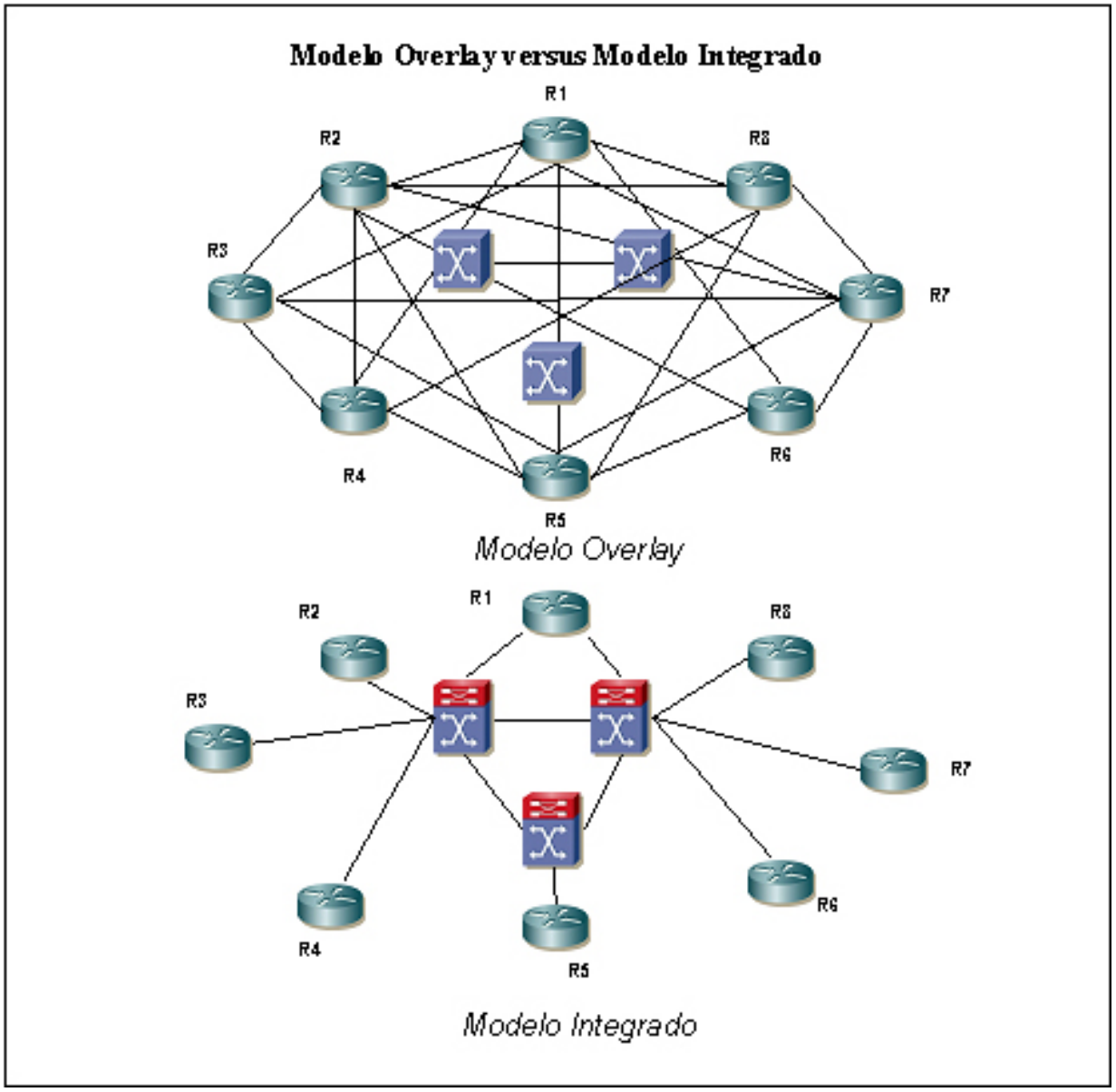


Figura 52 – Modelo overlay (A) / Modelo Integrado (B)

MPLS versus IP sobre ATM tradicional

Al integrar los switches ATM, la tecnología de conmutación de etiquetas toma ventaja en el equipamiento de conmutación (switches) optimizado para celdas ATM de tamaño fijo y conmutación de celdas a alta velocidad:

Integración: al ser aplicado en ATM, MPLS integra las funcionalidades de IP y ATM, en lugar de sobrecargar IP sobre ATM.

Mayor confiabilidad: MPLS se convierte en una solución fácil para integrar protocolos de ruteo en redes WAN con infraestructura ATM. El protocolo IP sobre ATM tradicional requiere de la configuración de una malla de PVCs entre routers de la red.

Implementación directa de Clases de Servicio: cuando es empleado con equipamiento ATM, MPLS hace uso de las capacidades de encolamiento (queuing) y almacenado (buffering) para proveer diferentes clases de servicio. Esto permite el soporte para empleo directo de IP Precedente (prioridad de paquetes IP) y CoS en switches ATM sin necesidad de realizar transformaciones a las clases de servicio de ATM.

Soporte eficiente de Multicast y RSVP: en contraste con MPLS, el IP sobre ATM tradicional posee grandes desventajas particularmente en el soporte de IP Multicast y el Protocolo de Reserva de Recursos (RSVP: Resource Reservation Protocol).

Escalabilidad y manejo de VPNs IP: MPLS puede convertir los servicios de redes privadas virtuales IP (IP Virtual Private Networks) en escalables y fáciles de manejar. Los servicios de VPN resultan muy importantes y atractivos para aprovisionar a las empresas que poseen redes IP dentro de su infraestructura. La combinación de MPLS y Multiprotocol BGP (MBGP) hace que el servicio de VPN basado en MPLS sea fácil de implementar y operar en los sitios remotos. Al mismo tiempo provoca que este servicio sea extremadamente escalable con una sola red capaz de soportar varios miles de VPNs.

Reducción de carga en las redes principales (core): Los servicios de VPN demuestran como MPLS soporta una jerarquía de conocimiento del ruteo. Adicionalmente, es posible aislar las tablas de las rutas de Internet de las rutas principales (core) de los proveedores. Mediante MPLS, el transito entrante en el borde del sistema autónomo del proveedor puede asignarle etiquetas que se encuentran asociadas con puntos de salidas específicos. Como resultado, los routers internos de transito y los switches necesitan solo procesar conectividad con los routers de borde del proveedor, aislando de esta manera los dispositivos internos del excesivo volumen de rutas intercambiadas en Internet.

Capacidades de Ingeniería de tráfico (Traffic Engineering): MPLS provee capacidades de ingeniería de tráfico necesaria para el eficiente empleo de los recursos de la red. La ingeniería del tráfico permite derivar carga de tráfico de las partes de la red sobre-utilizadas hacia las partes sub-utilizadas, de acuerdo al destino del tráfico, el tipo y carga del mismo, la hora del día, etc.

Retos a afrontar por los proveedores de servicios

Los Carriers y los proveedores de servicios también necesitan examinar de cerca sus costos de infraestructura de red y costos operacionales. El aprovisionar una infraestructura de transporte homogénea esta visto como la manera mas eficiente en cuanto a costo y la mas flexible para encarar las limitaciones.

Los Carriers y los proveedores de servicios buscan formas de integrar sus variadas propuestas tales como servicios basados en ATM, Frame-Relay, e IP, como también acceso a Internet, intranets y extranets sobre una única infraestructura de red en lugar de emplear redes paralelas para cada servicio.

En general los clientes corporativos no se encuentran satisfechos si deben manejar redes separadas para voz, datos y videoconferencias. Prefieren un circuito de terminación híbrida con un protocolo de acceso uniforme, como lo es IP. Además, necesitan niveles de servicios garantizados, como se detalla en el SLA (Service-Level Agreement), e implementados por el proveedor de servicios en la forma de QoS empleando múltiples clases de servicio para la voz, los datos y el video.

Arquitectura MPLS

Operación de MPLS

Las redes MPLS emplean etiquetas para enviar paquetes, y los mismos son asignados por única vez dentro de una clase de equivalencia de envió (FEC: Forwarding Equivalence Class) al ingresar en un nodo de borde de la red MPLS.

La FEC en la que el paquete es asignado, se codifica mediante un valor de tamaño fijo denominado etiqueta. Los paquetes son etiquetados antes de ser enviados, y en los saltos subsiguientes ningún análisis del encabezado del paquete necesita realizarse. Al mismo tiempo, cuando un paquete MPLS arriba en un nodo MPLS interno (backbone), la etiqueta del mismo es empleada como un índice dentro de una tabla para determinar el próximo salto y la nueva etiqueta para dicho paquete. Posteriormente, la etiqueta antigua es remplazada mediante la nueva, y el paquete es enviado hacia el próximo salto. Consecuentemente, en una red MPLS las etiquetas controlan todos los envíos (forwarding). Esto posee ciertas ventajas por sobre el ruteo tradicional.

- El envió MPLS puede llevarse a cabo por switches, los cuales pueden realizar búsquedas y reemplazos de etiquetas, aunque son incapaces de analizar los encabezados de capa 3.
- Cuando un paquete ingresa a la red es asignado a una FEC. El router de ingreso puede emplear cualquier información que posea el paquete, como por ejemplo la interface por la cual ingreso, aunque esta información no puede ser extraída del encabezado de red. Como resultado, las decisiones de

envió (forwarding) que dependen del router de ingreso podrán realizarse con facilidad. Por otro lado, en el tradicional envió de IP, esto no puede llevarse a cabo, ya que la identidad del router de ingreso no viaja junto con el paquete. En la operación de MPLS, los paquetes que ingresan en los CPEs (Customer Premises Equipment) por diferentes interfaces pueden ser asignados en diferentes FECs, y a su vez, las etiquetas adosadas representan dichas FECs. Esta funcionalidad conforma la base para la construcción de las Redes Privadas Virtuales (VPNs: Virtual Private Networks).

- Las redes que poseen ingeniería del tráfico pueden forzar los paquetes a seguir un camino particular, como por ejemplo un camino sub-utilizado. Este camino es elegido explícitamente antes o al momento en que el paquete ingresa en la red, en lugar de ser seleccionado por el normal algoritmo de ruteo dinámico a medida que el paquete viaja por la red.
- La Clase de Servicio (CoS) de un paquete puede ser determinado por los nodos MPLS de ingreso. Dicho nodo puede luego aplicar diferentes niveles de descarte o políticas programadas de disciplina en diferentes paquetes. Los saltos subsiguientes pueden reforzar la política de servicio empleando un conjunto de comportamientos locales. MPLS permite (aunque no requiere) inferir en forma total o parcial de la etiqueta del paquete el parámetro Precedente (prioridad) o Class of Service (clase de servicio). En dicho caso, la etiqueta representa la combinación de una FEC y una prioridad o clase de servicio. La funcionalidad anteriormente descripta forma la base de la implementación de Calidad de Servicio en redes MPLS (MPLS QoS).

