UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

TESIS FINAL

Previa la obtención del grado de

MAGISTER EN TELECOMUNICACIONES

TITULO:

Diseño de una red privada virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil

Elaborado por:

Ing. Fausto Raúl Orozco Lara.

Tutor:

Ing. Juan García Pérez, MSc.

Guayaquil, 3 Septiembre de 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster Fausto Raúl Orozco Lara como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, a los 24 días del mes Septiembre año 2014

DIRECTOR DE TESIS

_____

Ing. Juan García Pérez, MSc.

REVISORES:

_____ _____

Ing. Orlando Philco Asqui, MSc. Ing. Luzmila Ruilova, MSc.

DIRECTOR DEL PROGRAMA

_____

Ing. Manuel Romero Paz, MSc.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

YO, FAUSTO RAÚL OROZCO LARA

DECLARO QUE:

La tesis "**Diseño de una red privada virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil**", previa a la obtención del grado Académico de Magíster, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico de la tesis del Grado Académico en mención.

Guayaquil, a los 24 días del mes Septiembre año 2014

EL AUTOR

_____

FAUSTO RAÚL OROZCO LARA

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

AUTORIZACIÓN

YO, FAUSTO RAÚL OROZCO LARA

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución de la Tesis de Maestría titulada: "**Diseño de una red privada virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 24 días del mes Septiembre año 2014

EL AUTOR

_____

FAUSTO RAÚL OROZCO LARA

DEDICATORIA

A mis padres que me han dado la mayor enseñanza que se puede dar a un hijo amor y educación, a mi esposa Diana por siempre darme su apoyo en todo momento, a mis hermanos, a mis preciosos sobrinos Verónica, Diego, Michelle y Mateo. Dedico también este trabajo a un amigo y maestro mi Director de la Tesis, Ing. Juan García MSc. y a la Universidad Católica de Santiago de Guayaquil por permitirme seguir creciendo profesionalmente.

AGRADECIMIENTOS

El presente trabajo de tesis se da por el esfuerzo y la lucha constante de ser cada día mejor y superar las barreras que nos pone el destino, es por ello mi agradecimiento al Señor todo poderoso por contar siempre con su bendición. A mis padres Fausto y Gladys que son el mayor regalo de la vida que he tenido hasta el día de hoy ya que ellos han sido y serán por siempre el mayor de mis ejemplos en todo lo que me proponga realizar. A mis hermanos Rocío, Nancy y William que con sus buenos consejos y ejemplo de vida han hecho de mí, el más grande admirador de todas sus hazañas tanto en lo personal como profesional. A la futura madre mis hijos Diana, que es el pilar fundamental donde se realizaran uno de los mayores sueños del ser humano tener su propia familia.

Un agradecimiento especial al MSc. Juan García por su incondicional apoyo en la parte académico y por brindarme siempre su amistad y apoyo en la realización dela presente tesis.

A todos los docentes de la Maestría en Telecomunicaciones, con quienes hemos compartido muchos momentos de conocimiento y alegría dentro y fuera del salón de clase y por supuesto a todos mis compañeros de clase.

RESUMEN

En la presente tesis se realiza una descripción de la tecnología de Conmutación Multi-Protocolo mediante Etiquetas usando una red privada virtual para la comunicación de la Universidad de Guayaquil con su carrera de Ingeniería en Networking, la cual es una institución de educación superior estatal del Ecuador.

Se realizó una descripción de la tecnología MPLS con VPN mostrando sus cualidades, ventajas y desventajas, se promueve la introducción de esta tecnología a la red de comunicación de datos de la Universidad para que el tráfico tenga un performance y confidencialidad en los datos transmitidos, diseñando un esquema así como la infraestructura que podría ser usada en esta implementación, con características modulares las cuales permitirá a la Universidad ir creciendo a la medida de que su tráfico o demanda de transporte vaya aumentando al igual que la integración de las demás extensiones se amerita el caso; para el diseño nos ayudaremos del programa de simulación "GNS3" el mismo que se hará un bosquejo de la configuración y modelo para la transmisión de sucursal a matriz y viceversa.

ABSTRACT

This thesis is a description of MPLS VPN using a communication from the University of Guayaquil with its career networking engineering, which is a state higher education institution of Ecuador.

Was a description of MPLS VPN showing his qualities, advantages and disadvantages, promotes the introduction of this technology to the data communication network of the university to have a performance traffic and confidentiality of the data transmitted, designing scheme as well as the infrastructure that could be used in this implementation , modular features which allow the University to grow to the extent that their traffic and transport demand will increase as the integration of other extensions are merited case, to help us design simulation program " GNS3 " the same to be made a sketch of the model configuration and transmission branch to parent and vice versa.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

Hoy en día las tecnologías existentes como IP están diseñadas para que brinden seguridad y sean capaces de restablecer la conectividad luego de que se presente alguna falla en algún elemento de red. Aunque la conectividad pueda restablecerse, el tiempo que esto demande podría no estar en el límite para lo aceptable en lo que respecta a servicios de alta prioridad. Por esta razón se estudia las posibilidades para que un proveedor de servicios implemente en sus redes sistemas confiables que puedan brindar a los clientes la seguridad necesaria al momento de conectar sus redes, adaptando protocolos como IP y MPLS.

Cada empresa o institución tiene desarrollado su propia estructura interna, tanto en infraestructura como en lo humano que son realizadas dependiendo de sus necesidades y recursos que tengan a disposición, en base a estas estructuras se tienen servicios de comunicaciones que tratan de satisfacer los requerimientos de cada organización, enfocándose al transporte de información interna como externa con sus clientes o proveedores, que muchas veces no son cubiertos de manera total o eficientemente, ante ello día a día se van desarrollando nuevas soluciones en la búsqueda de la integridad de la información con el fin de que la confidencialidad del trabajo de cada empresa esté garantizado y respaldado.

Existen algunas alternativas a nivel de comunicaciones, pero entre las que más se destaca es la creación de redes virtuales usando MPLS, ya que la misma está caracterizada por la simplicidad de migración. La tecnología MPLS estudia el transporte de paquetes y tiene como objetivo principal tratar de abarcar varios problemas existentes con el envío de paquetes,mejorando el rendimiento de enrutamiento en la capa de red por lo que mejorara la escalabilidad y flexibilidad en la prestación de servicios de enrutamiento.

Si se habla de seguridad podemos mencionar la definición de VPN que es una red privada virtual la cual se da por recursos tecnológicos propios de la empresa u recursos de algún proveedor quedará la exclusividad de un camino único y convincente para poder dar protección a los archivos que se encuentran en la red

de nuestra compañía, con la implementación de la misma un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un ruteador VPN en la sede. (Scott, 1999).

CAPITULO I
DISEÑO METODOLÓGICO

1.1 Antecedentes de la propuesta

La Universidad de Guayaquil es una de las principales del país y una de las más grandes la misma que consta con diecisiete Facultades que ofertan 31 carreras de pregrado, 7 a nivel tecnológico con diferentes especializaciones y 8 carreras cortas, de uno y dos años, cuenta con 6 extensiones universitarias en la Costa, y provincia de Galápagos, 14 centros de estudios a distancias, 5 Institutos Superiores de Postgrado, y 18 Institutos de Investigaciones; además cuenta con: laboratorios, talleres, consultorios, hospital, bibliotecas, farmacia, librería, comedores estudiantiles; también, grupos artísticos, equipos deportivos y otros servicios a la comunidad.(Universidad Guayaquil, 2012)

Con el crecimiento tecnológico y con el desarrollo de las telecomunicaciones se crea la Carrera de Ingeniería en Networking, bajo la dirección de la Facultad de Ciencias Matemáticas y Físicas en el año 2009, la misma que se encuentra domiciliada en Baquerizo Moreno y Víctor Manuel Rendón junto con la Carrera de Ingeniería en Sistemas Computacionales. Por la calidad educativa y el auge de las carreras en mención se ha incrementado el número de estudiantes vertiginosamente y por ello se ve en la necesidad de construir un modelo de comunicación entre carreras y Matriz. Las carreras de Sistemas y Networking cuentan con 5 laboratorios de computación, 1 laboratorio de Networking, 1 laboratorio de Electrónica, y un centro de cómputo donde se encuentra radicado sus conexiones a red, equipos de comunicaciones y servidores, es decir donde reside la información principal de las mismas, la importancia de mantener la información segura y consolidada con la matriz se ve en la necesidad de implementar un centro de cómputo con acceso directo a los servidores de la matriz ubicada en la ciudadela universitaria la que domicilia en Av. Kennedy y Av. Delta.

