ESCUELA POLITÉCNICA DEL EJÉRCITO
DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA EN TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE GRADO DE INGENIERÍA

ESTUDIO DE REDES PRIVADAS VIRTUALES BASADAS EN LA TECNOLOGÍA MPLS

ANA LUCÍA SEGARRA ZAMBRANO

SANGOLQUI – ECUADOR

2009

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES

CERTIFICADO

Ing. Rubén León Msc. e Ing. Carlos Romero

CERTIFICAN

Que el trabajo titulado Estudio de Redes Privadas Virtuales basadas en la tecnología MPLS, realizado por Ana Lucía Segarra Zambrano, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Debido a que la información proporcionada es útil y acorde a las necesidades actuales que existen en la industria de las Telecomunicaciones en el país recomiendan su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a Ana Lucía Segarra que lo entregue al Ingeniero Gonzalo Olmedo, en su calidad de Director de la Carrera.

Sangolquí, martes 1 de diciembre de 2009

Ing. Rubén León M.Sc.	Ing. Carlos Romero
DIRECTOR	CODIRECTOR

RESUMEN

En los últimos años la demanda y popularidad del Internet ha crecido significativa y aceleradamente llevando al mundo de la industria de las telecomunicaciones a tener una visión más completa de cómo brindar soluciones corporativas con mayor valor agregado a través del uso eficiente de las redes disponibles y así mismo mediante la adopción de nuevas tecnologías que estén acordes a sus expectativas y necesidades.

Las redes privadas virtuales MPLS o MPLS VPN es una de las aplicaciones e implementaciones más populares de la tecnología MPLS. Adicionalmente se puede decir que es uno de los servicios a través de las cuales se consigue el mayor beneficio posible respecto de funcionalidad y rendimiento de los desarrollos actuales de MPLS y empata con dichas necesidades.

El presente trabajo, recopila información significativa y actualizada de diferentes autores con el objetivo de brindar al lector los conceptos básicos e indispensables de un conocimiento integral sobre la tecnología. Adicionalmente describe las ventajas que ofrece a los proveedores de servicios siempre y cuando se realiza un diseño e implementación adecuado de redes privadas virtuales basadas en MPLS, para lo cual se proporciona *i)* globalmente las causas y perspectiva histórica por las cuales se desarrolla el estándar, *ii)* la forma cómo MPLS opera dentro del backbone MPLS, *iii)* los protocolos usados en MPLS, *iv)* los principios de una red privada virtual y *v)* aspectos más relevantes de la arquitectura MPLS VPN.

DEDICATORIA

Al Rey de los siglos, inmortal, invisible, al único y sabio Dios, sea honor y gloria, quien con sus brazos de amor me ha traído hasta aquí.

Sin Él y fuera de Él nada de esto hubiera sido posible.

AGRADECIMIENTO

A mi Padre Celestial y a través de ÉL, a cada una de las personas que sin saberlo, fueron utilizadas como un bello y valioso instrumento para bendecir mi caminar.

PROLOGO

La indiscutible y evidente necesidad de constituir un estándar que normalizara un nuevo procedimiento para el transporte de tráfico en la red, fue con el tiempo acentuándose de tal manera que los fabricantes de productos se vieron en la imperiosa necesidad de crear un nuevo esquema por el cual se cubrieran y eliminaran las desventajas evidentes de sus redes tradicionales, nace MPLS y con ella una serie de servicios tales como redes privadas virtuales.

El presente trabajo, proporciona al lector la posibilidad de diferenciar los beneficios de una red privada virtual basada en la tecnología MPLS pero teniendo como antecedente el funcionamiento general de la arquitectura mediante el estudio y análisis de sus dos componentes principales el plano de control y el plano de datos, los protocolos necesarios en MPLS, una red privada virtual y como ésta es posible a través de MPLS mediante un PE router donde se encapsula la esencia de MPLS VPN.

INDICE DE CONTENIDO

INDICE DE FIGURAS

GLOSARIO

AES	Advanced Encryption Standard. Esquema de cifrado por bloques, estándar de adoptado por gobierno de Estados Unidos.
AppleTalk	Conjunto de protocolos desarrollados por Apple Inc., para conexión de redes.
AS	Security Association. Protocolo criptográfico que constituye la base del protocolo de intercambio de claves IKE. Definido en el RFC 2408
AS	Autonomous System. Conjunto de redes que se encuentran administrados por determinada entidad y que cuenta con determinadas políticas de red.
ATM	Asynchronous Transfer Mode.
Backbone	Referido a las conexiones principales y troncales al Internet.
BGP	Border Gateway Protocol. Protocolo de enrutamiento que opera entre sistemas autónomos diferentes.
CEF	Cisco Express Forwarding. Tecnología de conmutación de capa 3 avanzada usadas en el núcleo de la red o el Internet.
CLR	Conservation Mode Retention. Modo de distribución de etiqueta donde un LSR retiene las asignaciones de los routers downstream vecinos.
Core	Red troncal.
CPE	Customer Premises Equipment. Equipo local del cliente.
CR-LDP	Constraint-based Routing BGP. Protocolo de señalización desarrollado para soportar túneles.

DLCI	Data Link Connection Identifier. Identificador del canal del circuito establecido en Frame Relay.
EBGP	External Border Gateway Protocol.
Edge-LSR	Equipo de borde en una red MPLS.
EIGRP	Enhanced Interior Gateway Protocol.
Ethernet	Estándar de redes de área local con acceso al medio a través de CSMA/CD.
FEC	Forwarding Equivalence Class. Conjunto de paquetes que comparten los mismos atributos.
GRE	Generic Routing Encapsulation. Protocolo para el establecimiento de túneles a través de Internet.
IANA	Internet Assigned Numbers Authority. Ente de asignación de números de Internet.
IBGP	Internal Border Gateway Protocol.
IETF	Internet Engineering Task Force.
IGP	Interior Gateway Protocol.
IPsec	IP security.
IPv4	Versión 4 del protocolo IP, usa direcciones de 32 bits.
IPv6	Versión 6 del protocolo IP, usa direcciones de 128 bits.
KeepAlive	Define el tiempo que un nodo LDP espera antes de que decida que la sesión falló.
L3VPN	Layer 3 Virtual Private Network.
L2TP	Layer 2 Tunneling Protocol. Creado para corregir las deficiencias de

	PPTP y L2F.
L2VPN	Layer 2 Virtual Private Network.
LDP	Label Distribution Protocolo. Publicado en el RFC 3036.
L2F	Layer 2 Forwarding.
LFIB	Label Forwarding Information Base. Tabla que almacena un LSR y es usada en el reenvío de paquetes etiquetados
LIB	Label Information Base. Tabla que guarda las etiquetas de los paquetes que se usan como índice para una asignación etiqueta/FEC
LLR	Liberal Label Retention.
LSR	Label Switching Router. Un router que puede enviar paquetes basados en un valor de etiqueta que está añadida al paquete.
LSP	Label Switched Path.
MP-BGP	Multiprotocol Border Gateway Protocol. BGP con extensiones, permite a BGP transportar información de ruteo por múltiples protocolos de capa de red.
MPLS	Multiprotocol Label Switching.
MPLS-TE	Multiprotocol Label Switching Traffic Engineering.
OSPF	Open Shortest Path First. Protocolo de estado de enlace.
PDU	Protocol Data Units. Utilizado para el intercambio entre unidades parejas dentro de una capa del modelo OSI.
PHP	Penultimate hop Popping. Acto de remover la etiqueta MPLS un salto antes del LSR de salida.
PPTP	Point to Point Tunneling Protocol
PVC	Permanent Virtual Channel

QoS	Quality of Service. Medida de desempeño que refleja la calidad de servicio y su disponibilidad.
RD	Route Distinguisher. En el contexto de BGP MPLS L3 VPN, cadena de 8 bits que se concatena con un prefijo VPN.
RIB	Routing Information Base.
RIPv2	Routing Information Protocol version 2
RSVP	Resource reservation Protocol.
RSVP-TE	RSVP extendido que soporta túneles.
RT	Route Target. En el contexto de BGP MPLS L3 VPN, es una comunidad extendida de BGP la cual se añade al prefijo VPN. Define
SOO	Site of Origin. Comunidades extendidas que se puede usar en lugar de los RT.
SVC	Switched Virtual Circuit. Circuito que puede ser establecido por demanda.
IS-IS	System-to-Intermediate System.
TCP	Transmission Control Protocol. Protocolo de transporte seguro usado en IP.
TDM	Time Division Multiplexing.
TDP	Tag Distribution Protocol**.** Protocolo de distribución de etiquetas que antecedió a LDP.
TLV	Type-Lenght-Value. Tipo de codificación de información en mensajes de protocolo.
TTL	Time to Live.
UDP	User Datagrama Protocol. Protocolo de transporte poco fiable usado en IP.

VCI	Virtual Channel Identifier.
VPDN	Virtual Private Dial-up Network.
VPI	Virtual Path Identifier.
VPN	Virtual Private Network. Una red privada virtual realizada sobre una infraestructura compartida.
VRF	Virtual Routing and Forwarding. Tabla de enrutamiento y envío que permite el aislamiento entre diferentes VPN.

CAPÍTULO I

FUNDAMENTOS DE MPLS

1.1 INTRODUCCION

A partir de 1990 existió una gran explosión en el crecimiento del tráfico de red, millones de usuarios corporativos y residenciales se unieron a la red pública de datos (Internet) produciendo que existiese un incremento en el tamaño de las redes físicas y por ende, mayor consumo de ancho de banda. Con el pasar de los años las demandas de servicios son cada vez más múltiples; si anteriormente el Internet transportaba aplicaciones tolerantes en el tiempo tales como FTP, HTTP ó correo electrónico, en la actualidad son aplicaciones en tiempo real como videoconferencia, voz sobre IP (VoIP), telecontrol, entre otras. Siendo así, se desarrollaron nuevas tecnologías y los servicios de capa 2 llegaron a ser una fuente de ingresos significativa para los proveedores de servicios.

En la actualidad la gran mayoría de proveedores manejan múltiples redes en un mismo núcleo o *core* que soportan tecnologías como Frame Relay, ATM lo cual conlleva algunas desventajas como:

- Gastos significativos en la adquisición de los equipos para las diferentes tecnologías.
- Incremento en los costos operacionales.
- Escalabilidad.
- Reducida fiabilidad.
- Deficiente uso de los recursos de la red.

Multiprotocol Label Switching surge como una solución *escalable* cuya magnitud e importancia se resume en una "red multiservicio", es decir múltiples servicios que convergen en un único *core* MPLS.

1.2 PERSPECTIVA HISTÓRICA

El desarrollo de MPLS comienza en los años 90 con las empresas [3] Ipsilon y ***Toshiba*** como pioneras, quienes pusieron en el mercado los productos IP Switching y *Cell Switch Route* respectivamente. En respuesta a estas ofertas a partir de 1996, las compañías ***Cascade Communications*** (*IP Navigator*), ***Cysco Systems*** (*Tag Switching*) e **IBM** (*Aggregate Route-Based IP Switching*) anunciaron sus propios productos. El trabajo realizado por cada una de estas firmas fue realizado con el objetivo común de resolver un conjunto de problemas existentes en las tradicionales redes IP tales como:

- El enrutamiento IP presentaba dificultades tanto en hardware como en software. En hardware por la implementación y en software por la limitación de la tasa de envío de paquetes en los routers IP.
- Existía congestión de red debido a que en el proceso de enrutamiento IP el envío de paquetes era sobrecargado (debido a que envía los paquetes en base a la dirección de destino) y por este mismo hecho, algunas de las líneas principales eran sobre utilizadas mientras otras no eran ocupadas.
- Finalmente, redes IP eran colocadas sobre redes ATM lo cual implica mayores costos.

Dados estos primeros pasos, en abril de 1997 [3] la **IETF** (*Internet Engineering Task Force*) establece el grupo de trabajo MPLS con el fin de desarrollar un estándar común; en su primera serie de estándares publicado en el año 2001 se pueden destacar algunos de los ítems más relevantes:

1) MPLS consiste en la integración de "***label swapping***" con el enrutamiento de capa de red. Con esta base tecnológica se esperaba [1,4]:

- Mayor flexibilidad en la entrega de nuevos servicios de ruteo. MPLS tiene la habilidad de identificar el flujo de un tráfico en particular, es decir distinguir entre diferentes tipos de servicio. Por ejemplo, si se requiere separar paquetes de email de paquetes de video, en los routers tradicionales y mediante el ruteo IP, se escoge un único camino para todos los

paquetes; MPLS escoge diferentes caminos de acuerdo a la aplicación, los mismos que pueden estar basados en diferentes parámetros tales como ancho de banda requerido, **QoS** (Calidad de Servicio), dirección fuente, entre otros.

- Mejorar el desempeño, un ejemplo claro es a través de la Ingeniería de Tráfico. A diferencia del tradicional ruteo IP que siempre toma el camino más corto para el envío de información, usando por lo general las mismas rutas para destinos múltiples y por tanto creando congestión de tráfico; **MPLS-TE** (*MPLS – Traffic Engineering*) posibilita la creación de múltiples túneles al mismo destino y usar diferentes caminos para el envío de la información, proveyendo balance de carga a través de los diferentes enlaces, aliviando la congestión y asegurando la optimización del tráfico en cada router.

- Escalabilidad en el enrutamiento de capa de red, agregando información de envío a través de las etiquetas, mientras se trabaja en presencia de jerarquías de enrutamiento.

En la actualidad el trabajo y esfuerzos de la **IETF** continúan, creándose nuevos grupos de trabajo referidos a MPLS tales como [16] *Layer 3 VPN* (**l3vpn**), *Layer 2 VPN* (**l2vpn**), *Common Control and Measurement Plan (***ccamp***) y Pseudo Wire Emulation Edge to Edge* (**pwe3**).

1.3 DEFINICIÓN DE MPLS

Multiprotocol Label Switching [7] es una tecnología de envío en la cual los paquetes son enviados basados en etiquetas[1]. Su arquitectura describe los mecanismos para ejecutar la conmutación de etiqueta ó *label switching* combinando los beneficios de *IP switching* de la capa 2 con el *IP routing* de la capa 3.

[1] El mecanismo de envío que se realiza a lo largo de la red se denomina *label swapping*.

1.4 CARACTERÍSTICAS DE MPLS

Entre las características más importantes de MPLS se pueden mencionar [7]:

- En *MPLS* los paquetes son enviados basados en etiquetas.
- Las etiquetas pueden corresponder a redes de destino IP o también a otros parámetros tales como dirección fuente, QoS, entre otros.
- El mecanismo de envío a lo largo de la red se denomina *label swapping*.
- MPLS soporta el envío de otros protocolos.

1.5 ARQUITECTURA MPLS

Básicamente la arquitectura MPLS está conformada por dos componentes principales [1,7]: el componente de control (*control plane*) y el componente de envío (*data plane*). Adicionalmente existen nuevos términos introducidos los cuales permiten describir la funcionalidad y roles de cada uno de los equipos o dispositivos que en su conjunto forman la arquitectura. A continuación de manera breve se describen cada uno de ellos.

1.5.1 Red MPLS

Una red MPLS está conformada por una serie de nodos o puntos llamados LSR (*Label Switching Routers*), lo cuales son capaces de conmutar y enviar paquetes IP etiquetados [1].

1.5.2 Componente de control (Control Plane)

La función del componente de control es intercambiar información de ruteo y etiquetas, esto lo realiza mediante complejos mecanismos definidos en estándares tales como **BGP** (*Border Gateway Protocol*)**, OSPF** (*Open Shortest Path First*)**, EIGRP** (*Enhanced Interior Gateway Routing Protocol)* y **TDP** (*Tag Distribution Protocol*)**, LDP** (*Label Distribution Protocol*)**, RSVP** (*Resource Reservation Protocol*) respectivamente [7].

1.5.3 Componente de envío (Data Plane)

La función de este componente es el envío de paquetes basados en etiquetas. En la se observa la arquitectura básica de un nodo MPLS realizando enrutamiento IP.

1.5.4 LSR (Label Switch Router)

Un LSR o router de conmutación de etiqueta es cualquier router o switch que cumple las siguientes funciones:

- Intercambiar información de ruteo.
- Intercambiar etiquetas.
- Enviar paquetes basados en etiquetas o celdas[2].

En una red MPLS se pueden distinguir tres tipos de LSR [2]:

1) LSRs de Ingreso, un LSR de ingreso es un router que está ubicado en la periferia de la red MPLS cuya función es recibir paquetes IP, imponer una etiqueta (ó pila de etiquetas) y finalmente enviarlos al dominio MPLS.
La operación de imposición de etiqueta es conocida como ***Push Action*.**

2) LSRs de Salida, un LSR de salida es un router que está ubicado en la periferia de la red MPLS y cuya función es recibir paquetes IP etiquetados, remover la etiqueta (ó pila de etiquetas) y finalmente enviarlos fuera del dominio MPLS.
La operación de remover la etiqueta es conocida como ***Pop Action*.**

NOTA: los LSRs de entrada y salida son conocidos como **Edge-LSR** y realizan una conmutación basada en FECs (*Forwarding Equivalance Class*).

[2]En la arquitectura ATM, los ATM-LSR envían sólo celdas.

3) LSRs Intermedios, un LSR intermedio es un router que está ubicado en el núcleo de la red MPLS cuya función es recibir paquetes IP etiquetados, cambiar la etiqueta existente por otra y enviarlos al siguiente LSR. Realizan conmutación directa.
La operación de cambiar la etiqueta existente por otra es conocida como ***Swap Action*.**

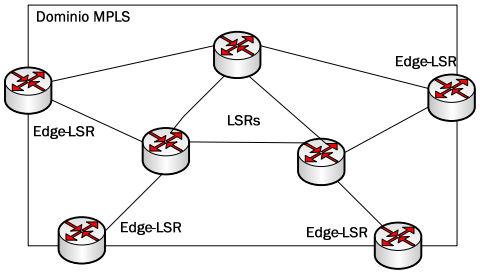


Figura. 1. 1 El LSR y Edge LSR en la red MPLS

1.5.5 FEC (Forwarding Equivalence Class)

Una Clase Equivalente de Envío [3] se define como un conjunto de paquetes IP que comparten los mismos atributos, que son enviados de la misma manera, a través del mismo camino (**LSP** ver sección 1.5.5) y/o requieren el mismo servicio.
Cuando los paquetes entran al dominio MPLS a través del **LSR** de ingreso, éste determina a qué Clase Equivalente de Envío corresponden los mismos y por tanto todos los paquetes que pertenecen a la misma **FEC** tienen la misma etiqueta[3].

1.5.6 LSP (Label Switched Path)

Un LSP se puede definir como un camino lógico, unidireccional de origen a destino que se forma por la concatenación de varios LSRs. El primer LSR de un LSP es el LSR de ingreso el último es el LSR de salida y entre los dos se encuentran los LSR intermedios (figura 1.2).
Un LSP es el mismo para paquetes que pertenecen a la misma FEC.

[3] No todos los paquetes que tienen la misma etiqueta pertenecen a la misma FEC.

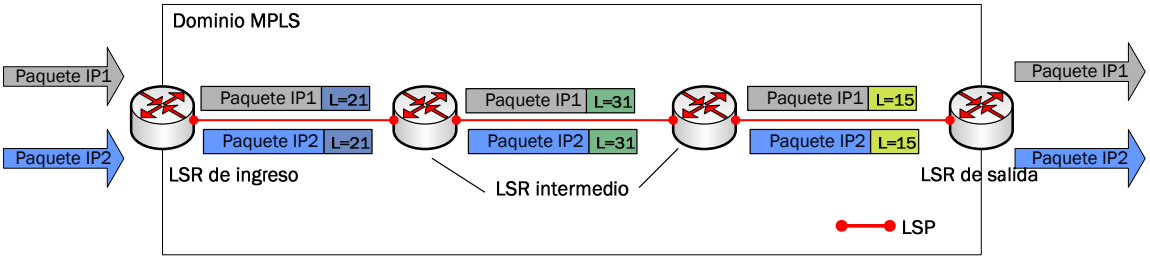


Figura. 1. 2 FEC y establecimiento de un LSP

Existe un caso particular conocido como LSP anidado *ó nested* LSP que consiste en un LSP dentro de otro. Es decir que, no necesariamente el LSR de ingreso del LSP es el primer router que etiqueta el paquete.

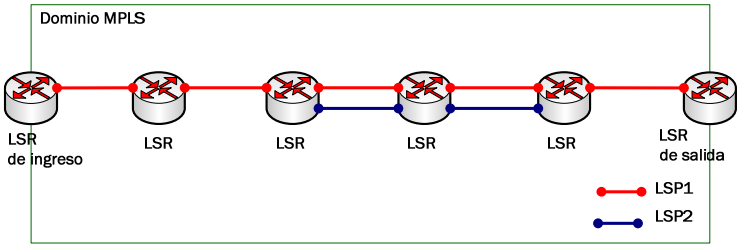


Figura. 1. 3 LSP anidado

1.5.7 Etiqueta MPLS

Una etiqueta MPLS es un conjunto pequeño de 32 bits cuya estructura se puede observar en la figura 1.4. Los campos contenidos en la cabecera MPLS contienen la siguiente información [3]:

Figura. 1. 4 Formato de la cabecera MPLS

- ***Etiqueta,*** este campo está conformado por 20 bits y su valor representa a determinada FEC durante el envío de paquetes. Su valor es usado como un indicador dentro de la tabla de envío almacenada en un LSR.
- ***EXP,*** 3 bits experimentales los cuales son usados para identificar la Clase de Servicio a la que pertenece el paquete.

- ***Bottom of Stack,*** un bit que sirve como indicador en el caso de existir dos o más etiquetas MPLS insertadas en el paquete (*label stack*), el mismo que dice si la etiqueta es la última en la cola.

- ***TTL,*** campo llamado *Time to Live* constituido de 8 bits y que representa el número de saltos que un paquete IP da antes de llegar a su destino. Su valor va decrementando en cada salto, cuando este valor es cero el paquete es eliminado. De esta manera se evita lazos o que el paquete permanezca innecesariamente en la red debido a un enrutamiento erróneo o defectuoso.

1.5.8 Encapsulación MPLS

La etiqueta MPLS o pila de etiquetas (ver sección 1.5.6.2) es insertada entre las cabeceras de capa de enlace y capa de red por lo que es conocida como "*shim header*" o cabecera acuñada (ver figura 1.5).

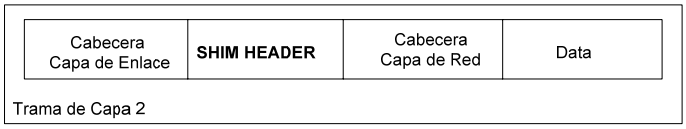


Figura. 1. 5 Cabecera acuñada "shim header" [3]

El uso de la *shim header* permite soportar conmutación de etiqueta sobre algunas tecnologías de capa 2 tales como Ethernet, FDDI, enlaces punto a punto, Token *Ring*, entre otras.

1.5.9 Pila de Etiquetas

Una de las opciones que ofrece *MPLS* es la agregación de dos o más etiquetas a un paquete lo cual se conoce como *label stack.* La primera etiqueta en la cola es conocida como *top label*, la última como *bottom label* y entre ellas se tienen cualquier número de etiquetas.

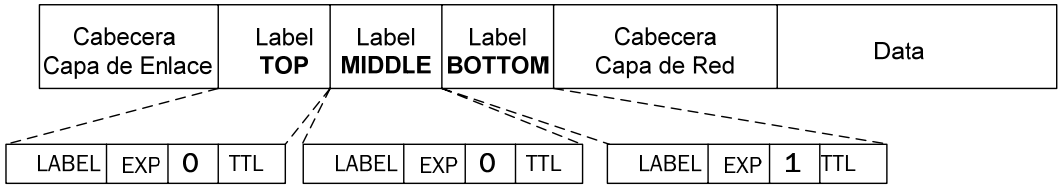


Figura. 1. 6 La pila de etiquetas [3]

Como se muestra en la figura 1.6 el valor del bit perteneciente al campo BoS en el caso de la etiqueta *bottom* es 1 y para el resto es cero. Existen algunas aplicaciones que necesitan más de una etiqueta como por ejemplo MPLS VPNs (2 etiquetas) y MPLS *Traffic Engineering* (2 ó más etiquetas).