Arquitectura del nodo MPLS

Los nodos MPLS poseen en su arquitectura dos planos: el plano MPLS de envió (MPLS forwarding plane) y el plano MPLS de control (MPLS control plane). Los nodos MPLS además de conmutar paquetes etiquetados, realizan ruteo de Capa 3 y conmutación de Capa 2. La Figura 40 detalla la arquitectura básica de un nodo MPLS.

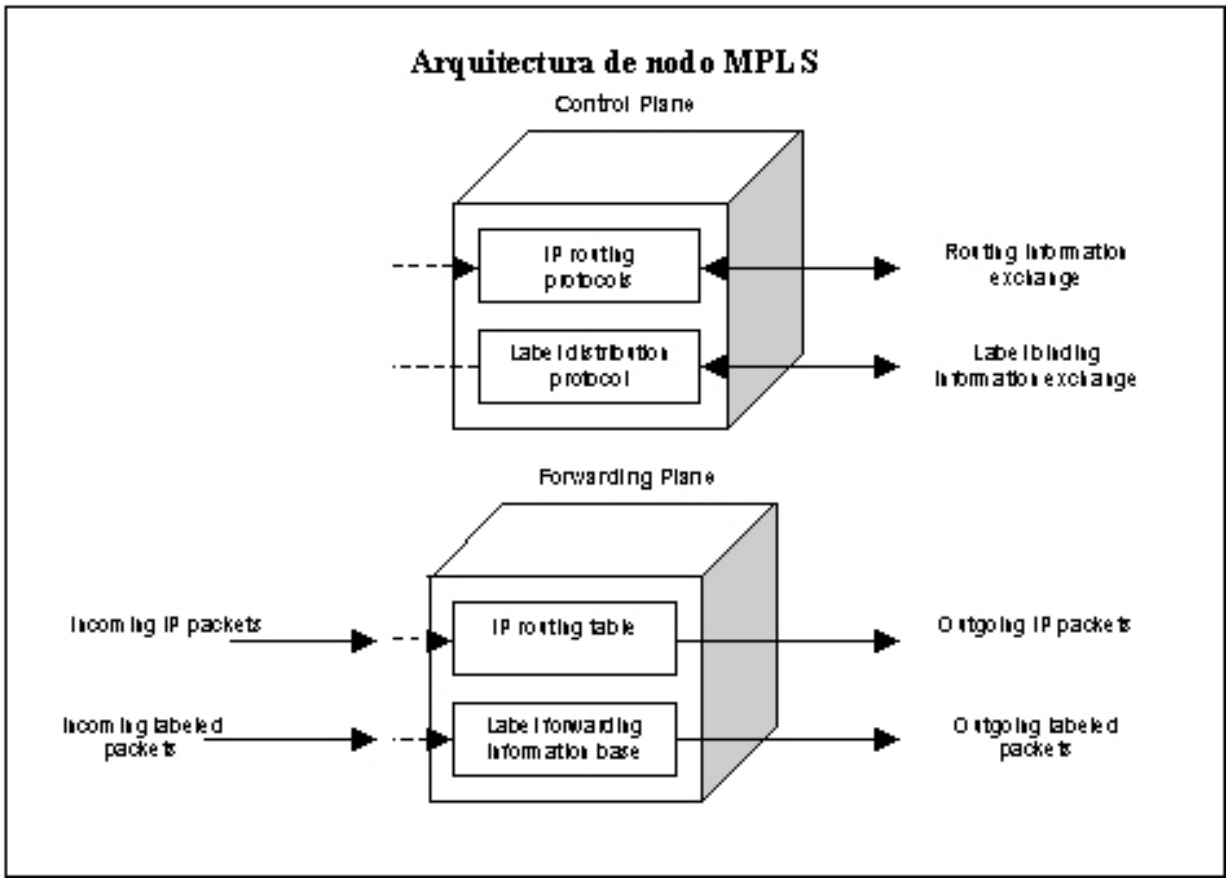


Figura 53 – Arquitectura MPLS

El plano de envío

El plano MPLS de envió (forwarding plane) es responsable del envió de paquetes basados en los valores contenidos en las etiquetas adosadas. El plano de envió emplea una base de etiquetas de envió (LFIB: label forwarding information base) mantenida por el nodo MPLS para el envió de paquetes etique-

tados. El algoritmo utilizado por la componente de conmutación de etiquetas (label switching forwarding component) emplea información contenida en la LFIB como así también la información contenida por el valor de la etiqueta. Cada nodo MPLS mantiene dos tablas importantes del protocolo MPLS: la base de información de etiquetas (LIB: label information base) y la LFIB. La LIB contiene todas las etiquetas asignadas localmente por el nodo MPLS y el mapeo de estas con las etiquetas recibidas de los nodos vecinos MPLS. La base LFIB emplea un subconjunto de etiquetas contenidas en la base LIB para el envió efectivo de paquetes.

Una etiqueta de tamaño fijo 32 bits es el identificador empleado para individualizar una FEC (generalmente con representación local). Por lo tanto, la etiqueta adosada a un paquete en particular representa la FEC en la cual el paquete fue asignado.

En el caso del protocolo ATM, la etiqueta es colocada en el campo VCI o VPI del encabezado ATM. Sin embargo si la trama es Frame-Relay, la etiqueta ocuparía el campo de DLCI dentro del encabezado de Frame-Relay.

Las tecnologías de capa de enlace (Capa 2) tales como Ethernet, Token Ring, FDDI, y los enlaces punto-apunto no pueden emplear sus campos de dirección de capa de enlace para transportar las etiquetas. Por lo tanto, las anteriores tecnologías transportan las etiquetas mediante encabezados espejados (shim header), y a su vez, dicho encabezado se inserta entre los de capa de enlace y capa de red, como muestra la Figura 41. El empleo del encabezado shim de etiquetas permite el soporte del protocolo MPLS sobre gran variedad de tecnologías de capa de enlace (Capa 2).

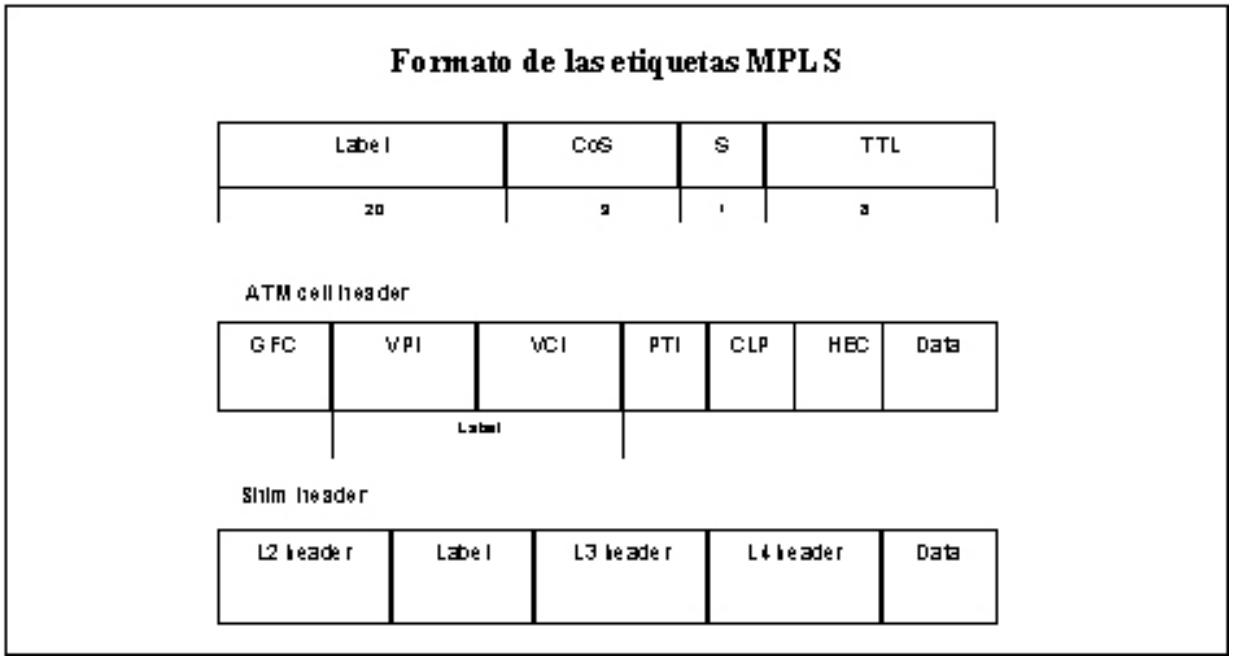


Figura 54 – Formato de etiqueta

El soporte de encabezado shim requiere que el router emisor posea alguna manera de indicarle al router receptor que la trama contiene un encabezado de este tipo. Esto es realizado en diferentes formas de acuerdo a la tecnología de nivel 2:

- El protocolo Ethernet emplea el tipo de trama ethernet 0x8847 para indicar el transporte de paquetes unicast MPLS y el tipo de trama 0x8848 para el transporte de paquetes multicast MPLS.
- El protocolo PPP (Protocolo punto-a-punto) emplea un NCP (Network Control Program) modificado denominado MPLS control plane (MPLSCP) y marca en el campo del protocolo PPP el valor 0x8281 todos aquellos paquetes que contengan encabezado shim.
- El protocolo Frame-Relay emplea el SNAP Network Layer Protocol ID (NLPID) cuyo valor es el 0x8847 y marca el campo SNAP indicando la presencia de tales encabezados.
- El protocolo ATM emplea los valores 0x8847 y 0x8848.
  La Tabla 6 muestra los valores reservados para las etiquetas dentro de un LSR:

Valor de etiqueta	Descripción
0	Etiqueta nula explicita de IPv4. Indica el fondo de la pila, y la extracción de la etiqueta de pila para el envío del paquete basado en el encabezado IP (IPv4).
1	Etiqueta de “alerta al router”. Este valor es permitido en cualquier parte de la pila salvo al fondo de la misma.
2	Etiqueta nula explicita de IPv6. Indica el fondo de la pila, y la extracción de la etiqueta de pila para el envío del paquete basado en el encabezado IP (IPv6).
3	Etiqueta nula implícita. Un nodo MPLS puede asignar y distribuir este valor pero no aparece en el encapsulado. Se emplea para la remoción de etiqueta en el penúltimo salto (penultimote hop popping).
4-15	Reservadas para uso futuro.

Tabla 11 – Valores reservados dentro de etiquetas

La etiqueta MPLS contiene los siguientes campos:

- Campo de etiqueta o label (20 bits): lleva el valor de la etiqueta MPLS.
- Campo de clase de servicios o CoS (3 bits): afecta al algoritmo de encolado y descarte del paquete dentro de la red.
- Campo de pila o snack (1 bit): soporta una pila (snack) jerárquica de etiquetas.
- Tiempo de vida o TTL time-to-live (8 bits): provee funcionalidad convencional de IP TTL.