Administrativamente todas las Facultades, carreras o extensiones necesitan comunicarse diariamente con la matriz ya que todos sus estatutos, reglamentos e

información residen en la misma, es por ello que en el día a día se ve necesario estar comunicado de manera rápida, eficaz y segura, ya que existe información valiosa para la parte educativa, administrativa, económica que debe estar a buen recaudo y a tiempo para mantener la integridad de la información.

Con la información que se maneja y la cantidad de estudiantes se plantea nuevas tecnologías que puedan abastecer la demanda de recurso para poder tener la información a primera mano y de manera eficaz por ello con el diseño de una infraestructura con tecnología MPLS (Conmutación Multi-Protocolo mediante Etiquetas) usando una VPN (Red privada virtual) se espera cubrir todas las necesidades a nivel de comunicación con la matriz y satisfacer las expectativas de la disponibilidad de acceso a los servidores, para que el enlace de comunicación no se vea colapsado por la cantidad de concurrencias en un día determinado por el aumento de estudiantes en este recinto educativo .

1.2 Problema de Investigación

La limitación de la red de acceso entre la Universidad de Guayaquil con las carreras de Networking para acceder a los recursos de la institución a nivel comunicación de datos.

1.3 Justificación

Las organizaciones que están formalmente desarrolladas se ven en la necesidad de estar comunicados con todas sus colaboradores y con sus usuarios tanto internos como externos para poder así agilizar las tareas que involucren el trabajo diario en su jornada laboral, de la misma manera fomentar la integración de datos y compartir recursos sin necesidad de ir a un lugar específico. El tener una red privada virtual con tecnología MPLS, nos permitirá tener conexiones seguras entre equipos de donde podremos acceder a los recursos de los mismos de manera confidencial, como por ejemplo documentos, servidores de base de datos, aplicaciones específicas, etc. que se encuentren distantes y a su vez se tendrá la información en tiempo real y actualizado.

La construcción del diseño de la red de comunicaciones para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil, tratara de cubrir

cualquier tipo de necesidad a nivel de comunicaciones ya que en la actualidad la misma no está cubierta en la infraestructura de la carrera. Por lo cual con la VPN se pretende generar un camino virtual usando tecnología MPLS para garantizar la transmisión de la data, el mismo que puede acomodarse a distintos tipo de infraestructura basado en IP, ya que debido a su naturaleza el protocolo brinda conexiones "*any to any*" entre distintos puntos que comprendan una VPN, teniendo así el mejor camino o ruta en cada punto. Adicionalmente la disponibilidad que se tiene a nivel de la información o los recursos de la empresa, también debe tenerse en cuenta la parte de calidad de servicio por lo que con la metodología planteada va a poder contar con clases de servicio (CoS) dentro de una VPN con MPLS para así complementar las necesidades de cada servicio en particular.

1.4 Objeto

La red de acceso IP-MPLS entre la Universidad de Guayaquil y sus distintas carreras.

1.5 Objetivos

1.5.1 Objetivo General

Diseñar la red de comunicación para la Carrera de Ingeniería en Networking de la Universidad de Guayaquil usando Redes Privadas Virtuales con tecnología MPLS.

1.5.2 Objetivos Específicos

- Estudiar los elementos teóricos y técnicos para uso de la tecnología VPN con MPLS.
- Diseñar el esquema de la red de comunicación de datos para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil
- Realizar una simulación de configuración básica de tecnología VPN con MPLS teniendo como herramienta GNS3.
- Seleccionar los dispositivos que soporte la tecnología así como la implementación a nivel de configuración.

1.6 Hipótesis

Con lasimulación de la tecnología IP-MPLS permitirá la implementación de una red VPN para la mejora de los accesos a los servicios de datos entre la Carrera de Ingeniería en Networking de la Universidad de Guayaquil y la matriz.

1.7 Variables

Las variables que se pueden mostrar usando la tecnología MPLS con VPN pueden estar determinadas por:

- Tráfico de la red en horas picos
- Cantidad de paquetes enviados correctamente
- Cantidad de usuarios trabajando paralelamente

1.8 Tipo de Investigación

El Método de investigación para esta tesis será deductivo porque según su definición "parte de una hipótesis que demuestra o refuta una idea". El método deductivo consiste en la totalidad de reglas y procesos con cuya ayuda es posible deducir conclusiones finales a partir de unos enunciados supuestos llamados premisas si de una hipótesis se sigue una consecuencia y esa hipótesis se da, entonces, necesariamente, se da la consecuencia. El método deductivo se suele decir que se pasa de lo general a lo particular (Gómez, 2006) de forma que partiendo de unos enunciados de carácter universal y usando instrumentos científicos, se infieren enunciados particulares, pudiendo ser axiomático-deductivo, cuando las premisas de partida están constituidas por axiomas, es decir, proposiciones no demostrables, o hipotéticos-deductivo, si las premisas de partida son hipótesis contrastables.

1.8.1 Enfoque Temático

El trabajo realizado según su enfoque de estudio será de tipo Aplicado porque según su definición se analiza fenómenos de la realidad y su fuente fundamental es la misma; también podemos indicar que es de tipo experimental porque intenta conocer fenómenos de la realidad objetiva y para ello influye sobre el objeto de estudio a fin de observar y sistematizar su comportamiento, es decir que su enfoque temático para el tema de tesis presentado está dado por ser aplicado-experimental.

1.8.2 Enfoque Metodológico

El enfoque metodológico está dado por un enfoque cuantitativo ya que según definición este método es un conjunto de procesos secuenciales y probatorios orientados a la demostración o negación de una hipótesis mediante la recolección de datos con base en la medición numérica y el análisis estadístico (Tamayo, 2004), a fin de tratar de establecer patrones de comportamiento y probar teorías.

En este tema de tesis partimos de una tecnología usada a nivel WAN y se la plantea realizar a nivel MAN para satisfacer necesidades de comunicación a nivel educativo, la misma que servirá para brindar servicios sea registros en línea, revisión de notas u otros servicios que demanden comunicación directa con la matriz de la Universidad asegurando transmisión y confidencialidad de la información.

1.8.3 Alcance

Determina la estrategia que debe seguir la investigación la misma que va ofrecer la posibilidad de ubicarse en tiempo y espacio y tener una proyección coherente a partir del objeto de estudio por lo cual va a posibilitar la determinación de niveles de factibilidad. Según su alcance se podría clasificar de la siguiente manera:

- *Exploratorio:* tipo de estudio sobre tema poco estudiado. Se identifican por primera vez los rasgos de un fenómeno (Gómez, 2006).
- *Descriptivo:* estudio que caracteriza propiedades, rasgos importantes, del objeto estudiado, presentación de lo «representativo», descripción de tendencias (Gómez, 2006).
- *Correlacional:* estudio que establece relaciones entre los componentes del problema y requiere de análisis comparativo de variables. (Gómez, 2006)
- *Explicativo:* estudio que profundiza en las causas de los eventos. Va más allá de la descripción y el establecimiento de relaciones. Intenta llegar a las causas y generalizar (Gómez, 2006).

Por la caracterización de lo expuesto anteriormente se puede definir que el alcance es tipo descriptivo por su objeto de estudio, por qué se estudiará en consiste la tecnología MPLS así como los elementos que lo integran la solución.