1.5.10 Asignación de Etiquetas

En la arquitectura MPLS el LSR es responsable de decidir qué etiqueta asignar a una *FEC* particular. Dicha asignación puede ser [2].

- ***Local***, la asignación de etiqueta es local cuando la etiqueta es escogida y asignada localmente por el router.

- ***Remota,*** la asignación de etiqueta es remota cuando el router recibe información de asignación de etiqueta desde otro LSR.

- ***Downstream,*** se denomina asignación de etiqueta downstream cuando la asociación entre la etiqueta que lleva el paquete y una FEC particular, es creada por el LSR que es

downstream (respecto al flujo de paquetes[4]) con respecto del LSR que pone la etiqueta en el paquete.

- ***Upstream,*** se denomina asignación de etiqueta upstream cuando la asociación entre la etiqueta que lleva el paquete y una FEC particular, es creada por el mismo LSR que pone la etiqueta en el paquete.

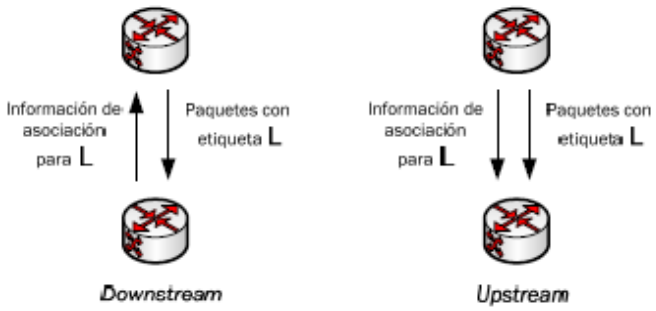


Figura. 1. 7 Asignación de etiquetas upstream y downstream

1.5.11 Modos MPLS

Existen diferentes modos a través de los cuales un LSR puede transmitir etiquetas a otro LSR. Estos modos han sido clasificados de la siguiente manera [2]:

- Modo de distribución de etiqueta.
- Modo de retención de etiqueta.
- Modo control de distribución de etiquetas.

- **Modo de distribución de etiqueta**

En la arquitectura MPLS se distinguen dos modos para distribuir asociación de etiquetas:

[4] Si se considera el caso de un flujo de paquetes fluyendo desde el LSR X al LSR Y, se denominan LSR *upstream* (Ru) y *Downstream* (Rd) respectivamente. Cuando el LSR asocia una etiqueta a una FEC particular, el LSR es *dowstream* respecto a dicha asociación.

- ✓ *Modo de distribución de etiqueta Downstream bajo Demanda (DoD),* cuando un LSR *upstream* solicita una asociación de etiqueta para determinada FEC a un LSR *dowstream.* Cada LSR recibe una asociación de etiqueta por FEC únicamente de su LSR *downstream*.

- ✓ *Modo de distribución de etiqueta Downstream no solicitado (UD),* sucede cuando cada LSR asocia una etiqueta a determinada FEC a los LSR adyacentes sin que ellos lo soliciten, es decir que en este modo un LSR recibe una asignación remota desde cada LSR adyacente.

- **Modo de retención de etiqueta**

Cuando un LSR recibe o ha recibido la asignación de una etiqueta para una FEC en particular desde un router *downstream*, aunque el router *downstream* no sea el próximo salto del router *upstream* para la FEC en cuestión, entonces el router *upstream* puede conservar el rastro de la asignación o descartarla. Siendo así, se definen dos modos de retención de etiqueta, los cuales son:

- ✓ *Modo de Retención de Etiqueta Liberal (LLR),* sucede cuando se retienen las asociaciones de etiqueta/FEC que se reciben en los LSR que no son del próximo salto para una FEC dada.

- ✓ *Modo de Retención de Etiqueta Conservador (CLR),* sucede cuando se descartan las asociaciones de etiqueta/FEC que se reciben en los LSR que no son del próximo salto para una FEC dada. Por tanto, el LSR únicamente retiene las asignaciones de etiqueta a una *FEC* por medio de los router *downstream* vecinos actuales.

- **Modo control LSP**

En la arquitectura MPLS se definen dos modos para asociar. Estos modos son:

- ✓ *Modo control LSP Independiente,* sucede cuando un LSR crea una asociación local para una *FEC* cuando éste reconoce la misma, es decir que el prefijo para la FEC está es su tabla de ruteo y independientemente de los otros LSRs.

- ✓ *Modo control LSP Ordenado,* sucede cuando un LSR crea una asociación local para una FEC sólo si reconoce que él es el LSR de salida para la FEC, ó si ha recibido una asociación local desde el siguiente salto para dicha FEC.

1.6 LABEL SWITCHING

En las arquitecturas de enrutamiento tradicionales, el enrutamiento de capa de red puede ser dividido en dos componentes: el de envío y control. Estos componentes no son aplicados únicamente a dichas arquitecturas, sino también nos permiten describir y entender la arquitectura de conmutación de etiqueta ó *label switching.*

Básicamente en el enrutamiento de capa de red estos componentes realizan las siguientes funciones [3]:

Componente de envío, es responsable del envío de paquetes de entrada a salida a través de los routers mediante una decisión de envío sobre el paquete; dicha decisión está basada en dos fuentes de información. *i)* Tabla de envío que guarda el router y *ii*) la información que tiene el paquete. Siendo así, el componente de envío consiste de un juego de procedimientos o algoritmos que el router usa para realizar la decisión de envío.

Componente de Control, es responsable de la creación y almacenamiento de la tabla de envío. El componente de control consiste de uno o más protocolos de enrutamiento que provee información de enrutamiento y que es intercambiada entre ruteadores. Y también de procedimientos o algoritmos que el router usa para convertir dicha información en la tabla de envío.

1.6.1 Label Switching: Componente de Envío

En la arquitectura de conmutación de etiqueta ó *label switching* el componente de envío usa dos fuentes de información en su algoritmo para hacer la decisión de envío sobre el paquete:

- ✓ La tabla de envío almacenada por un LSR.
- ✓ La etiqueta que lleva el paquete (Ver sección 1.5.6).

- ***Label Forwarding Information Base (LFIB)***

La tabla LFIB es usada durante el reenvío actual de paquetes etiquetados y es almacenada por el LSR. Está conformada por una secuencia de entradas, donde cada entrada consiste de una etiqueta de entrada y una o más subentradas. A su vez cada subentrada consiste de una etiqueta e interface de salida y la siguiente dirección de salto.

- **Algoritmo de Envío**

El algoritmo de envío usado por el componente de envío de *label switching* está basado en el concepto de *label swapping***,** el mismo que trabaja de la siguiente manera:

1) El LSR que recibe el paquete etiquetado, extrae la etiqueta del paquete y la usa como un índice en su tabla de envío LFIB**.**

2) Cuando una entrada (la cual tiene su etiqueta de entrada igual a la etiqueta que fue extraída del paquete) es encontrada en la tabla de reenvío, por cada subentrada (que pertenece a dicha entrada encontrada) el router reemplaza la etiqueta del paquete por una etiqueta saliente y envía el paquete por la interface de salida especificada para dicha subentrada así como el siguiente salto.

Cabe mencionar que una etiqueta siempre lleva semántica de envío y opcionalmente puede también llevar semántica de reservación de recursos. *i*) Semántica de envío ya que la etiqueta en el paquete únicamente determina una entrada particular en la tabla de envío y dicha entrada particular contiene información acerca de dónde el paquete será enviado. Y, *ii*) Semántica de reservación de recursos porque la entrada determinada por la etiqueta puede opcionalmente incluir información relacionada a qué recursos el paquete puede usar.

En tecnologías como ATM o Frame Relay la etiqueta en dichas cabeceras llevan ambas semánticas. En MPLS se tiene algunas opciones; en primer lugar la información relacionada con los recursos que el paquete puede usar puede ser codificada como parte de la *shim header* de modo que la etiqueta llevaría únicamente semántica de envío. En segundo lugar, usar la parte etiquetada y la no etiquetada de la *shim header* para codificar dicha información de reservación y finalmente con la *shim header* se puede llevar ambas, semántica de envío y reservación de recursos.

Entre las propiedades más significativas del algoritmo de envío usado por el componente de envío de *label switching* son:

- ✓ A través de él, un LSR es capaz de obtener toda la información requerida para enviar paquetes así como decidir qué recursos el paquete puede usar en una sola memoria de acceso. Esta propiedad hace de *label switching* una tecnología de alto desempeño de envío.

- ✓ Su implementación en hardware es económica, lo cual a su vez permite un rendimiento de envío rápido.

Es importante destacar que en las arquitecturas de enrutamiento tradicionales, diferentes aplicaciones provistas por el componente de control tales como enrutamiento *Unicast, Unicast* con Tipos de Servicio y *Multicast*, por ejemplo, requieren múltiples algoritmos de envío en el componente de envío. En MPLS, el componente de envío de *label switching* cosiste de un solo algoritmo el cual están basado en *label swapping*. Esto no significa una limitación sino más bien un amplio rango de aplicaciones con un único algoritmo.

- **Surgimiento de una solución multiprotocolo**

El componente de envío no está especificado para una capa de red particular, lo cual hace de *label switching* una solución multiprotocolo con respecto de los protocolos de capa de red. Es decir, *label switching* tiene la habilidad de soportar múltiples protocolos de capa de red y operar virtualmente sobre protocolos de capa de enlace por lo que es una solución multiprotocolo respecto de los protocolos de capa de enlace (figura 1.8). Es por esta razón se explica el nombre que el grupo de trabajo de la IETF estandarizó la tecnología como *Multiprotocol Label Switching.*

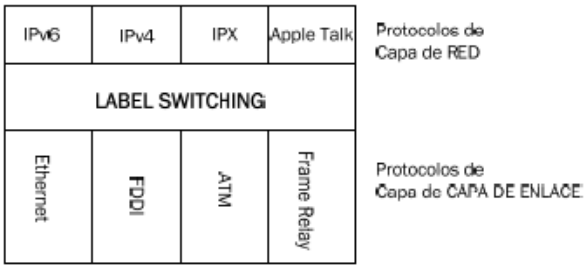


Figura. 1. 8 MPLS una tecnología Multiprotocolo [3].

1.6.2 Label Switching: Componente de Control

Como se mencionó anteriormente, la descomposición del enrutamiento de capa de red en el componente de envío y control no aplica únicamente a las arquitecturas de enrutamiento tradicionales, sino también en la arquitectura de conmutación de etiqueta ó *label switching*.
En la figura 1.9 se puede observar de manera global en qué consiste la estructura del componente de control de la arquitectura de conmutación de etiqueta.

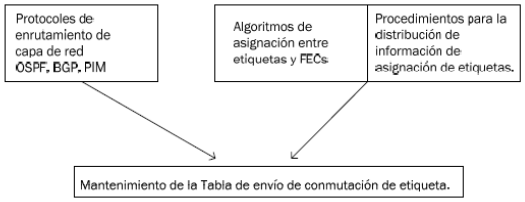


Figura. 1. 9 Label Switching: componente de control [3]

Mediante el componente de control, un LSR es provisto por dos fuentes de mapeo para construir la tabla de envío usada por el componente de reenvío. *i*) El mapeo entre las FECs y las siguientes direcciones de salto provistas por los protocolos de enrutamiento de capa de red y *ii*) el mapeo entre etiquetas y FECs mediante los algoritmos de creación de asignación de etiquetas/FECs y los de distribución de etiqueta entre los *switches*. Con lo cual el componente de control en la conmutación de etiqueta es responsable de *i*) distribuir información de ruteo entre los LSRs y *ii*) procedimientos ó algoritmos que el router usa para convertir dicha información en la tabla de envío.

- ***Label Information Base (LIB)***

Es la tabla donde se guardan las etiquetas que se usan como índice para realizar la asignación etiqueta/FEC. Es decir, que guarda todas las asignaciones de etiquetas que hace el LSR de ingreso cuando llega un paquete IP antes de ingresar al dominio MPLS y las asignaciones de estas etiquetas a las etiquetas recibidas por sus vecinos MPLS.

Cada LSR de ingreso crea una asignación local, es decir, liga una etiqueta al prefijo *IPv4* y distribuye esta asociación a todos sus vecinos LDP. Para sus vecinos LDP estas asignaciones recibidas llegan a ser asignaciones remotas. Los vecinos LSP, entonces almacenan las asignaciones locales y remotas en una tabla conocida como ***Label Information Base***. Cabe recalcar que cada LSR tiene únicamente una asignación local por prefijo cuando el espacio de etiqueta es por plataforma. Pero cuando el espacio de etiqueta es por interface una asignación local puede existir por prefijo por interface.

- ***Routing Instance Base (RIB)***

Esta tabla proporciona información sobre la red de destino y prefijos de subred usados para la asociación de etiquetas. Es decir proporciona la siguiente dirección de salto.

- ***Distribución de etiqueta* [2]**

Como parte de la estructura del componente de control están aquellos algoritmos por medio de los cuales un LSR informa a otro una asignación (creada ó destruida) etiqueta/FEC. Esta distribución de información de etiqueta se puede realizar por medio de dos caminos:

- ✓ "*Piggyback*[5]" de etiquetas en un protocolo de enrutamiento existente.
- ✓ A través de un protocolo de distribución de etiqueta.

- ***Piggyback de etiquetas en un protocolo de enrutamiento existente***

Este primer método consiste en que los protocolos de enrutamiento IP existentes sean extendidos de manera que puedan transportar/llevar la o las etiquetas haciéndose innecesario la existencia de un nuevo protocolo. Cabe mencionar que ninguno de los Interior Gateway *Protocol's* (por ejemplo, *Open Shortest Path First* [OSPF], *Intermediate System-to-Intermediate System* [IS-IS], y *Enhanced Interior Gateway Routing Protocol* [EIGRP]) ha sido cambiado para que transporte etiquetas, sin embargo el protocolo de enrutamiento *Border Gateway Protocol* [BGP], que no pertenece al grupo de IGP's puede transportar prefijos y distribuir etiquetas al mismo tiempo.

- ***Protocolo de distribución de etiqueta***

El segundo método consiste en utilizar un protocolo diferente e independiente para distribuir etiquetas. Siendo así, la alternativa de los fabricantes de routers fue tener un nuevo protocolo de distribución de etiqueta para prefijos *IGP* surgiendo el protocolo de distribución de etiqueta (*Label Distribution Protocol* [LDP]). Sin embargo este protocolo no es el único a través del cual se puede distribuir etiquetas sino también *Tag Distribution Protocol* [TDP] y *Resource Reservation Protocol* [RSVP].

---

[5] En inglés el término piggyback significa llevar a alguien a hombros o a sus cuestas. En telecomunicaciones, la trama ACK contiene una cantidad mínima de información útil, pero además ha de contener una serie de campos de control que ocupan más bits. Cuando se están transmitiendo datos en ambas direcciones, en vez de enviar el ACK en una trama se lo envía dentro de una trama de datos de tal manera que el ACK viaja "casi gratis" ahorrando de esta manera se ahorra el envío de una trama. Esta técnica se conoce como piggybacking o piggyback.

Es importante mencionar que TDP fue el protocolo que antecedió a LDP, el cual fue desarrollado e implementado por Cisco y por ende de su propiedad; siendo así la IETF formalizó el protocolo LDP el cual opera de manera similar que TDP pero con la diferencia que es más funcional. Por tanto, TDP se convirtió en un protocolo obsoleto siendo reemplazado rápidamente por el protocolo LDP.
Finalmente, el protocolo RSVP es utilizado únicamente en Ingeniería de Tráfico ó MPLS TE (*MPLS Traffic Engineering*).

1.7 PROTOCOLO DE DISTRIBUCIÓN DE ETIQUETA

El protocolo de Distribución de Etiqueta (*Label Distribution Protocol* [LDP]), es un protocolo que define una serie de procedimientos y mensajes a través de los cuales un LSR informa a otro cuando ha realizado una asociación etiqueta/FEC y sirve para la creación, establecimiento de un LSP. Es un protocolo útil en los casos donde un LSR no soporta *piggybacking*, es bidireccional y opera entre LSRs que son o no adyacentes [2].

1.7.1 Mensajes LDP

Cuando dos LSRs están corriendo el protocolo LDP intercambian cuatro tipos de mensajes [12,14]:

1) ***Mensajes de descubrimiento***, los LSRs deben descubrir a los demás LSRs por medio de mensajes de saludo ó *Hello messages* por lo que periódicamente mandará por la red dichos mensajes a través de un puerto UDP (646) con la dirección *multicast*. Los mensajes de descubrimiento sirven para anunciar y mantener la presencia de un LSR en la red MPLS.

2) ***Mensajes de sesión,*** los mensajes de sesión se utilizan para establecer, mantener y terminar sesiones entre pares LDP. Por medio de una conexión TCP un LSR utilizará un procedimiento de iniciación LDP.

3) ***Mensajes de anuncio,*** son usados para crear, cambiar o borrar asociaciones etiqueta/FEC y son transportados vía TCP. Finalmente,

4) ***Mensajes de notificación,*** se transportan vía TCP y son mensajes cuyo objetivo es proporcionar a los vecinos LDP información de avisos y señalización de errores. Las notificaciones de aviso se utilizan para pasar a un LSR información de la sesión LDP o el estado de algún mensaje anterior. El segundo tipo se utiliza para notificar errores por los cuales se termina la sesión y se descarta las asociaciones de etiquetas realizadas en la misma.

1.7.2 Espacios de etiqueta MPLS

El espacio de etiqueta es un conjunto de etiquetas del cual se asociará una etiqueta a una determinada FEC. En LDP existen dos tipos de espacios de etiquetas [5]:

- ***Por interfaz,*** un espacio de etiqueta es por interfaz cuando una etiqueta asignada a una interfaz puede ser nuevamente usada en otra interfaz con una dirección diferente de destino. Estas etiquetas deben ser únicas para determinada interfaz de entrada. Por tanto las etiquetas están ligadas a la interfaz de donde el paquete fue recibido.

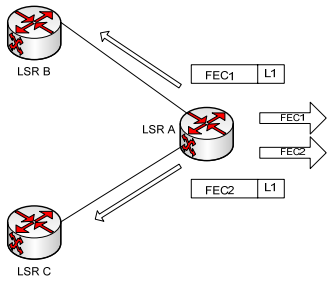


Figura. 1. 10 Espacio de etiqueta por interfaz

- ***Por plataforma***, un espacio de etiqueta es por plataforma cuando una única etiqueta es asignada a una red de destino y anunciada a todos sus vecinos. La etiqueta es localmente

única y válida sobre todas la interfaces de entrada es decir puede ser usada sobre cualquier interfaz de entrada.

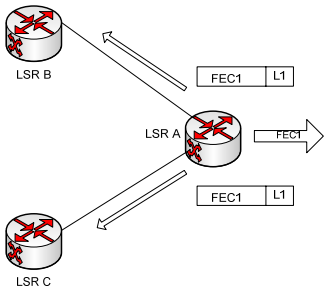


Figura. 1. 11 Espacio de etiquetas por plataforma

1.7.3 Pares LDP

El protocolo LDP realiza una asociación etiqueta/FEC; dos LSRs que usan LDP para intercambiar información de asociación etiqueta/FEC son conocidos como LDP peers (pares LDP) los cuales establecen una sesión entre ellos. LDP permite a un LSR distribuir etiquetas a sus pares LDP a través del puerto TCP 646.

1.7.4 Identificadores LDP

Un identificador LDP es un campo conformado de seis octetos donde los cuatro primeros identifican al LSR y los dos últimos identifican el espacio de etiquetas. Éste es utilizado para identificar el espacio de etiquetas de un LSR. Cuando los dos últimos octetos son cero el espacio de etiqueta será por plataforma.
El identificador LDP está representado por la nomenclatura definida por la especificación RFC3036 tal como se muestra en la figura 1.12.

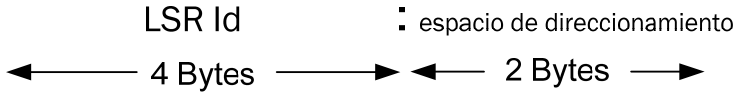


Figura. 1. 12 Nomenclatura del identificador LDP

1.7.5 Sesión LDP

En la especificación RFC 3036 se definen dos fases para el establecimiento de la sesión LDP: *i*) descubrimiento y *ii*) establecimiento y mantenimiento de sesiones LDP.

- ***Descubrimiento***

El mecanismo de descubrimiento LDP utiliza UDP como protocolo de transporte. Se pueden diferenciar dos modalidades de descubrimiento:

1) Descubrimiento básico, es un mecanismo utilizado para descubrir qué vecinos LSR están directamente conectados en el enlace. En esta modalidad un LSR envía periódicamente mensajes de saludo a un puerto con la dirección multicast (todos los ruteadores de la red). A su vez los ruteadores continuamente están escuchando a través del puerto esperando recibir los mensajes de saludo. Llega un momento en que el LSR conoce todos los LSRs con los que tiene una conexión directa.

2) Descubrimiento extendido, con el descubrimiento extendido se pretende localizar LSRs que no están conectados directamente en el enlace. Así mismo, en esta modalidad un LSR envía periódicamente mensajes de saludo a un puerto (UDP) bien conocido y con una dirección específica la cual obtuvo de algún modo (por configuración por ejemplo). El LSR al cual se están enviando los mensajes de saludo tiene la posibilidad de responder o ignorar el mensaje. En caso de que decida aceptar, debe mandar periódicamente mensajes de saludo al LSR que inició el proceso.

- ***Establecimiento y mantenimiento de sesiones LDP***

Cuando se ha logrado conocer los vecinos LDP se puede establecer la sesión la cual consta de dos fases:

1) Establecimiento de la conexión de transporte, establecimiento de una conexión TCP entre LSRs implicados.

2) Inicio de la sesión, establecida la conexión TCP, los LSRs deben negociar los parámetros de la sesión lo cual se logra intercambiando mensajes de iniciación. Dichos parámetros incluyen la versión del protocolo LDP, método de distribución de etiquetas, etc. Los LSRs implicados pueden desempeñar un papel activo o pasivo, si el LSR está jugando un papel activo, éste iniciará la negociación de los parámetros de la sesión enviando un mensaje de iniciación al LSRb, el cual contendrá el identificador LDP del LSRa y del LSRb.

   Cuando el LSRb recibe el mensaje de iniciación lo mirará determinando si los parámetros son aceptables; en caso de serlo, responderá con su propio mensaje de iniciación proponiendo los parámetros que desea usar y un mensaje de mantenimiento conocido como *KeepAlive* para notificar al otro LSR que acepta los parámetros. Si dichos parámetros no son aceptables, responderá con un mensaje de notificación de error de parámetros rechazados.

1.7.6 Codificación de los mensajes

Los mensajes intercambiados entre LSRs pares son enviados como **PDUs** (*Protocol Data Unit*) a través de la sesión LDP y conexiones TCP.

- ***PDU (Protocol Data Unit)***

Un PDU LDP es una cabecera LDP seguido por uno o más mensajes LDP, el cual puede transportar uno o más mensajes LDP. El formato de la cabecera PDU se muestra a continuación con sus respectivos campos.

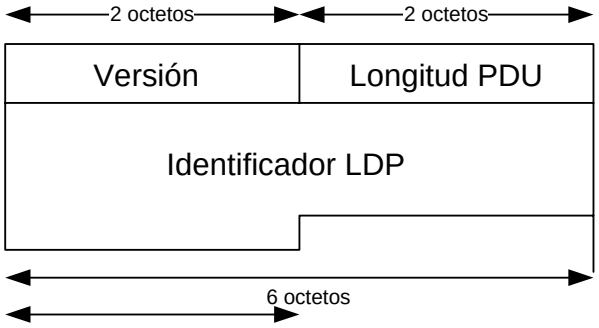


Figura. 1. 13 Formato de un PDU

Versión: dos octetos que representan y contienen el número de versión del protocolo. Actualmente es uno.

Longitud PDU: dos octetos que especifican la longitud total en octetos del PDU excluyendo los campos de la versión y de longitud del PDU[6].

Identificador LDP: campo de seis octetos que ha sido definido en la sección anterior.

