ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ANÁLISIS, DISEÑO Y SIMULACIÓN DE UNA RED MPLS DE UN PORTADOR NACIONAL QUE PERMITA COMPARAR LOS SERVICIOS DE VPN CAPA 2 Y CAPA 3"

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

Eduardo Xavier Chica Bermúdez

Carlos Patricio Samaniego Palacios

Guayaquil - Ecuador

2008

DEDICATORIA

ES DESEO MUTUO DEDICAR ESTA TESIS PRIMERAMENTE A DIOS COMO TUTOR DE NUESTRAS VIDAS, A NUESTROS PADRES, QUIENES HAN SIDO, SON Y SERÁN PILARES FUNDAMENTALES EN CADA PASO DE NUESTRAS VIDAS Y A TODAS LAS PERSONAS QUE NOS HAN BRINDADO SU APOYO EN EL TRANSCURSO DEL DESARROLLO DE NUESTRO PROYECTO DE GRADO.

AGRADECIMIENTO

NUESTRO MAS SINCERO AGRADECIMIENTO A NUESTROS .PADRES, FAMILIARES, AMIGOS, COMPAÑEROS Y PROFESORES QUE NOS HAN BRINDADO SU TIEMPO Y PACIENCIA PARA PODER CULMINAR EXITOSAMENTE NUESTRA TESIS, ASÍ TAMBIÉN AGRADECEMOS A NUESTRO DIRECTOR EL ING. ALBERT ESPINAL POR SU AYUDA INCONDICIONAL.

TRIBUNAL DE GRADO

Ing. Holger Cevallos

SUB DECANO DE LA FIEC

PRESIDENTE

Ing. Albert Espinal

DIRECTOR DE TESIS

Ing. Juan Carlos Avilés

VOCAL

Ing. Cesar Yépez

VOCAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de graduación de la ESPOL)

Carlos Patricio Samaniego Palacios	Eduardo Xavier Chica Bermúdez
Autor	**Autor**

RESUMEN

Dada la evolución de la tecnología en redes de computadoras para su interoperabilidad y eficiencia se han desarrollado protocolos estandarizados internacionalmente como es el de Conmutación de etiquetas multiprotocolo o MPLS (Multi Protocol Label Switching) con sus aplicaciones principales como son: Ingeniería de Tráfico, Calidad de Servicio y redes privadas virtuales (VPN) sobre MPLS. Cada una de estas aplicaciones se enfoca a resolver diferentes problemas o necesidades que se presentan día a día en la transferencia de datos interna y externa de una empresa.

La evolución de una empresa portadora de datos (ISP) es llegar a dar el soporte de multiprotocolos a sus clientes, junto con la integridad de sus datos y la velocidad de transferencia. MPLS se ha convertido actualmente en el factor común evolutivo de los ISPs a nivel mundial, razón por la cual consideramos es importante entrar a la investigación y desarrollo de esta tecnología en nuestro país.

El motivo de esta tesis, es analizar una de las aplicaciones principales de MPLS que es su soporte de redes privadas virtuales (VPNs) y comparar los servicios principales en base a su funcionalidad referentes a las capas del modelo OSI, de donde se conocen las MPLS/VPN capa 2 y capa 3, dado que son tecnologías en que vienen a resolver y mejorar la interconexión y transferencia de datos entre agencias a nivel local e internacional. Para cumplir con nuestro estudio nos apoyaremos en simular escenarios y comparar resultados de estas dos tecnologías sobre un prototipo de núcleo (backbone) ISP que se ajuste a nuestro alcance y necesidades sin alejarse de su estructura real y sirva como soporte para futuras implementaciones e investigaciones de esta tecnología.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO DE TÉRMINOS

ARP	ADDRESS RESOLUTION PROTOCOL
ATOM	ANY TRANSPORT OVER MPLS
ATM	ASYNCHRONY TRANSFER MODE
BGP	BORDER GATEWAY PROTOCOL
CEF	CISCO EXPRESS FORWARDING
CE	CUSTOMER EDGE ROUTERS
C	CUSTOMER ROUTERS
DLCI	DATA LINK CONTROL IDENTIFIER
ELSR	EDGE-LABEL SWITCH ROUTER
EIGRP	ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL
EOMPLS	ETHERNET OVER MPLS
EBGP	EXTERIOR BORDER GATEWAY PROTOCOL
FEC	FORWARDING EQUIVALENCE CLASS
FIB	FORWARDING INFORMATION BASE
FR	FRAME RELAY
GMPLS	GENERALIZED MULTIPROTOCOL LABEL SWITCHING
GRE	GENERIC ROUTING ENCAPSULATION

HDLC	HIGH DATA LEVEL CONTROL
IGP	INTERIOR GATEWAY PROTOCOL
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
IPSEC	INTERNET PROTOCOL SECURITY
ISP	INTERNET SERVICE PROVIDER
IPX	INTERNET WORK PACKET EXCHANGE
LFIB	LABEL FORWARDING INFORMATION BASE
LIB	LABEL INFORMATION BASE
LSR	LABEL SWITCH ROUTER
LSP	LABEL SWITCHED PATH
MTU	MAXIMUN TRANSMISIÓN UNIT
MPLS TE	MPLS TRAFFIC ENGINEERING
MP-BGP	MULTIPROTOCOL EXTENSIONS FOR BGP-4
MPLS	MULTIPROTOCOL LABEL SWITCHING
OSPF	OPEN SHORTEST PATH FIRST
PSN	PACKET SWITCHED NETWORK
PHP	PENULTIMATE HOP POPPING
PPP	POINT-TO-POINT PROTOCOL
PDU	PROTOCOL DATA UNITS
PE	PROVIDER EDGE ROUTERS
P	PROVIDER ROUTERS
QOS	QUALITY OF SERVICE

RSVP	RESOURCE RESERVATION PROTOCOL
RD	ROUTE DISTINGUISHER
RT	ROUTE TARGET
RIB	ROUTING INFORMATION BASE
RIP	ROUTING INFORMATION PROTOCOL
TDP	TAG DISTRIBUTION PROTOCOL
TTL	TIME TO LIVE
TLV	TIME-LENGH-VALUE
VC	VIRTUAL CIRCUIT
VLAN	VIRTUAL LAN
VPLS	VIRTUAL PRIVATE LAN SERVICE
VPN	VIRTUAL PRIVATE NETWORK
VPWS	VIRTUAL PRIVATE WIRE SERVICE
VRF	VIRTUAL ROUTING AND FORWARDING TABLE

INTRODUCCIÓN

El presente trabajo desarrolla el análisis, diseño y simulación de una red MPLS que nos permita comparar los servicios de MPLS VPN de capa 2 y capa 3. Para cumplir con este objetivo, hemos identificado las consideraciones tecnológicas necesarias, y desarrollar con ello un escenario de simulación acorde a la realidad, con el fin de conservar las características y comportamientos principales y así obtener resultados consistentes de acuerdo a la teoría investigada.

La metodología a utilizar comienza con un análisis teórico de MPLS, donde destacamos las características y ventajas principales de este protocolo, para luego ahondar en próximos capítulos en nuestras aplicaciones de interés que son las de MPLS VPN en capa 2 y capa 3. Adicional al análisis teórico, procedemos finalmente a comprobar la teoría simulando los escenarios establecidos, para lo cual nos apoyaremos en una herramienta llamada Dynamips, que nos permitirá emular ruteadores CISCO los cuales soportan esta tecnología y así cumplir con nuestros objetivos de proyecto.

Finalmente presentamos los resultados obtenidos, conjuntamente con un análisis de los mismos, justificando así la importancia de simular aplicaciones sobre redes MPLS y predecir su comportamiento, previo a la implementación en un portador de datos real de cobertura nacional o internacional.

1 DEFINICIÓN DEL ESCENARIO A DESARROLLAR

1.1 Justificación

Las tecnologías de redes de computadoras, como todas las tecnologías de telecomunicaciones evolucionan cada día para mejorar su soporte en varios servicios y características. Por ejemplo: velocidad, interoperabilidad, calidad y escalabilidad. Hasta hace no mucho tiempo, el pensar en redes integradas era solo un sueño, sin embargo las investigaciones de nuevas tecnologías y protocolos nos ha llevado a un concepto de Redes de Nueva Generación (NGN) donde la integridad es fundamental. MPLS es una tecnología de transporte de datos independiente del protocolo, lo que significa que brinda gran nivel de integración con redes de antigua generación como son: Frame Relay, ATM, etc. MPLS viene consigo con una amplia gama de aplicaciones que brindan soporte dependiendo de las necesidades actuales, entre las cuales podemos mencionar las principales:

- Ingeniería de Tráfico.
- Calidad de Servicio.
- MPLS VPN.

Cada aplicación está enfocada a resolver diferentes problemas o necesidades que pueden ser vistas desde un usuario final (una agencia de una corporación) o también desde una perspectiva global es decir interconexiones de empresas portadoras de datos e Internet a nivel mundial.

La evolución de una empresa portadora de datos (ISP) esta enfocada en ofrecer soporte multiprotocolar a sus clientes (integración) y una alta velocidad de transferencia. MPLS se ha convertido actualmente en el factor común evolutivo de estas empresas a nivel mundial, razón por la cual consideramos es importante entrar en la investigación y desarrollo de esta tecnología en nuestro país.

Una de las aplicaciones principales de MPLS son las redes privadas virtuales (VPNs) las cuales actualmente son el principal medio de interconexión de empresas que tienen dos o más sucursales a nivel regional, nacional o internacional, razón por la cual seleccionamos a esta aplicación como objetivo de estudio para nuestro tema de tesis.

Para analizar esta aplicación MPLS/VPNs se han desarrollado borradores (drafts), papers y estándares, de lo cual encontramos que existe una clasificación por su funcionalidad referente a las capas del modelo OSI, de donde se conocen MPLS/VPN capa 1, capa 2 y capa 3, dentro de esta

clasificación la más desarrollada es MPLS VPN de capa 3 seguida por la de capa 2 cuyos estándares ya han sido desarrollados publicados e implementados por diferentes compañías. Con estos antecedentes hemos decidido simular escenarios y comparar resultados de estas dos tecnologías sobre un prototipo de núcleo (backbone) ISP que se ajuste a nuestro alcance y necesidades sin alejarse de su estructura real.

1.2 Tecnologías Principales de un portador

En la actualidad las redes de comunicaciones a han venido evolucionado en función de los requerimientos de tráfico (Voz, Video, Videoconferencia, etc.), logrando una interacción entre los creadores de protocolos y fabricantes de equipos para suplir estas demandas, por tal motivo revisaremos algunas soluciones tecnológicas que se han venido implementado en las redes de empresas portadoras.

Al hablar de tecnologías de Capa 1 (L1) nos referimos al nivel físico de una red, es decir las características del medio de comunicación, y a la forma en la que se transmite la información (niveles de voltaje, codificación). A continuación presentaremos una tabla en la que listaremos las tecnologías L1.

Tecnologías de Capa 1 (L1) utilizadas por un Portador		
Medios de Comunicación	Alámbrico	Cable par trenzado
		Cable Coaxial
		Tecnologías xDSL
		PLC (Power Line Carrier)
		Fibra Óptica(FFTC,FFTH)
	Inalámbrico	Infrarrojo
		Radio (WI-FI , WIMAX,GSM,GPRS)
		Microonda (LMDS)
		Satélite
Métodos de Transmisión		QPSK
		xQAM
		OFDM
		CDMA,GSM

Figura 1.1 Tecnologías de Capa 1.

Consideramos una tecnología de L2 a los equipos y protocolos aplicables a la capa 2 del modelo OSI (Enlace de Datos).

Tecnologías de Capa 2 (L2)	
Protocolos	IEEE 802.3 (CSMA/CD)
	IEEE 802.5 (token passing)
	FDDI token passing
	IEEE 802.6 MAN DQDB
	VLANs
	ATM Adaptation Layer
	ISDN
	Frame Relay
	PPP
	SMDS
	SDLC

Figura 1.2 Tecnologías de Capa 2.

Las tecnologías L3 comprenden aquellos protocolos y equipos que hacen posible el enrutamiento de los datos a través de redes de origen a destino. De las cuales mencionaremos las más importantes:

Tecnologías de Capa 3 (L3)	
Protocolos	BGP
	OSPF
	EIGRP
	RIP v2

Figura 1.3 Tecnologías de Capa 3.

1.3 Diseño del Escenario de simulación

1.3.1 Modelo de un Portador de Datos Nacional

Una empresa dedicada al servicio de portador de datos, fundamenta su trabajo en su infraestructura física, lógica y operacional. Todos ellos con igual grado de importancia en el correcto funcionamiento de cada uno de estos.

Su infraestructura física da soporte a los requerimientos de acceso que tengan los clientes a nivel nacional o internacional, siendo pieza fundamental tener la mayor cobertura y de la mejor calidad; para así poder disponer de una mejor oferta de servicio con un mismo proveedor. Así

tenemos que la Fibra Óptica, el medio que ofrece mayor ancho de banda y la poca vulnerabilidad ante interferencias de otros medios.

El nivel operativo, corresponde a todo el sistema de gestión de diferentes procesos, como puede ser el monitoreo, cambios en la red, avivación de clientes, etc. Para esto existen estándares que se puede seguir como es el estándar de Gestión de Calidad ISO-9001 y el estándar del Sistema de Gestión de Seguridad de la Información ISO-27001.

El desarrollo lógico o tecnológico venía siendo muy bajo hace unos años, pero con la aparición del Protocolo de Internet IP, se desencadenaron una serie de aplicaciones y sistemas que permiten integrar múltiples servicios en un mismo enlace de red. Este desarrollo compromete a las empresas portadoras a migrar sus tecnologías a nuevos protocolos que ayuden a la eficiencia del uso de sus recursos.

Es así que como parte del desarrollo e incluso la estabilidad de una empresa portadora de datos en el mundo de las telecomunicaciones, va directamente ligado a su evolución tecnológica, por lo cual es muy importante conocer, entender, y probar estas nuevas tecnologías.

A continuación presentamos el modelo que sigue un proceso tecnológico en el tiempo.

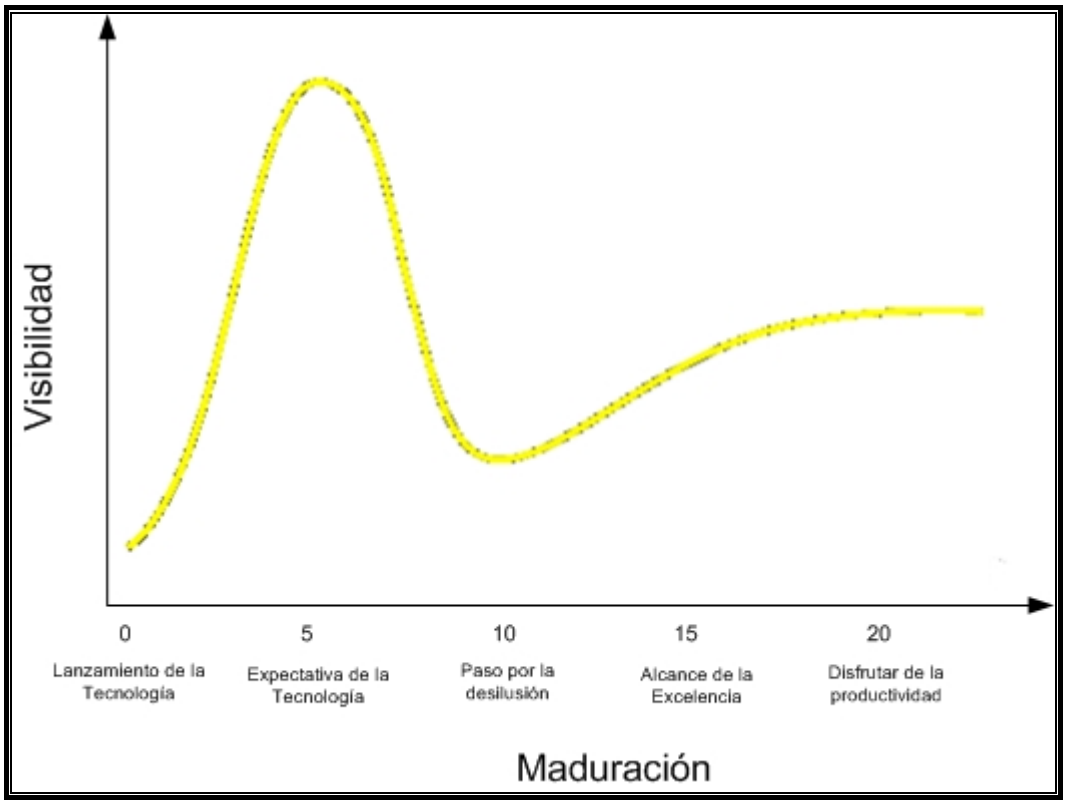


Figura 1.4 Maduración de un proceso tecnológico.

Ninguna empresa de Telecomunicaciones está exenta de saltarse alguno de estos pasos del proceso de evolución de una tecnología si se implanta desde el inicio del proceso, sin embargo, el saber determinar cuando una tecnología está lo suficientemente madura nos indica si está lista para ser implantada en el mercado. Cabe recalcar que esta es una realidad que afecta a cada país de manera independiente ya que como nos muestra la curva, el lanzar la tecnología, no implica que sea recomendable usarla.

Esto es lo que está sucediendo actualmente con el protocolo MPLS, en nuestro país, ya que al pasar por todas estas etapas en diferentes países ha madurado mucho y está lista para ser usada con confianza. Este protocolo lleva sin embargo tiene muchas aplicaciones que pueden estar sujetas a cierto tipo de inmadurez. Las aplicaciones de nuestro interés son las de VPN MPLS, que tienen principalmente consigo L3MPLS VPN, L2MPLS VPN; de estas L3 MPLS VPN ha podido atravesar todas las etapas del proceso y podemos usarla con confianza las cuales actualmente están en la etapa final del proceso. A pesar que L2MPLS VPN no es una tecnología totalmente madura, el mercado de hoy exige que dispongamos de soluciones de este tipo y por este motivo en Ecuador estamos incursionando en el transporte de protocolos de capa 2 sobre MPLS también.

En cuanto a la realidad que se vive en Ecuador, vemos que muchas de las empresas locales líderes, están con miras a evolucionar su equipamiento e infraestructura, con el afán de poder ofrecer a sus clientes este tipo de servicios avanzados.

Una empresa proveedora de Internet y Datos, está siempre ligada a entidades financieras, gubernamentales o militares, las cuales deben tener un servicio activo las 24x7, razón por la cual para implementar una nueva tecnología, debemos desarrollar un ambiente de laboratorio en el que

podamos probar los posibles problemas que puedan suscitarse ya que por contraparte deberíamos implementar la solución sobre equipos en producción, lo cual definitivamente es riesgoso al sistema de seguridad de información.

1.3.2 Consideraciones de diseño para Simulación

Nuestro objetivo es comparar las aplicaciones de los servicios de MPLS VPN de capa 2 y capa 3. Ambos servicios se implementan sobre equipos conocidos como ruteadores o comúnmente llamados equipos de L3. Por lo cual, para poder comparar estos servicios necesitamos únicamente disponer de ruteadores que soporten este tipo de tecnología.

Las consideraciones de capa 1 son mínimas, ya que esto no influye al comportamiento de la aplicación, sino más bien a la velocidad con la cual se va a implementar. Como mencionamos anteriormente, la fibra óptica es el medio que se usa para proveer de estas conexiones entre nuestros equipos de interés, así que podemos considerar que no va a ser una limitante el medio para nuestra simulación

Las consideraciones de capa 2 podrían ser muchas, debido a que existen diversas opciones por todo el mercado de las redes de computadores, pero

la mayoría están presentes como residuo de generaciones pasadas de capa de enlace de datos, MPLS soporta transportar tramas independientes del protocolo de enlace de datos , como lo veremos posteriormente.

Así como la fibra óptica es el medio físico más conocido en la actualidad, el ethernet es quien está perennemente impregnado en el medio de enlace de datos en un sistema de telecomunicaciones, por lo cual va a ser foco de interés en nuestras simulaciones.

Las consideraciones de capa 3 son las más importantes, ya que es aquí donde influye si se puede o no simular una red MPLS, existen en el mercado muchos desarrolladores de la tecnología MPLS. Genéricamente podemos mencionar que necesitamos simular un equipo que soporte el protocolo MPLS y no solo eso, sino que también sus aplicaciones principales de VPN de capa 2 y capa 3. Prácticamente por añadidura, un equipo que soporta MPLS suele tener implementados protocolos que ayudan a su funcionamiento como son el de BGP, OSPF, entre otros.

En el mercado, existen muchos simuladores, en los cuales nos podemos ayudar para desarrollar ambientes de pruebas de tecnologías de red, sin necesidad de ir más allá, podemos dar las características que debería cumplir un simulador ideal:

- Que soporte múltiples protocolos
- Que sea económico
- Que sea eficiente
- Que sea confiable

Como clasificación de los simuladores, podemos mencionar las más genéricas que serían: por su enfoque, y por su interés comercial.

Entre la lista extensa de simuladores, vemos que existe un simulador que cumple con las características ideales para ser usado en la simulación de una red IP/MPLS, debido a que simula ruteadores CISCO, cuyos desarrollos son los más usados a nivel mundial.

1.3.3 Modelo a de un Portador de Datos a simular.

Dado la consideraciones del modelo a simular, podemos concluir que vamos a simular una red que contenga solo equipos de capa 3 del núcleo de la red y similar con los equipos de los clientes. En los casos en que sea necesario la selección de la tecnología de enlace de datos, procederemos a dar preferencia al los enlaces de ethernet que son de principal interés en nuestra simulación.

1.4 Metodología a Utilizar

El desarrollo del proyecto se regirá por las metodologías propias de la ingeniería, de los cuales podemos dividir en los siguientes apartados:

Estudio del Entorno actual: En las primeras secciones analizamos las tecnologías que han venido aplicando los ISP en sus redes y enfocamos los puntos que originan los problemas que han incentivado a los ingenieros al desarrollo de nuevas soluciones.
Segmentaremos el área donde nuestro trabajo esta dirigido y los problemas que aquí se presentan.

Diseño de la solución: En este apartado planteamos un escenario que cumpla con las características del entorno real siguiendo el enfoque a la solución de problemas presentados en redes anteriormente.

Desarrollo: Luego de plantear el escenario efectuaremos un análisis teórico, mostrando el funcionamiento y los factores que facultan a la nueva tecnología a ser tomada como solución.

Simulación: Luego de diseñar un modelo del sistema real efectuaremos este apartado, con la finalidad de comprender el comportamiento del sistema o evaluar nuevas estrategias dentro de los límites impuestos por un cierto criterio o un conjunto de ellos para el funcionamiento del sistema.

Utilizaremos la herramienta dynamips y dynagen para emular ruteador de la serie cisco 7200 que soportan la tecnología estudiada.

Documentación: para que nuestro proyecto sea base para futura implementación, será debidamente documentado desde los planes de configuración, resultados por cada proceso y anexos que permitirán a los seguidores de nuestro análisis, plantear nuevas soluciones.

2. ARQUITECTURA MPLS

2.1 Generalidades MPLS

Multiprotocolo de Conmutación de Etiquetas (Multiprotocol Labe Switching) es una tecnología flexible y escalable que cambia el paradigma de enrutamiento de los paquetes, ahora se basa en etiquetas (labels) logrando mejores velocidades de procesamiento, y valor agregado a la red.

MPLS es una *tecnología flexible y escalable**,*** porque su arquitectura permite combinar los beneficios de equipo y de enrutamiento .Esta arquitectura separa la información de control y datos (Canal de Control y Canal de Datos) logrando dar *valor agregado* a la red con aplicaciones como Calidad de Servicio QoS (Quality of Service), VPNs, Ingeniería de Trafico, Enrutamiento Multicast, Pseudocables y GMPLS.

En este capitulo inicialmente analizaremos el entorno actual con las redes tradicionales y luego presentaremos una descripción funcional de la arquitectura MPLS y sus principales aplicaciones.

Redes Tradicionales

Las redes tradicionales como IP, ATM, Frame Relay han ido evolucionando dependiendo de los requerimientos del tráfico. En las ***redes IP*** la transferencia de los datos se realiza con la prioridad de que lleguen a su destino independiente de los parámetros como el tiempo de alcance, retardos, y ancho de banda. Este tipo de tráfico se conoce como mejor esfuerzo (best effort) donde no se incluyen calidad de servicio ni otros beneficios.

En estas redes se utilizan protocolos de enrutamiento para alcanzar la convergencia. Cada enrutadores recibe paquetes, y determinan el siguiente salto basándose en la dirección IP destino y la tabla de ruteo y envío. Este proceso de determinar el siguiente salto es repetido en cada ruteador como se muestra en la figura 2.1**.**

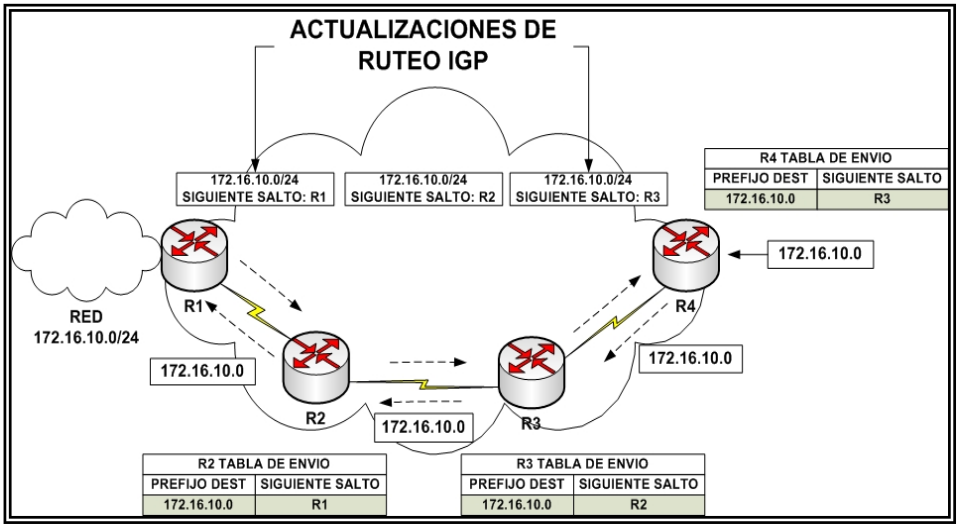


Figura 2.1 Proceso Tradicional de Ruteo.

Las redes ***Frame Relay*** es una red de conmutación de paquetes orientada a conexión, elimina la corrección de errores en los nodos intermedios de la red, delegando este a los extremos, es decir a un nivel superior, logrando mejores velocidades (hasta 2Mbps), fue creado para transmitir datos pero en la actualidad es posible transmitir trafico multimedia, esta tecnología emplea tramas de tamaño variable, que pueden causar retardos de procesamiento en los conmutadores de la red , es posible tener calidad de servicio pero de forma muy rudimentaria sin una norma ni estándar universal aceptado ,cada fabricante resuelve el problema mediante técnicas propias.

Las ***redes ATM*** aparecieron para solucionar las flaquezas de las redes IP, y Frame Relay. ATM tienen cabeceras de tamaño reducido, es orientada a conexión y existen parámetros para aplicar calidad de servicio y también permite tráfico multimedia. Pero los inconvenientes se presentan en el costo de la red, el tráfico a ráfagas y su integración con otras tecnologías.

En conclusión a nuestro análisis en la actualidad encontramos un sin numero de tecnologías para redes WAN, MAN o LAN donde el modelo aplicado es *Best Effort* con necesidades de trafico triple play (voz, dato, video) donde la utilización de tecnologías para satisfacer esta necesidad se ven estancadas en la **interoperabilidad** donde la solución no es viable en ningún aspecto, principalmente el económico.

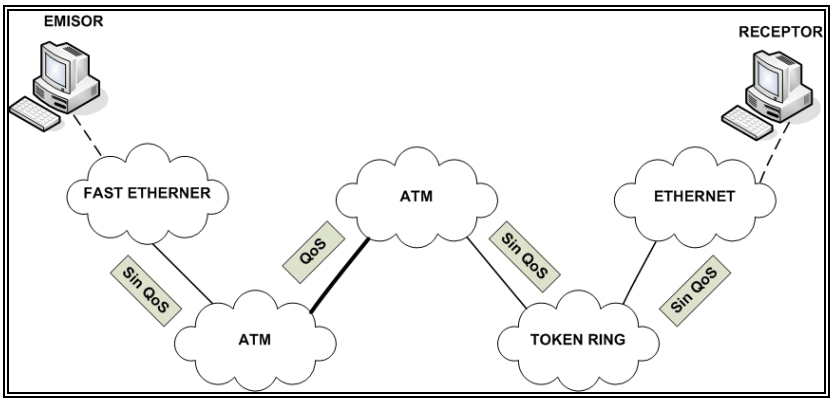


Figura 2.2 Red WAN Tradicional.

En la figura 2.2 podemos observar como el receptor y el emisor se comunican en diferentes protocolos, donde el valor agregado (ancho de banda, calida de servicio) añadidas a la red puede ser aplicada en tramos no en la red global. Frente a esta problemáticas los ISP (Carriers) han venido aplicando soluciones parciales, en el núcleo (backbone) de sus redes y en los últimos años las necesidades de integración de tecnologías como trafico triple play, ingeniería de trafico, ancho de banda, calidad de servicio se centran en una solución que es Multiprotocol Label Switching (MPLS).

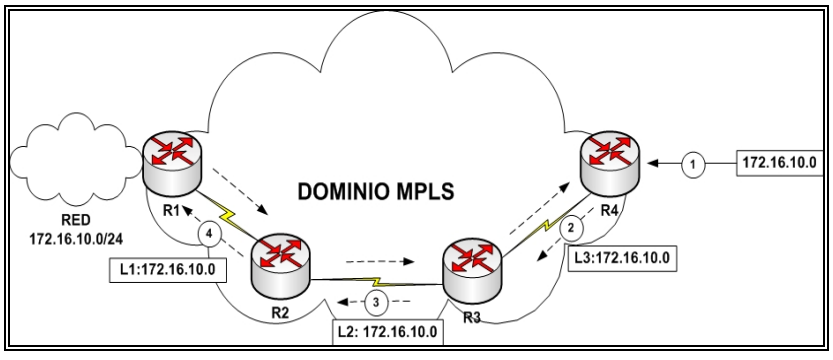


Figura 2.3 Dominio MPLS.

Una vez que conocemos porque MPLS es viable para la solución a los múltiples problemas, ahora conoceremos la terminología necesaria para entender MPLS.

2.2 Terminología MPLS

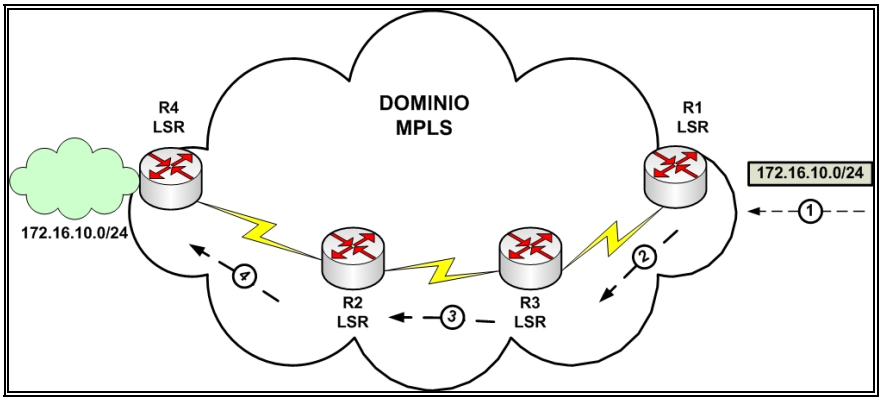


Figura 2.4 Terminología de una red MPLS.

Clase Equivalente de Envió (FEC - Forwarding Equivalence Class). - Es un grupo de paquetes que se envían de una misma manera. Es decir por un mismo camino con el mismo método de envío**.**

Ruteador Conmutador de Etiquetas (LSR - Label Switch Ruteador).- Es un ruteador con la capacidad MPLS. Realiza las funciones de cambiar las etiquetas entrantes por etiquetas salientes. El LSR dependiendo de la posición en el domino MPLS puede realizar varias funciones como

reemplazo, imposición, disposición de etiquetas. Durante la operación con las etiquetas el LSR solamente utiliza la etiqueta del tope de la pila, las demás permanecen intactas. Este dispositivo también es conocido como ruteador P (Proveedor).

Ruteador Conmutador de Etiquetas del Borde (LER - Edge-Label Switch Router).- Son los ruteadores que están ubicados en los bordes del domino MPLS. Son los encargados de insertar o quitar las etiquetas MPLS provenientes de otro dominio generalmente IP, este ruteador mas adelante lo llamaremos ruteador PE (Provider Edge) o (Ruteador Frontera del Proveedor).

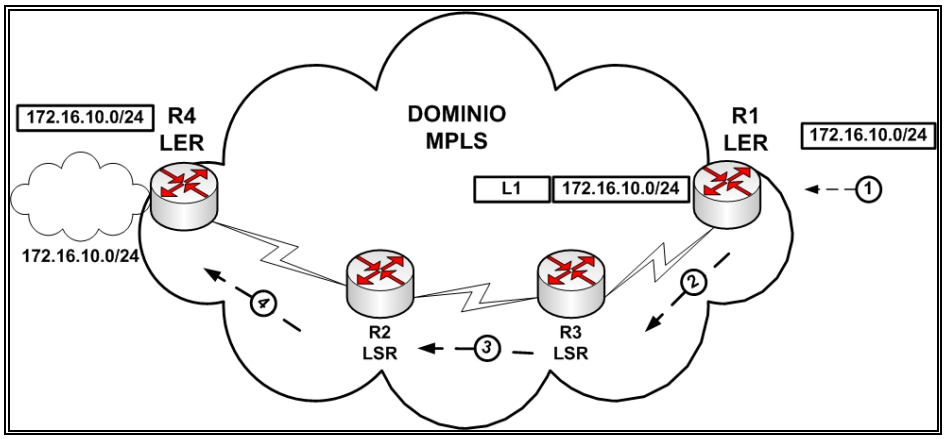


Figura 2.5 Ruteadores LERs y LSRs.

Camino Conmutado de Etiquetas (LSP - Label Switched Path).- Es un camino formado entre ruteadores donde se utilizan etiquetas MPLS. El LSP usualmente se forma según el protocolo de ruteo IGP habilitado en el dominio, este puede ser elegido según las preferencias aplicadas para formar caminos (Ingeniería de Trafico). En la figura C2-4 el camino formado de R4-R3-R2-R1 es un LSP a la red 172.16.10.0/24.

Etiqueta MPLS.- La etiqueta MPLS es la información asignada a un paquete según el prefijo destino. Permitiendo que ahora la información se enrute a su destino de acuerdo a estas etiquetas.

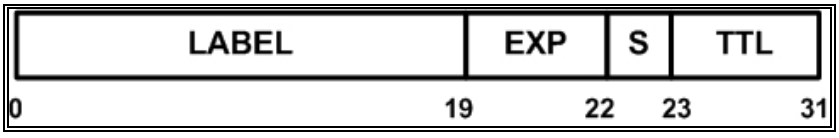


Figura 2.6 Formato de la Etiqueta MPLS.

Esta etiqueta esta formada por las siguientes partes:

- **Label.-20 bits**. Es un identificador de significado local de 20 bits, puede ser asignado por ruteador o por interfaz. Es posible utilizar 2^{20} 1'048.576 etiquetas, dentro de las cuales 16 son reservadas (0-15) mas adelante se conocerán como tipos especiales de etiquetas.

- **EXP 3 bits.-** Campo experimental, es usado en QoS para minimizar los retardos, y tener aplicaciones donde este parámetro es crítico como (VoIP), video, etc.

- **S.- 1 bit.-** Del inglés "*stack"* o pila, sirve para el apilado jerárquico de etiquetas. Cuando S=0 indica que hay mas etiquetas en la pila. Cuando S=1 estamos en el fondo de la jerarquía.

- **TTL.- 8- bits.**-Tiempo de Vida del Campo. Es un identificador similar a IP, su valor es reducido en cada nodo LSR ,puede ser equivalente al del paquete IP , si su valor es 0 y el paquete aún no alcanza su destino el paquete será descartado.

La etiqueta MPLS es insertada entre la cabecera de capa 2 y capa 3 como se muestra en la figura.

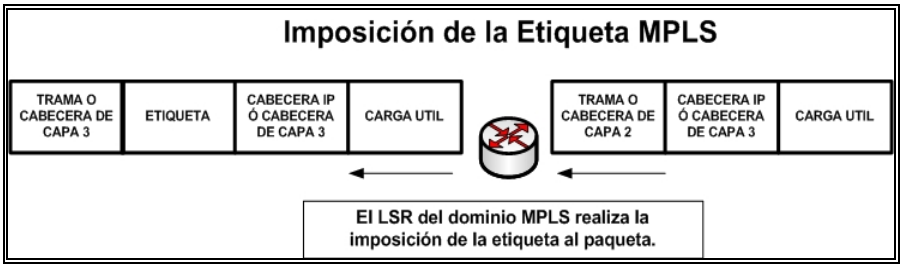


Figura 2.7 Proceso de Imposición de la Etiqueta MPLS.