1.9 Tareas

- ✓ Obtención de información relevante de los elementos que conforman la tecnología MPLS.
- ✓ Búsqueda de elementos físicos que soporten la tecnología MPLS
- ✓ Investigación de configuración básica y avanzada de enrutadores que soporten tecnología MPLS
- ✓ Obtención de la herramienta de simulación GNS3 y documentación necesaria para su configuración
- ✓ Descarga de imágenes IOS para los enrutadores que se usen en el diseño de la solución
- ✓ Aprendizaje del manejo y administración de la herramienta de simulación GNS3

CAPITULO II
MARCO TEÓRICO

2.1 Definición de MPLS

MPLS es unatecnología de transmisión de paquetes de alto rendimiento que integra la gestión del rendimiento y el tráficocapacidades de capa de enlace de datos de conmutación con la escalabilidad, flexibilidad y rendimiento dela capa de red de enrutamiento. Permite a los proveedores de servicios para responder a los desafíos provocados porcrecimiento explosivo y proporciona la oportunidad para que los servicios diferenciados sin necesitar lasacrificio de la infraestructura existente.La arquitectura MPLS es notable por su flexibilidad en los datos se pueden transferir a través de cualquier combinación de las tecnologías de capa 2, el apoyo que se ofrece para todos los protocolos de nivel 3.(Cisco, Guia de configuracion Cisco IOS Multiprotocol Label Switching, 2008)

Las etiquetas de MPLS se anuncian entre los enrutadores para que puedan construir un mapeo de etiqueta a etiqueta, estas etiquetas están asociadas a los paquetes IP, permitiendo que los enrutadores reenvíen el tráfico mirandoen la etiqueta y no la dirección de IP de destino. Los paquetes se envían por la conmutación de etiquetasen lugar de por la conmutación IP. El hecho de que las Etiquetas de MPLS se utilizan para reenviar los paquetes y ya no la dirección IP de destino han llevadoa la popularidad de MPLS. Estos beneficios como la mejor integración de IP sobre ATM yla red privada virtual MPLS (VPN) son los más populares en la tecnología MPLS.(Ghein, 2007)

2.2Beneficios de MPLS

MPLS ofrece muchos beneficios importantes a las redes de proveedores de servicios como, soporte escalable para redes privadas virtuales con MPLS que permite a los servicios de VPN tener apoyo en redes de proveedores de servicio, de ese modo acelera en gran medida el crecimiento de Internet.El uso de MPLS para VPN ofrece una alternativa atractiva a la construcción de redes privadas virtuales por medio de o bien circuitos ATM o Frame Relay virtuales permanentes o diversas formas de túneles a enrutadores de interconexión en sitios de clientes.El

modelo MPLS VPN también soporta la comunicación entre sitios VPN sin necesidad de una completa malla de tráfico a través de la red de proveedores de servicios. Para cada usuario de VPN de MPLS, la de red del proveedor de servicios parece funcionar como una red troncal IP privada sobre la que el usuario puede llegar a otros sitios dentro de la organización VPN, pero no los sitios de cualquier otra organización VPN. (Cisco, Guia de configuracion Cisco IOS Multiprotocol Label Switching, 2008)

Otro beneficio es la capacidad de enrutamiento explícito también llamados encaminamiento basado en restricciones o ingeniería de tráfico. En la ingeniería de tráfico MPLS, factores tales como los requisitos de ancho de banda, los requisitos de medios de comunicación y laprioridad de un flujo de tráfico frente a otro puede ser tomado en cuenta. Esta ingeniería de tráficocapacidades permiten que el administrador de una red de proveedores de servicio que realice tareas como control de flujo de tráfico en la red, reducción de la congestión en la red y mejor uso de los recursos de la red (Cisco, Guia de configuracion Cisco IOS Multiprotocol Label Switching, 2008)

Funcionalmente el protocolo MPLS añade una cabecera MPLS a cada paquete IP que ingresa a la WAN, esta acción cambia la forma en cómo los enrutadores de la WAN envían y procesan los paquetes IP. Lo que viaja por la WAN ahora son paquetes IP más una cabecera MPLS de 3 Bytes. La cabecera MPLS es insertada sobre la capa de enlace de datos y bajo la capa de red.

2.2. Componentes de una red MPLS

Los componentes de una red MPLS están dados por los siguientes elementos:

LER (Label Edge Enrutador - Enrutadores de Etiquetas de Borde): es el elemento que inicia o finaliza el túnel, los LER son dispositivos que opera en la periferia de la red de acceso y la red MPLS, el cual se encarga de insertar las etiquetas en base a información de enrutamiento. Un LER soporta múltiples puertos conectados a redes distintas como pueden ser ATM, Frame Relay y Ethernet, envía este tráfico a través de la red MPLS después de haber establecido

un LSP (Caminos conmutados mediante etiquetas) utilizando un protocolo de distribución de etiquetas. También se encarga de retirar las etiquetas y distribuir el tráfico a las redes de salida. (Wordpress, 2013)

LSR (Label Switching Enrutador - Enrutadores Conmutadores de Etiquetas): es un enrutador de alta velocidad en el corazón de la red MPLS, el cual debe soportar los protocolos de enrutamiento IP y participa en el establecimiento de las trayectorias de intercambio de etiquetas utilizando el protocolo de señalización de etiquetas adecuado. Permite conmutación de tráfico de datos a alta velocidad basado en las trayectorias establecidas, típicamente es un conmutador. Además, los enrutadores LSR en MPLS se clasifican en base a la dirección del flujo de datos, como enrutadores ascendentes (upstream, origen) o descendentes (downstream, destino).

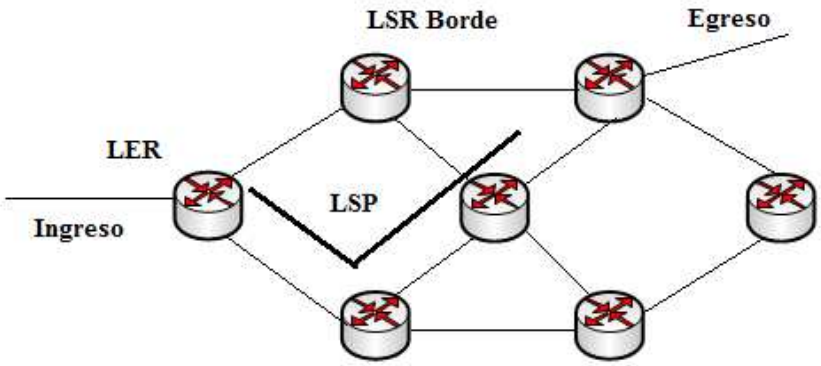

Figura 2.1: Componentes de una red MPLS
Elaborado por: Fausto Orozco Lara

LSP (Label Switched Path - Caminos conmutados mediante etiquetas): nombre genérico de un camino MPLS para cierto tráfico o FEC, es decir del túnel MPLS establecido entre los extremos. Es completamente similar a un canal virtual y puede ser punto a punto, punto a multipunto, multipunto a punto o multipunto a multipunto.

LDP (Label Distribution Protocol - Protocolo de Distribución de Etiquetas): es un protocolo para de distribución de etiquetas, por cada prefijo IGP IP en su tabla de enrutamiento IP, cada LSR crea una unión local es decir, que se une una etiqueta al prefijo IPv4. El LSR luego distribuye esta unión a todos sus vecinos

LDP. Estos enlaces se convierten en enlaces recibidos remotos. Los vecinos luego almacenar estos enlaces remotos y locales en una tabla especial, la base de información de la etiqueta (LIB). Cada LSR tiene sólo una unión local de por prefijo, al menos cuando el espacio de la etiqueta es por plataforma. Si el espacio de la etiqueta es por interfaz, un sello local de unión puede existir por prefijo por interfaz. Por lo tanto, usted puede tener una etiqueta por prefijo o una etiqueta por prefijo por interfaz, pero el LSR obtiene más de un control remoto de unión, ya que por lo general tiene más de un LSR adyacente. (Ghein, 2007)

Dominio MPLS: es la porción de la red donde los procedimientos de enrutamiento y de envío están acorde al protocolo MPLS.

FEC (Forwarding Equivalence Class - Clase Equivalente de Envío): es una representación de un grupo de paquetes que comparten los mismos requerimientos para su transporte. Todos los paquetes en un grupo determinado reciben el mismo trato, y siguen una misma ruta hacia su destino. En oposición al envío convencional por IP, en MPLS la asignación de un FEC particular a un paquete en particular se hace solo una vez, cuando el paquete entra a la red. Los FEC se basan en requerimientos de servicio para un conjunto dado de paquetes o simplemente para un prefijo de dirección.