- **Codificación TLV (Type-Lenght-Value)**

En el protocolo de distribución de etiqueta todos los mensajes utilizan un esquema de codificación conocido como TLV **(***Type-Lenght-Value***)** cuya cabecera tiene el siguiente formato:

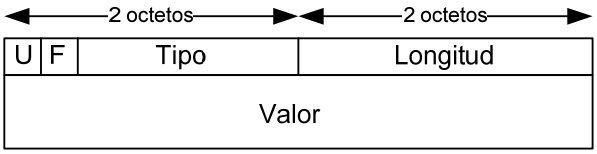


Figura. 1. 14 Formato de la cabecera TLV

Donde,

Bit U*: unknown bit* ó bit desconocido. Si su valor es cero se envía un mensaje de notificación al *LSR* de origen y se ignora el mensaje. Si su valor es uno se ignora el mensaje de notificación.

[6] La longitud del PDU es negociable cuando se inicia la sesión LDP. Antes de la negociación, el tamaño máximo admitido es de 4096 octetos.

Bit F: *forward unknown bit* ó bit de reenvío de una TLV desconocida. Este campo sólo se utiliza si en bit desconocido U está activo. Es decir si F=0 la TLV desconocida no es enviada, caso contrario si F=1 la TLV desconocida se reenvía.

Tipo: campo de catorce bits por el cual se define el tipo de mensaje y el que indica cómo debe ser procesado el campo de Valor.

Longitud: campo de dieciséis bits que especifica la longitud del campo de valor dado em octetos.

Valor: campo de longitud variable que codifica la información a ser interpretada como lo especifique el campo tipo. A su vez, este campo puede tener TLVs.

- **Codificaciones TLV comunes**

  En la versión uno del protocolo existen las siguientes TLV definidas:

  - ✓ FEC: TLV que contendrá las FECs que se intercambian los LSRs. Una FEC podrá ser un prefijo de dirección o una dirección completa de un host.

  - ✓ Etiquetas: TLVs que sirven para codificar etiquetas. Las TLVs de etiquetas son transportadas por los mensajes de anuncio, petición liberación y retiro de etiquetas.

  - ✓ Tipos de TLVs de etiquetas:
    Etiqueta genérica: un LSR utiliza este tipo de TLV para codificar etiquetas que se van a usar en donde sus valores son independientes de la tecnología del nivel de enlace.

    Etiqueta ATM: usada para codificar etiquetas en enlaces ATM y contiene los valores ATM VPI/VCI.
    Etiqueta de retransmisión de tramas (Frame Relay): usada para codificar etiquetas que se usarán en enlaces Frame Relay y contiene valores DLCI de Frame Relay.

- ✓ Lista de direcciones: TLV actualmente definida para IPv4 y que aparece en los mensajes de dirección y retiro de etiquetas.

- ✓ Cuenta de saltos: aparece como un campo opcional en los mensajes que establecen los LSPs. Calcula el número de saltos LSR a medida que el LSP se establece. También se puede usar para la detección de bucles.

- ✓ Vector camino: se utiliza conjuntamente con la TLV de cuenta de saltos en los mensajes de petición y asociación de etiquetas para implementar el mecanismo opcional de detección de bucles.

- ✓ Estado: los mensajes de notificación transportan TLVs de estado para especificar los eventos que se están señalizando.

- ✓ Estado extendido: TLV de estado con información adicional.

- ✓ PDU devuelta: puede operar con la TLV de estado. Un LSR la utilizará para devolver parte de la PDU LDP que le envió otro LSR.

- ✓ Mensaje devuelto: se puede usar conjuntamente con la TLV de estado. Sirve para devolver parte de un mensaje LDP al LSR que lo envió.

- ✓ Parámetros HELLO comunes: se usa para manejar mensajes HELLO por lo cual contiene parámetros comunes.

- ✓ Dirección de transporte IPv4: permite que se use una dirección IPv4 al abrir una conexión TCP.

- ✓ Número de secuencia de configuración: identifica el estado de configuración del LSR emisor y por tanto para que el LSR receptor detecte cambios en la configuración.

- ✓ Dirección de transporte IPv6: esta TLV permite que se use una dirección IPv6 al abrir una conexión TCP.

- ✓ Parámetros comunes de la sesión: contiene los valores propuestos por el LSR emisor para los parámetros que pretende negociar en una sesión LDP.

- ✓ Parámetros de la sesión ATM: esta TLV contiene las capacidades de un LSR ATM también existen estos parámetros para retransmisión de tramas.

- ✓ Identificador del mensaje de petición de etiquetas: este valor es el identificador del mensaje de petición de etiquetas.

- ✓ Privada de vendedor (propietaria): usada para transmitir información de privada de vendedor (propietaria). Y finalmente,

- ✓ Experimental: para usos experimentales.

1.7.7 Mensajes LDP

Los mensajes *LDP* sin excepción tienen el siguiente formato:

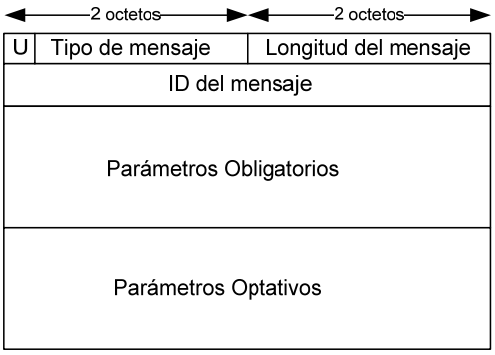


Figura. 1. 15 Formato mensaje LDP

Bit U: *unknown bit* o bit de mensaje desconocido. Al recibir un mensaje desconocido, si U = 0 se enviará una notificación al origen del mensaje. Si U = 1 simplemente se ignorará.

Tipo de mensaje: quince bits, campo que identifica el tipo del mensaje.

Longitud del mensaje: campo de dieciséis bits que especifica la longitud del identificador del mensaje, de los parámetros obligatorios y de los parámetros opcionales

Identificador del mensaje: treinta y dos bits, identificador del mensaje.

Parámetros: son campos de longitud variable. Los parámetros contienen los TLVs y pueden ser obligatorios u optativos. Obligatorios, conjunto de todos los parámetros obligatorios de los mensajes (algunos mensajes no tienen parámetros obligatorios). Y optativos, conjunto de los parámetros opcionales de los mensajes.

En la versión 1 del protocolo de distribución de etiqueta se han definido los siguientes tipos de mensajes (figura 1.16):

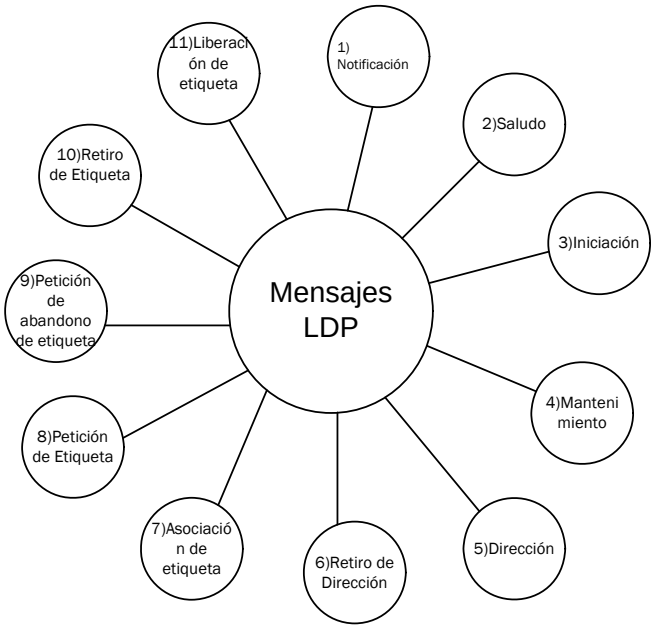


Figura. 1. 16 Mensajes en LDP

1) Mensaje utilizado por un LSR para notificarle a su par de una condición de error o para suministrarle información de aviso

2) Mensajes que son intercambiados entre pares LDPs durante la fase de descubrimiento.

3) Este mensaje se utiliza cuando dos pares LDP desean establecer una sesión LDP.

4) Mensajes que los intercambian pares LSRs para monitorizar la integridad de la conexión de transporte de la sesión LDP.

5) Mensaje que lo envía un LSR a su par para notificarle las direcciones de sus interfaces. El LSR que reciba este mensaje utilizará las direcciones aprendidas para actualizar una base de datos para las correlaciones entre los identificadores LDP de los pares y las direcciones de los siguientes saltos.

6) Mensaje que se utiliza para retirar las direcciones de interfaces notificadas anteriormente.

7) Mensaje que utiliza un LSR para notificarle a su par LSR una asociación de etiquetas.

8) Mensaje que un envía LSR a su par cuando quiere solicitarle una asociación de etiquetas.

9) Mensaje que abandona una petición de etiquetas pendiente.

10) Mensaje que se utiliza para retirar una asociación de etiquetas que está siendo usada. Un LSR le enviará este tipo de mensaje a su par LSR para indicarle que no puede continuar usando la asociación que previamente anunció. De esta forma se rompen las asociaciones entre etiquetas y FECs.

11) Este mensaje se utiliza cuando un LSR quiere informar a su par LSR que ya no necesita una asociación pedida o advertida anteriormente por su par LSR.

1.8 PROTOCOLO RSVP

El Protocolo de Reserva de Recursos (*Resource reSerVation Protocol* [RSVP]) es un protocolo de señalización que reserva recursos para una sesión en un entorno de red antes de empezar la transmisión información. Es un protocolo que se apoya en IP y cuya finalidad es proporcionar calidad de servicio estableciendo una reserva de recursos para un flujo determinado. Entre las principales características podemos mencionar [12,15]:

- Es un protocolo de reserva de recursos, que no transporta datos de usuario y cuyo objetivo no es determinar dónde se reenvían los paquetes sino de la calidad de servicio QoS de los paquetes que son reenviados de acuerdo con el enrutamiento.
- RSVP no es un protocolo de enrutamiento y está orientado al receptor ya que la reserva de recursos es iniciada por el receptor.
- Protocolo que permite diferentes tipos de reservas.
- No es un protocolo de transporte pero soporta IPv4 e IPv6.

1.8.1 Mensaje RSVP

Un mensaje RSPV está constituido de una cabecera normal, seguida de un número variable de objetos de longitud variable.

Vers: versión del protocolo, actualmente es la 1.
Flags: no está definido.
Msg Type: tipo de mensaje.
RSVP Chcksum: campo de verificación
Send_TTL: *Time To Live*, tiempo de vida del mensaje.
RSVP Length: longitud total del mensaje en bytes (cabecera y cuerpo)

- **Tipo de Mensajes**

Los dos mensajes fundamentales son:

Mensajes Path, son mensajes generados por el emisor quien hace uso de los mismos para establecer el camino de la sesión, por tanto estos mensajes son responsables del inicio de la sesión y son enviados a los participantes potenciales de la sesión.
Los mensajes *path* describen el flujo del emisor, y proveen información sobre el camino de retorno hacia el emisor. Cabe mencionar que al no poseer una dirección *IP* de origen ni destino, los mensajes RSVP pueden atravesar ruteadores que no entienden RSVP.

Mensajes Resv, son mensajes generados por los receptores que crean el estado de reserva en los ruteadores a través de una petición de reserva de recursos. Una petición, por lo general, implicará una reserva en todos los nodos del camino del flujo de datos. Por tanto el mensaje Resv se envía en respuesta del mensaje *Path*.

Pero de igual importancia: Path_Err, Resv_Err, PathTear, ResvTear, ResvConf.

1.8.2 Funcionamiento

1) La fuente o emisor envía un mensaje *Path* a los destinos a través de una dirección de sesión (Esta dirección puede ser *unicast* o *multicast*).

2) Al recibir el mensaje *Path* el destino/receptor, éste enviará un mensaje *Resv* a la fuente, el mismo que viajará por el camino inverso al mensaje *Path.*

3) El mensaje *Resv* identificará la sesión para la cual desea realizar la reserva. Y finalmente

4) El mensaje será reenviado hacia el emisor/fuente por los ruteadores los cuales reservarán los recursos necesarios analizando dicho mensaje.

1.9 PROTOCOLO CR-LDP EXTENSIONES DE LOS PROTOCOLOS LDP Y RSVP

En la actualidad existen extensiones para los protocolos LDP y RSVP [12] los cuales han sido desarrollados como complemento a estos protocolos.

1.9.1 CR-LDP (Constraint-based Routing LDP)

CR-LDP es un protocolo de señalización desarrollado con el objetivo de soportar rutas explícitas ó túneles, satisface las necesidades de QoS y además soporta CoS (Clase de Servicio).

- CR-LDP es una ampliación de LDP cuyo algoritmo CR (*Constraint-based Routing*) es de enrutamiento restringido que calcula los trayectos basándose en recursos reservados sin considerar la carga instantánea de los enlaces.
- CR-LDP usa los mensajes de LDP pero define TLVs adicionales en los mismos extendiéndose para implementar ingeniería de tráfico, no requiere de la implementación de un protocolo adicional.
- CR-LDP usa UDP para descubrir pares MPLS y TCP para el control, administración, petición de etiqueta y *label mapping*.

1.9.2RSVP-TE (RSVP Traffic)

RSVP-TE es un protocolo de señalización desarrollado con el objetivo de soportar distribución de etiquetas y rutas explícitas ó túneles.

- El uso de RSVP-TE en una red MPLS no implica una implementación completa del protocolo RSVP para que corra en un LSR, sólo basta extensiones con las cuales se logre soportar enrutamiento explícito.

- RSVP-TE usa datagramas UDP como mecanismo de señalización para establecer un LSP, lo cual incluye el descubrimiento del par, la petición, asignación de etiquetas y administración.

1.10 OPERACIÓN MPLS

Una vez que se ha aclarado y diferenciado cada uno de los componentes, términos, protocolos que la arquitectura de conmutación de etiqueta MPLS maneja, es necesaria una recopilación ordenada de la información de manera que se pueda resumir en algunos pasos cómo es el funcionamiento de la arquitectura. Este funcionamiento se puede simplificar gráficamente con el plano de control y datos de un Edge LSR y el LSR como se muestra a continuación [1,3]:

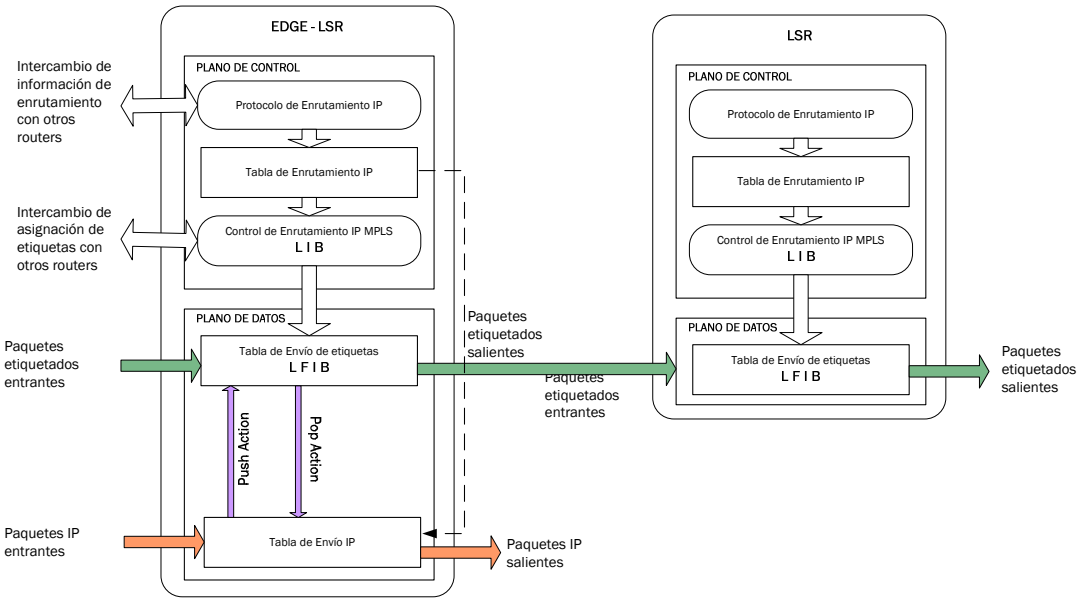


Figura. 1. 17 Operación MPLS desde el punto interno del Edge LSR y LSR [1]

Donde,

1) Un paquete entra al dominio MPLS a través de un LSR de ingreso, el paquete puede ser enviado como un paquete IP puro a otros puntos fuera de la red MPLS ó puede ser etiquetado y enviado a otro nodo MPLS. En el segundo caso cuando el paquete debe ser

enviado a otro punto MPLS, el LSR de ingreso asocia el paquete con una FEC y por ende a un LSP particular.

La FEC para un paquete puede determinarse por uno o varios parámetros, los cuales son especificados por la persona que administra la red.

En la figura 1.18, el host A envía un paquete IP puro al LSR V el cual es el LSR de ingreso de la red MPLS. Este asocia al paquete a una FEC particular y por ende a un LSP, asignando al mismo una etiqueta "*push action*". La etiqueta se almacena en la LIB la cual será utilizada como índice para cuando lleguen otros paquetes que serán asociados a la misma FEC.

2) Cuando el paquete viaja hacia el siguiente salto es decir hacia el LSR W, éste examina el paquete determinando la interfaz y etiqueta de entrada y mira en la tabla LFIB la interfaz y etiqueta de salida asociadas a dichas entradas. Los valores de la etiquetas son cambiados por un nuevo valor "*swap action*" y enviados al siguiente salto según la información proporcionada por la tabla RIB.

En la figura 1.18, los paquetes con la etiqueta 15 son enviados fuera a través de una interfase hacia el LSR X y con una nueva etiqueta la 19; los paquetes con la etiqueta 10 son enviados hacia el LSR Y con la etiqueta 62.

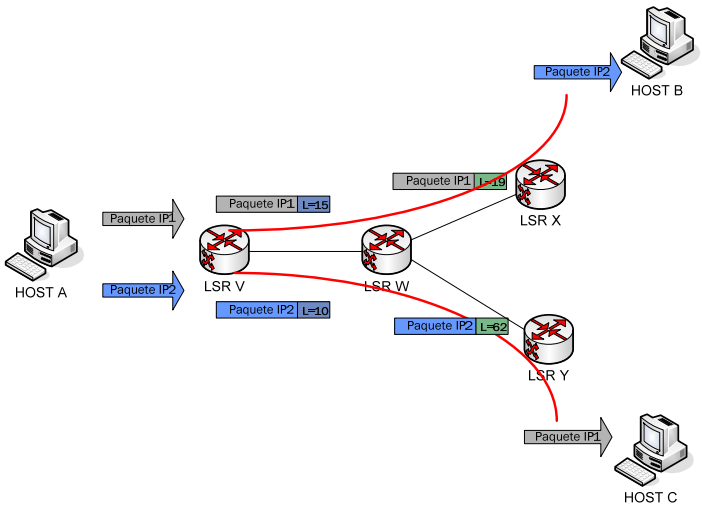


Figura. 1. 18 Viaje de paquetes a través de la red MPLS [3]

3) Finalmente el LSR X y el LSR Y son LSRs de salida los mismos que remueven la etiqueta "*push action*" y envían el paquete al Host B y C respectivamente como paquetes IP puros.

1.11 APLICACIONES CON MPLS

La tecnología de conmutación de etiqueta MPLS puede ser usada en diferentes aplicaciones, independientemente de cuál sea, la funcionalidad de cada una está divida en el plano de control y de datos.

Por tanto,

- Las aplicaciones difieren sólo en el plano de control.
- Todas las aplicaciones utilizan en forma común el plano de datos: conmutación de etiquetas, a excepción de un *Edge LSR* donde puede diferir.
- En general, una etiqueta es asignada a una FEC.

Entre las aplicaciones se pueden mencionar [7]:

- *Unicast IP Routing.*
- *Multicast IP Routing*.
- Ingeniería de Tráfico.
- Calidad de Servicio.
- Redes Privadas Virtuales, MPLS VPNs.
- AToM.

1.12 ASPECTOS RELEVANTES

- *Multiprotocol Label Switching* es un estándar desarrollado por la IETF con el objetivo de brindar a los proveedores de servicios mayor flexibilidad en la entrega de nuevos servicios de enrutamiento, mejorar el desempeño de la red y proporcionar escalabilidad a su *backbone*.

- MPLS a diferencia del enrutamiento tradicional IP, envía los paquetes basados en etiquetas y no en la dirección de destino. Combina los beneficios de IP *switching* de la capa 2 con el IP *routing* de la capa 3.

- El mecanismo de envío a través del *backbone* MPLS es a través del mecanismo e envío llamado *label swapping.*

- La arquitectura MPLS está conformada por dos componentes principales el *control plane* y el *data plane*. El primero es responsable de la creación y almacenamiento de la tabla de envío y el segundo es responsable del envío de paquetes de entrada a salida a través de los routers del *backbone*.

- La red MPLS está constituida por una serie de nodos o puntos llamados *Label Switching Routing* (LSR) que son capaces de conmutar y enviar paquetes etiquetados.

- Se distinguen tres tipos de LSR: LSR de ingreso que realiza una función "*push*" agregar una etiqueta o pila de etiquetas al recibir el paquete IP. LSR de salida el mismo que hace una función "*pop*" remover la etiqueta del paquete IP y enviarlo fuera del dominio MPLS.Finalmente el LSR intermedio ubicado entre el de ingreso y salida realiza una función "*swap*" conmutar la etiqueta que recibe por otra.

- Los paquetes que ingresan al dominio MPLS a través del LSR de ingreso son designados a una Clase Equivalente de Envío (*Forwarding Equivalence Class*) o conjunto de paquetes IP que comparten iguales atributos.
- Todos los paquetes que pertenecen a una FEC tienes la misma etiqueta.

- En MPLS se pueden implementar caminos lógicos conocidos como LSP (*Label Switching Path*). Un LSP es el mismo para paquetes que pertenecen a la misma FEC.

- Así mismo, los LSP pueden ser anidados, *nested* LSP.

- La etiqueta MPLS es un conjunto de 32 bits y es conocida como "*shim header*" (ó en español cabecera acuñada) ya que es insertada entre las cabeceras de capa de enlace y capa de red.

- En MPLS es posible agregar más de una etiqueta a un paquete (*label stack*). La primera etiqueta en la cola se llama *top label* y la última *bottom label*.

- Un LSR de ingreso decide qué etiqueta asignar a una FEC particular la misma que puede ser local, remota, *dowstream* y *upstream*.

- Existen tres modos de cómo un LSR transmite etiquetas a otro: modo distribución de etiqueta, modo de retención de etiqueta y modo control de distribución de etiqueta.

- La conmutación de etiqueta en los LSR se realiza a través de un algoritmo que se basa en el concepto de *label swapping*.

- A través de *label swapping* un LSR es capaz de obtener información para enviar paquetes y qué recursos el paquete debe usar.

- La implementación de *label swapping* es económica, una tecnología de alto desempeño y permite un rendimiento de envío rápido.

- En MPLS el componente de envío consiste de un solo algoritmo, lo cual le permite tener la habilidad de soportar múltiples protocolos de capa de red y operar virtualmente sobre protocolos de capa de enlace. De ahí su nombre de "*multiprotocol*".

- La distribución de información de asignación de etiqueta/FEC (creada o destruida) de un LSR a otro a través del *backbone* MPLS se lo puede hacer mediante *piggybac*k de etiquetas de enrutamiento existente o a través de un protocolo de distribución de etiqueta.

- *Piggyback* consiste en extender protocolos IP de enrutamiento existentes de manera que puedan transportar etiquetas. Ninguno de los IGP ha sido modificado para hacerlo, sin embargo BGP al ser un protocolo de enrutamiento externo puede transportar prefijos y etiquetas.

- EL protocolo de distribución de etiqueta que se utiliza es LDP el mismo que fue desarrollado por Cisco y formalizado por la IETF. Reemplaza a TDP.

- LDP define una serie de procedimientos y mensajes a través de los cuales un LSR informa a otro cuando ha realizado una asociación etiqueta/FEC y sirve para la creación de un LSP.

- LDP es útil en los casos que un LSR no soporta *piggyback*, es biderccional y opera entre LSRs que son y no adyacentes.

- Cuando un LSR está corriendo LDP se intercambian cuatro tipos de mensajes: de descubrimiento, sesión, anuncio y notificación.

- Una etiqueta puede ser asociada a una FEC por medio de dos espacios de etiquetas: por interfaz y por plataforma.

- Los pares LDP son dos LSR que usan LDP para intercambiar información de asociación etiqueta/FEC.