Pila de Etiquetas.- Una pila de etiquetas es un conjunto ordenado de etiquetas donde cada etiqueta tiene una función específica.

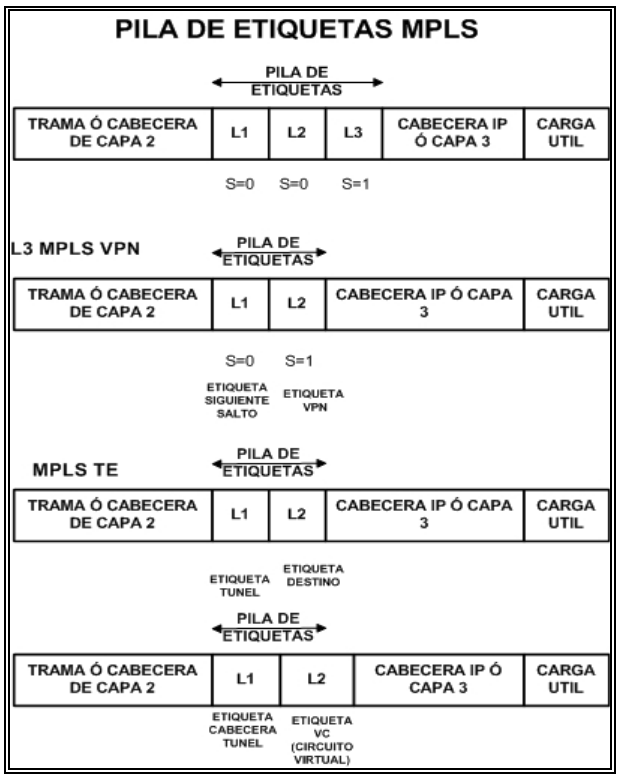


Figura 2.8 Pila de Etiquetas.

La pila de etiquetas es utilizada en varias aplicaciones como: VPNs de Capa 3 (L3 MPLS VPN) donde la segunda etiqueta de la pila indica la etiqueta VPN (esto se vera en el Capitulo 3), Ingeniería de Trafico (MPLS TE) donde el tope de la pila indica el punto final del túnel y la segunda etiqueta identifica el destino y L2 MPLS VPN donde el tope de la pila indica la cabecera del túnel y la segunda etiqueta el Circuito Virtual.

2.3 Tipos Especiales de Etiquetas

Existen diferentes tipos de etiquetas dependiendo de su localización en el dominio MPLS de las cuales mencionamos:

Sin etiqueta (Untagged).- Es una etiqueta usada en MPLS VPN para enviar un paquete del dominio MPLS a un dominio de destino diferente.

Etiqueta Nula implícita (Implicit-null).- Esta etiqueta es asignada y distribuida por un LSR, para indicarle al siguiente salto que la etiqueta debe ser removida de la pila, resultado un paquete sin MPLS. El valor para esta etiqueta es 3 y es usada en las redes MPLS en el ***Penúltimo Salto***.

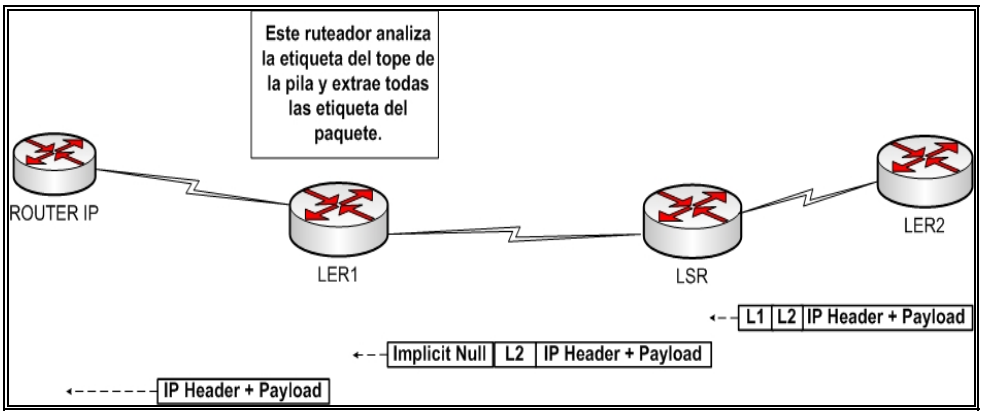


Figura 2.9 Etiqueta Pasiva Implícita.

Etiqueta Nula Explicita (Explicit-null Label).- Es una etiqueta ubicada en el fondo de la pila de etiquetas que nos indica que la operación a realizar es eliminar la etiqueta de la pila y remitir el paquete para que posiblemente sea procesado en base a la cabecera IPv4 o IPv6, su valor puede ser 0 (IPv4) o 2 (Ipv6) .También sirve para conservar el valor del campo experimental (EXP) de la etiqueta de la cima de un paquete entrante. La etiqueta es cambiada con un valor de 0 ó 2 y enviado como un paquete MPLS al próximo-salto. Esta etiqueta es utilizada en la implementación de QoS con MPLS.

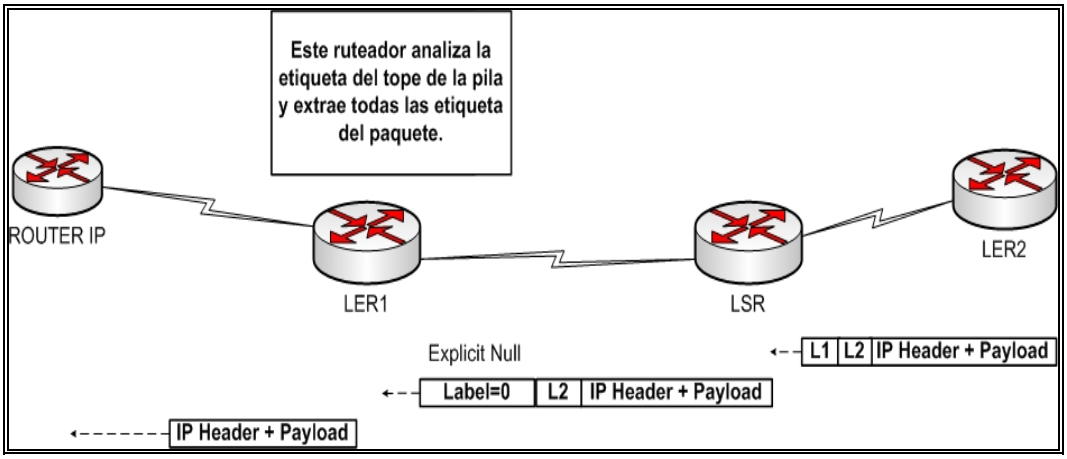


Figura 2.10 Etiqueta Nula explícita.

Etiqueta de Agregación (Aggregate).- Esta etiqueta permite identificar en una tabla la interfaz de salida cuando un paquete MPLS entrante es convertido a un paquete IP (quitando todas las etiquetas de la pila). Esta etiqueta es usada en las aplicaciones MPLS VPN.

2.4 Arquitectura MPLS

La arquitectura MPLS esta dividida en dos bloques principales Canal de Control y Canal de datos, donde cada entidad realiza funciones que hacen sinergia para lograr los beneficios de esta arquitectura.

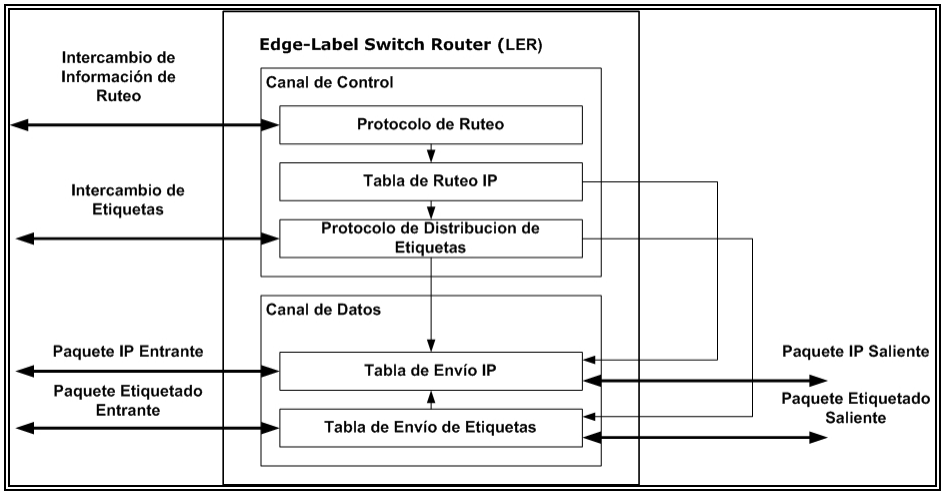


Figura 2.11 Arquitectura MPLS.

Canal de Control.- Realiza funciones relacionadas al manejo de información de capa 3, Protocolo de Enrutamiento, Tabla de Enrutamiento, y Base de Información de Etiquetas (LIB) .Además contiene todas las funciones del protocolo de distribución de etiquetas (LDP) que permite intercambio de etiquetas.

Canal de Datos.- Realiza las funciones relacionadas al envió de paquetes estos pueden ser dirigidos a un dominio MPLS o no MPLS. Utiliza información del canal de control para el envió de paquetes etiquetados.

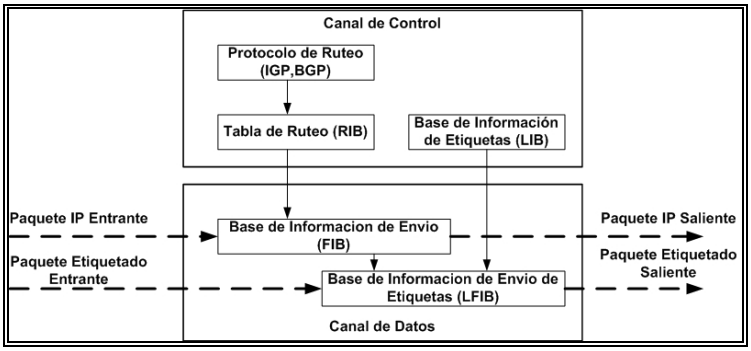


Figura 2.12 Entidades del Canal de Datos y Canal de Control.

Los procesos y funciones de cada canal, originan información que permite publicar o generar tablas que mencionaremos a continuación:

RIB (Tabla de Ruteo IP).- Contiene información originada por el protocolo de enrutamiento (IGP), esta situada en el Canal de Control y muestra información IP – IP.

LIB (Base de Información de Etiquetas).- Esta situada en el Canal de Control y es originada por el protocolo de distribución de Etiquetas (LDP), contiene información del siguiente salto, como la etiqueta de salida de acuerdo a una dirección IP destino.

FIB (Base de Información de Envió).- Esta situada en el canal de datos, y es una imagen de la tabla RIB, mapea las redes destinos y los ruteadores adyacentes.

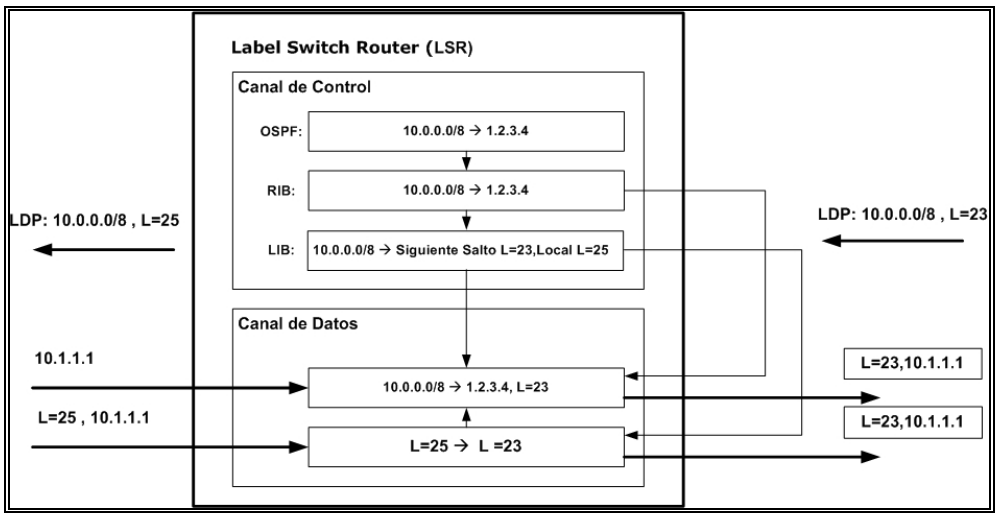


Figura 2.13 Datos del canal de datos y canal de control.

LFIB (Base de Información de Envió de Etiquetas): Esta situada en el canal de datos, utiliza información de la tabla FIB y LIB para generar una tabla de etiquetas entrantes y salientes.

Estas tablas son la base del funcionamiento de la arquitectura, por lo tanto el mantenimiento, actualización y otros procesos deben ser objetivo de estudio. A continuación analizaremos estos procesos y responderemos a las preguntas: *¿Cómo se distribuyen las etiquetas? ¿Cómo se actualizan las tablas?; entre otras preguntas.*

2.5 Descripción funcional de MPLS

Antes de sumergirnos al funcionamiento detallado de esta arquitectura explicaremos cual es el objetivo y funcionamiento de esta tecnología.

Como se menciono anteriormente esta tecnología ya no utiliza las cabeceras de capa de red para el envió de paquetes ahora los paquetes son enviados en base a etiquetas. Estas etiquetas corresponden a direcciones IP o a otros parámetros, como calidad de servicio (QoS), VPNs y etc. Las etiquetas son generadas por los LSRs, en algunos casos por interfaces en otros de forma global (por ruteador) y estas tienen un significado local. A continuación presentamos un ejemplo del trayecto de un paquete IP hasta llegar a su destino IP a través del dominio MPLS.

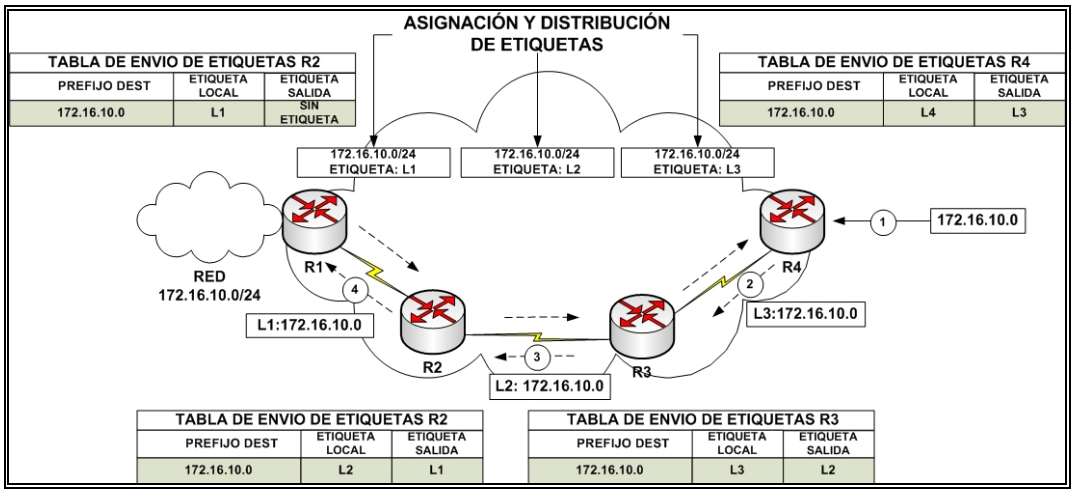


Figura 2.14 Funcionamiento de MPLS.

En la figura 2.12 se muestra, como se envían los datos desde el ruteador R1 a R4 (a través del LSP) la cual se realiza en cuatro pasos:

Paso 1. R4 (también conocido como LER) recibe un paquete de datos para la red 172.16.10.0 e identifica que el camino al destino es el que MPLS ha habilitado. Por consiguiente, R4 remite el paquete para próximo-salto R3 después de aplicar una etiqueta L3 en el paquete y enviándolo a R3 (LSR).

Paso 2. R3 recibe el paquete etiquetado con la etiqueta L3 y la cambia a L2 y lo envía a R2 (LSR).

Paso 3. R2 recibe el paquete etiquetado con la etiqueta L2 y la cambia por L1 y la envía a R1 (LER).

Paso 4. R1 es el ruteador fronterizo entre los dominios IP y MPLS; por consiguiente, R1 quita las etiquetas del paquete y lo envía a la red IP destino 172.16.10.0.

Como podemos apreciar el núcleo o actor principal de esta arquitectura es la etiqueta, la cual de acuerdo a su valor podemos identificar, el prefijo destino,

el protocolo de enrutamiento utilizado y la operación a realizar con el paquete etiquetado que ingresa a un ruteador.

Las operaciones necesarias para el funcionamiento de MPLS son:

- Asignación de etiquetas MPLS (por LSR).
- Establecimiento de la sesión MPLS LDP o TDP.
- Distribución de Etiquetas MPLS. (Usando el protocolo de distribución de etiquetas).

2.5.1 Asignación de Etiquetas.

Este proceso comprende en asignar una etiqueta de significado local a una red IP tomando como criterios el protocolo de red utilizado y el contenido de la tabla RIB del Canal de Control. La tabla RIB se conforma mediante el protocolo IGP aplicado y si este fuera un dominio IP la convergencia estaría lista. Pero este es un dominio MPLS, entonces utilizaremos un proceso similar para alcanzar la convergencia en este dominio. El Protocolo de Distribución de Etiquetas (LDP) es el proceso similar al protocolo IGP en una red IP, es decir nos va a permitir asignar e intercambia las etiquetas entre los LSRs adyacente en el dominio MPLS para luego realizar el establecimiento de la sesión LDP.

2.5.2 Establecimiento de la Sesión LDP

Luego del proceso de asignación de etiquetas, viene el establecimiento de la sesión LDP que consiste en enviar mensajes LDP para que los LSRs vecinos levanten una sesión LDP y así distribuir las etiquetas a sus vecinos directamente conectados y habilitados para MPLS. Esta distribución es realizada usando LDP o TDP, (En este trabajo utilizaremos el protocolo LDP). TDP y LDP funcionan de la misma forma pero no son interoperables. TDP usa el puerto TCP 711 y LDP usa el puerto TCP 646.

Estos mensajes para el establecimiento de la sesión son:

- **Mensajes de descubrimiento (Discovery Messages).-** Este mensaje sirve para anunciar y mantener la presencia de un LSR en la red.
- **Mensajes de Sesión (Session Messages).-** Sirve para establecer, mantener y terminar una sesión entre LSRs.
- **Mensajes Anuncio (Advertisement Messages).-** Es utilizado para crear, cambiar y borrar el mapeo de etiquetas a Clases Equivalentes de Envió (FECs).

- **Mensajes de Notificación (Notificación Messages).-** Son mensajes que proveen información de errores que han sucedido en la sesión LDP.

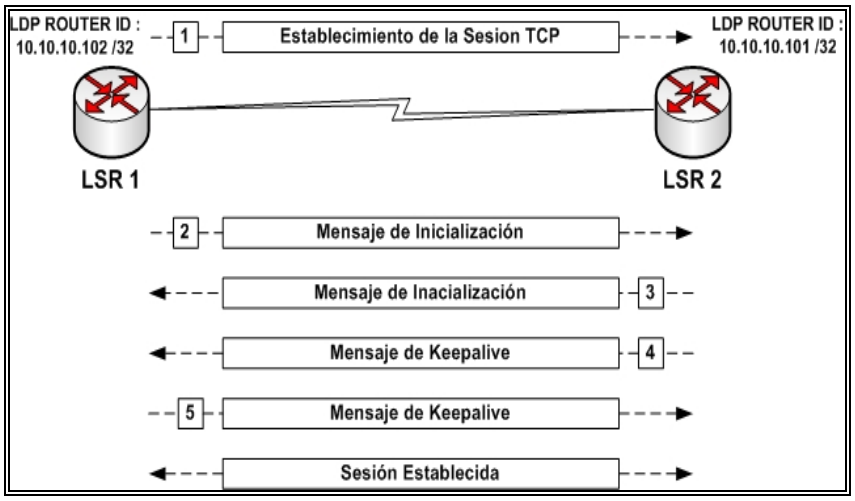


Figura 2.15 Establecimiento de la sesión MPLS.

Los mensajes que se presentan en la figuran son los que se utilizan para el establecimiento de la sesión LDP, el formato que estos mensajes contienen son Tipo, Longitud y Valor (Formato TVL).

Para el establecimiento se siguen los siguientes pasos:

- La sesión LDP es inicializada cuando los LSRs envían mensajes *Hello* periódicos (usando el protocolo UDP multicast 224.0.0.2) a las interfaces con MPLS habilitado. Si el LSR conectado atiende el establecimiento y posee un ID mayor que el vecino este procede a activar una conexión TCP al puerto 646.

- Al activarse la comunicación se envía mensajes que contienen información: como el tiempo de vida de la sesión, el método de distribución de etiquetas, máxima longitud PDU, ID del LDP y otra información que se profundizada en los capítulos siguientes.
- Luego del intercambio de mensajes de inicialización entre los LSRs se puede anunciar que la sesión esta establecida, y se puede proceder al siguiente proceso que es la distribución de las etiquetas a todos los LSRs del dominio MPLS (Distribución de Etiquetas).

2.5.3 Distribución de Etiquetas

Una vez que en el dominio MPLS ya se encuentra funcionando, es decir se asignaron las etiquetas locales a los LSRs de acuerdo a la tabla FIB, y se ha distribuido estas etiquetas a los vecinos directamente conectados. Se procede a la distribución de las etiquetas a todos los LSRs de acuerdo al método de distribución configurado, y así mapear estas etiquetas locales y prefijos destinos a etiquetas del siguiente salto, obteniendo esta información se proceden a guardar en las estructuras LFIB y LIB antes mencionadas.

Los métodos de distribución usados en MPLS son las siguientes:

Demanda con solicitud hacia abajo: Este modo de distribución de etiquetas permite a un LSR pedir explícitamente a un ruteador hacia abajo un mapeo de etiquetas para un prefijo IP específico.

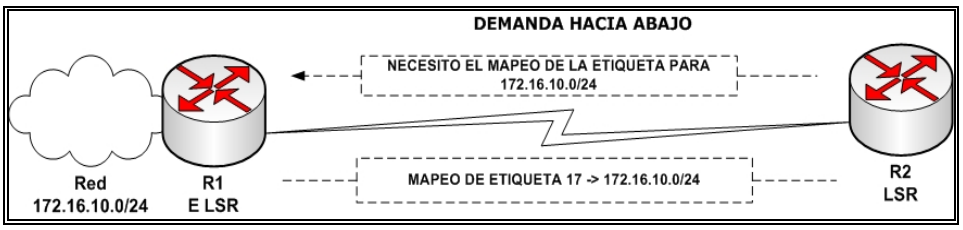


Figura 2.16 Distribución de Etiquetas con demanda hacia abajo.

Demanda sin solicitud hacia abajo: Este modo de distribución permite a un LSR recibir el mapeo de etiquetas de un prefijo hacia abajo si presentar solicitud a esta.

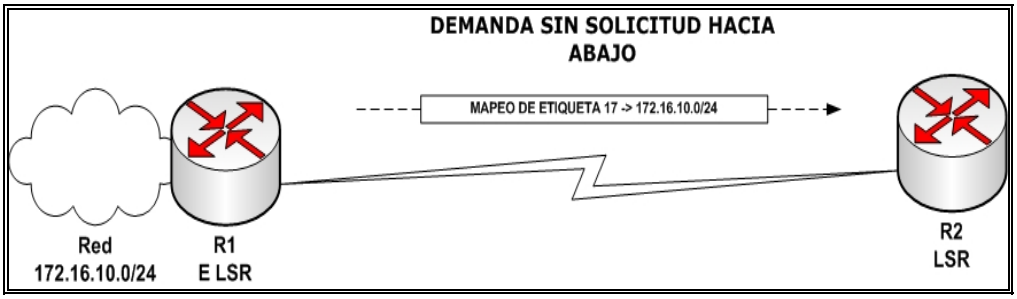


Figura 2.17 Distribución de Etiquetas sin demanda hacia abajo.

Una vez que la distribución se ha realizado, ya podemos conjeturar que el proceso MPLS esta listo y determinar cuales son las aplicaciones que podemos adjudicarle a esta tecnología.

2.6 Aplicaciones de MPLS

Como se menciono previamente, una ventaja clave de la arquitectura MPLS es que posee dos canales separados (Canal de Datos y Canal de Control).
El Canal de datos es usado para el transporte de paquetes, y el Canal de Control es analógico a la información de enrutamiento. Esta capacidad programada en el equipo tanto en interfaces (Canal de Datos) y procesador local (Canal de Control) permite aplicaciones escalables y flexibles.

Las principales aplicaciones MPLS son:

- Ingeniería de tráfico (MPLS TE).
- Calidad de servicio MPLS (QoS).
- Servicio de redes privadas virtuales (VPNs).

A continuación hablaremos de forma superficial de algunas aplicaciones pues no es objetivo de estudio de este trabajo, pero si en los capítulos 3 y 4 profundizamos nuestro estudio con las aplicaciones (L3 MPLS VPNs y L2 MPLS VPNs).

2.6.1 Ingeniería de Tráfico (MPLS TE).

La ingeniería de tráfico MPLS TE, permite adaptar los flujos de tráfico a los recursos físicos de la red. Eliminando la sub-utilización, nodos congestionados y cuellos de botella. La ingeniería de tráfico permite transportar flujos de tráfico de enlaces congestionados a otros menos cargados. La ingeniería de tráfico permite un control de enrutamiento del tráfico basada en restricciones de ruteo. Permite conducir una demanda, reservar recursos, y controlar el paradigma de coexistencia del enrutamiento con la actual topología de una red.

Ingeniería de tráfico es un proceso de enrutamiento de datos balanceando la carga de tráfico en varios enlaces, ruteadores, y conmutadores en una red y es ideal en redes donde existen múltiples caminos paralelos o alternativos habilitados. Las razones de la implementación de la ingeniería de tráfico son las siguientes:

- Congestión en la red.
- Comercio en línea, noticias, eventos deportivos.
- Mejor utilización del ancho de banda disponible.
- Ruteo sobre caminos que no están dañados.
- Ruteo alrededor de enlaces y nodos defectuosos.

- Construcción de nuevos servicios virtuales como el alquiler de líneas.
- Voz sobre IP, y garantía de ancho de banda punto a punto.

La ventaja de la ingeniería de tráfico MPLS es que se puede integrar varias tecnologías por debajo, de manera flexible y con menos costos de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

2.6.2 Calidad de Servicio (QoS)

Esta implementación consiste en un mecanismo de calidad de servicio que habilita la creación de LSPs con garantía de ancho de banda. Como ya se menciono, la cabecera MPLS contiene un campo EXP de 3 bits que se ha redefinido para diferenciar las clases de servicio, por lo que se puede implementar el modelo de servicios diferenciados y proveer a sus clientes calidad de servicio. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros , de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. MPLS se adapta perfectamente a ese modelo, ya que las

etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP.

2.6.3 MPLS VPN

Una red privada virtual (VPN) se construye sobre una infraestructura compartida, y es el soporte de aplicaciones intra/extranet, permite integrar aplicaciones como: multimedia, datos y video sobre infraestructuras de comunicaciones eficaces y rentables.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada, como se menciono anteriormente estas redes presentan barreras a nuevas aplicaciones y desventajas.

Luego, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los ISPs, se ha llegado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y con menores costos de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos. A continuación presentamos un cuadro que ilustra los tipos de VPN tradicionales y las de nueva generación.

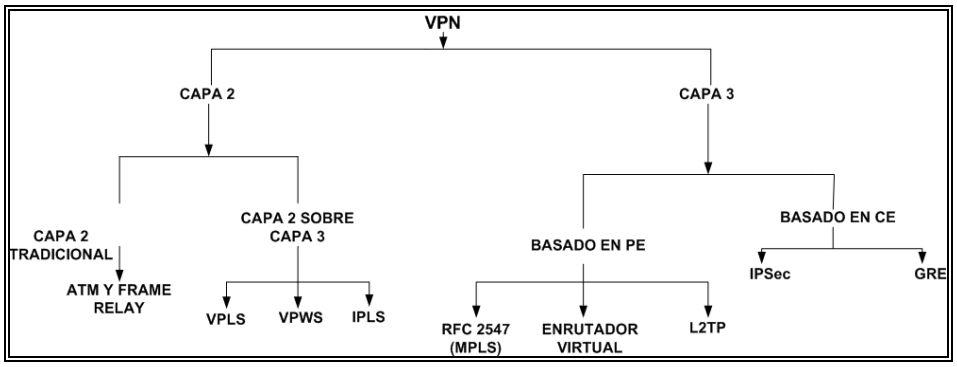


Figura 2.18 Tipos de VPNs Tradicionales y de la Nueva Generación.

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

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

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. IPSec permite crear VPNs a través de redes de distintos ISPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por

aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del ISP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP.

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

- Están basadas en conexiones punto a punto (PVCs o túneles).
- La configuración es manual.
- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.
- Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.
- La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Con una arquitectura MPLS se evaden estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor.

En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Utiliza el mecanismo de intercambio de etiquetas, y no ve el proceso de *routing* IP para el encaminamiento de paquetes. Se pueden aplicar técnicas QoS basadas en la examinación de las etiquetas, pudiendo así reservar ancho de banda, priorizar aplicaciones, y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

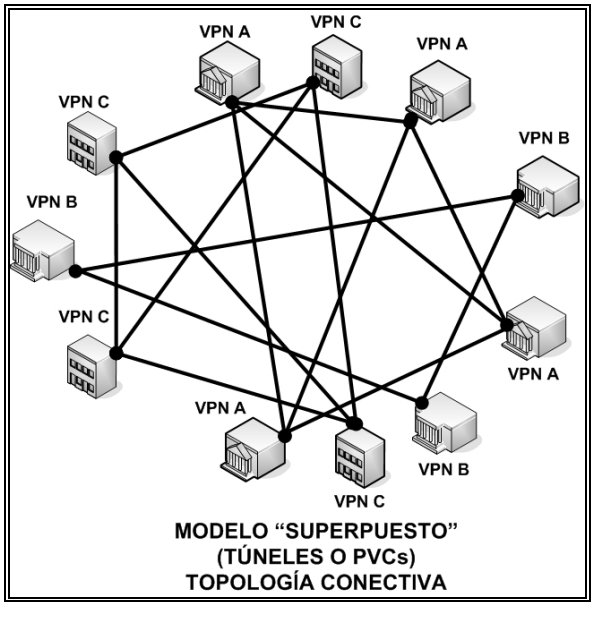


Figura 2.19 Modelo de VPN tradicional.

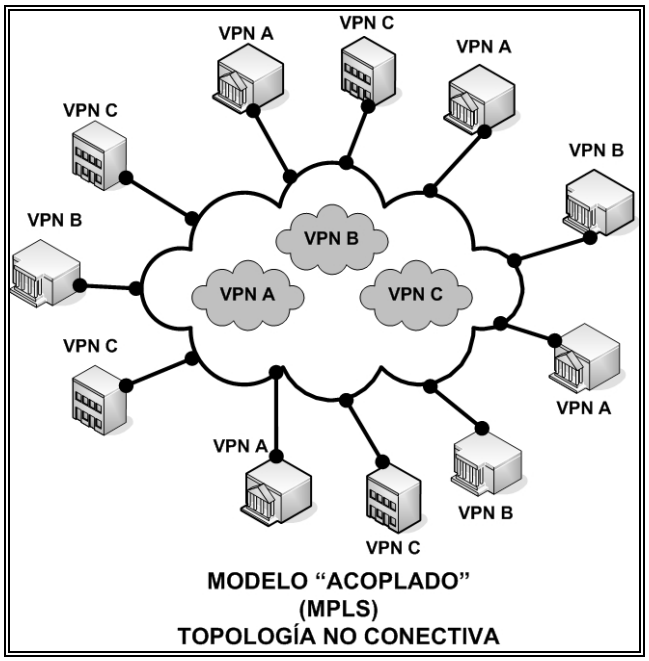


Figura 2.20 Modelo de VPN MPLS.

En las figuras 2.16 y 2.17 se representa una comparación entre los túneles IP convencionales y los "túneles MPLS" (LSPs).

Las ventajas que MPLS ofrece para VPNs son:

- Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).
- Evita la complejidad de los túneles y PVCs.
- La provisión de servicio es sencilla: una nueva conexión afecta a un solo ruteador.

- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.

- Permite aprovechar las posibilidades de Ingeniería de Tráfico para poder garantizar los parámetros críticos (ancho banda, retardo, fluctuación, etc.).

En conclusión una de las aplicaciones mas importantes de MPLS es la de crear VPNs y añadir servicios con valor agregado. Mas delante en el capitulo 3 y 2 analizaremos con mayor énfasis las aplicación L3 MPLS VPNs y L2 MPLS VPNs.

3 L3MPLS VPN

3.1 Introducción

L3 MPLS VPN es una de las aplicaciones más importantes y de mayor despliegue en tecnologías VPN IP. Este capítulo empieza con una apreciación global de la tecnología, luego discute sus ventajas, desventajas y aplicación como servicio.

Muchos clientes VPNs compran servicio de Capa 3 a los ISPs, como GRE (Encapsulation Routing Generic), IPSec y otra tecnología de tunneling que son una alternativa para redes IP pequeñas. Este trabajo no profundiza estas tecnologías por no ser objetivo de estudio pero podemos anunciar que se limitan en su escalabilidad para las redes grandes, es necesario n^2 o n(n-1) enlaces para tener conectividad en malla para n sitios. Mas adelante veremos como la tecnología L3 MPLS VPN vence este problema.

La tecnología L3 MPLS VPN se ubica de acuerdo a la clasificación de las VPNs como se muestra en la siguiente figura:

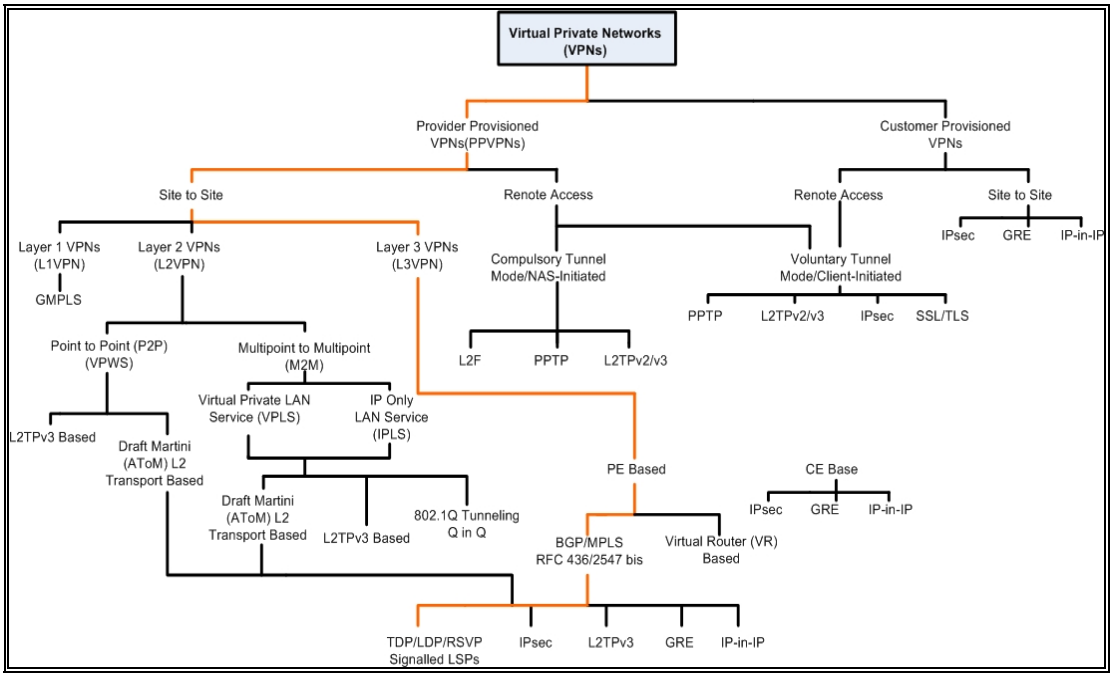


Figura 3.1 Clasificación de VPNs.

L3 MPLS VPN es una VPN provista por el proveedor (PP-VPNs), de Sitio-a-Sitio, Basada en Ruteador de Frontera del Proveedor (PEs ó LERs), y utiliza los protocolos BGP/MPLS y (TDP, LDP o RSVP) para ser implementada.