El bit de apilado o snack implementa el apilado jerárquico de etiquetas MPLS, donde mas de un encabezado de etiqueta puede adosarse a un único paquete. El fondo de la pila es indicado con el bit de snack en 1, mientras que los demás niveles son representados con 0. El envió de paquetes se lleva a cabo empleando los valores de etiquetas de la parte superior de la pila. Los paquetes IP unicast no emplean esta técnica, pero si la utilizan las VPNs MPLS y la ingeniería del tráfico (traffic engineering) para su operación.

El campo TTL es similar al campo TTL transportado por el encabezado IP, y los nodos MPLS solo procesan en campo TTL en la cima de la pila.

La base de etiquetas de envió (LFIB) mantenido por un nodo MPLS consiste de una secuencia de entradas. Como es indicado en la Figura 42, cada entrada consiste de una etiqueta de entrada, y una o más sub-entradas. La base LFIB se encuentra indexada por el valor de las etiquetas entrantes. Cada entrada consiste de una etiqueta de salida, una interface de salida, y la dirección del próximo salto o hop.

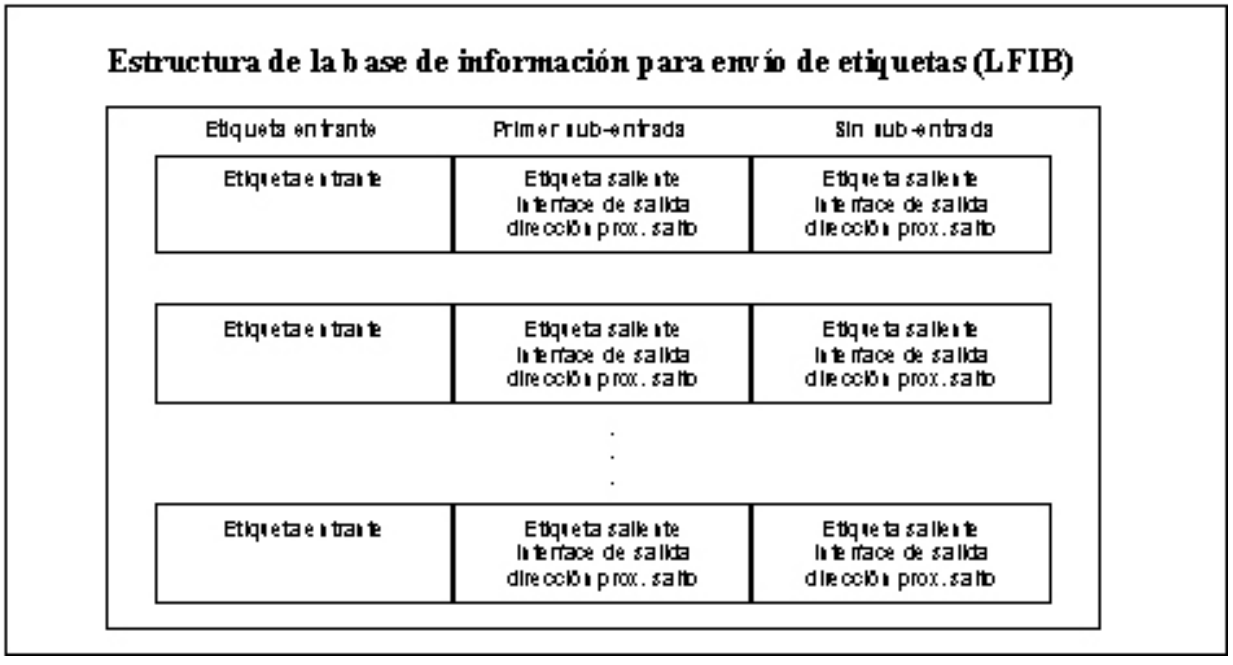


Figura 55 – Estructura LFIB

Un nodo MPLS puede mantener una sola tabla de envió, una tabla de envió por cada interface, o la combinación de ambas. En el caso de múltiples instancias de tabla de envió, el despacho del paquete es manejado por el valor entrante de la etiqueta como así también por la interface por la cual dicho paquete ingreso al nodo.

Los switches de conmutación de etiquetas emplean un algoritmo de despacho basado en el intercambio de etiquetas. Los nodos MPLS que mantienen una sola tabla LFIB extraen el valor del campo de etiqueta encontrado en los paquetes entrantes, y emplean el mismo como índice de la tabla. Luego que un valor de etiqueta sea encontrado en la tabla LFIB, el nodo MPLS remplaza la etiqueta entrante por el valor de etiqueta de salida, y envía el paquete por la interface de salida y hacia el siguiente salto especificado mediante el mismo índice. En caso de que la sub-entrada (para dicho índice) especifique una cola de salida, el nodo MPLS realiza dicha acción (se emplea para QoS).

Un nodo MPLS puede obtener toda la información relevante para el envió de un paquete, como así también determinar las reservas de recursos mediante un solo acceso a memoria (toda la información necesaria se encuentra mediante una sola búsqueda). Esta búsqueda de alta velocidad y la habilidad para el envió de paquetes hacen de la conmutación de etiquetas una tecnología de alta performance de conmutación. MPLS también puede emplearse para el transporte de otros protocolos de capa de red tales como IPv6, IPX, o AppleTalk además de IPv4. Consecuentemente, esta tecnología resulta atractiva para el proceso de migración de IPv4 a IPv6.

El plano de control

El plano de control de MPLS es responsable de la propagación y el mantenimiento de la tabla LFIB. Todos los nodos MPLS sin excepción deben correr algún protocolo IP de intercambio de información de ruteo con los demás nodos MPLS de la red. Los protocolos de estado de enlace o link-state protocolos tales como OSPF o IS-IS son los protocolos elegidos ya que proveen a cada nodo MPLS una vista completa del estado de la red (topología). En los routers convencionales, la tabla de ruteo se utiliza para construir la base de información de envió (FIB: Forwarding Information Base). De todas maneras, en el protocolo MPLS la tabla de ruteo provee información sobre redes de destino y prefijos de sub-redes empleados para la vinculación de etiquetas o label binding. La información para la vinculación de etiquetas puede ser distribuida por medio del protocolo estándar de distribución de etiquetas LDP (Label Distribution Protocol) o solicitando (piggbacking) la información de vinculación mediante protocolos de ruteo modificados para tal fin.

Los protocolos de estado de enlaces OSPF fluyen información de ruteo hacia un conjunto de routers que no se encuentren necesariamente adyacentes, mientras que la información de vinculación de etiquetas es distribuida entre los dispositivos adyacentes, con lo cual, tales protocolos de ruteo no resultan adecuados para la distribución de información de etiquetas. Sin embargo, extensiones de los protocolos de ruteo tales como PIM y BGP pueden emplearse para tal fin, alcanzando una sola consistencia entre la información de ruteo (redes destino) y la distribución de información sobre vinculación de etiquetas. Además, este hecho simplifica la operación de una red MPLS, donde es posible obviar la necesidad de un protocolo separado para la distribución de vinculación de etiquetas.

Como fue mencionado anteriormente, las etiquetas intercambiadas entre nodos MPLS adyacentes se emplea para la construcción de la tabla LFIB. El protocolo MPLS emplea un paradigma e envió basado en el intercambio y reemplazo de etiquetas que puede ser combinado con una gama de módulos de control diferentes, donde cada modulo de control es responsable de la asignación y distribución de información de un grupo de etiquetas, como así también de mantener otro tipo de relevante. Los protocolos de ruteo internos (IGP: Interior Gateway Protocol) se emplean entones para definir los aspectos de alcanzabilidad (conectividad de red con cierto destino), vinculación, y mapeo entre FECs y las direcciones del próximo salto.

Los módulos MPLS de control incluyen:

- Modulo de ruteo unicast (Unicast Routing Module): el modulo de ruto unicast construye la tabla de FECs empleando un protocolo IGP convencional tal como OSPF o IS-IS. La tabla de ruteo se utiliza para el intercambio de etiquetas de vinculación con los nodos adyacentes MPLS para las sub-redes contenidas en dicha tabla de ruteo. Por otro lado, el intercambio de información de vinculación de etiquetas se desarrolla mediante el protocolo LDP.
- Modulo de ruteo multicast (Multicast Routing Module): el modulo de ruteo multicast construye la tabla FECs empleando un protocolo de ruteo multicast tal como PIM (Protocolo-Independent Multicast).
- Modulo de ingeniería del trafico (taffic Engineering): el modulo de ingeniería del trafico permite especificar en forma explicita un determinado camino de conmutación de etiqueta y establecer el mismo a través de la red con propósitos de gestión de trafico existente. La ingeniería de tráfico emplea de-

finiciones de túneles MPLS o extensiones al protocolo de ruteo IGP (OSFP o IS-IS) para construir la tabla de FECs. El intercambio de información de etiquetas se realiza por medio de reserva de recursos (RSVP: Resource Reservation Prototol) o CR-LDP (Constraint-based routing LDP), el cual conforma un conjunto de extensiones del LDP que habilita el ruteo de coacción dentro de una red MPLS.

- Modulo de redes privadas virtuales (Virtual Private Network Module): el modulo de VPN construye la tabla de FECs en base a las tablas de ruteo de cada VPN, las cuales se forman mediante los protocolos de ruteo ejecutados entre el router CPE (en casa de cliente) y el nodo MPLS de borde de la red proveedor de servicios. El intercambio de la información de vinculación e etiquetas perteneciente a la tabla de ruteo de una VPN específica se lleva a cabo por medio del Multiprotocolo BGP extendido (Extended Multiprotocol BGP) dentro de la red del proveedor.
- Modulo de calidad de servicio (Quality of Service Module): el modulo de QoS genera la tabla de FECs empleando un protocolo IGP convencional, tal como OSPF o IS-IS. El intercambio de información de vinculación de etiquetas se realiza de la misma manera que para el ruteo unicast.

Elementos del protocolo MPLS

Los siguientes ítems corresponden a elementos necesarios del protocolo MPLS:

- Router de conmutación de etiquetas (LSR: Label-Switched Router).
- Camino de conmutación de etiquetas (LSP: Label-Switched Path).
- Protocolo de distribución de etiquetas (LDP: Label Distribution Protocol).

Router de conmutación de etiquetas

El router de conmutación de etiquetas (LSR) es un dispositivo que implementa los componentes MPLS de control y envió (forwarding), derivando los paquetes basándose en el valor de la etiqueta contenida en el encapsulado de los mismos. Adicionalmente, los LSR también envían paquetes IP nativos (solo IP, sin etiquetas).