- Mediante el uso de un identificador LDP campo conformado por seis octetos se puede identificar un espacio de etiquetas.

- Los mensajes que son intercambiados entre los LSR pares son enviados como PDUs. Los mismos que están conformados por una cabecera LDP y uno o más mensajes LDP.

- Los mensajes LDP utilizan un esquema de codificación TLV.

- RSVP es un protocolo de señalización que reservas recursos para una sesión antes de empezar la transmisión de la información.

- RSVP maneja dos mensajes fundamentales: mensajes *path* y mensajes *res*v.

- Se desarrollaron extensiones para los protocolos LDP y RSVP, CR-LDP y RSVP-TE respectivamente.

- Los protocolos CR-LDP y RSVP-TE fueron desarrollados con el objetivo de soportar rutas explícitas ó túneles.

- El protocolo RSVP es un protocolo de distribución de etiqueta utilizado en ingeniería de tráfico.

- MPLS permite ingeniería de tráfico en el cual es posible balancear carga a través de caminos desiguales.

- MPLS es usado en muchas aplicaciones: *unicast IP routing, multicast IP routing,* MPLS TE, QoS, MPLS VPNs, y AToM.

- Las Aplicaciones MPLS pueden usar diferentes protocolos de ruteo o intercambio de etiquetas siempre que usen el mismo proceso de envío de etiquetas.

- Redes tradicionales basadas en routers conectan los sitios del cliente a través de routers vía enlaces dedicados punto a punto.

CAPÍTULO II

REDES PRIVADAS VIRTUALES

2.1 INTRODUCCION

En la industria de las telecomunicaciones el término VPN (*Virtual Private Network*) o Red Privada Virtual es una de las palabras más conocida y usada por cada uno de los proveedores de servicios, los mismos que con el objetivo de brindar y satisfacer los requerimientos de sus clientes, han encontrado en la implementación de redes privadas virtuales una solución a través de la cual se logra extender las redes de sus clientes a nivel nacional, alrededor del mundo y a menores costos.

Una red privada virtual VPN reemplaza las redes tradicionales basadas en routers que conectan los sitios de los clientes a través de enlaces punto a punto dedicados emulando enlaces punto a punto a través de una infraestructura compartida. Usa una red pública, usualmente el Internet para conectar sitios remotos.

Con el crecimiento del Internet las redes privadas virtuales se han convertido en el área de mayor crecimiento y su popularidad está acompañada del surgimiento de muchas técnicas a través de las cuales se puede proveer esta función. Asimismo cada una de éstas técnicas usa diferentes protocolos y por ende el uso de una en especial tiene sus propias ventajas y desventajas.

2.2 DEFINICIÓN DE UNA RED PRIVADA VIRTUAL

Una red privada virtual se puede definir [6] como una red a través de la cual se interconectan sitios/puntos que se encuentran geográficamente dispersados mediante enlaces punto a punto a través de una infraestructura compartida. Para ello las redes privadas virtuales hacen uso de técnicas avanzadas de *encriptación* y *tunneling* permitiendo a las organizaciones seguridad extremo a extremo a través de una red pública como por ejemplo el Internet.

Cabe aclarar que la red es privada en el sentido de que el enrutamiento y direccionamiento utilizado en la red es totalmente independiente del enrutamiento y direccionamiento de otras redes. Y es virtual, ya que la infraestructura para operar la red de determinada compañía puede ser compartida con otras compañías que quieren contratar su propia VPN [3].
La empresa que presta las facilidades para establecer la red se denomina proveedor de servicios VPN y la empresa que contrata el servicio se conoce como cliente VPN.

2.2 TOPOLOGÍA BÁSICA DE UNA RED PRIVADA VIRTUAL

Se pueden diferenciar los siguientes componentes en la topología básica de una red privada virtual [6]:

- Una red existente con servidores y estaciones de trabajo.
- Conexiones al Internet.
- Puerta de enlaces VPNs, como por ejemplo *firewalls*, PIX, o concentradores VPNs.
- El *software* que crea y mantiene los túneles.

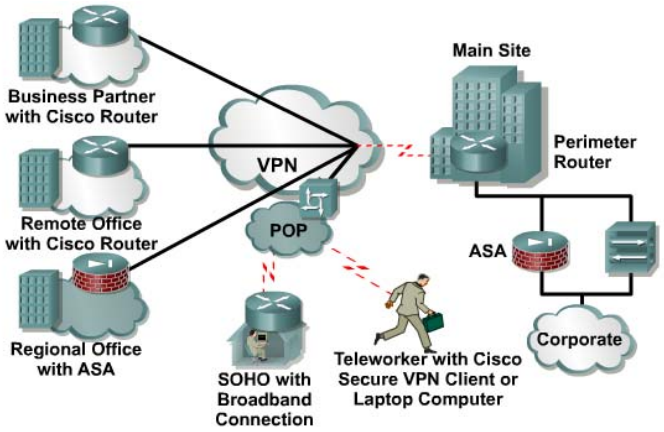


Figura. 2. 1 Elementos que conforman una VPN

Cabe recalcar que la palabra clave al momento de referirse a una *VPN* es la seguridad. La seguridad de los datos en una red privada virtual puede hacerse de tres maneras:

- Encapsultamiento de los datos.
- Encriptación,
- Encapsulamiento y encriptación.

2.3 TIPOS DE REDES PRIVADAS VIRTUALES

Existen tres tipos comunes de VPN*s* [5,11]:

- VPN de Acceso Remoto (*Remote Access* [RAS] VPN)

Una VPN de acceso remoto se conoce también con el nombre de *Virtual Private Dial-up Network* (VPDN), y consiste en una conexión usuario a LAN a través de la cual usuarios de determinada compañía necesitan conectar la red privada desde varios puntos remotos (VPN) y cuyo acceso es vía marcación (*dialing mode*). Es decir, es una red privada virtual donde el modo de acceso del usuario es a través de la marcación. El uso de una VPDN o VPN de acceso remoto permite a las empresas contar con conexiones seguras y cifradas entre su red privada y usuarios remotos a través de un tercero, es decir un proveedor de servicios.

Una empresa que crea y usa una VPN de acceso remoto, a través de un ISP (*Internet Service Provider*) proporciona una cuenta *dial-up* de Internet a cada uno de sus usuarios los mismos que al marcar un número 1800 determinado logra conectarse al Internet y mediante el uso de un software VPN de usuario/cliente acceder a la red corporativa.

- Site-to-Site VPN

Este tipo de VPN consiste en la conexión de múltiples puntos geográficamente dispersados a través de una red pública como por ejemplo el Internet. Cada punto requiere únicamente de una conexión local hacia la misma red pública. Las *Site-to-Site* VPNs pueden ser categorizadas en dos grupos:

1) Site-to-Site Intranet VPN

   Es aquella VPN que se construye con puntos/oficinas que pertenecen a la misma compañía. Es decir, una empresa que tiene uno o más puntos remotos los cuales se comunican a través de únicamente una red privada virtual.

2) Site-to Site Extranet VPN

   VPN que se construye para conectar una empresa con sus socios o clientes. Es decir, una compañía que posee vínculos con otra, ya sea un cliente, socio, proveedor; éstas pueden implementar una Extranet VPN mediante la cual se una la red LAN de cada empresa permitiendo así trabajar en un mismo entorno.

- VPN basadas en Firewall [5]

Una VPN basada en firewall está intrínsicamente incluida en una implementación Site-to-Site. Es una solución orientada a resolver los problemas de seguridad y es implementada cuando una compañía requiere mayores y avanzadas medidas de seguridad para sus VPNs.

El buen y correcto diseño de una VPN puede ser de gran beneficio para una empresa desde los siguientes puntos de vista:

- ✓ Ampliar la conectividad geográficamente.
- ✓ Reducir los costos operacionales.
- ✓ Reducir los tiempos de tránsito y costos de viaje para usuarios remotos.
- ✓ Mejorar la productividad.
- ✓ Se logra simplificar la topología de red y con ello se facilita la administración de la misma. Entre otras.

2.4 CARACTERISTICAS DE SEGURIDAD EN UNA VPN

Como se ha mencionado anteriormente el enfoque principal en la implementación de una red privada virtual es la seguridad para lo cual se hace uso de técnicas avanzadas de encriptación y *tunneling*. El fundamento de VPNs seguras está basado en la autenticación, la encapsulación y la encriptación [5,11].

2.4.1 Confidencialidad de los datos

Como característica de diseño de una VPN la confidencialidad de los datos tiene como objetivo proteger la interpretación del contenido de los mensajes desde fuentes no autenticadas o no autorizadas. Una VPN logra ofrecer confidencialidad a través de mecanismos encapsulación y encriptación.
Este es uno de los servicios más importantes que se pueden brindar a través de una implementación VPN.

- **Encapsulación**

La encapsulación es uno de los principales componentes de la confidencialidad en una implementación VPN. Los túneles son una excelente aplicación del encapsulamiento.

- **Tunneling [6]**

El enrutamiento punto a punto o *tunneling*, es el proceso de colocar un paquete dentro de otro paquete y al nuevo paquete compuesto enviarlo a través de la red. En la figura 2.2 se puede diferenciar los siguientes elementos, los datos que se transfieren se denominan carga, el paquete que se envía se encapsula utilizando la cabecera de un protocolo de enrutamiento punto a punto el cual es enviado desde y hacia los extremos del túnel, definidos como extremos finales del túnel o del canal. A través de la cabecera del protocolo de enrutamiento los routers intermedios deciden por donde encaminar el paquete hacia el punto final del túnel. En *tunneling* se usan tres protocolos diferentes:

- ✓ ***Passenger protocol,*** los datos originales (IPX, AppleTalk, IPv4, IPv6).

- ✓ ***Protocolos de encapsulamiento,*** protocolos que envuelven la información original (GRE, IPsec, L2F, PPTP, L2TP). Cabe mencionar que todos estos protocolos ofrecen el mismo nivel de seguridad.

- ✓ ***Carrier protocol,*** el protocolo por el cual viaja la información (Frame Relay, ATM, MPLS).

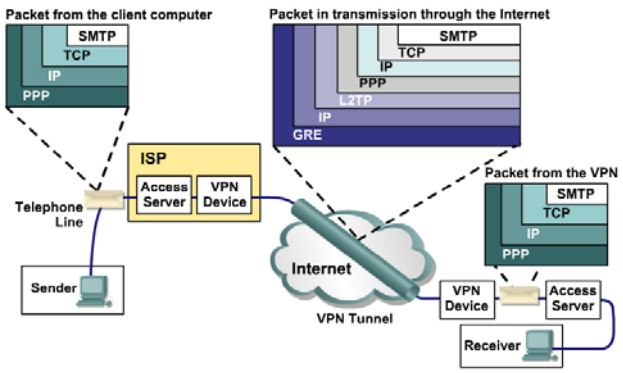


Figura. 2. 2 Encapsulamiento de información en la red VPN

El paquete original es encapsulado dentro de un protocolo de encapsulamiento el mismo que es puesto dentro de la cabecera de un protocolo de transporte (usualmente IP) para la transmisión del paquete a través de la red pública (Ver figura 2.2).

- **Criptografía**

La criptografía es otra de las principales características de confidencialidad en una implementación VPN. El cifrado es el proceso de tomar todos los datos que un computador está enviando a otro computador y codificarlos de tal manera que sólo el otro computador sea capaz de decodificar y pon ende entender. Existen dos tipos de algoritmos de criptografía:

✓ **Criptografía Simétrica o Llaves privadas.**

La criptografía simétrica o de llave privada (también conocida como criptografía convencional) está basada en una llave secreta que comparten ambas partes que se comunican. La parte emisora utiliza la llave secreta como parte de la operación matemática para cifrar (o codificar) texto plano a texto cifrado. La parte receptora utiliza la misma llave secreta para desencriptar (o descifrar) el texto cifrado a texto plano.

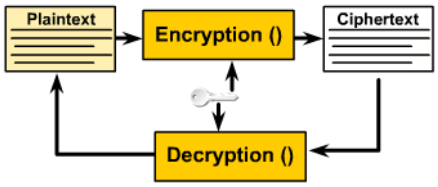


Figura. 2. 3 Bosquejo de criptografía de llave pública

Algunos ejemplos de los esquemas de criptografía simétrica son los algorimos DES, 3DES y AES.

➢ ***Data Encryption Data (DES)***[7], fue desarrollado por IBM y publicado como estándar en el año 1997. Este algoritmo utiliza una llave para la transformación, de modo que el

[7] DES es un algoritmo que fue seleccionado como un estándar de procesamiento de información federal (*Federal Information Processing Standard [FIBS]*) de los Estados Unidos en el año 1976 por tal razón, DES se aplica ampliamente a nivel internacional.

descifrado sólo pueda ser realizado por aquellos que conocen la clave concreta para cifrar. La llave o clave mide 64 bits de los cuales son utilizados 56 en el algoritmo, el resto se utiliza únicamente para comprobar la paridad y después son descartados.

En la actualidad, el algoritmo DES es considerado inseguro para muchas aplicaciones debido a que el tamaño de la clave (56 bits longitud efectiva) es demasiado pequeña. Se ha detectado que claves DES se han roto en menos de 24 horas y resultados de estudios demuestran que existen debilidades teóricas en su cifrado.

- ***Triple Data Encryption Data (3DES),*** triple DES se puede definir como un algoritmo de cifrado de bloque que se formó a partir de DES. Fue desarrollado por Walter Tuchman[8] en 1978. Se puede resumir su funcionamiento observando la figura 2.4.

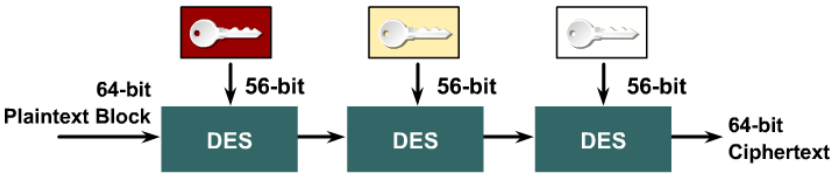


Figura. 2. 4 Bosquejo de 3 DES

- ***Advanced Encryption Standard (AES),*** algoritmo formalmente conocido como criptografía de Rijndael, sucesor de DES y 3 DES y aprobado por el Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology [*NIST*]*) en diciembre del año 2001.

  Este algoritmo está caracterizado por soportar llaves de 128, 192, y 256 bits siendo la llave de 128 segura es un algoritmo más seguro y rápido que 3 DES. El tamaño del bloque es de 18 bits.

  AES es un algoritmo que fue adoptado como estándar por el gobierno de los Estados Unidos y se espera que al igual que DES sea utilizado en todo el mundo.

[8] Líder del equipo de desarrollo de DES de IBM.

✓ **Criptografía Asimétrica o Llaves públicas.**

La criptografía asimétrica o de llave pública utiliza dos llaves diferentes para cada usuario: una es una llave privada conocida sólo por este usuario; la otra es una llave pública correspondiente, que es accesible para todos. Se utiliza una llave para encriptación y la otra para la *desencriptación*, dependiendo de la naturaleza del servicio de comunicación que se esté implementando. Estos algoritmos proporcionan no rechazo y autenticación.

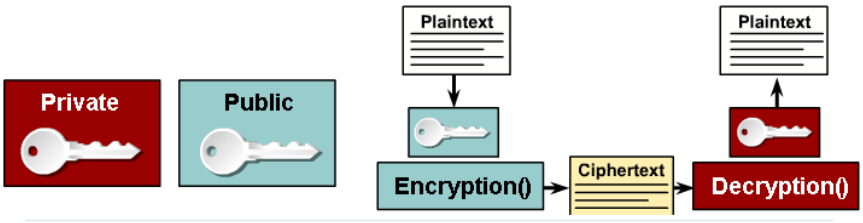


Figura. 2. 5 Bosquejo de criptografía de llave privada

En la actualidad existen dos sistemas de llave o clave pública: **RSA** (nombre de los diseñadores ***Rivest, Shamir* y *Adelman***) y ***Diffie-Hellman* (DH).**

- ***Algoritmo de llave pública RSA (Rivest, Shamir y Adelman),*** fue uno de los primeros grandes avances en la criptografía pública y el primero en desarrollarse. RSA utiliza los principios de intercambio de llave de Diffie-Hellman (IKE):

  Una llave pública para encriptar los datos y verificar firmas digitales y,
  Una llave privada para desencriptar los datos y para firmar con una firma digital.

- ***Algoritmo de llave pública Diffie-Hellman(DH),*** el algoritmo DH establece que si el usuario A y el usuario B intercambian claves públicas y mediante un cálculo que se realiza con llaves públicas y privadas del otro par el resultado final es un llave idéntica compartida. A través de esta llave se utiliza para encriptar y desencriptar los datos. En la figura 2.6 se puede observar el mecanismo del algoritmo DH.

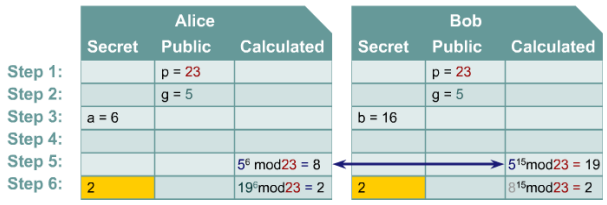


Figura. 2. 6 Algoritmo de Diffie-Hellman

2.4.2 Integridad de los datos

Existe la posibilidad que los datos sean modificados en el transcurso de su viaje a través del Internet. La integridad de los datos en VPNs garantiza que no se produzcan alteraciones y modificaciones mientras los datos viajan de origen a destino y para lograrlo VPNs suelen utilizar los siguientes métodos: one-way hash functions, message autentication codes (MAC) o firmas digitales.

- **Funciones Hash**

Una función hash consiste en tomar un mensaje de longitud variable y generar una cadena de longitud fija, lo cual se conoce como valor hash. Las funciones hash son usadas para asegurar la integridad de los datos y ejemplos de algoritmos hash son MD5 (*Message Digest 5*), *Secure Hash Algorith* (SHA-1) y RIPE-MD-m 160.

- **Códigos de Autenticación de Mensajes**

Los códigos de autenticación de mensajes MACs agregan una llave a las funciones hash. El emisor crea un archivo, calcula la MAC basado en la llave compartida con el destinatario y luego añade la MAC al archivo. Cuando el destinatario recibe el archivo calcula una nueva MAC y la compara con la MAC añadida.

- **Firmas Digitales**

Una firma digital es una criptografía de llave pública pero en sentido inverso, es decir que funciona de manera inversa al proceso de cifrado normar. La firma digital utiliza la llave privada en algunos bloques de datos (sólo un individuo tiene acceso a la clave privada) y el receptor descifra esos datos con la clave pública que está disponible y que es conocida. En otras palabras un emisor firma digitalmente un documento con la llave privada del emisor y el receptor puede verificar la firma usando la misma llave pública del emisor.

2.4.3 Autenticación

Mediante la autenticación se asegura que el mensaje llegue desde una fuente válida hacia una fuente válida. Mediante la autenticación se protege a la VPN de ataques que dependen de la suplantación de la identidad del remitente y adicionalmente permite a cada usuario de la comunicación saber exactamente con quién está hablando. La autenticación incluye contraseñas, certificados digitales, tarjetas inteligentes.

- Nombre de usuario y contraseña: utiliza nombres de usuarios y contraseñas predefinidos para diferentes usuarios o sistemas.

- One Time Password (OTP) (Pin/Tan): es un método más fuerte que el método de nombre de usuario y contraseña en el cual se generan nuevas contraseñas por cada autenticación.

- Biométrica: por lo general la biometría se refiere a las tecnologías que se utilizan para medir y analizar características del cuerpo humano tales como huellas dactilares, patrones de voz faciales, etc., enfocados principalmente en fines de autenticación.

- Llaves pre-compartidas: este método de autenticación utiliza un valor de llave secreta que es manualmente introducido por cada uno de los compañeros y luego se utiliza para autentificar a los pares.

- Certificados digitales: usa el intercambio de certificados digitales para autentificar los pares.

Un certificado es una estructura de datos que está firmada digitalmente por una autoridad certificadora (CA) en la que los usuarios del certificado pueden confiar. El certificado contiene varios valores, como el nombre y el uso del certificado, la información que identifica al propietario de la llave pública, la llave pública misma, una fecha de expiración y el nombre de la autoridad certificadora.

Los certificados de llaves públicas proporcionan un método conveniente y confiable para verificar la identidad de un remitente.

2.5 TERMINOLOGÍA USADA EN REDES PRIVADAS VIRTUALES

Una solución VPN tiene un cierto número de componentes los cuales se pueden diferenciar en la figura 2.7 y cuyo papel se describe a continuación [1,5].

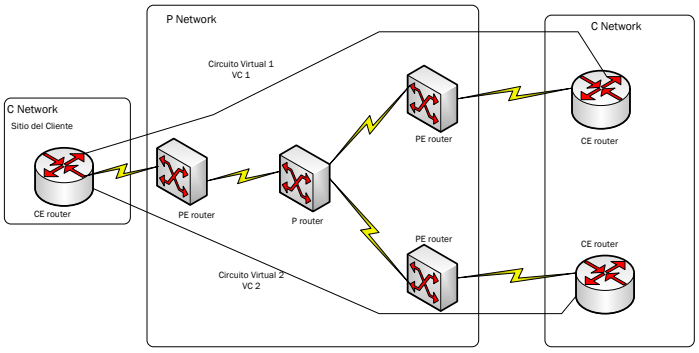


Figura. 2. 7 Dispositivos de una MPLS VPN

- ***Proveedor de servicios (Service Provider),*** es la organización que con su propia infraestructura la cual incluye equipo y medio de transmisión proporciona a sus clientes líneas dedicadas emuladas. El proveedor de servicios ofrece a sus clientes un Servicio de Red Privada Virtual (*Virtual Private Network Service*).

- ***Red de proveedor (Provider Network [P-Network])***, es la infraestructura, equipo y medio de transmisión del proveedor de servicios usada para ofrecer servicios VPNs.

- ***Red de cliente (Customer Network [C-Network])***¸ corresponde a la parte de la red que está bajo el control del cliente.

- ***Sitio del cliente (Customer Site),*** es una parte contigua a la C-Network que puede comprender muchas ubicaciones físicas.
- ***Equipo de proveedor (Provider device [P-device]),*** es el equipo que está dentro de la P-Network que no tiene conectividad con el cliente y tampoco ningún conocimiento de la VPN. Este equipo usualmente es un router y es comúnmente conocido como un P-router.

- ***Equipo de borde del proveedor (Provider Edge device [PE device]),*** el *PE* es un dispositivo que está en la P-Network al cual se conectan los CE. Usualmente es un router y es a menudo referido a un PE router.

- ***Equipo de borde del cliente (Customer Edge device [CE device]),*** equipo en la C-Network es el dispositivo a través del cual el cliente/usuario final se conecta a la red del proveedor de servicios también es conocido como equipo local del cliente (*Customer Premises Equipment [*CPE*]*). Usualmente es un router y es a menudo referido a un CE router.

- ***Circuito virtual (Virtual Circuit [VC]),*** es un enlace lógico punto a punto que se establece a través de una infraestructura compartida a nivel de capa 2. Un circuito virtual puede estar constantemente activo (*Permanent Virtual Circuit [*PVC*]*) ó establecido por demanda (*Switched Virtual Circuit [*SVC*]*).

2.6 MODELOS USADOS EN IMPLEMENTACIONES DE VPNs

Existen varios caminos a través de los cuales se puede clasificar las redes privadas virtuales a pesar de ello y por la utilización se puede categorizar a las VPNs según los siguientes criterios:

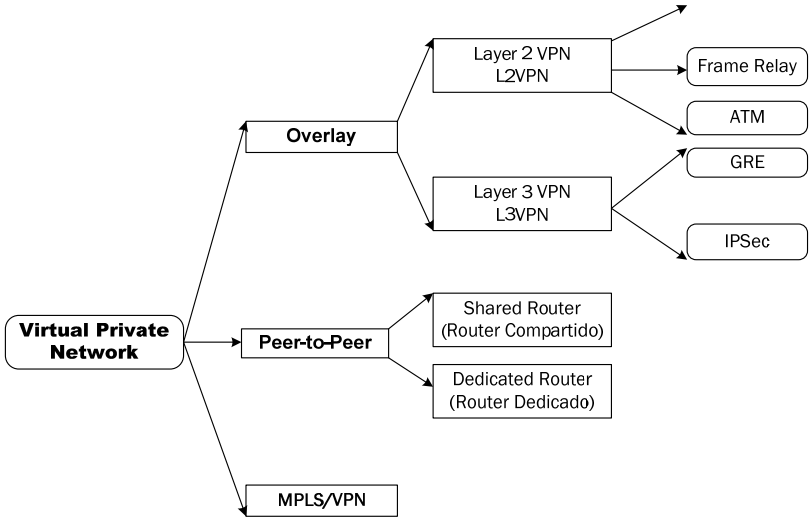


Figura. 2. 8 Clasificación de VPN

1) Redes privadas virtuales basadas en IP ó IP-VPN las cuales se caracterizan por usar o compartir los recursos de una red pública IP emulando características de una red privada IP.