3.2 Ventajas y Desventajas

Las ventajas y desventajas se proceden a detallar a continuación:

Ventajas de L3MPLS VPN

Algunas de las principales ventajas son:

- L3 MPLS VPNs es una arquitectura escalable, se pueden añadir miles de clientes de un sitio a otro.
- L3 MPLS VPNs puede ser ofrecido como un servicio de administración de las sucursales de una empresa, proveer particiones entre las unidades de negocios y servicios.
- L3 MPLS VPNs permite a una empresa simplificar el ruteo WAN. Los ruteadores clientes (CE) solo publican sus redes a los ruteadores PEs y no al núcleo (backbone) o ruteadores (P).
- L3 MPLS VPNs permiten conectividad de cualquier sitio a cualquier sitio de una empresa, donde podemos añadir calidad de servicio (QoS) para aplicaciones en tiempo real y negocios.
- L3 MPLS VPNs e Ingeniería de Trafico permite a los proveedores de servicios optimizar la utilización del ancho de banda.

Desventajas de L3 MPLS VPN

Algunas de las principales desventajas son:

- L3 MPLS VPNs soporta trafico IP nativo. A pesar de que en teoría debería soportar tráfico como IPX en redes tipo Novell, si un cliente

quiere enviar otros protocolos como IPX, se recomienda aplicar tecnologías como las de tunneling o GRE.

- Algunos proveedores de servicios no soportan trafico IP nativo multicast entre sus sitios en L3 MPLS VPNs. Para superar este inconveniente se puede aplicar el protocolo GRE entre sus clientes.
- En L3 MPLS VPNs los clientes no tienen el control total de sus rutas WAN. Los ruteadores CE no establecen directamente las adyacencias de ruteo, tan solo establecen instancias con los ruteadores PEs.
- L3 MPLS VPNs no establece un proceso de seguridad como Ipsec, pero si el de Frame Relay y ATM. Sin embargo podemos aplicar Ipsec entre los ruteadores PEs.

Ahora que ya sabemos las ventajas y desventajas de L3 MPLS VPNs, es el momento de discutir el funcionamiento de esta tecnología.

3.3 Funcionamiento L3MPLS VPN

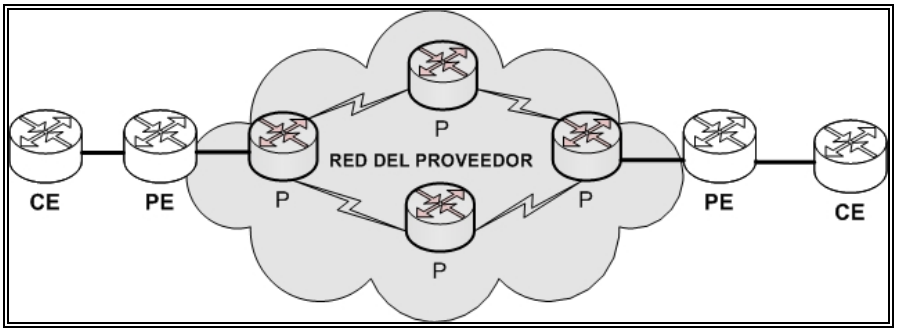


Figura 3.2 Elementos de L3MPLS VPN.

En las redes basadas en **L3MPLS VPNS**, la VPN se construye en la red del proveedor. El proveedor de servicio define las reglas y políticas para la conectividad. Los ruteadores cliente (CE) se conectan a la red del proveedor y envían los paquetes IP hacia el núcleo de la red. La red del proveedor es responsable de mantener y distribuir las rutas de los clientes. Ningún túnel de adyacencia se requiere entre los ruteadores clientes, justificando una de las principales ventajas de L3 MPLS VPN que es la escalabilidad.

Los tres componentes principales para el funcionamiento L3 MPLS VPNs son:

1. Separación de información de ruteo entre VPNs.
2. Distribución de la información de ruteo a los sitios dentro de una VPN.
3. Distribución de Etiquetas.

3.3.1 Separación de información de ruteo entre VPNs

La separación de información de ruteo entre VPNs es un requisito. Si la información de ruteo se mezclara, los paquetes VPN se enviarían a otro VPN. Los ruteadores frontera del proveedor (PEs o LERs) son responsables de mantener las rutas VPN A separadas VPN B. Los dispositivos PE mantienen las rutas de cada VPN en una tabla llamada (VRF) Tabla Virtual de Ruteo y Envió.

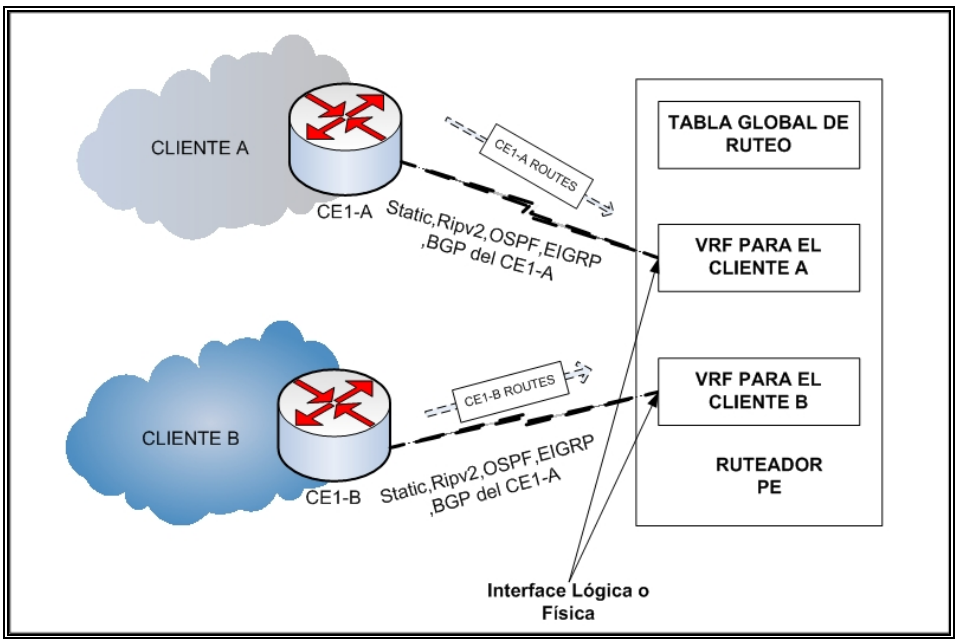


Figura 3.3 Separación de Información de Ruteo.

Cada VRF mantiene rutas del cliente. Todos los ruteadores PEs que conecta al mismo VPN debe tener una VRF para cada VPN, y todas las rutas dentro del VRF deben ser únicas. Permitiendo que las IP puedan reutilizarse entre VPNs. Por ejemplo, VPN A tiene una IP x.x.10.20/16, VPN B también puede tener una IP x.x.10.20/16 en sus tablas de ruteo.

Las rutas son importadas y exportadas de la VRF. Esta crece con el número de rutas dentro de una VPN y sólo se mantiene en los ruteadores PE, y ningún ruteador del núcleo del proveedor tiene conocimiento de la tabla VRF.

Cuando los ruteadores CEs se conectan a los ruteadores PEs, como se muestra en la Figura 3.3, los CEs distribuyen la información de enrutamiento.

El PE local aprende la información CEs y llena la tabla VRF. Después de que todos los PEs en la red aprenden la información de los CE, ellos necesitan comunicarse con otros para intercambiar rutas para que los paquetes puedan enviarse en la VPN.

3.3.2 Distribución de la información de ruteo a los sitios dentro de una VPN

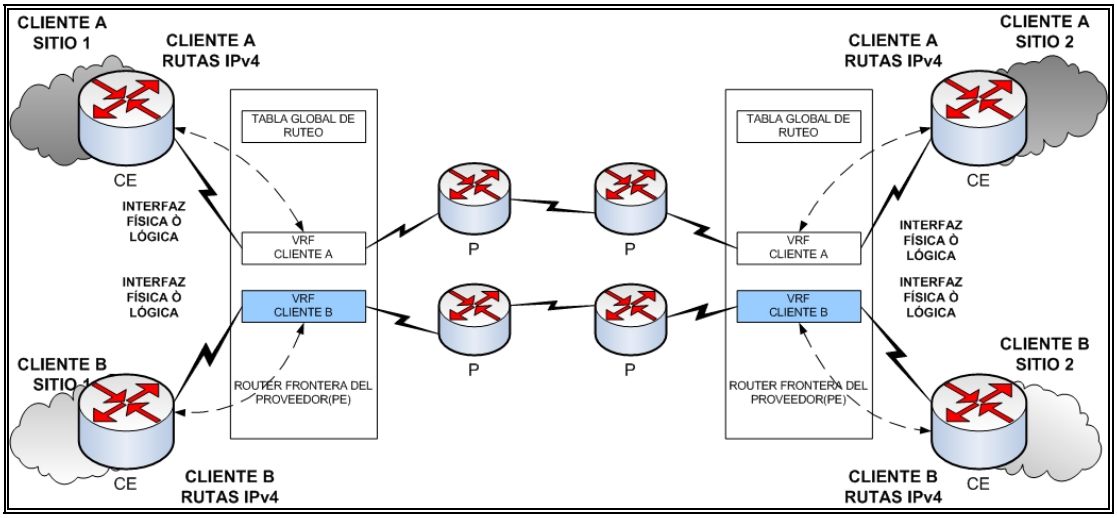


Figura 3.4 Distribución de información de ruteo.

Como se menciono antes, después de que los ruteadores PEs aprenden la información local de los CEs a través de los protocolos de enrutamiento dinámicos o a través de la configuración estática, ellos necesitan distribuir la información enrutamiento a otros PEs en la red. Para esta distribución se requieren dos cosas:

- Un plan central de direccionamiento.
- Un protocolo de distribución entre PEs.

El primer problema puede resolverse creando un esquema de direccionamiento que hace que las direcciones VPN sean únicas fijando

una dirección VPN IP por un Distinguidor de Ruta (RD) llamado identificador VPN mas adelante se hablaremos en mayor detalle.

- VPNv4 = RD + VPN IPv4

El protocolo usado para distribuir de información de ruteo es el Multi-protocolo BGP (MP-BGP), que es una extensión de BGP para llevar VPNv4 como parte de los atributos de capa de red. El PE recibe actualizaciones BGP, los procesa, y llena tabla VRF con las rutas remotas. Para recibir las actualizaciones, el PEs debe converger entre sí o debe converger con un ruteador reflector.

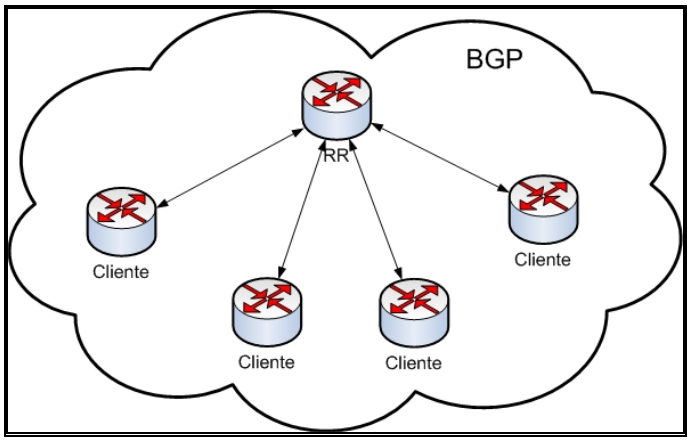


Figura 3.5 Ruteadores Reflectores.

Un ruteador reflector (Router Reflector) es un dispositivo especializado que ayuda a la escalabilidad, y tiempos de convergencia BGP, para la distribución de información de asignación de ruta a los ruteadores PEs.

Las etiquetas MPLS también son distribuidas junto con las direcciones VPNv4. Los ruteadores PEs identifican un prefijo VPN buscando la etiqueta asociada y los paquetes enviados.

3.3.3 Distribución de Etiquetas

Un protocolo de distribución de etiqueta, LDP (Label Distribution Protocol) o RSVP (Resource Reservation Protocol), se necesita para la convergencia de los PEs y formar LSP entre PEs proveyendo un camino para enviar los paquetes VPNs. Los LSP se forman con la primera etiqueta de la pila.

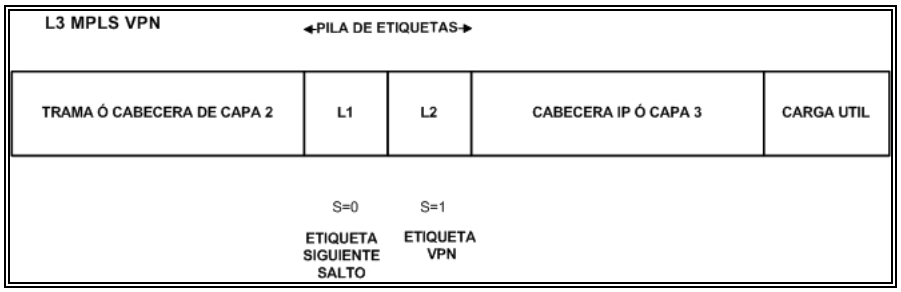


Figura 3.6 Formato de paquete para formar un LSP.

Los paquetes VPN etiquetados se envían hacia al LSP que se han fijado entre los ruteadores PE.

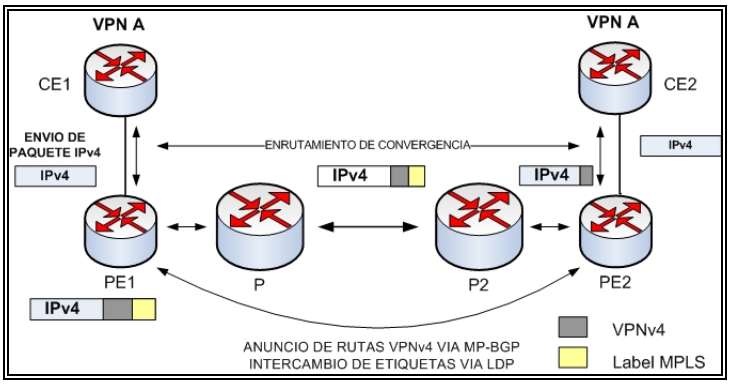


Figura 3.7 Flujo de paquetes en la red.

En la Figura 3.7 el ruteador CE1 envía un paquete a otro CE en su VPN, el paquete se envía hacia el ruteador PE1. Cuando PE1 recibe el paquete, sabe la VPN del paquete, e impone la etiqueta VPN (VPNv4). El PE1 debe ahora imponer una etiqueta MPLS y enviar los paquetes VPN al LSP hacia el centro de la red. Es así, como el ruteador PE1 impone dos etiquetas (una etiqueta VPN y una etiqueta MPLS. Los ruteadores (P) envían los paquetes hacia el destino PE2 basados en la etiqueta extrema (MPLS). En el ruteador del penúltimo salto (P2) es donde la etiqueta MPLS es retirada y es enviado el paquete VPN al destino PE2. Esto se llama el penúltimo salto. El destino PE busca la etiqueta VPN, la quita, y envía los paquetes IP al CE2.

3.3.4 Distinción de clientes con RD

Un RD (Route Distinguisher) es un identificador de 64-bits que es antepuesto a la dirección IP del cliente que es de 32-bits. Así, un único RD

se configura por VRF en un ruteador PE. La dirección resultante que es de 96-bits, se llama dirección VPN versión 4 (VPNv4).

El formato de un RD como se muestra en Figura puede ser de dos formatos. Si el proveedor no tiene un número de AS BGP, el formato puede usar la dirección IP, y, si el proveedor tiene un número de AS, este puede usarse. La figure muestra el mismo prefijo IP, 172.16.10.0/24, recibidos de dos clientes diferentes, pero de diferente valor RD, 1:100:1 y 1:101 en el ruteador PE.

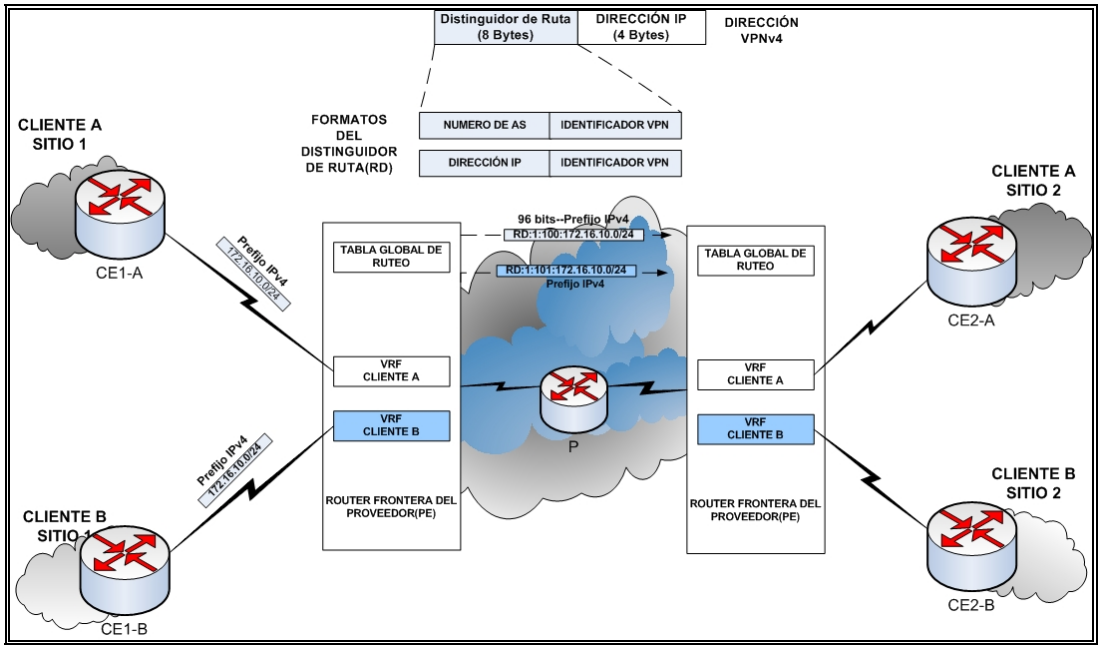


Figura 3.8 El Funcionamiento de RD en MPLS VPN.

3.3.5 Control de ruta objetivo con RT

Cada ruteador PE defina un valor numérico de 64 bits, llamado Ruta Objetivo o RT (Route Target) por sus siglas en inglés, asociado con las rutas que exporta a los puertos BGP. Para que una nueva ruta sea aceptada el valor de su ruta objetivo de salida (exportación) debe de coincidir con el valor de entrada (importación) del dispositivo de entrada. Los objetivos de ruta son distribuidos por las actualizaciones BGP.

La interacción de los valores RT y RD en el dominio MPLS VPN como las actualizaciones son convertidas a una actualización de MP-BGP como se muestra en Figura.

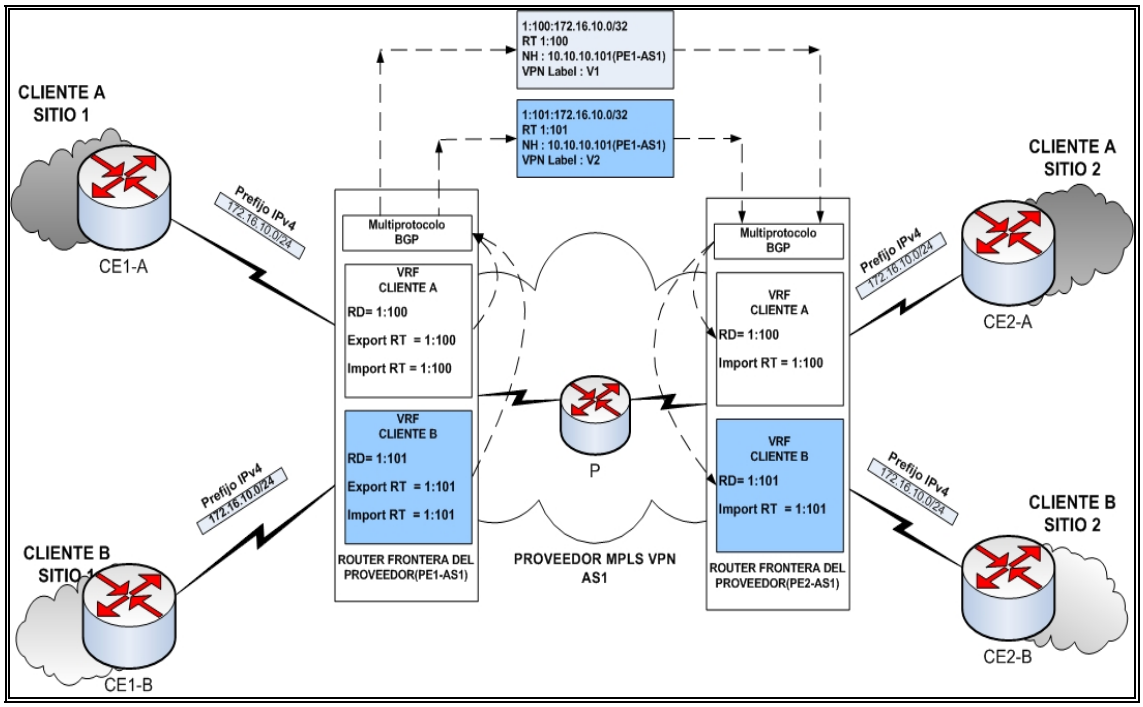


Figura 3.9 RT y Funcionamiento de RD en un MPLS VPN.

3.4 Arquitectura de L3MPLS VPN

La arquitectura de L3MPLS VPN consta de dos planos o canales de comunicación sobre los cuales se intercambia información necesaria para levantar el servicio de VPN sobre una red MPLS. La ventaja de distinguir estos dos planos, es que podemos diferenciar información necesaria para establecer los canales de comunicación como por ejemplo la información de ruteo o de intercambio de etiquetas para un LSP y el canal por el cual van a pasar simplemente los paquetes con sus respectivas cabeceras y etiquetas y simplemente se llevará a cabo el reenvío de paquetes o intercambio de etiquetas. Para ver mejor esta funcionalidad de las VPNs sobre MPLS vamos a analizar cada uno de estos planos de comunicación orientados al intercambio de información de una L3MPLS VPN.

3.4.1 Plano de Control en L3MPLS VPN

La administración de control se encarga de toda la información de enrutamiento de Capa 3 y los procesos como el intercambio de información de convergencia para un prefijo IP específico además de la asignación y distribución de etiquetas usando LDP.

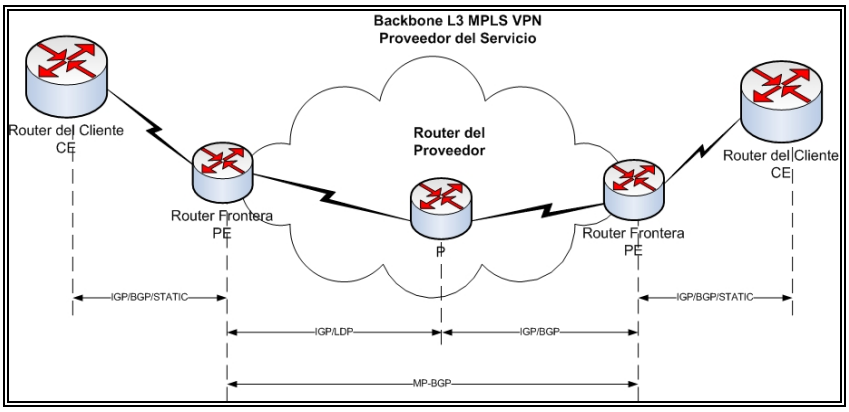


Figura 3.10 Interacciones del plano de Control en L3 MPLS VPN.

Los siguientes pasos explican el funcionamiento de la administración de control MPLS VPN. Los pasos hacen referencia a la figura:

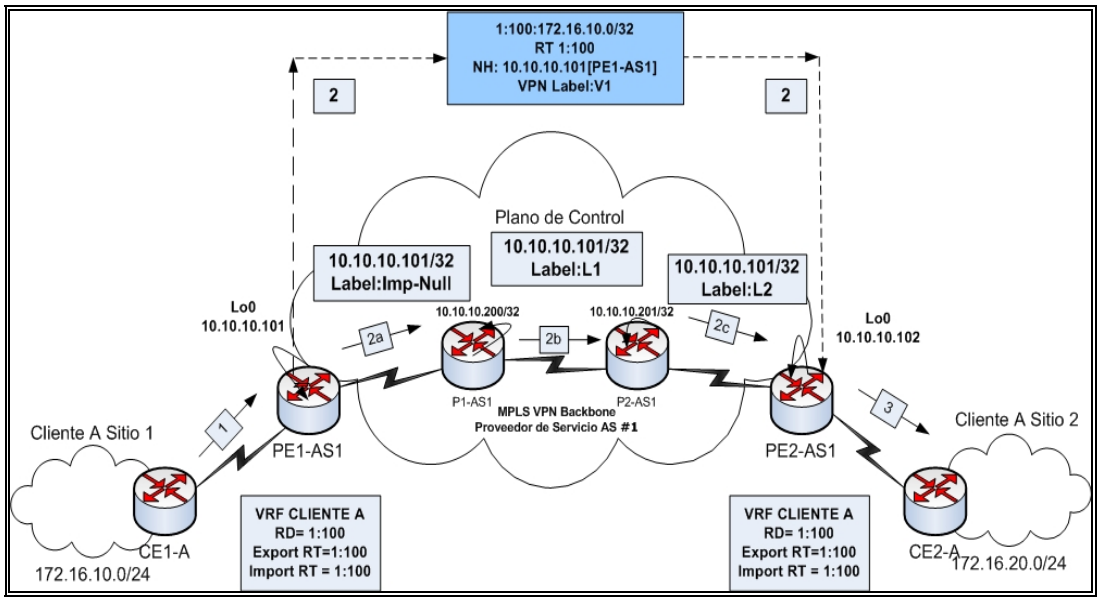


Figura 3.11 Flujo de información del canal de control.

Paso 1. Las actualizaciones IPv4 172.16.10.0 son recibidas por PE1-AS1.

Paso 2. PE1-AS1 acepta y transforma la ruta IPv4, 172.16.10.0/24, a una ruta VPNv4 asignando un RD 1:100, S0/0, y RT 1:100 basada en la configuración VRF PE1-AS1. Asigna una etiqueta V1 a la actualización 172.16.10.0/24 y reescribir el atributo del próximo-brinco a la loopback0 del PE1-AS1 con dirección IP 10.10.10.101. La loopback 10.10.10.101 PE1-AS1 es alcanzable vía OSPF y LDP.

2a: En Figura, LSR PE2-AS1 pide una etiqueta para el 10.10.10.101/32 y usa el LDP a su vecino río abajo, LSR P2-AS1. P2-AS1 pide una etiqueta para el 10.10.10.101/32 y usa el LDP río abajo LSR P1-AS1. P1-AS1, a su vez, las demanda una etiqueta para la 10.10.10.101/32 y usa el LDP río abajo, El LSR PE1-AS1 asigna una etiqueta de implícito-nulo a 10.10.10.101/32, modifica la entrada en de la LFIB y lo envía a P1-AS1 usando una contestación LDP.

2b: P1-AS1 usa la etiqueta implícito-nula recibida de PE1-AS1 como su valor de etiqueta de salida, asignando una etiqueta (L1) para 10.10.10.101/32, y modifica la LFIB para 10.10.10.101/32. P1-AS1 envía este valor de la etiqueta a P2-AS1 vía LDP.

2c: P2-AS1 usa la etiqueta (L1) recibió de P1-AS1 como su valor de la etiqueta de salida, asignando una etiqueta (L2) para 10.10.10.101/32, y modifica la LFIB para 10.10.10.101/32. P2-AS1 envía este valor de la etiqueta a PE2-AS1 vía una contestación LDP.

Paso 3. PE2-AS1 tiene la VRF configurada para aceptar las rutas con RT 1:100 y por consiguiente traduce la actualización VPNv4 a IPv4 e inserta la ruta en la VRF para el Cliente A. Propaga esta ruta entonces al CE2-A.

Tabla 3.1 Flujo de información del canal de control.

3.4.2 Plano de Datos en L3MPLS VPN

El Plano de datos realiza las funciones que relacionan al envió de las dos etiquetadas (IGP, VPNv4) así como los paquetes IP al próximo brinco hacia una red destino. Esto involucra el uso de la pila de etiquetas en que la etiqueta de la cima de la pila es la etiqueta asignada para la salida del ruteador PE a la dirección del próximo-brinco, y la segunda etiqueta en la pila es la etiqueta VPN.

La segunda etiqueta en la pila apunta hacia una interfaz saliente siempre que el ruteador CE sea el próximo brinco de la ruta VPN. La segunda etiqueta en la pila apunta a la tabla VRF para agregar una ruta VPN, la ruta VPN apunta a una interfaz nula, y las rutas las interfaces VPN directamente conectadas.

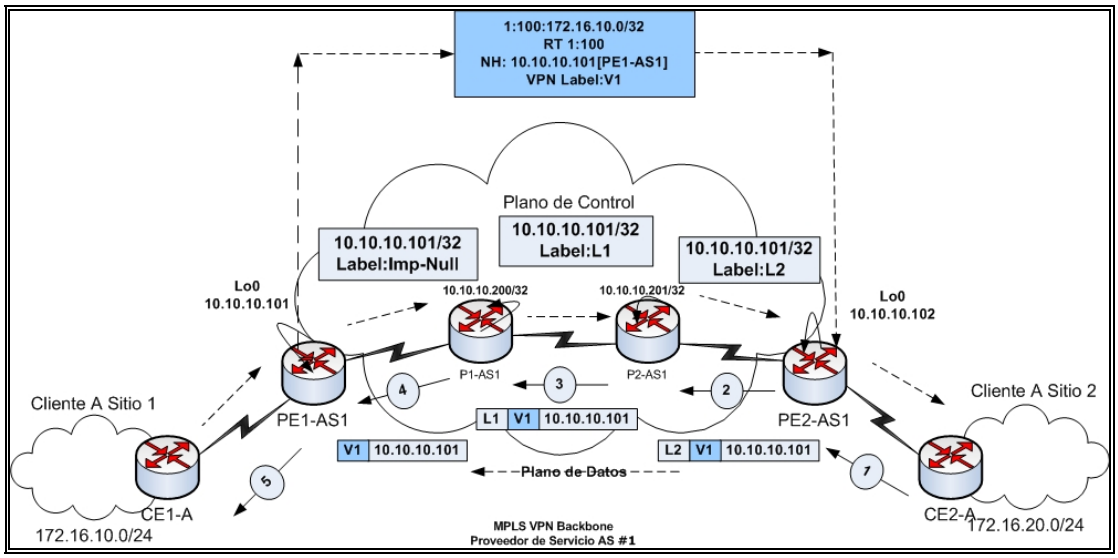


Figura 3.12 Funcionamiento del plano de datos.

Cuando el datos se remite a un prefijo específico que pertenece a una VPN por el núcleo MPLS-activado, la etiqueta de la cima en la pila es la única que cambia cuando atraviesa el núcleo. La etiqueta VPN se guarda intacta y sólo se remueve en los ruteadores PEs. El prefijo resultante es asociado con una interfaz saliente que pertenece a un VRF específico en el ruteador dependiendo del valor de la etiqueta VPN. A continuación tenemos los pasos que explican el funcionamiento de la administración de datos en L3 MPLS VPN:

Paso 1. CE2-A origina un paquete de datos con la dirección fuente 172.16.20.1 y destino 172.16.10.1.

Paso 2. PE2-AS1 recibe el paquete de los datos y añade la etiqueta VPN

V1 y la etiquetan LDP L2 y envía el paquete a P2-AS1.

Paso 3. P2-AS1 recibe el paquete de los datos destinado a 172.16.10.1 y cambia la etiqueta LDP L2 con L1.

Paso 4. P1-AS1 recibe el paquete de los datos destinado a 172.16.10.1 y saca la etiqueta de la cima porque recibe una etiqueta implícito-nula para 10.10.10.101/32 PE1-AS1. El paquete etiquetado resultando (con la VPN V1) se remite a PE1-AS1.

Paso 5. PE1-AS1 saca la etiqueta VPN y envía el paquete de los datos a CE1-A donde se localiza la red 172.16.10.0.

Tabla 3.2 Funcionamiento del canal de datos.

3.5 Servicios de L3MPLS VPN

Un servicio L3 MPLS VPN es una opción atractiva porque provee una capacidad de malla y gran ancho de banda en una WAN, a bajo costo.

A continuación se mencionan las aplicaciones más comunes de L3 MPLS VPN:

- Ingeniería de Tráfico y Servicios diferenciados por QoS.
- Acceso a Internet.
- Construcción de servicios de Extranet.
- Acceso Remoto.

- Servicios de Valor agregado como Telefonía IP, Video Conferencias, Telepresencia y demás servicios que demanden conectividad todos contra todos y gran ancho de banda.

Futuros Servicios de L3 MPLS VPN.

La idea de un solo plano de envió y los diferentes planos de control dan a esta tecnología su fortaleza. De esta idea, se pueden inventarse nuevos planos de control para proporcionar nuevos servicios.

Etiqueta de conmutación multicast (Label-Switched Multicast).

Una idea que se discute en IETF en estos momentos es la habilidad de tener conmutación de etiquetas punto-a-multipunto. Proporcionando las garantías de ancho de banda multicast para servicios como video, televisión, y otras aplicaciones.

Encriptación dinámica VPN.

Como se menciono anteriormente L3 MPLS VPNs proporcionan conectividad de malla que es excelente para construir IP VPNs. Nosotros también hemos visto MPLS VPNs proporcionar una separación de tráfico de cliente A al cliente B. Sin embargo, L3 MPLS VPNs no encripta el tráfico. Para algunas aplicaciones como en la banca o cuando el tráfico es el transmitido encima de la red pública, la encriptación es necesaria.

Encriptación dinámica VPN proporcionan la habilidad de encriptar cualquier tráfico entre CEs. La información de seguridad se configura estáticamente o por el intercambió vía nuevas extensiones BGP

Servicios basados en el contenido.

Otros tipos de servicios VPN incluyen los servicios basados en el contenido. Cada VPN puede representar un servicio y los subscriptores son los miembros de esta VPN.

Redes adaptables para la Integración de Voz y Video.

MPLS TE permite la creación de túneles TE. RSVP también es un protocolo excelente para el control de admisión por QoS. Para VoIP y video.

4 L2MPLS VPN

4.1 Introducción:

Las Redes Privadas Virtuales (VPN) surgen de la necesidad de las empresas con múltiples sedes, centros de producción, logística, etc., de estar permanentemente en contacto y compartir todos los recursos de su propia red, independientemente de la ubicación geográfica de cada uno de los centros o sedes, con total seguridad y máxima escalabilidad a unos costes razonables.

Según estimaciones, los ingresos por servicios VPN a nivel mundial pasarán de los 18.000 millones de dólares en 2003, a más de 30.000 millones de dólares en 2008. Este crecimiento vendrá condicionado, fundamentalmente, por la complejidad inherente al despliegue de VPN a escala corporativa, lo que lleva a las empresas a contratar a terceros este tipo de servicios.

Las implementaciones más conocidas y que actualmente usamos son:

- L3 túneles (IPSec, GRE)
- L3 MPLS (“Multiprotocol Label Switching”)

Estas tecnologías no hacen escalables ni eficientes a los servicios corporativos actuales, ya que el protocolo de enrutamiento que se manejen entre las agencias siempre depende del proveedor. Para poder manejar las políticas de enrutamiento que involucra ventajas como: control del ancho de banda, control de fallas y protocolos dinámicos es necesario utilizar otra tecnología más eficiente.

4.2 Objetivos de L2MPLS VPN

Dar al cliente el control total de sus tecnologías en L3, lo que involucra principalmente que toda implementación IP que deseen realizar, va a ser transparente para el proveedor y totalmente confiable para el cliente.

L2 MPLS VPN o (AToM) Cualquier transporte sobre MPLS (Any Transport Over MPLS), nació con el objetivo de unificar los protocolos de L2 existentes (ATM, FR, PPP, HDLC) en uno solo, un proveedor ISP que desee prestar estos servicios sobre MPLS lo podrá hacer sin ningún problema y no va a tener limitantes de vender este tipo de servicios dependiendo de la tecnología que use su cliente y menos aún manejar redes separadas para

satisfacer las necesidades de sus clientes. Incluso sus clientes pueden manejar tecnologías diferentes de L2 entre sus sucursales y L2 MPLS VPN lo hace transparente para ellos sin preocuparse por las diferencias entre los enlaces.