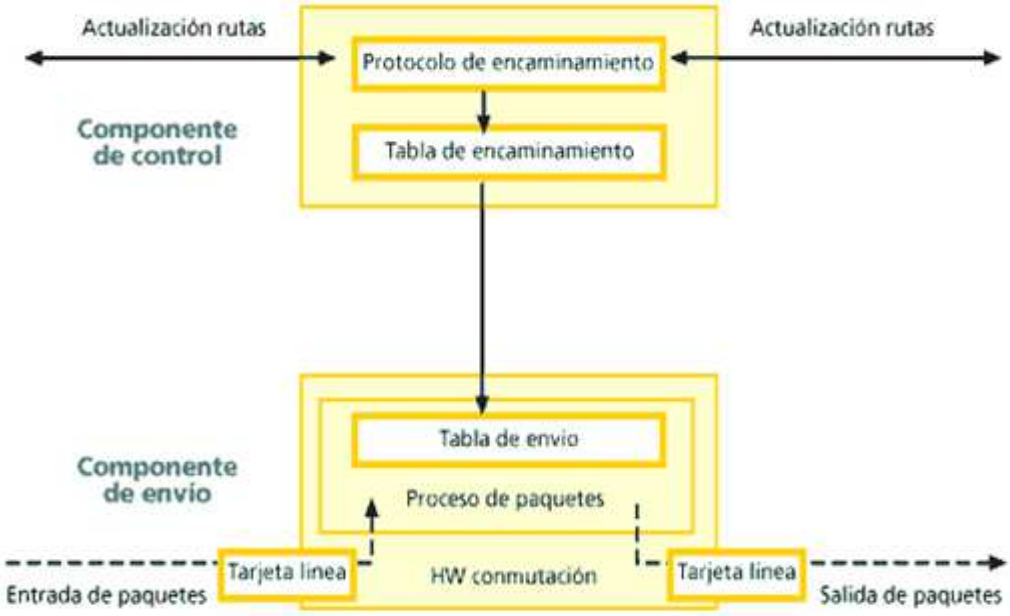

Figura 2.2: Funcionamiento de red MPLS
Fuente: Madrid, reproducción de ponencia presentada en el Congreso Usuarios de Internet, 2000

Cada LSR construye una tabla la cual especifica cómo será enviado cada paquete; a esta tabla se conoce como base de información de etiqueta (LIB). La funcionalidad de MPLS está compuesta en los componentes funcionales de envío y control y el intercambio de etiquetas para el envío de datos.(Rediris, 2013)

2.3 Cabecera MPLS

Una etiqueta MPLS es un número de 20 bits que se asigna a un prefijo de destino en un router que define las propiedades del prefijo, así como mecanismos de reenvío que se pueden realizar para un paquete destinado para el prefijo. (Lobo, 2005)

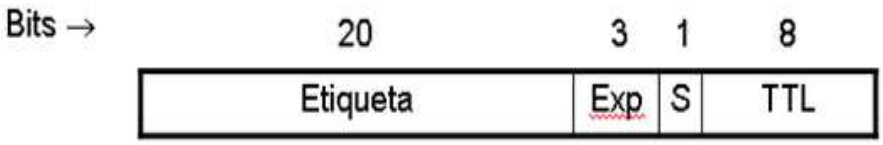

Figura 2.3: Etiqueta MPLS

Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

Una etiqueta MPLS se compone de las siguientes partes:

- Valor de la etiqueta de 20 bits
- 3 bits para campo experimental
- 1 bit para indicador de fondo de pila
- 8 bits para tiempo de vida de paquete

El valor de la etiqueta de 20 bits es un número asignado por el router que identifica el prefijo en cuestión. Las etiquetas pueden ser asignadas ya sea por interfaz o por chasis. El campo experimental de 3 bits define la clase de servicio asignados a la FEC en cuestión que se le ha asignado una etiqueta. Una pila de etiquetas es un conjunto ordenado de etiquetas, donde cada etiqueta tiene una función específica. Si el router (Edge LSR) aplica más de una etiqueta en un solo paquete IP, que conduce a lo que se llama una pila de etiquetas, donde se imponen varias etiquetas en un único paquete IP. Por lo tanto, el indicador de fondo de pila identifica si la etiqueta que se ha encontrado es la etiqueta inferior de la pila de etiquetas. El campo TTL realiza la misma función que un TTL IP, donde el paquete se descarta cuando el TTL del paquete es 0, lo que impide en bucle de

paquetes no deseados en la red. Cuando un paquete etiquetado atraviesa un LSR, el valor TTL etiqueta se disminuye en 1. (Lobo, 2005)

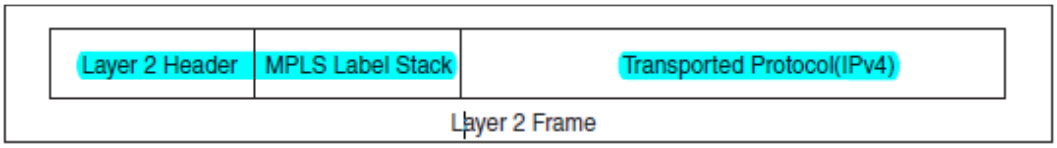

Figura 2.4: **Encapsulado para etiquetas**
Fuente: Fundamentos MPLS por Luc de Ghein

2.3.1 Pila de Etiquetas MPLS

MPLS puede ser que necesite más de una etiqueta en la parte superior del paquete a la ruta a través de la red MPLS, esto se hace mediante las etiquetas de embalaje en una pila. La primera etiqueta de la pila se llama la etiqueta superior y la última etiqueta que se llama la etiqueta inferior. En el medio, puede tener cualquier número de etiquetas(Ghein, 2007).

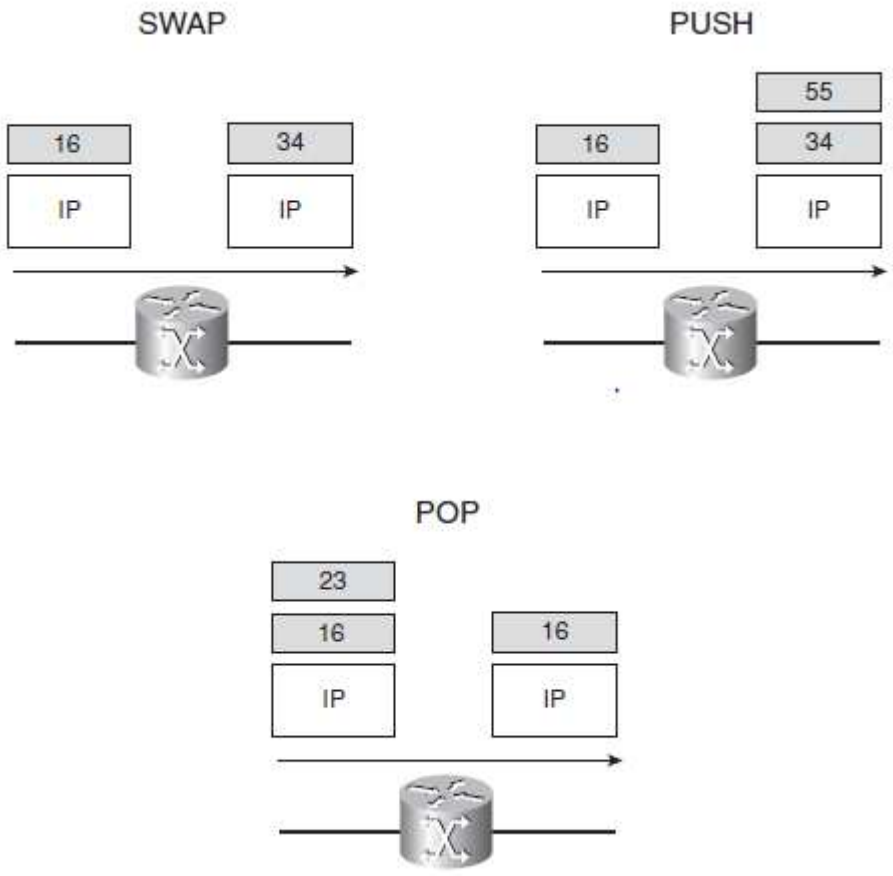

Figura 2.5: Apilamiento de etiquetas
Fuente: Fundamentos de MPLS por Luc De Ghein

El bit de QoS es 0 para todas las etiquetas excepto la etiqueta inferior que es 1. Algunas aplicaciones de MPLS en realidad necesitan más de una etiqueta en la pila de etiquetas para reenviar los paquetes etiquetados. Ejemplos de este tipo de aplicaciones MPLS son MPLS VPN y Atom. MPLS trabaja incorporando un encabezado a cada paquete el cual puede tener una o más etiquetasy al conjunto de etiquetas se le denomina pila. Estos paquetes MPLS son despachados después de una exploración de etiquetas en vez de una dentro de una tabla IP, por lo cual la búsqueda de etiquetas y el envío son más rápido que una búsqueda RIB (Base de información de Ruteo), ya que son hechas en el switch fabric y no en la CPU.