   Dentro de la clasificación de IP-VPN se pueden distinguir los siguientes modelos:

   - Basadas en dispositivos CE: en este tipo de VPN los PE desconocen la información de enrutamiento de las redes del cliente y ofrecen únicamente un servicio IP.

   - Basadas en dispositivos PE: en este tipo de VPN los PE de la red del proveedor de servicios proporciona la VPN, de esta manera se oculta la VPN de los CE.

2) La segunda clasificación se basa en la forma en que la información de enrutamiento se intercambia en la red privada. Esta clasificación está basada en el intercambio de información de enrutamiento de capa 3 entre el dispositivo CE del cliente y proveedor. Existen dos modelos de implementaciones VPN sustentadas en este criterio: el modelo *overlay* y el modelo *peer-to-peer*.

- Modelo Overlay: el proveedor de servicios efectúa enlaces virtuales punto a punto entre los sitios del cliente.

- Modelo Peer-to-Peer: modelo en el cual el proveedor de servicios participa en el enrutamiento del cliente.

2.6.1 Modelo Overlay

A través del modelo *Overlay* el proveedor de servicios provee la *VPN* al cliente a través de un conjunto de líneas arrendadas emuladas las cuales se conocen normalmente como circuitos virtuales (*virtual circuits* [VCs]) las cuales pueden estar constantemente disponibles PVC o ser establecidos por demanda SVC.

Adicionalmente el cliente establece la comunicación router a router entre los CE routers a través de los VC proporcionados por el proveedor de servicios. La información de enrutamiento siempre se intercambia entre los dispositivos del cliente y por ende el proveedor de servicios desconoce la estructura interna de la red del cliente.

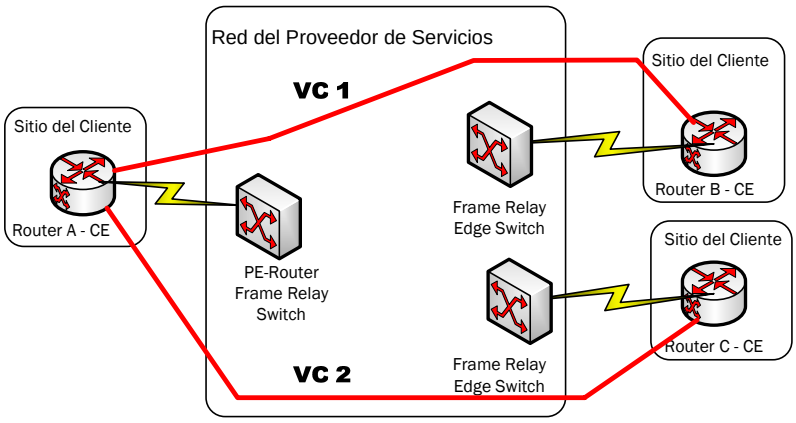


Figura. 2. 9 Modelo Overlay VPN

Este tipo de VPNs puede ser implementada a nivel de capa 1 usando líneas arrendadas, a nivel de capa 2 usando por ejemplo X.25, Frame Relay circuitos virtuales ATM y finalmente a nivel de capa 3 usando túneles IP (GRE).

- **Modelo Overlay implementación a nivel de capa 1:**

Adopta la solución tradicional de *multiplexación* por división en el tiempo TDM, en esta topología el proveedor de servicios establece la conectividad en la capa física entre los sitios del cliente y el cliente es responsable por todas las capas superiores.

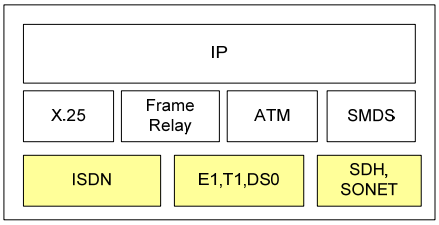


Figura. 2. 10 Overlay VPN a nivel de capa 1 [9]

- **Modelo Overlay implementación a nivel de capa 2:**

La implementación a nivel de capa 2 (L2VPN) adopta la solución tradicional de WAN switcheada: el proveedor de servicios establece circuitos virtuales de capa 2 entre los sitios del cliente y el cliente es responsable de las capas superiores.

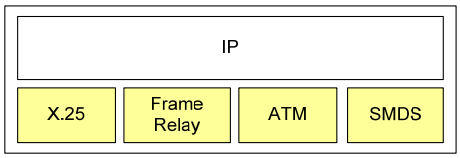


Figura. 2. 11 Overlay VPN a nivel de capa 2 [9]

- **Modelo Overlay implementación a nivel de capa3:**

Un modelo overlay de capa 3 (L3VPN) es a menudo una implementación con túneles “IP en IP” a través de protocolos tales como PPTP (*Point to Point Tunneling Protocol*), L2TP (*Layer 2 Tunneling Protocol*), GRE (*Generic Routing Encapsulation*) e IPsec (*IP Security*).

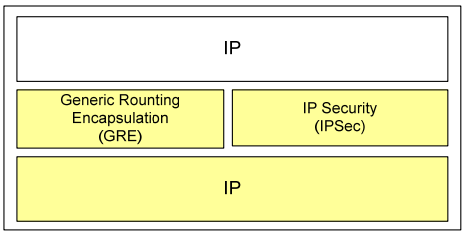


Figura. 2. 12 Overlay VPN a nivel de capa 3 **[9]**

Beneficios y Desventajas de la Implementación Overlay VPN

A través de una implementación *Overlay VPN* se puede tener los siguientes beneficios:

- ✓ Una *VPN Overlay* es bien conocida y fácil de implementar.
- ✓ El proveedor de servicios no participa en el enrutamiento del cliente.
- ✓ La red del cliente y del proveedor de servicio están aisladas.

Así mismo las desventajas son:

- ✓ Para un enrutamiento óptimo se requiere un *full mesh* de los circuitos virtuales.
- ✓ Los circuitos virtuales deben proporcionarse manualmente.

2.6.2 Modelo Peer-to-Peer

El modelo *Peer-to-Peer VPN* fue introducido con el objetivo de aliviar las desventajas existentes con el modelo *overlay*. En este modelo el router PE intercambia directamente información de enrutamiento con el CE router. Es decir que, tanto la red del proveedor como la del cliente usan el mismo protocolo de red y todas las rutas del cliente son transportadas dentro de la red del proveedor de servicios. En la figura 2.13 se puede observar de manera general el modelo *peer-to-peer VPN* y la función de los equipos.

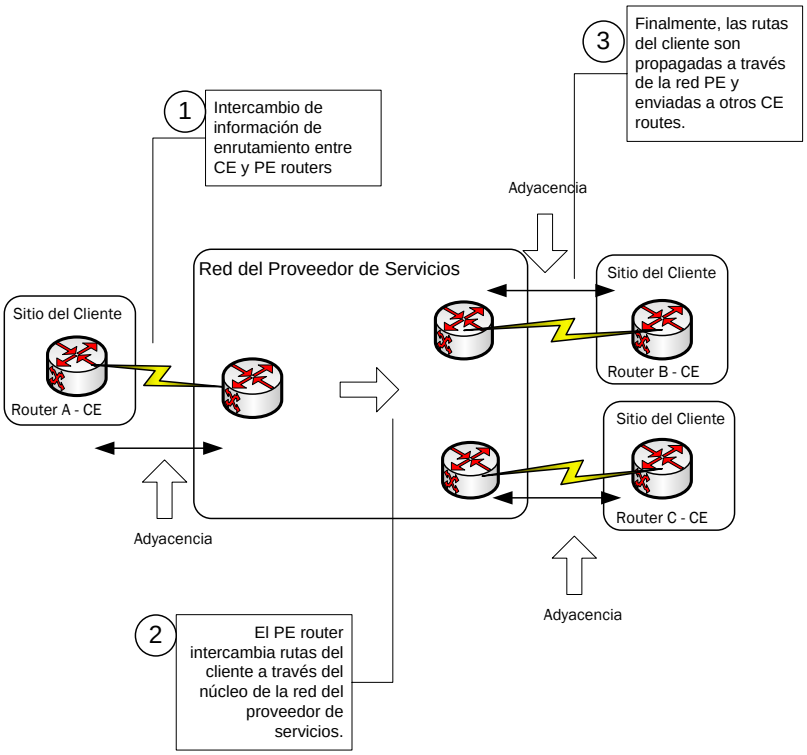


Figura. 2. 13 Modelo peer-to-peer VPN

Existen tres opciones de implementación a través del modelo *peer-to-peer*:

- **Modelo PE router compartido (Shared Router) [1]:**

En este modelo, varios clientes se pueden conectar al mismo PE router, pero listas de acceso son configuradas en cada interfaz PE-CE (es decir que, las rutas individuales de los clientes son separadas con filtros de paquetes en las interfaces PE-CE) de manera que se asegure el aislamiento entre los clientes VPN.

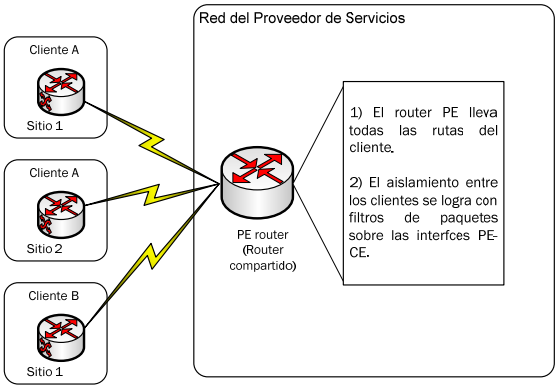


Figura. 2. 14 Modelo de router compartido "shared router"

Al implementar este tipo de VPN se presentan las siguientes desventajas:

- ✓ Todos los clientes comparten en mismo espacio de direccionamiento.
- ✓ Altos costos de mantenimiento son asociados con filtros de paquetes.
- ✓ El rendimiento es bajo.

- **Modelo PE router dedicado** (**Dedicated Router**):

En este modelo cada cliente VPN tiene un PE router dedicado que transporta únicamente sus propias rutas. A través de protocolos de enrutamiento cada PE router crea sus tablas, las cuales contienen sólo las rutas anunciadas por el cliente VPN conectados a ellos. De esta manera se logra aislar las VPN de los clientes.

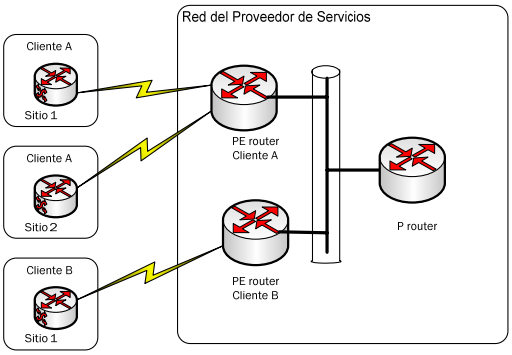


Figura. 2. 15 Modelo de router dedicado

Al implementar este tipo de *VPN* se presentan las siguientes desventajas:

- ✓ Todos los clientes comparten el mismo espacio de direccionamiento.
- ✓ Cada cliente requiere un router dedicado para cada punto de presencia (*POP*).

2.6.3 Modelo MPLS VPN

Una VPN basada en MPLS usa el modelo *peer-to-peer* y combina los beneficios de *overlay* y *peer-to-peer VPN*: *i*) seguridad y características de segregación, *ii*) simplificación del enrutamiento del cliente, respectivamente.

La arquitectura de una MPLS/VPN es bastante similar al modelo PE router dedicado pero con la diferencia que los routers dedicados por cliente son implementados como tablas de enrutamiento virtuales dentro del PE router. Es decir que el aislamiento entre los clientes VPN es por medio de routers virtuales levantados en el PE router a través de enrutamiento y envío virtual (*Virtual Routing and Forwarding [*VRF*])* los cuales pertenecen a diferentes clientes VPN.

Cabe resaltar algunas características puntuales de una MPLS/VPN lo cual surge de la combinación de beneficios de *overlay* y *peer-to-peer VPNs*.

- ✓ En una MPLS/VPN se permite el *overlapping* de direcciones en diferentes clientes/sitios VPN debido a que cada PE router virtual maneja su propia tabla de enrutamiento. Es decir los clientes pueden tener el mismo espacio de direcciones.

- ✓ La tabla de enrutamiento que almacena el PE router se reduce significativamente ya que sólo guarda la información de enrutamiento de la VPNs que están directamente conectadas.

- ✓ La cantidad de información de enrutamiento es proporcional al número de VPN conectadas al PE router, por tanto esta crece cuando el número de VPN directamente conectadas crece.

- ✓ Los PE routers participan en el enrutamiento del cliente pero asegurando el enrutamiento óptimo entre los sitios.

- ✓ Con MPLS/VPN el enrutamiento total dentro del *backbone* del proveedor de servicios ya no es necesario y tampoco el enrutamiento tradicional IP para enviar paquetes.

2.7 TOPOLOGÍAS COMUNES EN IMPLEMENTACIONES VPN

Las topologías que se pueden implementar de acuerdo a la necesidad del cliente y sus requerimientos se pueden agrupar en tres grandes grupos [1,9]:

- Por la topología de los circuitos virtuales: *hub and spoke*, parcial o *full mesh* y multinivel.
- Topologías según las necesidades del negocio: intranet, extranet y de acceso.
- Topologías que surgen de acuerdo al tipo de conectividad requerida entre los sitios: simple, *overlapping vpn*, de servicios centrales y de administración de red.

2.7.1 Categorías de Topología Overlay VPN

Las *VPN overlay* son clasificadas de acuerdo a la topología de los circuitos virtuales.

- **Hub and Spoke Overlay VPN:**

En la topología *hub and spoke* un determinado número de oficinas remotas (*spoke*) se conectan a través de circuitos virtuales a un sitio central (*hub*).

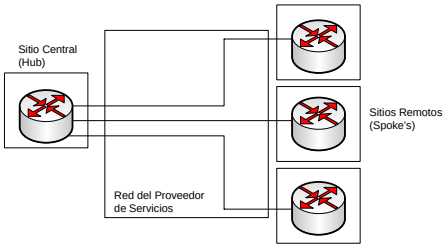


Figura. 2. 16 Hub and Spoke Overlay VPN

- **Partial y Full Mesh Overlay VPN:**

En la topología *partial* y *full mesh*, los sitios de la VPN son conectados por circuitos virtuales *VCs* que se crean de acuerdo a los requerimientos de tráfico lo cual depende de las necesidades de la empresa. La topología se denomina parcial (*partial*) cuando no todos los sitios están directamente conectados caso contrario la topología es *full*.

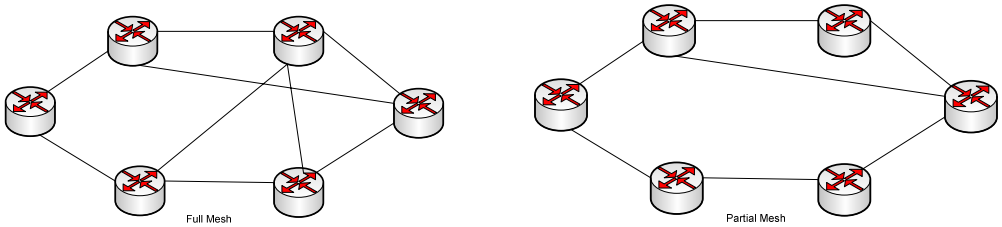


Figura. 2. 17 Full mesh y partial mesh VPN

- **Topología híbrida**

Las grandes redes VPN se pueden contruir a partir de una combinación de una topología *hub* and *spoke* con la topología *partial mesh*.

El enfoque del diseño de una topología híbrida es seguir el enfoque del diseño de una red modular:

- ✓ Dividir la red total en núcleo, distribución y redes de acceso.
- ✓ Diseñar individualmente el núcleo y partes de acceso de la red.
- ✓ Conectar el núcleo y la red de acceso a través de la capa de distribución de una forma que los aísla tanto como es posible.

2.7.2 Categoría VPN Business

Las VPN pueden ser clasificadas según las necesidades del negocio:

- Topología Intranet VPN:

Conecta sitios dentro de la organización y se enfoca principalmente en la topología física y lógica de la red VPN según lo dictado por la tecnología del circuito virtual por lo cual el modelo *overlay* es implementado.

- Topología Extranet VPN:

VPN que se crea al conectar una empresa con sus clientes ó proveedores. Cuando se trata de una topología de extranet un tema de mucha importancia son los requerimientos de seguridad que se debe proporcionar y asegurar entre los sitios. Una topología extranet tradicional permite a un número de empresas realizar intercambio de datos entre ellas (cualquiera con cualquiera), es decir que no se impone restricción en los datos intercambiados siendo cada sitio es responsable de su propia seguridad, filtrado de tráfico y *firewall*.

Una extranet VPN puede ser implementada a través del modelo *overlay* o *peer-to-peer*.

✓ Extranet VPN, implementación *Peer-to-Peer*

Es esta topología cada organización específica únicamente sólo la cantidad de tráfico que va a recibir y a enviar desde cada uno de sus sitios.

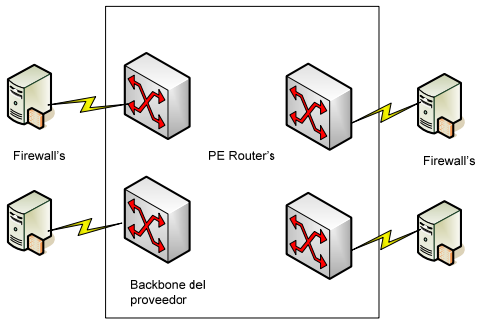


Figura. 2. 18 Peer-to-peer extranet VPN

✓ Extranet VPN, implementación Overlay VPN

El tráfico entre sitios se intercambia a través de VCs punto a punto.

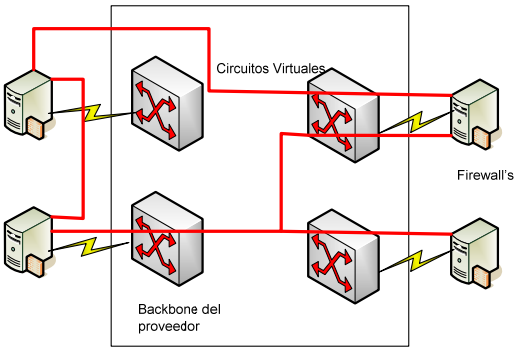


Figura. 2. 19 Overlay extranet VPN

2.7.3 Topología VPN de Acceso o VPDN

VPN que permite el acceso a usuarios remotos, trabajadores desde el domicilio, oficinas remotas, etc., a través de un medio dial-up a bajo costo. Una VPDN utiliza términos especiales que son únicos en el mundo VPDN.

✓ Nertwork Access Server (NAS)

El servidor de acceso remoto (*Remote Access Server [*RAS*]*) es administrado por el proveedor de servicios acepta la llamada del cliente, realiza una autenticación inicial y remite la llamada a la *home gateway* del cliente.

✓ Home Gateway

Es un router de administración del cliente el cual recibe la llamada enviada por el NAS, realiza una autenticación y autorización adicional y termina la sesión PPP[9] desde el usuario dial-up.

Una VPDN es implementada usualmente por un túnel tramas PPP intercambiados entre el usuario de acceso telefónico y su home gateway en paquetes IP intercambiados entre el servidor de acceso a la red.

[9] Ver sección “Protocolos usados en redes privadas virtuales”

2.7.3 Categoría de Conectividad VPN

Las VPN también pueden ser clasificadas de acuerdo a la conectividad requerida entre los sitios.

- VPN Simple:

  Cada sitio puede comunicarse con otro sitio.

- Overlapping VPNs:

  Algunos sitios participan en más de una VPN simple.

- VPN de Servicios Centrales:

  En este tipo de topología todos los sitios VPN pueden comunicarse con el o los servidores centralizados pero no entre ellos. Es este tipo de VPN la seguridad es responsabilidad de la organización central pero también los administradores de los sitios VPN pueden implementar sus propias medidas de seguridad.

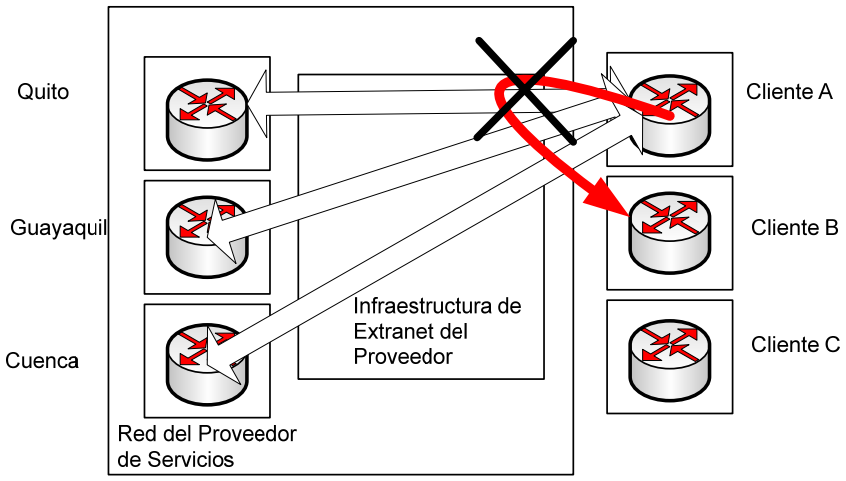


Figura. 2. 20 VPN de servicios centrales

2.8 REQUERIMIENTOS QUE DEBE CUMPLIR UNA VPN

Debido al tipo de conexión que ofrece una VPN se debe garantizar a través de la misma la privacidad e integridad de los datos que viajan a través de la red pública, o de una red corporativa. Siendo así se considera que una solución VPN debe proveer a cada uno de los clientes lo siguiente:

- Autenticación de usuario: verificando la identidad del usuario y restringiendo acceso a la VPN a usuarios no autorizados.

- Administración de dirección: deberá asignar una dirección al cliente en la red privada y deberá asegurarse que mismas se mantengan sin cambios.

- Encriptación de datos: a través de la encriptación asegurar que los datos no serán leídos por usuarios no autorizados.

- Administración de llaves: generando y renovando las llaves de encriptación tanto para el cliente como para el servidor.

- Soporte de protocolo múltiple: la red VPN debe poder manejar protocoles comunes utilizados en redes públicas.

2.9 PROTOCOLOS USADOS EN REDES PRIVADAS VIRTUALES

Para establecer un túnel tanto del lado del cliente como del servidor se debe levantar el mismo protocolo de túnel. Los protocolos de túnel se pueden clasificar de acuerdo al modelo OSI en protocolo del túnel de Nivel 2 o de Nivel 3, en el primer caso corresponde a la capa de enlace y utiliza **tramas** como su unidad de intercambio y en el segundo caso corresponden a la capa de red y utiliza paquetes.

De acuerdo a lo mencionado anteriormente, PPTP (*Point to Point Tunneling Protocol*), L2TP (*Layer 2Tunneling Protocol*) y L2F (*Layer 2 Forwarding*) pertenecen al grupo de protocolos de túnel de nivel 2 los cuales que encapsulan la carga útil (datos transferidos por el túnel) en una trama del protocolo punto a punto PPP (*Point to Point Protocol*) sección 2.8.1. Y, IP sobre IP e IPSec (*Internet Protocol Security*) pertenecen al grupo de protocolos de túnel de nivel 3[16].

2.9.1 Protocolo punto a Punto (PPP)

Los protocolos de túnel de Nivel 2 dependen principalmente de las funciones que se especifican en el protocolo punto a punto o PPP publicado por la IETF y estandarizado en la RFC 1661, siendo así cabe resaltar los aspectos más relevantes del mismo de manera que se logre entender los protocolos de túnel en cuestión.

