Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

ESTUDIO DE LAS VENTAJAS E IMPLEMENTACIÓN DE SERVICIOS IP VPN, SOBRE UNA INFRAESTRUCTURA MPLS, EN LA REGIÓN CENTROAMERICANA

Kelvin Roberto Silvestre Hernández
Asesorado por el Ing. Enrique Edmundo Ruiz Carballo

Guatemala, noviembre de 2008

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ESTUDIO DE LAS VENTAJAS E IMPLEMENTACIÓN DE SERVICIOS IP VPN, SOBRE UNA INFRAESTRUCTURA MPLS EN LA REGIÓN CENTROAMERICANA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA

1FACULTAD DE INGENIERÍA

POR

KELVIN ROBERTO SILVESTRE HERNANDEZ

ASESORADO POR EL INGENIERO ENRIQUE EDMUNDO RUIZ CARBALLO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, NOVIEMBRE DE 2008

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Milton De León Bran
VOCAL V	Br. Isaac Sultán Mejía
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Otto Fernando Andrino
EXAMINADOR	Ing. José Aníbal Silva
EXAMINADOR	Ing. Byron Arrivillaga
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ESTUDIO DE LAS VENTAJAS E IMPLEMENTACIÓN DE SERVICIOS IP VPN, SOBRE UNA INFRAESTRUCTURA MPLS, EN LA REGIÓN CENTROAMERICANA,

tema que me fuera asignado por la Dirección de la Escuela de Mecánica Eléctrica, el 13 de julio de 2007.

Kelvin Roberto Silvestre Hernández

Guatemala, 22 Septiembre del 2,008

Señor Coordinador del Area de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Señor Coordinador

Por medio de la presente, me permito informarle que he revisado completamente el trabajo de graduación titulado: "Estudio de las Ventajas e Implementación de Servicios IP VPN sobre una Infraestructura MPLS en la Región Centroamericana.", desarrollado por el señor Kelvin Roberto Silvestre Hernández, dicho trabajo cumple con los objetivos propuestos en el anteproyecto de tesis.

Por lo tanto, el autor de este trabajo y yo, como su asesor, nos hacemos responsables del contenido y conclusiones de la misma.

Atentamente,

Ing. Enrique Edmundo Ruiz Carballo
Asesor Nombrado
Colegiado 2225

FACULTAD DE INGENIERIA
Escuelas de Ingeniería Civil, Ingeniería Mecánica Industrial, Ingeniería Química, Ingeniería Mecánica Eléctrica, Técnica y Regional de Post-grado de Ingeniería Sanitaria.
Ciudad Universitaria, zona 12
Guatemala, Centroamérica

Guatemala, 23 de octubre de 2008

Señor Director
Ing. Mario Renato Escobedo Martínez
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC

Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **"ESTUDIO DE LAS VENTAJAS E IMPLEMENTACION DE SERVICIOS IP VPN SOBRE UNA INFRAESTRUCTURA MPLS EN LA REGION CENTROAMERICANA"**, desarrollado por el estudiante **Kelvin Roberto Silvestre Hernández**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA

Ing. Julio César Solares Peñate
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Area, al trabajo de Graduación del estudiante: Kelvin Roberto Silvestre Hernández, titulado: Estudio de las Ventajas e Implementación de Servicios IP VPN sobre una Infraestructura MPLS en la Región Centroamericana, procede a la autorización del mismo.

Ing. Mario Renato Escobedo Martínez
DIRECTOR

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA

GUATEMALA, 24 DE OCTUBRE 2,008.

AGRADECIMIENTOS A

DIOS	Por regalarme la vida y darme la oportunidad de cumplir con mis metas.
MIS PADRES	Mario Roberto Silvestre Aroche y Marina Eliseth Hernández de Paz, por todo el amor, soporte y apoyo durante los años de estudio a lo largo de mi vida.
MIS HERMANOS	Mario Augusto, Roxana Liseth y Lynn Nicté, gracias por su paciencia, apoyo y comprensión, en especial a mi hermano, gracias por ser mi mejor amigo y darme tu ejemplo de rectitud y tenecidad.
MI ABUELITA Y TÍA	Francisca de Paz y Gladys Hernández, gracias por el cariño y muestras de apoyo durante lo largo de mi carrera profesional.
MI AMADA	Jeniffer Elisa Pérez H., por tu amor, comprensión, apoyo y confianza que me has brindado durante todo este tiempo. Te amo mi vida.
FAMILIARES	Que me brindaron su apoyo y comprensión a lo largo de la carrera.
AMIGOS Y COMPAÑEROS	Por toda la ayuda y solidaridad a lo largo de la carrera.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE ABREVIATURAS

ASN (*Autonomous system Number)*

ATM (*Asynchronous transfer mode*) Red de modo de transferencia asíncrono.

ATM PNNI (ATM *Private Network-Node Interface*) Interface Red-Nodo Privada.

BGP (*Border Gateway Protocol*) Protocolo de acceso de borde o frontera.

CPE (*Customer Premises Equipment*) Equipo de acceso del cliente.

FEC (*Forwarding Equivalent Class*) Clase de envío equivalente .

IANA (*Internet Assigned Numbers Authority*) Autoridad de Internet de Asignación de Números.

IETF (*Internet Engineering Task Force*) Fuerza de Tareas de Ingeniería de Internet.

IGP (*Interior Gateway Protocol*) Protocolo de Acceso Interno.

IS – IS (*Intermediate System to Intermediate System*) Sistema Intermedio a sistema intermedio.

LAN (*Local Area Network*) Red de Área Local o simplemente Red Local.

LDP (*Label Distribution Protocol*) Protocolo de distribucion de etiquetas.

LER (*Layer Edge Router*) Conmutador Frontera entre capas.

LSP *(Label Swichet Path*) Camino Conmutado de Etiquetas.

LSR (*Label Switch Router*) Conmutador de Etiquetas.

MPLS (*Multi-Protocol Level Swiching*) Protocolo múltiple de conmutación de etiquetas.

OSPF (*Open Shortest Path Frist*) Primero la ruta más corta.

QoS (*Quality of Service*) Calidad de servicio.

RD (*Route Distinguisher*) Descriptor de Rutas.

RSVP (*Resource Reservation Protocol*) Protocolo de Reserva de Protocolos.

TCP/IP (*Transport Control Protocol / Internet Protocol*) Protocolo de control de transporte / Protocolo de internet.

VPN (Virtual Private Network) Red Privada Virtual.

GLOSARIO

ASBR: Enrutador Límite del Sistema Autónomo: *Autonomous System Boundary Router*: es un router localizado entre un sistema autónomo OSPF y una red no OSPF como por ejemplo RIP. ASBR corre sobre OSPF y otros protocolos de enrutamiento como lo es RIP.

ATM: Con esta tecnología, a fin de aprovechar al máximo la capacidad de los sistemas de transmisión, sean estos de cable o radioeléctricos, la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser enrutadas individualmente mediante el uso de los denominados canales virtuales y trayectos virtuales.

Best Effort: Se refiere a un servicio de la red que intenta entregar los mensajes a los correspondientes destinatarios, los cuales no necesiten de un tratamiento especial que retransmita los paquetes corruptos o perdidos. Así es que no hay garantías con respecto a la entrega.

CUG: (*Closed User Group,* en inglés) es un grupo de usuarios de una misma red pública que se comunican entre sí por mutuo acuerdo y que excluyen a otros. CUG previene correspondencia no requerida en los sistemas de mensajería instantánea, por ejemplo, y proveen un nivel significativo de seguridad.

EBGP: EBGP describe el peering BGP entre vecinos de diferentes AS, los vecinos eBGP deben de tener una subred en común.

Extranet: Es una red privada virtual que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización. Se puede decir en otras palabras que una extranet es parte de la Intranet de una organización que se extiende a usuarios fuera de él. Usualmente utilizando el *Internet.*

FEC: Para cualquier protocolo de ruteo que tenga alguna oportunidad de sobrevivir, la escalabilidad es un problema que debe ser resuelto desde el principio. Para asegurar la escalabilidad, los flujos de estado deben ser manejados en conjunto y nunca en flujos individuales. MPLS asegura la escalabilidad soportando la agregación con lo que se llama *Forwarding Equivalence Class* (Clase de Redireccionamiento Equivalente) FEC.

FTP: Es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo.

IETF: (*Internet Engineering Task Force* - Grupo de Tareas de Ingeniería de Internet). Organización de técnicos que administran tareas de ingeniería de telecomunicaciones, principalmente de Internet (ej: mejora de protocolos o darlos de baja, etc.).

Intranet: Una Intranet es un conjunto de contenidos compartidos por un grupo bien definido dentro de una organización.

***Jitter*:** Es una variación o perturbación en los pulsos de una transmisión digital, sino que puede ser pensado, en cierto modo, como pulsos irregulares. *Jitter* puede manifestarse a través de variaciones en la amplitud, intensidad de la señal, y otros elementos de estas olas. Las causas son habituales tiempos de conexión, conexión de retardos, congestiones de tráfico de datos, y la injerencia. En pocas palabras, este es un temblor de la voz de salida a las fallas de sistema e interrupciones.

***Loopback*:** El dispositivo de red *loopback* es un interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado. El valor en IPv4 es 127.0.0.1 y ::1 para el caso de IPv6. Se utiliza en tareas de diagnóstico de conectividad y validez del protocolo de comunicación, así como para indicar que el destino del puntero o URL es el mismo host.

OSPF: *Open Shortest Path First* es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (*Interior Gateway Protocol*), que usa el algoritmo *Dijkstra* enlace-estado (LSA - *Link State Algorithm*) para calcular la ruta más corta posible. Usa c*ost* como su medida de métrica. Además, construye una base de datos enlace-estado (*link-state database*, LSDB) idéntica en todos los enrutadores de la zona.

QoS: (*Quality of Service*, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio.

RIP: Son las siglas de ***R**outing **I**nformation **P**rotocol* (Protocolo de encaminamiento de información). Es un protocolo de puerta de enlace interna o **IGP** *(**I**nternal **G**ateway **P**rotocol*) utilizado por los enrutadores, aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

RSVP: Es un protocolo de capa de transporte designado para reservar recursos a través de una red integrada de servicios de internet. "RSVP no es una aplicación de transporte, es más bien un protocolo de control de internet, como ICMP, IGMP, o protocolos de encaminamiento". RSVP reserva los canales o rutas en redes internet para la transmisión por unidifusión y multidifusión con escalabilidad y robustez.

RESUMEN

MPLS (*Multi-Protocol Label Switching*) es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios *Prívate Line, Frame Relay* o ATM. Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia. Una VPN (*Virtual Private Network*) consiste de una red de datos privada que puede utilizar una infraestructura de telecomunicaciones compartida, mediante protocolos de encaminamiento (*routing*) o tunelización (*tunneling*) y protección de seguridad. Las IP VPN's utilizan una red IP, que puede ser la Internet pública o la red de datos propia de un proveedor de servicios (ISP *Internet Service Provider*), para transportar tráfico; este método representa la próxima generación de soluciones de red gestionadas.

El Mercado objetivo clave para los servicios de IP VPN se basa principalmente en las empresas con múltiples sedes, ya sean multinacionales o empresas locales medianas o de gran tamaño. Las VPN's suelen utilizarse para interconectar redes de área local (LAN) empresariales a una red troncal IP; lo que significa que pueden deshacerse de los circuitos dedicados que requieren las conexiones basadas en frame relay o ATM. Además, las IP VPN's se utilizan para conectar emplazamientos remotos a la red de área extensa (WAN) de una empresa. Durante este trabajo se realiza un estudio de la forma de implementar este tipo de servicio y de las ventajas que conlleva dicha implementación para las empresas que lo contratan como para los Proveedores del servicio que la implementan, también se realiza una comparación de un enlace de datos centralizado con un enlace IP VPN MPLS en los aspectos técnicos y económicos de cada uno en varios países de la región centroamericana. .

OBJETIVOS

General:

Estudiar las ventajas e Implementación de servicios IP VPN sobre la infraestructura MPLS en la región Centroamericana.

Específicos:

1. Realizar un estudio general de lo que es una IP VPN sobre MPLS.

2. Optimizar los recursos lógicos y físicos de los servicios regionales al configurar servicios IP VPN.

3. Describir los pasos requeridos para configurar un enlace del tipo IP VPN a través del equipo Tellabs 8660.

4. Dar a conocer las distintas calidades de servicio que se pueden implementar en los enlaces del tipo IP VPN a través del equipo Tellabs 8660.

5. Desarrollar una comparación técnica y económica en la implementación de un enlace de datos con un enlace IP VPN sobre MPLS.

INTRODUCCIÓN

En un mundo en el que día a día las empresas incursionan en nuevos mercados, en busca de más y más clientes de diferentes países, y realidades sociales, se hace necesaria la comunicación dentro de sus diferentes sedes para transmitir información sobre ventas o estrategias de negocio, para informar sobre la producción minuto a minuto, o cualquier otro fin; este tipo de crecimiento empresarial ha dado lugar a que se desarrollen tecnologías convergentes que satisfagan las necesidades del cliente, en el sentido de velocidad, disponibilidad y seguridad de su comunicación.

La tecnología de MPLS (Switch de Cabeceras Multiprocolos) ha dado lugar a la implementación de redes privadas virtuales basadas en el protocolo de internet, siendo esto una ventaja para el proveedor de servicio de Internet como para los clientes, las razones son abundantes, como por ejemplo, la versatilidad de poder usar las mismas redes para varios clientes una y otra vez, sin provocar esto problemas entre los enlaces, ya que se hace de manera independiente; otro ejemplo radica en la facilidad de integrar diversos tipos de tecnologías, lo que permite la integración con otros proveedores o la posibilidad de entregar los enlaces de datos con distintos tipos de tecnologías como lo pueden ser: ATM, FR, *Clear Channel,* etc.

Sin embargo, hay otras maneras de conectar las sucursales de una empresa, se puede hacer a través de internet utilizando redes privadas virtuales o también entregando enlaces de datos en todos los puntos y centralizándolos en un enrutador en la casa matriz, dentro de este trabajo de graduación simularemos estos escenarios y se hace la comparación entre los mismos para ver las ventajas y desventajas que cada uno de ellos representa en cuanto a las necesidades del cliente se refiere.

1.- MPLS & VPN

1.1.- Fundamentos de MPLS:

Bajo MPLS (*Multiprotocol Label Switching*) o Protocolo múltiple de conmutación de etiquetas, se encuentra una tecnología de conmutación de circuitos que ofrece capacidades de multiprotocolo, porque sus técnicas son aplicables a cualquier protocolo de nivel de red. MPLS es un mecanismo de enrutamiento flexible basado en la asignación de flujos a rutas extremo-extremo dentro de un Dominio Autónomo.

La flexibilidad ofrece la libertad de escoger el criterio por el cual los flujos de tráfico serán reconocidos y tratados de forma distintiva. En particular, tal libertad permite que un tráfico entre un par origen-destino pueda separarse en rutas paralelas para evitar congestionar los enlaces de red. La ingeniería de tráfico en Internet es una de las aplicaciones primarias previstas para MPLS.

Las principales ventajas que ofrece MPLS son:

- Permite especificar mecanismos para la administración de flujos de tráfico de diferentes tipos (Ej.: flujos entre diferente *hardware,* diferentes máquinas, etc.).

- Independiza los protocolos de la capa de enlace y la capa de red.

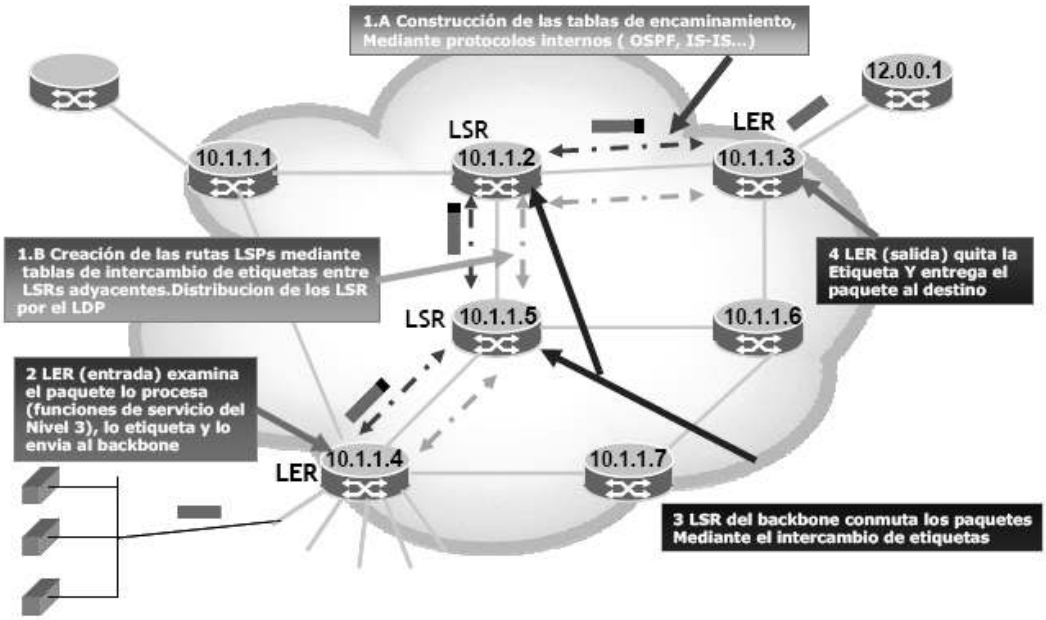
- Dispone de medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes.

- Ofrece interfaces para diferentes protocolos de encaminamiento y señalización.

- Soporta los protocolos de la capa de enlace usados tradicionalmente para IP. Además opera perfectamente sobre ATM y Frame Relay, dado el parecido en el mecanismo de transporte y conmutación.

Una red MPLS está compuesta por enrutadores MPLS: LSR (*Label Switched Router*) que representan el núcleo de la red (*backbone*) y los LER (*Label Edge Router*), que son los encargados de realizar la interfaz con otras redes, como se observa en la figura 1:

Figura 1. Componentes de una red MPLS y establecimiento de un LSP.



Fuente: Introducción a las tecnologías MPLS, MPλS y GMPLS,
Universidad Politécnica de Catalunya, Barcelona, España.

Los LSR son enrutadores de gran velocidad en el núcleo de la red MPLS. Sus principales funciones son: participar en el establecimiento de los circuitos extremo-extremo de la red o LSPs (*Label Switched Path*) usando un protocolo de señalización apropiado y conmutar rápidamente el tráfico de datos entre los caminos establecidos. Los LER son los enrutadores situados en la frontera de la red. Son responsables de enviar el tráfico entrante a la red MPLS utilizando un protocolo de señalización de etiquetas y distribuir el tráfico saliente hacia las distintas redes destino. Los LERs se clasifican en nodos de entrada (*ingress node*) y nodos de salida (*egress node*).

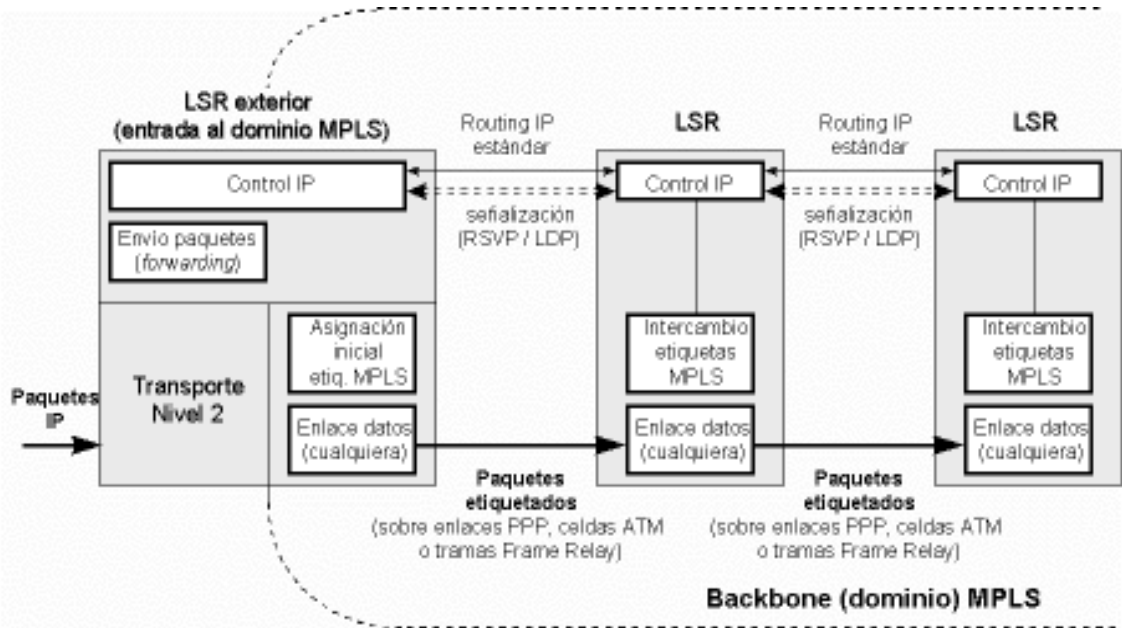
Cuando un paquete entra a una red MPLS, se le asigna un determinado FEC. Un FEC es un conjunto de paquetes que comparten unas mismas características para su transporte, así todos recibirán el mismo tratamiento en su camino hacia el destino. Cada FEC puede representar un requerimiento de servicio para un conjunto de paquetes o para una dirección fija. La clase FEC a la cual se asigna el paquete se codifica como un valor corto de longitud fija conocido como *etiqueta.* Esta etiqueta es usada por los conmutadores de la red para encaminar el paquete hacia su siguiente nodo. Cuando un paquete se envía a su siguiente enrutador, la etiqueta es enviada con él. La etiqueta se usa como un índice en la tabla que especifica el próximo salto y una nueva etiqueta. La etiqueta vieja es sustituida por la nueva y el paquete es enviado al salto siguiente.

1.2 Funcionamiento del envío de paquetes en MPLS

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); para el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (*hops*) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (*Label-Swiching*

enrutador) a otro, a través del dominio MPLS. Un LSR no es sino un enrutador especializado en el envío de paquetes etiquetados por MPLS.