Un paquete en MPLS puede tener más de una etiqueta, organizadas a modo de pila, que es a lo que se conoce como pila de etiquetas. Aunque MPLS soporte una jerarquía gracias a la pila de etiquetas, el procesamiento de un paquete etiquetado es completamente independiente del nivel de la jerarquía. Siempre que se procese una etiqueta, ésta será la de la cima, sin importar cuántas etiquetas pueda haber debajo.

Las posibles operaciones de etiquetas son de intercambio (swap), empujar (push), y pop. Al mirar la etiqueta de la parte superior del paquete etiquetado recibido y la entrada correspondiente en la LFIB, la LSR sabe cómo reenviar el paquete. El LSR determina lo que necesita la operación etiqueta a realizar-swap, empujar, o pop y lo que el siguiente salto es la que necesita el paquete que se transmitirá. La operación de intercambio significa que la etiqueta superior en la pila de etiquetas se sustituye con otra, y la operación de empuje significa que la etiqueta superior se sustituye con otra y luego una o más etiquetas adicionales se inserta en la pila de etiquetas. La operación pop significa que la etiqueta superior es eliminada. (Ghein, 2007)

2.3.2 Etiquetas especiales de salida

Los enrutadores conmutadores de etiquetas llevan a cabo la operación de adherir, remover e intercambiar etiquetas dependiendo de su ubicación sobre su dominio local MPLS. A un paquete de datos se le puede asociar un conjunto de etiquetas especiales las cuales pueden ser:

- ***Untagged:*** es una transición de un dominio MPLS a un dominio IP, el paquete MPLS es convertido a un paquete IP y enviado a su destino. Este proceso es empleado en la implementación de MPLS VPN (Lobo, 2005)

- ***Implicit-null o POP label:*** esta etiqueta es asignada cuando, la etiqueta del tope superior de la pila es removida y el paquete resultante es enviado al próximo salto hacia el enrutador vecino downstream. El valor de esta etiqueta es 3, es usada en redes MPLS que implementan la preparación del penúltimo salto (Lobo, 2005)

- ***Explicit-null Label:*** esta etiqueta es asignada para preservar el valor EXP de la etiqueta tope de un paquete. La etiqueta del topo es cambiada con un valor de 0 y enviada hacia el próximo salto a su vecino downstream. Esta etiqueta es empleada para la implementación de QoS con MPLS (Lobo, 2005)

- ***Aggregate:*** en esta etiqueta el paquete MPLS es convertido a un paquete IP y un proceso de consulta es llevado a cabo para identificar la interfaz de salida para el destino deseado. De igual forma este proceso se emplea para la implementación de MPLS VPN (Lobo, 2005)

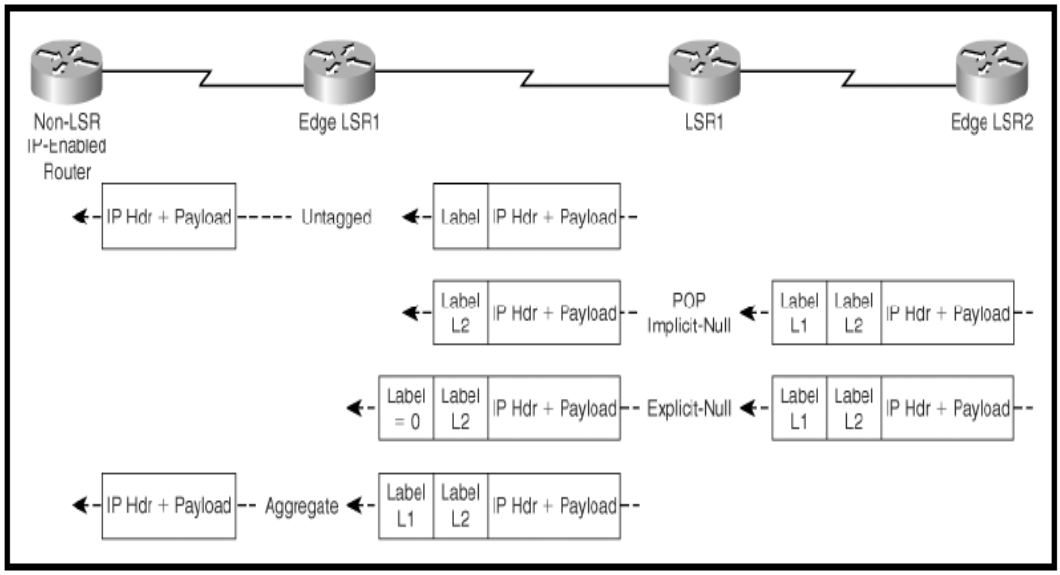

Figura 2.6: Etiquetas especiales de salida
Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

2.4 Arquitectura MPLS

La arquitectura MPLS está conformada básicamente por dos bloques: plano de control y plano de datos

Plano de control: es la encargada de llevar a cabo tareas destinadas a determinar la disponibilidad del acceso hacia una red destino. Por lo tanto el plano de control contiene toda la información de direccionamiento de la capa tres. Algunos ejemplos comunes acerca de las funciones de la capa de control es el intercambio de información por parte de los protocolos de enrutamiento tales como OSPF y BGP. Por lo tanto el intercambio de información acerca del direccionamiento IP es una función del plano de control, además de todas las funciones que cumplen aquellos protocolos responsables del intercambio de etiquetas entre enrutadores vecinos tal como el protocolo de distribución de etiquetas (Lobo, 2005)

Plano de Datos: lleva a cabo tareas relacionadas con el forwarding o envío de paquetes. Esos paquetes pueden ser ya sea paquetes IP o paquetes IP etiquetados. La información en el plano de datos, tal como el valor que llevan las etiquetas, se obtienen del plano de control (Lobo, 2005)

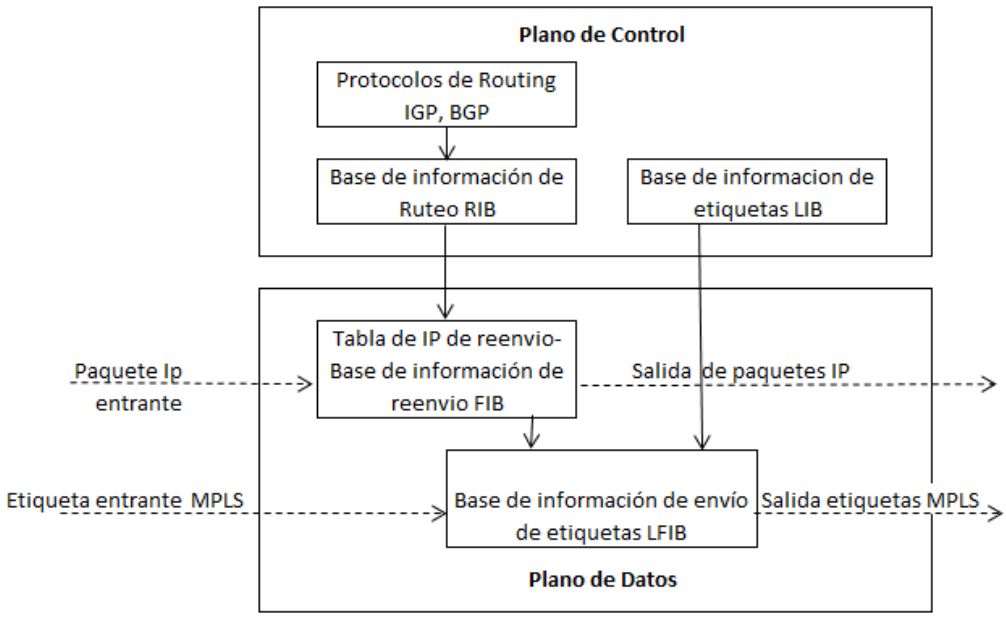

Figura 2.7: Componentes de Cabecera
Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