Los LSRs son routers o switches de ATM ambos con soporte MPLS que emplean etiquetas para el envió de trafico. Un punto de suma importancia en la conmutación de etiquetas resulta del hecho que los LSRs se ponen de acuerdo en las etiquetas a usar. Llegan a dicho entendimiento mutuo por medio del empleo de LDP (Label Distribution Protocol) o por extensiones de los protocolos PIM, BPG, RSVP, o CD-LDP.

Los LSR de borde o Edge LSRs se encuentran en los puntos de presencia (POP: Point of Presence) de la frontera de la red MPLS y aplican las etiquetas o pila de etiquetas en los paquetes entrantes al mismo. El proceso de imposición o agregado de etiquetas a los paquetes también es llamo acción de forzar etiquetas (label push action). Los routers LSR de borde al mismo tiempo producen una función de remoción de etiquetas en los puntos de salida del dominio MPLS, que también recibe el nombre de acción de remover etiquetas (label pop action). Además de estas dos ultimas funciones, los LSRs manejan paquetes IP convencionales (IP Plano).

Las diferentes acciones que un LSR puede realizar sobre un paquete etiquetado se enumeran en la Tabla 7:

Acción	Descripción
Agrégate	Remueve la etiqueta del tope de la pila y realiza una búsqueda de Capa 3.
Pop	Remueve la etiqueta del tope de la pila y transmite la carga remanente tanto como un paquete etiquetado o como un paquete IP sin etiqueta.
Push	Reemplaza la etiqueta del tope de la pila por un conjunto de etiquetas.
Swap	Reemplaza la etiqueta del tope de la pila por otra etiqueta.
Untag	Remueve la etiqueta del tope de la pila y envía el paquete IP a la dirección IP del próximo salto especificado.

Tabla 12 – Acciones de un LSR

La tecnología MPLS basada en paquetes emplea el paradigma de envió basado en etiquetas para el transporte de paquetes de capa de red sobre una red compuesta de routers. Esta técnica también es llamada MPLS en modo trama (frame mode MPLS).

La operación básica de la técnica MPLS en modo trama para el ruteo unicast con un solo nivel de etiqueta (snack) se ilustra en la Figura 43. El router LSR1 realiza funciones de router de borde para

conmutación de etiquetas. Este aplica el paquete de etiqueta inicial luego de realizar una búsqueda convencional en la tabla de ruteo basada en el encabezado IP y la correspondiente FEC para el mismo. Los parámetros tales como la interface de ingreso para el caso de una VPN o de un camino predeterminado con ingeniería de tráfico, también pueden determinar una FEC para el paquete. Dicha determinación solo se realiza una vez., en el ingreso de la red.

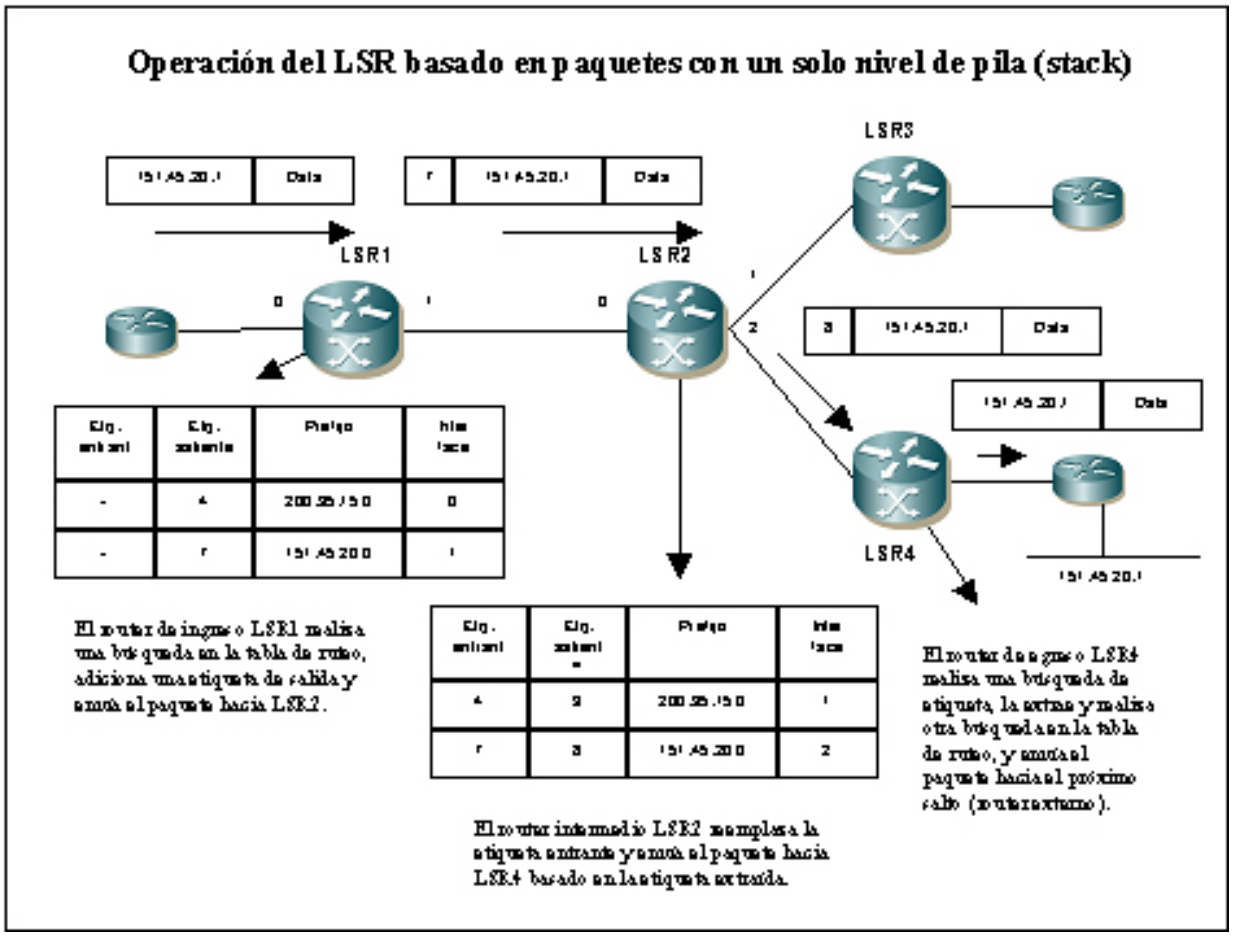


Figura 56 – Operación de un LSR

Cada FEC se mapea con una correspondiente etiqueta. Luego de que el paquete es etiquetado, los subsiguientes routers LSR envían el paquete utilizando solamente dicha etiqueta; cada LSR remplaza la etiqueta de un paquete entrante con un nuevo valor y luego lo despachan. En el egreso, el router LSR4 realiza una búsqueda en la tabla de etiquetas, quita la misma del paquete, realiza una búsqueda en la tabla de ruteo IP y finalmente envía el paquete al router externo.

La técnica anteriormente descripta para la operación de los routers LSR basados en paquetes, posee ciertas deficiencias, ya que LSR4 realiza las mismas operaciones que LSR2 para llegar a la conclusión de que debe solamente realizar una búsqueda en la tabla IP global para enviar en forma correcta el paquete hacia el próximo salto externo. La funcionalidad penultimate hop popping (detallada en la Figura 44) consiste en que el router de borde LSR4 indique a su vecino superior LSR2 la remoción de la etiqueta tope. Esto último se logra mediante el envió en LDP de una etiqueta especial: implicit-null (etiqueta con valor 3). Con lo cual, el LSR2 remueve la etiqueta superior antes de enviar el paquete hacia el router de borde LSR4.

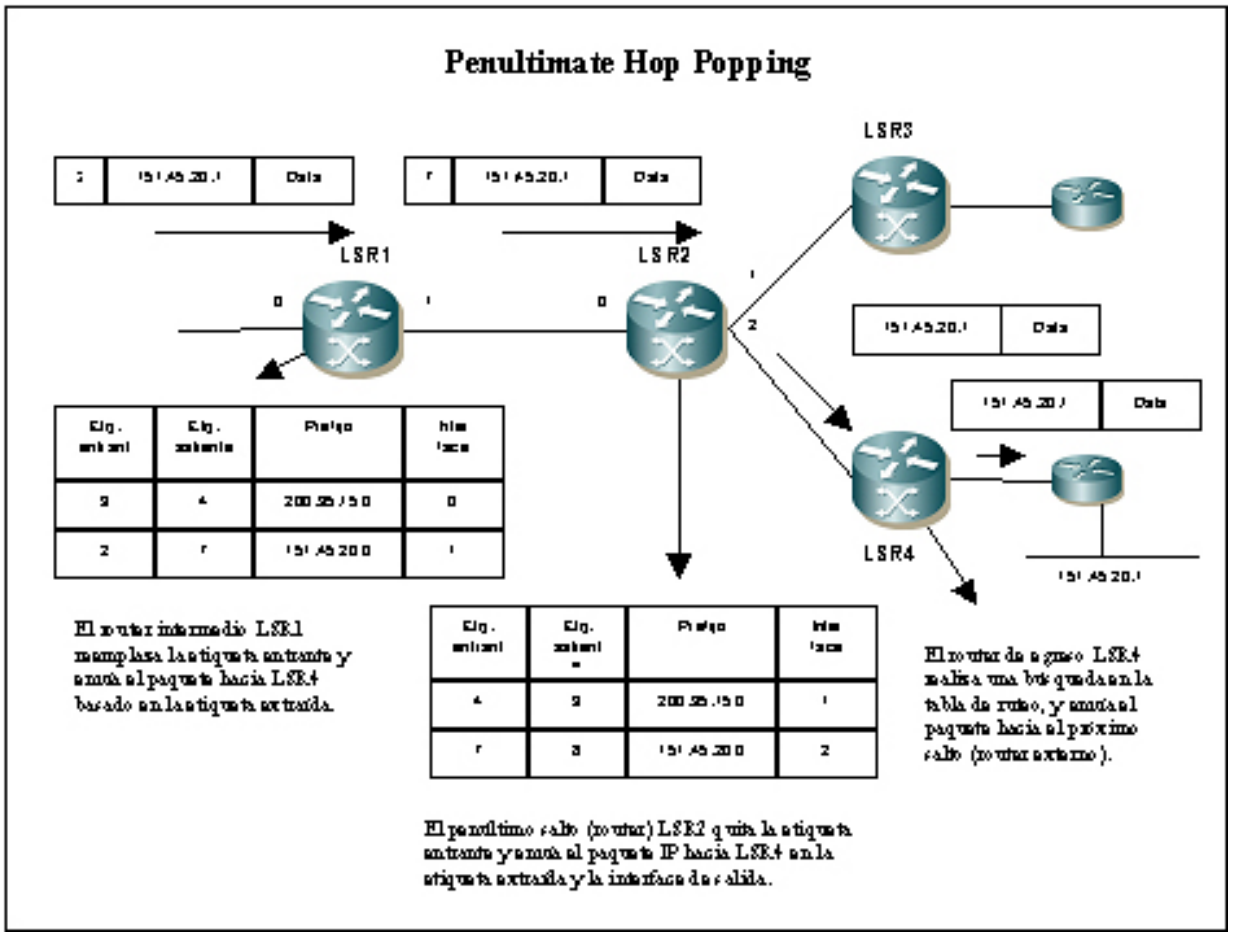


Figura 57 – Acción de PHP

El ambiente ATM MPLS emplea el paradigma de envió basado en etiquetas para transportar paquetes de nivel 3 en celdas ATM a través de una red ATM. Esta técnica también es llamada MPLS en modo celda (cell mode MPLS).