Figura 2. Esquema funcional de MPLS



Fuente: MPLS "Multiprotocol Label Switching": Una Arquitectura de Backbone para la Internet del Siglo XXI. María Sol Canalis 1 Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina

Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (*routing*) y de envío (*forwarding*). Del mismo modo, el envío se implementa mediante el *intercambio de etiquetas* en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM Forum; en lugar de ello, en MPLS se utiliza el protocolo RSVP o bien un nuevo estándar de señalización (*Label Distribution Protocol*, LDP). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de

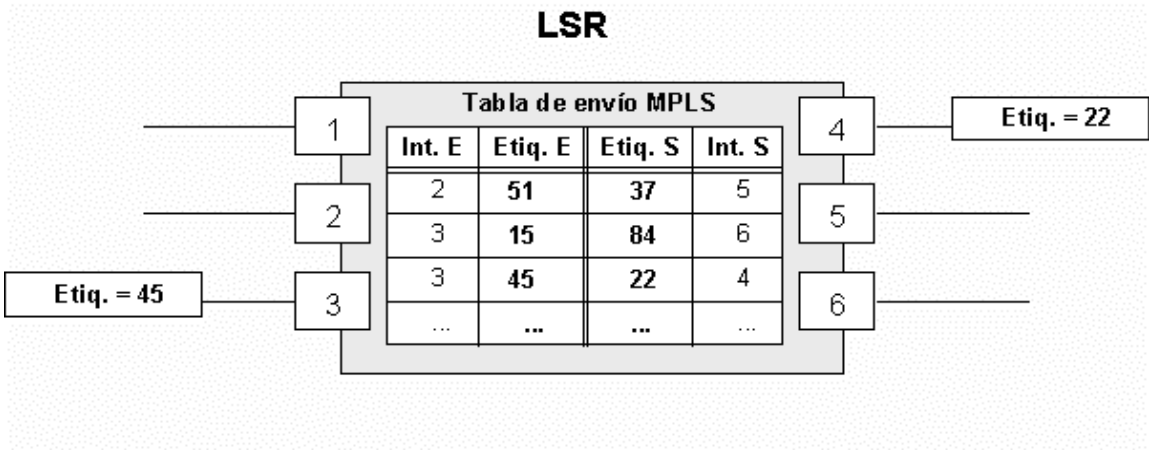
encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido específicamente al transporte de datos basado en celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como *Frame Relay*, o directamente sobre líneas punto a punto.

1.2.1 Establecimiento de un LSR

Un LSR es como un enrutador que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control, según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola).

En la figura 3 se ilustra un ejemplo del funcionamiento de un LRS del núcleo MPLS. A un paquete que llega al LSR por la interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

Figura 3. Detalle de la tabla de envío de u n LSR.



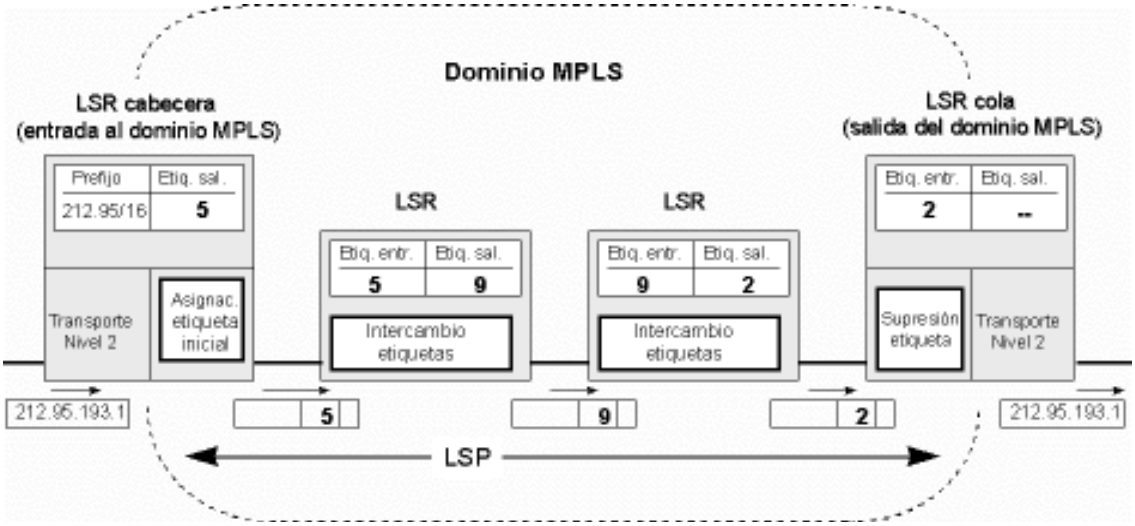
Fuente: MPLS "Multiprotocol Label Switching": Una Arquitectura de Backbone para la Internet del Siglo XXI. María Sol Canalis 1 Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 4 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95.0.0/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por *routing* convencional.

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS

debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de *Frame Relay*), se utilizan esos campos nativos para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas por ejemplo enlaces PPP o LAN, entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

Figura 4. Ejemplo de un envío de paquete por un LSP



Fuente: MPLS "Multiprotocol Label Switching": Una Arquitectura de Backbone para la Internet del Siglo XXI. María Sol Canalis 1 Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina

1.2.2 Establecimiento de un LSP

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

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

- Encaminamiento explícito: El LER de entrada determina la secuencia de saltos explícito desde la entrada hasta la salida. Puede que la ruta no esté completamente especificada, es decir, puede haber un conjunto de nodos que sean representados como un único salto en la ruta. También puede contener un identificador de Sistema Autónomo (AS) que permita que el LSP sea encaminado a través de un área de la red que está fuera del control administrativo de quien inició el LSP. Dentro de estos dos casos se hará un encaminamiento salto a salto.

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

Para conseguir esta adaptación al tráfico real de la red, los mecanismos de ingeniería del tráfico deben realizar tareas de monitorización. Por lo tanto, se puede

afirmar que los mecanismos de gestión de recursos están constantemente pendientes del estado real de la red y fuertemente relacionados con el establecimiento de LSP de trabajo y de respaldo con algoritmos de encaminamiento con calidad de servicio. Por este motivo, la gestión de recursos también cubre la detección de las alarmas en el momento en que se produce un fallo en la red y la activación de los LSP de respaldo, así como la monitorización del estado real de la red y procede a su adaptación (cambiando los LSP existentes) al tráfico real y a los posibles fallos que puedan surgir (activando los LSP de respaldo necesario). Una vez establecidos los LSP, éstos tendrán una cierta vida, corta o larga, durante la cual pueden sufrir una serie de problemas. Se puede establecer un LSP con un cierto ancho de banda asignado para una cierta cantidad de tráfico con una determinada calidad de servicio.

Sobre este LSP puede suceder que, al cabo de un cierto tiempo, la demanda de tráfico supere la reserva inicial y se produzca un rechazo de tráfico de entrada. Este rechazo o bloqueo se produce debido a algún tipo de mecanismo de control de admisión, necesario para garantizar la calidad de servicio de las distintas conexiones existentes, y puede cuantificarse calculando la probabilidad de bloqueo para cada LSP. Otro fenómeno que puede suceder es que, una vez reservada una cierta cantidad de ancho de banda para un cierto LSP, después de cierto tiempo este LSP esté poco utilizado y se estén desperdiciando los recursos de la red, cuando posiblemente otros LSP puedan estar congestionados y rechazando tráfico.

La técnica habitual para adaptar el ancho de banda de los LSP al tráfico real es la reasignación de banda de los mismos, incrementándola o decrementandola según sea el caso. Para poder incrementar la banda de un LSP es necesario que a lo largo del camino que sigue este LSP (los diferentes enlaces físicos que atraviesa) existan los suficientes recursos libres. Si esto no sucede, existen dos posibles acciones a tener en cuenta: La primera es buscar en qué enlaces físicos no se cumple la condición de que no exista suficiente banda disponible, y posteriormente, en estos enlaces comprobar si existe otro

LSP subutilizado y del que se pueda tomar la banda necesaria. En otras palabras, consiste en traspasar banda de LSP's poco usados a un LSP congestionado y que necesita incrementar su banda. La segunda posibilidad, en el caso de que la primera no sea posible, es reencaminar el LSP que necesita mayor ancho de banda a través de otro camino que pueda satisfacer sus necesidades. También en este caso, si no es posible reencaminar al LSP congestionado, existe la posibilidad de reencaminar uno o varios demás LSP con los que comparten los mismos enlaces físicos, con lo cual se liberan recursos y permite incrementar su banda. En los casos en los que hay que reencaminar LSP se puede hacer uso de los algoritmos de encaminamiento dinámicos y con calidad de servicio.

De ahí que estos mecanismos de gestión de recursos estén estrechamente relacionados con los mecanismos de establecimiento de LSP de trabajo y de respaldo con calidad de servicio, creando un entorno global de ingeniería de tráfico. Otro aspecto a tener en cuenta es qué mecanismos toman la decisión de adaptar la banda de los LSP y realizar las operaciones anteriormente descritas. Existen diferentes ejemplos en la literatura, y dependiendo de dónde se tome la decisión, se puede hablar de mecanismos centralizados o distribuidos. Estos mecanismos, por las tareas que realizan, se situarían dentro del plano de gestión. Tradicionalmente la gestión, en este caso de recurso y de fallos, se ha realizado de forma centralizada, lanzando algoritmos de optimización que, disponiendo de los datos de monitorización de toda la red, calculan la distribución óptima de los LSP.

En redes troncales relativamente grandes, por las que circula gran cantidad de LSP, es muy difícil disponer de todos los datos de monitorización de forma centralizada y calcular la distribución óptima a tiempo antes de que el respaldo de la red ya haya cambiado. Una de las opciones que aparecen en la literatura reciente es tratar de mantener la distribución de LSP lo más cercana posible a la óptima haciendo pequeños ajustes usando algoritmos distribuidos. La ventaja principal de los algoritmos

distribuidos es que disponen de la información de forma local y permanentemente actualizada. Por el contrario, la desventaja está en que no se dispone de una visión global de la red. Por esta razón algunos algoritmos de este tipo se basan en distintas técnicas de inteligencia artificial y/o en distintas heurísticas para intentar realizar las mejores adaptaciones, aunque no se disponga de una completa información.

1.2.3 Control de la información en MPLS:

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

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

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

El segundo aspecto se refiere a la información de "señalización", pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin

embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF (recuérdese que ése era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, el cual es el caso del *Label Distribution Protocol* (LDP).

1.3 Protocolo de distribución de etiquetas:

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por los cuales un enrutador LSR informa a otro de la relación etiqueta FEC que ha hecho. Dos enrutadores LSR, que usan un protocolo de distribución de etiquetas para intercambiar la información de la etiqueta/FEC se le conoce como "puertos de distribución de etiquetas" respecto a la información que intercambian. Si dos enrutadores LSR son puertos de distribución de etiquetas, se habla de que hay una "distribución de etiquetas adyacente" entre ellos. El protocolo de distribución de etiquetas también abarca las negociaciones en el que dos puertos de distribución de etiquetas necesitan comunicarse con el fin de aprender de las posibilidades de MPLS del otro.

Dependiendo de cómo se establezcan los LSP se pueden presentar diversas opciones: si se utiliza la aproximación de salto a salto (*hop by hop*) para el establecimiento de los LSP la IETF ha reconocido (*no obligatorio*) el uso del protocolo LDP (*Label Distribution Protocols*) para la asignación de etiquetas, en este caso también se pueden utilizar los protocolos RSVP y CR-LDP. Si la estrategia utilizada es la "*downstream unsolicited*" donde el LER de salida distribuye las etiquetas que deben ser utilizadas para alcanzar un determinado destino, la única opción disponible es LDP.

Cuando la estrategia es "*downstream on demand*" iniciada por el LER de entrada y no se desea seguir el camino calculado paso a paso, sino que se desea utilizar el que permita definir una ruta explícita, las opciones actualmente disponibles son CR-LDP y RVSP.

1.3.1 El protocolo LDP

Es la opción recomendada aunque no obligatoria del IETF. Para el intercambio de mensajes entre LSR's se realiza mediante el envío de PDU's de LDP. Este envío se basa en la utilización de sesiones LDP que se establecen sobre conexiones TCP. Es importante destacar que cada LDP PDU puede transportar más de un mensaje LDP, sin que estos mensajes tengan relación entre ellos. El protocolo LDP utiliza el esquema de codificación de mensajes conocido como TLV (Tipo, Longitud, Valor), cada mensaje LDP tiene la siguiente estructura:

- **U** Campo de un bit que indica el comportamiento en caso de recibir un mensaje desconocido. U=0 hay que responder con un mensaje de notificación al LSR origen, U=1 se ignora el mensaje y se continua procesando el PDU.

- **F** Campo de un bit. Este campo sólo se utiliza cuando el bit U está en 1. Si se recibe un mensaje desconocido que debe propagarse y el bit F está en 0, este mensaje no progresa al siguiente LSR, en caso contrario sí se hace.

- **Tipo** Campo de 14 bits que define el tipo de mensaje y, por lo tanto indica cómo deber ser interpretado el campo valor.

- **Longitud** Campo de 2 octetos que especifica la longitud del campo valor.

- **Valor** Campo de longitud variable que contienen la información del mensaje. La interpretación de la cadena de octetos de este campo depende del contenido del campo tipo.

Figura 5. Esquema de formato de protocolo LDP con codificación TLV

U	F	Type	Length
		Value	

TLV format

http://www.javvin.com/protocolLDP.html, artículo sobre LDP.

1.3.2 RSVP (*Resource Reservation Protocol*)

Para poder utilizar este protocolo en el entorno MPLS se le han agregado nuevas capacidades, estas se refieren a los objetos formados de los paquetes y procedimientos necesarios para establecer los túneles LSP. Para el establecimiento de los túneles LSP el protocolo de señalización utiliza el modelo *downstream on demand.* Esto significa que la petición de asociación entre el FEC y una etiqueta para crear un túnel LSP es iniciada por el LSR de entrada; para lograr este objetivo hay que agregar un objeto (*LABEL_REQUEST*) al mensaje del tramo propio de RSVP antes mencionado.

Un requisito adicional para este protocolo RSVP es que el dominio MPLS debe soportar encaminamiento explicito (*Explicit_Route*) en los mensajes del tramo. Este nuevo objeto encapsula el conjunto de nodos ordenados que constituyen la ruta explícita que deben seguir los datos. Como la asignación de etiquetas se realiza desde el destino hacia el origen, en sentido contrario al flujo de datos, es necesario incrementar el mensaje *resv* con un objeto adicional (*Label*) capaz de transportar la nueva información requerida para este uso del protocolo. El funcionamiento de este protocolo para el establecimiento de túneles LSP se describe a continuación:

- Cuando un LER de entrada al dominio MPLS decide que necesita establecer un LSP hasta determinado LER de salida, debe iniciar un procedimiento para establecerlo, mediante un mensaje de tamo. La ruta que debe seguir el LSP puede ser una ruta explícita determinada por el gestor de la red (esta ruta no puede coincidir con la calculada por los algoritmos de encaminamiento de la capa de red).

- Cuando los LSR intermedios reciben el mensaje de tramo lo procesan de acuerdo con las especificaciones del protocolo y una vez reconocido que no son el extremo del FEC, transmiten el mensaje hacia el siguiente nodo de la ruta.

- Cuando el mensaje de path finalmente alcanza el LSE destino, éste procede a reservar los recursos internos, selecciona la etiqueta a utilizar para este túnel LSP y procede a propagarla hacia el anterior LSR mediante un mensaje de reserva (*resv)*.

- Cuando los LSR's intermedios reciben la asignación de la etiqueta con el mensaje *resv* proceden a reservar los recursos internos necesarios y determinar la etiqueta a utilizar para el flujo. Una vez calculada la propagan para el LSR anterior de nuevo con la ayuda del mensaje *resv.* Este proceso se repite hasta alcanzar el LSR origen donde también se realiza el proceso de reservar recursos internos, pero en este caso no es necesario asignar etiqueta y propagarla ya que se ha alcanzado el origen del FEC.

Proceso del flujo de datos:

Al contrario que los protocolos de ruteo, RSVP está diseñado para manejar el flujo de datos en lugar de tomar decisiones individuales de cada datagrama. El flujo de

datos consiste en sesiones discretas entre máquinas con destino y origen específico. Una sesión es definida específicamente como el flujo simple de datagramas hacia un destino y etiqueta de protocolo particular. Además, las sesiones están identificadas por los siguientes datos: Dirección de destino, ID del protocolo y puerto destino. RSVP soporta ambas sesiones *simplex, unicast y multicast.*

1.3.3 CR-LDP (*constraint-based router label distribution protocol)*:

Es un encaminamiento basado en restricciones (*Constraint-based routing*). Esta extensión del LDP se basa en el cálculo de trayectos que están sujetos a ciertas restricciones: ancho de banda, los requisitos de calidad de servicios QoS, demora (delay), variación de demora o jitter, o cualquier otro requisito asociado al trayecto que defina el operador de la red. Esta es una de las herramientas más útiles para controlar el dimensionado del tráfico y el QoS en la red que pueden ofrecer a sus clientes y/o usuarios.

Debido a ello, el capítulo MPLS de la IETF ha elaborado las extensiones necesarias para que el protocolo LDP pueda soportar este tipo de encaminamiento; esta extensión es conocida como CR-LDP (*Constraint-Based Routing Label Distribution Protocol*) y se ha definido expresamente para soportar el establecimiento y mantenimiento de LSP encaminados en forma explícita y las modificaciones de los LSP, pero no incluyen los algoritmos necesarios para calcular trayectos según los criterios definidos por el operador de la red.

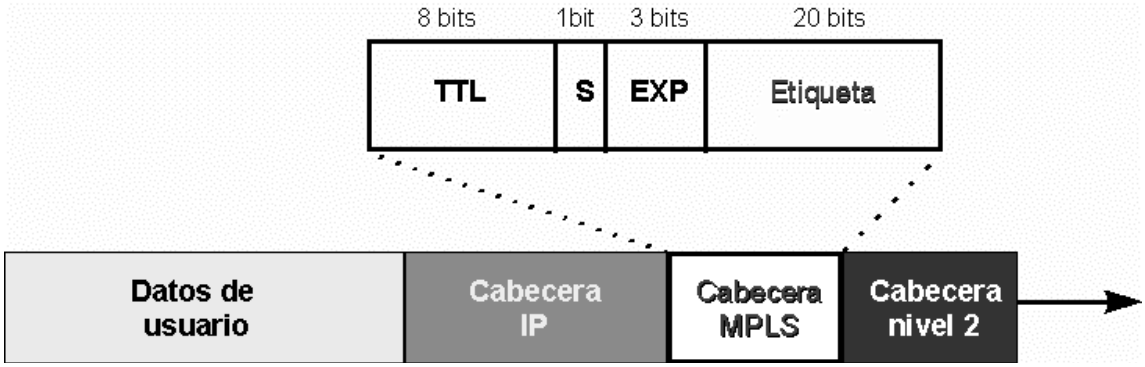
Las principales limitaciones son las siguientes:

- Solo se soportan LSP's punto a punto
- Solo se soportan LSP's unidireccionales
- Sólo se soporta una única etiqueta por LSP

1.3.4 Cabecera de MPLS:

En la figura 6 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS), 1 bit de *stack* para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (*time to-live*) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

Figura 6: Estructura de la cabecera genérica de MPLS



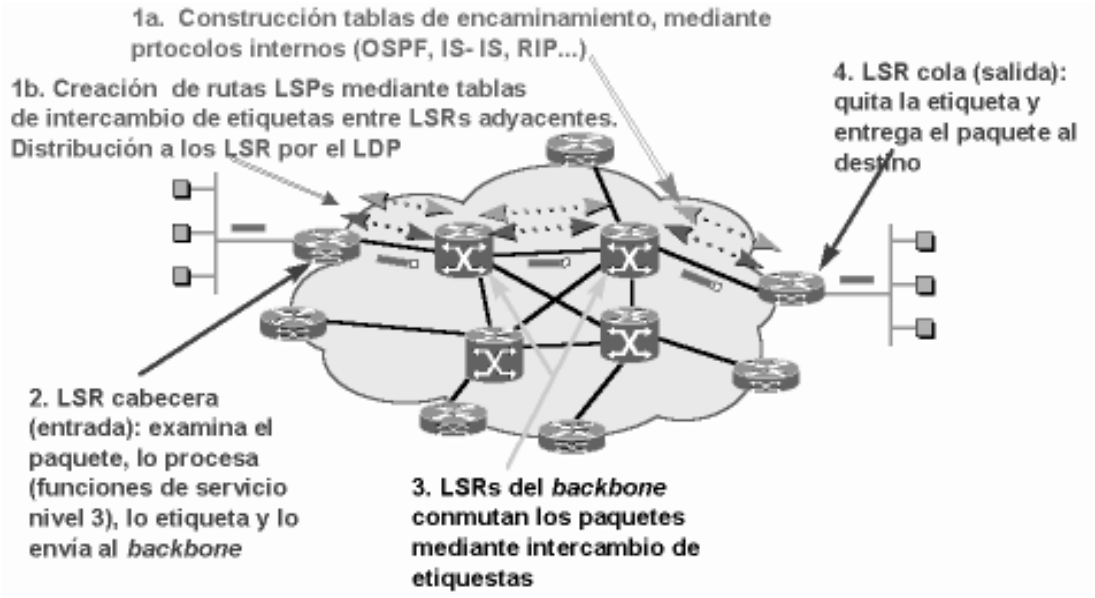
Fuente: MPLS "*Multiprotocol Label Switching*": Una Arquitectura de *Backbone* para la Internet del Siglo XXI. María Sol Canalis 1 Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina

1.3.5 Funcionamiento global de MPLS:

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura 7, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de *enrutadores*

IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de *enrutadores* a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de *enrutadores*). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP.

Figura 7: Funcionamiento de una red MPLS



Fuente: MPLS "*Multiprotocol Label Switching*": Una Arquitectura de *Backbone* para la Internet del Siglo XXI. María Sol Canalis 1 Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina

1.4 VPN's (*virtual private networks*):

Para permitir la comunicación entre redes que no tienen una conexión física entre si pero que tienen como red común a la red Internet, se hace necesario la implementación de una VPN *(Virtual Private Network)* por sus siglas en ingles, para poder transmitir datos entre ellas como si estuvieran físicamente conectadas entre si. La implementación de VPN (Virtual Private Network) permite opcionalmente la transferencia de datos de manera segura utilizando un mecanismo de cifrado de datos que garantice la confidencialidad de la información, así mismo las políticas de seguridad del sistema impedirán que personas no autorizadas tengan acceso a la VPN. Existen varias maneras de implementar una VPN, afortunadamente ya existe un estándar establecido para Internet II y que es soportado en la actual versión de Internet I (IP v.4), este estándar se llama IPSec. Con una VPN no requiere adquirir canales dedicados excesivamente costosos, por lo que ofrecen la mejor relación costo / beneficio.

Los posibles escenarios de red privada virtual basados en la configuración habitual de un servidor VPN son:

- Acceso remoto de VPN para empleados.
- Acceso de sucursales a petición.
- Acceso persistente de las sucursales.
- Extranet para socios comerciales.
- VPN y conexión telefónica con autenticación *RADIUS.*

Las razones que empujaron a adoptar la solución en ese sentido son fundamentalmente de costes: resulta mucho más barato interconectar a los empleados utilizando una infraestructura pública que desplegar una red físicamente privada, también abaratará los costes en facturas telefónicas debido a que las tarifas de conexión

a Internet son sensiblemente más baratas que las de las llamadas directas sobre todo con las relacionadas con la telefonía móvil.

Para imitar un vínculo punto a punto, los datos se encapsulan o se envuelven con un encabezado que proporciona información de enrutamiento, lo que permite que los datos atraviesen la red compartida o pública hasta llegar a su punto de destino. Para imitar un vínculo privado, los datos se cifran para conservar la confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar sin las claves de cifrado.