PPP está diseñado para enlaces simples que envían paquetes entre dos pares; estos enlaces proveen operación simultánea bidireccional full duplex y se asume entregar los paquetes en orden. Generalmente se usa para enviar datos a través de conexiones de marcación o punto a punto dedicadas entre un cliente de marcación y un NAS.

El protocolo PPP tiene tres componentes principales:

- Encapsulamiento, a través de la cual el protocolo PPP permite la multiplexación de diferentes protocolos de la capa de red operar sobre el mismo enlace.
- Un Protocolo de Control de Enlace (*Link Control Protocol* ***[*LCP*]***) a través del cual se establece, configura y prueba la conexión PPO.
- Una familia de protocolos de control de red (*Network Control Protocol* ***[*NCP*]***), los cuales alivian los problemas que surgen en enlaces punto a punto con la familia actual de protocolos.

En la negociación en una sesión de marcación PPP se pueden distinguir cuatro fases[10]:

[10] Cada una de las fases debe completarse antes de que la conexión PPP esté lista para transferir datos.

1) Establecimiento del enlace, PPP utiliza el protocolo LCP para establecer, mantener y terminar la sesión física. Durante esta fase se seleccionan los protocolos de autenticación pero no se implementan y se toma la decisión de que si son iguales negociarán el uso de encriptación pero sin elegir realmente los algoritmos respectivos.

2) Autenticación del usuario, cada extremo del enlace se autentifica con el otro extremo empleando métodos de autenticación que se seleccionaron en la fase 1.

   La mayoría de implementaciones PPP proporcionan métodos de autenticación limitados por ejemplo:

   - Protocolo de autenticación de contraseñas (PAP): en este protocolo el NAS solicita el nombre de usuario y contraseña y el PAP le contesta el texto claro es decir sin encriptación.

   - Protocolo de autenticación de saludo *Challenge* (CHAP): es un algoritmo de autenticación encriptado que evita la transmisión de contraseñas reales en la conexión.

   - Negociación de la configuración del protocolo de red: una vez que se han terminado las fases previas, PPP invoca a los diferentes protocolos NCPs que fueron seleccionados en la fase 1 para configurar los protocolos que utiliza el cliente remoto.

- Terminación del enlace: el protocolo LCP puede terminar el enlace en cualquier momento lo cual sucede normalmente por petición de un usuario o eventualmente puede ocurrir por un evento físico.

Una vez terminadas las cuatro fases de negociación, PPP comienza a transferir los datos hacia y desde los dos pares, cada paquete de dato transmitido se envuelve en el encapsulado del PPP el mismo que se quita al llegar al receptor.

2.9.2 Protocolo de Túnel Punto a Punto (PPTP)

En junio de 1996 un grupo de trabajo conformada por un grupo de compañías miembros entre las que se incluye *Microsoft Corporation*, *Ascend Communications*, *3Com/Primary Access*, ECI *Telematics* y US *Robotics* (ahora 3Com) presentaron un proyecto ante la IETF el mismo que está documentado en la RFC preliminar. El protocolo de túnel de punto a punto es un protocolo de Nivel 2 que encapsula tramas del PPP en datagramas IP para la transmisión sobre una red IP como por ejemplo el Internet, de esta manera permite la realización de transferencias seguras desde clientes remotos a servidores ubicados en redes privadas.

En la figura 2.21 se puede observar un escenario típico donde opera el protocolo PPTP: el cliente de marcación establecerá una conexión dial-up con el NAS del proveedor; establecida la conexión, el cliente de marcación establecerá una segunda conexión ahora con el servidor PPTP ubicado en la red privada. El servidor PPTP es el servidor intermediario de la conexión establecida cuya función será recibir los datos del cliente externo y transmitirlos al destino en la red privada.

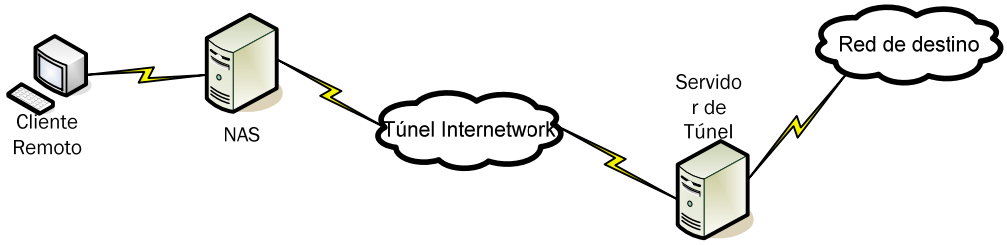


Figura. 2. 21 Escenario típico donde opera PPTP

2.9.3 Protocolo de envío de capa 2 (L2F)

L2F, una tecnología propuesta por Cisco, protocolo cuyo objetivo es proporcionar un mecanismo de transporte de tramas a nivel de enlace. L2F permite que los servidores de acceso de marcación incluyan el tráfico de marcación en el PPP y lo transmitan sobre enlaces WAN hacia un servidor L2F (un ruteador). El servidor L2F envuelve entonces los paquetes y los inyecta en la red. A diferencia del PPTP y L2TP, L2F no tiene un cliente definido. Entre las principales ventajas que se pueden destacar del protocolo L2F se pueden mencionar:

soporte multiprotocolo, multiplexación de múltiples sesiones remotas disminuyendo el número de túneles abiertos en un momento dado, gestión dinámica de los túneles por la cual los recursos de los servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario, L2F evita problemas de duplicidad debido al mantenimiento de un número de secuencia de las sesiones multiplexadas.

2.9.4 Protocolo de túnel de capa 2 (L2TP)

El protocolo de túnel de capa 2 es un protocolo que encapsula las tramas del PPP que se enviarán sobre redes IP, X.25, *Frame Relay* o ATM y combina las mejores funciones de los protocolos PPTP y L2F, los túneles L2TP pueden llevarse a cabo en redes públicas IP o no. En L2TP se crea el túnel mediante mensajes L2TP y utiliza UDP para enviar tramas del PPP encapsuladas del L2TP como los datos enviados por el túnel, las cargas útiles de las tramas encapsuladas PPP pueden encriptarse o comprimirse.

A pesar que PPTP y L2TP utilizan PPP para proporcionar un encapsulamiento inicial a los datos y luego incluir encabezados adicionales para transportarlos a través de la red y ser protocolos similares se pueden distinguir las siguientes diferencias:

- ✓ En PPTP se requiere que la red sea IP, en L2TP requiere sólo que los medios del túnel proporcionen una conectividad punto a punto orientada a paquetes: L2TP sobre IP, circuitos virtuales (PVCs), circuitos virtuales X.25, Frame Relay o ATM.
- ✓ PPTP soporta sólo un túnel único entre dos puntos, L2TP permite el uso de varios túneles entre puntos terminales.

- ✓ PPTP no proporciona autenticación de túnel, L2TP sí.

2.9.5 Protocolo de seguridad IPsec

El protocolo de Seguridad de Internet IPSec es un protocolo de capa 3 desarrollado por la IETF y definido en una serie de RFCs especialmente 1825, 1826, 1827, 2401-2402 mediante el cual se da soporte a la transferencia protegida de datos de extremo a extremo a través de una red IP.

- **Características de IPSec**

✓ Ipsec es un mecanismo de seguridad para transmitir datos a través de redes IP pero asegurando confidencialidad, integridad autenticación de los datos sobre redes no protegidas como el Internet.

✓ IPsec actúa sobre la capa de red protegiendo y autentificando paquetes IP entre equipos IPsec pares.

✓ Es un estándar de capa 3 que provee confidencialidad, autenticación, integridad de los datos, *replay detection*.

- **Protocolo IPsec y Cabeceras**

El estándar IPsec define dos funciones que aseguran la confidencialidad: encriptación e integridad de los datos; provee un método para administrar la autenticación y la protección de los datos entre múltiples pares. IPsec usa tres principales protocolos para crear la seguridad: incluye un protocolo de intercambio de llaves conocido como *Internet Key Exchange (IKE)* y dos protocolos IPsec IP, *Encapsulation Security Payload (ESP)* y *Autentication Header (AH).*

✓ Encabezado AH y ESP

IPsec provee autenticación, integridad y encriptación a través de la inserción de uno o ambos encabezados AH o ESP en el datagrama IP.

Utiliza el encabezado AH (MD5, SHA-1 HMAC) para proporcionar la autenticación e integridad de la fuente, sin encriptación y el ESP (DES, 3DES ó AES) para proveer la autenticación, la integridad junto con la encriptación.

✓ Protocolo de Intercambio de llaves IKE

IKE es un protocolo utilizado para establecer una asociación de seguridad (*Security Association [SA[11]]*) mediante el intercambio de llaves de Diffie-Hellman. La utilización de IKE solventa los problemas de la implementación manual y no escalable de IPsec debido a automatización del proceso entero de intercambio de llaves:

- Negociación de características SA
- Generación automática de la llave.
- Refrescamiento automático de la llave.
- Configuración manual manejable.

Cabe mencionar que el protocolo IKE surge de la integración de dos protocolos complementarios: ISAKMP (*Internet Security Assocciation and Key Managment Protocol*), Oakley (*Oakley Key Determination Protocol*). ISAKMP arquitectura para el intercambio de mensaje incluyendo los formatos del paquetes estados de transiciones entre dos pares. Oakley especifica la lógica de cómo se realiza el intercambio de forma segura de una clave entres dos entidades que no se han conocido previamente.

2.10 BENEFICIOS DE UNA VPN

La implementación de una red VPN trae consigo algunos beneficios para las empresas entre los cuales se puede citar:

- ✓ Reducción de costos operacionales
- ✓ Simplificación de la de la topología de red.
- ✓ Alta seguridad mediante la utilización de algoritmos complejos de autenticación, encriptación, etc.

[11] La Asociación de Seguridad (SA) es el establecimiento de seguridad de la información entre dos entidades de la red para lograr una comunicación segura. Un SA puede incluir llaves criptográficas, certificados digitales, etc.

- ✓ Escalabilidad de la red.
- ✓ Seguridad, fiabilidad, administración de la red menos compleja.
- ✓ Entre otras.

2.11 ASPECTOS RELEVANTES

- Las redes privadas virtuales (VPNs) reemplazan a los circuitos dedicados emulando enlaces punto a punto en una infraestructura compartida.

- Los servicios VPN permiten que los usuarios se conecten de manera confiable a servidores remotos, sucursales u otras compañías, sobre redes públicas y privadas pero manteniendo una comunicación segura.

- Cuando se refiere a una red privada virtual implícitamente se habla de seguridad; el proveedor del servicio debe garantizar la confidencialidad de su información de terceros. La seguridad se puede proporcionar a través del encapsulamiento, encriptación ó ambos.

- En una red MPLS VPN los equipos basados en su posición son: PE router, CE router y P router.

- Los dos modelos principales de VPNs son *overlay VPN* y *peer-to-peer VPN*

  Donde,

  Overlay VPNs puede ser implementado usando tecnologías de capa 1, 2 o 3, son fáciles de implementar y los circuitos virtuales deben provisionarse manualmente.

  VPNs peer-to-peer son implementadas usando tecnología de ruteo IP, requieren que el proveedor de servicios participe en el enrutamiento del cliente, garantizan que sea óptimo entre los sitios.

- Desde el punto de vista de un proveedor de servicios, la implementación de una *overlay VPN* conlleva implícitamente problemas de escalamiento. Administrar y proveer una gran cantidad de circuitos/túneles entre los equipos del cliente y el diseño de IGP es típicamente complejo.

- Con el objetivo de aliviar las desventajas de las *overlay VPN* fueron introducidas *las peer-to-peer VPN* en las que se diferencia dos modelos: PE router compartido y PE router dedicado. Así mismo, desde el punto de vista de un proveedor, surgen desventajas al momento de su implementación: altos costos para el mantenimiento de filtros de paquetes y la implementación de un router dedicado para cada cliente.

- A partir de una *overlay* y *peer-to-peer* existen diferentes topologías que dependiendo de la necesidad y requerimientos del cliente se pueden implementar: por la topología de los circuitos virtuales (*hub-and-spoke, parcial* o *full mesh* y multinivel), según las necesidades del negocio (intranet, extranet y de acceso) y topologías que surgen de acuerdo al tipo de conectividad requerida entre los sitios (simple, *overlapping vpn*, de servicios centrales y de administración de red).

- A través de una solución VPN, cualquiera que fuese, se debe garantizar al cliente la privacidad e integridad de los datos por tanto esta debe proveer autenticación, encriptación de datos, administración de llaves, soporte de protocolos múltiples, entre otras.

- Para levantar una VPN existen diferentes protocolos de capa 2 y de capa 3 que han sido estandarizados de tal manera que se logre la comunicación entre los sitios. Entre los protocolos de capa 2 se tiene PPTP, L2TP y L2F y protocolos de capa 3 como IP sobre IP, e IPsec.

- Implementar un diseño adecuado de una red privada virtual ofrece a los proveedores algunos beneficios. Reducción de costos operacionales, simplificación de la topología de la red y por ende menor manejo de hardware lo que se traduce en costos operacionales y de mantenimiento. Alta seguridad, escalabilidad de la red, fiabilidad, administración de red menos compleja.

CAPÍTULO III

REDES PRIVADAS VIRTUALES BASADAS EN LA TECNOLOGIA MULTIPROTOCOL LABEL SWITCHING (MPLS VPN's)

3.1 INTRODUCCION

Las redes privadas virtuales MPLS o MPLS VPN es una de las aplicaciones e implementaciones más populares de la tecnología MPLS. En la actualidad proveedores de servicios han optado por la migración de sus tradicionales redes Frame Relay y ATM a redes MPLS VPN.

MPLS VPN sigue teniendo un creciente interés dentro de la industria de las telecomunicaciones donde las grandes empresas lo ven como el próximo paso en el **diseño** de la red. La implementación y uso de estas redes puede proporcionar a los proveedores de servicios escalabilidad y facilitar a la vez el funcionamiento y administración de la red.

3.2 MPLS VPN

Como se ha mencionado en el transcurso del estudio, las redes privadas virtuales han existido antes del surgimiento de MPLS y las implementaciones más populares han sido a través de Frame Relay y ATM.

Ahora bien, las MPLS VPN a breves rasgos estudiada en la sección 2.6.3 es un ejemplo del modelo peer-to-peer altamente escalable, que combina las mejores características de una overlay VPN y una peer-to-peer VPN:

- Los PE routers participan en el enrutamiento del cliente lo cual garantiza y un óptimo ruteo entre los sitios y fácil provisionamiento.

- Los PE routers tienen la posibilidad de transportar un grupo separado de rutas para cada cliente emulando un PE dedicado. Los clientes pueden manejar el mismo espacio de direcciones.

Existen dos tipos de VPN que pueden ser implementadas a través de MPLS:

- MPLS VPN de capa 2 (MPLS L2 VPN): también conocidas como VPNs Martini/Kompella permiten la conectividad de capa 2 a través de una estructura MPLS.

- MPLS VPN de capa 3(MPLS L3 VPN): también conocidas como VPNs BGP MPLS usan las extensiones del protocolo de enrutamiento BGP para interconectar lugares remotos.

3.2.1 Modelo MPLS VPN

Similar a la terminología y dispositivos que se diferencian en una VPN común (sección 2.5), una MPLS VPN también está conformada por un PE router, dispositivo de borde el mismo que tiene una conexión directa con el dispositivo de borde del cliente CE router de capa 3. El P router es un dispositivo que no tiene conexión directa con los routers del cliente y el router del cliente ó C router con el PE router.
Cuando se realiza una implementación MPLS VPN los routers P y PE deben correr MPLS de tal manera que puedan distribuir y enviar etiquetas entre ellos mientras que el CE router no necesita correr MPLS.

Se deben tener algunas consideraciones [2]:

- Los routers CE y PE interactúan a nivel de capa 3 por tanto necesitan correr un protocolo de enrutamiento dinámico o estático entre ellos.

- El CE router tiene únicamente un par fuera del sitio VPN el mismo que es el PE router. No puede tener otro par CE router de otro sitio VPN a través de la red del proveedor.
- En el caso de que el CE router sea *multihomed*, puede ser par con múltiples PE routers.

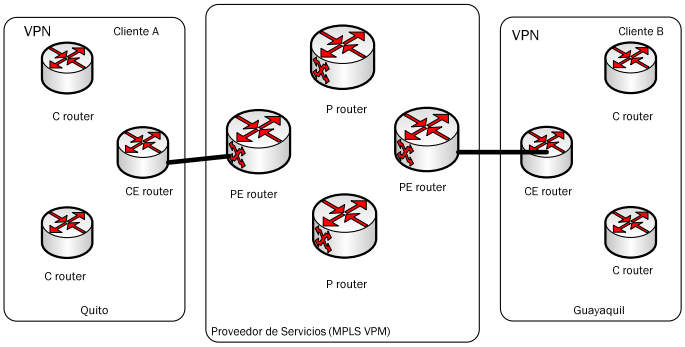


Figura. 3. 1 Terminología de dispositivos en la red MPLS VPN

En una VPN, los clientes del proveedor de servicios VPN mantienen su propio esquema de direccionamiento, esto significa usar sus direcciones IP registradas, direcciones IP privadas ó también direcciones IP que están siendo usadas por otros clientes conectados al mismo proveedor de servicios (conocido como *overlapping IP addressing*). En el caso de que los paquetes sean reenviados como paquetes IP a través del proveedor de servicios esto podría causar problemas debido a que el P router estaría confundido. Por tanto el esquema de direccionamiento privado y el *overlapping* de direcciones no estarían permitidos. Siendo así, cada paquete debería ser reenviado buscando una dirección IP de destino en cada router que conforma la red del proveedor de servicio, esto significa que el P y el PE router tengan una tabla completa de cada cliente lo que a su vez implica una tabla de direccionamiento bastante grande.

Para lograr este trabajo se tienen tres soluciones:

1) El único protocolo capaz de transportar un largo número de rutas es **BGP** (*Border Gateway Protocol*) por tanto en el proveedor de servicios entre el P y el PE router debería correr el iBGP (*Internal BGP*). Esta solución no es aceptable debido a que la red dejaría de ser privada para los clientes y ya no sería una VPN.

2) La segunda opción sería que cada P y PE router mantengan una tabla de enrutamiento privada por cada cliente y un proceso de un protocolo de enrutamiento corra sobre todos los routers P por cada VPN. Esta solución no es escalable debido a que, cada vez que una VPN sea agregada a la red, un nuevo proceso de enrutamiento debe ser también agregado a cada P router.

3) La tercera y escalable solución es a través de MPLS, donde los paquetes IP son etiquetados en la red del proveedor de servicios para realizar una VPN por cada cliente. En este caso los P routers no necesitan corren BGP y tampoco tener la tabla de enrutamiento de los clientes, los routers VPN son únicamente conocidos por los PE routers es decir por los routers de borde en la red MPLS VPN, lo cual hace de MPLS VPN una solución escalable.

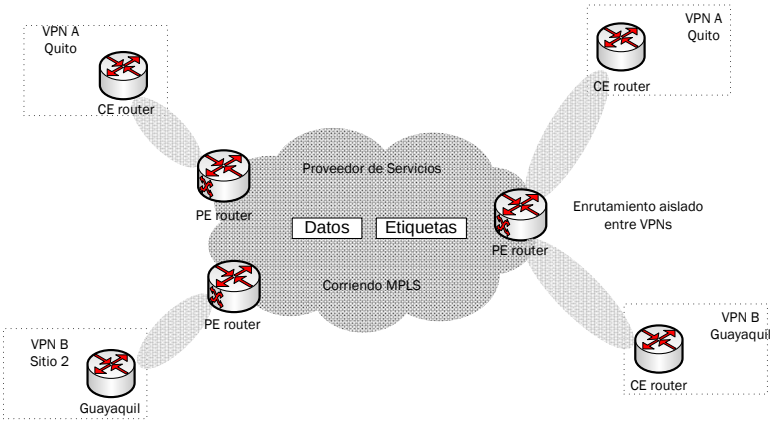


Figura. 3. 2 Modelo MPLS VPN

3.3 ARQUITECTURA MPLS VPN

Para lograr entender la arquitectura MPLS VPN es necesario estudiar cada uno de los bloques que conformar un PE router (ver figura 3.3): **Virtual Routing Forwarding** *(*VRF*), route distinguisher* (RD), *route targets* (RT), propagación de rutas a través de *Multiprotocol BGP* y reenvío de paquetes etiquetados [2].

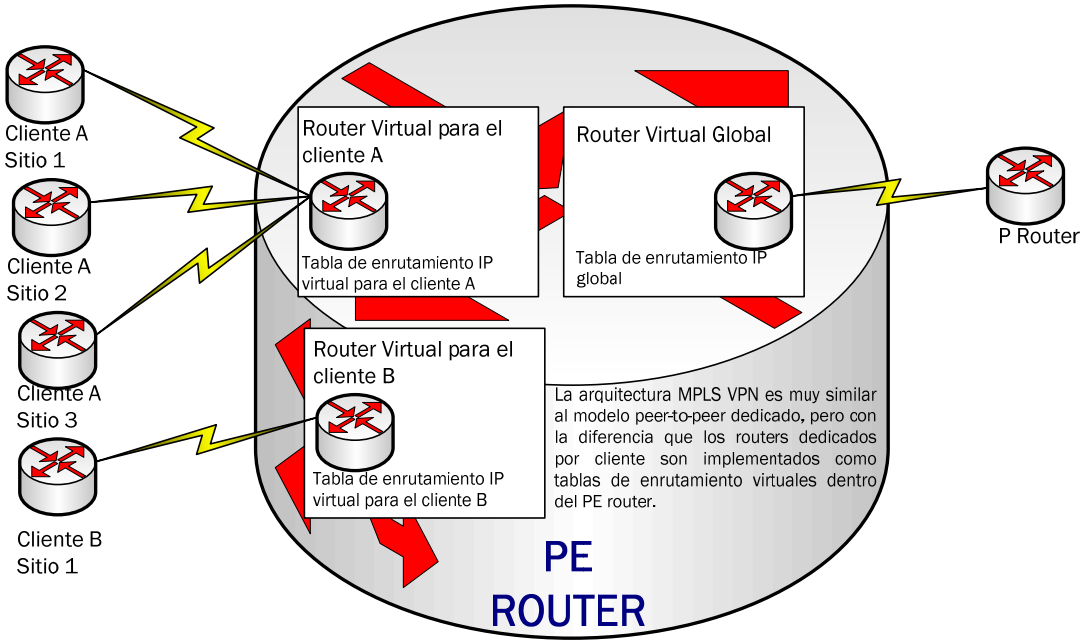


Figura. 3. 3 Arquitectura de un PE

3.3.1 Virtual Routing Forwarding (VRF)

La arquitectura MPLS VPN como se ha descrito en la sección 2.6.3 es bastante similar al modelo peer-to-peer PE router dedicado pero con la diferencia que los routers dedicados por clientes son implementados dentro del PE router como tablas de enrutamiento virtuales. Un enrutamiento/reenvío virtual (*virtual routing/forwarding*) es una instancia VPN de enrutamiento y reenvío cuyo nombre combina la tabla de enrutamiento VPN, la tabla VRF CEF (*Cisco Express Forwarding*) y la asociación de protocolos de enrutamiento IP sobre el PE router. Un PE router tiene una instancia VRF por cada VPN agregada al proveedor de servicios.

Ahora bien, como se puede observar en la figura 3.3 el PE router almacena una tabla de enrutamiento global y adicionalmente una tabla de enrutamiento separada y privada por cada VPN conectada al PE la cual se denomina tabla de enrutamiento VRF. Las tablas de enrutamiento VRF están en adición a la tabla de enrutamiento y reenvío global usada para tráfico no perteneciente a la VPN y contienen rutas de destino de los sitios locales y remotos

de los clientes. En este escenario, la interfaz (física ó lógica) del PE router conectada al CE router puede pertenecer a una sola VRF, por tanto los paquetes IP recibidos en una interfaz VRF son identificados inequívocamente como pertenecientes a esa VRF.