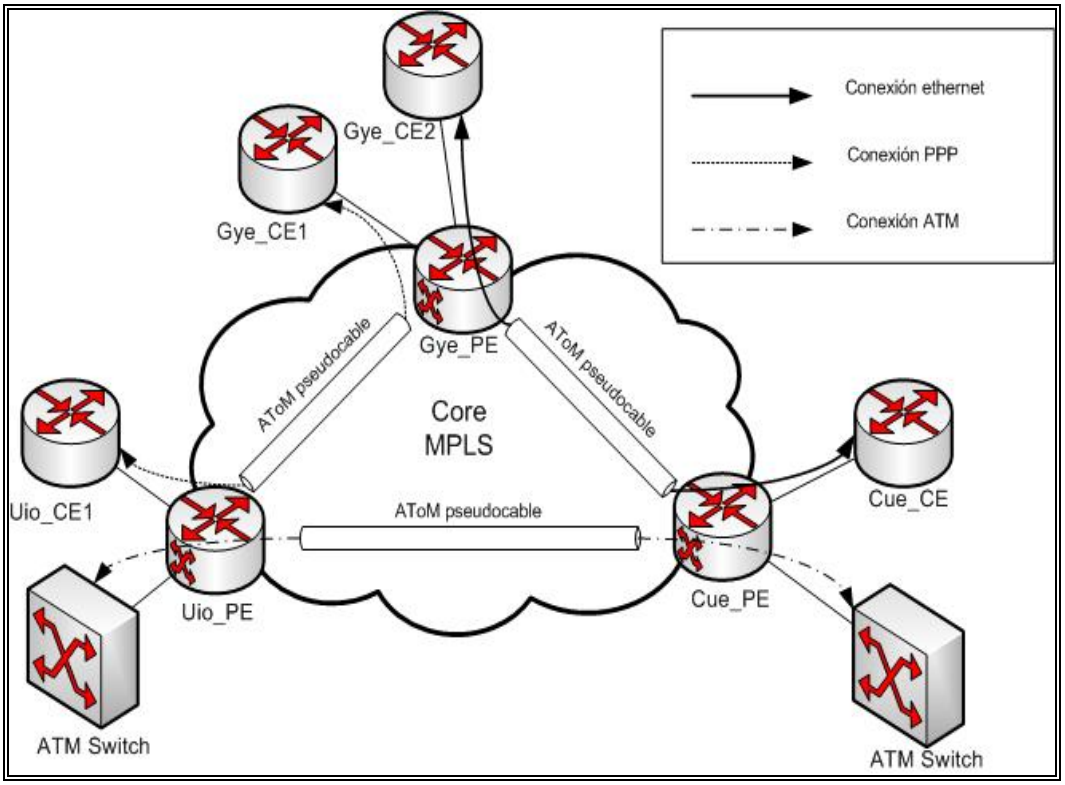


Figura 4.1 Protocolos de capa 2 sobre pseudocables AToM.

4.3 Ventajas y desventajas

Las ventajas y desventajas se proceden a detallar a continuación:

Ventajas de VPNs de capa 2 con AToM

Algunas de las principales ventajas para el ISP son:

- La implementación de VPNs sobre AToM se basa en la tecnología MPLS, lo cual le permite trabajar sobre un núcleo (backbone) MPLS. También puede trabajar sobre Túneles GRE (Generic Routing Encapsulation) y sobre un núcleo (backbone) IP, aunque no es muy común esta implementación.
- AToM permite la integración de los servicios en producción de un ISP con una red MPLS, lo que le permite a una empresa de Servicios Portadores ahorrar costos operacionales mientras mantiene y mejora los servicios de IP y MPLS que brinde.
- AToM permite integrar múltiples tecnologías de capa 2 sobre el mismo núcleo (backbone) MPLS dando así flexibilidad a los clientes de manejar su propia tecnología y recibir los mismos beneficios de VPNs sobre MPLS.
- Dado que la implementación de L2 VPNs sobre AToM trabaja sobre el protocolo MPLS, permite al proveedor dar de una alta disponibilidad y protección de tráfico con aplicaciones de MPLS como lo son Ingeniería de Tráfico (MPLS-TE) y rápido re-ruteo (MPLS-TE-fast-reroute) sobre MPLS.

Algunas de las principales ventajas para las empresas son:

- L2 MPLS puede ser usado para transportar tráfico no IP como IPX (Internetwork Packet Exchange) entre los diferentes sitios de las empresas.
- Las empresas que contraten servicios de L2 MPLS VPN tienen control total de su enrutamiento cuando usan AToM L2 MPLS VPN ya que los PEs (extremos) del proveedor no participan en el proceso de enrutamiento en lo absoluto a diferencia de L3 MPLS VPNs donde el proveedor configura un ruteo virtual entre los sitios involucrados.
- MPLS basado en pseudocables puede ser usado para proveer de tanto VPWS (Virtual Private Wire Service) y VPLS (Virtual Private LAN Service) ya que el LDP para señalizar los pseudocables es usado en ambas tecnologías.

Desventajas de VPNs de capa 2 con AToM

Algunas de las principales desventajas son:

- Es una tecnología relativamente nueva y como tal aún está propensa a fallos y mejoras para su funcionamiento.

- Es diseñada para trabajar en topologías punto a punto lo que indica que se establece un pseudocable por cada par de CPEs que formen parte del circuito.

4.4 TIPOS DE L2 MPLS VPNS

Por la orientación del desarrollo podemos contar con 2 tipos principales de L2 MPLS VPN que son:

- Basadas en BGP
- Basadas en LDP

4.4.1 Basadas en BGP

Las L2 MPLS VPNs basadas en BGP fueron desarrolladas por Kireeti Kompella de Uniper Networks, el cual está referenciado en un draft de la IETF como draft-kompella-l2vpn-l2vpn, el cual como su nombre lo indica se basaban en una extensión del protocolo de puerta de enlace de borde (BGP) para el establecimiento de estas pseudoconexiones y el transporte de sesiones de capa 2. Este draft aun no se ha convertido en un estándar oficial de la IETF, sin embargo está siendo usado por algunos desarrolladores de este tipo de tecnologías.

4.4.2 Basadas en LDP

Las L2 MPLS VPNs basadas en LDP fueron desarrolladas por Luca Martín de Cisco Systems, el cual está referenciado en la IETF por el estándar RFC 4906. Este método se basa en el establecimiento de pseudocabes formados por una pila de etiquetas MPLS y administradas por el protocolo LDP para el transporte de conexiones de capa 2 sobre una red MPLS.

Métodos usados por desarrolladores:

A Continuación mostramos una lista de algunos desarrolladores de esta tecnología y su respectivo método:

- Foundry Networks: LDP-based (NetIron XMR Series, NetIron MLX Series)
- Juniper Networks: BGP-based (M/T/J-series)
- Juniper Networks: LDP-based (E-series)
- Cisco Systems: LDP-based
- Lucent Technologies (formerly Riverstone Networks): LDP-based
- Ericsson (formerly Redback Networks): LDP-based
- Huawei Technologies: LDP-based & BGP-based (NE/S-series)

4.5 Operación de L2MPLS VPN

Para explicar la operación de AToM, partimos de la premisa que deseamos pasar PDUs de capa 2 de un ruteador de ingreso LER1 hacia un ruteador de egreso LER2, sobre una red MPLS. Asumimos que existe un camino LSP (Label Switched Path) entre ellos, que no es más que un conjunto de etiquetas que representan una ruta de saltos en una red MPLS. Por lo tanto gracias al LSP R1 puede enviar paquetes a R2, colocando una etiqueta como cabecera del paquete y enviando el resultado por la interfaz de una de sus adyacencias. A esta etiqueta le llamaremos *Etiqueta de Túnel*, y a su correspondiente camino LSP lo denominaremos *Túnel LSP*.

El túnel LSP simplemente lleva los paquetes desde el LER1 a LER2, la etiqueta no le dice que hacer con el contenido del paquete, de hecho si se usa el removimiento de etiquetas en el penúltimo salto (penultimate hop popping) LER2 nunca ve la etiqueta de su correspondiente LSP. Por lo tanto si esta etiqueta no le dice que hacer al LER2, debe haber otra etiqueta que si lo haga, a esta etiqueta se la conoce como *Etiqueta de Circuito Virtual (Etiqueta de VC)*. A este camino formado por la etiqueta de circuito virtual, se lo conoce como un *pseudocable* AToM.

Los conceptos de un pseudocable AToM que menciona este capítulo es el especificado en el RFC: 4905 que referencia al trabajo realizado por Luca Martín con el draft-martini-l2circuit-encap-mpls-12.

Cuando el LER1 envía un PDU de capa 2 al LER2, este primero coloca la etiqueta de VC en la pila de etiquetas y luego coloca la etiqueta de túnel. La etiqueta de túnel es la que lleva al paquete MPLS desde el LER1 a LER2, mientras que la etiqueta VC no es visible hasta que el paquete llega a R2. R2 determina que hacer con el paquete basado en etiqueta de VC. Este procedimiento se lo puede ver en la figura a continuación.

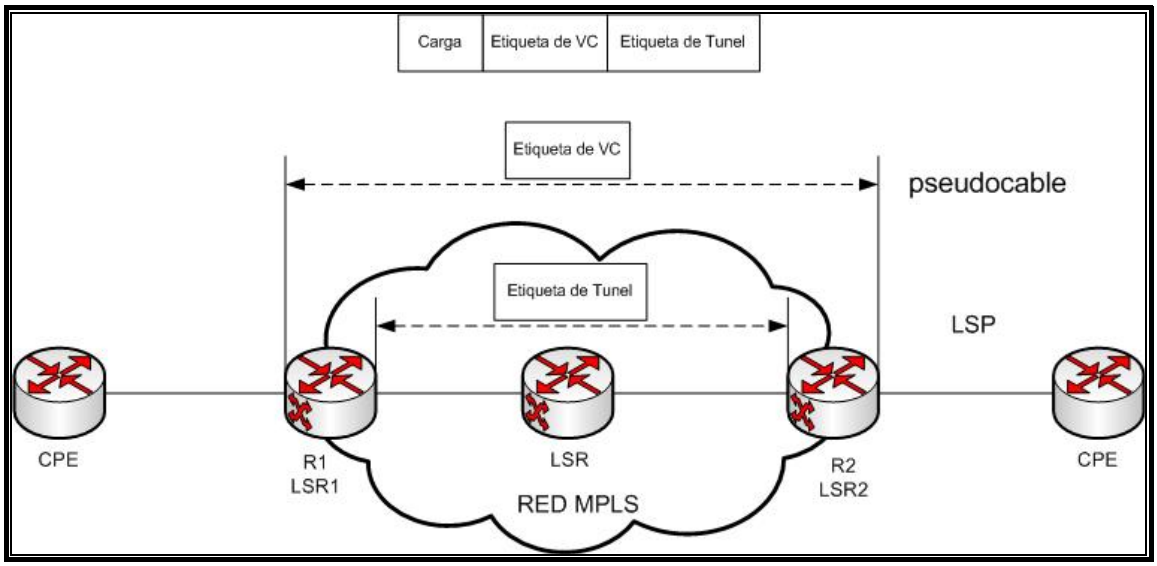


Figura 4.2 Fronteras de etiquetas en AToM.

En la figura 4.2 podemos ver el uso de las etiquetas de VC y de túnel en una red MPLS. Si por ejemplo en el campo carga que se muestra en esta figura es un identificador de un circuito ATM, la etiqueta de VC será la

correspondiente a un circuito virtual ATM en R2. R2 necesita inferir en la etiqueta VC y corresponder a un circuito ATM definido. Si por ejemplo la carga es de un circuito Frame Relay, la etiqueta de VC de la interfaz de salida corresponderá a un DLCI. Este proceso en unidireccional y debe ser repetido para la conexión bidireccional. Un requerimiento que se debe tomar en consideración es que el mismo identificador de circuito y tipo de circuito debe ser usado en ambas direcciones.

Note que el paquete puede cambiar al ser transportado desde el ruteador de ingreso hasta el ruteador de egreso gracias a que las etiquetas del túnel LSP pueden ir variando, sin embargo la cabecera de capa 2 del paquete que corresponde a la etiqueta de VC solo puede ser manipulada por el ruteador de egreso.

La etiqueta de VC siempre va bajo la etiqueta de túnel LSP, claro esto en ambientes MPLS; las etiquetas de túnel pueden ser agregadas o removidas según lo mande el túnel LSP, es mas si consideramos que R1 y R2 pueden estar directamente conectados, no seria siquiera necesario tener una etiqueta de túnel para establecer el circuito.

Por lo tanto debemos tener en claro que para poder transportar conexiones de capa 2 sobre una red MPLS debemos comprender lo siguiente:

a) Método para establecer y mantener un túnel LSP
b) Método para establecer y mantener un pseudocable.
c) Método para transportar conexiones L2 sobre un pseudocable.

A medida que vamos analizando cada uno de estos puntos entenderemos los procedimientos para establecer, mantener y cerrar conexiones que nos permitan transportar protocolos de capa 2 sobre un enlace MPLS.

4.6 Canal de Control y canal de Datos en L2 MPLS VPN

La operación de AToM se basa en dos canales principales de comunicación que definimos anteriormente para entender el proceso de etiquetamiento MPLS que son:

4.6.1 El canal de Control

El Canal de Control es por donde se transportan mensajes LDP usados para establecer, mantener y desconectar AToM pseudocables. Este proceso es el que más consume recursos en un equipo de redes; la ventaja es que este proceso solo se lo lleva a cabo al inicio de un establecimiento de un pseudocable y luego da paso al canal de datos para que simplemente reenvíe tramas MPLS.

4.6.2 El canal de Datos

El canal de Datos es por donde los paquetes son reenviados y se le asigna las etiquetas correspondientes que fueron establecidas en el canal de control. El separar el canal de control y el canal de datos en un tecnología es sumamente importante, ya que una vez que tenemos establecido el pseudocable AToM, el trabajo de los equipos que hacen la función de

ruteadores LSRs intermedios o P (provider) es de simplemente reenviar tramas MPLS con sus respectivas etiquetas intercambiando claramente la etiqueta correspondiente, sin embargo este proceso no consume muchos recursos de procesamiento, por lo cual podemos alcanzar grandes velocidades de transmisión de datos con magnitudes de 10/100/1000 Gbps de velocidad según de la capacidad de equipo, pudiendo así soportar tecnologías de última generación que requieren alta disponibilidad y grandes velocidades.

4.6.3 Mensajes del Canal de Control y del Canal de Datos

Los mensajes del canal de control y el canal de datos se pueden diferenciar gracias a que cada uno cumple con una función específica que explicamos anteriormente.

La figura 4.3 muestra en macro el formato de los paquetes del canal de control y del canal de datos usados en AToM.

Mensaje LDP - Canal de Control

Cabecera IP
Cabecera TCP/UDP (Puerto 646)
LDP PDU Cabecera LDP + Mensaje(s) LDP

Mensaje - Canal de Datos

Etiquetas de Túnel
Etiqueta PW (CV)
Palabra de control Opcional
Carga

Figura 4.3 Paquetes del canal de control y el canal de datos.

En el transcurso del capítulo, vamos a ir explicando detalladamente como son formados cada uno de estos paquetes y para que son usados así como también los procesos necesarios para establecer un camino mediante el cual se puedan transportar los paquetes de capa de enlace de datos sobre una nube MPLS.

Diferenciar el canal de Control y Canal de Datos es muy importante para comprender la magnitud de una implementación de redes avanzadas. El plano de comunicación que maneja un equipo de L3 diferencia las tareas que se necesitan ejecutar, separando fuertemente el establecer, mantener y operar las tecnologías implementadas con respecto al reenvío de paquetes.

Para alcanzar grandes velocidades de transferencia, MPLS usa procesos y tablas diferentes en cada uno de estos planos. Con respecto al manejo

adyacencias, intercambio de información de enrutamiento y así mismo intercambio de etiquetas MPLS o LDP. Un ruteador usa su plano de control formando tablas como las de adyacencias, de vecinos, de rutas aprendidas, etc. Sin embargo en el plano de datos solamente se manejan las variables o tablas necesarias para completar el reenvío de tramas o intercambio de etiquetas de un paquete MPLS.

El manejo del plano de control o plano de datos en la tecnología L2 MPLS, se referencia a su protocolo de comunicaciones principal que es el Protocolo de Distribución de Etiquetas (Label Distribution Protocol), el cual lo analizamos previamente en el capítulo de MPLS y lo profundizaremos posteriormente.

4.7 Protocolo de Distribución de Etiquetas (LDP)

El Protocolo de Distribución de Etiquetas o LDP (Label Distribution Protocol) como se lo conoce por sus siglas en inglés es un protocolo diseñado específicamente para la distribución de etiquetas MPLS. Este es un conjunto de procedimientos y mensajes mediante los cuales los LSRs (Label Switch Routers) establecen LSPs (Label Distribution Path) a través de una red mapeando o asignando información de enrutamiento de capa de red (L3) directamente a un enlace conmutado de capa de enlace de datos (L2). Este

LSP puede tener los puntos finales con vecinos directamente conectados (comparable a un reenvío IP de salto en salto), o puede tener el punto final en el nodo de egreso de la red, habilitando la conmutación por todos los nodos intermedios.

4.7.1 Estructura del Mensaje LDP

La estructura del Paquete LDP o LDP PDU como se conoce por su nomenclatura en ingles de Paquet Data Unit (PDU) está formada por 2 partes principales, una cabecera LDP más el Mensaje LDP. Este mensaje puede ser enviado sobre TCP o UDP en el puerto 646, esto dependerá del tipo de mensaje LDP que sea.

Cada mensaje LDP es enviado como un LDP PDU (Packet Data Unit). Cada PDU puede contener uno o más mensajes LDP. Cada LDP PDU consiste en una cabecera LDP seguida de uno o más mensajes LDP.

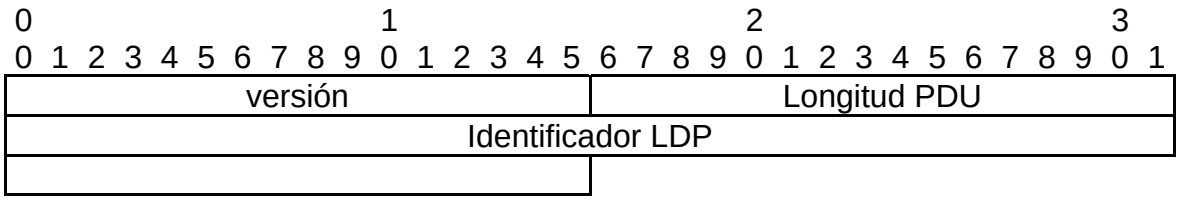


Figura 4.4 Formato de cabecera LDP.

En la figura 4.4 podemos ver la estructura del encabezado LDP. Donde el significado de cada uno de estos campos se detalla a continuación:

- Versión: Este campo especifica la versión del LDP. actualmente existe solo una versión v1
- Longitud PDU: Este campo indica la longitud del PDU sin contar los campos de de versión y Longitud PDU.
- Identificador LDP: Este campo funciona como un identificador único en el espacio de etiquetas de un ruteador LSR/PE. Un espacio de etiquetas puede ser usado tanto para una interfaz en particular como para una plataforma por completo. Este es un campo de 6 octetos, compuesto con los primeros 4 octetos por un valor único global (usualmente una dirección IP) y los 2 últimos que identifican el espacio de etiquetas de un LSR. Si una plataforma es etiquetada por completo, los últimos 2 octetos son 0.

Todos los mensajes LDP tienen un esquema de codificación similar que se la conoce como **TLV** por sus siglas en inglés **Time-Lengh-Value**. Se la conoce así por la forma del paquete, ya que consta principalmente de tres partes como se lo puede apreciar en la siguiente figura.

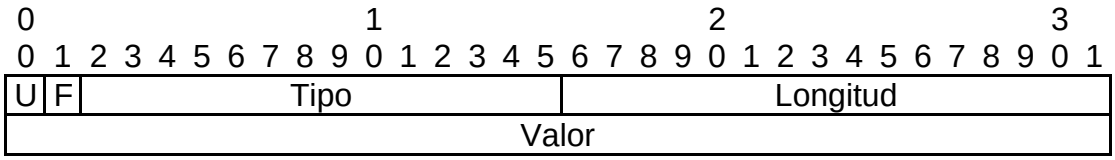


Figura 4.5 Formato de código TLV.

Para lo cual explicaremos el uso de los 2 bits no tan intuitivos como parte del mensaje:

- U: Unknown TLV bit: Bit desconocido: si está con el valor de 0 el mensaje no es procesado por el receptor y a su vez hace que este envíe un mensaje de notificación al original. Si el bit es colocado en 1 el bit U es ignorado y el mensaje se lo procesa con normalidad, que es como si este no existiera.
- F: Forward Unknown TLV bit: Se usa en combinación con el bit U, si este bit está en 0 el bit U no es reenviado junto con el cuerpo del mensaje; pero si está en 1 se lo envía a su siguiente salto junto con el contenido del mensaje.

El mensaje LDP mantiene la forma TLV, sin embargo un mensaje LDP puede llevar consigo un conjunto de mensajes LDP como se lo puede ver a continuación donde damos un ejemplo de un mensaje LDP.

Figura 4.6 Estructura del mensaje LDP.

- U: Bit de mensaje desconocido. Puede ser tanto 1 o 0.
- Tipo: Identifica el tipo de mensaje LDP.
- Longitud: Indica la longitud de la longitud de los campos Identificador, parámetros mandatarios y parámetros opcionales.
- Identificador: Este campo es usado en mensajes de notificación para indicar el mensaje al cual corresponde.
- Parámetros Mandatarios: Parámetros que deben ser incluidos con el mensaje.
- Parámetros Opcionales: Parámetros que pueden o no ser incluidos en el mensaje.

4.7.2 Tipos de Mensaje LDP

Existen 11 tipos de mensajes LDP, los cuales los podemos ver en la siguiente tabla.

Nombre	Tipo	Descripción
Notificación	0x0001	Sirve para indicar a un PE de algún evento como un error.
Saludo	0x0100	Paquetes de saludo son enviados como parte del proceso de descubrimiento LDP
Inicialización	0x0200	Mensajes usados para la inicialización de sesiones LDP
Actividad	0x0201	Mensajes utilizados para indicar que la sesión LDP está activa.
Dirección	0x0300	Un LSR usa este mensaje para publicar la dirección de sus interfaces.
Abandono de Dirección	0x0301	Usado para abandonar la dirección de interfaces previamente publicadas
Asignación de etiqueta	0x0400	Usado para publicar las Clases de Equivalencia de Reenvío (FEC) a una etiqueta
Solicitud de etiqueta	0x0401	Este mensaje es usado para pedir una etiqueta de su vecino LDP
Abandono de Etiqueta	0x0402	Usado para abandonar una etiqueta previamente solicitada
Liberación de etiqueta	0x0403	Usado para comunicar que no se necesita mas de la etiqueta prestada
Rechazo de solicitud de etiqueta	0x0404	Este mensaje es usado para abortar una solicitud de etiqueta
Vendedores Privados	0x3E00-0x03EFF	Extensiones LDP para vendedores privados
Experimental	0x3F00-0x03FFF	Extensiones LDP para uso experimental

Tabla 4.1 Tipos de mensajes LDP.

Todos estos mensajes, se pueden clasificar según su función, dividiéndose en 4 tipos principales:

- **Mensajes de descubrimiento** (discovery messages): se usan para anunciar y mantener la presencia de un LSR en la red. Un LSR mandará periódicamente por la red mensajes HELLO a través de un puerto UDP con la dirección multicast que represente a todos lo equipos involucrados.
- **Mensajes de sesión** (session messages): se utilizan para establecer, mantener y terminar sesiones entre pares LDP. Cuando un LSR descubre a otro por medio de mensajes HELLO utilizará un procedimiento de iniciación LDP por medio de TCP.
- **Mensajes de anuncio** (advertisement messages): se usan para crear, modificar y eliminar asociaciones de etiquetas a FECs. Se transportan vía TCP. Cuando se haya establecido la asociación los pares LDP podrán intercambiarse este tipo de mensajes.
- **Mensajes de notificación** (notificación messsages): Los mensajes de notificación también se transportan vía TCP. Hay dos tipos de mensajes de notificación: notificaciones de error y notificaciones de aviso. El primer tipo se utiliza para notificar errores fatales, en cuyo caso terminará la sesión y se descartarán todas las asociaciones de etiquetas aprendidas en dicha sesión. El segundo tipo se utiliza para pasarle a un LSR información de la sesión LDP o el estado de algún mensaje anterior

4.8 Establecimiento de un pseudocable

El funcionamiento de los pseudocables en L2MPLS VPN o AToM como también se conoce a esta tecnología, se basan principalmente en el protocolo de distribución de etiquetas MPLS LDP, razón por la cual es muy importante el comportamiento de este protocolo y poder así comprender como funcionan estos túneles de capa 2 sobre MPLS llamados pseudocables MPLS.

El proceso de establecimiento de un pseudocable, lo podemos resumir en tres pasos principales, los cuales los mostramos en el siguiente diagrama:

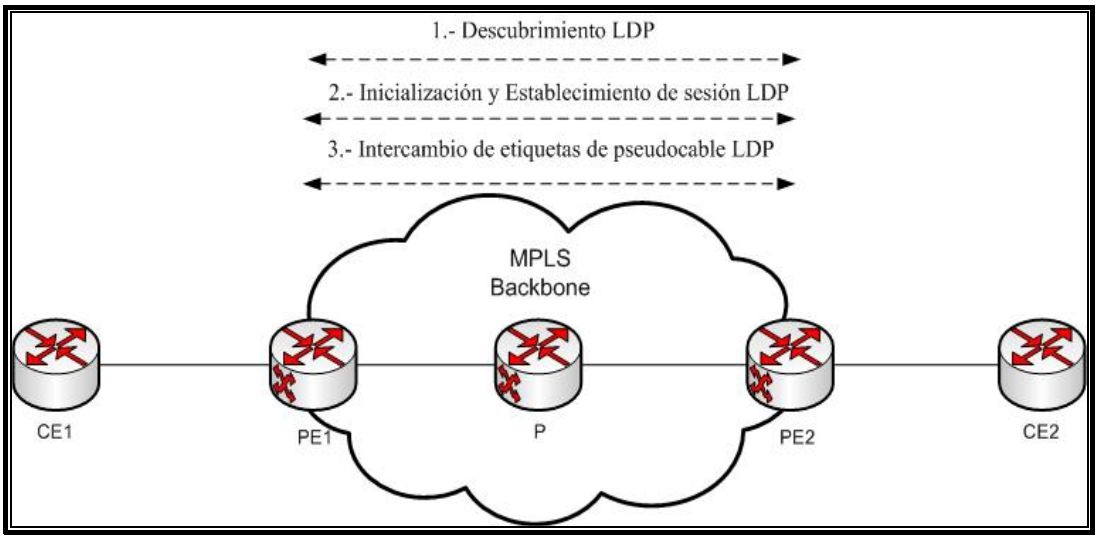


Figura 4.7 Establecimiento de un pseudocable.

Vamos a analizar cada uno de estos pasos y a medida que avancemos, profundizaremos en los conceptos necesarios de L2MPLS VPN para entender un pseudocable MPLS.

4.8.1 Descubrimiento LDP

El proceso de descubrimiento LDP es un mecanismo que le permite a un LSR descubrir posibles compañeros LDP. Esto hace innecesario configurar un LSR específico.

Este descubrimiento puede darse de dos formas:

- **Descubrimiento Básico:** que es utilizado entre extremos PE directamente conectados (en L2), y se comunica con todos los ruteadores por medio de la dirección multicast 224.0.0.2.
- **Descubrimiento Extendido:** es utilizado por extremos PE que no están directamente conectados en L2; a diferencia del descubrimiento básico, este usa direcciones unicast para identificar los extremos del pseudocable.

Los mensajes HELLO transportarán el identificador LDP con el espacio de etiquetas que LSR pretende usar en esa interfaz, además de otro tipo de información.

Los mensajes LDP de descubrimiento, son los únicos mensajes que se propagan por el puerto UDP 646, el resto de mensajes LDP son transportados por el protocolo TCP y sobre el mismo puerto. La razón de ser mensajes sobre el puerto UDP es debido a que este protocolo no es orientado a conexión, por lo cual no necesita acuse de recibo en el descubrimiento de posibles pares LDP, mas bien usan un proceso diferente como es el de contadores de tiempo para mantener activa una relación de vecinos por mensajes de saludo.

Dependiendo de que si un LSR tienen o no una adyacencia con un par LDP, este reiniciará el contador de expiración de adyacencia o creará una nueva relación de adyacencia. En caso de no tener una sesión LDP con el que envía el paquete, este procede a la intentar establecer una sesión LDP, que es el siguiente paso para el establecimiento de un pseudocable AToM.

El formato de un mensaje de saludo es como se muestra a continuación:

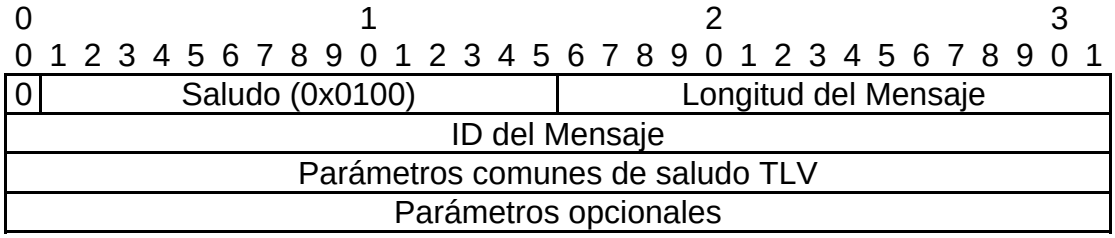


Figura 4.8 Formato del Mensaje de Saludo LDP.

Donde el significado de cada uno de los parámetros es el siguiente:

- ID del mensaje: 32 bits usados para identificar el mensaje.
- Parámetros comunes de saludo TLV: especifica parámetros comunes en todos los mensajes de saludo que incluyen principalmente los parámetros de tiempo necesarios para mantener estable una sesión LDP. Se recomienda tener una relación de 1 a 3 entre la transmisión de mensajes de saludo y el tiempo de expiración de la sesión.
- Parámetros opcionales: puede ser uno o más parámetros opcionales, cada uno codificado con el formato TLV (Tipo, Longitud, Valor). Estos parámetros pueden ser usados por ejemplo para determinar la dirección IPv4 o IPv6 usada para la sesión LDP o también establecer una secuencia para los paquetes de saludo, identificando así algún cambio de configuración en la sesión LDP (incrementando el contador).

Después de la fase de descubrimiento, los extremos están listos para poder establecer una conexión de transporte y empezar la fase 2 de este proceso.

4.8.2 Inicialización y establecimiento de la sesión LDP

El intercambio de mensajes de saludo (Hello), activan el proceso de establecimiento de una sesión LDP o túnel LSP. El proceso de establecimiento de una sesión LDP consiste principalmente en 2 pasos:

- Establecimiento de la conexión de transporte.
- Inicialización de la sesión

El siguiente proceso describe es establecimiento de una sesión LDP entre dos LSRs, PE1 y PE2.

Establecimiento de la conexión de transporte.

Después del intercambio de paquetes de Hello entre dos LSRs, se crea una relación de adyacencia inicial en la cual los LSRs conocen de la existencia de un posible par LDP, esta relación también se la conoce como relación de adyacencia de saludo.

El procedimiento de establecimiento de una sesión de transporte se la puede describe en los siguientes pasos.

- Si no existe un camino válido para intercambiar espacios de etiquetas asignados a cada LSR, se intenta crear una nueva sesión TCP con un nuevo LSP entre los pares LDP.
- Cada LSR utilizará como dirección de origen la misma que usó en el proceso de descubrimiento LDP, a menos que se hayan usado parámetros opcionales en la etapa se saludo, que indiquen lo contrario.
- Se determina quien va a ser del papel de activo y quien va a ser el papel de pasivo. Esto se puede determinar con las direcciones Ip de referencia que tengan estos equipos, para lo cual, el que tenga la dirección IP más alta va a tomar el papel de Activo y el otro de Pasivo.
- El equipo que tenga el papel de activo, intentará establecer una conexión LDP TCP sobre un puerto bien conocido, mientras que el otro espera por dicha conexión.

Inicialización de la sesión

Después que la conexión TCP es establecida, el LSR que tome el papel de activo, este empieza a enviar parámetros de sesión mediante mensajes de inicialización al su vecino. Estos parámetros incluyen la versión del protocolo LDP, el método de distribución de etiquetas, temporizadores y demás parámetros necesarios para establecer una sesión LDP.

El formato de mensajes que usan los LSRs para intercambiar mensajes de inicialización es el siguiente:

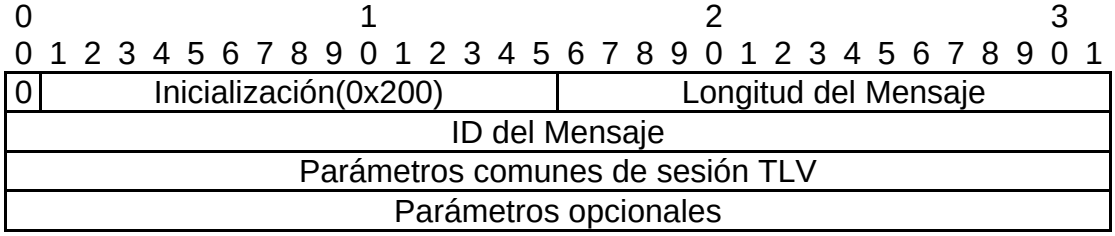


Figura 4.9 Formato del Mensaje de Inicialización LDP

Donde el significado de cada uno de los parámetros es el siguiente:

- ID del mensaje: 32 bits usados para identificar el mensaje.
- Parámetros comunes de sesión: especifica los valores propuestos por el que inicial la sesión LDP y que deberán ser negociados para cada sesión LDP.

- Parámetros opcionales: puede ser uno o más parámetros opcionales, para la versión de LDP que estamos estudiando que es la uno, solo son usados para protocolos como ATM y Frame Relay.

El formato como se envían los parámetros comunes es el siguiente:

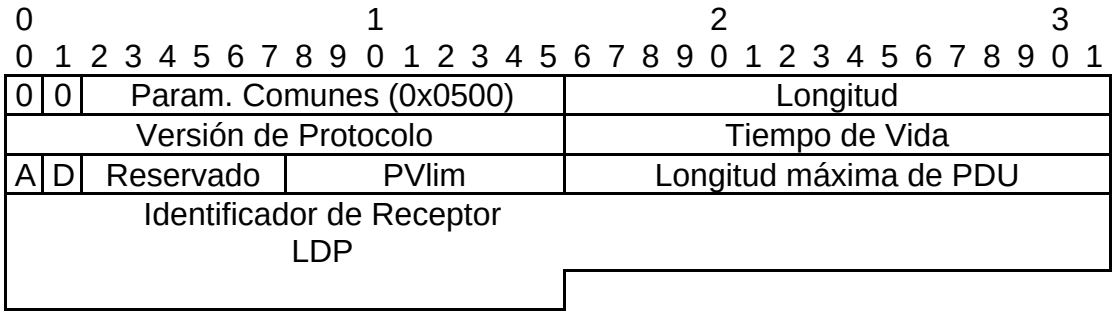


Figura 4.10 Parámetros comunes de Inicialización LDP

Donde el significado de cada uno de los parámetros es el siguiente:

- Versión de Protocolo: Especifica la versión de protocolo LDP, actualmente usamos la versión 1.
- Tiempo de vida (Keepalive): específica el número en segundos que el LSR propone sea el tiempo de vida de la sesión LDP. El LSR receptor debe calcular el tiempo de vida antes de que termine ya publicado. Este parámetro se establece como el tiempo máximo en que una sesión LDP puede esperar entre la llegad de PDUs, antes de suponer que la sesión ha culminado (hold timer).

- A: Disciplina de publicación de etiquetas: indica el método de distribución de etiquetas; si es 1 se usa el método no solicitado y si es 0 se usa el método por demanda. Usualmente se usa el método de demanda de etiquetas, a menos que estemos trabajando con enlaces ATM o de Frame Relay controlado.
- D: Detección de Lazo: indica si está (1) o no (0) establecida la detección de lazos por vector de camino.
- PVlim: Limite de Vector de Camino (Path Vector Limit): configura la longitud máxima del vector de camino usado papar la detección de lazos.
- Reservado: para futuras investigaciones, deben ser 0 e ignorados.
- Longitud máxima de PDU: un valor de 0 a 255 especifica la longitud máxima por defecto que es de 4096 octetos. Este parámetro será el menor de los 2 configurados en cada uno de los LSRs, en caso de no aceptar, se envía u mensaje de rechazo de parámetros y no se inicia la sesión.
- Identificador de receptor LDP: identifica el espacio de etiquetas del receptor. Este identificador, junto con el identificador LDP que envía la cabecera LDP PDU es e que le permite el LSR receptor identificar que el mensaje le corresponde, o dicho de una mejor manera, que corresponde a la adyacencia de saludo establecida en su primera fase.

Para comprender el proceso de inicialización, vamos a explicarlo con un ejemplo que se lo describe a continuación:

Asumiendo que el LSR1 es el que cumple el papel de activo y el LSR2 el papel de pasivo:

a. Cuando un LSR2 recibe un mensaje de inicialización, este busca entre sus relaciones de adyacencia de saludo para ver a quien corresponde el mensaje.
b. LSR2 con el mensaje de inicialización, chequea si los parámetros de sesión son aceptables para el, si lo son se envía un mensaje inicialización con sus parámetros que el desearía tener e indica que ha aceptado los parámetros de LSR1 con un mensaje de actividad (keepalive). Si los parámetros recibidos no son aceptables por LSR2, este envía un mensaje de rechazo de parámetros de sesión y procede a cerrar la conexión TCP y por consiguiente LSR1 procede a cerrar la conexión TCP.
c. Cuando LSR1 recibe ambos mensajes, tanto el de inicialización y el mensaje de actividad, la sesión está activa desde el punto de vista de LSR1 y por consiguiente envía este par de mensajes a LSR2 para que el también vea la conexión inicializada.