En los enlaces Cliente-Red que se crearán se encapsula con el protocolo PPP (*Point To Point Protocol*). Las tramas del cliente se encapsulan en PPP, y el PPP resultante se encapsula para crear el VPN. Este tipo de enlace nos proporciona un acceso seguro de un cliente a la red, con total movilidad y con independencia del Proveedor de Servicios de Internet (ISP) por el que se ingresa.

El encapsulado de las tramas PPP en datagramas se puede realizar de dos formas según el protocolo a usar:

- **PPTP (*point-to-point tunneling protocol*)**: Encapsulado de tramas PPP en datagramas IP, utilizando una versión extendida del GRE (*Generic Routing Encapsulation*, protocolo IP 47). La conexión de control se realiza sobre TCP, puerto 1723. Actualmente este protocolo, aunque muy popular en el mundo Microsoft, está siendo sustituido por el L2TP. La implementación de Microsoft, además, sufre de varios importantísimos errores de diseño que hacen que su protección criptográfica sea inefectiva para alguien más motivado que un simple observador casual.

- **L2TP (*layer 2 tunnelling protocol*)**: Encapsulado de tramas PPP sobre cualquier medio, no necesariamente redes IP. En el caso IP se usa UDP, puerto 1701. Tras un largo proceso como borrador, L2TP pasa a ser una propuesta de estándar en Agosto de 1.999.

También se hace uso del protocolo:

- **IPSec:** IPSec es el nuevo marco de seguridad IP, definido con el advenimiento del IPv6. Aunque IPv6 está muy poco difundido en este momento, la tecnología marco IPSec se está utilizando ya, lo que asegura, entre otras cosas, la interoperatividad de los sistemas de diversos fabricantes. IPSec integra confidencialidad, integridad y autentificación en un mismo marco interoperante.

El servidor VPN, que se encuentra en la oficina central, proporciona acceso remoto y conexiones VPN PPTP y L2TP. Además, el servidor VPN proporciona el enrutamiento de paquetes hacia ubicaciones en Intranet o Internet.

Esta empresa será provista de una dirección IP fija con un dominio en Internet proporcionado por un proveedor ISP que además proveerá una página Web, cuentas de correo electrónico y servidor FTP. Todo esto será creado, mantenido y administrado por dicha empresa a la que se le pagará una cuota mensual.

El esquema general de la red es el indicado por la siguiente figura:

Figura 8: Esquema general de la red VPN

http://www.javvin.com/protocolLDP.html, artículo sobre LDP

2.- SOLUCIONES BGP/MPLS VPN EN LA CAPA 3

2.1.- Fundamentos de la construcción de la solución BGP/MPLS VPN:

Es utilizado para distribución de rutas a través del *backbone*. La principal meta de este método es soportar el *outsourcing* de los servicios de *backbone* IP para las redes empresariales. Esto permite hacerlo de una manera simple para la empresa, mientras sigue siendo escalable y flexible para el proveedor de servicios, y además le permite al proveedor de servicios dar valores agregados.

El escenario de esta solución es el siguiente: un cliente que tiene geográficamente dispersos sus sitios y requiere conectividad entre ellos para llevar sus negocios del día a día. El cliente no desea invertir en infraestructura para conectar estos sitios, ni siquiera el esfuerzo para administrar dicha infraestructura. En un mundo competitivo, él o ella se pueden concentrar en el negocio y contratar a alguien externo que haga la tarea de proveer conectividad entre los sitios, a alguien experto en redes, a un Proveedor de Servicios.

Del lado del cliente lo que requiere es que esta conectividad sea hecha de una manera simple. Principalmente al conectar los sitios dispersos deben de tener la misma calidad de servicio y garantías de privacidad como si fuera una red privada, y no debería de sufrir cambios en la manera en que el cliente tiene su red configurada.

Del lado del proveedor de servicios la meta es llenar las expectativas del cliente mientras maximiza las ganancias. Para llenar estas expectativas, el proveedor tiene que ser capaz no solo de proveer la conectividad sino también de extender los servicios de una manera fácil y permitir a los clientes de usar direcciones de red privadas. Para

maximizar las ganancias, el proveedor debe poder soportar una gran cantidad de clientes con respecto al número de sitios, desde clientes con uno o dos sitios hasta otros con cientos de sitios por todos lados. No solo esto, el proveedor debe ser capaz de ofrecerle al cliente servicios de valor agregado que pueden ser cargados como un servicio *premium*. Finalmente, los recursos usados para proveer el servicio débe de ser compartido entre todos los clientes.

Basados en estas metas, veamos porque la solución es la llamada *Virtual Private Network* (VPN). Primero, es una red porque provee conectividad entre sitios separados. Segundo, es privada porque los clientes requieren que tenga las mismas propiedades y garantías como las de una red privada, ambas en términos de la operación de la red (direcciones, espacios, ruteos) y en términos del direccionamiento de tráfico. Tercero, es virtual porque el proveedor pude usar los mismos recursos y facilidades para dar servicios a más de un cliente.

Los PE enrutadores utilizan BGP (*Border Gateway Protocol*) para distribuir las rutas VPN a cada uno (más acertado, para causar la distribución de las rutas entre una y otra.). Un BGP speaker puede instalar y distribuir únicamente una ruta a prefijo de dirección dada. Aún así nosotros permitimos que cada VPN tenga su própio espacio de direcciones, lo que significa que las mismas direcciones o rangos de direcciones pueden ser usadas en cualquier número de VPNs, donde en cada VPN la dirección denota un sistema diferente. Lo que sigue es que necesitamos permitir al BGP que aprenda y redistribuya múltiples rutas a una símple prefijo de dirección IP. Luego debemos asegurarnos que los Policy (políticas), sean usados para determinar que sitios pueden usar que rutas; dado a que múltiples de esas rutas están establecidas por BGP, solo una de estas debe aparecer en la tabla de ruteo de cada sítio.

2.2. La familia de direcciones VPN-IPv4:

Una VPN-IPv4 tiene una dirección de 12 *bytes*, empezando por 8 *bytes* del RD (*Route Distinguisher*) "Descriptor de Ruta" y terminando con la dirección de IPv4 4 *bytes*. Si dos VPNs usan el mismo prefijo de dirección IPv4, el PE traduce esto a un prefijo de dirección VPN-IPv4 único. De esta manera se asegura que si la misma dirección es usada en dos diferentes VPNs, es posible poner dos rutas completamente diferentes para esas direcciones, una para cada VPN.

El RD puede ser usado para crear múltiples rutas diferentes para el mismo sistema. Esto permite al BGP conocer múltiples rutas diferentes en el mismo sistema, y permite utilizar políticas para decidir que paquetes usan que rutas.

El RD está estructurado para que cada proveedor de servicios pueda administrar su propio "espacio de numeración" (por ejemplo, puede hacer sus propias asignaciones del descriptor de rutas), sin entrar en conflicto con los RD asignados por otros SP. Un RD consiste en un tipo de campo de 2 bytes, un campo del administrador y el campo del número asignado. El valor del tipo de campo determina la longitud de estos dos campos, así como la semántica del campo del administrador. El campo del administrador, identifica un número asignado de la autoridad, y el campo del número asignado contiene el número que ha sido asignado por la la autoridad identificada, para un propósito particular. Por ejemplo, uno puede tener un RD cuyo campo de administrador tenga el ASN (*Autonomous System Number*) "Número de Sistema Autónomo", y cuyo campo de número (4 bytes) contiene un número asignado por el SP a el cual el IANA ha asignado ese ASN. Los RD tienen esta estructura para asegurar que el SP que provee el servicio de backbone para la VPN pueda crear siempre únicas RD cuando sea necesario. De cualquier manera, la estructura no contiene ninguna semántica. Cuando BGP compara dos direcciones, ignora la estructura completamente.

Si el sub campo del administrador y el del número asignado para la dirección VPN-IPv4 son ambos puestos a cero, la dirección VPN-IPv4 se considera como que tiene el mismo significado que su correspondiente dirección IPv4 global única. En particular, esta dirección VPN-IPv4 y su correspondiente dirección IPv4 global única serán consideradas comparables por BGP. En todos los demás casos, la dirección VPN-IPv4 y su correspondiente dirección IPv4 global única serán consideradas como no comparables por BGP.

Una tabla de ruteo de sitios solo podrá tener una ruta VPN-IPv4 para cualquier dirección IPv4. Cuando la dirección de destino del paquete concuerda con la ruta VPN-IPv4, solo la parte IPv4 es realmente comparada. Un PE necesita ser configurado para asociarle rutas que lo lleven a un CE en particular con una RD particular. El PE puede ser configurado para asociar todas las rutas que lo lleven al mismo CE con el mismo RD, o puede ser configurado para asociar diferentes rutas con diferentes RDs, aún si estas llevan el mismo CE.

2.3. Distribución de rutas entre PEs por BGP

Si dos sitos de una VPN están juntos a PEs que están en el mismo ASN, los PEs pueden distribuir las rutas entre las VPN-IPv4 por medio de la conexión IBGP entre ellos.

Si dos sitios de una VPN están en diferente ASN (por ejemplo, debido a que están conectadas por diferentes SPs), entonces el enrutador PE necesitará utilizar IBGP para redistribuir las rutas de la VPN IPv4 ya sea a un Autonomous System Border enrutador (ASBR), o a una ruta reflectora de la cual el ASBR es cliente. El ASBR necesitará entonces usar EBGP para redistribuir esas rutas a un ASBR en otro AS. Esto nos permite conectar diferentes sitios de la VPN a diferentes Proveedores de Servicio. De cualquier manera, las rutas de las VPN-IPv4 podrían solo ser aceptadas en conexiones EBGP de puntos de peering privados, como parte de un arreglo de confianza

entre SPs. Las rutas de las VPN-IPv4 no deberían ser ni distribuidas ni aceptadas desde la Internet pública.

Si hay muchas VPNs que tienen sitios ligados a diferentes Sistemas Autónomos, no es necesario que haya un solo ASBR entre esos dos Ases que tienen todas las rutas para todas las VPNs; pueden haber múltiples ASBRs, cada uno de los cuales contiene las rutas de una serie de VPNs.

Cuando un enrutador PE distribuye rutas de VPN-IPV4 vía BGP, usa su propia dirección como el "BGP próximo salto". Así mismo asigna y distribuye las etiquetas MPLS. (Esencialmente, los enrutador PE no distribuyen las rutas VPN-IPv4, sino las rutas VPN-IPv4 Etiquetadas) Cuando el PE procesa un paquete recibido que tiene su etiqueta al principio del *stack*, el PE salta el *stack*, y envía el paquete directamente al sitio donde la ruta indica. Esto significa usualmente que solo envía el paquete al enrutador CE de donde aprendió la ruta. La etiqueta también determinar la encapsulación del link de datos.

En la mayoría de los casos, la etiqueta asignada por el PE causará que el paquete sea enviado directamente al CE, y el PE que recibe el paquete etiquetado no verá la dirección de destino del paquete en ninguna tabla de ruteo. De cualquier manera, es posible para el PE asignar una etiqueta que implícitamente identifica una tabla de ruteo en particular. En este caso, el PE recibe paquetes en cuya etiqueta podrá ver la dirección de destino y encontrarlo en su tabla de ruteo.

Nótese que la etiqueta de MPLS que es distribuido en esta forma es útil si hay un *label switched path* entre el enrutador que pone la ruta y el próximo salto de BGP de esa ruta. No estamos asumiendo un procedimiento usado para fijar ese *label switched path* puede ser fijado en una base preestablecida, o puede ser fijada cuando una ruta necesita que así lo sea. Puede ser una ruta "*best effort*", o puede ser una ruta con ingeniería de

tráfico. Entre enrutador un PE particular y sus rutas BGP del siguiente salto para una ruta en particular debe haber un LSP (*Label Switch Path*), o puede haber varias, quizá con diferentes características de QoS (*Quality of Service)*. Todo lo que concierne para la arquitectura de VPN es que algunas LSP entre el enrutador y su próximo salto BGP exista.

Sí un determinado enrutador PE no está vinculado a ninguno de los objetivos de las rutas particulares de las VPNs, no debería de recibir esa ruta; el otro PE que le está distribuyendo las rutas debe de aplicar un filtro de salida para evitar enviar rutas innecesarias. Por supuesto, si un enrutador PE recibe una ruta vía BGP, y este PE no está incluido en ninguna de las rutas destino de las VPNs, el PE debe aplicar un filtro de entrada a dicha ruta, ni de distribución ni de utilización. En pocas palabras, un enrutador que no está ligado a ninguna VPN, no debería de tener ninguna ruta VPN-IPV4. Estas reglas de distribución aseguran que no hay ninguna caja que necesite conocer todas las rutas VPN-IPv4 que son utilizadas a través del *backbone*. Como resultado, el número total de dichas rutas que pueden ser soportadas a través del *backbone* no se ven limitada por la capacidad de un equipo, y por lo mismo puede incrementarse virtualmente sin límites.

2.4 Las VPNs con atributos de origen

Una ruta VPN IPv4 puede estar opcionalmente asociada a una VPN con atributos de origen. Este atributo único identifica un grupo de sitios, e identifica las rutas correspondientes que han venido de uno de los sitios en ese grupo. Los usos típicos de estos atributos pueden ser para identificar la compañía a la que pertenece el sitio de la ruta recibida, o identificar los sitios en una intranet. De cualquier forma, otros usos pueden ser posibles. Este atributo puede ser entendido como un atributo extendido de las comunidades BGP.

En situaciones en donde es necesario identificar el origen de una ruta, es este atributo, no el RD, que es el más usado. Estos atributos pueden ser usados cuando se construyen las VPNs, como se describe más adelante.

Sería más acertado, si menos sugestivo, llamar a esta cualidad el atributo del "Origen de la Ruta" en lugar de "Origen de la VPN". Realmente identifica la ruta solo como proveniente de un grupo particular de sitios, sin el prejuicio de que si este grupo en particular de sitios realmente constituyen una VPN.

2.4.1 Construyendo VPNs usando los atributos del origen y destino

Al ajustar las cualidades de origen y destino apropiadamente, podemos construir diferentes tipos de VPNs. Supóngase que se desea construir una *Closed Used Group* (CUG) que contenga un grupo particular de sitios. Esto puede ser posible al crear un valor de atributo particular de VPN de Destino que represente el CUG. Este valor entonces necesita ser asociado con una tabla de ruteo por sitio para cada uno de los sitios en el CUG, y necesita ser asociado con cada ruta aprendida de los sitos en el CUG. Cualquier ruta que tenga este atributo de VPN de destino necesitará ser redistribuida para que pueda alcanzar todo PE enrutador añadido a cada sitio en el CUG.

Alternativamente, suponga que uno desea, por cualquier motivo, crear una VPN del tipo "*hub and spoke*". Esto puede ser realizado por el uso de dos valores del atributo de destino, uno que signifique "*Hub*" y otro "*Spoke*". Entonces las rutas de *spoke* pueden ser distribuidas al *hub*, sin crear rutas en el *hub* para que sean distribuidas en *spoke*.

Suponga ahora que uno tiene un número de sitios que están en la intranet y en la extranet, así como un número de sitios que están únicamente en la intranet. Entonces puede haber ambas, intranet y extranet, rutas que tengan un número de VPN Destino que

identifique todo el grupo de sitios. Los sitios que deben tener solo las rutas de la intranet pueden filtrar todas las rutas con el número incorrecto de la VPN de Origen.

Estos dos atributos permiten gran flexibilidad ya que podemos, a través de ellos, controlar la distribución de la información de las rutas entre varios grupos de sitios, que alternadamente proveen gran flexibilidad al construir VPNs.

2.5 Encaminamiento a través del *backbone*

Si las rutas intermedias en el *backbone* no tienen ninguna información acerca de las VPNs, ¿Cómo son direccionadas las rutas de un sitio de VPN a otro?

Esto es hecho en términos de MPLS con los apilados de dos niveles en la etiqueta. PE enrutadores (*ASBRs que redistribuyen direcciones VPN-IPv4*) necesitan insertar direcciones /32 para ellos mismos en las tablas de ruteo IGP del *backbone*. Esto le permite a MPLS, en cada nodo en la red del *backbone*, asignar una etiqueta correspondiente a la ruta de cada enrutador PE. (*Ciertos procedimientos para poner las label switched paths en el backbone pueden no requerir la presencia de las direcciones /32*).

Cuando un PE recibe un paquete de un equipo CE, este escoge de una tabla de direccionamiento de los sitios particulares en donde busca la dirección de destino del paquete.

Si el paquete es destinado a un equipo CE que está pegado al mismo PE, el paquete es enviado directamente al equipo CE.

Si el paquete no está destinado al equipo CE pegado al mismo PE, el "próximo salto de BGP" se encuentra, así como la etiqueta a la cual ese próximo salto de BGP es asignada para la dirección de destino de dicho paquete. Esta etiqueta es puesta en el apilado de etiquetas del paquete, y se convierte en el fondo de la etiqueta. Entonces el PE mirá en la ruta IGP por el próximo salto de BGP, y en base a esto determina el siguiente paso IGP, así como la etiqueta asignada a la dirección del próximo salto de BGP por el próximo salto de IGP. Esta etiqueta es empujada hacia el tope de la etiqueta del paquete, y el paquete es entonces re direccionado hacia el próximo salto IGP. (Si el próximo salto BGP es el mismo que el de IGP, entonces la segunda etiqueta no es necesaria para ser puesta al tope de la etiqueta.).

A este punto, MPLS llevará el paquete a través del *backbone* hasta el equipo CE apropiado. Esto es, todas las decisiones de direccionamiento por los enrutadores P y PE son hechas por medio de MPLS, y el encabezado del paquete IP no se usa sino hasta que el paquete alcance el equipo CE. El último enrutador PE quitará la última etiqueta del apilado de etiquetas MPLS antes de enviar el paquete al equipo CE, de esta forma el equipo CE verá nada más un paquete IP ordinario.

Cuando un paquete entra al *backbone* desde un sitio en particular vía un enrutador PE, la ruta del paquete es determinada por el contenido de la tabla de ruteo que dicho enrutador PE asoció a ese sitio. La tabla de ruteo del enrutador PE donde el paquete deja el *backbone* no es relevante. Como resultado, uno puede tener múltiples rutas hacia el mismo sistema, donde la ruta particular elegida para un paquete en particular es basada en el sitio desde donde el paquete entra al *backbone*.

Tome en cuenta que es el etiquetado de segundo nivel el que hace posible mantener todas las rutas de las VPN fuera de los enrutadores P, y esto es crucial para asegurar la escalabilidad del modelo. El *backbone* no necesita tener rutas hacia los CEs, solo hacia los PEs.

2.6 Cómo los equipos PEs aprenden rutas de los equipos CEs:

Los enrutadores PE que están ligados a una VPN particular necesitan saber, para cada uno de los sitios de la VPN, que direcciones en esa VPN están en cada sitio. En el caso donde el equipo CE es un *host* o un *switch*, esta sería de direcciones que son configuradas regularmente en el enrutador PE pegado al equipo. En el caso donde el equipo CE es un enrutador, hay muchas maneras posibles en las que el enrutador PE puede obtener esta serie de direcciones.

El PE traduce estas direcciones en direcciones VPN-IPv4, usando una RD configurada. El PE entonces trata estas direcciones VPN-IPv4 como entradas de BGP. En ningún caso la rutas de un sitio van a entrar en las IGP's del *backbone*. Exactamente que técnicas de distribución de rutas PE/CE posibles dependen si una CE particular es una VPN de tránsito o no.

Una VPN en tránsito es una que contiene un enrutador que recibe rutas de un tercer lado (por ejemplo de un enrutador que no está en la VPN, pero que tampoco es un enrutador PE), y que redistribuye esas rutas al enrutador PE. Una VPN que no es de tránsito es una "VPN de Porciones". La mayoría de VPNs, incluyendo casi todas las redes corporativas de las empresas, se espera que sean de "Porciones" en este sentido.

Las técnicas de distribución PE/CE posibles son:

1. Rutas estáticas (*es decir configuración*) puede ser usada. Es probable que sea útil solo para las VPN de porciones.

2. los enrutadores PE y CE pueden ser pares RIP (*Routing Information Protocol*), y el equipo CE puede usar RIP para decirle al enrutador PE la serie de prefijos de direcciones que son alcanzables en el sitio del enrutador CE. Cuando el RIP es

configurado en el CE, se debe de tener cuidado con asegurarnos que los prefijos de direcciones de otros sitios (*por ejemplo, direcciones aprendidas por el enrutador CE del enrutador PE*) nunca sean propagadas al enrutador PE. Para ser más precisos: si un enrutador PE, digamos PE1, recibe una ruta R1 VPN-IPv4, y como resultado distribuye una ruta R2 IPv4 al CE, entonces R2 no debe de ser distribuida por el sitio CE hacia el enrutador PE nuevamente, pero digamos que PE2, donde PE1 y PE2 pueden ser el mismo enrutador o diferente, trace una ruta VPN-IPv4 que es diferente a la de R1, entonces si lo podría redistribuir ya que el camino que tomaría sería diferente.

3. Los enrutadores PE y CE pueden ser parejas OSPF. En ese caso, los sitios pueden ser una simple área OSPF, el CE debe de ser el ABR en esa área, y el PE debe de ser el ABR que no está en esa área. Además, el enrutador PE no debe de reportar *links* de rutas que no sean del CE que están en la misma área. (*Esta técnica puede ser usada solo en loas VPN de Porciones*).

4. Los enrutadores CE y PE pueden ser parejas BGP, y el enrutador CE debe de usar BGP (*en particular, EBGP para decirle al enrutador PE la red de dirección que están en el sitio del enrutador Ce*). Esta técnica puede ser usado para ambos tipos de VPN.

Desde la perspectiva técnica puramente, esta es por mucho la mejor técnica:

a. A diferencia de las alternativas IGP, esto no requiere que el PE tenga múltiples algoritmos para lograr hablarse con múltiples CEs.

b. BGP está diseñado explícitamente solo para esta función: pasar información de ruteo entre sistemas que corren por diferentes administradores.

c. Si el sitio contiene "BGP *backdoors*", por ejemplo, enrutador con conexiones BGP hacia otros enrutadores que no sean los PE, este procedimiento trabajará correctamente en todas las circunstancias. Los otros procedimientos pueden o no trabajar, dependiendo de circunstancias precisas.

d. El uso de BGP hace mucho más fácil el transporte de atributos de rutas del enrutador CE hacia el PE. Por ejemplo, el CE pude sugerir un destino en particular para cada ruta, a través de las cualidades de destino que el PE está autorizado a añadir a cada ruta.

Por otro lado, al usar BGP es probable que sea algo nuevo para los administradores de los enrutador CE, excepto en los casos donde el cliente mismo es un *Intenet Service Provider* (ISP).

Si un sitio no es una VPN de Tránsito, obsérvese que no necesita tener un único número del sistema autónomo (ASN), cada CE donde el sitio no es una VPN de tránsito puede usar el mismo ASN. Esto se puede elegir del espacio privado del ASN, y será llevada afuera del PE. *Loops* de ruteo pueden ser prevenidos por el uso de las Cualidades del Origen del Sitio.