3.3.2 Route Distinguisher (RD)

El protocolo BGP cumple con las características como protocolo de enrutamiento para transportar rutas VPN a través de la red del proveedor de servicios, BGP transporta prefijos **IPv4** los mismos que deben ser únicos. Al ser así, en el caso de que los clientes tuviesen overlapping de direcciones IP, el enrutamiento podría ser erróneo. Para resolver este problema surge el concepto de *Route Distinguisher* a través del cual se logra hacer los prefijos IPv4 únicos y cuya combinación (**IPv4** y **RDs**) es conocida como prefijo **vpnv4**. Así mismo para transportar los prefijos **vpnv4** entre los PE routers es necesario el protocolo **MP-BGP.**

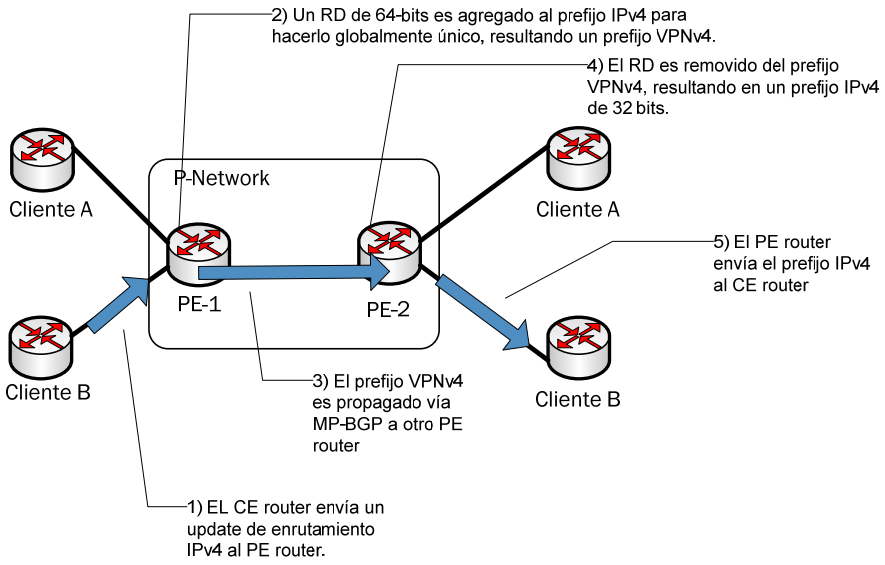


Figura. 3. 4 Propagación de información de ruteo a través de la P-Network

El *route distinguisher* es un campo de 64 bits y puede ser representado por medio de dos formatos: ASN:nn**,** donde ASN es el número de sistema autónomo que el *Internet Assigned Numbers Authority (*IANA*)* asigna al proveedor de servicios y el ***nn*** es el número que el proveedor de servicios asigna únicamente a una VRF. E IP-address:nn.

3.3.3 Route Targets (RT)

A través de la utilización de prefijos RD se identifica la pertenencia a una VPN pero la comunicación entre los sitios de diferentes VPNs no es posible. Siendo así, los *route targets* (**RDs**) fueron introducidos en la arquitectura MPLS con la finalidad de soportar complejas topologías de VPNs donde los sitios de los clientes pueden participar en más de una VPN.
Los route targets son atributos adicionales añadidos a las rutas VPNv4 BGP con lo cual se indica pertenencia a una VPN. Para codificar dichos atributos se hace uso de comunidades extendidas de BGP las mismas que transportan los principales atributos.

Entre las características principales de un RT se pueden mencionar:

- Uno o más RTs pueden ser añadidos a la misma ruta.
- El mismo RT puede ser agregado a todas las rutas de un sitio en particular ó RTs diferentes pueden ser añadidos a cada ruta.
- En un sistema autónomo (AS) están habilitadas 2^{32} RTs.

Los RTs pueden trabajar de dos maneras [9]:

1) *Export RT*, identifican la pertenencia a una VPN y va adjunta a la ruta del cliente cuando ha sido convertida en una ruta VPNv4.

2) *Import RT*, asociada con cada tabla de enrutamiento virtual y selecciona las rutas que van a ser insertadas en la VRF.

Tanto las *Export RTs* e *Import RTs* son el bloque central de las VPN debido a que la utilización de las mismas expresan las políticas que determinan la conectividad entre los sitios de los clientes.

3.3.4 Modelo de Ruteo en las MPLS VPNs

Según lo estudiado en la sección 3.3.1, las tablas VRF permiten separar las rutas de los clientes en el PE router, ahora bien la pregunta es cómo se transportan los prefijos a través de la red de proveedor de servicios y como los PE router reenvían los paquetes originados en la red del cliente.

Los requerimientos de enrutamiento en las redes MPLS VPN se resumen en tres puntos [9]:

- ✓ Los CE routers deben correr un software de enrutamiento IP estándar.
- ✓ Los routers PE soportan servicios de MPLS VPNs y enrutamiento de Internet.
- ✓ Finalmente los routers P no tienes rutas VPN.

- **Enrutamiento en la MPLS VPN: CE router**

Desde el punto de vista de un CE router los PE routers corren son como cualquier otro router en la C-Network. Corren un protocolo estándar de enrutamiento IP: eBGP, OSPF, RIPv2, EIGRP y rutas estáticas. E intercambian *updates* con el PE router.

- **Enrutamiento en la MPLS VPN: PE router**

El PE router intercambia rutas entre el CE router, P router y otros PE routers. Rutas de VPNs con los CE routers a través de protocolos de enrutamiento (mencionados anteriormente), rutas de core con los P y PE routers a través de IGP de core, y rutas VPNv4 con otros PE routerss a través de sesiones MP-iBGP[12].

- **Enrutamiento en la MPLS VPN: P router**

[12] Se conoce como iBGP debido a que el protocolo BGP corre entre dispositivos que están dentro del mismo sistema autónomio (AS).

Los P routers no participan en el enrutamiento de las MPLS VPN y por tanto no transportan rutas VPN. Corren un IGP con los PE routers e intercambian información global acerca de subredes (enlaces de *core*).

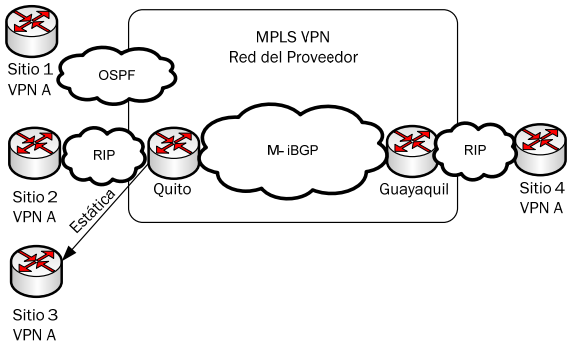


Figura. 3. 5 Protocolos de enrutamiento levantados en entre los dispositivos de la MPLS VPN [1]

- **Flujo de actualizaciones o updates:**

En la figura 3.6, se puede observar de manera global y como ejemplo la propagación de rutas en una red MPLS VPN.

Donde,

1) Los PE routers reciben rutas IPv4 desde el CE router a través de un IGP (*Interior Gateway Protocol*) o a través de un BGP externo (eBGP).
2) Las rutas IPv4 del sitio VPN son insertadas en la tabla VRF.
3) Un RD es añadido a la ruta IPv4 haciéndola una ruta VPNv4.
4) El PE router exporta las rutas VPNv4 a través de MP-BGP al PE de destino.
5) En el PE de destino remueve los RDs de la ruta VPNv4 y envía al CE router un update IPv4 a través de un protocolo IGP o eBGP.
6) La distribución de rutas hacia los CE routers es determinado por las comunidades BGP. Estas comunidades identifican las rutas del CE usando los RTs y el SOO (opcional).

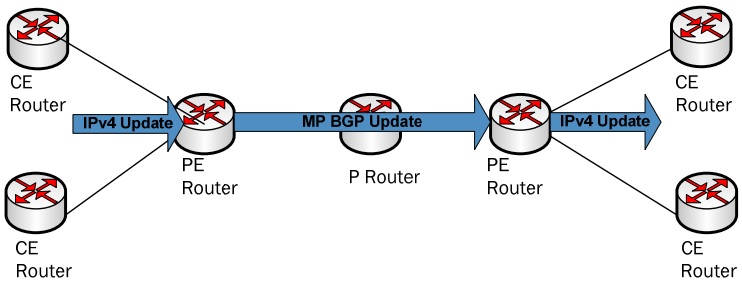


Figura. 3. 6 Flujo de updates de extremo a extremo

Un update MP-BGP contiene lo siguiente [9]:

- Dirección VPNv4.
- Cominidades extendidas (*route targets*, opcional SOO).
- Etiquetas usadas por el envío de paquetes VPN.
- Cualquier otro atributo BGP como el *AS path*, *local preference*, *MED*, comunidades estándar.

3.3.5 Envío de Paquetes a través del Backbone MPLS VPN

Como se estudió en secciones anteriores, cuando un paquete IP ingresa al backbone MPLS VPN a través del PE router, un prefijo de 64 bits es añadido al paquete y esto lo hace único. Dentro del backbone MPLS VPN, es necesario también que el paquete sea singularmente reconocible.

Con la introducción de MPLS esta función es posible, cada paquete VPN es etiquetado por el PE router de ingreso y viaja a través de los routers donde dicha etiqueta es conmutada por otra hasta finalmente llegar al PE router de salida. A través de esta función de conmutación los routers no ven el paquete en sí sino su etiqueta.

El protocolo de distribución de etiqueta (*Label Distribution Protocol [LDP]*) es el camino más común y utilizado en este caso. LDP es configurado entre el P y PE routers donde todo el tráfico es etiquetado-conmutado entre ellos.

El envío de paquetes se lo puede analizar de la siguiente manera [2]:

- ✓ El PE router debería etiquetar el paquete VPN con una etiqueta LDP para el router PE saliente y enviar los paquetes etiquetados a través del *backbone* MPLS. Los routers P realizan conmutación de etiquetas, y el paquete alcanza al router PE de salida Sin embargo, el router de salida no conoce cual VRF usar para el paquete conmutado y por tanto el paquete es eliminado.

- ✓ El router PE debería etiquetar el paquete VPN con un *stack* de etiquetas, usando la etiqueta LDP para el router de salida como etiqueta TOP, y la etiqueta VPN asignada por el router PE de salida como segunda etiqueta en el *stack.*
  Los routers P realizan el switcheo de etiquetas, y el paquete alcanza al router PE de salida. El router PE de salida realiza un *lookup* sobre la etiqueta de VPN y envía los paquetes al router CE.

Los paquetes IPv4 son etiquetados en el PE router de ingreso con una etiqueta LDP conocida como ***IGP label***. Se conoce con este nombre por dos razones: la primera porque está ligada a un prefijo IPv4 y la segunda porque a través de un protocolo IGP es anunciada a través del *backbone*. Cabe recalcar que la IGP *label* sólo se usa para enviar el paquete a través de la red del proveedor de servicios y por tanto el PE router de salida desconoce a cual VRF pertenece.

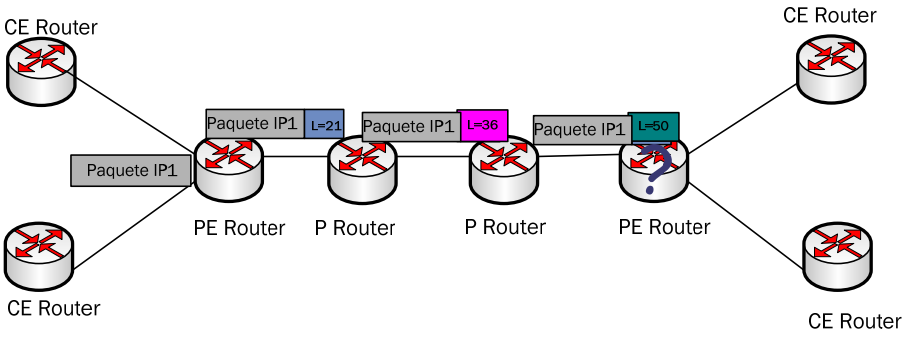


Figura. 3. 7 Envío de paquetes IPv4 a través del backbone MPLS VPN

Siendo así, es necesario añadir otra etiqueta en el stack de etiquetas MPLS que indica a que VRF pertenece el paquete. Por tanto los paquetes de todos los clientes son enviados con dos etiquetas: la IGP label como la etiqueta TOP la misma que es distribuida por LDP o RSVP entre todos los P y PE routers salto por salto, y la etiqueta VPN (refererida también como BGP *label*) como etiqueta *bottom* (ver sección 1.5.7.2) distribuida por MP-iBGP desde un PE router a otro PE router. Los P routers usan la BGP label para enviar el paquete al PE router de salida correcto y el Pe router de salida usa la BGP label para enviar el paquete IP al CE router correcto.

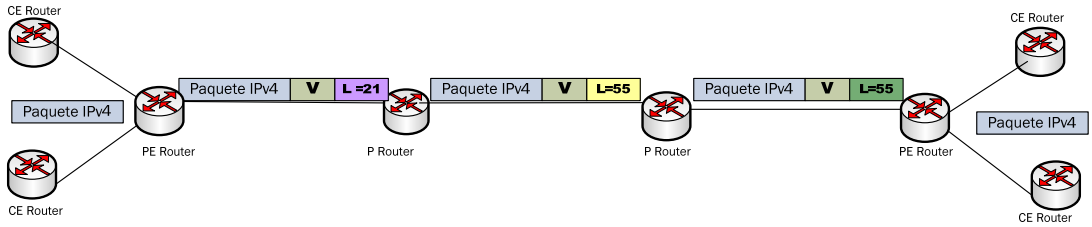


Figura. 3. 8 Envío de paquetes con stack de etiquetas

- **Penultimate hop Popping en MPLS VPN [1]**

➢ ***Penultimate hop Popping en MPLS:***

En un escenario MPLS el LSR de salida (sección 1.5.4) tiene dos funciones realizar una acción POP es decir remover la etiqueta y leer la cabecera IP para enviar el paquete fuera del dominio. Llevar a cabo estas dos acciones significa reducir el desempeño del nodo y puede

incrementar la complejidad del hardware significantemente. Siendo así el concepto de *Penultimate hop Popping* fue introducido en la arquitectura MPLS de tal manera de resolver ambos problemas.

Con PHP un LSR de salida solicita una operación de etiqueta pop desde su vecino *upstream*, el mismo que remueve la etiqueta del paquete y lo envía como un paquete IP puro al LSR de salida el mismo que lee la cabecera y lo envía a su destino.

- ***Penultimate hop Popping en VPN:***

En las MPLS VPN, *penultimate hop popping* sobre la IGP *label* puede ser realizado sobre el último P router. El PE router realiza un *lookup* sobre la etiqueta de VPN o BGP *label* y envía el paquete al CE router correspondiente.

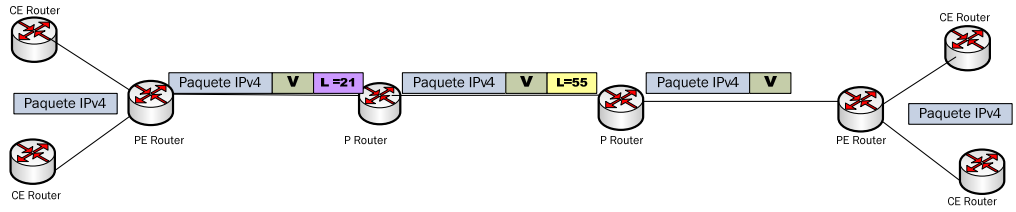


Figura. 3. 9 MPLS VPN Penultimate Hop Popping

3.4 TOPOLOGIAS MPLS VPN

Dependiendo de las necesidades y requerimientos del diseño de la red, existe una gran variedad de topologías que pueden ser implementadas a través de la arquitectura MPLS VPN pero en la actualidad existen topologías que son mayormente usadas [10]. Cabe recalcar que cada una de estas topologías/modelos de conectividad VPN, son posibles debido a la utilización de RTs como se ha mencionado en la sección 3.3.3.

3.4.1 Topología Full Mesh MPLS VPN

En la topología *full mesh* todos los sitios de diferentes VPN pueden comunicarse directamente entre sí. En este tipo de conectividad un RT singular para importar y exportar políticas a todos los sitios.

3.4.2 Topología Hub and Spoke MPLS VPN

En la topología Hub and Spoke los sitios pueden comunicarse indirectamente con otro a través de un sitio designado o hub. Esta topología puede ser implementada mediante la utilización de dos RTs: RT-Spoke para los sitios remotos (*spoke*) y un RT-*Hub* para el sitio central (*hub*) [1].

1) El UIO-PE-Spoke PE router exporta todas las rutas desde la tabla VRF de *MusicLife* usando un valor de RT de *Hub*.

2) El GYE-PE-Hub PE router es configurado para importar el Hub-RT en una de sus tablas VRFs. Esta interfaz VRF se adjunta al sitio central *MusicLifeDVD* y reenvía todas las rutas aprehendidas desde los sitios *spoke* al GYE-CE3-Hub, lo cual está localizado dentro del sitio central.

3) El GYE-CE3-Hub CE router, anuncia las rutas a través del sitio central.

4) Los rutas son eventualmente anunciadas de regreso a al GYE-PE-Hub a través de una interfaz diferente.

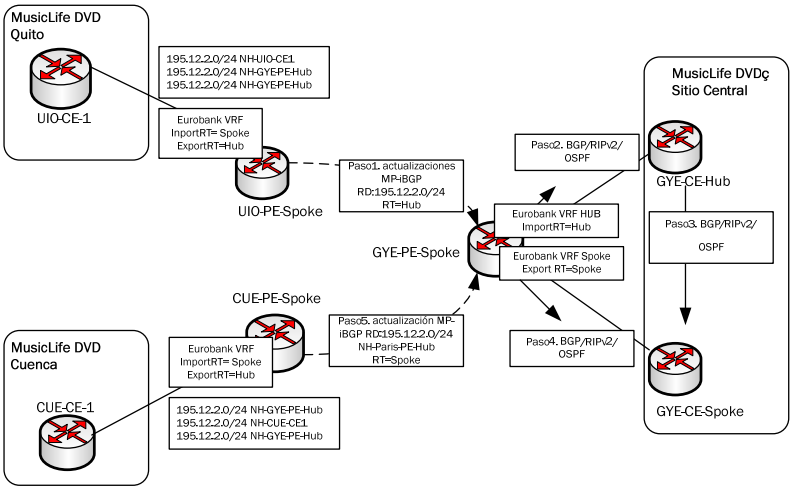


Figura. 3. 10 Topología MPLS VPN Hub and Spoke [1]

5) Entonces GYE-PE-Hub PE router anuncia las rutas de regreso en el *backbone* MPLS VPN con un valor de RT *spoke*.

6) Cada PE router es configurado para importar cualquier ruta con una valor de RT spoke en la VRF de *MusiLifeDvD*, lo cual significa que las direcciones de siguiente salto para todos los sitios *spoke*, como los vistos por otros sitios *spoke*, es a través del sitio central GYE-PE-Hub Pe router.

3.4.3 Servicios Centrales MPLS VPN

Una de las topologías comúnmente implementadas en la tecnología MPLS VPN es la de servicios centrales VPN.

- **Características**

✓ Los clientes necesitan acceder a servidores centrales.
✓ Los servidores tienen la posibilidad de comunicarse entre ellos.
✓ Los clientes pueden comunicarse con todos los servidores pero no entre ellos.

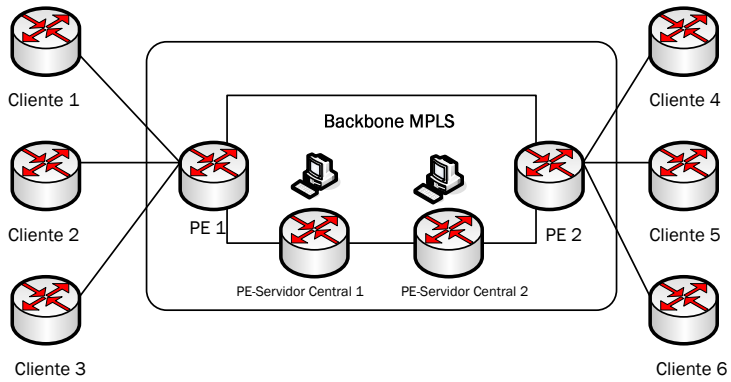


Figura. 3. 11 Topología de Servicios Centrales MPLS VPN

- Las rutas de los clientes necesitan ser exportadas a un *server site*.
- Las rutas del servidor necesitan ser exportadas a los clientes y *server sites*.
- Las rutas no son intercambiadas entre los sitios de los clientes.
- El cliente VRF contiene las rutas del servidor y por tanto los clientes pueden hablar con los servidores.
- El servidor VRF contiene rutas de los clientes por tanto los servidores pueden hablar con los clientes.
- El cliente VRF no contiene rutas de otros clientes por tanto los clientes no pueden comunicarse entre sí.

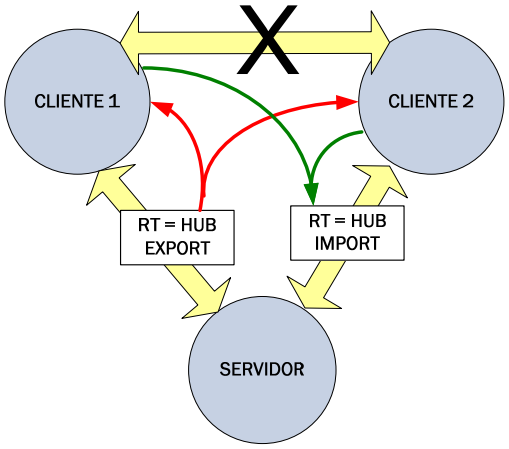


Figura. 3. 12 Enrutamiento en la MPLS VPN de servicios centrales [10]

Basados en dichas características, se puede diferenciar algunos de los requerimientos de conectividad de una VPN de servicios centrales, siendo así se deben tener las siguientes consideraciones para configurar el sitio del cliente y el *server site*.

Sitio del cliente:

- Una VRF por cada tipo de servicio diferente.
- Un RD único por cada tipo de servicio diferente.
- Las rutas exportadas e importadas con RT del mismo valor por cada sitio del cliente.
- Rutas exportadas con un RT asociado con el server site.

Server Sites:

- Una VRF por cada tipo de servicio diferente.
- Un RD único por cada tipo de servicio diferente.
- Las rutas exportadas e importadas con RT del mismo valor por cada sitio del cliente.
- Las rutas exportadas del *server site* con un RT (servidor a cliente).
- Las rutas importadas con RT en el servidor VRF.

3.4.4 Modelo Overlapping MPLS VPN

Un modelo overlapping VPN surge de la integración de una extranet e intranet VPN, es decir cuando se provee conectividad entre segmentos de dos VPNs.

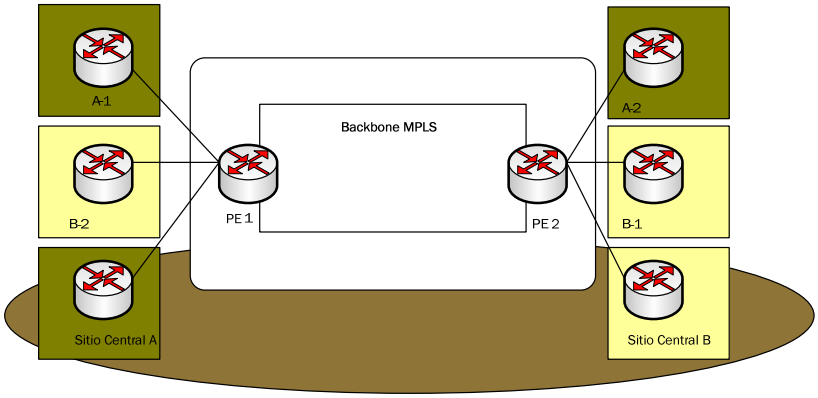


Figura. 3. 13 Topología Overlapping MPLS VPN

Características:

- Los sitios que participan en más de una VPN importan y exportan rutas con RTs desde cualquier VPN en las cuales ellos están participando.
- Los sitios *overlapping* VPN son configurados con una VRF del mismo RD para un grupo de sitios que pertenecen a la misma VPN. Los RTs son configurados basados en la pertenencia de VPN de cada sitio.