Camino de conmutación de etiquetas

El camino de conmutación de etiquetas o LSP (Label-switched Path) es una conexión configurada entre dos LSRs que emplean la técnica de conmutación de etiquetas para el envió de paquetes. Un LSP es un camino de trafico especifico a través de una red MPLS. Los LDPs pueden aprovisionarse a través de LDP, RSVP-TE (Resource Reservation Protocol with Traffic Engineering), CR-LDP (Constraint-based Router Protocol), o extensiones de los protocolos de ruteo tales como Multiprotocolo BGP (Multiprocol Border Gateway Protocol).

Un LSP puede ser considerado como el camino a través de un conjunto de dispositivos LSR que los paquetes pertenecientes a una FEC toman para alcanzar su destino.

MPLS permite una jerarquía de niveles de etiquetas conocido como pila de etiquetas o label stack, por lo tanto, es posible determinar para un paquete diferente LSPs en distintos niveles de etiquetas para que alcance su destino. Al mismo tiempo, los LSPs son unidireccionales, esto significa que la respuesta de un paquete puede tomar un camino de vuelta distinto al camino de ida.

En la Figura 46, el LSR1 y 4 son routers LSR de borde, mientras LSR 2 y LSR3 son routers LSR de core. Para construir un LSP, los LSRs hacen uso de los protocolos de tuteo y de las rutas aprendidas de los mismos.

El establecimiento del LSP puede realizarse por medio de una de estas formas:

- Control Independiente (Independent control)
- Control Ordenado (Ordered control)

En una misma red pueden convivir estos dos métodos de control para el establecimiento de LSPs sin que ocurra ningún inconveniente. El control independiente provee convergencia y establecimiento de

LSPs en forma mas rápida, mientras que el control ordenado provee capacidades para la prevención de lazos cerrados (Loops).

El la Figura 46, se detalla paso a paso el establecimiento de LSP con control independiente:

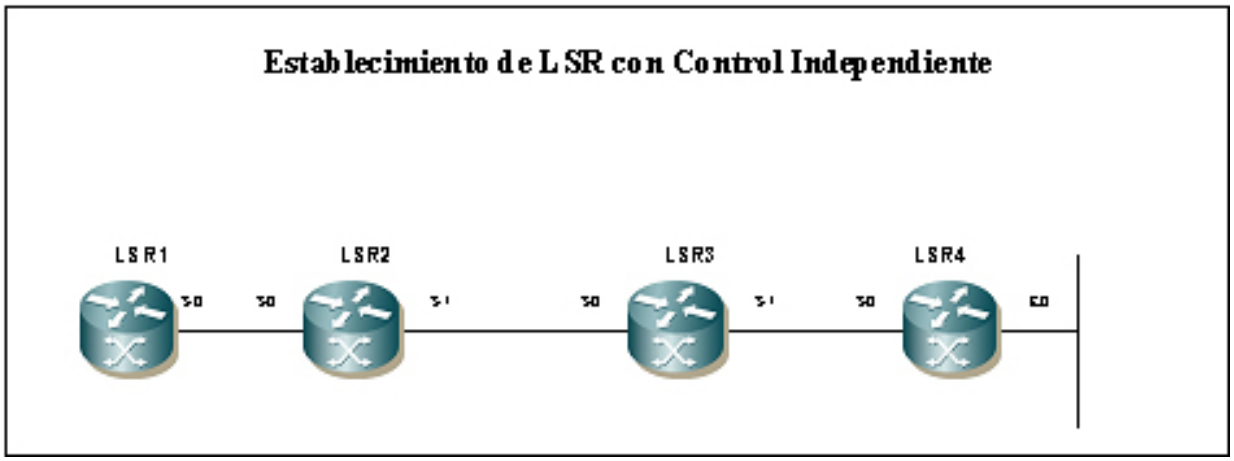


Figura 58 – Control independiente (LSR)

- Paso1: El dispositivo LSR1 determina a través del protocolo unicast de ruteo, como por ejemplo OSPF, que LSR2 es el próximo salto para la FEC asociada al prefijo 172.16.0.0/16. LSR1 entonces, arbitrariamente selecciona una etiqueta libre de su rango empleando la tabla LIB, y supongamos que el valor es 50; automáticamente dicho valor es utilizado como índice (etiqueta entrante o incoming label) para la entrada FEC 172.16.0.0/16, y el próximo salto resulta LSR2, y el campo next hop a LSR2, y el campo de interface de salida a S0. En este punto todavía no ha sido solicitada la etiqueta de salida para la FEC en cuestión (172.16.0.0/16). LSR1 envía entonces su información de vinculación de etiquetas local a LSR2. Este ultimo al recibir la información de LSR1, no puede actualizar su tabla para la FEC 172.16.0.0/16 porque LSR1 no es su próximo salto para dicho prefijo, en cambio, LSR1 si actualiza su tabla para la FEC correspondiente porque LSR2 lo es.
- Paso 2: El dispositivo LSR2 determina que LSR3 es su próximo salto para la FEC, y arbitrariamente elige del rango libre el valor de etiqueta 25; automáticamente dicho valor es utilizado como índice (etiqueta entrante o incoming label) para la entrada FEC 172.16.0.0/16, y el próximo salto LRS3, es decir, dentro de la LFIB existente un registro donde el campo FEC es 172.16.0.0/16, el campo etiqueta de entrada posee el valor 25, en el campo next hop a LSR3, y el campo interface de salida a S1. LSR2 envía entonces su información de vinculación a LSR1 y a LSR3.

- Paso 3: Al recibir LSR3 dicha tabla, reconoce que la FEC 172.16.0.0/16 tiene como próximo salto a LSR4, con lo cual toma un valor arbitrario de etiqueta, y asumamos que es el 45; automáticamente dicho valor es utilizado como índice para la entrada FEC 172.16.0.0/16; y el próximo salto resulta LSR4, es decir dentro de la LFIB existe un registro donde el campo FEC es 172.16.0.0/16, el campo de etiqueta de entrada posee el valor 45, el next hop a LSR4, y el campo de interface de salida es S1. LSR3 envía entonces su infamación a LSR2 y a LSR4.
- Paso 4: Cuando el dispositivo LSR4 envía su tabla local de información de vinculación a LSR3, este emplea la información que recibe para la vinculación de la etiqueta de salida para la FEC 172.16.0.0/16. Asumamos que el valor elegido por LSR4 es 33, entonces LSR3 actualiza su tabla LFIB para la entrada FEC 172.16.0.0/16, colocando para dicho registro el valor 33 en el campo etiqueta de salida. LSR4 no necesita una etiqueta de salida para la FEC 172.16.0.0/16, ya que el mismo es LSR de borde para la FEC (la misma se encuentra directamente conectada), con lo cual solo salen paquetes IP y deberá realizar una quita de etiqueta de los paquetes MPLS entrantes desde la red destinados a dicha FEC.

A este punto, como se muestra en la Tabla 8, todos los LSRs involucrados poseen sus tabla LFIB completas para la FEC 172.16.0.0/16, y se encuentran listos para enviar paquetes (hacia dicha red, es decir, solo el camino de ida desde una red X hacia el destino 172.16.0.0/16).

Cuando LSR1 reciba un paquete con etiqueta 50, empleará este valor como índice en su tabla LFIB para la acción a tomar. Cuando encuentre la entrada correspondiente, remplazara dicha etiqueta por el valor 25 y enviará el paquete por la interface S0 hacia LSR2. El dispositivo LSR2 realizara una búsqueda similar en su LFIB, reemplazara dicha etiqueta por el valor 45 y enviar el paquete hacia LSR3 por la

interface S1. LSR3 al recibir el paquete con la etiqueta 45 y realizará la búsqueda en la LFIB, remplazará el mismo por el valor 33 y lo enviará hacia LSR4 por la interface S1. Finalmente, LSR4 leerá la etiqueta entrante 33 y extraerá la misma del paquete, realizara una búsqueda en su Tabla LFIB o en su tabla de ruteo (en el caso de implementar penultimote hop popping) y determinara enviar el paquete IP por la interface E0 hacia su destino final.

	Etiqueta entrante	Etiqueta saliente	Próximo salto	Interface saliente
LSR1	50	25	LSR2	S0
LSR2	25	45	LSR3	S1
LSR3	45	33	LSR4	S1
LSR4	33	-----	LSR4	E0

Tabla 13 – Tabla LFIB

El Control ordenado por su parte para el establecimiento de LSPs: los LSRs de ingreso y egreso inician el establecimiento del LSP, y la asignación de etiquetas sucede en forma mas ordenada. La solicitud de etiquetas puede comenzar desde cualquier extremo, tanto desde un LSR de ingreso como de egreso. El establecimiento ordenado requiere que la propagación de sus vinculaciones de etiquetas se realice antes del establecimiento del LSP, con lo cual converge en mayor tiempo que el modo de control independiente. De todas maneras, este método proporciona mejores capacidades de prevención de lazos cerrados (loops). Este método resulta el indicado en el empleo de redes MPLS basadas en circuitos ATM (ATM MPLS).

Protocolo de distribución de etiquetas

El protocolo de distribución de etiquetas (LDP: Label Distribution Protocol) se emplea conjuntamente con los protocolos estándares de ruteo a fin de distribuir la infamación d vinculación de etiquetas entre los dispositivos LSR en una red de conmutación de paquetes. LDP permite a los LSRs distribuir etiquetas a sus vecinos LDP empleando el protocolo TCP y su puerto numero 646. El empleo del protocolo TCP provee de reparto confiable de la información LDP con control de flujo robusto y mecanismos de congestión.