Si una serie de sitios constituyen una VPN de tránsito, es conveniente representarlas como una confederación de BGP, así la estructura interna de la VPN es ocultada de los enrutadores que no estén dentro de la VPN. En este caso, cada sitio en la VPN necesitará dos conexiones BGP con el *backbone*, una que es interna para la confederación y la otra que es externa a ella. Los procedimientos usuales para la intra-confederación serán modificados levemente ya que hay que tomar en cuenta el hecho de que el *backbone* y los sitios pueden tener diferentes políticas. El *backbone* es miembro de la confederación en una de las conexiones, pero no en la otra. Estas técnicas pueden

ser útiles si el cliente del servicio VPN es un ISP. Esta técnica permite a los clientes que son ISP obtener servicios de *backbones* VPN de alguno de sus ISP *peers*.

Cuando no necesitamos distinguir entre las diferentes maneras en que un PE puede ser informado de las direcciones que existen en un sitio, simplemente decimos que el PE ha aprendido las rutas de ese sitio.

Antes de que el PE pueda redistribuir una ruta VPN-IPv4 aprendida de algún sitio, este debe de asignarle ciertos atributos a la ruta. Hay tres de estos atributos:

- Sitio de origen: este atributo único identifica el sitio desde donde el enrutador PE aprende la ruta. Todos las rutas aprendidas de un sitio en particular debe de ser asignado el mismo atributo de sitio de origen, aún si el sitio tiene múltiples conexiones a un único PE, o si está conectado a múltiples PEs. Diferentes cualidades de Sitio de Origen debe ser usados para sitios distintos. Esta cualidad puede ser interpretada como una cualidad de comunidad BGP extendida.

- VPN de origen

- VPN de destino

2.7 Cómo los equipos CE aprenden la rutas de los equipos PE.

En esta sección asumimos que el equipo CE es un enrutador. En general, el PE distribuye a un CE cualquier ruta que el PE tenga puesta en la tabla de ruteo que utiliza para realizar el ruteo de paquetes de ese CE. Hay una excepción: si un sitio de ruta con Atributo de Origen identifica un sitio en particular, esa ruta no debe de redistribuirse a ningún CE en ese sitio.

En la mayoría de los casos, será suficiente para el PE simplemente distribuir la ruta default al equipo CE. En algunos casos, puede que sea suficiente para el CE ser configurado con la ruta default apuntando al PE. Esto puede funcionar generalmente en cualquier sitio que no necesite distribuir la ruta default para otros sitios, (por ejemplo, si un sitio de una VPN corporativa tiene acceso al Internet de la corporación, este sitio necesita tener una ruta *default* al otro sitio, pero no pude distribuir una ruta *default* así mismo).

Cualquier procedimiento se utiliza para distribuir las rutas del CE al PE también serán utilizadas para distribuir las rutas del PE al CE.

2.8 CE que soportan MPLS

En el caso donde el equipo CE soporta MPLS, y esta dispuesto a importar la serie completa de rutas de sus VPNs, el PE puede distribuirle una etiqueta para cada ruta. Cuando el PE recibe un paquete del CE con dicha etiqueta, este primero reemplaza la etiqueta con la correspondiente que ha aprendido vía BGP, y luego empuja en la etiqueta el siguiente salto BGP para la correspondiente ruta.

2.8.1 Sitios virtuales

Si la distribución de rutas entre CE/PE se hace vía BGP, el CE puede usar MPLS para soportar múltiples sitios virtuales. El CE puede tener para sí mismo una tabla de ruteo aparte para cada sitio virtual, que va llenando como le es indicado por la VPN con atributos de Origen y Destino por las rutas que recibe del PE. Si el CE recibe todas las rutas del PE, el PE no necesitará hacer ninguna busqueda de direcciones en los paquetes que reciba del CE. Alternativamente, el PE puede en algunos casos ser capaz de distribuir al CE una simple ruta default (etiquetada) para cada VPN. Así cuando el PE recibe un paquete etiquetado del CE, sabrá a que tabla de ruteo debe de ir a buscar; la

etiqueta colocada en el paquete por el CE identificará solo el sitio virtual de donde el paquete viene.

2.9 Seguridad

Bajo las siguientes condiciones:

a) Los paquetes etiquetados que vienen de fuentes no confiables no son aceptados por los enrutadores *backbones*, a menos que sea conocido que dichos paquetes dejarán el *backbone* antes que el encabezado de ip o cualquier etiqueta menor en el apilado sea examinado.

b) Las rutas VPN-IPv4 etiquetadas no son aceptadas cuando vienen de fuentes desconocidas o poco fiables.

La seguridad proveída por esta arquitectura es virtualmente idéntica a la dada por las VPNs *Frame Relay* y ATM *backbones*. Vale la pena observar que el uso de MPLS hace mucho más simple proveer este nivel de seguridad que al utilizar algún tipo de túneles IP dentro de IP en lugar de MPLS. Es solo cuestión de aceptar o rechazar los paquetes etiquetados a menos que la primera de las condiciones de arriba se aplique. Es mucho más difícil configurar un enrutador para que acepte o rechace un paquete IP si el paquete es un paquete de un túnel ip-ip que va a un sitio incorrecto.

El equipo de MPLS también permite a las VPNs conectar múltiples SPs sin depender en ninguna forma de la distribución inter-dominio de la información de las rutas Ipv4. También es posible para un usuario de VPN proveer para sí mismo seguridad, haciendo uso de Túnel modo IPSEC.

2.9.1. Seguridad punto a punto en túneles entre enrutadores CE.

Un usuario de VPN consciente de la seguridad querrá asegurarse que algunos o todos los paquetes que atraviesen el *backbone* sean autenticados y/o encriptados. La manera estándar de conseguir esta funcionalidad hoy sería crear un túnel de seguridad entre cada pareja de enrutador CE en la VPN, usando el modo de túnel IPSEC. De cualquier forma, los procedimientos descritos hasta ahora no permiten al enrutador CE transmitir un paquete para determinar o identificar el siguiente enrutador CE que el paquete atravesará. Toda esta información es requerida para poder usar el túnel modo IPSEC. Así que debemos extender estos procedimientos para poder hacer esta información disponible.

Cara ruta VPN-IPv4 puede tener un atributo que identifique el siguiente enrutador CE que atravesará si se sigue esa ruta. Si esta información es enviada a todos los enrutadores CE en la VPN, el modo estándar del túnel IPSEC puede ser usada. Si el CE y el PE son parejas BGP, es natural presentar esta información como un atributo BGP. Cada CE que deba utilizar IPSEC debe de estar configurado también con un sistema de prefijos de dirección. Esto previene al CE de mandar tráfico inseguro a cualquiera de esas direcciones y también si por alguna razón, este falla de obtener la información necesaria.

Cuando MPLS es usado para transportar paquetes entre dos puntos finales de un túnel IPSEC, el encabezado externo de IPSEC no realiza prácticamente ninguna función. Sería beneficioso desarrollar una forma de túnel IPSEC que permita al encabezado externo ser omitido cuando se esté utilizando MPLS.

2.9.2 Asociación de seguridad multi-partida

En lugar de poner un túnel de seguridad entre cada pareja de enrutadores CE, puede ser más ventajoso poner una simple asociación de seguridad multi-partida. En dicha asociación de seguridad, todos los enrutadores CE que son parte de una VPN en particular podrán compartir los mismos parámetros de seguridad (*por ejemplo, los mismos secretos, mismos algoritmos, etc.*). De esta forma el CE de ingreso no necesita saber cual CE es el siguiente en recibir la información, solo necesitará saber a que VPN la información va dirigida. Un CE que esté en múltiples VPN's puede usar diferentes parámetros de seguridad para cada una, para proteger por ejemplo, paquetes de la intranet de ser expuestos en la extranet.

Con dicho esquema, el túnel estándar en modo IPSEC no será usado, porque no hay modo de llenar en el campo IP de dirección de destino el "encabezado externo". De cualquier forma, cuando MPLS se utiliza para transmitir, no hay necesidad de este encabezado externo, el enrutador PE puede usar MPLS para obtener un paquete de la salida de un túnel sin saber siquiera la dirección IP de ese *endpoint*; solo necesita ver la dirección IP de destino del "encabezado interno".

Un avance significativo de un esquema de este tipo es que hace cambio de ruteo (en particular, cambios en el CE de egreso por una dirección en particular) transparente a la seguridad del mecanismo. Esto puede ser particularmente importante en el caso de VPN's con multiproveedores, donde la necesidad de distribuir información acerca de dicho ruteo cambia debido a los mecanismos de soporte de seguridad que puede dar lugar a asuntos de escalabilidad.

Otra ventaja es que se elimina la necesidad del encabezado IP, dado que la encapsulación MPLS realiza esta función.

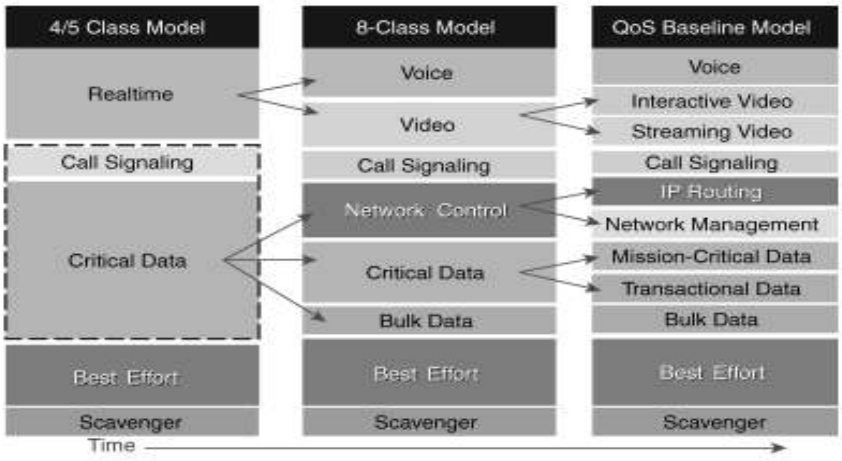
2.10 Calidad de servicio y clase de servicio

Para proveer un mecanismo para priorizar los diferentes tipos de tráfico IP que existen en la red, es importante adoptar un modelo de Clase de Servicio que sea flexible, simple de mantener y que cumpla con las necesidades de comportamiento de las diferentes aplicaciones.

Las aplicaciones pueden ser categorizadas dentro de clases apropiadas dependiendo de los requerimientos de entrega. Basado en esta estrategia, las siguientes clases de servicio de QoS serán definidas para direccionar los diferentes requerimientos de todo el tráfico mientras se mantiene un pequeño número de clases.

La figura 9 muestra una aproximación de un modelo a seguir para una empresa. Un modelo de clase de servicio con cuatro o cinco clases de precedencia puede ser un punto de partida a considerar para las empresas. Este modelo permite que pueda tenerse clases más granulares conforme se van añadiendo con el paso del tiempo.

Figura 9: Esquema de clases de servicio



Fuente: *Selecting MPLS VPN Services*, por Chips Lewis, Steve Pickavance. Cisco *Press, Networking Technology*.

Entendiendo el modelo de desarrollo de las necesidades se pueden seguir estos pasos durante el proceso:

- Paso 1: Definir estratégicamente los objetivos de la empresa que serán alcanzados a través de la implementación de los QoS.

- Paso 2: Analizar los requerimientos de niveles de servicio que serán aprovisionados para las distintas clases de tráfico.

- Paso 3: Diseñar y probar las políticas de QoS antes de ponerlas en producción dentro de la red.

- Paso 4: Poner en producción dentro de la red las clasificaciones de QoS que previamente fueron probadas.

- Paso 5: Monitorear los niveles de servicio para asegurarse que los objetivos trazados para el QoS se han alcanzado.

Estos pasos pueden requerir que sean repetidos mientras las condiciones de uso vayan cambiando y evolucionando. La clasificación está dividida en dos áreas diferentes: Clasificación Capa 3 y CoS capa 2.

2.10.1 Requerimientos de calidad de servicio para la voz, video y datos.

El siguiente paso es identificar los requerimientos detallados para las clases que se crearán como parte del marco de QoS. Estas características están bien definidas, y el proceso que conlleva a su identificación es un componente crítico para asegurar un acercamiento consistente a lo que deseamos lograr.

Para alcanzar dichos valores, las empresas y los Proveedores de Servicio deben cooperar y ser conscientes en clasificar, aprovisionar e integrar sus respectivas soluciones de QoS.

Adicionalmente, los Proveedores de Servicio deben tener al menos 3 clases de servicio en todas las interfaces. Esto es para asegurar que las empresas no necesiten modificar o volver a trabajar sus políticas para entenderse con las políticas del SP o transportar sus clases transparentemente. Estas clases deben de incluir una clase de Real Time, una Clase de datos de Alta Prioridad y la clase de *Best-effort*.

2.10.2 Requerimientos QoS para la voz.

Las llamadas de voz, ya sea uno a uno o las conexiones de conferencia requieren lo siguiente:

- ≤ 150 ms de latencia en un sentido de la oreja a la boca.
- ≤ 30 ms de *jitter*.
- ≤ 1 por ciento de pérdida de paquetes.
- 17 to 106 kbps de ancho de banda garantizado por llamada (dependiendo de la rata de muestreo, codec y la cabecera de la capa 2).
- 150 bps (más la cabecera de la capa 2) por teléfono de ancho de banda garantizado para el control de tráfico de voz.

La elección del *codec* tiene impacto en muchas áreas. La más importante es la capacidad de planeación en la red, porque el ancho de banda consumido en diferentes *codecs* varía. Cuando exploraba a detalle estas necesidades en su trabajo de IP SLA, John Evans y *Clarence Filsfils* escribieron que el Codec G.114 con 150 ms de *delay* de punto a punto no causaba degradación perceptible en la calidad de la voz para el uso de la telefonía. Algunos *carriers* tratan de tener como objetivo 100 ms de *delay*, por supuesto para brindar la mejor calidad posible. Sin embargo un objetivo usual es mantenerlo en 150 – 120 ms sin propagación.

Es recomendable que se ponga atención al consumo de cabecera en la Capa 2. un método exacto para aprovisionar VoIP es incluir la cabecera de la capa 2. La cabecera de capa 2 incluye preámbulos, cabeceras, banderas, chequeo de redundancia cíclica (CRCs), y una celda ATM de colchón. Cuando la cabecera de capa 2 está incluida en los cálculos de ancho de banda, el ancho de banda de una llamada por VoIP necesita llenar los requisitos de la tabla I que se muestra abajo.

Tabla I: tabla de consumo de los *codecs* para voz

Codec	**Rata de Muestreo**	**Tamaño de paquete de voz en Bytes**	**Paquetes por segundos**	**Ancho de banda por conversación**
G.711	20 ms	160	50	80 kbps
G.711	30 ms	240	33	74 kbps
G.729A	20 ms	20	50	24 kbps
G.729A	30 ms	30	33	19 kbps

Fuente: *Selecting MPLS VPN Services*, por Chips Lewis, Steve Pickavance.
Cisco *Press, Networking Technology*.

Un método más exacto para aprovisionar es, como mencionamos antes, incluir la cabecera de la capa 2 en los cálculos de ancho de banda, así como se muestra en la tabla II de abajo.

Tabla II: Tabla de consumo de los *codecs* para voz + cabecera capa 2

Codec	**801.Q *Ethernet* + 32 *Layer* 2 *Bytes***	**MLP + 13 *Layer* 2 *Bytes***	***Frame Relay* + 8 *Layer* 2 *Bytes***	**ATM + *Variable Layer* 2 *Bytes (Cell Padding)***
G.711 at 50 pps	93 kbps	86 kbps	84 kbps	104 kbps
G.711 at 33 pps	83 kbps	78 kbps	77 kbps	84 kbps
G.711 at 50 pps	37 kbps	30 kbps	28 kbps	43 kbps
G.711 at 33 pps	27 kbps	22 kbps	21 kbps	28 kbps

Fuente: *Selecting* MPLS VPN *Services*, por Chips Lewis, Steve Pickavance.
Cisco *Press, Networking Technology*.

2.10.2.1 Ejemplo de cálculo.

Los siguientes cálculos son usados para determinar las entradas en la planeación del consumo de una llamada de voz:

- Tamaño total del paquete = (*Encabezado capa 2: MP o FRF.12 o Ethernet*) + (*encabezado IP/UDP/RTP*) + (*Tamaño de la carga de voz*).

- PPS (*Paquetes por segundo*) = (*rata de muestreo del codec) / (tamaño de la carga de voz).*

- Ancho de Banda = (*tamaño total del paquete * pps*).

Por ejemplo, el ancho de banda requerido para una llamada con *codec* G.729 (con rata de muestreo de 8 kbps) con cRTP, MP, y la carga default de 20 bytes por paquete de voz, quedaría como sigue:

- Tamaño total del paquete = (cabecera de MP de 6 bytes) + (cabecera de IP/UDP/RTP compresa de 2 bytes) + (carga de voz de 20 bytes) = **28 bytes.**

- Tamaño total de paquete (bits): (28 bytes)*8 bits por byte = **224 bits.**

- PPS = (8 kbps rata de muestreo del codec)/(160 bits) = **50 pps.**

  Nota: 160 bits = 20 bytes (carga default de la voz)*8 bits por byte.

2.10.3 Requerimiento de QoS para video.

Los requerimientos para la transmisión de video, como IP *multicast*, transmisiones ejecutivas y actividades de entrenamiento en tiempo real, son los siguientes:

- De cuatro a cinco segundos de latencia son permitidos (dependiendo de las capacidades de buffer de la aplicación de video). No hay requerimientos significativos de *jitter*.

- 2 % de pérdida de paquetes es permitido. Ancho de banda depende de la codificación y la rata de transmisión del video.

- La distribución del contenido de video como el video por demanda son replicados para distribuir el contenido de los *engines*.

- Insensible al *Delay* y al *Jitter*.

- Transferencia grande de archivos (patrones de tráfico similar a las sesiones de FTP).

- Restricción a la distribución para las horas con menor tráfico durante el día.

- Aprovisionamiento de datos como menor-a-*best-effort*.

Los requerimientos para video conferencias pueden ser aplicables ya sea como la modalidad uno a uno o una conferencia de multipuntos.

- ≤ 150 ms de latencia en un sentido desde la boca a la oreja (para el estándar ITU G.114).

- ≤ 30 ms *jitter*.

- ≤ 1 de pérdida de paquetes.

- Mínimo de ancho de banda garantizado para la sesión de video conferencia + un 20 %. por ejemplo, una sesión de video conferencia de 384 kbps requiere un ancho de banda con prioridad garantizada de 460 kbps.

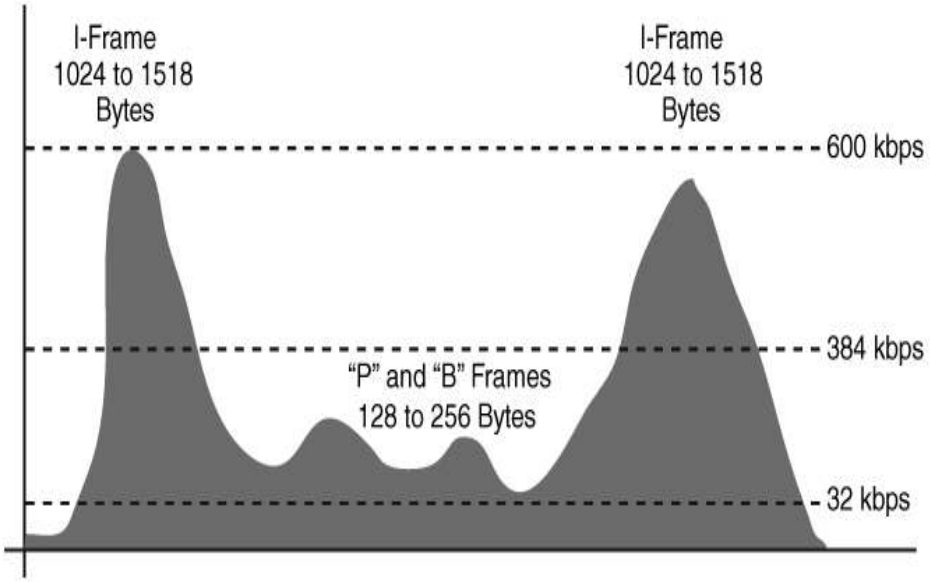
Las tramas I son muestras de trama completa, mientras que las tramas P y B son diferenciales (o delta). Las videoconferencias comparten la misma latencia, *jitter* y pérdida de paquetes como los requerimientos de la voz, pero tiene un *burst* más radical y un patrón de tráfico más pesado.

Un *stream* de 384 kbps puede tomar hasta 600 kbps en ciertos puntos en lugar de aprovisionar el *stream* + 60 % (para acomodar el *burst* ocasional de 600 kbps). El *stream* de video incluye un ancho de banda adicional de 20% con un *burst* permitido en el LLQ de 30,000 bytes por cada *stream* de 384 kbps, como se muestra en la figura de abajo.

- Aprovisionamiento de *stream* LLQ + 20%. por ejemplo, un *stream* de 384 kbps es un *stream* de 460 kbps en LLQ.

- Adicionalmente, el LLQ extiende el *burst* para capturar las tramas I sin requerir reservar ancho de banda adicional.

Figura 10: Figura del consumo de las tramas I, B y P, secuencia de un *stream* de video



Fuente: *Selecting* MPLS VPN *Services*, por Chips Lewis, Steve Pickavance. Cisco *Press, Networking Technology*.

2.10.4 Requerimientos de QoS para datos.

Acerca de la identificación de tráfico, hay algunos puntos claves que se deben recordar acerca de la clasificación del tráfico de datos:

- Perfiles de aplicaciones para tener un entendimiento básico de los requerimientos de la red. Presentar una planificación de la capacidad para asegurar que se cuenta con un ancho de banda adecuado.

- Usar no más de 4 clases de tráfico de datos:
  - Datos Transaccionales (misión crítica): ERP, transaccional, y aplicaciones internas de alta prioridad.
  - *Bulk* data (ancho de banda garantizado): *stream* de video, mensajería e intranet.
  - *Best Effort* (la clase default): navegación en *Internet, e-mail* y aplicaciones sin clasificar.
  - *Scavenger* (menor que *best effort*): FTP, backups, aplicaciones no críticas.

- Minimizar el número de aplicaciones asignadas a el tipo de datos usados en las clases Transaccional y *bulk* (tres o menos son recomendables).

- Usar políticas de aprovisionamiento proactivas antes de utilizar políticas reactivas.

Estos requerimientos para las clases de datos son únicamente lineamientos. Se debe de tomar en cuenta muchos factores diferentes, incluyendo el proveedor de servicio. Ellos deben de ser capaces de soportar las diferentes clases requeridas por la empresa que lo contrata. Así como, pueden afectar el proceso de decisión en la creación de políticas.

El gobierno juega un papel clave a la hora de identificar y clasificar las aplicaciones. Al construir un punto de chequeo del gobierno en el desarrollo de nuevas aplicaciones, muchos ciclos pueden ser reducidos al determinar las necesidades de ancho de banda y su impacto en los requerimientos de red. El proceso puede ser la punta de lanzamiento ya sea para nuevas aplicaciones que conlleven a cualquier avance en las redes o para determinar las bases para aplicaciones, que puede llevar a un plan predictivo o a un plan incremental anual de añadir las aplicaciones a la red. Permite para una mejor planeación, remover el reto que puede ser creado debido a los cuellos de botella o asuntos de escalamiento, y el administrador clave de la red como un asunto de tipo empresarial.