3.4.5 Redefinición de una VPN

La arquitectura MPLS ha permitido el diseño e implementación de modelos complejos de VPN con lo cual su concepto tradicional comienza cada vez más a ser obsoleto [9].
Se hace necesario entonces redefinir su concepto. Por tanto una VPN es una colección de sitios que comparten información de enrutamiento en común donde un sitio puede ser parte de diferentes VPNs y las diferentes topologías complejas pueden ser soportadas por múltiples tablas de enrutamiento virtual sobre los PE routers. Todo ello conlleva a optimización de recursos físicos, mayor facilidad de administración de la red y amplia escalabilidad.

3.5 BENEFICIOS DE UNA IMPLEMENTACION MPLS VPN

La implementación de MPLS VPN ofrece a los proveedores de servicios una serie de ventajas y a su vez ayuda a la creación de nuevos servicios.
Los beneficios que resultan de una implementación VPN se pueden resumir en los siguientes puntos [3,4]:

- **Seguridad**

A través de la configuración de las tablas virtuales en el PE router es posible el aislamiento del tráfico entre VPNs donde el PE router es el único en tener conocimiento acerca de cada VPN que está configurada en el *backbone*.

Adicionalmente la utilización de etiquetas para distinguir los paquetes IP asegura que los paquetes serán entregados a la VPN correcta.

- **Escalabilidad de la red**

MPLS VPN permite al proveedor de servicios la implementación de múltiples VPNs usando el mismo core de la red, donde la *Routing Information Base* (RIB) de la VPN es independiente de la tabla RIB del core haciendo de MPLS VPN más escalable.

La arquitectura e inteligencia de la red está implementada básicamente en los PE routers los mismos que mantienen una RIB por cada VPN permitiendo la implementación de VPNs que soportan *overlapping* (mismo espacio de direcciones) en el mismo core.

- **Extranets e Intranets**

A diferencia de las implementaciones tradicionales de extranets e intranets mediante el uso de políticas de enrutamiento cuya administración se convierte en algo bastante complejo, mediante MPLS VPN se puede hacer de una manera bastante simple y rápida.

- **Otras**

MPLS VPN permite al cliente "endosar" el enrutamiento de sus sitios al proveedor de servicios y al proveedor de servicios ofrecer servicios de valor agregado a sus clientes.

MPLS VPN mantiene un backbone virtual por cada cliente ya que permite en la misma infraestructura levantar múltiples clientes VPN.

La implementación de túneles PE-PE MPLS son usados para transportar tráfico para múltiples VPN y múltiples aplicaciones. En este contexto es una de las propiedades más poderosas y posibilita: enviar tráfico a direcciones que no son conocidas en el medio de la red, identificar tráfico perteneciente a una VPN en particular en el punto de salida de la red del proveedor de servicios y proveer protección fácil y a bajo costo.

3.6 ASPECTOS RELEVANTES

- Dentro de la industria de las telecomunicaciones, el campo mayormente explorado y explotado es el de las redes privadas virtuales a través de MPLS. El modelo MPLS VPN combina los mejores beneficios de una *overlay* y *peer-to-peer VPN* y es similar al modelo *peer-to-peer* router dedicado con la diferencia que los routers dedicados son implementados virtualmente en el PE-router.

- La diferencia entre MPLS VPN y el modelo *peer-to-peer* router dedicado es que el punto de presencia por cada cliente son implementados como tablas de enrutamiento virtuales dentro del PE router.

- En una red MPLS VPN al igual que una VPN tradicional también se distinguen los mismos dispositivos de red, con la diferencia que el P y PE router deben correr MPLS de tal manera que puedan enviar y distribuir etiquetas entre ellos, mientras que el CE router no necesita correr MPLS.

- En MPLS VPN los PE routers participan en el enrutamiento del cliente, transportan un grupo separado de rutas para cada cliente (similar al PE dedicado) y los clientes pueden tener el mismo espacio de direcciones.

- La arquitectura MPLS VPN se basa en los distintos bloques que conforman un PE router, en el cual se distinguen: las VRF, los RD, los RT, propagación de rutas a través de BGP y el reenvío de paquetes etiquetados.

- *Virtual Routing/Forwanding* es una instancia VPN de enrutamiento cuyo nombre combina tabla de enrutamiento VPN, la tabla VRF CEF y la asociación de protocolos de enrutamiento IP sobre el PE router. Un PE router tiene una instancia VRF por cada VPN agregada al *backbone* MPLS.

- La arquitectura de un router PE en MPLS VPN usa routers virtuales separados que contienen las rutas de cada cliente dentro de un router físico

- El método más escalable para el intercambio de rutas a través del *backbone* MPLS VPN es a través del uso de BGP de PE a PE.

- *Route distinguishers* transforman una dirección de 32 bits en una única dirección de 96 bits VPNv4 que es globalmente única en el escenario MPLS VPN. Para transportar protocolos VPVv4 es necesario levantar un protocolo MP-BGP entre los PE routers.

- Route targets es una comunidad extendida de BGP los cuales permiten identificar la pertenencia a una VPN en una topología *overlapping*.

- Con la introducción de RTs es posible una gran variedad de topologías complejas con lo cual las VPNs son ahora consideradas como una colección de sitios que comparten información de ruteo común.

- En enrutamiento MPLS VPN es escalable siempre y cuando los CE routers corran un protocolo estándar como enrutamiento estático ó dinámico a través de RIPv2, OSPF, EIGRP, EBGP hacia los PE routers.

- Los PE routers proveen los servicios y enrutamiento VPN, intercambiando información de ruteo del cliente a través de MP-BGP. Mientras que los P routers no participan en el enrutamiento VPN sino que proveen enrutamiento de *backbone* IGP a los routers PE.

- El enrutamiento MPLS VPN empieza en el instante que un PE recibe actualizaciones (*updates*) IPv4 desde el CE router y exporta las rutas IPv4 al router de destino PE como rutas VPNv4 vía MP-BGP. Finalmente el PE de destino importa las rutas VPNv4 y las envía al CE router como un *update IPv4*.

- Las comunidades BGP determinan la distribución de rutas hacia los CE routers, a su vez identifican las rutas del CE usando RTs y el SOO.

- El envío de los paquetes a través del PE router en el *backbone* MPLS se lo realiza a través de *stack* de etiquetas. En el *stack*, la etiqueta LDP es TOP y la etiqueta VPN es *bottom*.

- La etiqueta LDP es también conocida como IGP *label* porque está ligada a un prefijo IPv4 y la segunda porque a través de un protocolo IGP es anunciada a través del *backbone*. Se usa para enviar el paquete a través de la red del proveedor de servicios.

- La etiqueta VPN también es conocida como BGP *label* debido a que se anuncia a través de MP-BGP entre PE routers.

- A través de PHP el P router en el túnel LSP remueve la IGP *label* y el PE router final recibe el paquete que contiene únicamente la BGP l*abel* lo cual implica mejor desempeño del nodo y simplifica la complejidad del hardware.

- Una VPN MPLS tiene muchas ventajas asociadas en su implementación entre las cuales se puede mencionar seguridad, escalabilidad, implementación de complejas topologías complejas como la integración de intranets y extranets, costo de mantenimiento de red menor, etc.

CAPITULO IV

CONCLUSIONES

- La tecnología MPLS es un campo bastante amplio de exploración y de análisis. En el transcurso del estudio se ha logrado visualizar de manera global la gran cantidad y variedad de temas que se pueden abarcar y en muchos casos la complejidad de los mismos. En el presente documento se ha recopilado información valiosa de libros de diferentes autores de manera simplificada cuyo objetivo es proporcionar las bases fundamentales de MPLS y MPLS VPN de tal manera que sea una herramienta útil para personas con poco o nada conocimiento de la tecnología.

- A través del estudio se ha podido diferenciar cada uno de los temas más relevantes, permitiendo tener una visión global de la esencia, puntos claves, y su respectiva aplicación sobre las redes privadas virtuales, lo cual facilita el estudio de la tecnología.

  Adicionalmente se ha conseguido tener claridad sobre su importancia y los beneficios que brinda cuando se ha realizado un diseño e implementación adecuados por parte de los proveedores de servicios, entre las cuales se pueden mencionar: seguridad, escalabilidad, implementación de complejas topologías complejas como la integración de intranets y extranets, costo de mantenimiento de red menor, etc.

- Dados los beneficios de la tecnología, en la actualidad y específicamente en Ecuador, grandes proveedores han optado por la migración de sus redes originales a MPLS, y por ende en la implementación de sus respectivas aplicaciones. Es tan importante el tema en la industria de las telecomunicaciones a tal punto que existe la necesidad de capacitación por

parte de los participantes en dicho entorno. Este documento aporta significativamente en parte de la capacitación pero no es suficiente. Siendo así se sugiere que el estudio de MPLS no se limite únicamente a los conceptos, lo cual es importante, sino que se haga también énfasis en como estas redes son implementadas: conocerla a nivel de hardware y como se levantan los servicios en redes reales.

- MPLS es un campo tecnológico innovador, convergente, el presente y futuro de la nueva generación de redes cuyo campo de aplicación no se limita a los estudios hasta ahora realizados, sino que está ampliamente abierta a la investigación y desarrollo de nuevas y transformadores aplicaciones.

- MPLS es una tecnología que fue desarrollada hace algunos años, continúa siendo nueva, pobremente explotada y un beneficio que en el país muy pocos participantes disfrutan.

ANEXO 1

RFC 2858 MULTIPROTOCOL EXTENSIONS FOR BGP

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

Currently BGP-4 [BGP-4] is capable of carrying routing information only for IPv4 [IPv4]. This document defines extensions to BGP-4 To enable it to carry routing information for multiple Network Layer protocols (e.g., IPv6, IPX, etc...). The extensions are backward compatible - a router that supports the extensions can interoperate with a router that doesn't support the extensions. This document obsoletes RFC 2283.

1. Overview

The only three pieces of information carried by BGP-4 that are IPv4 specific are (a) the NEXT_HOP attribute (expressed as an IPv4 address), (b) AGGREGATOR (contains an IPv4 address), and (c) NLRI(expressed as IPv4 address prefixes). This document assumes that any BGP speaker (including the one that supports multiprotocol capabilities defined in this document) has to have an IPv4 address(which will be used, among other things, in the AGGREGATOR attribute). Therefore, to enable BGP-4 to support routing for multiple Network Layer protocols the only two things that have to be added to BGP-4 are (a) the ability to associate a particular Network Layer protocol with the next hop information, and (b) the ability to associated a particular Network Layer protocol with NLRI. To identify individual Network Layer protocols this document uses Address Family, as defined in [RFC1700].

One could further observe that the next hop information (the information provided by the NEXT_HOP attribute) is meaningful (and necessary) only in conjunction with the advertisements of reachable destinations - in conjunction with the advertisements of unreachable destinations (withdrawing routes from service) the next hop information is meaningless. This suggests that the advertisement of reachable destinations should be grouped with the advertisement of the next hop to be used for these destinations, and that the advertisement of reachable destinations should be segregated from the advertisement of unreachable destinations.
To provide backward compatibility, as well as to simplify introduction of the multiprotocol capabilities into BGP-4 this document uses two new attributes, Multiprotocol Reachable NLRI (MP_REACH_NLRI), and Multiprotocol Unreachable NLRI (MP_UNREACH_NLRI). The first one (MP_REACH_NLRI) is used to carry the set of reachable destinations together with the next hop information to be used for

forwarding to these destinations. The second on (MP_UNREACH_NLRI) is used to carry the set of unreachable destinations. Both of these attributes are optional and non-transitive. This way a BGP speaker that doesn't support the multiprotocol capabilities will just ignore the information carried in these attributes, and will not pass it to other BGP speakers.

2. Multiprotocol Reachable NLRI - MP_REACH_NLRI (Type Code 14):

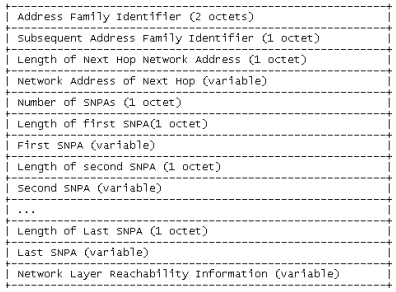
This is an optional non-transitive attribute that can be used for the following purposes:

(a) to advertise a feasible route to a peer

(b) to permit a router to advertise the Network Layer address of the router that should be used as the next hop to the destinations listed in the Network Layer Reachability Information field of the MP_NLRI attribute.

(c) to allow a given router to report some or all of the Subnetwork Points of Attachment (SNPAs) that exist within the local system

The attribute is encoded as shown below:



The use and meaning of these fields are as follows:

Address Family Identifier:
This field carries the identity of the Network Layer protocol associated with the Network Address that follows. Presently defined values for this field are specified in RFC 1700 (see the Address Family Numbers section).

Subsequent Address Family Identifier:
This field provides additional information about the type of the Network Layer Reachability Information carried in the attribute.

Length of Next Hop Network Address:
A 1 octet field whose value expresses the length of the "Network Address of Next Hop" field as measured in octets

Network Address of Next Hop:
A variable length field that contains the Network Address of the next router on the path to the destination system

Number of SNPAs:
A 1 octet field which contains the number of distinct SNPAs to be listed in the following fields. The value 0 may be used to indicate that no SNPAs are listed in this attribute.

Length of Nth SNPA:
A 1 octet field whose value expresses the length of the "Nth SNPA of Next Hop" field as measured in semi-octets

Nth SNPA of Next Hop:
A variable length field that contains an SNPA of the router whose Network Address is contained in the "Network Address of Next Hop" field. The field length is an

integral number of octets in length, namely the rounded-up integer value of one half the SNPA length expressed in semi-octets; if the SNPA contains an odd number of semi-octets, a value in this field will be padded with a trailing all-zero semi-octet.

Network Layer Reachability Information:
A variable length field that lists NLRI for the feasible routes are being advertised in this attribute. When the Subsequent Address Family Identifier field is set to one of the values defined in this document, each NLRI is encoded as specified in the "NLRI encoding" section of this document.
The next hop information carried in the MP_REACH_NLRI path attribute defines the Network Layer address of the border router that should be used as the next hop to the destinations listed in the MP_NLRI attribute in the UPDATE message. When advertising a MP_REACH_NLRI attribute to an external peer, a router may use one of its own interface addresses in the next hop component of the attribute, provided the external peer to which the route is being advertised shares a common subnet with the next hop address. This is known as a "first party" next hop. A BGP speaker can advertise to an external peer an interface of any internal peer router in the next hop component, provided the external peer to which the route is being advertised shares a common subnet with the next hop address. This is known as a "third party" next hop information. A BGP speaker can advertise any external peer router in the next hop component, provided that the Network Layer address of this border router was learned from an external peer, and the external peer to which the route is being advertised shares a common subnet with the next hop address. This is a second form of "third party" next hop information.

Normally the next hop information is chosen such that the shortest available path will be taken. A BGP speaker must be able to support disabling advertisement of third party next hop information to handle imperfectly bridged media or for reasons of policy.
A BGP speaker must never advertise an address of a peer to that peer as a next hop, for a route that the speaker is originating. A BGP speaker must never install a route with itself as the next hop.
When a BGP speaker advertises the route to an internal peer, the advertising speaker should not modify the next hop information associated with the route. When a BGP speaker receives the route via an internal link, it may forward packets to the next hop address if the address contained in the attribute is on a common subnet with the local and remote BGP speakers.

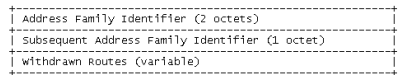
An UPDATE message that carries the MP_REACH_NLRI must also carry the ORIGIN and the AS_PATH attributes (both in EBGP and in IBGP exchanges). Moreover, in IBGP exchanges such a message must also carry the LOCAL_PREF attribute. If such a message is received from an external peer, the local system shall check whether the leftmost AS in the AS_PATH attribute is equal to the autonomous system number of the peer than sent the message. If that is not the case, the local system shall send the

NOTIFICATION message with Error Code UPDATE
Message Error, and the Error Subcode set to Malformed AS_PATH.

An UPDATE message that carries no NLRI, other than the one encoded in the MP_REACH_NLRI attribute, should not carry the NEXT_HOP attribute. If such a message contains the NEXT_HOP attribute, the BGP speaker that receives the message should ignore this attribute.

3. Multiprotocol Unreachable NLRI - MP_UNREACH_NLRI (Type Code 15):
This is an optional non-transitive attribute that can be used for the purpose of withdrawing multiple unfeasible routes from service.

The attribute is encoded as shown below:



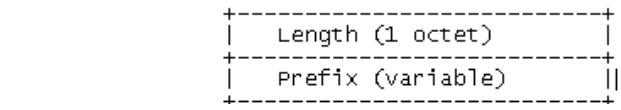
The use and the meaning of these fields are as follows:

Address Family Identifier:
This field carries the identity of the Network Layer protocol associated with the NLRI that follows. Presently defined values for this field are specified in RFC 1700 (see the Address Family Numbers section).

Subsequent Address Family Identifier:
This field provides additional information about the type of the Network Layer Reachability Information carried in the attribute.

Withdrawn Routes:
A variable length field that lists NLRI for the routes that are withdrawn from service. When the Subsequent Address Family Identifier field is set to one of the values defined in this document, each NLRI is encoded as specified in the "NLRI" section of this document.
An UPDATE message that contains the MP_UNREACH_NLRI is not required to carry any other path attributes.

4. NLRI encoding
The Network Layer Reachability information is encoded as one or more 2-tuples of the form <length, prefix>, whose fields are described below:



The use and the meaning of these fields are as follows:
a) Length:
The Length field indicates the length in bits of the address prefix. A length of zero indicates a prefix that matches all (as specified by the address family) addresses (with prefix, itself, of zero octets).
b) Prefix:
The Prefix field contains an address prefix followed by enough trailing bits to make the end of the field fall on an octet boundary. Note that the value of trailing bits is irrelevant.

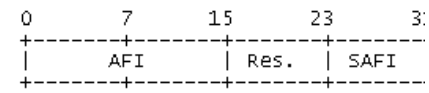
5. Subsequent Address Family Identifier
This document defines the following values for the Subsequent Address Family Identifier field carried in the MP_REACH_NLRI and MP_UNREACH_NLRI attributes:

1 - Network Layer Reachability Information used for unicast forwarding
2 - Network Layer Reachability Information used for multicast forwarding
3 - Network Layer Reachability Information used for both unicast and multicast forwarding

6. Error Handling
If a BGP speaker receives from a neighbor an Update message that contains the MP_REACH_NLRI or MP_UNREACH_NLRI attribute, and the speaker determines that the attribute is incorrect, the speaker must delete all the BGP routes received from that neighbor whose AFI/SAFI is the same as the one carried in the incorrect MP_REACH_NLRI or MP_UNREACH_NLRI attribute. For the duration of the BGP session over which the Update message was received, the speaker then should ignore all the subsequent routes with that AFI/SAFI received over that session.
In addition, the speaker may terminate the BGP session over which the Update message was received. The session should be terminated with the Notification message code/subcode indicating "Update Message Error"/"Optional Attribute Error".

7. Use of BGP Capability Advertisement
A BGP speaker that uses Multiprotocol Extensions should use the Capability Advertisement procedures [BGP-CAP] to determine whether the speaker could use Multiprotocol Extensions with a particular peer.
The fields in the Capabilities Optional Parameter are set as follows.

The Capability Code field is set to 1 (which indicates Multiprotocol Extensions capabilities). The Capability Length field is set to 4. The Capability Value field is defined as:
The use and meaning of this field is as follow:



AFI - Address Family Identifier (16 bit), encoded the same way as in the Multiprotocol Extensions
Res. - Reserved (8 bit) field. Should be set to 0 by the sender and ignored by the receiver.
SAFI - Subsequent Address Family Identifier (8 bit), encoded the same way as in the Multiprotocol Extensions.

A speaker that supports multiple <AFI, SAFI> tuples includes them as multiple Capabilities in the Capabilities Optional Parameter.

To have a bi-directional exchange of routing information for a particular <AFI, SAFI> between a pair of BGP speakers, each such speaker must advertise to the other (via the Capability Advertisement mechanism) the capability to support that particular <AFI, SAFI> routes.

Served" policy defined in RFC 2434. SAFI values 128 through 255 are for "private use", and values in this range are not to be assigned by IANA.

8. IANA Considerations
As specified in this document, the MPL_REACH_NLRI and MP_UNREACH_NLRI attributes contain the Subsequence Address Family Identifier (SAFI) field. The SAFI name space is defined in Section 9. The IANA will maintain and register values for the SAFI namespace as follows. SAFI value 0 is reserved. SAFI values 1, 2, and 3 are assigned in this document. SAFI values 4 through 63 are to be assigned by IANA using the "IETF Consensus" policy defined in RFC 2434. SAFI values 64 through 127 are to be assigned by IANA, using the "First Come First

As specified in this document, the MPL_REACH_NLRI and MP_UNREACH_NLRI attributes contain the Subsequence Address Family Identifier (SAFI) field. The SAFI name space is defined in Section 9. The IANA will maintain and register values for the SAFI namespace as follows. SAFI value 0 is reserved. SAFI values 1, 2, and 3 are assigned in this document. SAFI values 4 through 63 are to be assigned by IANA using the "IETF Consensus" policy defined in RFC 2434. SAFI values 64 through 127 are to be assigned by IANA, using the "First Come First Served" policy defined in RFC 2434. SAFI values 128 through 255 are for "private use", and values in this range are not to be assigned by IANA.
10. Security Considerations
This extension to BGP does not change the underlying security issues inherent in the existing BGP [Heffernan].

REFERENCIAS BIBLIOGRAFICAS

[1] PEPELNJAK, Ivan y GUICHARD, Jim. *MPLS and VPN Architectures*, tomo 1, tercera edición, Cisco Press, Estados Unidos, 2001.

[2] GUEIN DE, Luc, *MPLS Fundamentals*, tomo 1, segunda edición, Cisco Press, Estados Unidos, 2007.

[3] DAVIE, Bruce S. y FARREL, Adria, *MPLS: Next Steps*, volumen 1, primera edición, Elsevier, Estados Unidos, mayo 2008.

[4] MINEI, Ina y LUCEK, Julian, *MPLS Enabled Applications: EmergingDevelopments and New Technologies*, volumen 1, primera edición, John Wiley & Sons, Ltd, Inglaterra, octubre 2005.

[5] TAN, Nam-Kee, *Building VPNs with IPsec and MPLS*, tomo 1, primera edición, Mc-Graw-Hill, Estados Unidos, julio 2008.

[6] CCNP2, "IPsec VPN", *CCNP2 Módulo 3*, Quito, septiembre del 2008.

[7] OLEAS, Juan Carlos, "Modulo 1 Introducción a MPLS", *Configuración de redes MPLS*, Quito, julio 2008

[8] OLEAS, Juan Carlos, "Modulo 2 Asignación de etiquetas MPLS", *Configuración de redes MPLS*, Quito, julio 2008.

[9] OLEAS, Juan Carlos, “Modulo 4 MPLS VPN”, *Configuración de redes MPLS,* Quito, julio 2008.

[10] OLEAS, Juan Carlos, “Modulo 6 Complex MPLS VPNs”, *Configuración de redes MPLS,* Quito, julio 2008.

[11] Cisco Document ID: 14106, How Virtual Private Networks Work, http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094865.shtml, 13 octubre de 2008, Martes 21 de Julio de 2009.

[12] García J., Protocolos de Distribución de Etiqueta, http://panoramix.fi.upm.es/~jgarcia/Curso_MPLS/, Viernes, 19 de Junio de 2009.

[13] TYSON, Jeff, How Virtual Private Networks Work, http://www.howstuffworks.com/vpn.htm, Martes 21 de Julio de 2009.

[14] ANDERSON, L., LDP Specification, http://www.ietf.org/rfc/rfc3036.txt, Domingo 05 de Julio de 2009.

[15] BRANDEN, Ed., Resource ReSerVation Protocol (RSVP), http://tools.ietf.org/html/rfc2205, Domingo 05 de Julio de 2009.

[16] Microsoft Corporation, *Windows NT Service*, Microsoft Corporation, Estados Unidos, 1998.

El presente proyecto de grado fue entregado al Departamento de Eléctrica y Electrónica reposando en la Escuela Politécnica del Ejército desde el martes 1 de diciembre de 2009.

Sangolquí a,

Ana Lucía Segarra Zambrano	Ing. Gonzalo Olmedo, Ph.D
AUTORA	DIRECTOR DE CARRERA