Cuando un dispositivo LSR asigna a una etiqueta a una FEC, necesita que sus vecinos conozcan dicha información, además de su significado, para lo cual se emplea LDP. Un conjunto de etiquetas define un LDP dentro de un dominio MPLS desde el LSR de ingreso hacia el LSR de egreso, donde las mismas corresponden a mapas de redes y caminos. LDP entonces, facilita el establecimiento del LSP proporcionando un conjunto de procedimientos para la distribución de etiquetas entre LSRs vecinos. Consecuentemente, el protocolo LDP provee un mecanismo para distribuir LSRs vecinos y establecer la comunicación:

- Discovery: los mensajes de descubrimiento corren sobre UDP y emplean paquetes *hello multicast* para aprender de otros LSRs con conexión directa. Luego se establece una sesión bidireccional TCP para LDP.
- Adjacency: los mensajes de adyacencia corren sobre TCP y proveen inicialización de sesión LDP mediante el mensaje INICIALIZATION y el modo de distribución. La información intercambiada durante la sesión incluye modo de asignación de etiquetas, temporizadores de actividad, etc. Los mensajes de *keepalive* se envían entre vecinos con periodicidad.
- Label Advertisement: los mensajes de publicación de etiquetas proveen la información de vinculación de etiquetas (Label mapping Label withdrawal y Label release).
- Notification: los mensajes de notificación proveen información de aviso y error entre los dispositivos LSRs.

La distribución y asignación de etiquetas por medio de LDP puede realizarse de los siguientes modos:

- Downstream-on-demand: cuando los LSRs de MPLS solicitan explícitamente una etiqueta de vinculación al próximo salto (LSR) de una FEC particular. Se emplean mensajes tales como Label request y Label requets abort. Este método es indicado para redes ATM MPLS.
- Unsolicited Downstream: se produce por la distribución de información de vinculación aunque no se haya solicitado explícitamente una etiqueta de vinculación al próximo salto (LSR) de una FEC particular. Dicho modo es especialmente indicado para redes MPLS basadas en paquetes.
- Liberation Label Retention: cuando los LSRs de MPLS mantienen información de distribución provenientes de LSRs que no son el próximo salto (LSR) para una FEC particular. El LSR puede mantenerlo

o descartar la información, en el primer caso, permite la rápida convergencia de la red en caso de falla de una troncal. El método es indicado para redes MPLS basadas en paquetes.

- Conservative Label Retention: cuando los LSRs de MPLS descartan información de distribución proveniente de LSRs que no son el próximos salto (LSR) para una FEC particular. Este método es indicado para redes ATM MPLS.

Calidad de servicio en redes MPLS

La calidad de servicio (Qos)

Internet esta cambiando aspectos de nuestros vivir del día a día, incluyendo la forma de trabajar, estudiar comunicarse y hasta divertirse. El mayor factor del éxito de Internet es su accesibilidad universal, fácil empleo y la convivencia practica de las tecnologías basadas en aplicaciones Web. Al mismo tiempo, Internet es empleada para la utilización de aplicaciones variadas que requieren estrictos recursos. Como ejemplo de las aplicaciones en cuanto a términos de ancho de banda y otros recursos, se encuentran: Voz sobre IP (VoIP), videoconferencia en tiempo real, video de ráfaga, educación a distancia, transacciones financieras seguras, aplicaciones comerciales B2B (business-to-business), etc. Cada una de estas aplicaciones a su vez, poseen necesidades variadas en cuanto a retardo (delay), variación de retardo (jitter), ancho de banda (bandwidth), perdida de paquetes (packet loss), y disponibilidad (availability). Todos estos parámetros forman la base de la calidad de servicio (QoS: Quality of Service). Las redes IP deben ser diseñadas para proveer la calidad de servicio requeridas por estas aplicaciones.

Varios proveedores ofrecen servicios de privilegio definidos por medio de acuerdos de nivel de servicio (SLA: Service Level Agreement) para priorizar trafico de ciertos clientes o aplicaciones. La calidad de servicio (QoS) aplicadas en redes IP provee de inteligencia suficiente a los dispositivos para manejar trafico preferentemente de acuerdo al SLA y aseguran una política en la red. La calidad de servicio (QoS) se define como aquellos mecanismos que permiten a los operadores de red controlar la mezcla de tráfico, el retardo, la desviación de retardo y la perdida de paquetes dentro de la red. La calidad de servicio (QoS) no es una funcionalidad dentro de un dispositivo, sino que es una arquitectura de extremo a extremo. Las capacidades de IP QoS permiten a los proveedores priorizar clases de servicio, alojar ancho de banda, y evitar congestiones.

Los proveedores que ofrecen servicios IP sobre un backbone MPLS deberán soportar IP QoS dentro de su infraestructura de red. Esto significa que deberán soportar IP QoS sobre MPLS.

La agrupación IETF ha definido dos modelos para la implementación de IP QoS: Servicios Integrados o IntServ (Integrated Servicies) y Servicios Diferenciados o DiffServ (Differentiated Servicies). IntServ sigue el modelo QoS señalizado, en el cual el anfitrión final señaliza (informa) la red con la calidad de servicio requerida reservando ancho de banda y recursos de dispositivos. Por otro lado, DiffServ funciona en el modelo de QoS provisionada, en donde los elementos de red se configuran para dar servicio a múltiples clases de trafico con diversos requerimientos de QoS.

Servicios Integrados

Los servicios integrados o IntServ proveen: una solución de QoS en todo el recorrido por medio de señalización extremo a extremo, un mantenimiento de estado (para cada flujo y reserva RSVP), y un control de admisión para cada elemento de red. El modelo IntServ especifica un numero de clases de servicio diseñadas para cubrir las necesidades de diferentes tipos de aplicaciones, y varios protocolos de señalización; el protocolo RSVP corresponde a uno de ellos, y es empleado para realizar solicitudes de QoS para clase de servicios.

IntServ ha definido una especificación para el trafico denominada Tspec, la cual clasifica el tipo de trafico de la aplicación que ingresa a la red. Este modelo requiere que cada router o switch en la red realice funciones tales como políticas de tráfico y verificación del mismo, observando que cumpla su Tspec, y en caso de no cumplir dicho valor, descarte los paquetes fuera de acuerdo.

IntServ ha definido una especificación de reserva denominada ASPEC, la cual determina niveles de QoS y la reserva de recursos en la red. Este modelo requiere que cada router o switch realice funciones tales como control de admisión, que verifiquen si existen suficientes recursos para cubrir la solicitud de QoS, y en caso de que los recursos sean escasos, la solicitud será denegada.

IntServ también precisa que los elementos de red realicen clasificación de paquetes que requieran niveles específicos de QoS, como también encolado y mecanismos de propagación.

Clases de IntServ

El modelo IntServ define dos clases de servicio: servicio garantizado (guaranteed service) y carga controlada (controlled load) que pueden ser solicitados vía RSVP (asumiendo que todos los dispositivos

de la red soportan RSVP en el camino entre el origen y el destino).

La clase de servicio garantizada (guaranteed service) provee límites rígidos de retardo extremo a extremo, y asegura ancho de banda para tráfico que conforme las especificaciones reservadas.

La clase de control de carga (controlled load) provee un nivel superior de "mejor esfuerzo" (en el ruteo sin QoS se emplea por defecto el "mejor esfuerzo" o best effort), y servicio de bajo retardo para redes moderadamente cargadas.

RSVP

RSVP es el protocolo de señalización del modelo IntServ que permite que las aplicaciones notifiquen sus requerimientos de QoS hacia la red. La red posteriormente, confirma la solicitud de QoS mediante una respuesta satisfactoria o fallida. El protocolo RSVP transporta información de clasificación incluyendo la dirección IP fuente y destino y los puertos UDP, para de esta manera los flujos con requerimientos particulares de QoS puedan ser identificados y reconocidos en la red. RSVP también lleva los parámetros Tspec y Rspec, además de información sobre la clase de servicio deseada, y la misma debe ser transportada a través de cada uno de los elementos involucrados en el camino entre el emisor y el receptor.

Como se detalla en la Figura 47, RSVP transporta su información empleando dos tipos de mensajes: PATH (camino) y RESV (reserva). Los mensajes PATH desde el emisor hacia uno o más receptores (en el caso de Multicast con RSVP) incluyen el parámetro Tspec y la clasificación de la información provista por el emisor. Cuado el receptor recibe el mensaje PATH, envía de vuelta un mensaje RESV hacia el emisor, identificando la sesión por la cual fue hecha la reserva. Incluye además, el parámetro Rspec indicando el nivel de calidad de servicio QoS requerida por el receptor.

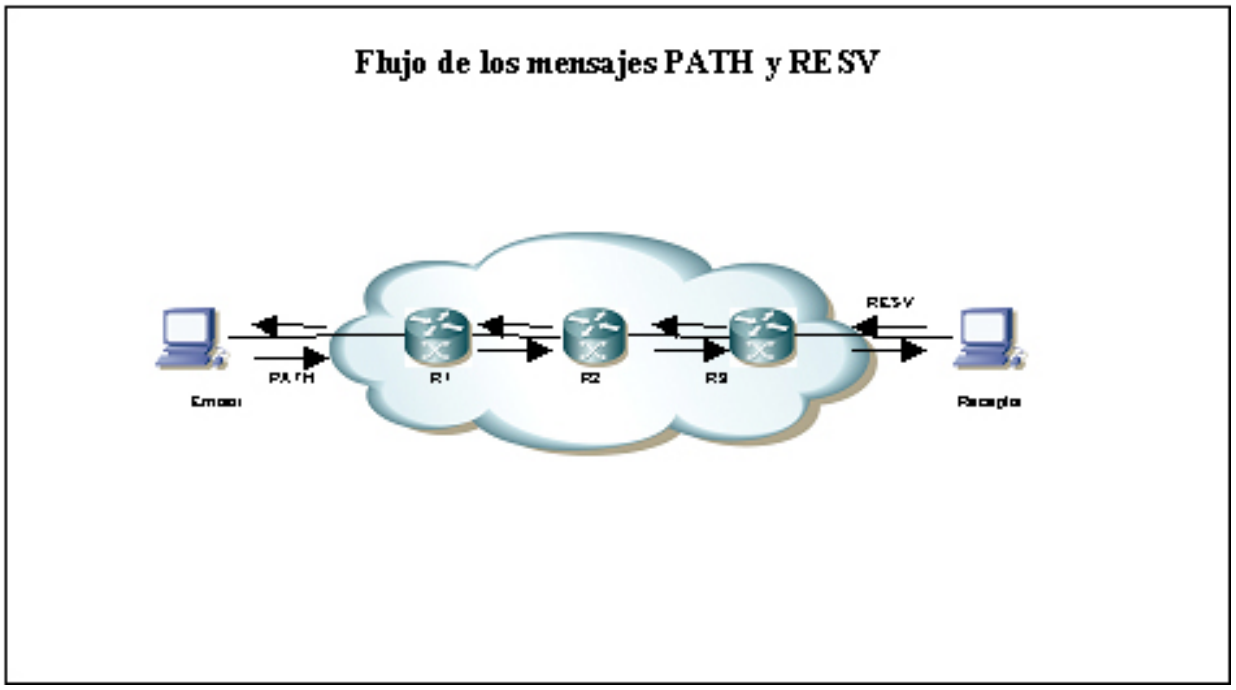


Figura 59 – PATH y RESV

La reserva RSVP es solamente unidireccional, y en el caso de necesitar que la misma sea bidireccional, resultará necesario el envío por parte del receptor de dos mensajes adicionales de PATH y RESV.