2.5 Operación de MPLS

La puesta en práctica de MPLS para el envío de datos involucra las siguientes tareas:

- Asignación de etiquetas MPLS, por LSR
- Establecimiento de un sesión LDP o TDP de MPLS, entre LSRs /E-LSRs
- Distribución de etiquetas MPLS
- Retención de etiquetas MPLS

La operación MPLS involucra a enrutadores conmutadores de etiquetas adyacentes formando una sesión LDP asignando etiquetas locales a prefijos de destino y cambiando estas etiquetas durante las sesiones LDP establecidas (Lobo, 2005)

2.5.1 Asignación de etiquetas MPLS

Los protocolos de enrutamiento IP indican que tan accesible es una red destino y son los encargados de generar secuencias de saltos para los paquetes dentro de una red, el mismo proceso tiene que ser implementado para enrutadores o dispositivos que son parte del dominio MPLS, es decir la red automáticamente establece valores de etiqueta entre dispositivos adyacentes. Esta operación crea caminos conmutados mediante etiquetas, es decir mapas pre configurados entre puntos finales de destino. El protocolo de distribución de etiquetas LDP asigna y cambia etiquetas entre LSRs adyacentes en un dominio MPLS, luego del establecimiento de la sesión (Lobo, 2005)

2.5.2 Establecimiento de la sesión LDP

Después de la asignación de etiquetas en el enrutador, son distribuidas entre LSRs directamente conectados siempre y cuando las interfaces entre ellos estén activadas para el envío MPLS, esto se realiza usando LDP. Existen cuatro categorías de mensajes LDP:

- ***Mensajes de descubrimiento:*** son los que anuncian y mantienen una presencia LSR en la red
- ***Mensajes de Sesión:*** establecen, mantienen y remueven las sesiones entre LSR

- ***Mensajes de advertencia:*** anuncian la correspondencia de etiquetas a las clases equivalente de envío
- ***Mensajes de notificación:*** muestra las señales de errores

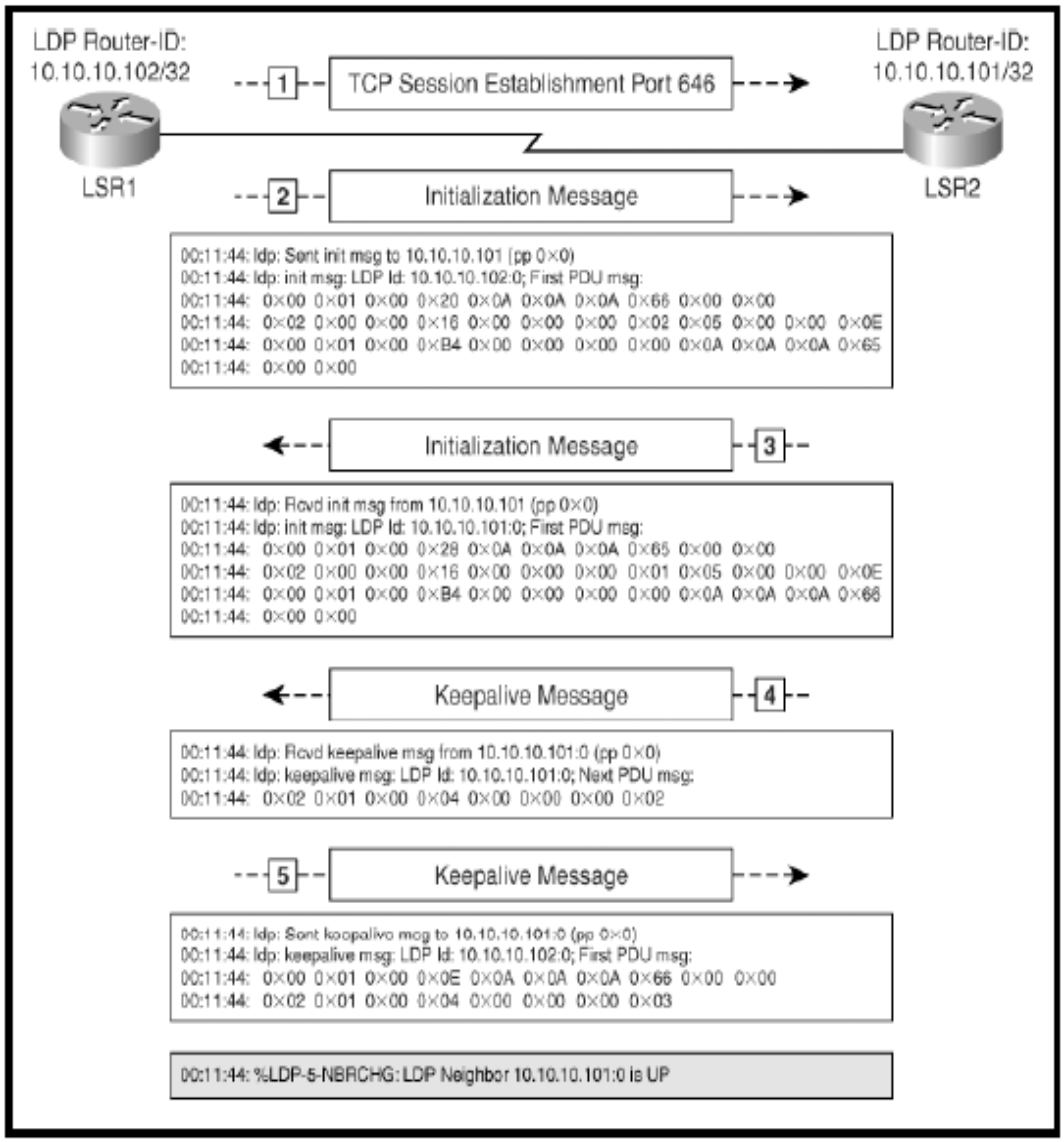

Figura 2.8: Establecimiento de sesión LDP
Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

Todos los mensajes LDP siguen el tipo, longitud, formato de valor (TLV), por defecto LDP usa el puerto 646 de TCP, de donde el procedimiento para establecer la sesión LDP es la siguiente:

1. Las sesiones LDP son iniciadas cuando un LSR envía saludos periódicos sobre las interfaces permitidas para el envío MPLS, si otro LSR está conectado con esa interfaz y está habilitada para MPLS, el LSR directamente conectado intenta establecer una sesión con la fuente de los

mensajes de saludos del LDP. El LSR con la ID más alta del enrutador LDP es el LSR activo. El LSR activo intenta abrir una conexión TCP con el LSR pasivo sobre el puerto 646 de TCP.