Un factor crítico en la entrega del Proveedor de Servicio es el SLA, afectando la habilidad de soportar clases sensitivas al *delay*, como lo visto en los requerimientos de la voz y el video. En algunos casos, otros factores dificultan la habilidad del SP de entregar el nivel acordado de servicio, entre estos puede estar la ubicación geográfica de los sitios y las interconexiones a través de la red del proveedor de servicio.

Por ejemplo, supongamos que tenemos un sitio en un lugar geográficamente remoto que tiene un *delay* muy grande debido a su distancia. Puede que no sea posible cumplir con los requerimientos para la entrega de los servicios de tiempo real para este sitio. En dicho caso, hay una compensación entre lo que es posible para la mayoría de los sitios corporativos y los sitios remotos y su capacidad de interconexión con el resto de la red.

3. OPERACIÓN DE LAS MPLS VPN'S

3.1 VPN *routing y forwarding tables* (VRF's)

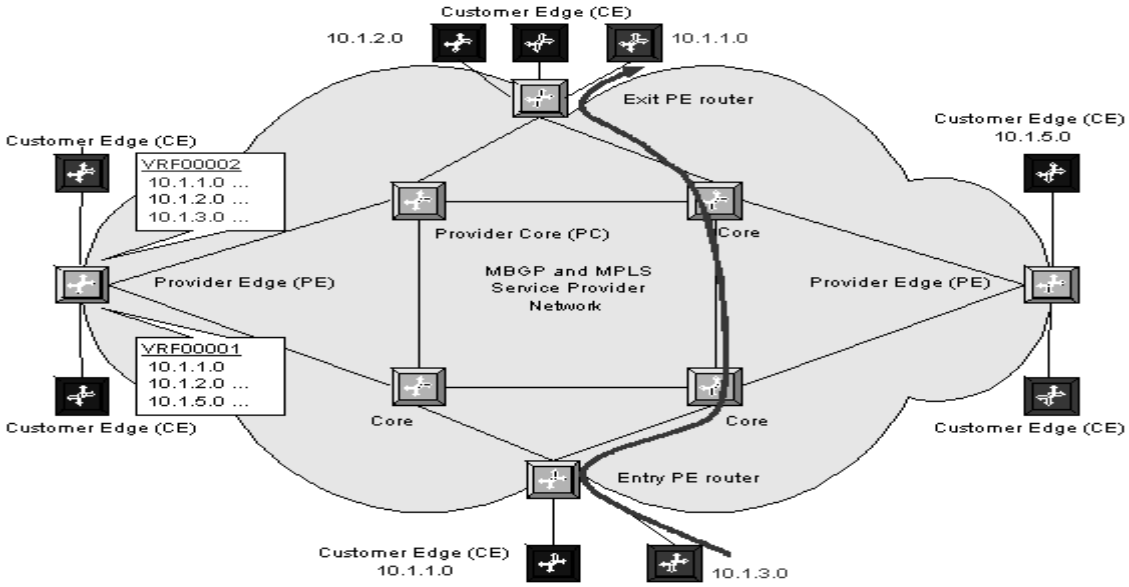
Las tablas de ruteo y reenvío virtuales (VRF) es una tecnología incluida en las redes IP que permite que múltiples casos de tablas de ruteo existan en un mismo enrutador y trabajen simultáneamente. Esto incrementa la funcionalidad al permitir que los caminos de red sean segmentados sin el uso de múltiples equipos. Debido a que el tráfico es segregado automáticamente, la VRF incrementa la seguridad de la red y puede eliminar la necesidad de encriptación y autenticación.

Los Proveedores de Servicios de Internet (ISP) a menudo toman ventaja de las VRF para crear redes privadas virtuales (VPN) separadas para los clientes, además la tecnología es también referida como VPN de ruteo y reenvío.

Las VRF actúan como enrutador lógico, pero mientras el enrutador lógico puede incluir muchas tablas de ruteo, el caso de la VRF usa solo una tabla de ruteo. En adición, la VRF requiere una tabla de ruteo que designe el siguiente salto para cada paquete de información, una lista de reglas y protocolos de ruteo que digan como será reenviado el paquete.

Estas tablas previenen que el tráfico sea reenviado afuera de los caminos específicos de las VRF y también mantienen alejado el tráfico que debe de estar afuera del camino de la VRF. La imágen de abajo sirve de ejemplo de la utilización de las VRF's.

Figura 11: Ejemplo del uso de VRF's.



Fuente: BGP *and* MPLS-*Based* VPNs. Peter J. Welcher. NetCraftsmen

En la figura vemos algunos ejemplos de cómo podemos asociar las VRF's con las interfaces de un enrutador PE. La VRF llamada *VRF00001* contiene las rutas de los otros sitios azules (sub redes). La VRF llamada *VRF00002* contiene las redes de color rojo y también una subred de la VPN azul. Un mapeo de rutas puede ser usado para proveer un control más fino sobre cuales rutas azules son importadas a la *VRF00002*.

Supongamos que somos un ISP y que nuestro número AS es el 888. para el cliente A, vamos a crear una VRF llamada vrf00001 y la asociaremos con el Descriptor de Ruta 888:1 (abreviación para dos bytes que son 888 en decimal, seguido por seis bytes terminando en 1). También importaremos y exportaremos rutas para la comunidad extendida 888:1, es decir, otros sitios de la intranet en esta VPN. Para otro cliente, Cliente B, crearemos la VRF llamada vrf00002 con RD 888:2. Ésta segunda VRF importará y exportará en la comunidad extendida 888:2, otros sitios en la intranet del Cliente B. Así mismo, también importaremos rutas de la comunidad extendida 888:1 de acuerdo al mapa de ruteo llamado vrf00002-import-map, así el sitio que esté usando la

VRF vrf00002 pueda alcanzar los sitios seleccionados del Cliente B, como un socio de la extranet.

Para realizar lo anterior, configuramos lo siguiente, en un enrutador Cisco:

```
ip vrf vrf00001
 rd 888:1
 route-target both 888:1

ip vrf vrf00002
 rd 888:2
 route-target both 888:2
 route-target import 888:1
 import map vrf00002-import-map

route-map vrf00002-import-map permit 10
```

Es importante hacer notar que la tabla de ruteo solo es necesaria para ajustes finos. Las importaciones/exportaciones normales se pueden realizar simplemente con las comunidades extendidas. En cuanto a la seguridad, la seguridad básica se proporciona a nivel de las comunidades extendidas, haciendo que la ruta oculte la situación normal. Entonces los mapas de ruteo se pueden utilizar para limitar conectividad a los sitios del cliente de la extranet si los clientes no desean hacer eso por sí mismos por el BGP en los enrutadores del PE.

Estas VRF's estarán típicamente asociadas con interfaces:

```
interface Fastethernet 0/2
 ip vrf forwarding vrf00001
 ip address ...

interface Fastethernet 0/3
 ip vrf forwarding vrf00002
 ip address ...

interface Fastethernet 0/4
 ip vrf forwarding vrf00002
 ip address ...
```

La VRF vrf00002 está asociada con dos interfaces que conectan a dos sitios del Cliente B. Se muestran deliberadamente interfaces Fast Ethernet, porque mucha gente piensa que de esta forma se conectan a la red de los Proveedores de Servicio.

3.2 Configuración de enrutadores, basados en MPLS VPN's

Esta parte describe de forma resumida los principales comandos de configuración de un enrutador Cisco para la creación de redes VPN con topología de acoplamiento completo (*Full-Mesh)* en un dominio MPLS.

El encaminamiento entre los equipos de cliente (CE) y los equipos del proveedor (PE) se realiza de forma dinámica mediante OSPF. Se supone que los equipos CE han sido correctamente configurados, ofreciendo en la interfaz de interconexión a la troncal un área cero OSPF, y que han sido configurados como parte de un sistema OSPF multi-área.

La configuración de equipos con funcionalidad PE en VPNs sobre MPLS requiere los siguientes pasos en cada uno de los enrutadores con funcionalidad "PE":

.1 Configuración de la VRF asociada a la VPN que vamos a configurar en los enrutadores con funcionalidad "PE"

Una VRF (*VPN routing and forwarding)* incluye las tablas de envío y encaminamiento de los sitios pertenecientes a una VPN. Los parámetros necesarios para crearla son:

• Identificador de Rutas (*Route Distinguisher* RD) que permite identificar unívocamente un prefijo de VPN-IPv4.

• Ruta destino (*Route-Target* RT) que identifica las VFR en las que se instalan las rutas.

cisco# configure terminal
cisco (config)# ip vrf <nombre de la VRF>
cisco(config-vrf)# rd <valor del rd>
cisco(config-vrf)# route-target export <valor que tiene que exportar>
cisco(config-vrf)# route-target import <valor que tiene que importar>

El siguiente comando unifica en uno solo los dos últimos, para indicar que el enrutador donde se ejecuta debe exportar e importar la misma ruta destino.

cisco(config-vrf)# route-target both <valor que tiene que importar y exportar>

2. Configuración del "direccionamiento" en las interfaces de los enrutadores "PE" que están relacionadas a los enrutadores "CE":

La configuración a aplicar es la siguiente:

cisco# configure terminal
cisco(config)# interface <nombre de la interfaz>
cisco(config-if)# ip vrf forwarding <nombre de la VRF>

3. Reasignación de la dirección IP a la interfaz donde acabamos de configurar el "*direccionamiento*":

Esto se hace dentro de la VPN, ya que pierde el direccionamiento de dicha interfaz. Después de ejecutar este último comando se mostrará un mensaje indicando que

en la interfaz anterior se le ha quitado la configuración IP, por lo que habrá que volver a configurarla:

cisco(config-if)# ip address <dirección IP> <máscara>

4. Configuración del encaminamiento dinámico en la VRF creada:

Hay que arrancar un nuevo proceso OSPF dedicado al encaminamiento dentro de la VRF:

cisco# configure terminal
cisco(config)# enrutador ospf <identificador del proceso> vrf <nombre VRF>

Definir el área en la que se encuentran las interfaces pertenecientes a la VPN:

cisco(config-enrutador)# network <red> <wildcard> area 0

Por ejemplo:

cisco(config-enrutador)# network 192.168.43.52 0.0.0.3 area 0

5. Configuración de iMBGP:

Para que los prefijos aprendidos puedan ser transmitidos a los otros equipos PE, hay que configurar iMBGP siguiendo los siguientes pasos:

- Comprobar que los vecinos iBGP siguen activos y operativos. Utilizar el comando:

Show ip bgp summary.

- Nos metemos en la configuración de BGP del enrutador:

cisco# configure terminal
cisco(config)# enrutador bgp <número de proceso BGP que esté configurado>

- Entramos a configurar iMBGP para la VPN:

cisco(config-enrutador)#address-family vpnv4

- Hay que activar los vecinos existentes con la nueva funcionalidad. Según se vayan ejecutando los comandos siguientes se irán reseteando las sesiones BGP, este comportamiento es normal porque los vecinos vuelven a negociar sus capacidades. Hay que configurar para cada vecino iBGP mostrado con el comando ***show ip bgp summary*** lo siguiente:

cisco(config-enrutador-af)# neighbor <dir IP del vecino iBGP> activate
cisco(config-enrutador-af)#neighbor <dir IP del vecino iBGP> send-community both

6. Configuración del envío de los prefijos aprendidos al resto de los equipos con funcionalidad PE.

Una vez establecidas las sesiones iMBGP con el resto de equipos PE y verificada la conectividad local con los integrantes de la VPN, queda pendiente propagar los prefijos locales al resto de equipos PE para que éstos sepan encaminar los paquetes hacia dichos prefijos. Para ello, bastará con redistribuir OSPF en el iMBGP:

cisco# configure terminal

cisco(config)# enrutador bgp <número de proceso BGP que esté configurado>
cisco(config-enrutador)# address-family ipv4 vrf <nombre del VRF>
cisco(config-enrutador-af)# redistribute ospf <identificador del proceso OSPF> vrf <nombre del VRF>

NOTA: El identificador del proceso OSPF se corresponde con el identificador del proceso OSPF que hemos utilizado para configurar el encaminamiento dinámico en la VRF en el paso 4. Conviene resetear las sesiones IMBGP con el comando:

*cisco# clear ip bgp **

7. Configuración del envío de los prefijos aprendidos a los equipos con funcionalidad CE:

Esto lo logramos al ejecutar la siguiente configuración:

cisco# configure terminal
cisco(config)# enrutador ospf <identificador del proceso OSPF> vrf <nombre del VRF>
cisco(config-enrutador)# redistribute bgp <número de proceso BGP que esté configurado> subnets metric 20

8. Verificación del funcionamiento de la VPN-MPLS

Con los siguientes comandos, ejecutados en un enrutador PE, podremos verificar que la VPN que hemos configurado está funcionando según lo esperado:

1. *show ip route vrf <nombre VRF>*

Con este comando podremos comprobar los prefijos que se han exportado y los que se han importado en la tabla de ruteo de la VRF y por ende los prefijos que formarán parte de la VPN.

2. *traceroute vrf <nombre VRF> <Dirección a la que queremos llegar>*

El funcionamiento de este comando es exactamente el mismo que el de un trazador de rutas normales, pero para comprobar el funcionamiento de la VPN y usando direcciones destino de la propia VPN, con origen un equipo que pertenezca a la misma VPN necesitamos añadir el parámetro *vrf* junto al nombre de la vrf que pertenece a nuestra VPN.

3. *ping vrf <nombre VRF> <Dirección a la que queremos llegar>*

El funcionamiento es exactamente el mismo que el de un ping normal, la explicación del uso del parámetro vrf se aplica exactamente igual que en el comando anterior.

3.3 VPN's basadas en IPSEC

El protocolo IPSec es un stándar de la IETF que brinda un esquema de trabajo para las VPNs de capa 3 basadas en CPE. Para proteger los datos mientras viajan a través de la red pública o dentro de una red privada, IPSec soporta una combinación de las siguientes funciones de seguridad de red:

- Confidencialidad de datos: encriptación de los paquetes antes de transmitirlos.

- Integridad de datos: autentica paquetes para asegurarnos que los datos no son alterados mientras se transmiten.

- Autenticación de los datos de origen: con esto se autentica la fuente de los paquetes recibidos en conjunto con la integridad de los servicios de datos.

- Anti repetición: detecta paquetes duplicados o con mucho tiempo, los rechaza para evitar ataques por repetición.

El estándar IPSEC también define nuevos formatos de paquetes, tales como la encapsulación de seguridad de carga útil (*ESP por sus siglas en inglés*), para la confidencialidad, ESP soporta cualquier tipo de encriptación simétrica, incluyendo la estándar 56-bit *Data Encryption Standard* (*DES por sus siglas en inglés*), la más segura Triple DES (3DES), y la emergente *Advanced Encryption Standard* (AES). Los parámetros de IPSec son comunicados y negociados entre los equipos de la red de acuerdo al protocolo de intercambio de llave de Internet (*Internet Key Exchange* IKE).

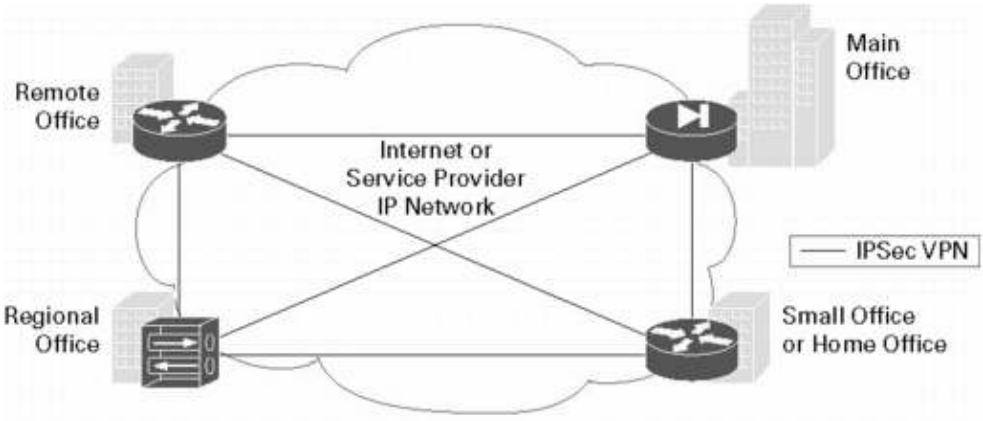
El protocolo IPSec brinda protección a los paquetes IP al permitir a los diseñadores de la red especificar el tráfico que necesita protección, define la manera en que el tráfico será protegido, y controla quien puede recibir el tráfico. Las VPNs IPSec reemplazan o aumentan las redes privadas existentes basadas en las infraestructuras WAN tradicionales tales como las líneas dedicadas, *Frame Relay* y ATM. Estos llenan los mismos requerimientos que las alternativas WAN incluido el soporte para múltiples protocolos. La ventaja de IPSec es tal que llena los requerimientos de red a un menor costo y con gran flexibilidad en el uso de las tecnologías de transporte más usadas: el servicio de Internet público y los servicios de los proveedores con redes basadas en IP.

Cuando la empresa contrata a alguien para que provea el servicio de IPsec VPN, los proveedores de servicio configuran típicamente el IPsec en una topología de estrella, donde todas las ramas mantienen una conexión punto a punto con el *hub, switch* o el punto central. IPSec soporta inherentemente IP *unicast*. Las empresas que necesitan

otros protocolos capa 3, como IPX, Voip pueden usar túneles sobre IPSec con la encapsulación de ruteo genérico (GRE). IPSec puede ser utilizado para las VPNs de tipo sitio-sitio y también para las de acceso remoto.

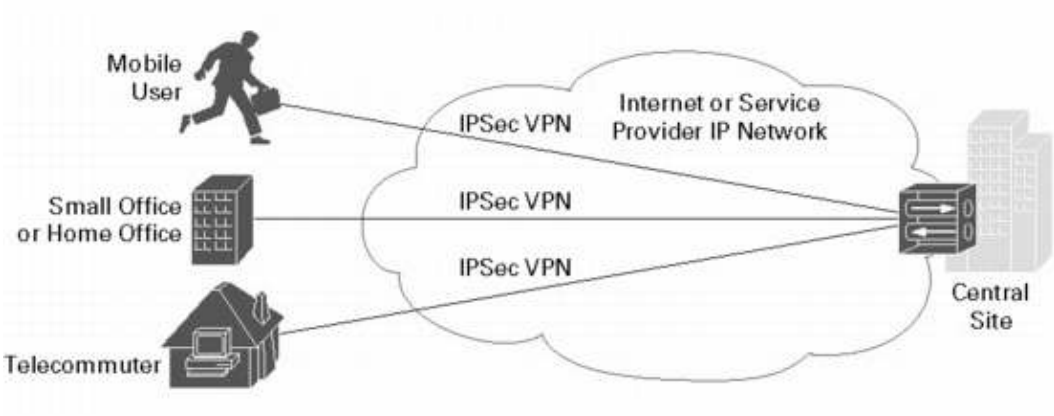
A continuación vemos ejemplos gráficos de IPSec:

Figura 12: Ejemplo de una IPSec sitio-sitio



Fuente: Cisco *white paper, Managed* VPN - *Comparison of* MPLS, IPSec, *and* SSL *Architectures*

Figura 13: Ejemplo de una IPSec de acceso remoto



Fuente: Cisco *white paper, Managed VPN - Comparison of MPLS, IPSec, and SSL Architecture*s

3.3.1 Indicadores que IPSec es una buena opción:

Los siguientes factores nos ayudarán a determinar cuándo usar IPSec.

- Las empresas que necesiten medidas de seguridad tales como la encriptación de datos o autenticación de usuarios y equipos. IPSec provee mucha seguridad más alla de la separación de tráfico de la red, ya sea MPLS, *Frame Relay* o ATM. Las empresas que eligen la arquitectura de VPN MPLS por su escalabilidad y el soporte de QoS algunas veces usan IPSec para aumentar la ayuda en cuanto a las funciones de seguridad, tales como encriptación de datos.

- Las consideraciones de costos son importantes. Una IPSec VPN puede implementarse en una red IP existente, evitando los gastos de operación de construir una nueva red.

- Cuando la empresa necesita extender sus recursos de red corporativa a trabajadores dispersados geográficamente o a trabajadores que se mantienen viajando.

- La implementación rápida es importante debido a que se pueden agregar nuevos sitios para extender una red o agregar un nuevo sitio. IPSec ahorra tiempo porque requiere pocos cambios en la infraestructura de red existente.

- El flujo de tráfico sigue la topología estrella, es decir todos los puntos tienen conectividad entre sí.

Veamos en cuanto a la experiencia se refiere, como varía la forma en que utilizamos el tipo de VPN, ya sea del tipo de Acceso Remoto o del sitio a sitio, a continuación se verá una breve descripción de ambos.

Acceso remoto: típicamente, el usuario llama al cliente del software de la VPN y selecciona el destino apropiado, tal como un nombre de anfitrión o un dirección IP. Sobre esta disposición de la autentificación y del túnel de IPSec, los usuarios pueden tener acceso remoto a sus aplicaciones aunque estas están limitadas a la IP o el nombre del anfitrión al que están conectándose, mientras que de sus oficinas IPSec permite el acceso a casi todas las aplicaciones dentro de la lan, sin ninguna modificación al sitio o al cliente conectado.

Sitio a Sitio: para este tipo de conectividad a través de VPN IPSec, los usuarios no necesitan tener software instalado en sus computadoras, en lugar de esto, los usuarios en una rama de la oficina lanzan una aplicación como si esta residiera localmente. Un enrutador IPSec-habilitador VPN permitido en una rama de oficina, inicia automáticamente una sesión IPSec con la sede central. Sobre la negociación y la autenticación acertadas de la sesión, un túnel seguro de VPN es establecido entre la rama y la sede central, sin ninguna acción por parte del usuario.

3.3.2 Fortalezas del IPSec:

Las principales fortalezas de las VPN basadas en IPSec son:

- Internet de bajo costo puede ser usado para el transporte de la red.
- Características de seguridad como la autenticación de usuarios, confidencialidad de los datos e integridad. Los usuarios son autenticados con certificados digitales o con claves de seguridad. Los paquetes que no cumplen con las políticas de seguridad son descartados.

- Trabajadores móviles pueden conectarse a la IPSec VPN desde cualquier sitio geográfico a través de la conexión de Internet.