Cuando una reserva es establecida, los routers a lo largo del camino pueden identificar los paquetes que pertenezcan a la reserva misma por medio de la inspección de hasta cinco campos en el encabezado de los protocolos IP y transporte: dirección IP origen y destino, puerto origen y destino, y numero de protocolo. El conjunto de paquetes identificados de esta manera recibe el nombre de flujo reservado o reserved flow. Los paquetes pertenecen a un flujo reservado son siempre medidos y adaptados para asegurar que el flujo no se encuentre generando mayor trafico que el publicado por el parámetro Tspec. Al mismo tiempo, dichos paquetes son encolados y programados para cumplir la calidad de servicio (QoS) deseada.

Esta solución parece a simple vista falta de escalabilidad ya que podrían existir millares de flujos reservados en toda la red, sin embargo, el protocolo RSVP puede realizar reservas para trafico agregado, formando la base de la implementación en redes MPLS, donde un paquete perteneciente a un flujo reservado puede ser definido como perteneciente a una FEC.

Implementación de IntServ en redes MPLS

En LSRs con MPLS puede habilitarse la posibilidad de asociar etiquetas con flujos que posean reservas de RSVP. Los paquetes para los cuales fue hecha una reserva RSVP pueden ser considerados como una FEC, y la vinculación entre etiquetas y flujos RSVP puede ser distribuida a los restantes LSRs mediante el empleo de LDP. Como se muestra en la Figura 48, al momento de recepción de un mensaje RSP PATH, el receptor responde con un mensaje RSVP RESV. El dispositivo LSR3 recibe dicho mensaje, aloja una etiqueta del rango libre, y envía hacia LSR2 un mensaje RESV con el valor de etiqueta 7 (además asigna en su LFIB una entrada con el valor 7 como etiqueta entrante). LSR2 crea a su vez una entrada en su LFIB con el valor 7 como etiqueta saliente, aloja la etiqueta 3 como entrante en la LFIB, y envía un mensaje RSVP con la misma hacia LSR1. A medida que el mensaje RESV se despliega hacia el emisor, un LSP se establece a lo largo del camino, y consecuentemente cada LSR podrá asociar recursos de QoS con dicho LSP.

En el modo de operación, cuando LSR2 reciba un paquete proveniente de LSR1 con valor de etiqueta 3, reconocerá al buscar la etiqueta dentro de la LFIB todos los mecanismos de QoS asociados con el paquete, tales como adaptación y encolado. Resulta por lo tanto, innecesario examinar dentro de la red MPLS los encabezados IP y el transporte del paquete.

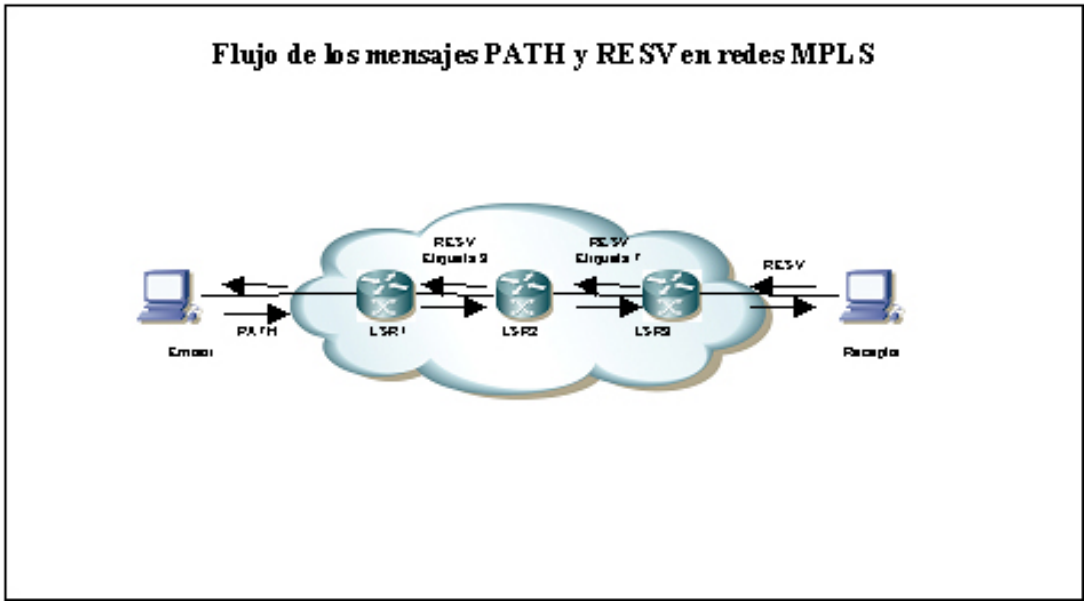


Figura 60 – PATH y RESV en MPLS

Prioridad IP

El método de flujo de RSVP en IntServ para la implementación de QoS muestra claramente su falla de escalabilidad y lleva a una complejidad de implementación. La prioridad IP o también llamada precedencia (IP precedente) definida por el grupo IETF ha simplificado el método de IP QoS adoptando un modelo de agregación para flujos por medio de la clasificación de los mismos dentro de clases.

Los paquetes son clasificados en el borde de la red en una de las ocho diferentes clases. Esto se logra mediante el correspondiente leteo de los tres bits de prioridad (precedente) en el campo ToS (Tipo de Servicio) del encabezado IP. La Tabla 9 muestra las ocho categorías o niveles de prioridad para el ToS.

Valor de ToS	Nombre
0	Rutina
1	Prioridad
2	Inmediato
3	Flash
4	Flash override
5	Critico
6	Control de Internet
7	Control de Red

Tabla 14 – Prioridad IP

Tan rápido como un paquete sea marcado con prioridad IP apropiada, cualquier nodo en la red a lo largo del camino, conoce los niveles relativos de priorización y puede aplicar un mecanismo selectivo y preferencial de envió para paquetes de alta prioridad. El esquema de prioridad IP permite solo la determinación de la prioridad relativa entre paquetes, y no provee diferentes especificaciones de descarte para paquetes dentro de un mismo nivel. En caso de congestión de la red, los paquetes con prioridad mas baja son descartados en pos de los paquetes con mayor prioridad.

Servicios Diferenciados

El modelo de Servicios Diferenciados (DIffServ) divide el tráfico en un pequeño número de clases y aloja recursos en función de las mismas. Este modelo es similar al modelo de prioridad IP. En DiffSer se emplea un código de 6 bits o DSCP (differentiated services code point) para marcar la clase del paquete en el encabezado IP. Existen 64 clases diferentes, aunque en la práctica son implementadas solo algunas de ellas. La Tabla 10 muestra el mapeo de la prioridad IP en clases fijas DSCP. Las RFCs 2474 y 2475 definen la arquitectura y el uso general de los bits del campo DiffServ (las mismas reemplazan a la RFC 1349 para la definición de IPv4 ToS).

Prioridad IP	¨DSCP
0	DSCP 0
1	DSCP 1
2	DSCP 2
3	DSCP 3
4	DSCP4
5	DSCP 5
6	DSCP 6
7	DSCP 7

Tabla 15 – Servicio diferenciado

Comportamiento por salto (PHB)

Los elementos de la red o saltos (hops), a lo largo del camino examinan el valor del campo DSCP y determinan el nivel de QoS requerido para el paquete. Esto se conoce como el comportamiento por salto (PHB: Per Hop Behavior). Cada elemento de red posee una tabla que mapea el valor del DSCP encontrado en el paquete con el comportamiento de este salto, que posteriormente determinará como el paquete será tratado. Los DSCP son valores transportados en los paquetes, mientras que los PHB son comportamientos bien específicos a aplicar a los paquetes. Al día de hoy, existen disponibles cuatro implementaciones PHB estándares en DiffServ:

- Default PHB: provoca la entrega mediante el tradicional servicio “mejor esfuerzo” (best effort) para paquetes IP.
- Class-selector PHB: provoca el mismo comportamiento de envío de paquetes que los nodos que implementan clasificación y envío por prioridad IP.
- Expedited Forwarding (EF) PHB: provoca el envío inmediato con bajo retardo, baja pérdida de paquetes, bajo jitter, y con ancho de banda garantizado. Los paquetes marcados con EF son priorizados para la entrega por sobre otros.
- Assured Forwarding (AF) PHB: los paquetes marcados con AF especifican una clase AF y una preferencia de descarte para paquetes IP.

Implementación de DiffServ en redes MPLS

Los LSRs MPLS no examinan los contenidos de los encabezados IP y el calor del campo DSCP como requiere DiffServ. Esto significa que el apropiado PHB dentro del dominio MPLS debe determinarse por medio de la etiqueta. El encabezado shim del paquete MPLS posee un campo de tres bits llamado Exp (experimental) o CoS. Dicho campo soporta ocho valores diferentes y es empleado en MPLS para soporte de hasta ocho clases de DiffServ.

Como se indica en la Figura 49, los bits de prioridad IP o los primeros tres bits del campo DSCP son copiados en el campo Exp del encabezado MPLS en el borde de la red. Cada LSR a lo largo del LSP mapea los bits Exp en un PHB. Los LSPs creados de esta manera son conocidos como E-LSP o Exp-LSP, y pueden soportar hasta ocho PHB por LSP.