2. El LSR envía un mensaje de inicialización al LSR básico que contiene información tal como el método de distribución de etiqueta, tiempo de sesión, longitud máxima PDU, ID LDP del receptor, y si el bucle de detección está activado.
3. El LDP LSR pasivo responde con un mensaje de inicialización si los parámetros son aceptables, sino lo son el LDP LSR pasivo envía una mensaje de notificación de error.
4. LSR pasivo envía el mensaje keepalive al LSR activo después de enviar un mensaje de inicialización
5. El LSR activo envía paquetes de tiempo de vida al LDP LSR pasivo y la sesión LDP tiene lugar, en ese momento los planos de etiquetas FEC puede ser cambiados entre los LSR. (Lobo, 2005)

2.5.3 Distribución de etiquetas MPLS con LDP

En un dominio MPLS dirigido LDP, una etiqueta es atribuida a un prefijo de destino encontrado en el FIB y es distribuido a vecinos upstream en el dominio MPLS después del establecimiento de la sesión. Las etiquetas que son de significado local para el enrutador son cambiadas con LSRs adyacentes durante la distribución de etiquetas. La unión de etiquetas de un prefijo específico para una etiqueta local y una etiqueta del próximo salto es entonces guardada en LFIB y las estructuras de LIB. Los métodos de distribución de etiquetas usados en MPLS son:

- ***Dowstream on demand***: permite que un LSR pida explícitamente de su enrutador downstream la etiqueta correspondiente para un prefijo destino particular, conocido como distribución de etiqueta bajada sobre demanda (Lobo, 2005)
- ***Unsolicited dowstream:*** permite que un LSR distribuya etiquetas a LSR upstream que no los ha pedido explícitamente y es referido como la distribución de etiqueta bajada no solicitada (Lobo, 2005)

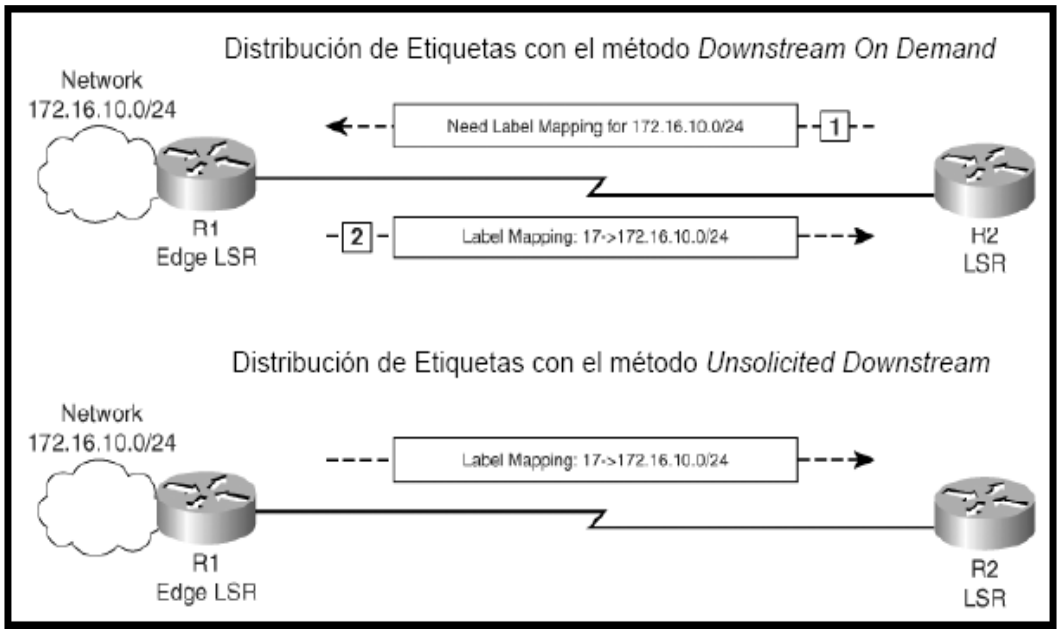

Figura 2.9: Tipos de distribución de etiquetas
Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

2.5.4 Retención de etiquetas MPLS

Si un LSR soporta el denominado modo liberal de retención de etiquetas, entonces mantiene las etiquetas que son recibidos de los LSR downstream que no puede ser el próximo salto para ese destino. Si un LSR soporta el modo conservador de retención de etiquetas entonces descarta las etiquetas recibidas de los LSR downstream que no constituyen el próximo salto para ese destino, por lo tanto con el modo de retención liberal un LSR puede empezar casi inmediatamente el envío de paquetes etiquetados después de la convergencia de IGP (Protocolo de pasarela interior), donde es grande el número de etiquetas mantenidos para un destino especial y por lo tanto consumen memoria. Con la retención de etiquetas conservadoras, las etiquetas mantenidas son etiquetas de LDP confirmadas que por lo tanto consumen mínima memoria (Lobo, 2005)

2.6 Aplicaciones de MPLS

Entre las aplicaciones más importantes que maneja MPLS tenemos las siguientes:

- Ingeniería de trafico TE
- Implementación de QoS en MPLS
- Redes Privadas Virtuales

2.6.1 Ingeniería de tráfico en MPLS

Ingeniería de tráfico es el proceso de mapear la demanda de tráfico sobre la topología de la red. Es la habilidad de controlar el flujo de tráfico sobre la red. Se establece que la ingeniería de trafico concierne a la optimización de la performance de una red e involucra diversas áreas: mediciones de tráfico, modelado de tráfico y redes, control del tráfico en Internet, evaluación de performance. (Guichard, 2003)

Se establece que los principales objetivos de TE son:

- Mover el tráfico del camino establecido por el IGP(Protocolo de pasarela interno) a un camino menos congestionado
- Utilizar el exceso de ancho de banda sobre los enlaces sub-utilizados
- Maximizar la utilización de los enlaces y nodos de la red.
- Aumentar la confiabilidad del servicio
- Alcanzar requerimientos impuestos

Los requerimientos pueden ser:

- Orientados al tráfico: pérdidas de paquetes, retardos, etc.
- Orientados a los recursos: básicamente utilización de capacidad de la red.

Las acciones de control tomadas al realizar TE pueden involucrar:

- Modificación de los parámetros de gestión de tráfico
- Modificación de los parámetros asociados al ruteo
- Modificación de los parámetros y atributos asociados con los recursos

En general se busca también minimizar la intervención manual para tomar acciones de control. La ingeniería de tráfico debe resolver tres problemas básicos:

- Cómo mapear paquetes en FEC
- Cómo mapear FEC en troncales tráfico.
- Cómo mapear troncales en la red física

2.6.2 Implementación de QoS en MPLS

Es la habilidad para diferenciar diversas clases de servicio y asignarles prioridades sobre cada enrutador en la red. El primer paso para la implementación de QoS es

identificar las distintas clases de tráfico que la red va a soportar. El tráfico puede ser clasificado basado en el tipo como voz, aplicaciones, datos, etc., y sobre las propiedades de patrones de tráfico, luego de que el tráfico ha sido clasificado el próximo paso es identificar que operaciones de QoS serán llevadas a cabo para cada uno de esos tipos sobre el enrutador local. Debemos notar que aunque QoS es una implementación extremo-extremo, debe ser configurada sobre cada enrutador en el camino desde el origen al destino, sin embargo varias secciones de la red pueden ser configuradas con diferentes esquemas de QoS para mejorar distintos tipos de tráfico. Este proceso de definir las operaciones de QoS para un cierto tipo de tráfico se denominan Políticas de servicio.

2.6.3 Redes privadas virtuales

Entendemos por red privada virtual a la interconexión de un conjunto de ordenadores haciendo uso de una infraestructura pública, normalmente compartida, para simular una infraestructura dedicada o privada. Una VPN también es vista como una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas, al fin y al cabo no es más que la creación en una red pública de un entorno de carácter confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local.(WordpressMpls, 2013)

2.6.3.1 Funcionamiento de Redes Privadas virtuales

El funcionamiento de una VPN es similar al de cualquier red normal, aunque realmente para que el comportamiento se perciba como el mismo hay un gran número de elementos y factores que hacen esto posible. La información entre los mismos se efectúa con túneles virtuales y usando sus respectivos procedimientos de seguridad que cerciorenla confiabilidad e integridad de los datos transferidos.

2.6.3.2 Tipos de encriptación

Todas las VPN trabajan con algún tipo de tecnología de encriptación, para garantizar integridad de los datos para su traslado por la red pública. La encriptación hay que considerarla tan esencial como la autenticación, ya que

permite proteger los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. (WordpressMpls, 2013).