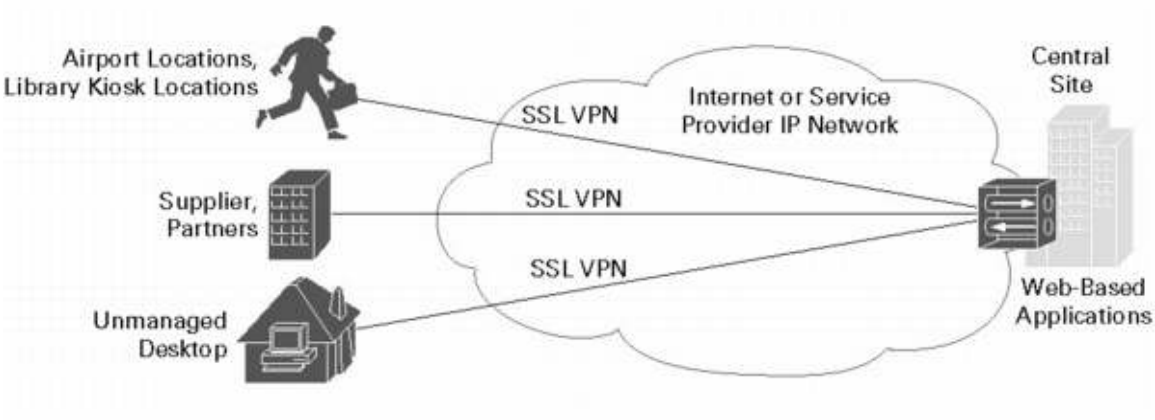
- Facilidad de implementación, no se requiere de la intervención de un proveedor de servicio para establecer la VPN, de igual forma, muchas empresas optan por contratar a un Proveedor del Servicio para aprovechar las ventajas de la experiencia de estos en la entrega de este tipo de servicio a nivel regional o nacional, para reducir costos, acelerar la entrega del servicio y minimizar los riesgos.

- Reducción de congestión en el *Hub* central cuando se configura un "*split tunneling"*, lo que quiere decir que un cliente remoto de la VPN puede direccionar el tráfico de Internet directamente en lugar de pasar por el túnel IPSec, y establecer el túnel únicamente con el tráfico relacionado al de la VPN. Esto reduce la congestión en el *hub*.

3.4 VPN's basadas en SSL (*secure sockets layer*)

SSL es una alternativa emergente de IPSec para las VPNs de acceso remoto. No está diseñada para VPNs de sitio a sitio. SSL provee acceso a las aplicaciones de acceso basadas en la web desde cualquier lugar que tenga un buscador y conexión a Internet, y sin ningún software especializado para los clientes. Provee seguridad en la conexión por medio de autenticación de los clientes que se comunican y encriptando el tráfico que intercambian. Debido a que SSL opera en la capa de sesión, funciona únicamente para aquellas aplicaciones codificadas por SSL, así como los buscadores y el mail basado en la web. Las VPNs basadas en SSL no soportan aplicaciones que no hayan sido codificadas por SSL, incluyendo a los clientes con e-mail convencional, telnet, FTP, Telefonía IP, aplicaciones de multidifusión y aplicaciones que requieran QoS.

Figura 14: Ejemplo de una VPN SSL de acceso remoto



Fuente: Cisco *white paper, Managed* VPN - *Comparison of* MPLS, IPSec, *and* SSL *Architectures*

Una ventaja de SSL como solución de VPN de acceso remoto es que no requiere ningún software especial más que un buscador de la red (Internet Explorer, Mozilla Fire Fox, Safari, etc). Además de esto, el proveedor de servicio puede brindar control de acceso granular, limitando a usuarios individuales el acceso a páginas web específicas u otros recursos internos. Los requerimientos de las VPNs basadas en SSL incluyen proxys de aplicación debido a que SSL necesita estar al tanto de cada conexión individual o sesión de aplicación. Además de esto, la central necesita una memoria adecuada para mantener todas las conexiones de las aplicaciones individuales. Debido a la encriptación de SSL, el servidor debe de contar con un procesador y memoria adecuada, para no volverse un cuello de botella.

La mayoría de empresas ven a las VPN basadas en SSL como una mejora de IPSec para el acceso remoto, no como un reemplazo. Su simplicidad en la implementación y manejo de los clientes remotos lo hacen una buena alternativa para la conectividad de las VPN cuando la empresa no tiene el control del cliente remoto. Cuando las empresas utilizan ambas, SSL y IPSec para sus VPNs, generalmente usan SSL para proveer acceso a clientes por un tiempo limitado hacia las aplicaciones web de las computadoras de casa o de las que no tienen gestión, así como aeropuertos o kioscos

y cafés Internet y utilizan IPSec para el acceso remoto de las computadoras manejadas por la corporación para proveer acceso total de la red, dando a los usuarios la misma experiencia como que si estuvieran en la misma oficina.

Estas son las siguientes consideraciones que nos pueden ayudar a determinar que SSL es la mejor opción:

- Conexiones originadas desde un buscador de la Web.
- Cuando el departamento de IT tiene limitado o no tiene el control del sistema remoto o el software del cliente, como en el caso de un socio o cliente.
- Acceso remoto que requiera acceso limitado a los recursos de red de la compañía, sin acceso total a la red.

Los usuarios que están acostumbrados a acceder a las aplicaciones vía un buscador, no notarán ninguna diferencia cuando SSL ha sido añadido a la red. Los usuarios que accedan sin un buscador dependen de Activex o Java Applet para acceder a las aplicaciones.

Las fortalezas de SSL para un acceso remoto seguro son las siguientes:

- Bajo costo de entrenamiento, SSL cuenta con mucho soporte en páginas web comerciales.
- Soporte para los métodos de autenticación actuales y planificados entre el Server y el software del usuario, así como soporte a las aplicaciones SSL son apoyados por los métodos existentes de autenticación, así como los métodos de autenticación que utilizan certificados digitales.

- Provee acceso desde cualquier punto utilizando un buscador desde cualquier PC: puede ser desde un café Internet, puntos de acceso WiFi, desde redes de otras empresas, desde cualquier computadora con acceso a Internet.

- Reduce interoperabilidad de la red porque el protocolo utilizado es el mismo para las transacciones seguras de la web, una VPN SSL funciona desde cualquier lugar con un buscador de red, incluyendo ambientes de negocio-a-socios y a través de los servidores proxy, sin ningún cambio a la infraestructura de seguridad.

- Debido a que el software del cliente ya viene dentro de los buscadores de red, no hay necesidad de instalar nuevos software de VPN.

3.5 Comparación de la arquitectura de las IP VPN:

La siguiente tabla muestra las ventajas y limitaciones de los servicios a manejar en las tres opciones de arquitectura: MPLS, IPSec y SSL.

Tabla III: Comparación de VPNs

	VPN Basada en MPLS	**VPN Basada en IPSec**	**VPN Basada en SSL**
Topología	Sitio-a-Sitio VPN: *Hub-and-spoke o full-mesh*	Sitio-a-Sitio VPN: principalmente *hub-and-spoke*	VPN de acceso remoto.
Seguridad **Autenticación de sesión.**	Establece una membrecía durante el aprovisionamiento, basada en un Puerto lógico y un descriptor de ruta	Autentica a través de certificados digitales o de claves pre-compartidas. Bota los paquetes que no llenen	Autentica a través de certificados digitales.

	único. Define el acceso a los servicios de VPN de grupo durante la configuración, rechaza todo acceso no autorizado.	las políticas de seguridad.	
Confidencialidad	Separa el tráfico, que alcanza los mismos resultados que en una red ATM o *Frame Relay.*	Utiliza Fuentes flexibles de mecanismos de encriptación y *tunneling* en la capa de red.	Encripta el tráfico utilizando Infraestructura de Llave Pública (PKI).
QoS and SLAs	Permite SLAs con un mecanismo de QoS escalable y robusto; así como capacidad de ingeniería de tráfico.	No utiliza QoS y SLAs directamente, sin embargo hay algunas aplicaciones que permiten clasificar el tráfico dentro de un túnel IPSec.	No aplicable.
Escalabilidad	Altamente escalable, ya que no requiere un *peering* sitio a sitio, es capaz de soportar muchas VPNs a través de la misma red.	Aceptable escalabilidad sobre todo en las configuraciones del tipo hub-and-spoke, la escalabilidad se vuelve un reto para la entrega de IPSec VPNs muy grandes del tipo *full-meshed.*	No aplicable
Administración **Soporte sitio a sitio.**	Sí	Sí	Sí
Soporte de Acceso Remoto	Sí, si es usado en conjunto con IPSec	Sí	Sí
Aprovisionamiento	Requiere de una sola vez el aprovisionamiento de los equipos del	Reduce los costos operacionales a través del aprovisionamiento de redes centralizadas	No Aplicable.

	usuario de del lado del proveedor para habilitar el sitio como miembro de un grupo VPN de MPLS.	para la oferta de servicios CPE. Utiliza el aprovisionamiento centralizado para ofrecer servicios basados en red.	
Entrega de Servicio	Requiere elementos de red basados en MPLS en la red *core* del proveedor de servicio.	Puede ser implementada a través de cualquier red IP existente o a través del Internet.	No Aplicable.
Cliente VPN	No es requerida porque las VPN MPLS es una red basada en el servicio VPN.	Es necesario para los clientes IPSec VPN.	No requerido, se usa el buscador de red.
Sitio de la Red	En la red *Core* del ISP	Local *loop, edge*, y fuera de la red.	Local *loop, edge*, y fuera de la red.
Transparencia	Reside en la capa de Red, transparente a las aplicaciones.	Reside en la capa de Red, transparente a las aplicaciones.	Reside en la capa de sesión, trabaja solo con aplicaciones codificadas para SSL.

3.6 Enlace de datos:

Definamos la palabra enlace como un conjunto de medios utilizados para transmitir entre 2 puntos designados una señal digital que tiene una velocidad binaria nominal especificada. El conjunto de 2 estaciones de trabajo de datos que están controlados por medio de un protocolo de enlace y del circuito de datos de interconexión que habilita los datos a transferir desde una fuente de datos a un destino de datos, también puede definirse como la conexión física y los protocolos de conexión entre unidades que intercambian datos a través de una línea de telecomunicaciones.

Un Proveedor de Servicios es el encargado de unir los puntos remotos o subsedes de un negocio, hay varias topologías que se pueden ofrecer, entre estas tenemos dos que son las más utilizadas y que describimos a continuación:

3.6.1 Enlaces centralizados:

Este tipo de enlace reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central. Cuando se aplica a una red basada en esta topología, este concentrador central reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto.

La desventaja radica en la carga que recae sobre el nodo central. La cantidad de tráfico que deberá soportar es grande y aumentará conforme vayamos agregando más nodos periféricos, lo que la hace poco recomendable para redes de gran tamaño. Además, un fallo en el nodo central puede dejar inoperante a toda la red. Esto último conlleva también una mayor vulnerabilidad de la red, en su conjunto, ante ataques.

En cuanto al ruteo, se hace más fácil agregar otros nodos, ya que solo necesitamos poner una ruta por defecto a todos los nodos para que cualquier red la encuentren a través del enrutador central, y en el erutador central se agrega la red del nuevo nodo y una ruta hacia la interface donde la vamos a conocer.

3.6.2 Enlaces tipo malla:

La topología en malla es una topología de red en la que cada nodo está conectado a uno o más de los otros nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada enrutador tiene sus propias conexiones con todos los demás enrutadores.

El establecimiento de una red de malla es una manera de encaminar datos, voz e instrucciones entre los nodos. Las redes de malla se diferencian de otras redes en que las partes de la red (nodo) están conectadas unas con otras por uno u otro camino, mediante conexiones separadas. Esta configuración ofrece caminos redundantes por toda la red, de modo que si falla una conexión, otro se hará cargo del tráfico.

Esta topología, a diferencia de otras *(como topología en árbol y topología en estrella),* no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento *(un error en un nodo, sea importante o no, no implica la caída de toda la red)*.

Las redes de malla son autoregenerables: la red puede funcionar incluso cuando un nodo desaparece o la conexión falla, ya que el resto de nodos evitan el paso por ese punto. Consecuentemente, se forma una red muy confiable, es una opción aplicable a las redes sin hilos (*Wireless*), a las redes con cable (*Wired*), y a la interacción del software.

Una red con topología en malla ofrece una redundancia y fiabilidad superiores. En una topología en malla, cada equipo está conectado a todos los demás equipos. Aunque la facilidad de solución de problemas y el aumento de la fiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que el Proveedor de Servicio tiene que crear una conexión para cada punto hacia los demás.

Estos dos escenarios son los que llenan las expectativas de los clientes, dependiendo de sus necesidades, en ambos casos es necesario utilizar enrutadores en cada punto, y este es un punto que hace estos tipos de enlaces costosos.

3.7 Topologías de redes privadas virtuales en MPLS:

Existen varios tipos de VPN's basados en la arquitectura de MPLS, las cuales son muy flexibles en términos de implementar diferentes modelos de conectividad IP entre los sitios del cliente, son varias las topologías de VPN que se pueden crear con la configuración de VRF's y específicamente con los atributos de rutas de destino en una manera apropiada. A continuación describimos algunas de las topologías:

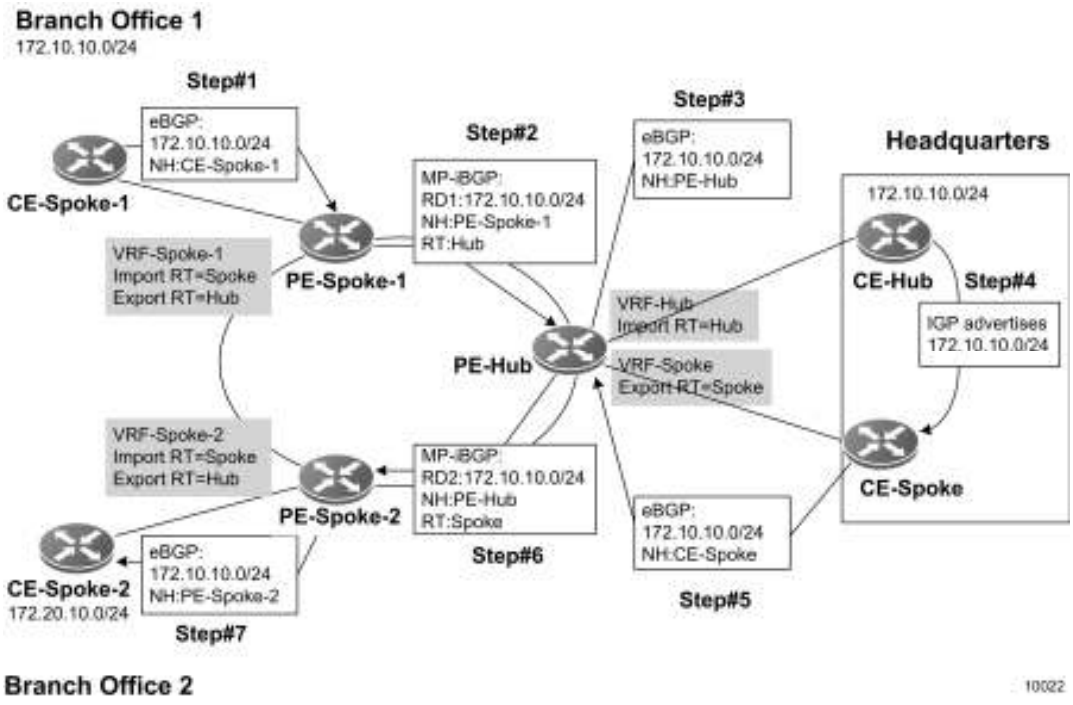
3.7.1 VPN de acoplamiento completo (*full mesh*):

En este tipo de topología todos los sitios tienen conexión directa con los demás a través de una red en común. Este tipo de topología es la más simple de implementar. La implementación es de tal manera que todas las VRF's que se utilicen para esta topología son configuradas con las mismas Rutas de Destino de importación y exportación.

3.7.2 Topología *hub-and-spoke*:

En este tipo de topología, los sitios (*spoke)* no pueden comunicarse directamente uno con otro, pero lo pueden hacer a través del sitio *Hub*. Todo el tráfico de los sitios *spoke* que está destinado para el sitio *hub* o para un sitio interno, debe de fluir a través del sitio *hub*. La figura de abajo representa una implementación básica de la topología *Hub* and *Spoke* en donde hay algunas redes de acceso de Capa 1 y Capa 2 y enrutadores PE y CE. La figura muestra dos enrutadores CE en el sitio del *Hub*. Es también posible tener solo un enrutador CE con dos interfaces hacia el enrutador PE.

Figura 15: Ejemplo de una VPN *Hub and Spok*e.



Fuente: Tellabs 8000 *Manager Online Documentation.*

Explicación de la gráfica:

1. Primero el equipo CE-*Spoke*-1 muestra su prefijo al equipo PE-*Spoke*-1.

2. Con la finalidad de distribuir las rutas al PE-*Hub*, PE-Spoke-1 utiliza MP-iBGP y añade RT con el valor "*hub*" para el mensaje nuevo BGP.

3. Note que el PE-*Hub* tiene dos VRFs. la que está configurada para importar RT=*Hub* da la ruta y la muestra al enrutador CE-*Hub*, que está conectado a la interface que está asociada a la VRF-*Hub*.

4. EL IGP en el sitio *Hub* distribuye la ruta al enrutador CE-*Spoke*.

5. El enrutador CE-*Spoke* informa de la ruta al enrutador PE-*Hub*, y la ruta es ahora puesta a la VRF-*Spoke*.

6. El enrutador PE-*Hub* utiliza RT=*Spoke* cuando distribuye las rutas.

7. PE-*Spoke*-2 obtiene la ruta y la instala a la VRF y le informa al CE-Spoke-2 de la ruta. Desde el punto de vista del CE-Spoke-2, la rama de la oficina 1 es ahora alcanzable a través de las oficinas centrales (*Headquarters* en la figura).

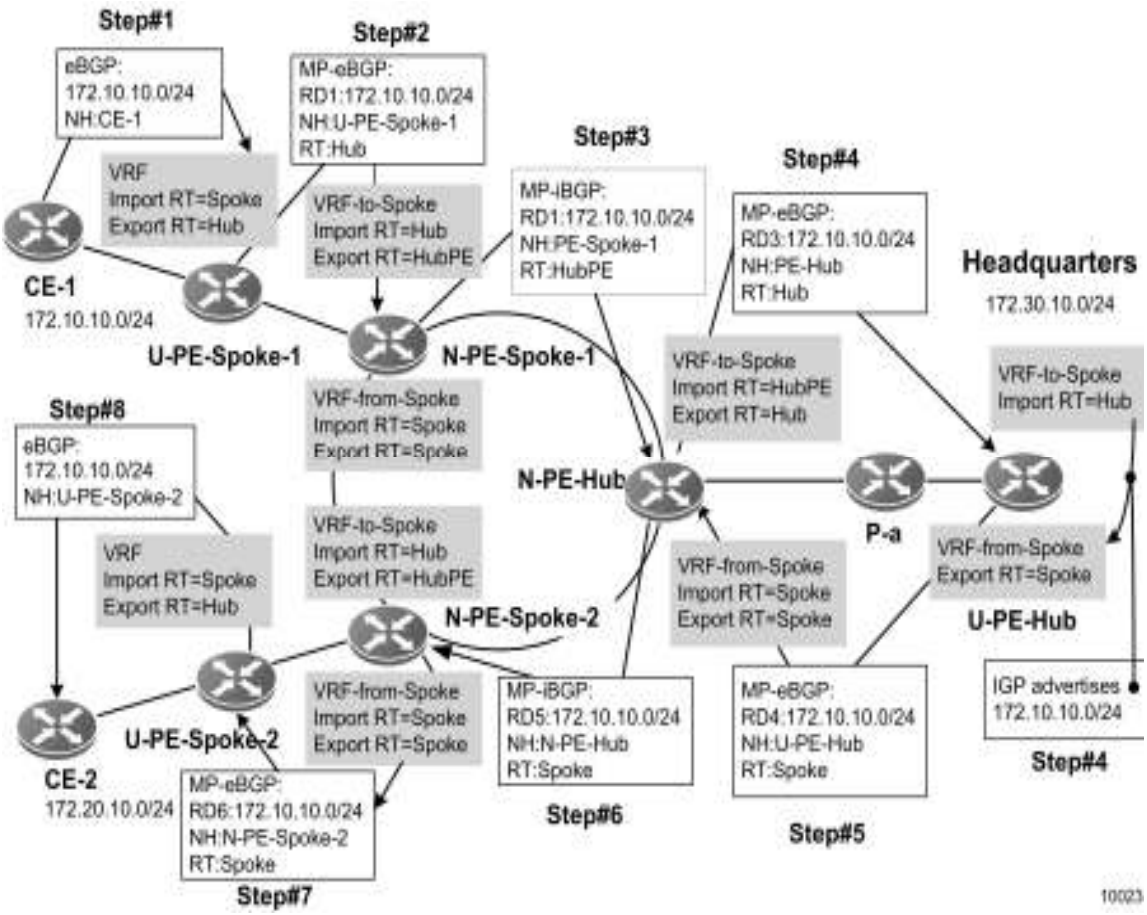
El siguiente ejemplo muestra la implementación de la topología *hub-spoke* cuando se utiliza el sistema de distribución de Tellabs 8660 para implementar la red de acceso. En la figura de abajo hay un enrutador U-PE entre el enrutador CE y PE para las ramas de oficina y el sitio Hub. El enrutador P-a agrega tráfico al enrutador N-PE-Hub.

También nos muestra la figura como CE-2 aprende las rutas de CE-1. Hay que darse cuenta que todos los enrutadores PEs tienen VRFs, VRF-*to*-*Spoke* y VRF-*from*-*Spoke*, para implementar esta VPN.

Los nombres de las VRFs reflejan la dirección del flujo de tráfico actual. Los mensajes BGP avanzan en la posición contraria. N-PE-Spoke-1 y N-PE-Spoke-2 usan para importar RT=*Hub* y para exportar RT=*HubPE* esto para prevenirlos de aprender las rutas directamente una de la otra.

Si estuvieran usando "*hub*" para ambos RTs aprenderían las rutas directamente uno del otro, lo cual no es la intención. Ahora solo el N-PE-*Hub* aprende las rutas de los *spokes* y distribuye la información al U-PE-*Hub*. U-PE-*Hub* en las oficinas centrales tiene un puerto asociado a la VRF-*to*-*Spoke* y un puerto para la VRF-*From*-*Spoke*. En este ejemplo IGP en las oficinas centrales es el encargado de distribuir las rutas entre los puerto. U-PE-*Hub* anunciará entonces las rutas a los *spokes*.

Figura 16: Ejemplo de aplicación de una VPN *Hub and Spoke.*



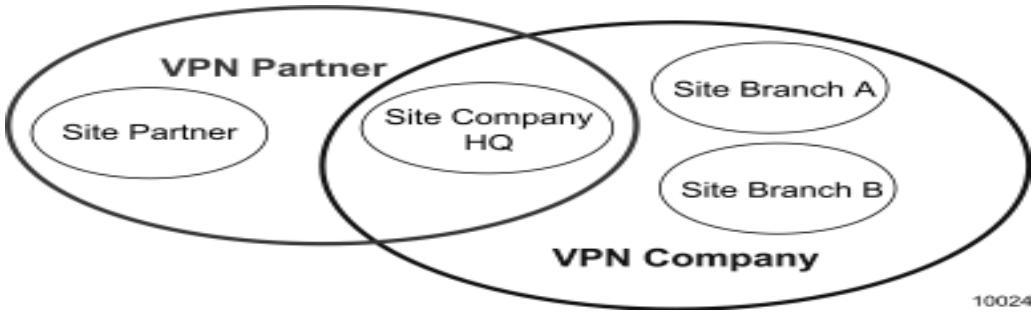
Fuente: Tellabs 8000 *Manager Online Documentation*.