Un LSR debe controlar la retransmisión de inicialización de sesión con el algoritmo de backoff exponencial (2s, 4s, 8s …) cuando estos no han podido ser establecidos y notificados por un mensajes de rechazo de parámetros de sesión, considerando que este retrazo no puede ser menos de 15 segundos, ni más de 2 minutos(por estándar). Este reintento de establecimiento de sesión continúa con este proceso hasta que exista la intervención en la configuración de uno de los 32 LSRs y estén de acuerdo los parámetros entre los 2 equipos. Todo este proceso, lo comanda el LSR que tome el papel de activo, razón por la cual este procedimiento se vuelve asimétrico y cualquier configuración en el LSR2 (pasivo) será imperceptible en el establecimiento de la sesión, para solucionar esto, se activa el parámetro opcional de identificador de reconfiguración en el paquete de saludo, el cual identifica un cambio en la configuración y se procesan los cambios del equipo pasivo.

Es importante describir el comportamiento de negociación de la sesión LDP en términos de una máquina de estados. Definimos la máquina de estados de la sesión LDP en 5 posibles estados, en el cual describimos el comportamiento y la transición de los estados en el siguiente diagrama:

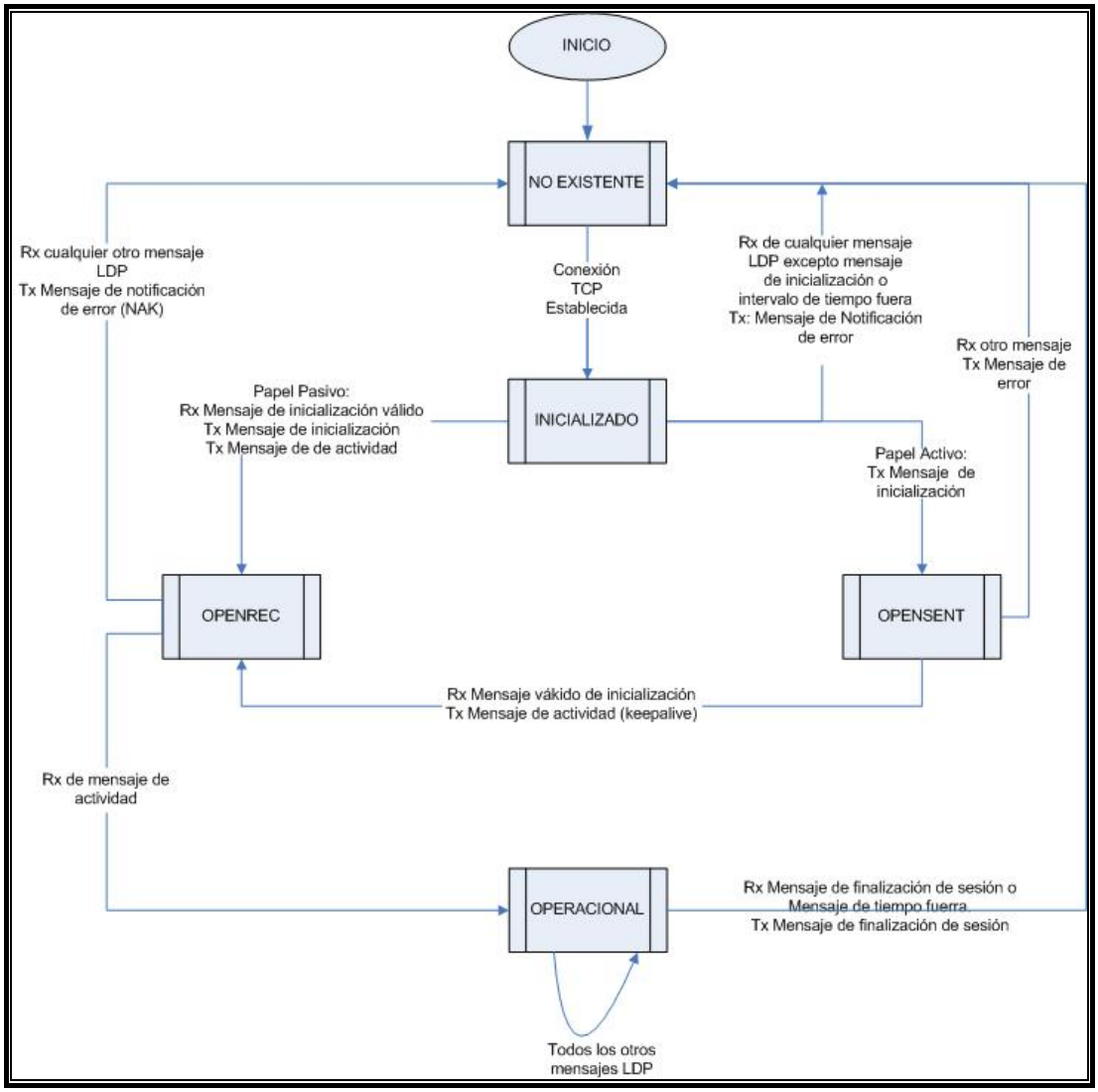


Figura 4.11 Máquina de estados del establecimiento de una sesión LDP.

En el diagrama podemos ver con facilidad cada uno de los estados del establecimiento de una sesión LDP que fue previamente explicado paso a paso. Cabe recalcar que el establecimiento de la sesión LDP toma caminos diferentes, dependiendo de el papel que esté ejerciendo cada uno de los LSRs, que puede ser el de activo o pasivo.

4.8.3 Intercambio de etiquetas de pseudocable LDP

Hasta el momento hemos aprendido mucho sobre el funcionamiento, protocolos necesarios, componentes y demás del establecimiento de un pseudocable MPLS, sin embargo aún no hemos descrito la manera en si del establecimiento de un pseudocable.

Un pseudocable MPLS nace del protocolo de distribución de etiquetas LDP, siendo una extensión de este protocolo y basándose en su funcionamiento. Por esta razón hemos explicado en detalle este protocolo.

El proceso de establecimiento de un pseudocable, es prácticamente una asignación de etiquetas adicional que pueden manejar los LSRs, los cuales van a poder identificar un circuito de capa2 y poder transportarlo sobre un enlace MPLS o un enlace de etiquetas conmutadas (LSP) como lo hemos conocido hasta el momento. Como podemos observar, y podemos adelantar aquí no involucramos protocolos de enrutamiento, razón por la cual podemos crear una conexión virtual de un circuito en L2, gracias a las propiedades de MPLS y su protocolo de distribución de etiquetas LDP, se hace independiente la tecnología de capa 2 que deseemos manejar, razón

por la cual a esta tecnología también la han llamado AToM (Any Transport Over MPLS), que significa Todo Transporte sobre MPLS.

Con esta introducción, podemos continuar con el aprendizaje de los pseudocables MPLS.

Dado la importancia del protocolo LDP, este define 4 procesos, mensajes y TLVs para las siguientes áreas:

- Descubrimiento
- Mantenimiento de sesión
- Distribución de etiquetas
- Notificación de errores

Como mencionamos anteriormente, el formato principal de cualquier mensaje LDP está dado por el formato TLV. Para este formato se han definido algunos tipos de mensajes o algunos tipos de TLVs, los cuales mostramos algunos en la siguiente tabla.

Nombre TLV	Tipo TLV	Descripción
TLV de FEC	0x0100	Codifican FECs que son asignaciones usadas para identificar la correspondencia de un paquete a un LSP, referenciando un conjunto de IPs a un específico LSP.
TLV de Etiqueta	0x0200-0x0202	Codifica etiquetas, estos TLVs son usados por los mensajes para publicar, requerir, soltar y rechazar asignaciones de etiquetas.
TLV de Lista de Direcciones	0x0101	Codifican direcciones, estos TLVs son usados para codificar direcciones o rechazar direcciones asignadas a una familia de direcciones, que puede ser IPv4 o IPv6.
TLV de Contador de Salto	0x0103	Aparece como un campo opcional en los mensajes que establecen un LSP, este calcula el número de LSRs que existen en un determinado LSP.
TLV de Vector de Camino	0x0104	Este TLV es usado como en conjunto con el de TLV de Contador de Salto en los mensajes de requerimiento y asignación de etiquetas, para poder habilitar el mecanismo LDP de detección de lazo.
TLV de Estado	0x0300	Usados por los mensajes de notificación para llevar los diferentes estados que de desee publicar.

Tabla 4.2 Tipos de TLV

Los mensajes de establecimiento de un pseudocable contienen principalmente 2 tipos de parámetros TLV que son: TLV de FEC y TLV Genérico. Ambos se ven en el mensaje LDP como se ve a continuación:

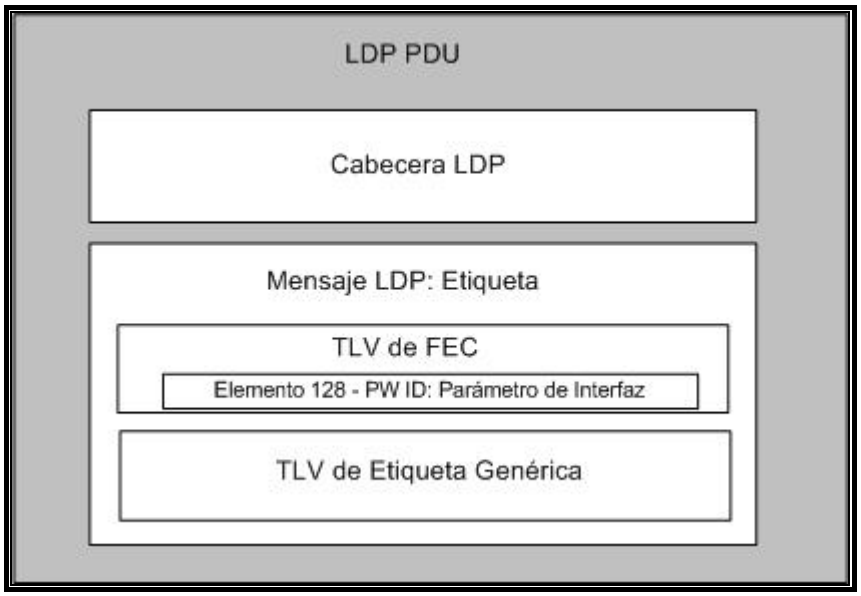


Figura 4.12 Estructura del LDP PDU

Para comprender los conceptos de la inicialización de un pseudocable, vamos a definir algunos términos:

TLV de Etiqueta Genérica.

Dentro de los TLV de etiquetas tenemos los siguientes tipos de TLV:

- TLV de Etiqueta Genérica.
- TLV de Etiqueta ATM

- TLV de Etiqueta Frame Relay

De los cuales, nos vamos a concentrar en el TLV de etiqueta genérica ya que es la usada para identificar circuitos Ethernet que son estudio en este capítulo.

Un LSR usa un TLV de Etiqueta Genérica para codificar etiquetas usadas en enlaces donde los valores de estas, son independientes del direccionamiento usado en la tecnología del enlace. Para comprender mejor, podemos comparar la tecnología de Ethernet con la de ATM, donde en Ethernet, las etiquetas asignadas son independientes de los valores que esta usa para identificar sus enlaces; a diferencia de los enlaces ATM, donde las etiquetas son relacionadas con los ID de circuitos virtuales que estos usan.

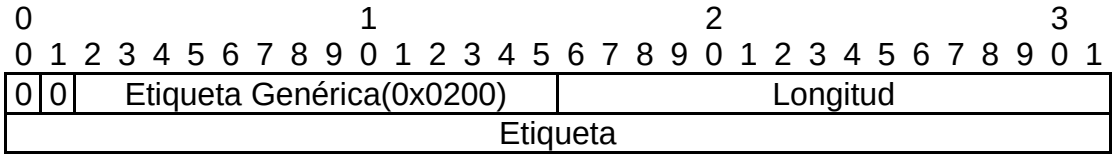


Figura 4.13 Estructura del TVL de Etiqueta Genérica.

La etiqueta que se menciona en este mensaje es la misma que está definida en el protocolo MPLS [RFC3032] y es la que se encarga de formar el LSP por donde se va a establecer el pseudocable MPLS y transportar la etiqueta

identificadora de un pseudocable en L2MPLS VPN como lo veremos posteriormente.

TLV de FEC.

FEC: Fordward Equivalence Class (Reenvío de Equivalencia de Clase): en una sesión LDP es necesario especificar precisamente que paquetes son asignados a cada LSP. Esto se puede lograr dando una especificación de reenvío de equivalencia de clase. Cada FEC identifica un conjunto de paquetes IP que son asignados a cada LSP.

Podemos hablar de una dirección IP en particular concuerda con un prefijo si y solo si esta IP está dentro del rango que establece ese prefijo. Así también podemos decir que un paquete en particular concuerda con un LSP si y solo si ese LSP tiene un elemento FEC de prefijo de dirección que concuerda con la dirección de destino del paquete.

El formato de un TLV de FEC lo mostramos a continuación:

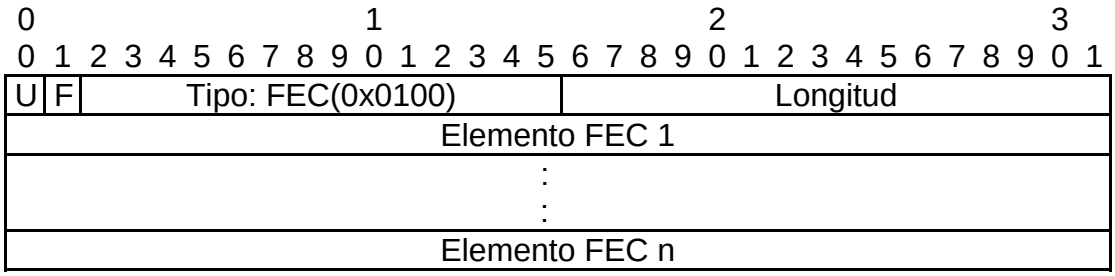


Figura 4.14 Formato del TLV de FEC.

Como vemos en el formato del TLV de FEC, este puede contener uno o más elementos FEC.

Los siguientes son los tipos de elementos FEC definidos. Pueden existir más elementos FEC dependiendo de la necesidad, por ejemplo los usados para un pseudocable como lo veremos posteriormente.

Nombre de FEC TLV	Tipo FEC	Descripción
Wildcard	0x01	Es usado solo en los mensajes de liberación de etiquetas o de rechazo de etiqueta. Indica la liberación o el rechazo de todos los FECs asociados con la etiqueta dentro del siguiente TLV de etiqueta.
Dirección	0x02	Este elemento denota una dirección única, Ejm: 10.1.1.1, 172.16.1.1, 192.168.1.1.
Prefijo	0x03	Este elemento representa una dirección de prefijo, usado para agrupar un conjunto de IPs. Ej.: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

Tabla 4.3 Tipos de TLV de FEC.

4.8.4 Elemento FEC PWid

Para poder transportar circuitos de L2 sobre un túnel MPLS, es necesario especificar sobre cada paquete enviado una cabecera de pseudocable, que consiste en un campo demultiplexor colocado en el PDU encapsulado (ver figura: Figura 4.12 Estructura del LDP PDU). Esta etiqueta es colocada sobre cada PDU antes de ser transportado por a red MPLS, por consiguiente en el otro extremo del pseudocable esta cabecera nos permite identificar a que pseudocable corresponde cada paquete. A esta etiqueta se la conoce como etiqueta de pseudocable o **Etiqueta PW**. Estos paquetes necesitan ser transportados por un Túnel de una Red de Paquete Conmutado (PSN Packet Switched Network Tunnel) que en nuestro caso es un Túnel MPLS (LSP).

Este modelo de red, lo podemos apreciar en la siguiente figura, donde podemos diferenciar cada una de las partes que conforman un pseudocable MPLS.

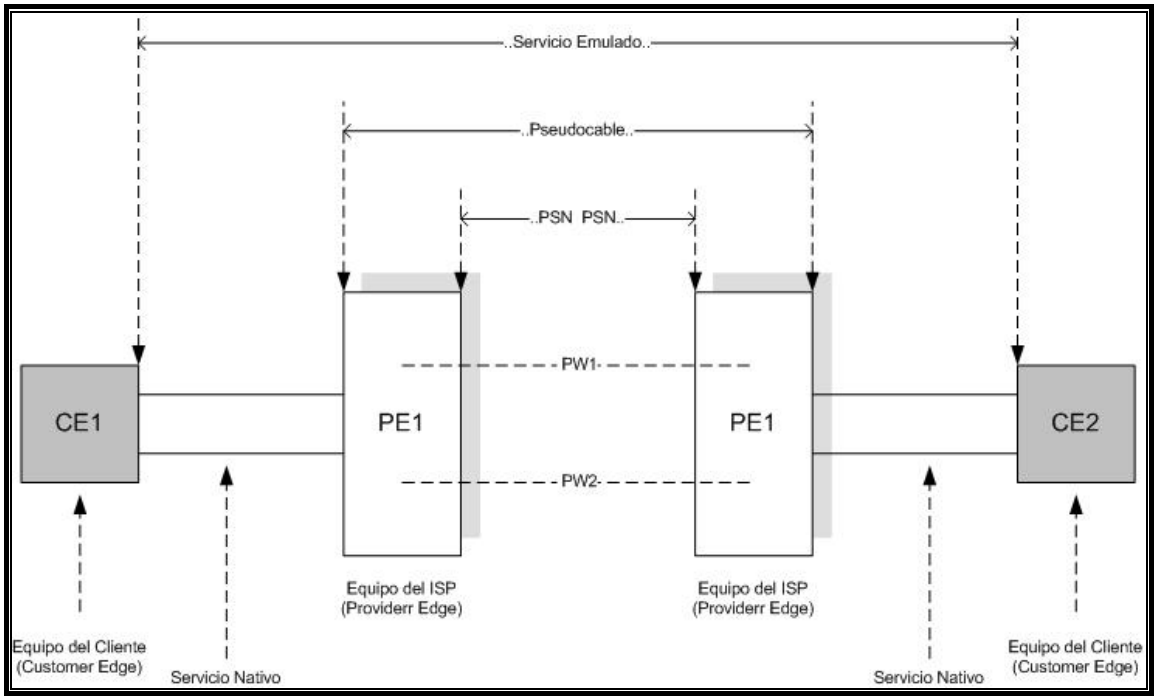


Figura 4.15 Partes de un pseudocable MPLS.

La distribución de las asignaciones de etiquetas de pseudocable son distribuidas usando LDP en modo no solicitado y la formación de la sesión LDP se dará por el mecanismo de descubrimiento extendido.

Como vamos a utilizar el protocolo de distribución de etiquetas LDP para establecer y mantener un pseudocable, es necesario definir nuevos TLVs, elementos FEC, parámetros y códigos para LDP, quienes le permiten a LDP identificar pseudocables y asignar atributos a un pseudocable.

Los FEC TLV son los indicados para indicar el significado de una etiqueta y por lo cual podemos ayudarnos en este para identificar que una etiqueta en

particular es asignada a un pseudocable. Para esta especificación definimos dos nuevos tipos de FEC TLVs usados para identificar pseudocables. Para el establecimiento de un pseudocable, solo uno de estos es utilizado.

LDP permite a cada FEC TVL referenciar a un conjunto de elementos FEC. Sin embargo, para establecer y mantener pseudocables, cada FEC TLV debe contener exactamente un elemento FEC.

TLV	**Definido para mensajes**
TLV de Estado de PW	Notificación
LTV de Parámetros de Interfaz de PW	FEC
TLV de ID de Grupo de PW	FEC
Elemento FEC	**Definido para mensajes**
PWid (0x80) PWid Generalizado (0x81)	FEC FEC
Código de Estado	
C-Bit ilegal	
C-Bit erróneo	
Bit-rate incompatible	
No configuración CEP/TDM	
Estado de PW	
TAI No asignado/No reconocido	
Error de configuración genérica	
Método de estado de PW no soportado	

Tabla 4.4 Extensiones TLV.

El elemento FEC que usamos para intercambiar etiquetas de pseudocable es el de PWid, cuyo formato lo vemos a continuación.

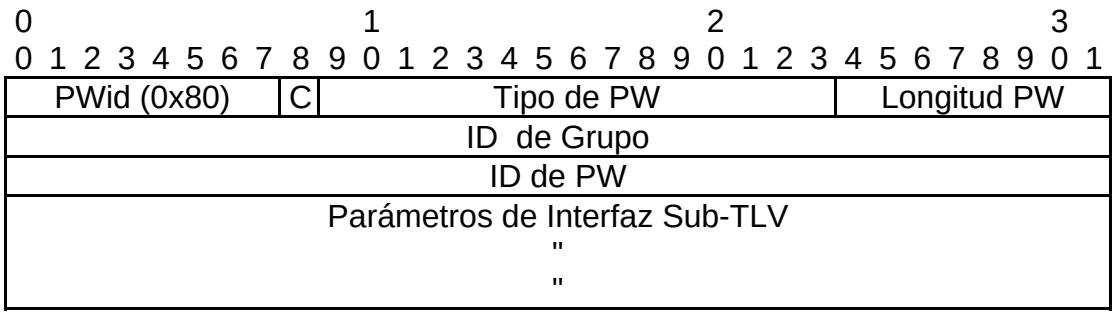


Figura 4.16 Formato del elemento FEC PWid.

Donde el significado de cada uno de los parámetros es el siguiente:

- C bit: Indica si es usada (1) o no (0) en el pseudocable (incluidos en los paquetes del Canal de Datos).
- Tipo de PW: Indica el tipo de pseudocable.
- Longitud de PW: especifica la longitud del ID de PW y los parámetros de interfaz.
- ID de Grupo: Contiene un valor para identificar un grupo de pseudocables, usado para señalizar grupos de pseudocables previamente establecidos.
- ID de PW: Junto con el tipo de PW identifica un único pseudocable.
- Parámetros de Interfaz: Este campo es usado para señalizar parámetros del circuito en L2 como el MTU o la descripción de la interfaz.

Los tipos de pseudocable definidos son los que mostramos a continuación:

Tipo de PW	Descripción
0x0001	DLCI Frame Relay
0x0002	Transporte ATM AAL5 SDU VCC
0x0003	Transporte ATM de celda transparente
0x0004	Ethernet – VLAN
0x0005	Ethernet
0x0006	HDLC
0x0007	PPP
0x0008	SONET/SDH Emulación de Servicios de Circuitos sobre MPLS
0x0009	Transporte de celdas ATM n-a-uno VCC
0x000A	Transporte de celdas ATM n-a-uno VPC
0x000B	Transporte de ATM AAL5 PDU VCC
0x000C	Modo de puerto de Frame Relay
0x000D	SONET/SDH Emulación de Circuito sobre paquete
0x000E	Transporte ATM AAL5 PDU VCC
0x000F	Modo de puerto de Frame Relay
0x0010	SONET/SDH Emulación de Circuito sobre paquete
0x0011	E1 sobre paquete
0x0012	T1 (DS1) sobre paquete
0x0013	E3 sobre paquete
0x0014	T1 (DS3) sobre paquete
0x0015	CESoPSN Modo básico
0x0016	TDMoIP nodo AAL1
0x0017	CESoPSN TDM con CAS
0x0018	TDMoIP nodo AAL2
0x0019	DLCI Frame Relay

Tabla 4.5 Tipos de Pseudocable.

Para que un pseudocable pueda funcionar, este debe establecer los parámetros de circuito correspondientes a los extremos del pseudocable. Para esto, se usa el parámetro de interfaz sub-TLV del FEC PWid, el cual tiene el siguiente formato:

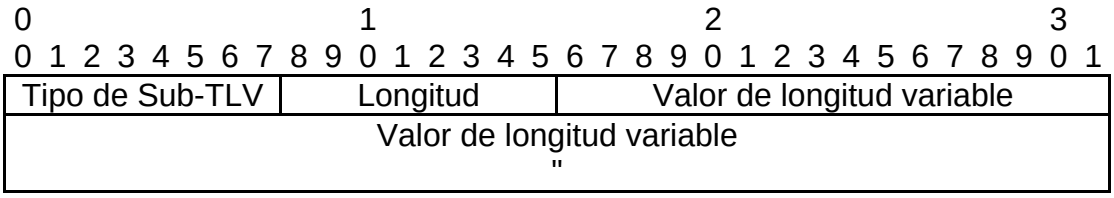


Figura 4.17 Formato del parámetro de interfaz sub-TLV.

El campo de Tipo de Sub-TLV indica el tipo de parámetro que va a ser identificado en el paquete. El campo longitud es definido como la longitud del parámetro de interfaz incluido el campo longitud también. Con respecto al los tipos de parámetros que pueden ser establecidos en un pseudocable, la IANA ha registrado los siguientes tipos de parámetros de interfaz:

ID	Longitud	Descripción
0x01	4	MTU de Interfaz
0x02	4	Máximo numero de celdas ATM concatenadas
0x03	hasta 82	Descripción opcional de Interfaz
0x04	4	Bytes de carga CEP/TDM
0x05	4	Opciones CEP
0x06	4	Identificador de VLAN
0x07	6	Bit-rate de CEP/TDM
0x08	4	Longitud de LDCI Frame Relay
0x09	4	Indicador de Frame Relay
0x0A	4	Identificador de retención FCS
0x0B	4/8/12	Opciones TDM
0x0C	4	Parámetro VCCV

Tabla 4.6 Tipos de parámetros de interfaz.

4.8.5 Señalización de estado de un pseudocable

LDP no es solo usado para establecer un pseudocable sino también para señalizar el estado en el que este se encuentra. Esto es importante por ejemplo, si un ruteador PE, quiere indicar el estado de un circuito emulado en un pseudocable AToM.

Un PE puede usar 2 maneras de señalizar el estado de un circuito sobre un pseudocable y son:

- Mensajes LDP de Liberación de Etiquetas.
- Mensaje LDP de Notificación.

Los mensajes de señalización de estado con mensajes LDP de liberación de etiquetas son los más básicos en la señalización de un pseudocable, usados para indicar que el pseudocable ha dejado de estar activo.

Para usar mensajes de señalización de estado con mensajes LDP de notificación, esto se debe ser negociar en la fase de establecimiento de un pseudocable. Si el ruteador PE que empieza el establecimiento de un pseudocable soporta la señalización de estado por mensajes de notificación,

este incluye un TLV de estado de PW junto con el FEC TLV y con el TLV genérico en la fase de mapeo de etiquetas LDP.

Si el ruteador que recibe este mensaje soporta también la señalización de estado por mensajes LDP de notificación, este responde con un mensaje TLV de estado de PW en los mensajes LDP de mapeo de etiquetas.

El formato de los mensajes LDP de notificación lo podemos ver a continuación.

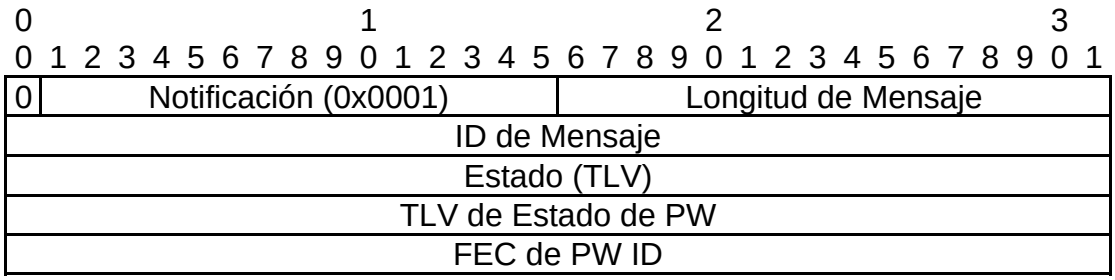


Figura 4.18 Formato del mensaje LDP de notificación.

Donde el significado de cada uno de los parámetros es el siguiente:

- ID de Mensaje: Es un valor usado para identificar el mensaje.
- Estado (TLV): Valor colocado en 0x00000028 indicando que lo que sigue es un mensaje de estado de pseudocable.
- TLV de Estado de PW: Indica en código, el estado del pseudocable.

- FEC de PW ID: es el encargado de llevar la información que identifica al pseudocable (ID de PW) o grupo de pseudocables (ID de grupo) que estamos señalizando, este mensaje no necesita llevar consigo parámetros de interfaz sub-TLV.

El estado de un pseudocable está codificado y lo mostramos a continuación.

Código de Estado de PW	Descripción
0x00000000	Pseudocable reenviando (Reinicia toda falla)
0x00000001	Pseudocable no reenviando
0x00000002	Falla de recepción del circuito local (ingreso)
0x00000004	Falla de transmisión del circuito local (egreso)
0x00000008	Falla de recepción en la PSN Local (ingreso)
0x00000010	Falla de transmisión en la PSN Local (egreso)

Tabla 4.7 Código de estado de un pseudocable.

Podemos acotar que los códigos pueden ser combinados para hacer más eficiente este trabajo.

5 SIMULACIÓN DE LOS SERVICIOS L2 Y L3 MPLS VPN

5.1 Requerimientos de simulación

A continuación analizaremos los requerimientos necesarios para realizar la simulación y los beneficios de utilizar la herramienta seleccionada.

5.1.1 Requerimientos de Software

El emulador de equipos CISCO, Dynamips lo podemos instalar tanto en Windows como en Linux, lo que lo hace muy flexible en cuanto a la plataforma que lo soporta.

Este emulador es de código abierto y no tiene precio, sin embargo su funcionalidad es excelente comparada con algunos simuladores existentes en el mercado. La comparación de algunos simuladores podemos verla como uno de los anexos a este capítulo.

El único software propietario indispensable para poder emular los dispositivos CISCO con el Dynamips es el IOS o sistema operativo de los equipos CISCO de una plataforma real, el cual lo podemos obtener de sitio web de CISCO con una cuenta CCO.

5.1.2 Requerimientos de Equipamiento

Dynamips utiliza una buena cantidad de RAM y CPU para realizar su emulación. Si intentamos simular un ruteador que requiere 256 MB de RAM para un ruteador 7200, y colocamos 256 MB de RAM en la creación de nuestra instancia virtual, se almacenará 256 MB de memoria real de trabajo de nuestro computador. Dynamips también almacena (por defecto) 64 MB de RAM por instancia en sistemas Unix y 16 MB en Windows para almacenar translaciones JIT (Just in Time) para mejorar su sistema de compilación. Sin embargo, Dynamips permite optimizar el uso de memoria mediante procesos de mapeo de memoria por inactividad o la creación de una imagen tipo fantasma compartirla entre plataformas similares, que permiten elaborar laboratorios mucho más complejos.

Dynamips también utiliza una gran cantidad de CPU, porque se trata de emular el procesador de un ruteador instrucción por instrucción. Inicialmente no tiene forma de saber cuando el CPU del ruteador virtual está inactivo por

lo que deber ejecuta todas las instrucciones que componen el IOS a pesar de no necesitarlas. Para esto utilizamos el Valor de PC inactivo (Idle-PC-Value) que analiza de una imagen emulada los puntos de código más representativos que son identificados como lazos en el sistema operativo y permiten ahorrar recursos significativamente. Esto permite al equipo reposar por intervalos de tiempo cuando ve inactividad o no hay cambios en el equipo, sin dejar de tener todas las funcionalidades configuradas ni dejar de cumplir sus tareas esenciales.

5.1.3 Requerimientos Económicos

Los requerimientos de implementar un laboratorio a nivel de un ISP sería sumamente costoso, ya que la cantidad de equipos necesarios para representar toda una infraestructura a nivel de un ISP es sumamente grande y hasta hace algún tiempo la única manera de hacerlo era aplicando los cambios directamente en los equipos en producción.

En situaciones excepcionales podríamos considerar el IOS de CISCO un posible punto de inversión para un poder utilizar este emulador y poder aprovechar todas las ventajas que este proporciona, sin embargo dado que CISCO es una plataforma a nivel mundial, no será un problema conseguir

una imagen estándar que nos permitiría implementar gran variedad de escenarios.

Para realizar simulaciones a mediana escala, que sería para una empresa portadora de datos, se puede considerar un requisito una plataforma robusta como un Servidor SuperMicro con 2 procesadores y con un sistema Operativo Linux en modo consola, con lo cual podríamos emular hasta unos 7 o 10 ruteadores 7200 con toda su capacidad.

5.1.4 Dynamips

Dynamips es un emulador de ruteadores Cisco escrito por Christophe Fillot. Emula las plataformas de ruteador 2691, 3620, 3640, 3660, 3725, 3745, 7206 y corre imágenes IOS estándares. Permite una relación más cercana con los dispositivos Cisco; siendo Cisco un líder a nivel mundial en tecnologías de Networking, Dynamips se convierte en una poderosa herramienta de desarrollo y aprendizaje para el campo de networking.

Claramente, este emulador no puede reemplazar a un ruteador real, es solamente una herramienta complementaria en laboratorios de administradores de redes Cisco, o personas que quieren incrementar su

conocimiento y aprobar certificaciones Cisco entre las cuales tenemos a CCNA, CCNP, CCIE.

Dynamips se apoya con un gestor de simulaciones llamado Dynagen, el cual utiliza un simple archivo configuración, fácil de comprender, y especifica configuraciones tanto de equipo como de software para ruteadores a emular. Usa una sintaxis simple de interconexión de ruteadores, puentes, conmutadores frame-relay, ATM, y conmutadores Ethernet.

Puede funcionar en modo "Cliente / Servidor", conectando instancias emuladas en servidores remotos e integrando una solución, mucho más escalable. Dynagen también puede controlar simultáneamente múltiples servidores Dynamips para distribuir grandes redes virtuales a través de varios equipos.

Provee administración vía comandos para listar los dispositivos, iniciar, detener, recargar, suspender, resumir, y conectar a las consolas de los ruteadores virtuales.

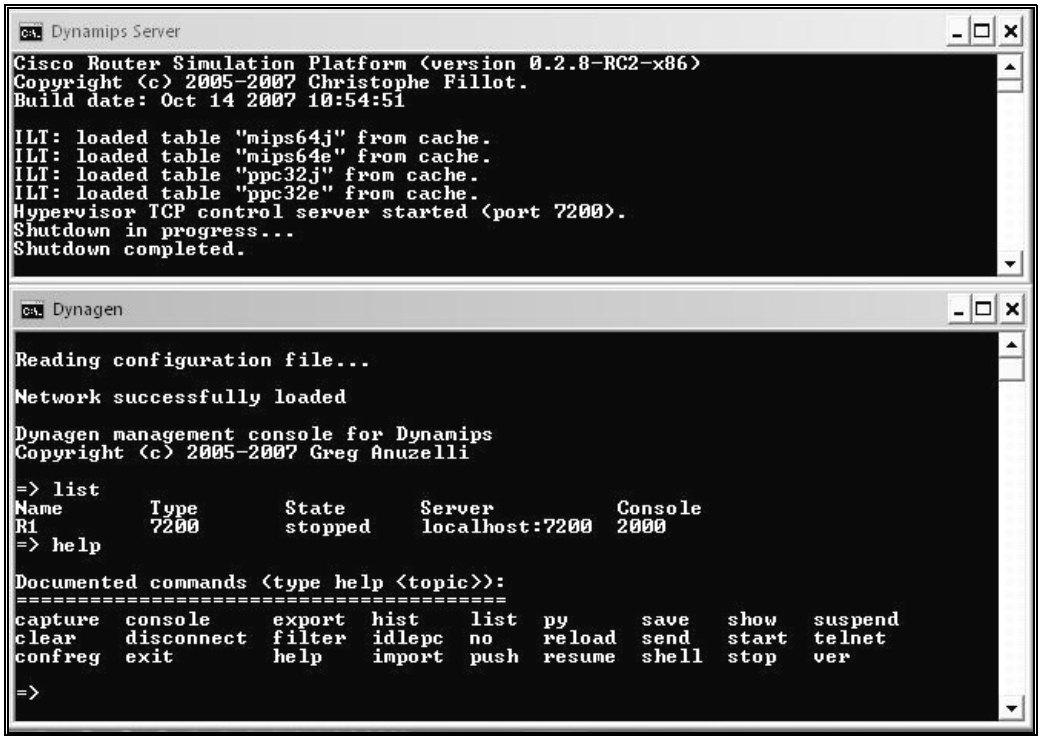


Figura 5.1 Dynamips y Dynagen

Actualmente posee desarrollos gráficos que complementan la interacción con el usuario como lo son, el Dynagui orientado principalmente para sistemas Linux y el GNS3 que es el mejor orientado para sistemas Windows los cuales los podemos presentar a continuación:

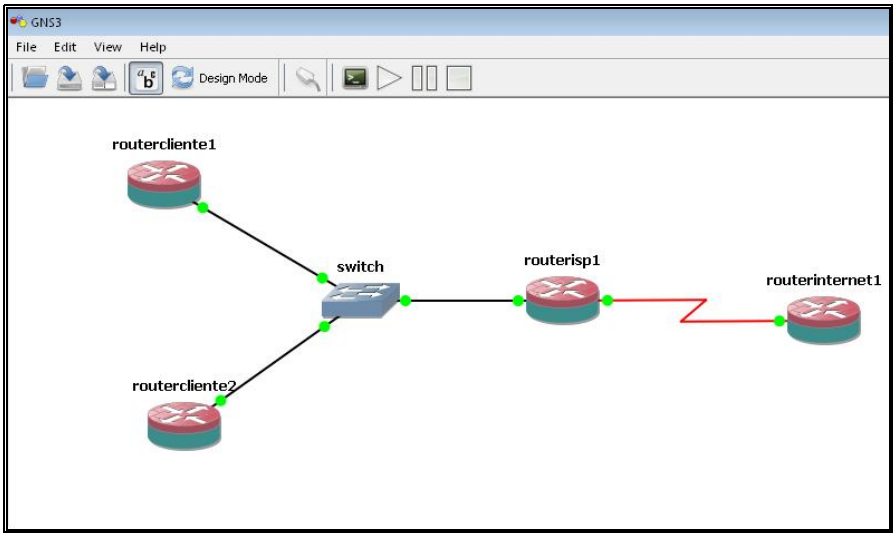


Figura 5.2 GNS 3.