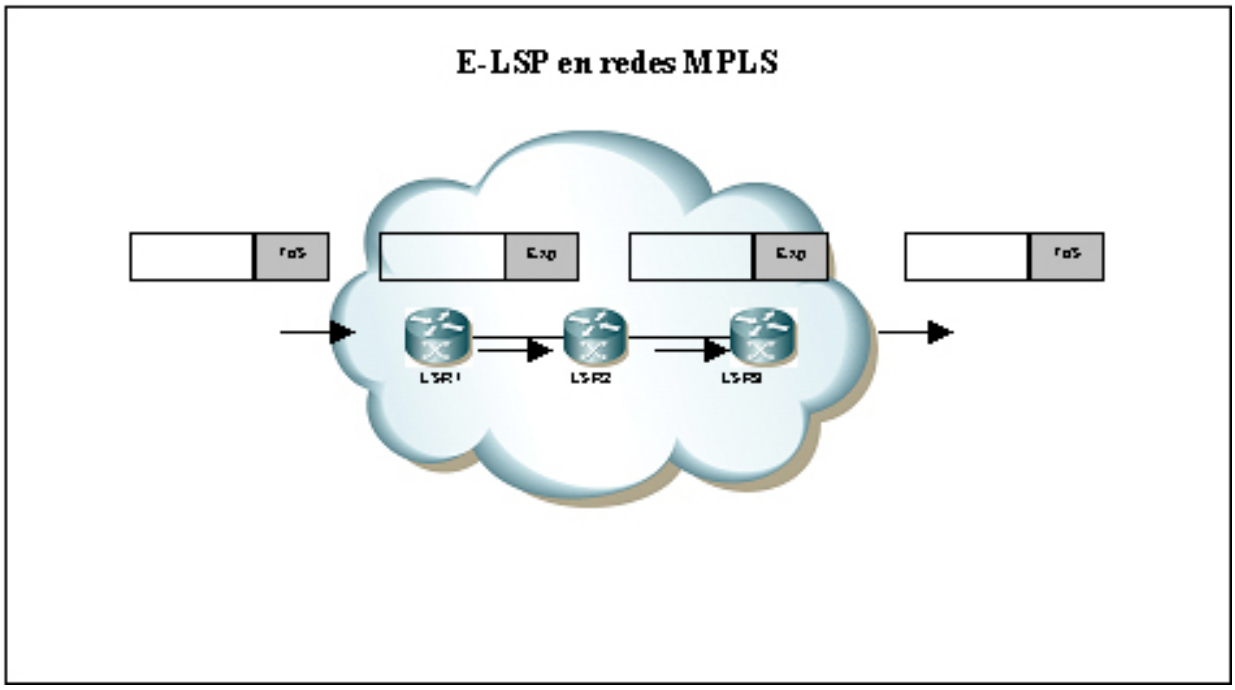


Figura 61 – E-LSP en MPLS

Soporte de QoS en VPNs MPLS

Una VPN es definida como un grupo cerrado de usuarios que comparten una infraestructura de red publica que posee un conjunto de políticas administrativas que controlan la conectividad y la QoS entre los sitios. Las variadas clases de servicios (CoS) para redes MPLS con QoS deberán poder aplicarse dentro de una VPN, como por ejemplo, aplicaciones en tiempo real como VoIP deben recibir un trato preferencial de CoS frente a una transferencia de archivo (ftp).

Modelo de QoS de conexión para VPNs MPLS

En el modelo de conexión (pipe model), el proveedor de servicios aprovisiona dentro de la VPN al cliente con ciertas garantías de QoS para el flujo de trafico entre un CPE (o CE) y otro.

Este modelo puede ser representado como una conexión en dos routers CPEs. Cualquier tráfico que ingrese en dicha conexión obtendrá ciertas garantías de QoS, tales como minino ancho de banda garantizado entre CPEs (o CEs). El modelo QoS de conexión para redes MPLS es similar al modelo de calidad de servicio que los clientes están acostumbrados en VPNs con ATM o Frame-Relay. Sin embargo, las conexiones en ATM y Frame-Relay son bidireccionales, mientras que el modelo de las VPNs MPLS las conexiones son unidireccionales. La naturaleza unidireccional del modelo de conexión permite patrones de tráfico asimétricos facilitando diferentes tasas de tráfico en cada dirección entre CPEs (o CEs).

Como se detalla en la Figura 50, el proveedor de servicios aprovisiona la VPN1 con una conexión que garantiza 30Mbps para el trafico entre el sitio 1 y el sitio 3, una segunda conexión garantiza 10Mbps de tráfico entre el sitio 1 y el sitio 2, y una tercera conexión garantizada de 45Mbps de trafico entre el sitio 3 y el sitio 2.

Por otro lado, la VPN2 posee conexiones simétricas para un tráfico garantizado de 20 Mbps entre el sitio 1 y el sitio 2, y viceversa. Este ejemplo muestra que es posible originar o terminar más de una conexión en un mismo CPE (o CE).

Para lograr una correcta implementación del modelo de conexión el cliente debe poseer una buena idea del modelo de trafico (o mapa de trafico), y debe realizar un análisis del trafico de red para el apropiado planeamiento de capacidad. El modelo de conexión se asemeja al modelo IntServ para QoS y puede proveer garantías estrictas.

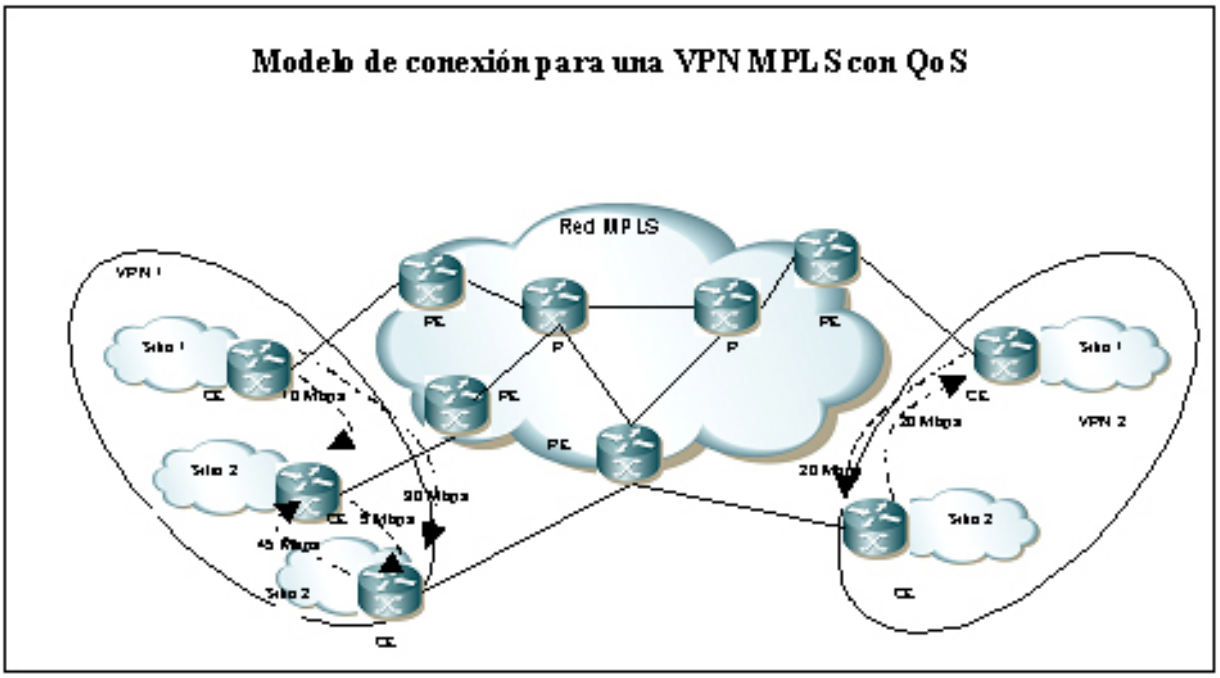


Figura 62 – Modelo QoS sobre MPLS

En el modelo de conexión los LSPs se originan y terminan en los routers PE y proveen ancho de banda garantizado para todas las conexiones CPE (o CE). Dentro del modelo. El mecanismo de LSP para ancho de banda garantizado mejora la escalabilidad de la calidad de servicio (QoS) en las VPNs MPLS, ya que los proveedores de servicios no necesitan configurar conexiones entre CPEs para cada par particular de sitios del cliente (solo son configuradas en los routers PE).

Diccionario

- **ATM**. Asynchronous Tranfer Mode (modos de transferencia asincrónica). Tipo de red de conmutación de celdas.
- **Backbone**. Centro de una red. El núcleo de una red.
- **Carriers**. Operador que brinda servicios de transporte sobre redes de comunicaciones.
- **Core**. Centro de una red. El núcleo de una red.
- **CoS**. Class of Service (clase de servicio). Permite clasificar usuarios o grupos de usuarios.
- **CPE**. (equipo de borde del proveedor en casa de cliente).
- **Datacenter**. Centro de datos. Agrupación de equipos que brindan servicios de Internet.
- **Delay**. Retardo.
- **DLCI**. Data-Link Connection Identifier (identificador de conexión de link de datos).
- **Draft**. Documento borrador con intenciones de documento estándar.
- **Extranet**. Red compartida entre una empresa, sus proveedores y sus clientes.
- **Frame-Relay**. Tipo de red de conmutación de paquetes.
- **Intranet**. Red interna.
- **IP**. Internet Protocol (protocolo de internet).
- **IPSec**. Internet Protocol Security (protocolo de seguridad en internet).
- **IPv4**. Internet Protocol versión 4.
- **ISPs**. Internet Service Provider (proveedor de servicios de Internet).
- **Jitter**. Variación de retardo.
- **Label**. Etiqueta.
- **LDP**. Label Distribution Protocol (protocolo de distribución de etiquetas).
- **LSP**. Label-Switched Path (camino de conmutación de etiquetas).
- **LSR**. Label Switch Router (router de conmutación de étiquetas). Idem P router.
- **MPLS**. Multi-Protocol Label Switching (protocolo múltiple de conmutación de etiquetas).
- **NGN**. Next Generation Network (redes de próxima generación). Unificación de las redes de tradicionales de datos y voz.

- **P**. Provider (equipo de core del proveedor)
- **PE**. Provider Edge (equipo de borde del proveedor).
- **POP**. Point of Presence (punto de presencia de un Carrier).
- **PSTN**. Public Switched Telephone Network (red pública conmutada de telefonía).
- **PVC**. Permanent Virtual Circuit (circuito virtual permanente).
- **QoS**. Quality of Service (calidad de servicio). Priorización de tráfico según prioridades.
- **RD**. Route Distinguisher (identificador de VRF).
- **RFC**.
- **Router**. Equipo encargado de tomar decisiones de ruteo de paquetes.
- **SLA**. Service Level Agreement (servicio de nivel agregado).
- **Trunking**. Servicio de transporte de voz sobre una red IP.
- **VPN**. Virtual Private Network (red privada virtual).
- **VRF**. Virtual Router Forwarding (instancia de ruteo virtual). Permite generar diferentes instancias de ruteo virtuales sobre un único router.

Bibliografía/Fuentes de Información

Advanced MPLS Design and Implementation.
Cisco Press, 2002.Viveck, Alwayn.

MPLS and VPN architecture.
Cisco Press, 2001. Jivan, Pepelnjak, Jim Guichard.

MPLS Technology and Applications.
Bruce Davie, Yakov Rekhter; Morgan Kaufmann Publishers

MPLS - Multiprotocol Label Switching Architecture. E. Rosen, A. Viswanathan y R. Callon, Enero 2001

www.mplsrc.com
www.iec.org/online/tutorial/mpls/
www.ieee.org
www.mplsforum.org
www.cisco.com
www.ietf.org/html.charters/mpls-charter.html

RFC-2547: BGP/MPLS VPNs
RFC-2917: A core MPLS IP VPN Architecture
RFC-3031: MPLS Architecture
RFC-3036: LDP Specification
RFC-3270: MPLS Support of Differentiated Services