3.7.3 VPN traslapadas:

En las VPNs traslapadas un sitio puede pertenecer a múltiples VPNs. Este tipo de conectividad IP puede ser utilizada por ejemplo para implementar una Extranet o Servicios Centrales.

La figura de abajo muestra la conectividad IP en las VPNs traslapadas utilizando Extranet como ejemplo. Nótese que se requiere de una dirección de IP única entre las VPNs traslapadas.

Figura 17: Ejemplo de una VPN traslapada.



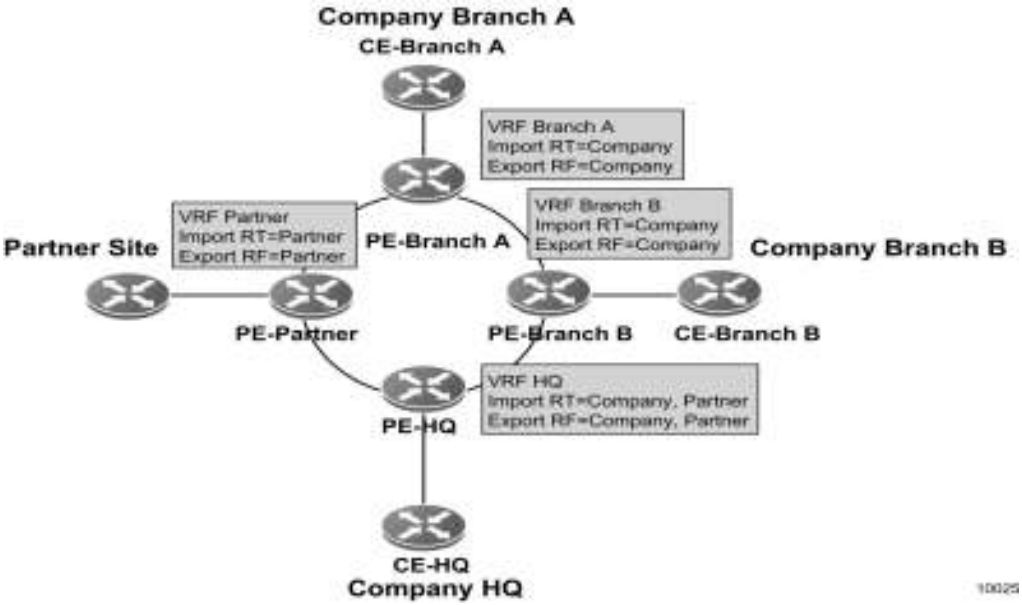
Fuente: Tellabs 8000 *Manager Online Documentation*.

En la figura de la siguiente página, el socio (*partner*) tiene conectividad con el sitio de la compañía HQ pero no con otros sitios. Las VPNs traslapadas pueden ser implementadas con el uso de rutas de destino en una manera correcta. La figura de abajo muestra como la conectividad necesitada puede ser lograda.

La implementación en la figura de la siguiente página, le permite al sitio del Socio alcanzar todas las redes del sitio de la compañía HQ. El requerimiento actual de conectividad puede ser tal que el sitio del Socio tenga acceso únicamente a cierto

servidor en el sitio de la Compañía HQ, en cuyo caso solo ese prefijo deberá ser anunciado al Socio. (RT=Partner).

Figura 18: Ejemplo de una aplicación de una VPN traslapada.

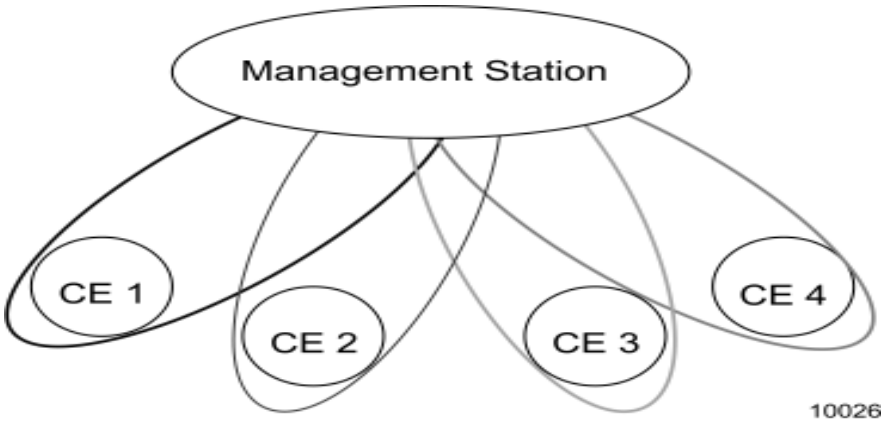


Fuente: Tellabs 8000 *Manager Online Documentation.*

3.7.4 VPN Centralizada

La conectividad IP de las VPNs centralizadas debe ser tal que la estación Central puede comunicarse con cualquier enrutador CE, pero los enrutadores CE no se pueden comunicar entre sí. La figura de abajo muestra los requerimientos de la conectividad IP. Se puede observar que desde el punto de vista de conectividad IP, hay múltiples VPNs traslapadas. La estación Central pertenece a todas esas VPNs.

Figura 19: Ejemplo de una VPN centralizada

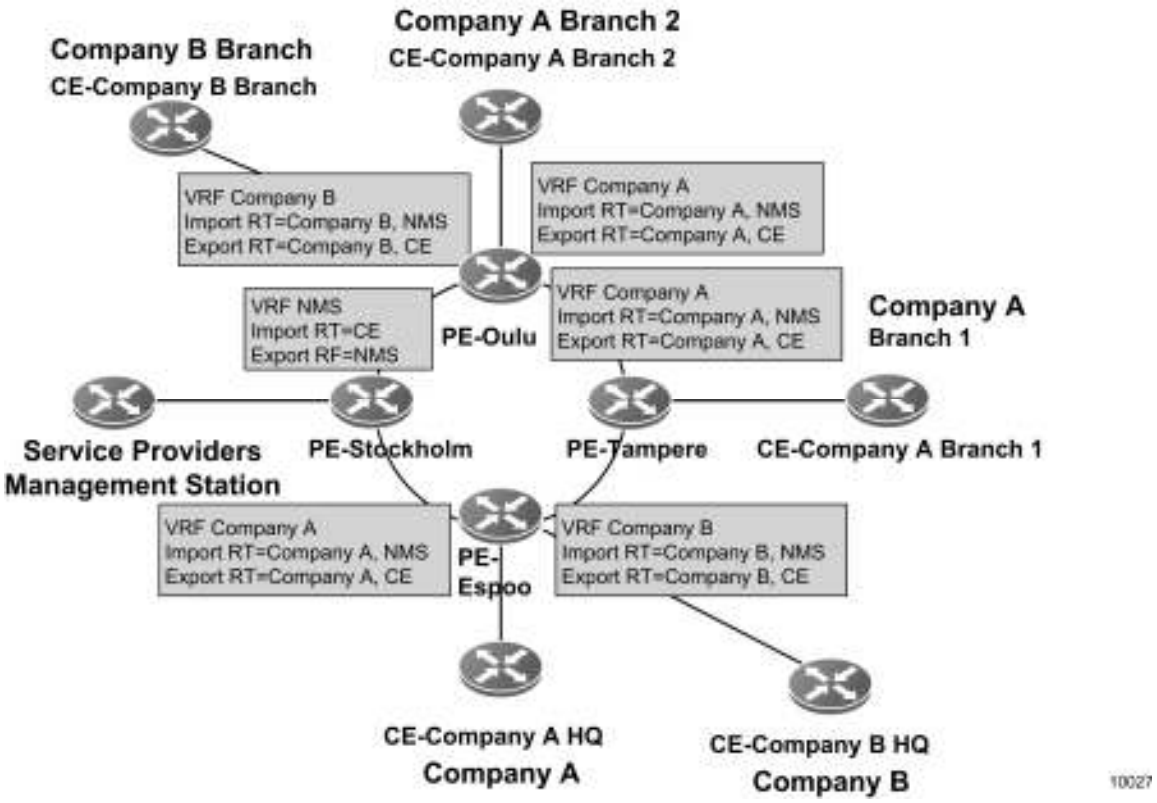


Fuente: Tellabs 8000 *Manager Online Documentation*.

La figura siguiente muestra una forma de configurar las Rutas Destino para poder alcanzar la conectividad IP deseada para las VPNs centralizadas. En la figura se puede observar una VPN centralizada y dos intranets. Hay que notar que es suficiente que la estación Central aprenda una dirección que pueda utilizar para comunicarse.

Otras direcciones de red de los clientes no deben ser publicadas al NMS. Esto por razones de seguridad y para reducir las direcciones propagadas a la VRF que la estación central está conectada. RT=CE en la figura de abajo debe de estar añadida solo a una dirección (*loopback* o dirección de interface del CE).

Figura 20: Ejemplo de una aplicación de una VPN centralizada.



Fuente: Tellabs 8000 *Manager Online Documentation.*

4. SIMULACIÓN DEL ESCENARIO MPLS VPN Y ANÁLISIS ECONÓMICO

4.1 Simulación del escenario MPLS VPN:

Dentro de las opciones que se venden para implementar una VPN sobre MPLS, ya vimos que se pueden dar varios escenarios: *Full Mesh, Hub and Spoke, Management* y del tipo Traslape, dependiendo de la necesidad del cliente, junto con estos escenarios también se puede dar clasificación de tráfico, es decir asignar prioridad o ancho de banda específico a ip's con origen y destino, por protocolo o por puerto.

En el equipo que trabajaremos para proveer este servicio es un Tellabs 8660, que es un sistema que puede ser usado para implementar VPN's de capa 3, así como le permite al Proveedor de Servicio usar el núcleo de IP/MPLS para configurar las VPN's para los clientes. En este tipo de método basado en *Provider Edge*, la configuración de la VPN se encuentra en los enrutadores *Provider Edge* del proveedor de servicio. Es un modelo de Punto a punto donde los enrutador CE y el PE son pares de ruteo. Se utiliza BGP para distribuir las rutas de las VPN's dentro de los PE's.

MPLS es utilizado para separar el tráfico de los diferentes clientes dentro de la red central. Las redes de los clientes pueden usar direcciones de IP que se traslapen. Es común para las redes de los clientes usar direcciones de IP privadas. El uso de direcciones IP privadas dentro de las redes de los clientes no es problema, dado a que las tablas de ruteo y direccionamiento pueden mantenerse separadas para cada VPN.

Un sitio de cliente puede pertenecer a múltiples VPN's. En ese caso una VRF contiene rutas para múltiples VPN's. Estas VPN's traslapadas no pueden tener direcciones de IP iguales. También es posible permitir a un sitio del cliente acceder a múltiples VRF's en cuyo caso la dirección de IP puede traslaparse. Cuando un sitio está ligado a múltiples VRF's, la VRF seleccionada puede determinarse por el puerto físico de entrada, el encabezado de capa 2 (VLAN) o desde la etiqueta de MPLS. Las VRF's en el enrutador pueden usarse para implementar diferentes tipos de topología de VPN's.

4.1.2 Descripción del escenario:

Supongamos que un cliente se acerca a nosotros para plantearnos el siguiente escenario:

Requiere una VPN para interconectar sus sitios en la región centroamericana, el tiene una sucursal en Guatemala, Salvador, Honduras y Nicaragua; desea que estos sitios tengan comunicación entre sí, es decir que cada uno de los sitios se pueda comunicar con cualquier otro.

Además de esto, el quiere que se asigne cierto ancho de banda a los siguientes tipos de tráfico: Videoconferencia con el 40% del ancho de banda, a su Intranet con un 35% del ancho de banda y a todo el tráfico restante que se le asigne el 25% del ancho de banda. Pide que las redes sean distribuidas de la siguiente manera:

- Guatemala: 192.168.1.0 con máscara: 255.255.255.0
- Salvador: 192.168.2.0 con máscara: 255.255.255.0
- Honduras: 192.168.3.0 con máscara 255.255.255.0

- Nicaragua: 192.168.4.0 con máscara 255.255.255.0

Al mismo tiempo el cliente nos dice que va a utilizar una dirección ip específica para realizar las videoconferencias en cada país, las direcciones ip a utilizar son:

- Guatemala: 192.168.1.5
- Salvador: 192.168.2.5
- Honduras: 192.168.3.5
- Nicaragua: 192.168.4.5

Para la conexión de su Intranet utilizará el puerto 445.

La conexión de última milla debe de ser entregada con fibra óptica. El ancho de banda en la conexión debe de ser de 2 Mbps, esto implica que el máximo ancho de banda alcanzado en todo momento por los cuatro sitios es de 2 Mbps.

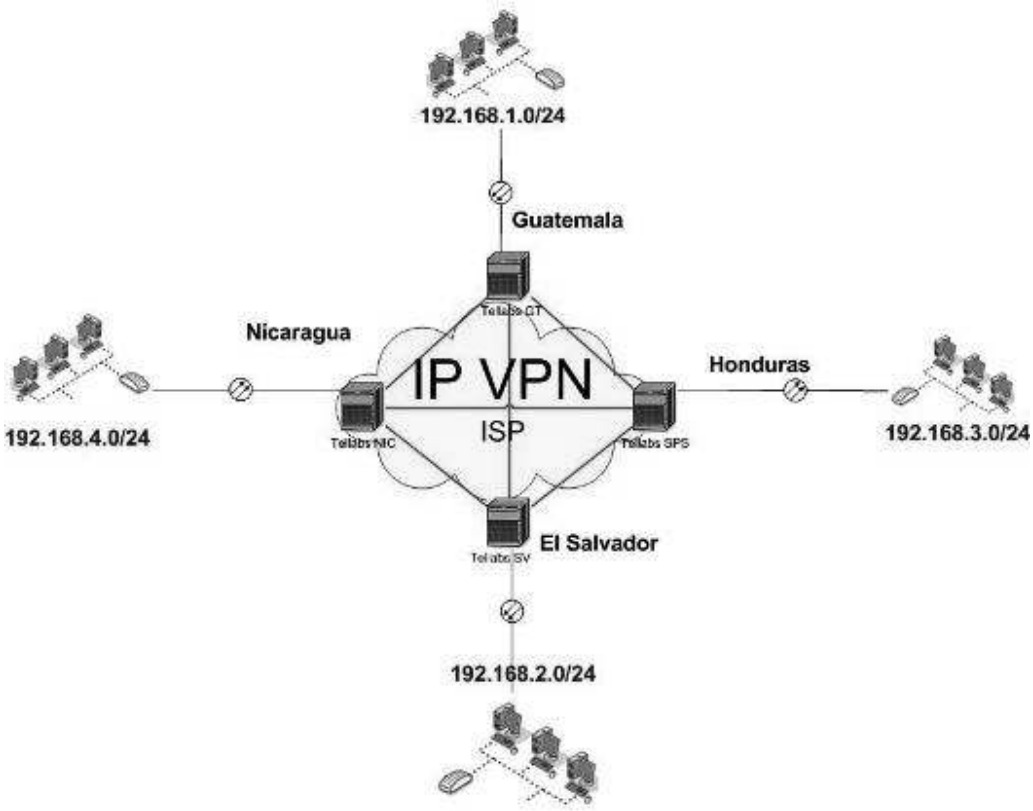
Hay que hacer un señalamiento importante en este punto, la topología a utilizar es la del tipo Full Mesh y los 2 Mbps asignados a la VPN es el consumo total de los cuatro sitios, no 2 Mbps por cada uno, se hace esta mención porque en algunas ocasiones los clientes piensan que es de esa forma en que se entrega el enlace.

De cualquier forma, una de las ventajas de MPLS es la versatilidad con la que puede ampliar o disminuir el ancho de banda según los requerimientos de los clientes, esto les permite a ellos realizar sus pruebas pertinentes y en base a esto aumentar o disminuir el ancho de banda contratado para la optimización de los recursos

.

El diagrama de conexión de este cliente es como sigue:

Figura 21: Escenario de una red IP VPN MPLS.



Fuente: Autoría Propia.

4.2 Creando un IP VPN *full mesh*.

La topología *Full Mesh* para las IP VPN's es usada en casos donde todos los sitios pertenecientes a la VPN tienen que comunicarse directamente con las otras.

Dentro del equipo Tellabs 8660 se deben de cumplir con las siguientes condiciones antes de poder crear la IP VPN.

- Los parámetros globales de aprovisionamiento de la VPN deben de haber sido definidos.

- El mapeo del QoS debe de haber sido definido en la base de datos del equipo. Estos son los siguientes: Real Time (*para tráfico de voz y video*), Control (*para manejo del tráfico de la red*), PG Prioridad Garantizada (*para tráfico sensible al retardo*), G + E Garantizado más Exceso (*para datos críticos dentro de la empresa*) y BE Best Effort (*para el tráfico de internet*).

- Los puntos de entrega de la VPN y los elementos de red del PE a través del cual está conectado la VPN a la red central, estén configurados de la siguiente manera: una VPN de punto de entrega se refiere a una interface a través de la cual el cliente final accede a la IP VPN. Un nodo de punto de entrega de VPN se refiere al elemento de red donde la interface está alojada.

- El ID del enrutador ha sido definido para todos los elementos de red que serán usados en la IP VPN.

- Hay una interface que contiene el ID del enrutador como una dirección IP para cada elemento de la red que serán utilizados en la IP VPN. Es recomendable que se utilice una interface *loopback* para esto.

- Debe de haber sesiones de BGP y vecinos de BGP con rutas maestras u otras rutas reflectoras de los equipos configurados a través de la red del PE que serán utilizados en la IP VPN.

- Todos los elementos de red deben haber sido correctamente configurados para todos los PE y equipos de acceso a la red (en).

- Las VPN de punto de entrega deben haber sido definidas como puntos de acceso de usuario.

- Las interfaces IP (direcciones IP y máscara de red) deben haber sido configuradas en las interfaces donde los puntos de acceso de la VPN serán utilizadas.

- Es recomendado que los clientes y los sitios estén configurados para los puntos de acceso de las VPN.

- Todos los enlaces de acceso a la red entre los puntos de acceso de la VPN y los equipos PE deben estar configurados de la siguientes forma: una ruta para uno más enlaces de las IP/MPLS exista en la red de acceso.

- Una interface MPLS debe estar configurada para todos las interfaces de enlace: las etiquetas de *switcheo* deben estar habilitadas y ya sea LDP o RVSP deben estar también habilitadas.

- Las interfaces IP (dirección ip y máscara de red) deben estar configuradas para las interfaces a las cuales los enlaces IP/MPLS estén relacionados.

- Ya sea LDP o RSVP deben estar habilitados para los enlaces IP/MPLS.

- Si se está utilizando Clasificación de Servicio, un *template* de la clasificación de servicio debe estar creado.

- En orden de conectar una VPN, todos los elementos de la red y enlaces deben de estar en USO y funcionales.

- Se debe de tener OSPF configurado en los elementos de red y en la red central y conectividad a nivel IP debe existir entre ellos.

- LSP así como LDP o RSVP tienen que estar habilitados en los elementos de la red Central si se usará Ingeniería de Tráfico.

- Debe de estar habilitado RSVP en los parámetros de las interfaces de acceso a la red entre los puntos de la VPN y los equipos PE.

- RSVP debe de estar habilitado en los links IP/MPLS.

Con los requisitos arriba descritos cumplidos, podemos proceder a configurar la VPN siguiendo los pasos que a continuación describimos:

Paso 1: Crear una nueva IP VPN:

- El primer paso a seguir es crear una nueva IP VPN, esto lo hacemos abriendo la aplicación de IP VPN y seleccionando la opción de crear una nueva VPN.

Paso 2: Definir los parámetros de la VPN:

- Como siguiente paso tenemos que definir los parámetros de la VPN. Ingresar el nombre de la VPN en el campo correspondiente y seleccionar el propietario de la lista de Clientes y la categoría de falla en la lista de Categoría.

- En la lista de Topología seleccionar la opción *Full Mesh*. (en este caso se da este ejemplo pero se pueden seleccionar los otros tipos de topología mencionados anteriormente.

- Marcar la opción de Habilitar (*Enable*) para *Test Loopback Interface* si se quiere que la crear una interface *loopback* para pruebas de bucles en los paquetes.

- Marcar la opción Habilitar *(Enable*) para poder realizar pruebas con la herramienta de bucles de paquetes para las Calidades de Servicio.

- Si queremos usar Políticas para las clases de servicio debemos habilitar la opción del Uso de Políticas.

- Tenemos que seleccionar el tipo de Clasificación de Servicio usaremos en el submenú de Clasificación de Servicio. Los valores escogidos acá serán los que se utilizarán para los puntos de acceso de las VPN. Después se pueden cambiar estos valores para asignar un ancho de banda diferente a cada punto de acceso. La selección de la capacidad es usada para crear las políticas de servicios y reservar el RSVP – TE de los Túneles.

- Si se desea crear túneles TE para la IP VPN y no se requiere del ruteo manual de túneles, hay que seleccionar la opción sí en Auto generar túneles RSVP – TE en las redes de Acceso. Los túneles de esta forma serán creados en base a la clase de servicio y capacidades definidas en la opción de Capacidad para las clases de servicio.

- Si se desea, seleccionar el grupo administrativos para los túneles TE de la lista Grupo Administrativo.

- Si se desea dirigir el tráfico IP VPN a túneles específicos, hay que seleccionar el campo de afinidad de túnel de la lista correspondiente. Hay que hacer notar que los túneles (los que se auto generan o los que se crean manualmente en la herramienta de Ingeniería de Túneles) deben de tener un grupo administrativo especificado.

- Seleccionar la opción *OK*.

Paso 3: Seleccionar los puntos de acceso de la VPN.

- Seleccionar la interface en la vista de Clientes o Nodos.

- Seleccionar la interface y presionar el botón derecho del ratón y dentro de las opciones que despliega debemos seleccionar la que dice añadir a la VPN. Si hay varios PEs que se pueden usar para acceder al punto de entrega del servicio, se nos preguntará que definamos cual será el PE primario para el punto de entrega de la VPN.

- Repetir este paso para cada punto de entrega en la VPN.

Paso 4: Si se desea, se puede cambiar los valores por defecto de los parámetros del punto de entrega. Este paso es opcional.

- Seleccione el punto de entrega deseado en la vista configuración VPN.

- Dar clic en el punto de entrega seleccionado con el botón derecho del mouse y seleccione la opción *propiedades* del menú desplegable. Con esto se abre el diálogo del punto de entrega.

- Seleccionar la opción *habilitar* en el cuadro prueba de bucle en Interface si se quiere que en el aprovisionamiento de la VPN se pueda crear una interface *loopback* para las pruebas de bucle de paquetes.

- Cambiar los parámetros del servicio, por ejemplo, Capacidad por Clase de Servicio, para cada punto de entrega individualmente. Hay que hacer notar que los valores en el campo Capacidad por Clase de Servicio son usados cuando se configura tanto las políticas como los Túneles TE.