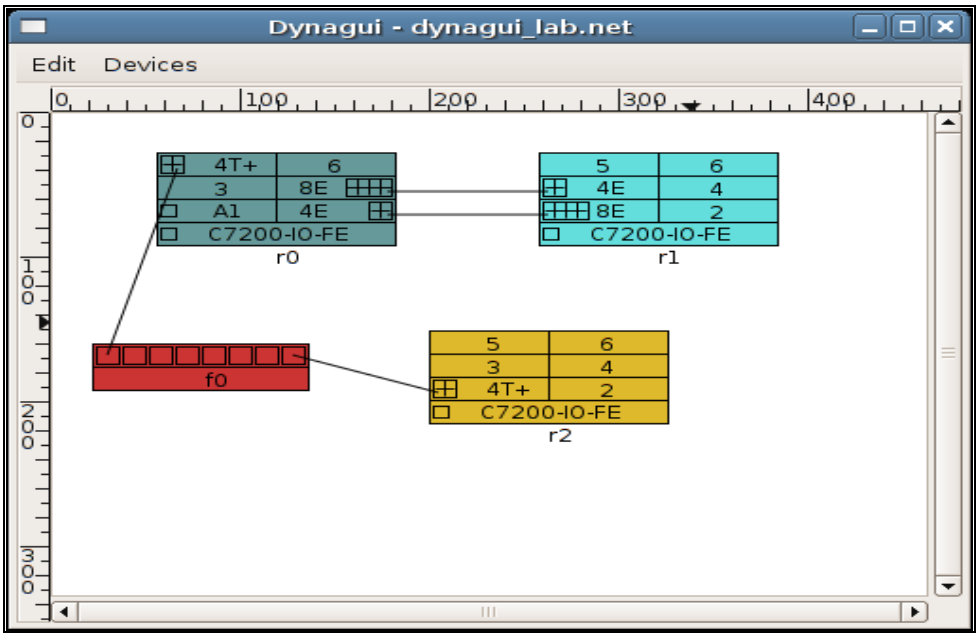


Figura 5.3 Dynagui.

5.2 Simulación del servicio L3MPLS VPN

Como se menciono anteriormente L3 MPLS VPN es una de las aplicaciones predominantes hoy en día, ya que ofrece muchas ventajas a sus clientes como conectividad total ente sitios y soporte de aplicaciones de tiempo real (voz, video, y etc.). En esta sección utilizaremos una herramienta que nos permitirá simular y explicar las bases que han justificado este trabajo, donde aseveraremos en la práctica la teoría antes mencionada.

5.2.1 Objetivos

Los objetivos planteados para la simulación de este servicio son:

1. Presentar un esquema o escenario práctico que cumplan con las características de una red real, para el entendimiento de la tecnología L3 MPLS VPN.
2. Esquematizar un plan de desarrollo que muestre los requerimientos necesarios para el establecimiento de una red L3 MPLS VPN.
3. Analizar y justificar cada una de las ventajas de esta tecnología presentada desde el punto de vista de un ISP a sus clientes y viceversa.

4. Incentivar al lector a que presente nuevos servicios que se pueden ofrecer en base a esta tecnología.

5.2.2 Escenario a simular

En un mundo globalizado donde las distancias ya no es un inconveniente para la comunicación entre personas, las redes privadas virtuales forman un factor tecnológico importante dando la posibilidad de establecer la seguridad y fidelidad como una comunicación cara a cara. Cada red presenta un escenario diferente de acuerdo a las características demandadas de servicio y trafico. Se han venido aplicado tecnologías de redes virtuales como Frame Relay, ATM e IP que como se menciono tienen varias dificultades.

A continuación presentamos un escenario actual de una red hub-spoke donde se utiliza la red del Proveedor de Internet (ISP), y tecnologías de tunneling IPIP o VPN con IPsec para establecer la comunicación directa entre tres sitios remotos brindando cierto independencia y seguridad.

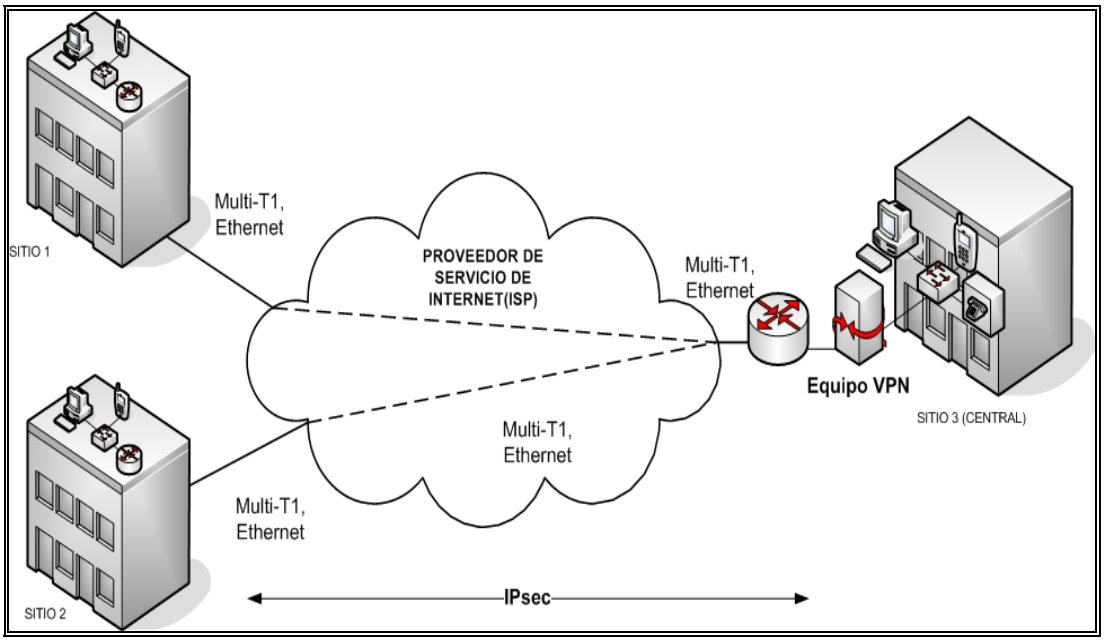


Figura 5.4 Escenario de una red privada virtual aplicando IPsec.

Como se observa en este escenario cada conexión o túnel de la VPN requiere recurso físico en proporción al número de sucursales clientes necesarios, presentando inconvenientes en escalabilidad y flexibilidad a la hora de la implementación. Por tales motivos las tecnologías evolucionaron para mitigar esta problemática, diseñando topologías y protocolos acordes a los requerimientos, cumpliendo con los objetivos de nuestro trabajo y apoyándonos en la tecnología de MPLS nosotros presentamos el siguiente modelo mejorado, justificado en el Capitulo 1.

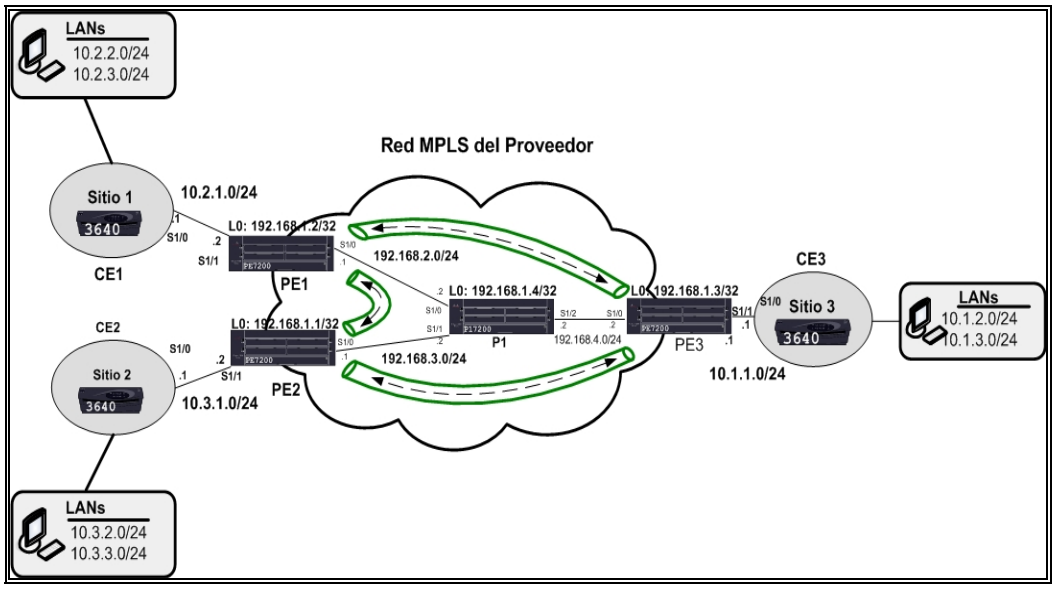


Figura 5.5 Escenario L3 MPLS VPN.

En este escenario instalaremos una topología mallada entre varios sitios de una VPN que se sujeta en un núcleo (backbone) MPLS con sus principales elementos como los ruteadores fronteras (PEs), ruteadores clientes (CEs) y ruteadores del proveedor (Ps) que instalados entre enlaces físicos y de acceso establecemos una L3 MPLS VPN full mesh. Con este escenario y su nomenclatura a partir de este momento referiremos los pasos a seguir para el establecimiento de la VPN.

Como observamos tenemos un cliente con tres sitios remotos (Sitio 1, 2, 3) cada sitio tiene sus redes LAN establecidas, el cliente requiere tener conexión entre sus sucursales a través del la red del proveedor (ISP) para ello procederemos con el siguiente plan de configuración.

5.2.3 Desarrollo del escenario

Para llevar acabo la implementación de L3 MPLS VPN hemos segmentado los procesos en los siguientes bloques:

1. Direccionamiento IP.
2. Enrutamiento IGP.
3. Activación de MPLS.
4. Configuración de BGP.
5. Definición VPN VRF y sus Atributos.
6. Redistribución de las Rutas.

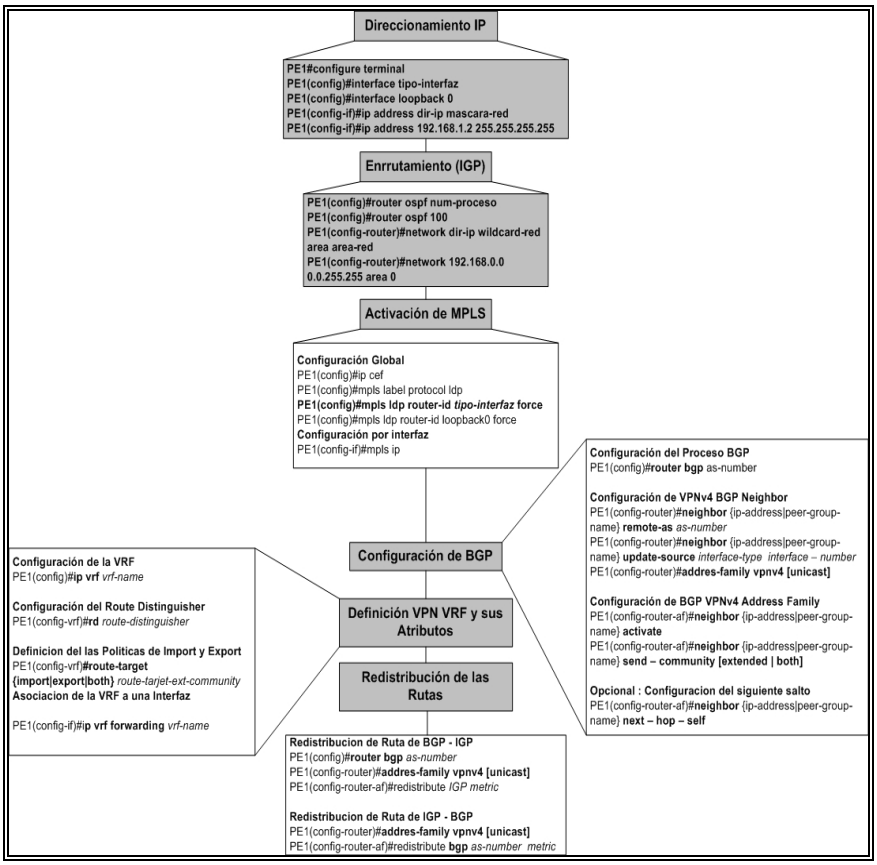


Figura 5.6 Plan de Implementación de L3 MPLS VPN.

Cada bloque mencionado es detallado y justificado en las siguientes secciones.

5.2.3.1 Direccionamiento IP

El direccionamiento de nuestro escenario utiliza el protocolo IPv4, que es un protocolo de manejo convencional y generalizado sin embargo presentamos una breve referencia de su configuración.

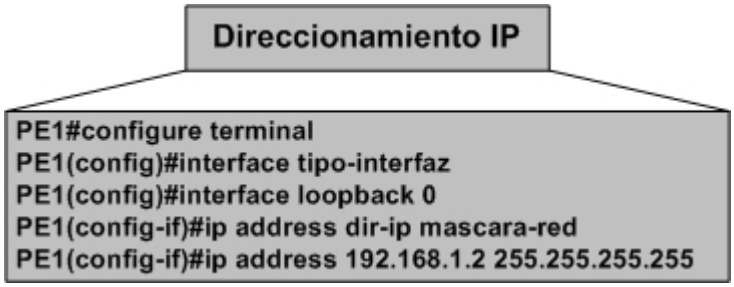


Figura 5.7 Direccionamiento IP.

La figura 5.2 muestra el esquema de direccionamiento utilizado para nuestro escenario el cual puede ser adaptado a las diferentes situaciones según convenga considerando que podemos tener sobrecarga entre direcciones de los clientes VPNs entre otras ventajas mencionadas en la sección 3.3.1.

En este punto es importante las direcciones loopback aplicadas al núcleo (backbone) ya que mas adelante servirán como identificadores (IDs) para las secciones LDP y BGP.

Las loopback establecidas en los ruteadores son utilizadas como LDP ID ya que son interfaces lógicas que siempre están activas, pero cave mencionar que también pueden afectar al proceso de establecimiento LDP por lo tanto es importante configurar a los ruteadores tipo P para que no acepten actualizaciones BGP. En el ruteador P1 de nuestro escenario configuramos el comando ***no mpls ldp advertise-labels*** para deshabilitar a que este

ruteador procese actualizaciones LDP y con el comando ***mpls label advertise –labels for 10*** habilita a que procese actualizaciones ldp dirigidas a las interfaces loopback de los ruteadores tipo P.

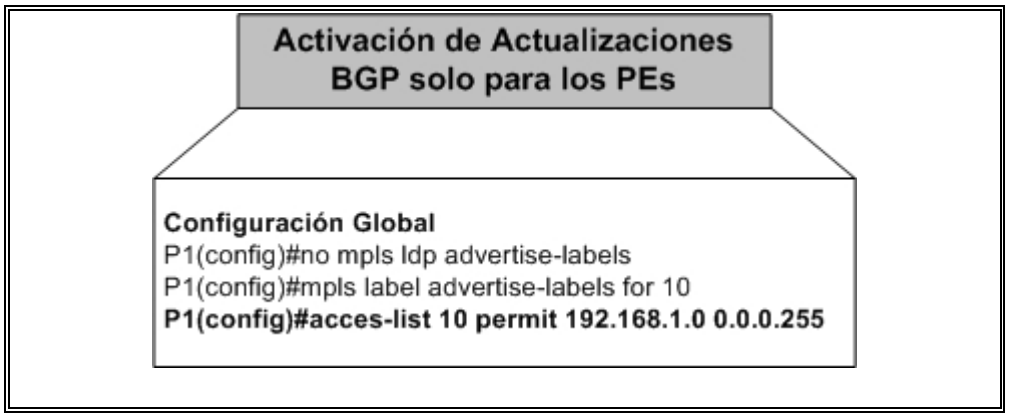


Figura 5.8 Activación de actualizaciones BGP solo en los rutedores PEs.

Una vez configurado el direccionamiento procedemos a la configuración del protocolo de enrutamiento IGP.

5.2.3.2 Enrutamiento IGP

Si nos referimos a la red del proveedor que en este caso es el núcleo (backbone) formado por los dispositivos PE y P utilizaremos el protocolo OSPF, ya que este protocolo permitirá mas adelante tener aplicaciones como MPLS TE. Otro protocolo que puede ser utilizado es IS-IS.

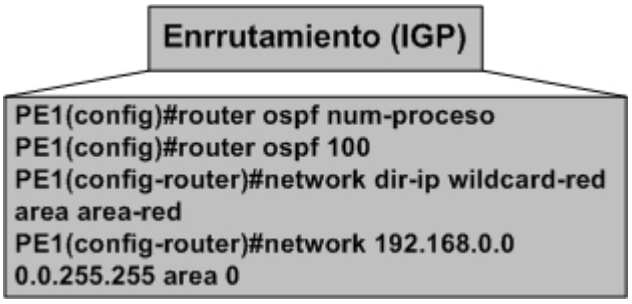


Figura 5.9 Configuración del protocolo de enrutamiento IGP.

En la figura se muestra los comandos básicos para la configuración del protocolo IGP la cual inicialmente la aplicaremos en los ruteadores PE1, PE2, P1, y PE3.

En el caso de las redes formadas entre el cliente y el proveedor (CEs y PEs) aplicaremos el protocolo RIPv2 por ser un protocolo ligero y simple sin embargo pueden ser aplicadas otras alternativas como (RIPv2, EIGRP, OSPF, eBGP).

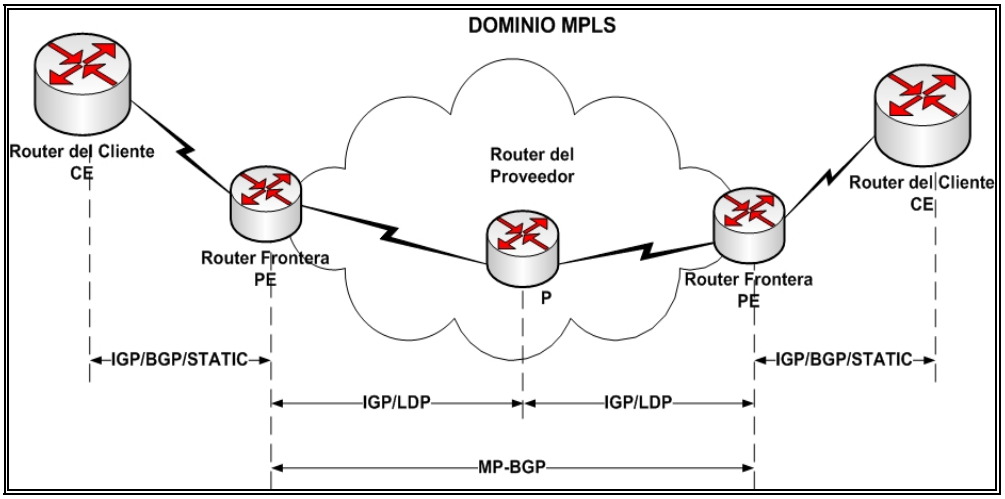


Figura 5.10 Implementación de los protocolos IGPs.

Una vez establecido los protocolos IGPs podemos anunciar que existe conectividad en el núcleo (backbone) IP y conectividad entre CEs a PEs en cada extremo. Ahora que tenemos conectividad procederemos a la activación del protocolo MPLS en el núcleo (backbone) del ISP.

5.2.3.3 Activación del protocolo MPLS

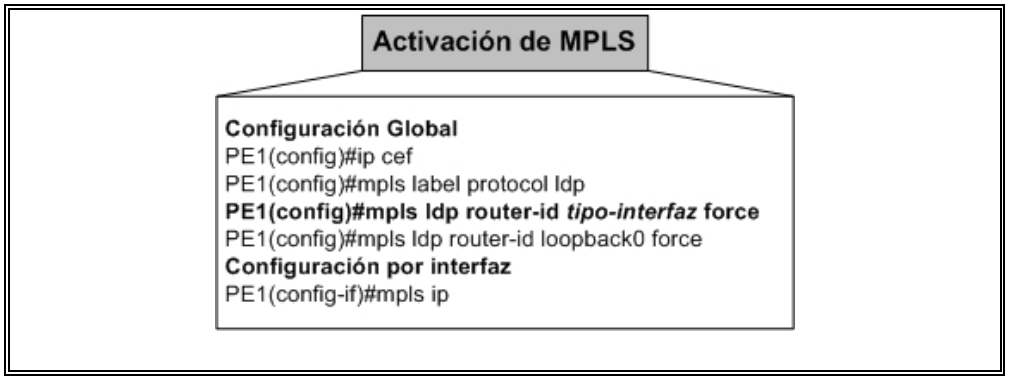


Figura 5.11 Activación del protocolo MPLS.

La activación de MPLS en el núcleo (backbone) de nuestro escenario radica en generar un proceso que permita realizar las operaciones de imposición y disposición de las etiquetas MPLS y este proceso se logra habilitando IP CEF (Cisco Express Forwarding) utilizando el comando ***ip cef*** puede ser habilitado de forma global o por interfaz***.*** Luego es necesario un protocolo que distribuya estas etiquetas y aquí tenemos alternativas como LDP, TDP, o RSVP. En nuestro trabajo utilizaremos el protocolo LDP por ser el de

mayor despliegue. En la figura 5.8 mostramos la configuración para el ruteador PE1, esta configuración es similar en los ruteadores PE2, PE3 y P1.

Finalmente activamos el protocolo MPLS en las interfaces que forman el dominio MPLS con el comando ***mpls ip***.

En este punto ya tenemos activado el dominio MPLS junto con sus tablas en el Canal de Control (Tabla RIB, LIB) y Canal de Datos (LFIB). Ahora es necesario la conectividad entre los sitios del Cliente lo cual inicia con la configuración del protocolo BGP.

5.2.3.4 Configuración de BGP

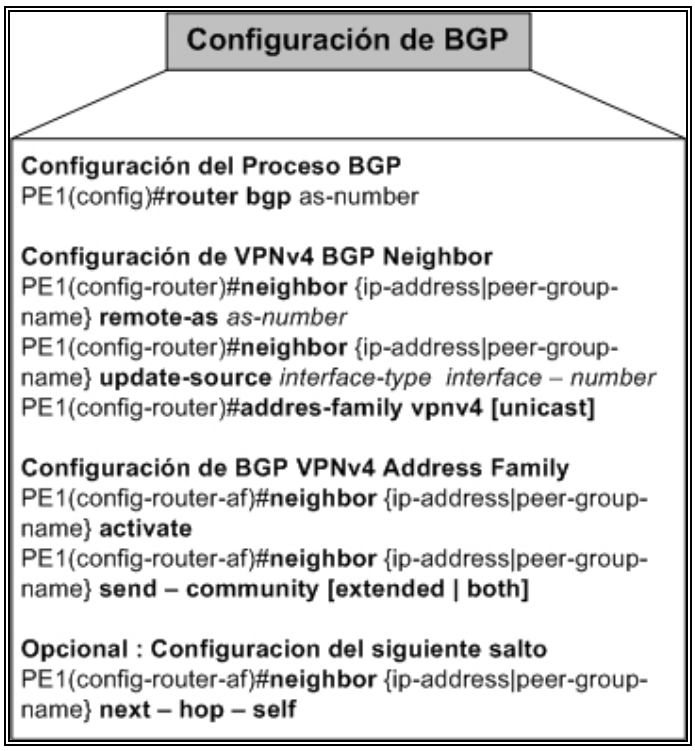


Figura 5.12 Configuración de BGP.

Esta configuración tiene como objetivo intercambiar las rutas VPNv4 con los ruteadores PE's o Ruteadores Reflectores. Para lo cual es necesario los siguientes pasos.

1. Configuración del Proceso BGP.
2. Configuración de VPNv4 BGP Neighbor.
3. Configuración de BGP VPNv4 Address Family.
4. Opcional: Configuración del siguiente salto.

El primer comando requerido para la configuración de BGP entre los ruteadores PE es el número del sistema autónomo. Con este comando habilitamos BGP. Luego usamos el comando ***no synchronization*** para habilitar o deshabilitar sincronización entre BGP e IGP. Usamos el comando **neighbor** *ip-addres* **remote-as** *autonomous-system-number* y **neighbor** *ip-addres* **update-source** *interface* para designar cual es el vecino PE o ruteador reflector de donde se reciben los mensajes y actualizaciones BGP en este caso las interfaces utilizadas para identificar los destinos de las actualizaciones son las interfaces loopback ya que siempre están activas.

El comando **address-family vpnv4** es usado para designar el modo del prefijo vpn versión 4 a utilizar. El ruteador PE remoto es activado para intercambiar rutas VPNv4 con el comando **neighbor** *ip-addres* **activate.**

Finalmente utilizamos el comando **neighbor** *ip-address* **send-community extended** para habilitar el envío de extensiones de BGP donde se incluyen RT. Este comando es configurado por defecto por cada vecino que activa el intercambio de rutas VPNv4.

Una vez establecida las rutas entre los ruteadores PE's iniciaremos la creación de las VRF.

5.2.3.5 Definición de las VPNs VRFs y sus Atributos

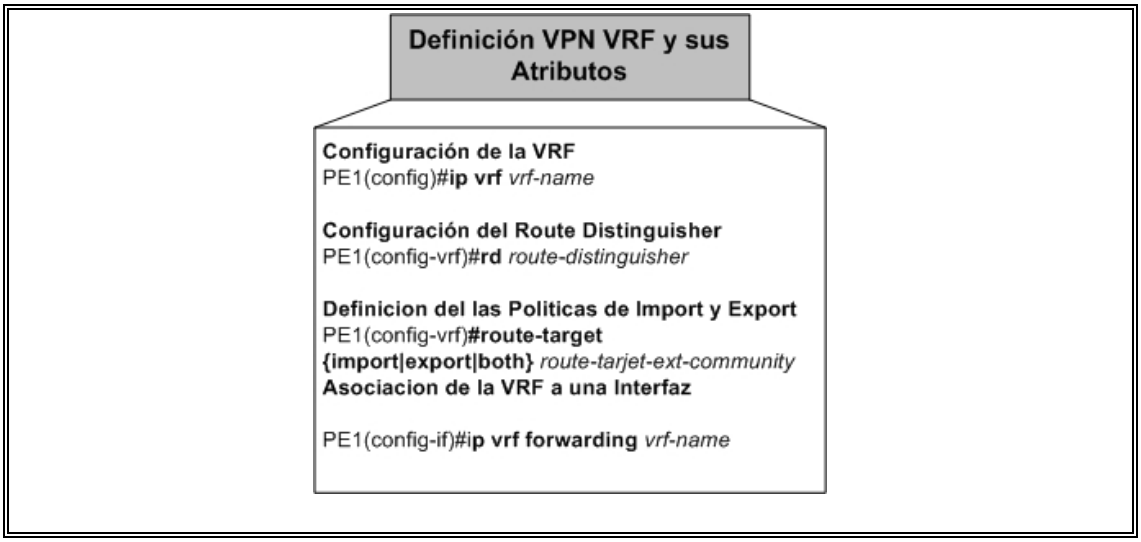


Figura 5.13 Definición de las VPNs VRFs y sus Atributos.

Para la creación de las VRFs consideramos los siguientes pasos:

1. Configuración de la VRF.
2. Configuración del Route Distinguisher.
3. Definición del las Políticas de Import y Export.
4. Asociación de la VRF a una Interfaz.

Configuración de la VRF consiste en utilizar el comando **ip vrf** *vrf-name* para designar el nombre que se utilizara para la VRF, el cual tiene significado local(a menudo se utiliza el mismo nombre en todas las VRF por este motivo).

Configuración del Route Distinguisher como se menciono anteriormente utilizamos RD como dirección global única y evitar la sobrecarga ip, utilizamos el comando **rd** *route-distinguisher* que es la dirección VPNv4 de la tabla de VPN VRF.

Definición del las Políticas de Import y Export Configuramos el RT para controlar la importación y exportación de rutas dentro de la apropiada VRF. Para ello utilizamos el comando **route-target [import | export | both]** *route-target-ext-community. (*En la conectividad de malla a menudo RT y RD son idénticos en una VPN).

Una vez configuradas las VRFs y asociadas a las interfaces el plano de control ya esta casi listo, finalmente es hora de redistribuir esta información entre los PEs y CEs.

Asociación de la VRF a una Interfaz luego de configurar las VRF podemos asociar las interfaces que están conectadas a los ruteadores PEs y CEs con la VRF. Utilizamos el comando **ip vrf forwarding** *vrf-name.*

5.2.3.6 Redistribución de Rutas PE-CE.

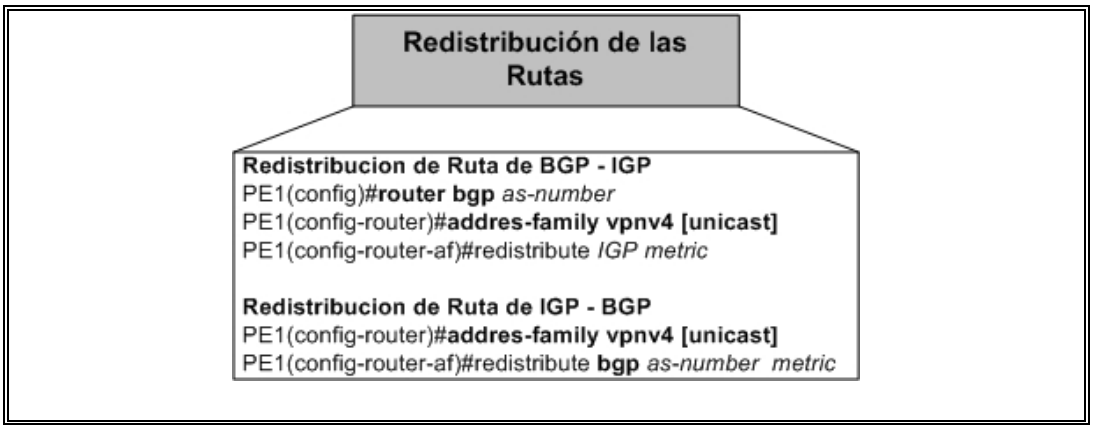


Figura 5.14 Redistribución de Rutas.

Finalmente procedemos redistribuir las rutas entre los sitios remotos, tanto la información VPN como la información de ruteo de los clientes.

Los comandos utilizados son **redistribute** *IGP metric* y **redistribute** *bgp as-number metric* .Estos comandos son aplicables en los ruteadores PE1, PE2 y PE3.

Cumpliendo con nuestro plan de implementación donde ya establecido los Canales de Control y Datos con sus entidades como VRFs, RIB, LIB y LFIB procederemos al análisis de resultados de la simulación.

5.2.4 Resultados

En esta sección nos centraremos en la verificación de los resultados y al análisis de las tablas formadas para obtener el funcionamiento de L3 MPLS VPN.

5.2.4.1 Resultados de Configuración del Enrutamiento IGP

Una vez configurado el protocolo IGP en el núcleo (backbone) IP se inicia el proceso de convergencia OSPF llegando a establecerse la conectividad entre vecinos. A continuación mostramos la tabla de ruteo (RIB) formada en el ruteador PE1 que es similar a la de los ruteadores PE2 y PE3 (Apéndice).

```
PE1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O    192.168.4.0/24 [110/128] via 192.168.2.2, 00:05:01, Serial1/0
     192.168.1.0/32 is subnetted, 4 subnets
O       192.168.1.1 [110/129] via 192.168.2.2, 00:05:01, Serial1/0
O       192.168.1.3 [110/129] via 192.168.2.2, 00:05:01, Serial1/0
C       192.168.1.2 is directly connected, Loopback0
O       192.168.1.4 [110/65] via 192.168.2.2, 00:05:01, Serial1/0
C    192.168.2.0/24 is directly connected, Serial1/0
O    192.168.3.0/24 [110/128] via 192.168.2.2, 00:05:01, Serial1/0
```

Figura 5.15 Tabla de Enrutamiento o RIB formada en el ruteador PE1.

La tabla muestra las rutas alcanzables por el ruteador PE1 que con la respectiva prueba de conectividad obtenemos.

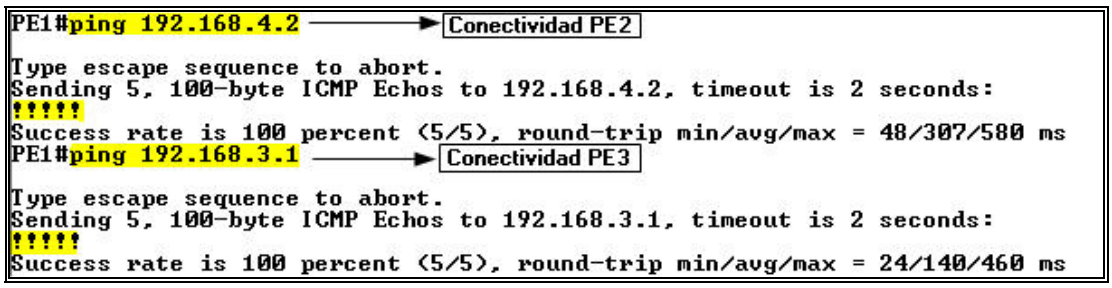


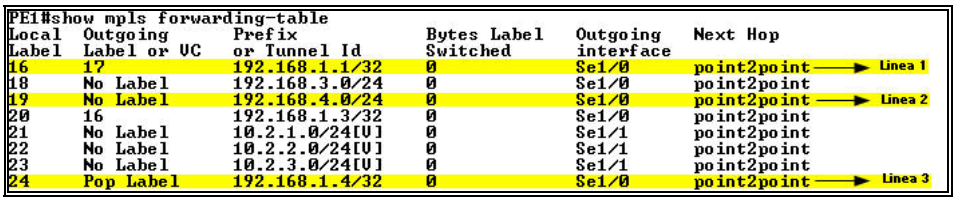
Figura 5.16 Conectividad entre ruteadores PE's.

5.2.4.2 Resultados de la Activación del protocolo MPLS

Cuando activamos MPLS, el protocolo de distribución de etiquetas automáticamente empieza a asignar y distribuir las etiquetas entre los PEs y Ps, el modo de distribución de etiquetas por defecto es el de *Demanda sin solicitud hacia abajo*.

La tabla LFIB como se menciono anteriormente se encuentra en el Canal de Datos donde se mapean las etiquetas a FECs respectivamente.

Tabla LFIB formada en el ruteador PE1 es la siguiente:



```
PE1#show mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     17            192.168.1.1/32   0             Se1/0       point2point ---> Linea 1
18     No Label      192.168.3.0/24   0             Se1/0       point2point
19     No Label      192.168.4.0/24   0             Se1/0       point2point ---> Linea 2
20     16            192.168.1.3/32   0             Se1/0       point2point
21     No Label      10.2.1.0/24[V]   0             Se1/1       point2point
22     No Label      10.2.2.0/24[V]   0             Se1/1       point2point
23     No Label      10.2.3.0/24[V]   0             Se1/1       point2point
24     Pop Label     192.168.1.4/32   0             Se1/0       point2point ---> Linea 3
```

Figura 5.17 Tabla LFIB del ruteador PE1.

En esta tabla podemos observar tres tipos de etiquetas, la etiqueta normal que se asigna cuando se realiza la operación de intercambio (swapping), etiqueta de Retiro (Pop Label) y la etiqueta sin etiqueta (Untagged).

En la línea 1 observamos que si un paquete ingresa con una etiqueta 16 con destino al FEC: 192.168.1.1, el LER o PE1 realizaría la operación de cambio de etiqueta por la etiqueta 17 y saldría por la interfaz S1/0.

En la línea 2 observamos que si un paquete ingresa con una etiqueta 19 dirigida al FEC 192.168.4.0/24 el ruteador PE1 no asignara ninguna etiqueta tan solo enviara el paquete a la correspondiente dirección ip destino.

En la línea 3 observamos que si un paquete ingresa con una etiqueta 24 dirigida al FEC 192.168.1.4 se debería intercambiar a una etiqueta nula implícita (3) que indica realizar la operación de retirar o eliminar la etiqueta a este paquete.