Paso 5: Definir el método de ruteo que se utilizará en la red del cliente si fuese necesario.

- Para cada punto de entrega de la VPN, hay que seleccionar que tipo de ruteo se utilizará en la red del cliente, ya sea ruteo estático, OSPF o BGP y ajustar los parámetros apropiados en el cuadro de diálogo del Punto de Entrega.

- Seleccionar el botón de aplicar.

- Seleccionar el botón de cerrar para cerrar el cuadro de diálogo.

Paso 6: Generar la configuración de la VPN dentro de la base de datos.

- Dar clic sobre la VPN con el botón derecho del ratón y seleccionar Crear la Configuración de la VPN del menú desplegable. El estado de la VPN cambia a Instalada. Ahora se puede observar los elementos de configuración de la VPN creados para la base de datos en la vista de Configuración de VPN.

Paso 7: Conectar la VPN, con esto se envía la configuración a los elementos de red.

- Dar clic sobre la VPN con el botón derecho del ratón y seleccionar la opción Conectar la VPN del menú desplegable.

4.2.1 Creando plantillas de clasificación de servicios generales:

Las plantillas de clasificación de servicios son utilizadas para definir los requerimientos de la calidad de servicio para el tráfico de las IP VPN. El uso de plantillas simplifica el proceso de provisión: los requerimientos de clasificación de los servicios pueden ser predefinidos y las plantillas ya hechas se pueden utilizar para aprovisionar la IP VPN. Las reglas de clasificación de servicios son implementadas como Listas de Control de Acceso (ACLs).

Procedimiento:

Aprovisionando la VPN.

Paso 1: Añadir una nueva plantilla de clasificación.

- Seleccionar **Herramientas –** en el menú de opciones de las plantillas de clasificación de servicios. Luego se abre el cuadro de diálogo de la plantilla de clasificación de servicios.

- Seleccionar el botón **Añadir** en el cuadro de la Clasificación de Plantilla. Con esto se abre el cuadro de diálogo de añadir plantilla de clasificación de servicios.

- Ingresar el nombre de la plantilla y la descripción en los campos correspondientes.

- Seleccionar el botón **OK.**

Paso 2: Agregar las entradas de la plantilla de clasificación.

- Seleccionar la nueva plantilla de clasificación de la lista de **Plantillas de clasificación** y seleccionar el botón **Añadir** en el cuadro de **entrada de la plantilla de clasificación.** Se abre el cuadro de diálogo de la **Entrada de clasificación de servicio**.

- Seleccionar ya se la opción de **Permitir** o **Denegar** para la acción a tomar en la entrada de datos. Todas las plantillas deben de tener por lo menos una entrada de permitir, ya que si no se coloca esto ningún tráfico será permitido y no pasará a su destino.

- Clasificar el tráfico de acuerdo al criterio deseado. Se puede clasificar el tráfico basado en la dirección origen y/o destino, protocolo, puerto de origen y/o destino o tipo de servicio en los cuadros correspondientes. La clasificación del tipo de servicio nos permite definir el punto de código distinguido de los servicios o DSCP por sus siglas en inglés, o la precedencia de IP y los bits del tipo de

servicio de los paquetes entrantes del sitio del cliente a ser mapeados a una clase de servicio específica en la red del operador.

- Ingresar un nombre descriptivo para la entrada de clasificación en el campo **Nombre** y utilizar el campo **Descripción** para notas adicionales.

- Seleccionar el botón **OK.**

Paso 3: Repetir el paso 2 para cada entrada necesitada en la plantilla. Hay que hacer notar que se puede utilizar el botón copiar para copiar la entrada del parámetro en otra plantilla.

Paso 4: Definir el orden de las entradas de las plantillas.

- Utilizar los botones **Arriba** y **Abajo** para definir el orden de las entradas de la clasificación. Cuando se decide si el tráfico debe permitir o denegar, las entradas son evaluadas desde arriba hacia abajo. Debido a que se evalúan las entradas de arriba hacia abajo, si la primer entrada permite al tráfico pasar, el siguiente es evaluado y así continúa. La última entrada en la lista debe de coincidir con el tráfico restante. Hay, sin embargo, una regla implícita de denegar todo al final de cada lista de entrada, significando esto que todo el tráfico que no coincida con ninguna de las entradas, estas serán rechazadas.

- Seleccionar el botón **Cerrar** para salir del cuadro de diálogo.

Con esto hemos terminado de configurar la IP VPN, como nos damos cuenta, la configuración general se hace dentro de los equipos MPLS y no en cada enrutador como sucedería para un enlace de datos punto a punto. Como veremos adelante esta forma de configuración nos lleva a una optimización de recursos que repercute en mayores beneficios económicos.

4.3 Comparación de una IPVPN MPLS con un enlace de datos multipunto

Ahora viene una parte importante que interesa tanto al Proveedor de Servicio como para el cliente, ya que haremos una comparación entre estos dos tipos de enlaces, la comparación se realiza en base a los productos ofrecidos por el mismo ISP, es decir que puede darle ambas soluciones a su cliente, acá veremos las ventajas de cada uno y si atienden las necesidades del cliente.

El esquema a trabajar es el que se presentó al principio del capítulo para la parte de IP VPN que resumimos a continuación:

Una empresa multinacional requiere interconectar sus sedes de la región centroamericana, el requiere que cada sede tenga conectividad con todas las demás, ya que comparten recursos y desean establecer videoconferencias para realizar reuniones semanales, el también quiere que todos los puntos se entreguen con Fibra Óptica. El ancho de banda solicitado es de 2mbps.

Del lado del enlace de datos Multipunto lo que se desea es lo siguiente, 3 enlaces de datos, desde Salvador, Nicaragua y Honduras hacia Guatemala, lo que quiere decir que la sede central será Guatemala, se solicita un ancho de banda de 1Mbps para cada punto, de igual forma se requiere que el transporte sea a través de Fibra Óptica.

Analicemos ambas alternativas, empezaremos con el enlace de datos multipunto.

4.3.1 Conectividad a través de un enlace de datos multipunto:

En este tipo de topología, el ISP debe de entregar 3 enlaces en el lado de Guatemala, debe de entregar el enlace de Honduras, Nicaragua y El Salvador. Además de esto se debe de realizar la configuración de las rutas de cada punto en el enrutador del sitio donde se entrega, en este ejemplo en el enrutador de Guatemala creamos las rutas para que conozca los demás sitios, en este tipo de topología es más trabajoso para el ISP

configurar nuevas redes si fuera el caso que se extienda debido a crecimiento de la red en cada punto.

Enumeremos entonces los componentes que requiere un punto para poder tener conectividad hacia los otros sitios:

- Conexión física: dependiendo del requerimiento del cliente y de la tecnología con la que el ISP puede entregar el enlace puede ser: Fibra óptica, Cobre, Inalámbrico, etc. En este caso en particular se entregaría con Fibra Óptica.

- Conexión Lógica: El tipo de conexión lógica depende de la conexión física, por ejemplo, un enlace Inalámbrico puede entregar conexión *Frame Relay, Clear Channel* y también IP. En este caso se entregaría a través de una conexión IP.

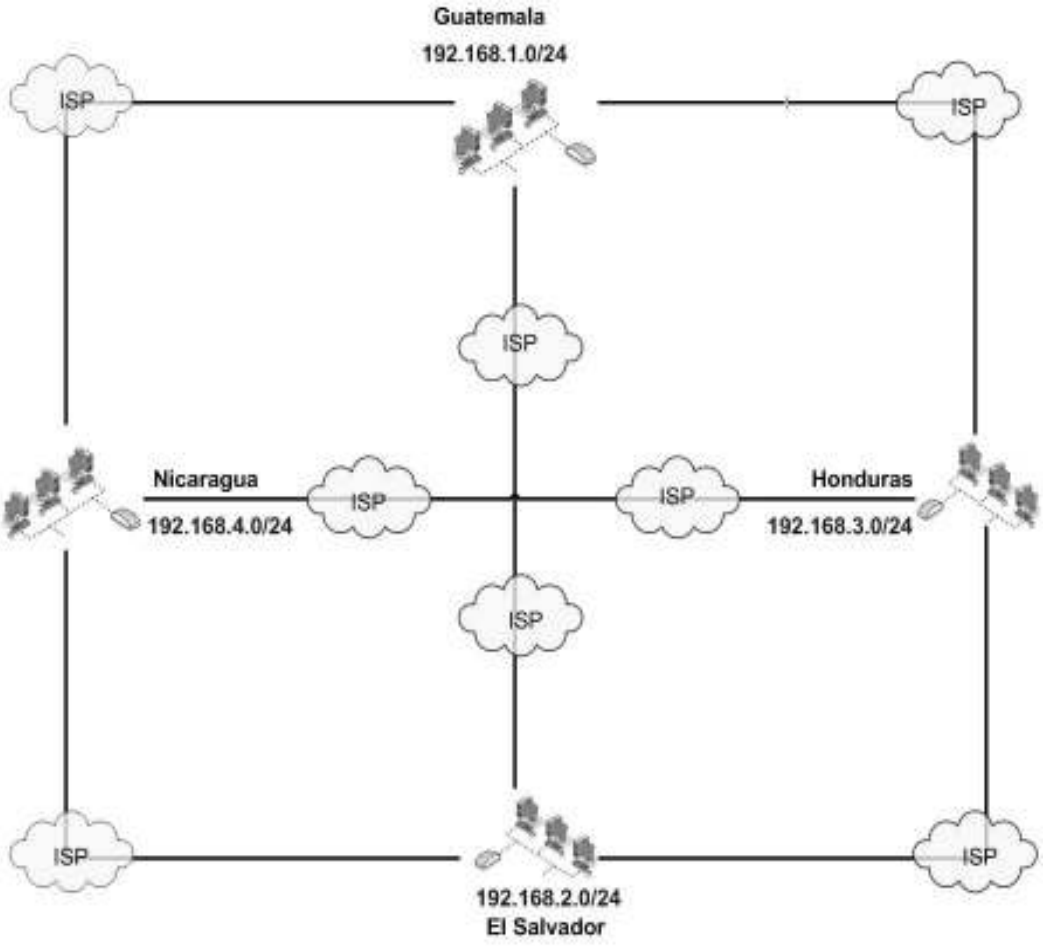
- Enrutador en cada Sede: dependiendo de los requerimientos es necesario para poder recibir los enlaces de los otros países y para realizar el ruteo necesario, así como para configurar la red que utilizará el cliente en dicha sede.

- Transporte Regional: es necesario para realizar la conectividad entre sedes, de esto se encarga el ISP, lo lleva a través de su red de un punto a otro.

Contando con estos recursos ya el ISP se encarga de configurar las redes dentro de cada uno de los enrutadores, para que cada país conozca las redes de los demás. Esto requiere de rutas específicas para conocer las redes de un país y de otro, por decirlo de alguna forma, es necesario decirle al enrutador de Guatemala por donde va a conocer la red de Salvador y así con cada uno de los países.

El diagrama del enlace de datos multipunto es como el que se presenta a continuación.

Figura 22: Escenario de un enlace de datos multipunto.



Fuente: Autoría Propia.

4.3.2 Conectividad a través de un enlace de datos IP VPN MPLS

En este tipo de enlaces el ISP debe de entregar un enlace en cada punto, por decirlo de alguna manera, entregará un cable RJ45 con conexión Ethernet donde llega la red lan de dicho sitio, no necesita entregar un enrutador para distribuir las rutas o realizar configuraciones extras, ya que desde su equipos centrales puede realizar este tipo de configuraciones, lo que debe de hacer es configurar una IP VPN, conectarla a los distintos sitios del cliente, crear las rutas para que se conozcan entre todos los países y asignarles las ip's de la lan de cada sitio.

Ahora enumeremos los componentes necesarios para realizar la instalación de este tipo de enlace en los sitios del cliente:

- Conexión física hacia cada uno de los sitios del cliente, en este caso por disposiciones del cliente se requiere que sea a través de Fibra Óptica.

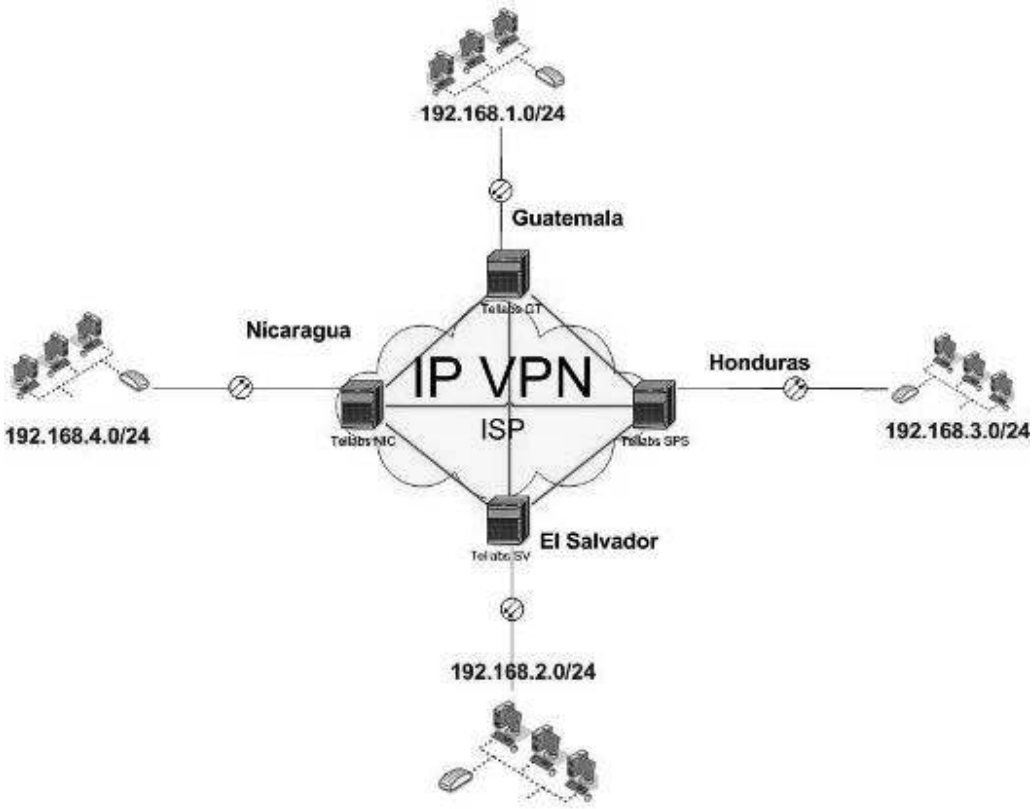
- Conexión Lógica, se entregará cada enlace a través del protocolo tcp/ip, ya que el cliente recibirá directamente la red de su conexión de área local, específicamente la señalada por el cliente para cada sitio, acá estamos hablando de: Guatemala: 192.168.1.0 con máscara: 255.255.255.0, Salvador: 192.168.2.0 con máscara: 255.255.255.0, Honduras: 192.168.3.0 con máscara 255.255.255.0 y Nicaragua: 192.168.4.0 con máscara 255.255.255.0.

- Transporte Regional: es necesario para realizar la conectividad entre sedes, de esto se encarga el ISP, lo lleva a través de su red MPLS de un punto a otro.

- Configuración de la calidad de servicio y de la IP VPN. Como se describió en la sección anterior, se puede dar calidad de servicio a cierto tipo de tráfico o también se puede restringir ip's o tipo de protocolo, esto de acuerdo a la conveniencia del cliente.

El diagrama de la conexión es como sigue:

Figura 23: Escenario de una red IP VPN MPLS.



Fuente: Autoría Propia.

4.4 Análisis económico sobre el enlace de datos multipunto.

Realizando una cotización sobre un enlace de datos multipunto a cierto ISP con las siguientes características: enlace de datos con un ancho de banda de 1Mbps, enrutador en cada sitio, sede central en Guatemala, conexión de Salvador, Honduras y Nicaragua hacia Guatemala. El rango de precios de cada enlace es el siguiente:

Tabla IV: Valores enlace de datos multipunto

Concepto	Precio
Enlace de Datos 1Mbps Guatemala hacia Salvador.	US$ 2000.00
Enlace de Datos 1Mbps Guatemala hacia Honduras.	US$ 4000.00
Enlace de Datos 1Mbps Guatemala hacia Nicaragua.	US$ 4000.00
Alquiler 4 Enrutadores Cisco 1841, a US$150 cada uno.	US$ 600.00
TOTAL	**US$ 10,600.00**

El precio total de este escenario asciende a un precio arriba de los US$10,000.00 un monto bastante oneroso dependiendo del tipo de empresa y de la magnitud de operaciones regionales.

4.5 Análisis económico sobre el enlace de datos IP VPN sobre MPLS.

De igual forma que en el enlace de datos multipunto, se le consultó al mismo ISP sobre un enlace de datos de 2mbps del tipo IP VPN interconectando a Guatemala, Honduras, Nicaragua y Salvador. La tabla de precios indicada por el ISP es la que se muestra en la siguiente Tabla en la siguiente página:

Tabla V: Valores enlace de datos IP VPN sobre MPLS.

Concepto	Precio
Enlace de Datos 2Mbps Guatemala.	US$ 1,200.00
Enlace de Datos 2Mbps Salvador.	US$ 1,200.00
Enlace de Datos 2Mbps Honduras.	US$ 1,500.00
Enlace de Datos 2 Mbps Nicaragua	US$ 1,500.00
Servicio IP VPN MPLS	US$ 3,000.00
TOTAL	**US$ 8,400.00**

4.6 Comparación económica entre el enlace de datos multipunto y la IP VPN MPLS.

Presentamos a continuación una pequeña tabla de comparación entre los dos tipos de enlaces para su respectivo análisis.

Tabla VI: Comparación precios enlace de datos vrs IP VPN sobre MPLS.

Enlace de Datos Multipunto	Enlace IP VPN MPLS	Diferencia
US$ 10,600	US$ 8,400	US$ 2,200

Como podemos observar en los cuadros anteriores, hay una diferencia notable en cuanto a los dos tipos de enlaces, tanto en el producto en sí como en los precios, veamos los siguientes puntos importantes al respecto:

- El enlace de datos multipunto tiene una sede que hace la funciones de la central, allí se concentran todos los enlaces de las demás ciudades; por su lado la IP VPN

la red central del proveedor ISP funciona como enrutador central para todas las sedes, esto representa ventaja tanto para el proveedor como para el cliente ya que es mucho más sencillo realizar cambio de configuraciones.

- El enlace de datos multipunto necesita de enrutadores para implementar los enlaces, esto conlleva a gastos ya sea de alquiler o de compra del mismo, además añade un punto de falla al enlace debido a las fallas del equipo utilizado, para el ISP conlleva mayor trabajo la administración y configuración de los mismos. Para el enlace IP VPN, como lo mencionamos arriba, no se necesita de enrutador ya que el equipo de red central realiza esa función, se minimiza el tiempo de configuración, elimina equipos en el sitio del cliente como posibles puntos de falla y es mucho más versátil para realizar solicitudes especiales del cliente.

- Los costos de operación y de implementación del enlace de datos multipunto son bastante elevados, podemos observar en la tabla de arriba la diferencia significativa que existe, la solución IP VPN es de menor costo.

- La velocidad del enlace de datos Multipunto si está garantizada de 1Mbps para cada sitio, por otro lado, el enlace de datos IP VPN MPLS está limitado a 2Mbps para los cuatro sitios, por decirlo de alguna manera, lo máximo a consumir al mismo tiempo entre los cuatros sitios es de 2Mbps.

- Una gran diferencia en cuanto al costo – beneficio de estos enlaces es el valor agregado que se le puede dar al tráfico del cliente a través de las Calidades de Servicio de las IP VPN MPLS, ya que esto permite al cliente distribuir el tráfico de acuerdo a sus necesidades, optimizando de esta forma el uso del ancho de banda y priorizando sus actividades críticas.

CONCLUSIONES

1. MPLS, es un avance de la tecnología IP que permite la comunicación entre varios equipos de tecnología ya existentes, además de dicha versatilidad, hace posible manejar Calidad de Servicio dentro de los enlaces de datos e internet que entrega, hace más eficientes los tiempos en el transporte y elección de rutas, permite definir prioridades asegurando la calidad en la transmisión de voz, video y datos críticos, también agrega seguridad en cuanto al transporte de la información se refiere.

2. Las IP VPN a través de MPLS son más sencillas de implementar comparado con un enlace de datos normal, ya que todo se realiza a través de un equipo central que almacena la configuración de cada sucursal así como la interconexión en las mismas, por lo que allí mismo se realiza la configuración de entrega del enlace y el mantenimiento de la red del cliente.

3. Gracias a la facilidad con que MPLS puede entregar Calidad de Servicio, las empresas multinacionales se ven beneficiadas al darle mayor prioridad a las aplicaciones críticas que necesitan ser compartidas y dándole menos prioridad a las aplicaciones de menor importancia.

4. Además de las ventajas que implica un enlace de datos IP VPN sobre MPLS, representa una alternativa con relación costo – beneficio muy favorable tanto para el ISP que entrega el servicio como para las empresas multinacionales que los contratan, esto debido a su menor costo comparado con un enlace de datos normal y al valor agregado que obtienen con el tratamiento especial que se le da a las aplicaciones a transmitirse por dicho medio.

RECOMENDACIONES

Luego del desarrollo del presente trabajo de investigación, se presentan las siguientes recomendaciones:

1. El Proveedor de Servicios debe de tomar en cuenta en la estructura de su red, contar con los equipos necesarios para entregar los servicios MPLS en todo el tramo que utilice el enlace.

2. Es importante realizar laboratorios de simulación de las calidades de servicio que MPLS puede ofrecer para tener un panorama bien definido de las cualidades de cada tipo de configuración y poder presentar con esto mejores ofertas de enlaces a los clientes.

3. Del lado de los clientes, deben de tener claro que beneficios obtendrán al adquirir un enlace del tipo IP VPN por MPLS y en base a esto definir las políticas necesarias para sacarle el mayor provecho a su conexión.

BIBLIOGRAFÍA

1. Stephenson, Ashley **MPLS: A Quality Choice**, Tutorial técnico, Cisco Systems, Noviembre de 1999.

2. Robert E. Shepard, **Interfacing MTR2000**, June 11, 2006.

3. ***Label Switch Router***. the free encyclopedia, Wikipedia, modified 9 February 2006.

4. De León Carlos, **Migración IP-ATM a MPLS** Tésis Ingeniería Electrónica Universidad de San Carlos de Guatemala, Abril 2007.

5. Yakov Rekther, Bruce Davie **MPLS: Tecnology and Applications**, Primera edición. Academic Prees, 2000.

6. Motorola, **MTR2000, Base Station, Repeater and Receiver For Analog conventional.**

7. **and Trunking Systems Service Manual**, año 1997.

8. Multitech Systems, **Multimodem, wireless Modems, User Manual,Version 2.0,** año 2005.

9. Rifat A. Dayem, **PCS & DIGITAL CELLULAR TECHNOLOGIES**, Prentice Hall, New Jersey 1997.

10. de Miguel, Tomás P. **Redes Privadas Virtuales y MPLS**, DIT Univ. Politécnica Madrid, marzo del 2003.