A continuación presentaremos un ejemplo donde detallaremos el proceso MPLS:

Enviaremos un paquete IP desde el ruteador PE1 (192.168.2.1) al ruteador PE3 (192.168.1.3), el paquete sale de la interfaz se1/0 con la etiqueta 16, luego ingresa al ruteador P1 y según la tabla LFIB P1 (Penúltimo hop popping) este realizar la operación de popping y envía el paquete por la se1/0 sin etiqueta, el ruteador PE1 recibe el paquete IP y lo rutea de acuerdo a la tabla RIB al ruteador PE1.

Entonces anunciamos que cumplimos con nuestro objetivo de tener el domino MPLS establecido ahora veamos los resultados obtenidos después de la configuración VPN.

5.2.4.3 Resultados de la Configuración de la VPN

Una vez establecidas las VRFs y la configuración de los parámetros RD y RT procedemos a verificar las tablas formadas a continuación:

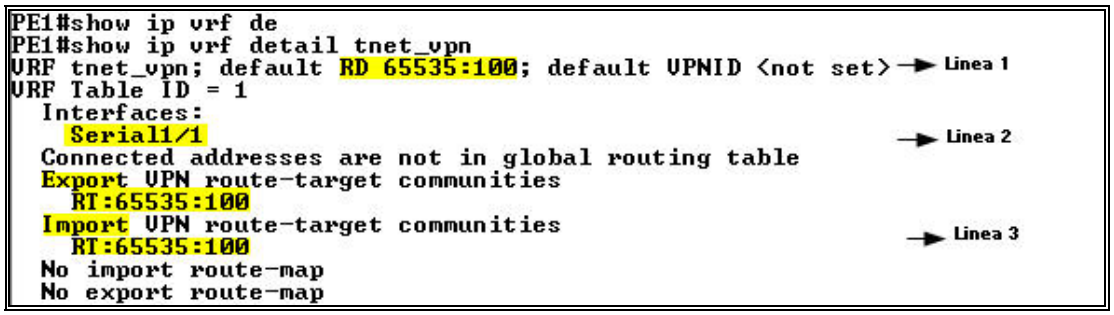
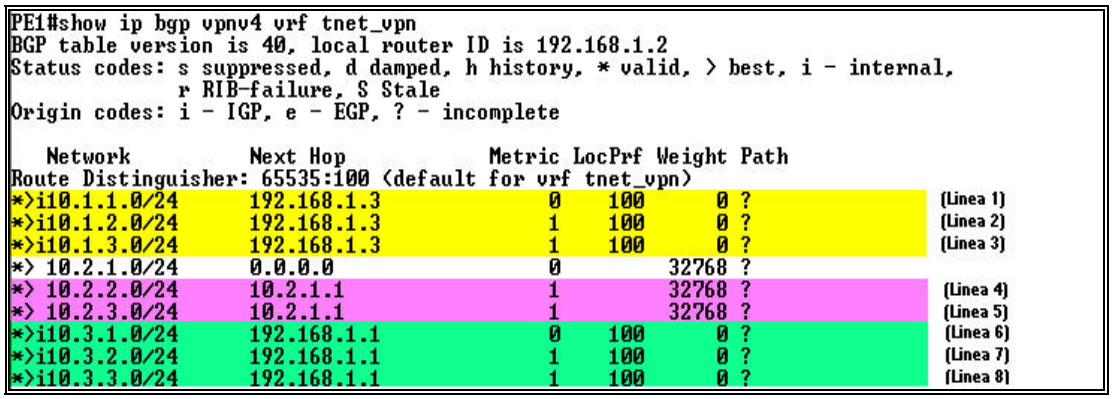


Figura 5.18 Verificación de la configuración VRF.

El comando que utilizamos para verificar la configuración de la VRF es ***show ip vrf detail*** donde podemos verificar el nombre de la vpn, la interfaz asociada a la vrf (Línea 2) y la dirección RD y RT (Línea 3).

Las tabla VRFs restantes son idénticas tan solo se diferencia en la interfaz asociada a la VRF.

Luego de la redistribución de las rutas PE-CE y viceversa podemos verificar el intercambio de rutas MP-BGP con el comando ***show ip bgp vpnv4 vrf Command.***



```
PE1#show ip bgp vpnv4 vrf tnet_vpn
BGP table version is 40, local router ID is 192.168.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65535:100 (default for vrf tnet_vpn)
*>i10.1.1.0/24      192.168.1.3              0    100      0 ?     (Linea 1)
*>i10.1.2.0/24      192.168.1.3              1    100      0 ?     (Linea 2)
*>i10.1.3.0/24      192.168.1.3              1    100      0 ?     (Linea 3)
*> 10.2.1.0/24      0.0.0.0                  0         32768 ?
*> 10.2.2.0/24      10.2.1.1                 1         32768 ?    (Linea 4)
*> 10.2.3.0/24      10.2.1.1                 1         32768 ?    (Linea 5)
*>i10.3.1.0/24      192.168.1.1              0    100      0 ?     (Linea 6)
*>i10.3.2.0/24      192.168.1.1              1    100      0 ?     (Linea 7)
*>i10.3.3.0/24      192.168.1.1              1    100      0 ?     (Linea 8)
```

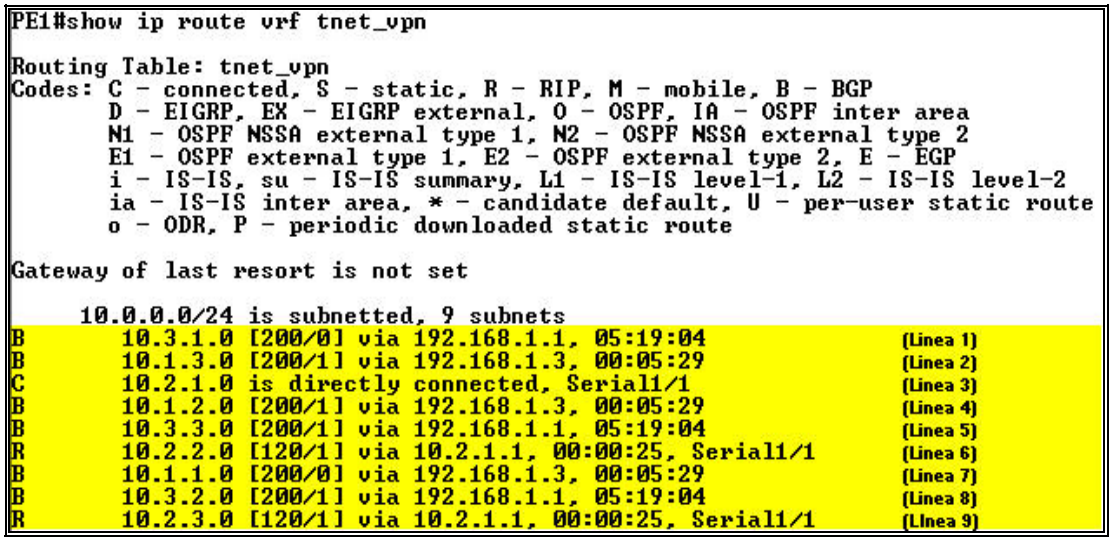
Figura 5.19 Verificación de la VRF VPN.

Desde la Línea 1 a 3 muestra las rutas VRF tnet_vpn señaladas por el ruteador PE3. Notemos que el siguiente salto a las rutas es la interfaz loopback 192.168.1.3 que es la fuente de actualizaciones BGP, estas rutas junto a la correspondiente etiqueta MPLS asignada podemos enviar el trafico VPN a los clientes.

Las líneas 4 y 5 muestras las rutas VPN redistribuidas por MP-BGP en el ruteador local.

En las líneas 6 a 8 contienen las rutas VRF tnet_vpn señaladas por el ruteador PE2. De forma similar las actualizaciones BGP son recibidas desde la interfaz loopback 192.168.1.1.

También podemos verificar la tabla de ruteo VRF usando el comando ***show ip route vrf.***



```
PE1#show ip route vrf tnet_vpn

Routing Table: tnet_vpn
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 9 subnets
B       10.3.1.0 [200/0] via 192.168.1.1, 05:19:04          (Linea 1)
B       10.1.3.0 [200/1] via 192.168.1.3, 00:05:29          (Linea 2)
C       10.2.1.0 is directly connected, Serial1/1           (Linea 3)
B       10.1.2.0 [200/1] via 192.168.1.3, 00:05:29          (Linea 4)
B       10.3.3.0 [200/1] via 192.168.1.1, 05:19:04          (Linea 5)
R       10.2.2.0 [120/1] via 10.2.1.1, 00:00:25, Serial1/1  (Linea 6)
B       10.1.1.0 [200/0] via 192.168.1.3, 00:05:29          (Linea 7)
B       10.3.2.0 [200/1] via 192.168.1.1, 05:19:04          (Linea 8)
R       10.2.3.0 [120/1] via 10.2.1.1, 00:00:25, Serial1/1  (Linea 9)
```

Figura 5.20 Rutas clientes VPN.

Las líneas 2, 4, y 7 muestra las rutas VPN clientes señalizadas por el ruteador PE3 (192.168.1.3) usando MP-BGP en la VRF tnet_vpn. De la misma forma las líneas 1, 5, y 8 muestra las rutas VPN clientes señalizados por el ruteador PE2 (192.168.1.1). También observamos que en las líneas 6 y 9 se muestran las rutas vpn clientes señalizadas por el ruteador local PE1 obtenidas de las rutas originadas por el protocolo RIP configurado entre PE1-CE1.

En adición y a manera de verificación de una de las desventajas de MPLS es el problema del máximo MTU permitido sin fragmentar en el núcleo (backbone) MPLS.

Para ello realizamos las siguientes pruebas asiendo uso del comando ping:
Inicialmente realicemos una prueba con un paquete cuya MTU sea de 1500 sin fragmentar desde el ruteador PE1

5.2.5 Conclusiones

Una vez que se mostraron los resultados obtenidos, el servicio de L3 MPLS ya se estableció por tales motivos concluimos:

El escenario práctico planteado cumple con las características de una red real, pues pudimos observar cada detalle de la tecnología L3 MPLS VPN.
El plan de desarrollo cumple con los requerimientos necesarios para el establecimiento de la red L3 MPLS VPN.

L3 MPLS VPN es un servicio que no presenta inconvenientes a la hora de añadir nuevos clientes, pues no es necesario la reconfiguración de toda la red pues tan solo con modificar el ruteador frontera entre el cliente y la red del proveedor podemos añadir una nueva VPN justificando la escalabilidad de L3 MPLS VPN.

L3 MPLS VPN necesita generalmente soporte de ruteo a nivel de los CPEs lo que encarece la solución del lado del cliente, aunque hoy en día un

soporte de protocolos de enrutamiento a nivel de CPE es muy común ya que la mayoría de fabricantes de ruteadores le dan soporte al mismo integrado en el equipo.

5.3 Simulación del servicio L2MPLS VPN

En esta sección desarrollaremos la simulación del servicio de L2MPLS VPN, conocido como AToM o pseudocable MPLS.

Como vimos, el servicio AToM brinda el encapsulamiento de circuitos de capa 2 como por ejemplo Frame Relay, ATM, Ethernet, PPP, etc, sobre un núcleo (backbone) MPLS. Así también vimos que el protocolo de capa 2 principal que se usa para el transporte de datos es el Ethernet, por lo cual va a ser cuestión de nuestro estudio. A este servicio de encapsular un circuito de capa 2 tipo ethernet sobre una red MPLS se lo conoce como Ethernet sobre MPLS o por sus siglas en inglés EoMPLS (Ethernet over MPLS) y así lo conoceremos en adelante.

5.3.1 Objetivos

Los objetivos planteados para la simulación de este servicio son:

1.- Comprobar la independencia en L3 del la red del cliente con la red del proveedor usando el servicio de L2MPLS VPN.

2.- Determinar y comprobar en base a la simulación las ventajas y desventajas de disponer del servicio de L2MPLS VPN.

3.- Determinar la importancia para un ISP en proveer el servicio de L2MPLS VPN a sus clientes.

5.3.2 Escenario a simular

El propósito del análisis de las tecnologías de red que vimos en el capítulo 1, fue identificar de una manera global las tecnologías con las que cuenta un ISP para poder cubrir las necesidades actuales como empresa de servicios portadores. En base a los criterios previamente analizados, y considerando las partes más importantes de diseño, hemos diseñado un núcleo (backbone) práctico, ideal para la simulación del servicio de L2MPLS VPN el cual lo podemos apreciar a continuación.

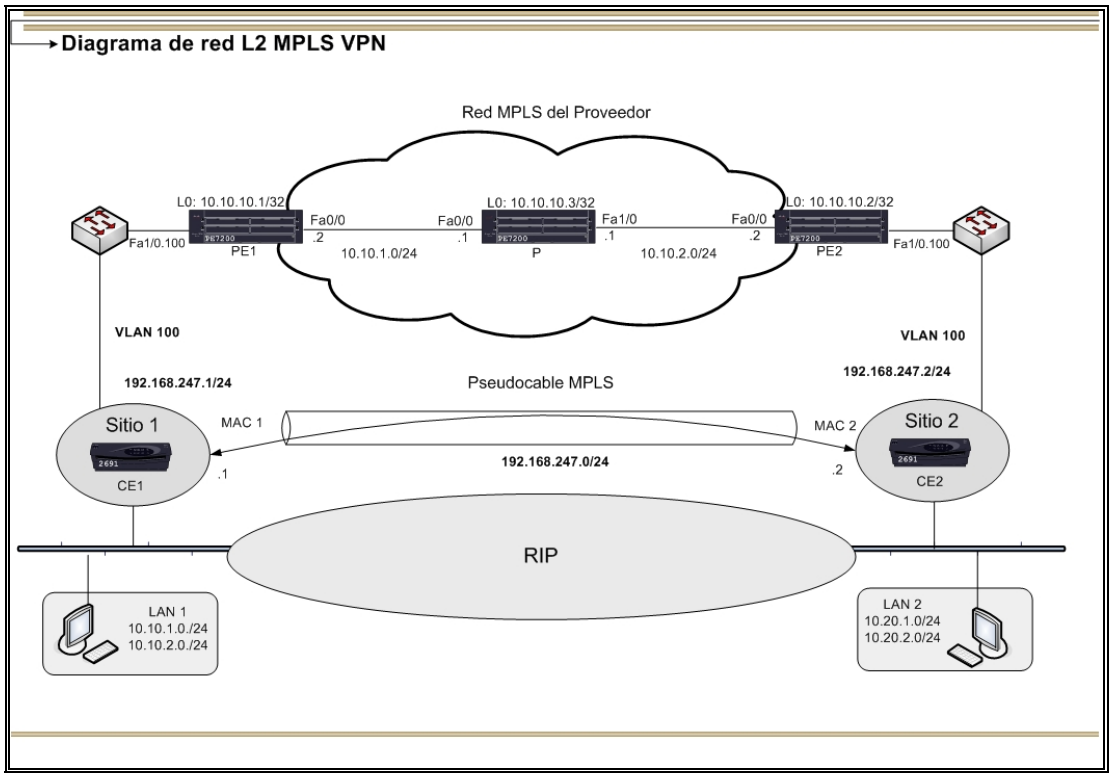


Figura 5.21 Simulación del servicio L2MPLVPN.

Como vimos en el capítulo 4, el servicio de L2MPLS VPN nos permite emular varios servicios de capa 2 sobre un núcleo (backbone) MPLS. Sin embargo la tendencia tecnológica nos indica que los circuitos de uso más común son sobre ethernet, razón por la cual será nuestro caso de ejemplo a simular como un servicio de pseudocable ethernet en una red MPLS.

Dado que la relación del cliente con el proveedor en un servicio L2MPLS VPN se da solo en la capa de enlace de datos, es imposible separar cada uno de los clientes a nivel IP, razón por la cual, parecería necesario disponer

de una interfaz ethernet en nuestro PE por cada cliente que se le brinde el servicio de pseudocable MPLS.

El servicio de emulación de un circuito ethernet sobre un núcleo (backbone) MPLS nos permite separar cada uno de los circuitos de los clientes por medio del encapsulamiento ieee802.1q o más conocido como VLANs. Para complementar nuestro núcleo (backbone) MPLS con soporte de pseudocables MPLS encapsulados con 802.1q, necesitamos conectar una red L2 de equipos que soporten este encapsulamiento, típicamente se usan conmutadores (switches) con soporte de VLANs, sobre los cuales se propagan la información de VLANs desde el cliente al ISP.

Con el uso del simulador seleccionado y con un equipamiento de fácil acceso, vamos a proceder a simular el servicio de L2MPLS VPN.

5.3.3 Desarrollo del escenario

A continuación vamos a analizar los pasos que debemos seguir para poder simular el servicio de L2MPLS VPN en nuestro núcleo (backbone) simulado de equipos CISCO con el Dynamips, es importante tomar en cuenta que para haber llegado a este escenario de simulación, hemos pasado por el

análisis de cada una de las partes que conforman o son parte de la red de un ISP.

Los pasos que vamos a seguir para levantar este servicio los describimos a continuación.

Primeramente vamos establecer el direccionamiento IP referente a la topología mostrada según un esquema de direccionamiento previamente diseñado, luego vamos configurar el protocolo de enrutamiento interno o IGP que se va a encargar de dar conectividad total a nuestra red a nivel de capa 3, con esto, vamos a permitirnos levantar el protocolo MPLS en los equipos de núcleo (backbone) para que se puedan establecer los LSP y posteriormente habilitar el servicio de L2MPLS VPN en los equipos de borde o PEs de la red del proveedor. Posterior a la configuración, analizaremos el resultado de las configuraciones propuestas tanto a nivel del proveedor como a nivel del ISP para así poder cumplir nuestro objetivo dando las conclusiones de nuestra simulación. Lo que hemos mencionado lo podemos apreciar en la figura a continuación.

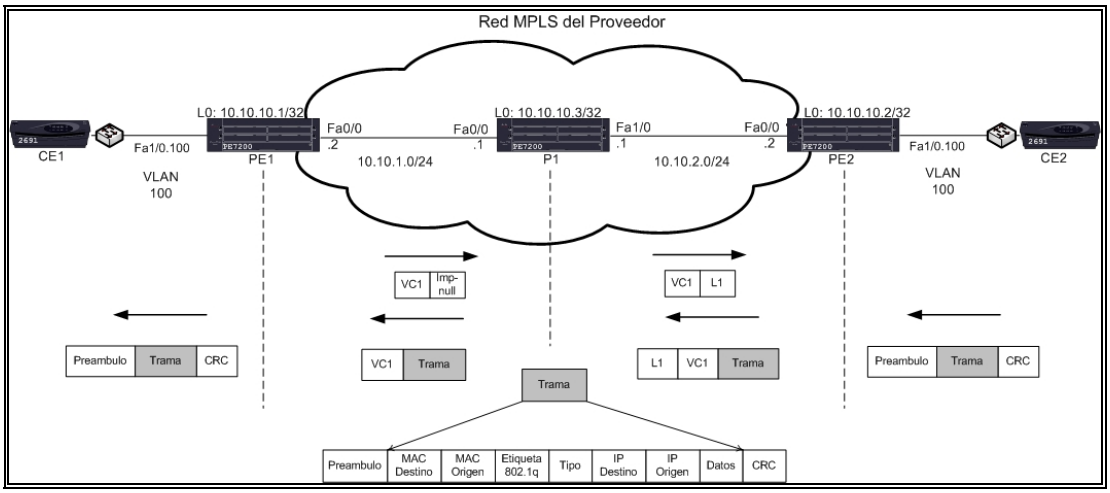


Figura 5.22 Intercambio de paquetes en EoMPLS.

La configuración del servicio EoMPLS seguirá el esquema propuesto anteriormente, para lo cual hemos separado esta configuración en 4 procedimientos bien definidos, los cuales los podemos apreciar en el siguiente diagrama.

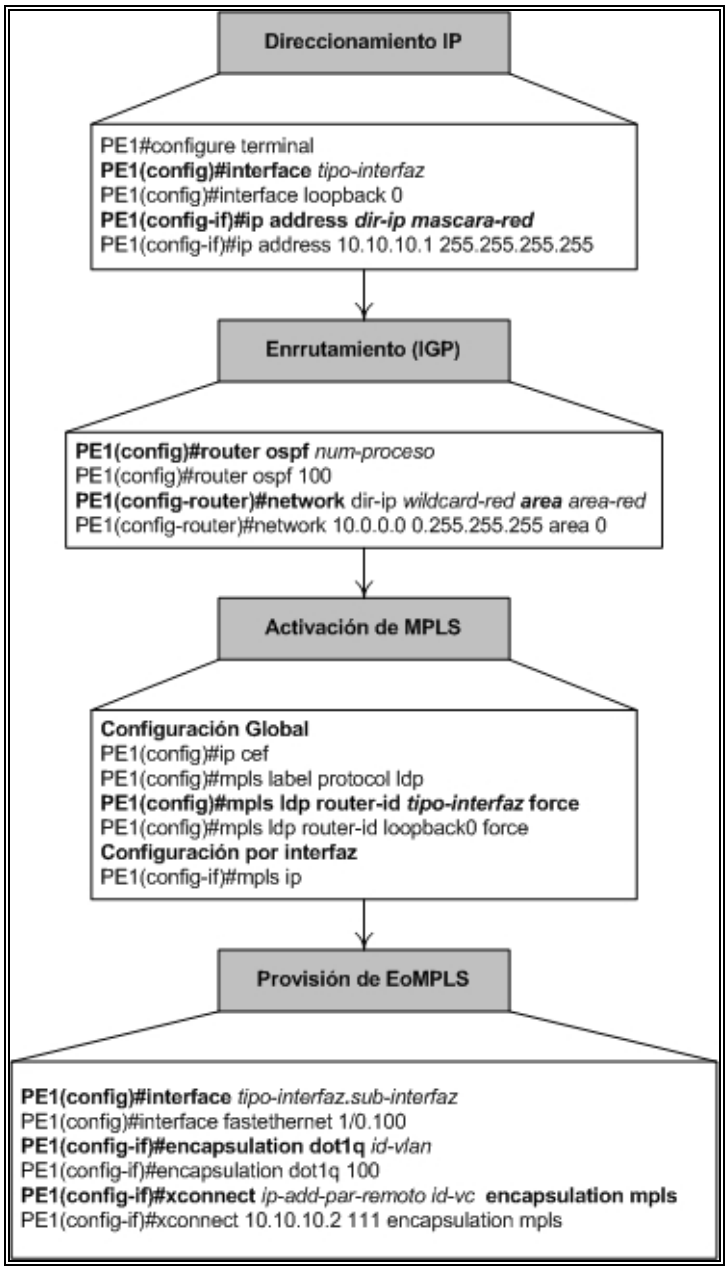


Figura 5.23 Configuración de EoMPLS.

Para entender el esquema de configuración del servicio de EoMPLS sobre un núcleo (backbone) de equipamiento CISCO, vamos a explicar paso a paso cada una de las fases de configuración de los equipos involucrados a

nivel del proveedor. Cabe recalcar que a nivel del cliente, no es necesaria ninguna configuración con relación al proveedor, es más veremos posteriormente que tiene independencia total del mismo.

5.3.3.1 Configuración del direccionamiento IP

El direccionamiento IP es esencial todo núcleo (backbone) IP/MPLS, debido que es el protocolo universal de comunicación de redes de computadoras. Antes de configurar cualquier topología sobre un núcleo (backbone) de un portador de datos, es esencial definir un direccionamiento IP, considerando el crecimiento de la red y hacerlo lo más representativo posible, así tomará mucho menos tiempo resolver cualquier problema a nivel de capa 3(IP).

A continuación mostramos los comandos esenciales de configuración del protocolo IP sobre un equipo CISCO.

Figura 5.24 Configuración de direccionamiento IP.

El direccionamiento IP viene dado por dos partes principales que son: la configuración de las interfaces físicas y la configuración de las interfaces lógicas, ambas configuradas con el comando **ip address** usado en el modo de configuración de interfaz. El direccionamiento de las interfaces físicas, es usado para poder referenciar el equipamiento en forma física y poder intercomunicar los enlaces por los cuales van a pasar la información, estas pueden ser interfaces de cobre (Ethernet, FastEthernet) o de fibra óptica (POS). Las interfaces lógicas al contrario de las físicas, sirven como identificador del equipo a nivel de protocolos que pueden ser de enrutamiento como OSPF o de etiquetado como LDP. Es muy importante considerar ambos direccionamientos para el establecimiento de una red IP/MPLS por consideraciones de convergencia y de resolución de problemas. Estas consideraciones y configuraciones son aplicadas a todos los equipos del núcleo (backbone) del ISP.

5.3.3.2 Configuración del enrutamiento

El enrutamiento consiste en definir una forma de cómo propagar cada una de las redes que disponen o controlan los equipos de capa 3 (ruteadores) en la red del proveedor. Estas redes pueden ser usadas como identificación lógica o física de los equipos del ISP o redes asignadas a clientes. Así también un protocolo de enrutamiento, nos permite propagar rutas que no son nuestras sino que las aprendemos de otra red diferente a la nuestra, como es el caso del protocolo de enrutamiento externo BGP, cuya principal utilidad es para publicar las redes de grandes proveedores de Internet. Existen protocolos de enrutamiento dinámico y estático, siendo ambos muy comunes en la configuración de núcleo (backbone) de un ISP, el decidir que protocolo se va a implementar va a depender de muchos factores, entre los cuales podemos mencionar: recursos, capacidad, tecnología, capacidad técnica, escalabilidad. En nuestro caso, necesitamos un protocolo de rápida convergencia y fácil administración dado que vamos a simular un servicio sobre una red de un proveedor. Por estas razones, el protocolo más ideal para usarlo como IGP es el OSPF el cual cumple con todos los requerimientos a nuestra simulación.

A continuación veremos los comandos necesarios para la configuración de OSFP como IGP en un núcleo (backbone) de un ISP.

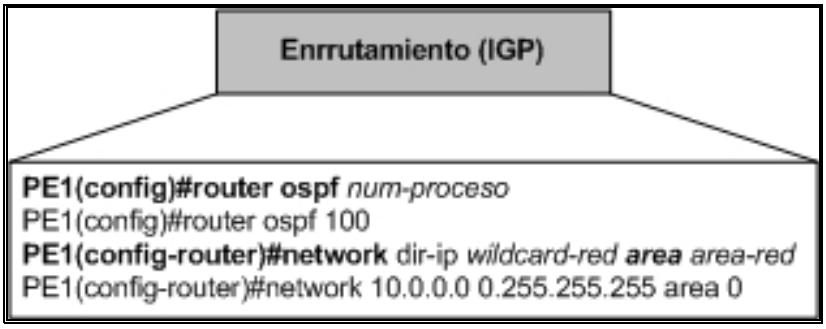


Figura 5.25 Configuración de IGP.

En el protocolo de enrutamiento OSPF es declarado con el comando **router ospf**, definimos un número de proceso con validez local, para nuestro caso será **100**, además debemos definir las redes que van a formar parte del proceso de propagación de rutas con el comando **network**, la dirección de **wildcard**, nos permite agrupar redes para simplificar el proceso de configuración. La división de OSPF por áreas es usada en redes de grandes proveedores, para nuestro caso no es necesario definir áreas OSPF, por consiguiente usamos solo el área de núcleo (backbone) que es el **área 0**.

5.3.3.3 Activación de MPLS

El componente principal para establecer un pseudocable MPLS o un servicio de EoMPLS como también se lo conoce, es habilitar la capacidad de establecer LSPs entre los pares LDP o PEs mediante la red del proveedor,

para esto hacemos uso del protocolo MPLS. El soporte de este protocolo depende de la plataforma, recursos y el sistema operativo que este disponga.

La configuración del protocolo MPLS en el núcleo (backbone) del proveedor la veremos a continuación

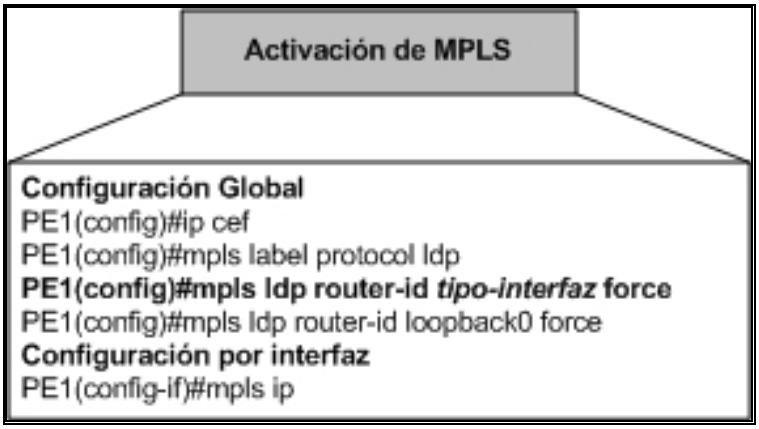


Figura 5.26 Configuración de activación de MPLS.

El comando **ip cef,** es un comando para los equipos CISCO usado para habilitar la conmutación rápida de paquetes, el cual es sumamente necesario para soportar MPLS. Luego de habilitar el CEF (Cisco Express Forwarding), procedemos a definir el método de distribución de etiquetas para MPLS, que puede ser el LDP (Label Distribution Protocol) o el TDP (Tag Distribution Protocol). El TDP es el protocolo estandarizado que hemos estudiado, por consiguiente será el que usaremos en nuestra simulación, sin

embargo el TDP podemos mencionar que funcionaría perfectamente, sino que este es un protocolo propietario de CISCO y no funcionaría con otros equipos. Para la configuración del protocolo de distribución de etiquetas, usamos el comando **mpls label protocol ldp**, donde LDP viene a ser nuestro protocolo seleccionado.

Ahora pasamos a definir uno de los parámetros más importantes de las buenas prácticas de configuración de MPLS, que es el identificador de ruteador (router ID) con el comando **mpls ldp router-id**, el cual es que nos va a permitir referenciar a los pares de los pseudocables MPLS, ya que si no definimos este parámetro, estamos expuestos a que cambie con la mayor dirección local configurada y nos impediría referenciar correctamente los puntos de extremo de los pseudocables.

Para finalizar esta sección, procedemos a habilitar el intercambio de etiquetas en las interfaces que forman parte del proceso MPLS con el comando **mpls ip** el cual es recomendable usarlo por interfaz. Es importante definir bien por donde se va a intercambiar información de etiquetamiento, ya que de esto será un factor importante para la seguridad de nuestra red MPLS.

5.3.3.4 Provisión de EoMPLS

Una ves que tenemos ya tenemos configurado nuestro núcleo (backbone) con el direccionamiento, enrutamiento y hemos activado el protocolo MPLS, por consiguiente podemos empezar a proveer de los servicios de pseudocable MPLS o EoMPLS.

Como definimos anteriormente, este servicio se puede dar directamente sobre ethernet sin embargo, por recursos y la gran cantidad de clientes que maneja un ISP, debemos usar una etiqueta extra de vlan para poder cubrir el aprovisionamiento de EoMPLS.

A continuación veremos la configuración de EoMPLS en un equipo de borde CISCO.

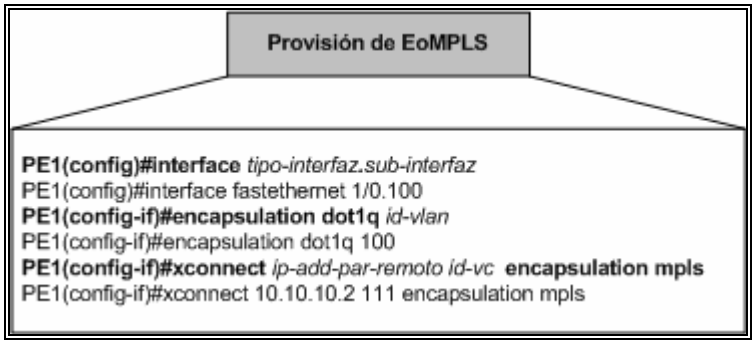


Figura 5.27 Configuración de provisión de EoMPLS

Las líneas de comando que vimos anteriormente son las necesarias para levantar un circuito MPLS. Esta configuración debe ir en los equipos de borde del proveedor donde van a ser conectados los clientes.

Primero se define una sub-interfaz en el equipo especificada con un punto al final del nombre de la interfaz (fastethernet1/0.100). Luego de esto, definimos que esta sub interfaz va a ser encapsular tramas con ieee 802.1q, para lo cual usamos el comando **encapsulation**, para nuestro ejemplo, vamos a encapsular los paquetes con la etiqueta de vlan 100; esta etiqueta de vlan, debe ser la misma en la configuración del otro extremo del pseudocable, caso contrario no se podrá definir a que segmento de capa 2 corresponde el paquete. Finalmente creamos el identificador de circuito con el comando **xconnect**, el cual no va a permitir definir el equipo con el cual vamos a crear un pseudocable, este equipo se lo define según el identificador de ruteador como lo vimos en la configuración de direccionamiento, para nuestro caso, el equipo PE1 (10.10.10.1) va a establecer un pseudocable ethernet con el equipo de dirección 10.10.10.2, que corresponde a PE2, el cual es juntamente el otro extremo que necesitamos del pseudocable. El identificador de circuito también se lo define con este comando, para nuestro caso el circuito EoMPLS es el 111 y este deberá coincidir exactamente con la configuración que coloquemos en el PE2.

Con esta configuración realizada en cada uno de los equipos del ISP, automáticamente se levantará el pseudocable ethernet sobre MPLS en cuanto el PE1 o PE2 reciban un paquete ethernet desde los equipos del cliente (CE1 o CE2). Como primera observación, podemos darnos cuenta que no hemos necesitado configurar ni una línea de comando en los equipos del cliente, lo que lo hace totalmente independiente de la configuración de capa 3 del proveedor.

Los resultados de la configuración expuesta previamente, los veremos en la siguiente sección

5.3.4 Resultados

Para mostrar los resultados obtenidos, podemos considerar tres tipos principales de equipos distribuidos en la red del ISP y del cliente, estos son los PEs, los Ps y los CEs, donde en cada uno podremos encontrar información específica que detalle la funcionalidad de los pseudocables.

5.3.4.1 Resultados de direccionamiento IP

El primer paso, que es el de configurar el direccionamiento IP, nos lleva a tener conectividad entre cada uno de los equipos que estén directamente conectados entre ellos o que pertenezcan al mismo segmento de red.

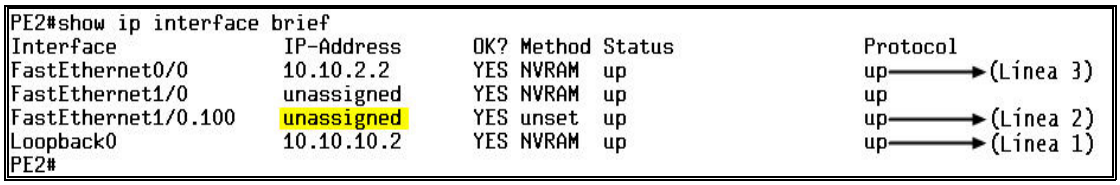


Figura 5.28 Resultados de direccionamiento

Cada equipo del núcleo (backbone) del portador va a tener configuraciones IP de interfaces físicas y lógicas. El comando para visualizar este direccionamiento es el **show ip interfaces brief**, el cual nos muestra el direccionamiento IP usado en la interfaz de loopback (Línea 1) la cual es una dirección de equipo con prefijo /32, luego tenemos la sub-interfaz del equipo, la cual tiene configurada una encapsulación 802.1q que nos permite diferenciar clientes que dependen de una misma interfaz y van a ser separados por equipos de L2 que soporten ieee 802.1q. Como podemos apreciar en la imagen (Línea 2), vemos que NO existe un direccionamiento configurado y sin embargo nuestros extremos del pseudocable MPLS van a tener conectividad en L3. Finalmente tenemos el direccionamiento de la interfaz física (Línea 3) que es la que nos permitirá tener conectividad entre equipos cercanos.

5.3.4.2 Resultados de enrutamiento

El poder alcanzar las direcciones y rutas que manejan los equipos es de suma importancia, por lo que debemos siempre verificar que todas las redes o IPs sean accesibles desde cada equipo en la red. En nuestro laboratorio, consideramos el enrutamiento dinámico OSPF.

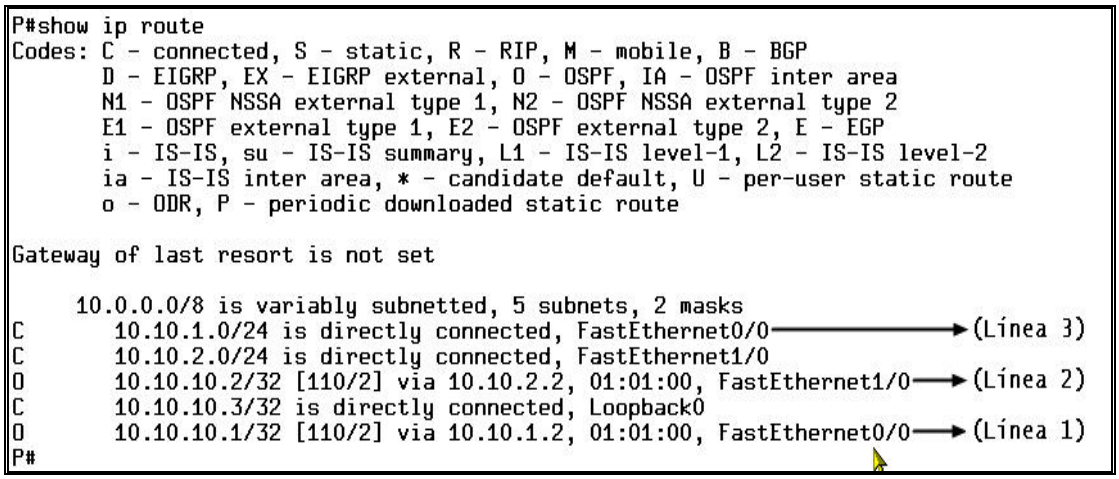


Figura 5.29 Tabla de ruteo del ruteador P.

Una ves que el protocolo OSPF ha alcanzado el estado final, los equipos se vuelven completamente adyacentes y tienen la información correspondiente a las rutas publicadas como mejores desde sus vecinos. Una manera de ver las rutas que ha aprendido el equipo es con el comando **show ip route**, el con el cual nos muestra todas y cada una de las rutas que se han aprendido por cualquier método existente. Como podemos apreciar en la figura anterior

identificamos que se ha aprendido por OSPF la dirección de loopback del PE1 (Línea 1) y también del equipo PE2 (Línea 2), que es sumamente importante, dado que estas direcciones son las que identifican a los equipos para el establecimiento del EoMPLS. Así también podemos apreciar las rutas directamente conectadas que se aprenden simplemente levantando el protocolo IP en las interfaces de los equipos.

5.3.4.3 Resultados de activación de MPLS

El objetivo de activar MPLS en los equipos del núcleo (backbone) es el poder asignar etiquetas LDP a cada IP o prefijo alcanzable en nuestra red. Los resultados de la activación de este protocolo dependerán definitivamente de cada equipo, sin embargo podemos describir el comportamiento basados en uno de ellos.

```
PE1#show mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     No Label      l2ckt(111)       29524         none       point2point →(Línea 3)
17     Pop Label     10.10.2.0/24     0             Fa0/0      10.10.1.1
18     17            10.10.10.2/32    0             Fa0/0      10.10.1.1 ⟶ (Línea 2)
19     Pop Label     10.10.10.3/32    0             Fa0/0      10.10.1.1 ⟶ (Línea 1)
PE1#
```

Figura 5.30 Tabla de reenvío MPLS.

El comando **show mpls forwarding-table**, nos permite ver la tabla de reenvío de etiquetas MPLS que nos va a permitir intercambiar tramas MPLS

de una manera rápida. En la salida del comando, vemos referenciado la asignación de etiquetas, las IPs a las cuales corresponden esta asignación y el medio por donde tienen que ir los paquetes que cumplen con las condiciones mencionadas.

En la figura, podemos apreciar las asignaciones locales que hace el PE1 para la IP 10.10.10.3 que corresponde al ruteador P (Línea 1), cuya acción o etiqueta de salida es “remover la etiqueta”, debido a que P está justamente conectado con el PE, lo cual lo convierte en el ruteador de penúltimo salto, por lo cual no necesita asignación de etiqueta alguna. Caso contrario ocurre con en reenvío de paquetes hacia el PE2 el cual lo podemos ver en la Línea 2, donde los paquetes dirigidos a el van a tener asignada la etiqueta 17 y el ruteador P será el encargado de reenviar este paquete. En la figura anterior, podemos también apreciar en la línea 3 una etiqueta de salida como “No Label”, lo que nos indica que no hay asignación necesaria para alcanzar el destino con esta etiqueta y ya veremos como nos afecta el tratamiento de estos paquetes.

```
P#show mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     10.10.10.1/32    272084        Fa0/0      10.10.1.2 (Línea 2)
17     Pop Label     10.10.10.2/32    271849        Fa1/0      10.10.2.2 (Línea 1)
P#
```

Figura 5.31 Tabla de reenvío para el ruteador P.

Para complementar el análisis que vimos anteriormente, podemos ver la tabla de reenvío del ruteador P. En la Línea 1 podemos apreciar la el reenvío que tiene a cargo el ruteador P con respecto a la IP de loopback del ruteador PE2. Como era de esperarse, dado que este es el ruteador de penúltimo salto desde el ruteador PE1 el cual enviaba paquetes con etiqueta de 17 al ruteador PE2, el removerá la etiqueta (Pop Label) y dejará que el paquete continúe con la carga disponible que puede ser un paquete IP alcanzable para el ruteador PE2 o una segunda cabecera LDP como veremos posteriormente. Situación similar ocurre con el ruteador PE1 en la Línea 2.

5.3.4.4 Resultados de provisión de EoMPLS

Todos los resultados anteriores son básicamente el establecimiento de MPLS en el núcleo (backbone) de la red, ahora tenemos que ver el establecimiento del pseudocable MPLS o EoMPLS en nuestros equipos.

Primero observaremos el trabajo que realiza el protocolo LDP al usar el método de descubrimiento extendido para hacer que el PE1 se relacione o cree un LSP con el PE2.

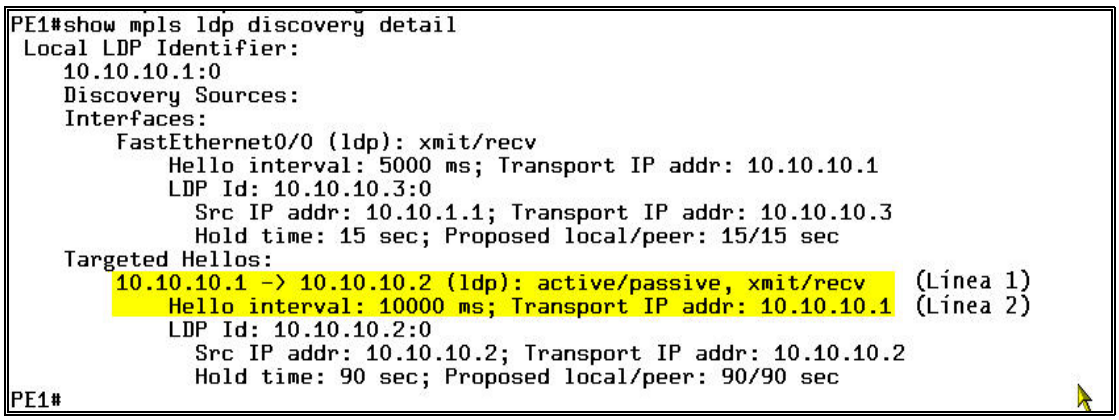


Figura 5.32 Descubrimiento LDP extendido.

El descubrimiento LDP para un pseudocable es el extendido, debido a que no siempre se encuentran directamente conectados. En la figura anterior podemos apreciar como se ha establecido la adyacencia LDP gracias al descubrimiento LDP extendido, en la Línea 1 identificamos información de que el PE1 fue el que tomó el papel de activo en el descubrimiento y así en la línea 2 encontramos el parámetro de 10 segundos establecido para el intervalo de mensajes de saludo.

Después que los PEs se han percatado de la existencia de cada uno de ellos con los mensajes de saludo, pueden empezar estableciendo la conexión TCP entre ellos e iniciar la sesión de establecimiento.

Durante la inicialización, los PEs negocian parámetros de sesión como versión y temporizadores, una vez que acuerdan estos parámetros, pueden ser considerados pares LDP.

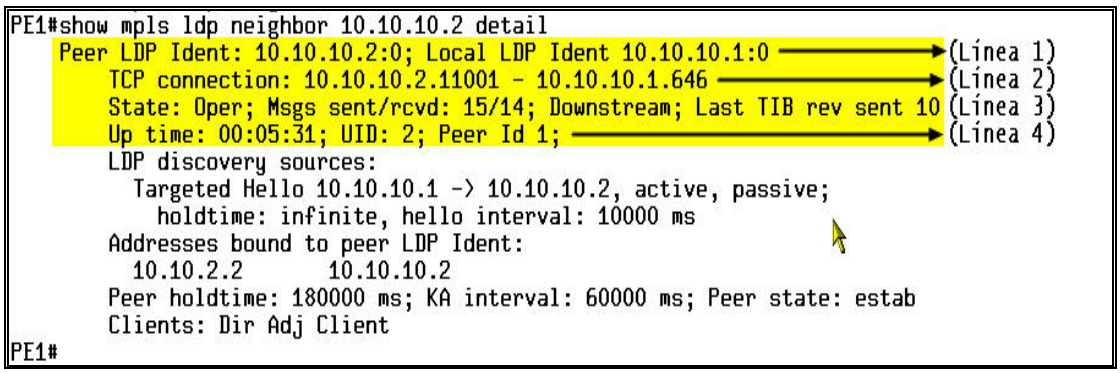


Figura 5.33 Detalles de sesión LDP

En la figura anterior, podemos apreciar en la Línea1, las IPs que fueron elegidas como IDs de cada ruteador, para nuestro caso, forzamos que estas sean las direcciones de loopback tanto para PE1 como para PE2 (10.10.10.1 y 10.10.10.2 respectivamente). En la línea 2 podemos confirmar que se ha establecido una sesión TCP para establecer el LSP entre los extremos del pseudocable, los puertos usados para nuestro caso fueron para PE1 el 646 y para el PE2 el 11001, cabe recalcar que el 646 lo tiene el equipo que tiene el papel de activo en el establecimiento del LSP. Las líneas 3 y 4 nos muestran el estado en detalle de la sesión LDP (operacional), el método de distribución (no solicitado) y el tiempo de actividad de la sesión (5 min, 31 seg).

Ahora podemos ver el estado en el que se encuentra nuestro pseudocable MPLS.

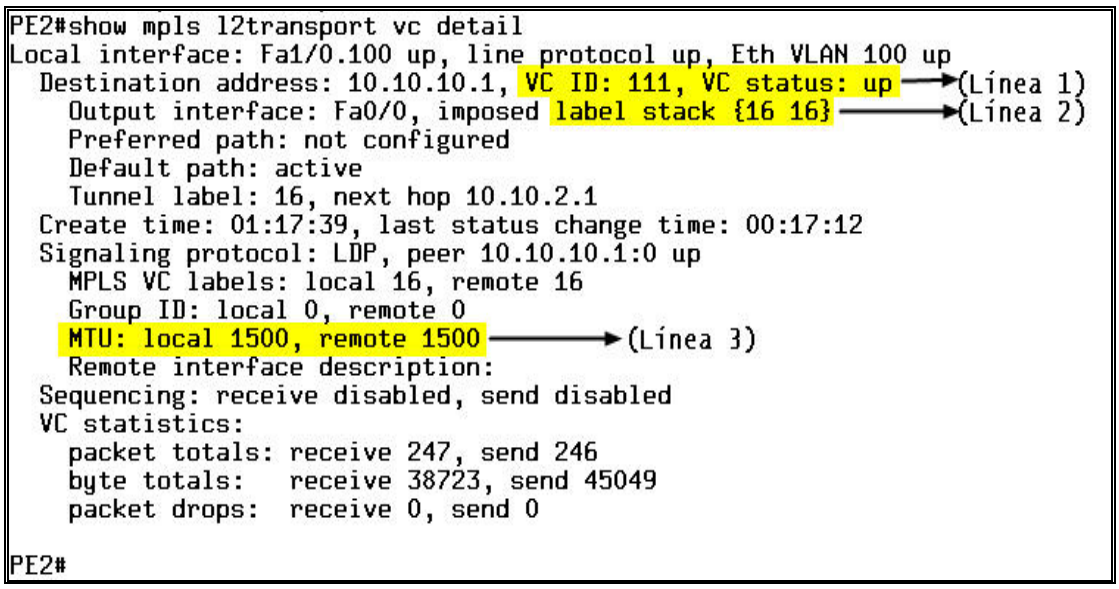


Figura 5.34 Estado del pseudocable MPLS.

Con el comando **show mpls l2transport vc detail** podemos ver toda la información necesaria acerca de nuestro pseudocable MPLS. En la línea 1, apreciamos que el pseudocable con el **ID 111** de pseudocable (que fue el que configuramos) está activo. La línea 2 nos indica la pila de etiquetas que se requiere para llevar a cabo el intercambio de paquetes por medio del pseudocable, siendo una la etiqueta de túnel y la otra la etiqueta de pseudocable. En la línea 3, podemos ver uno de los parámetros más importantes en una configuración MPLS el MTU (1500), y lo vemos tanto a nivel local como remoto.

5.3.4.5 Conectividad del cliente.

Como punto final de la verificación del establecimiento de nuestro pseudocable, podemos veri si efectivamente el cliente tiene conectividad remota con el equipo extremo del pseudocable. Para lograr este objetivo, primero realizaremos una prueba de conectividad ICMP (ping).

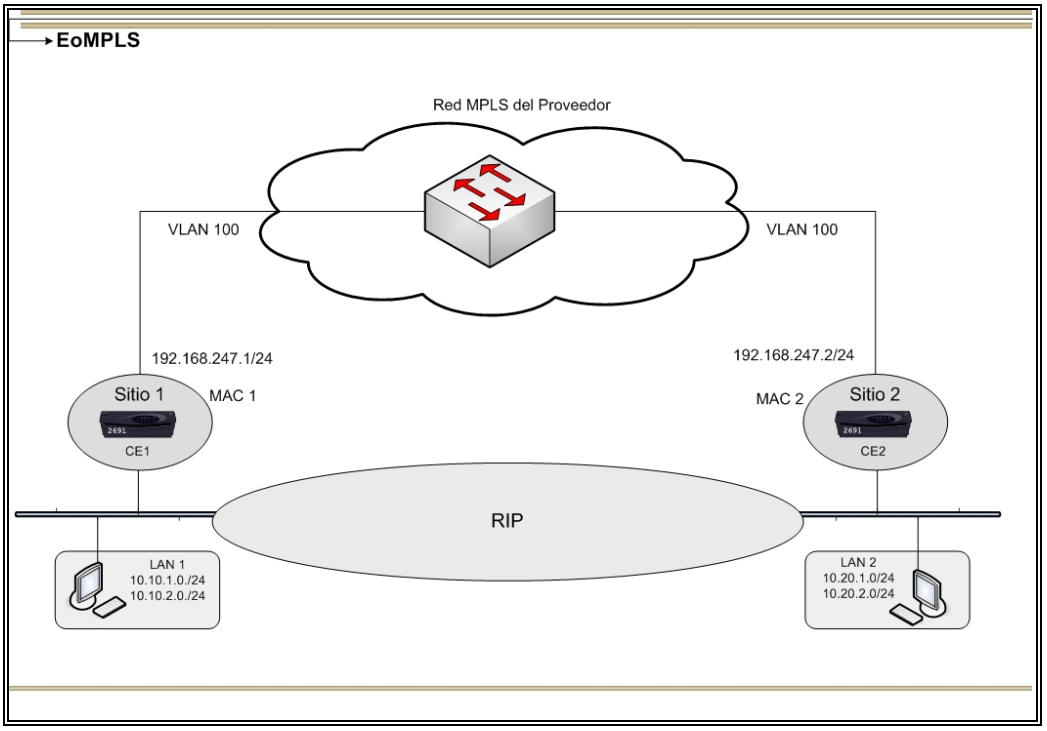


Figura 5.35 Servicio EoMPLS para el cliente.

El servicio que el cliente está topológicamente esquematizado en la figura anterior. Como podemos apreciar, la red del proveedor se percibe como un mismo circuito de capa 2 para el cliente, lo que puede representarse como un equipo que soporta 802.1q entre los extremos del cliente.

```
CE1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.247.2          154   c004.1ef5.0000  ARPA   FastEthernet0/0(Línea 1)
Internet  192.168.247.1            -   c003.1ef5.0000  ARPA   FastEthernet0/0(Línea 2)
CE1#
```

Figura 5.36 Tabla ARP del cliente.

En la figura anterior, tenemos los resultados del ARP (Address Resolution Protocol) para el PE1. Con lo cual si nos fijamos en la línea 1, encontramos que la IP del equipo remoto PE2 (192.186.247.2) junto con la MAC correspondiente a su tarjeta de red (c003.1ef5.0000) se encuentran listadas. Esto nos da fiel seguridad de que el camino en medio de estos dos equipos no es un dispositivo de L3 sino un conmutador de circuitos Ethernet, al cual podemos comparar con un conmutador y vendría a ser nuestro pseudocable MPLS.

```
CE1#ping 192.168.247.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.247.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 160/200/232 ms
CE1#
```

Figura 5.37 Prueba de conectividad ICMP.

En la figura anterior comprobamos la conectividad entre los puntos finales con el protocolo ICMP haciendo un ping entre los equipos extremos.

Una ves que hemos conseguido tener conectividad entre los extremos del pseudocable, podemos levantar cualquier servicio o protocolo entre la LAN del sitio 1, con la LAN del sitio 2.

En nuestro caso, vamos a configurar el protocolo de enrutamiento dinámico RIP, para probar que podemos intercambiar sin ningún problema la información de este protocolo y dar conectividad entre redes de sitios remotos por medio del pseudocable MPLS.

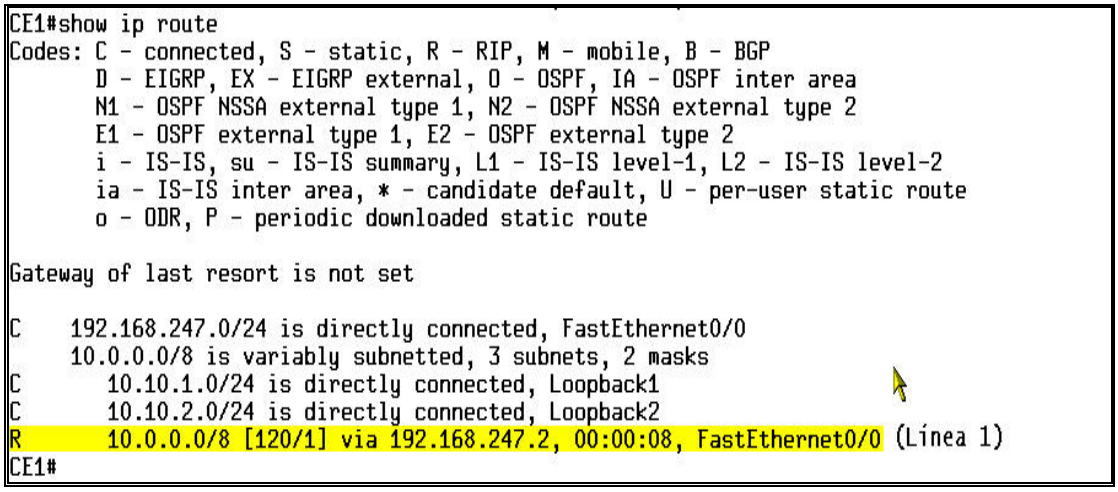


Figura 5.38 RIP sobre EoMPLS.

En la figura anterior, podemos comprobar que efectivamente desde el sitio 1 hemos aprendido las redes del sitio 2 mediante RIP (Línea 1).

```
CE1#ping 10.20.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 256/276/344 ms
CE1#
```

Figura 5.39 Accesibilidad de redes propagadas.

En la figura anterior comprobamos que efectivamente hemos podido establecer conectividad con la IP 10.20.1.1 que es una de las direcciones configuradas como loopbacks en el equipo CE2.

5.3.4.6 Cálculo del MTU EoMPLS.

El parámetro más importante cuando usamos protocolos que encapsulan datos como por ejemplo un túnel encriptado o una red MPLS, es el máximo tamaño del paquete que podemos enviar sobre esta red.

El MTU (Maximun Transmisión Unit) expresa en bytes el tamaño más grande que puede ser enviado sobre una capa de un protocolo de comunicaciones.

Valores característicos de MTU	
Protocolo	**MTU (bytes)**
Ethernet	1500
PPP	576
ATM	8190
FDDI	4470

Tabla 5.1 Valores característicos de MTU.

En la tabla anterior, podemos ver los valores característicos de MTU enlaces de capa 2. Para nuestro caso, tomaremos como referencia el MTU para Ethernet, que es el protocolo que mantienen nuestros enlaces.

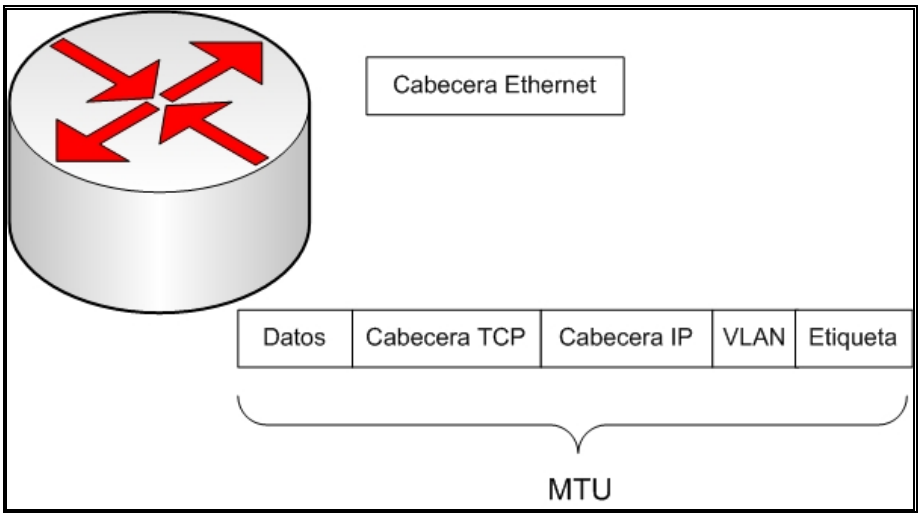


Figura 5.40 Estructura de MTU.

Como vemos en la figura anterior, el MTU es el conjunto de los datos que son enviados mas cada una de las cabeceras que sean colocadas antes de poder ser enviada la trama sobre el enlace Ethernet.

A continuación mostramos los resultados del análisis del MTU para el camino formado entre los sitios con EoMPLS.

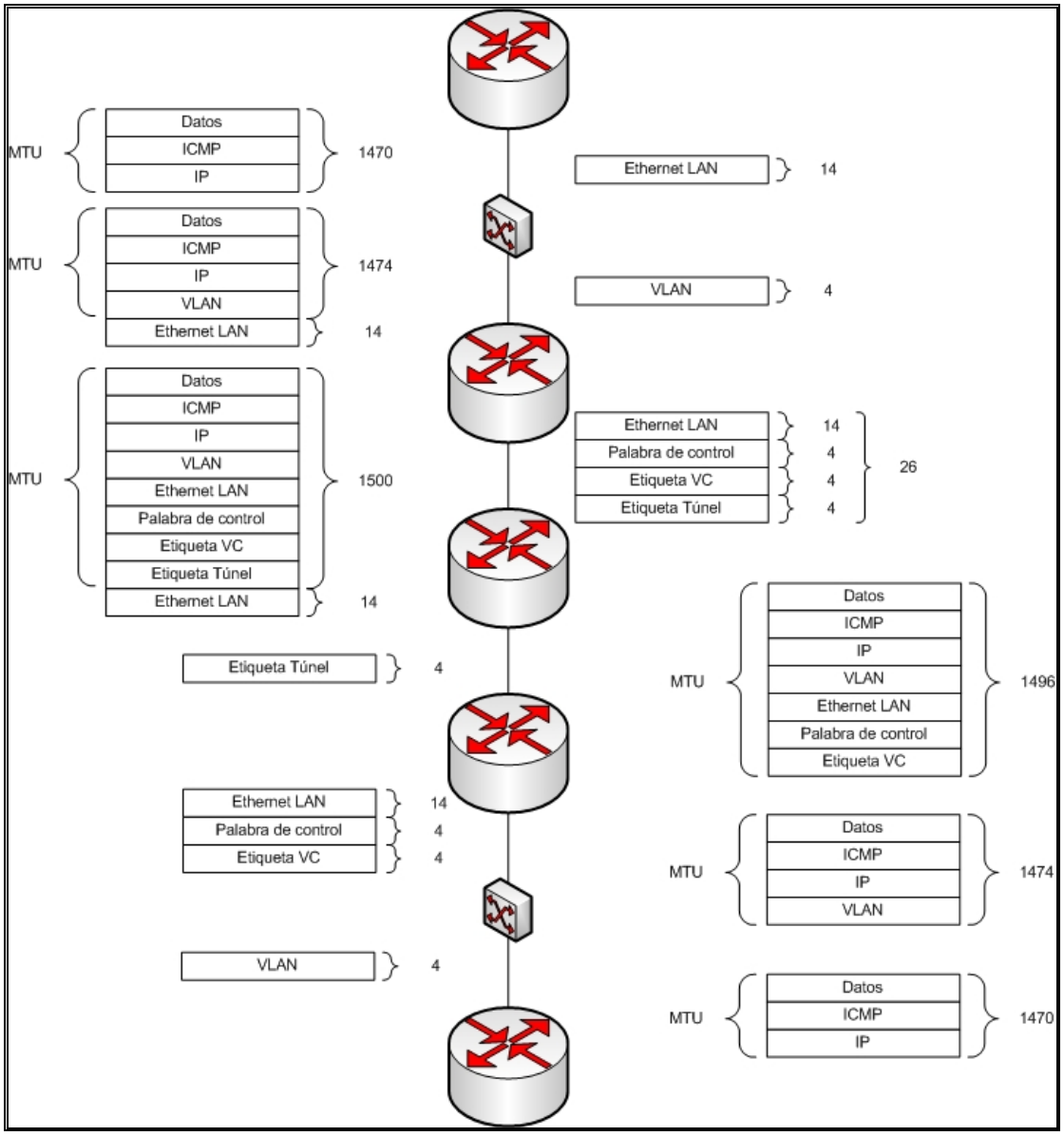


Figura 5.41 Análisis de MTU.

Como parte de las pruebas realizadas en de laboratorio de implementación de EoMPLS, fue el de realizar pruebas de conectividad ICMP con diferentes tamaños de paquetes desde CE1 a CE2. Y pudimos apreciar que el máximo tamaño de paquetes ICMP que podíamos configurar en el ping extendido fue

de 1470. Esta situación la vemos justificada en la figura anterior, ya que al agregarse todas las etiquetas correspondientes al enlace EoMPLS, hace que llegue al límite del MTU permitido en un enlace ethernet (1500 bytes).

```
CE1#ping
Protocol [ip]:
Target IP address: 192.168.247.2
Repeat count [5]:
Datagram size [100]: 1470
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1470-byte ICMP Echos to 192.168.247.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 244/299/460 ms
CE1#
CE1#
CE1#ping
Protocol [ip]:
Target IP address: 192.168.247.2
Repeat count [5]:
Datagram size [100]: 1471
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1471-byte ICMP Echos to 192.168.247.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 5.42 Ping vs MTU.

Como vemos en la figura anterior, el ping de 1470 es el máximo tamaño de paquete que podemos enviar sobre un camino EoMPLS. Este análisis es muy importante para poder calibrar bien el tamaño de paquetes que van a pasar por la red y evitar inconvenientes con posibles aplicaciones que requieran de paquetes demasiado grandes.

5.3.5 Conclusiones

Una vez desarrollado el escenario de simulación, verificamos el procedimiento para configurar un pseudocable MPLS con sus requisitos respectivos para poder operar.

El AToM cumple su funcionalidad de multiprotocolo a nivel de la capa de enlace de datos del modelo OSI y EoMPLS es su soporte para redes Ethernet.

El EoMPLS podría tener limitantes de escalabilidad si consideramos que es necesario un enlace por pseudocable, sin embargo el soporte del encapsulamiento 802.1q o VLANs, nos permite hacer escalable esta solución siendo así la mejor opción a configurar en una red Ethernet sobre MPLS.

El MTU es un valor muy importante de considerar cuando se habla de encapsulamiento, dado que algunas aplicaciones pueden estar configuradas para enviar paquetes de gran tamaño, lo que se vería reflejado en un obstáculo para la red MPLS, razón por la cual el núcleo (backbone) sobre el cual estamos transportando un pseudocable MPLS debe soportar paquetes mayores al estándar de la tecnología encapsulada, en este caso ethernet con 1500 Bytes.

A pesar de las ventajas de transparencia a nivel de IP de un pseudocable MPLS tiene una deficiencia y es que los circuitos que se pueden levantar son punto a punto, lo cual nos lleva nuevamente a una topología Hub-Spoke con un concentrador principal, mas no a una Full Mesh como desearíamos.

5.4 Comparación de los servicios de L2 y L3 MPLS VPN

En esta sección se realizara un análisis comparativo entre L2 y L3 MPLS VPN. En la siguiente tabla se registran la comparación de estas tecnologías de acuerdo a las características de recursos e información.

L3MPLS VPN tiene como prioridad procesar información de capa 3 y tomar decisiones de envío en base a esta información donde se requiere un proceso de enrutamiento entre los ruteadores de borde PE a CE. En L2MPLS VPN, las decisiones de envío se basa en información de capa 2 como por ejemplo la dirección MAC, VLAN ID, DLCI o una interfaz de línea dedicada y no es requerido un proceso de enrutamiento entre los ruteadores del cliente y el proveedor.

De acuerdo a estos antecedentes L3MPLS VPN es una tecnología que requiere mayor robustez en los ruteadores del cliente por consiguiente es de

mayor costo, pero presenta más flexibilidad en la implementación de nuevos servicios como QoS, Diff servicio, etc.

L2MPLS VPN en sus orígenes fue pensado como un protocolo punto a punto, a diferencia de L3MPLS VPN quien desde sus inicios ya se estandarizó como un protocolo multipunto. L2MPLS VPN se proyecta a ser una tecnología multipunto con aplicaciones como IPLS (IP only Lan Service) y VPLS (Virtual Private LAN Service) que incluso están presentes en otros países.

Con respecto a la escalabilidad podemos mencionar que L3MPLS VPN es excelente a nivel del proveedor; ya que la conexión que se necesita para levantar este servicio es de tipo lógica, a diferencia de L2MPLS VPN que necesita de recursos físicos como pueden ser tarjetas que soporten las interfaces del lado del cliente, las mismas que estarían instaladas del lado del proveedor, lo cual puede sobrepasar el nivel máximo soportado y se necesitaría de nuevo equipamiento lo que se vería reflejado en costos para el mismo.

Con la evolución de los servicios integrados, el alcance o la cobertura de un servicio es sumadamente importante en las licitaciones que los proveedores de servicios participan. L3MPLS VPN está limitado por el alcance del núcleo

(backbone) MPLS del proveedor, debido a los protocolos de enrutamiento que deben manejar; a diferencia de L2MPLS VPN cuyo funcionamiento se basa en LDP y no en un protocolo de enrutamiento, logrando así cobertura a nivel mundial mediante la interconexión de redes MPLS entre diferentes proveedores. Visto esto, podemos considerar que la evolución de los portadores de datos, no solo está enfocada a brindar servicios locales (nacionales), sino establecer interconexiones a nivel Mundial como un servicio de valor agregado a su red MPLS.

El soporte de tráfico Multicast no es nativo en L3MPLS VPN y tiene que ser habilitado como un componente especial, a diferencia de L2MPLS VPN que fue diseñado con soporte multicast para a futuro poder soportar servicios de última generación como lo son IPTv y servicios unificados.

L3MPLS VPN no tiene soporte multiprotocolo sino más bien se han estandarizado diferentes protocolos para cada tecnología del mercado como lo es Ethertnet, Frame Relay, ATM, etc. L2MPLS VPN tiene soporte multiprotocolo, ya que trabaja independientemente del tipo de trama, lo cual es una ventaja a nivel del portador al momento de brindar servicios.

Tanto L3MPLS como L2MPLS VPN tienen soporte de QoS, debido a que ambos trabajan sobre MPLS con soporte nativo de QoS en sus paquetes.

El resumen de la comparación de L2MPLS VPN con L3MPLS VPN lo podemos apreciar en la siguiente tabla.

CARACTERÍSTICA	L2 MPLS VPN	L3 MPLS VPN
Tipo de Información	Información de Capa 2:Dirección MAC, VLAN ID, información DLCI, o una interfaz de una línea dedicada	Manejo de información de Capa3 como: IP
Proceso de Enrutamiento Cliente- Proveedor (CEs-PEs)	No requiere	Si requiere y pueden ser los protocolos (RIPv2, EIGRP, OSPF, eBGP,estatico).
Proceso de Enrutamiento Bordes del Proveedor (PEs-PEs)	No requiere	Si requiere y pueden ser el protocolo (MPBGP).
Tecnología VPN	MPLS/BGP VPNs(RFC 2547)	Pseudo-Wire y Pseudo-LAN (Martini-drafts,L2TPv3, VPWs,VPLS)
Costos para el cliente	Disminuyen los costos por la simplicidad del equipo requerido en el cliente	Aumentan los costos por las características requeridas en el router del cliente(Protocolo de ruteo)

Figura 5.43 Comparación de los servicios L3 y L2 MPLS VPN.

CONCLUSIONES Y RECOMENDACIONES

La simulación realizada de los servicios de L2MPLS VPN y L3MPLS VPN se realizó satisfactoriamente pudiéndose ver las ventajas y desventajas de cada una de estas para realizar así una comparación en medida de su funcionalidad, rentabilidad, escalabilidad y proyecciones a futuro.

A pesar de la inmadurez de la tecnología de L2MPLS VPN vemos que existe una gran tendencia en el mercado a solicitar este tipo de servicios sin importar que sea un servicio punto a punto ya que le las empresas le dan más valor a su independencia de tecnología de ruteo con el proveedor. L3MPLS VPN a pesar de no ser transparente para el cliente, soluciona un gran problema que es el soporte multipunto entre agencias, lo que incrementa los niveles de disponibilidad en el servicio que brinda un portador de datos, que se ve reflejado en ingresos e imagen para el mismo y satisfacción para el cliente.

Definitivamente comprobamos que todo cambio a nivel de un ISP debe ser probado antes de entrar en producción y más aún donde la tecnología que

se desea implementar es de la magnitud de MPLS donde inclusive se necesita automatizar el proceso de proveer y administrar servicios como son los de VPNs de tipo L2 y L3 sobre MPLS.

Existen en el mercado muchas herramientas de simulación con orientaciones académicas y tecnológicas, sin embargo pudimos comprobar que el Dynamips es una herramienta que cubre ambos campos de una excelente manera ya que soporta emulación de una de las plataformas más robustas como lo es la de CISCO y está licenciado como herramienta gratuita donde todos podemos usarla a plenitud.

Podemos recomendar que se use esta tesis como base para nuevas investigaciones de los diferentes servicios que brinda MPLS; ya que con un hardware más robusto, podemos crear redes inclusive de la magnitud de un portador de servicios real y analizar cada uno de los requerimientos y consideraciones que se deben tener para administrar una red compleja como esta representa y a la vez ser proactivos en el desarrollo de soluciones y servicios.

Dynamips es una herramienta que se la puede masificar para la enseñanza de redes de computadoras ya que esta no tiene límites a nivel de las nuevas topologías y protocolos que se puedan implementar. Es una herramienta

que nos puede ayudar a preparar para obtener certificaciones internacionales como son las de CISCO CCNA, CCNP, e incluso existen registros de CCIEs que es la más alta jerarquía en certificaciones CISCO que se han apoyado en esta herramienta.

Consideramos que la contribución de esta tesis es muy importante ya que puede ser usada para la capacitación de nuestros jóvenes y en un futuro no muy lejano tener grades administradores de redes y minimizar la inversión del soporte externo para resolver incidencias a nivel de redes de computadoras, lo cual conlleva a tener personal más capacitado que pueda ingresar al área laboral de una manera más sólida con conceptos que hoy en día son fundamentales con la evolución de los servicios integrados y las redes de computadoras a nivel mundial.

BIBLIOGRAFÍA

- USA, Mark Lewis, "*Comparing, Designing, and Deploying VPNs,"* Cisco Press, 800 East 96th Street, Indianapolis, Abril 2006.

- USA,Wei Luo,Carlos Pignataro , Dmitry Bokotey, Anthony Chan, "Layer 2 VPN Architectures," ,Cisco Press, 800 East 96th Street, Indianapolis, Marzo10, 2005.

- USA, Lancy Lobo, Umesh Lakshman., "MPLS Configuration on Cisco IOS Software," Cisco Press, 800 East 96th Street, Indianapolis, Octubre 21, 2005.

- USA, Iftekhar Hussain, "Fault-Tolerant IP and MPLS Networks," *Cisco Press*, 800 East 96th Street, Indianapolis, November 11, 2004.

- USA, Monique Morrow, Azhar Sayeed, "MPLS and Next-Generation Networks," *Cisco Press*, 800 East 96th Street, Indianapolis, Noviembre 06, 2006.

- USA, Mark Lewis, “Troubleshooting Virtual Private Networks,” *Cisco Press*, 800 East 96th Street, Indianapolis, Mayo 27, 2004.

- USA, Jim Guichard, Ivan Pepelnjak, “*MPLS and VPN Architectures Volumen I*,” *Cisco Press*, 201 West 103rd Street Indianapolis, Marzo 2001.

- USA, Jim Guichard, Ivan Pepelnjak, Jeff Apcar, “*MPLS and VPN Architectures Volumen II,” Cisco Press*, 201 West 103rd Street Indianapolis, Junio 06, 2003.