- **En la encriptación con clave secreta:** se usa una contraseña secreta conocida por todos los participantes que van a hacer uso de la información encriptada. La contraseña se utiliza tanto para encriptar y desencriptar la información. Este tipo de sistema tiene el problema que, al ser compartida por todos los participantes y debe mantenerse secreta, al ser revelada, tiene que ser cambiada y distribuida a los participantes, lo que puede crear problemas de seguridad (WordpressMpls, 2013).
- **La encriptación de clave pública:**se necesita dos claves una pública la que se envía a todos los involucrados y una secreta para proceso de desencriptación, su principal desventaja es que la encriptación es más lenta que la de clave secreta. (WordpressMpls, 2013).

2.6.3.3 Tipos de VPN

La VPN es un servicio que ofrece conectividad segura y confiable en una infraestructura de red pública compartida, como la Internet y conservan las mismas políticas de seguridad y administración que una red privada. A continuación se describen los principales tipos de VPN:

VPN de acceso remoto

El modelo más usado que consiste en usuarios o proveedores que acceden con la empresa desde lugares distantes como oficinas, domicilios, hoteles, etc. teniendo como medio principal el servicio de internet para acceder.(VPN, 2013)

Figura 2.10: VPN de acceso remoto

Fuente: México, referenciado de empresa de tecnología nethumans, 2013

Luego que se haya realizado la validación respectiva van a poder trabajar como si estuviese conectado localmente en la compañía. (VPN, 2013)

VPN sitio-a-sitio

Se usa para conectar oficinas remotas con la sede principal de la organización. El equipo central VPN tiene acceso a Internet permanente y está a la espera de conexiones vía Internet provenientes de los sitios para establecer la conexión VPN, las sucursales se enlazan usando servicios de su proveedor (VPN, 2013)

Figura 2.11: VPN sitio a sitio
Fuente: México, referenciado de empresa de tecnología nethumans, 2013

Tunneling

Consiste en encapsular un protocolo de red sobre otro protocolo de red encapsulador creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. (VPN, 2013).

VPN Interna

Es el menos difundido pero uno de los más poderosos para usar dentro de la empresa. Es una variante del tipo acceso remoto pero en vez de utilizar Internet como medio de conexión, emplea la misma red LAN de la empresa. Sirve para aislar zonas y servicios de la red LAN interna. (VPN, 2013).

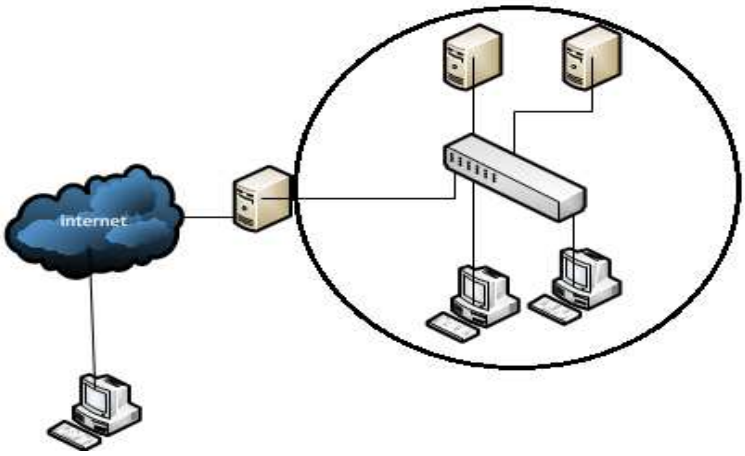

Figura 2.12: VPN interna
Elaborado por: Fausto Orozco Lara

2.6.3.4 Protocolos usados en VPN

Existe gran variedad de protocolos para el uso de VPN entre los cuales podemos mencionar los más importantes como los siguientes:

PPTP

PPTP Point-to-Point Tunneling Protocolo es un protocolo que fuedesarrollado por un consorcio de fabricantes, incluyendo Microsoft, 3Com, Ascend y Comunicaciones. Como L2F, PPTP permite que el túnel de cliente de acceso remoto PPP cuadreentre un NAS y un gateway VPN/concentrador.El Protocolo de túnel punto a punto (PPTP) es una extensión de la norma PPP Protocolo (a Punto Punto). Los servicios proporcionados por túneles PPTP están destinados a montar en la parte superior de la capa de IP, mientras que el protocolo PPP tradicional subyace IP. PPP era ideal para la modificación debido a que su funcionalidad ya imita el comportamiento de lo que necesitaría un VPN: un túnel punto a punto. Lo único que faltaba era la seguridad. PPTP, sin embargo, es más de un canal de host a host comunicaciones seguras, en lugar de una LAN-to-LAN. Aunque es muy posible para enrutar el tráfico a través de un túnel PPTP, las soluciones IPSec se adapten mejor para este tipo de aplicación.(Scott, 1999)

IPSec

El protocolo de seguridad de Internet (IPSec) es una estructura genérica iniciado y mantenido por un grupo de trabajo de la IETF para proporcionar diversos

servicios de seguridad para el protocolo de Internet (IP), tanto para IPv4 e IPv6. IPSec presenta objetivos de diseño para una estructura orientada a componentes de nivel superior, en lugar de detallar los algoritmos de cifrado específicas o metodologías de intercambio de claves.Conceptualmente, IPSec fue creado para asegurar la propia red, que no presentó cambios reales a las aplicaciones que se ejecutan por encima de ella. Dado que el protocolo TCP/IP es tan general es una evolución natural para producir un sistema de red segura desarrollado casi en paralelo con el sistema existente.

Los documentos IPSec reproducidos por la IETF son en su mayoría preocupados por tres áreas básicas de asegurar el protocolo IP: algoritmos de encriptación, algoritmos de autenticación y gestión de claves, estos componentes ayudan a definir toda la arquitectura de un sistema de seguridad. IPSec se ha diseñado para que los nuevos métodos se puedan añadir a la suite con muy poco trabajo y poco efecto sobre las implementaciones anteriores.(Scott, 1999)

IPSec fue diseñado para soportar dos modos de cifrado. El modo de transporte protege sólo la parte de carga útil de cada paquete, mientras que el modo de túnel encripta el encabezado y la carga útil. Lógicamente, el modo de túnel es más seguro, ya que protege la identidad del remitente y el receptor, así como ocultar ciertos otros campos de IP que pueden dar un intermediario de información útil.Para IPSec funcione como se esperaba, todos los dispositivos deben compartir una clave común. A pesar de que los protocolos utilizados para cifrar los datos son muy importantes para el éxito global del sistema, una gran cantidad de trabajo ha sido la autenticación y el intercambio de claves por el remitente y el receptor. (Scott, 1999)

L2TP

L2TP (Layer 2 Tunneling Protocol) fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661). L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El

transporte de L2TP está definido para una gran variedad de tipos de paquete de datos, incluyendo X.25, Frame Relay y ATM.Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.(Wikipedia, 2014)

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.(Wikipedia, 2014)

2.6.3.5 VPN en MPLS

Una de las aplicaciones de uso más popular de MPLS es la creación de VPN. En lo que concierne a los proveedores de servicios de Internet, MPLS ha simplificado la configuración e implementación de soluciones VPN para sus usuarios. MPLS también facilita la interconexión de diferentes usuarios, cuando ellos lo soliciten. Las redes privadas virtuales fueron originalmente introducidas para permitir a los proveedores de servicios usar una infraestructura física común para implementar la emulación de enlaces punto a punto. En redes tradicionales basadas en enrutadores diferentes puntos de clientes se conectan uno con otro empleando enlaces dedicados. El costo de una implementación es dependiente del número de clientes conectados así como de la participación del proveedor de servicio en el proceso de enrutamiento al cliente, la implementación de una VPN puede ser:

- Modelo de capa superpuesta(Overlay Model)
- Modelo igual-igual (peer to peer Model)

Las redes privadas virtuales de modelo de capa superpuesta fueron inicialmente implementadas por los proveedores de servicio para establecer conectividad de capa 1 o una capa 2 de transporte entre las ubicaciones clientes. En cuanto a la implementación de capa 1, el proveedor establecería la conectividad de capa física

entre sitios del cliente y el cliente era el responsable de todas las otras capas. En cuanto a la implementación de la capa 2 el proveedor de servicios era el responsable del transporte de las tramas de capa 2 entre los sitios clientes, lo cual era tradicionalmente la red del proveedor era transparente al cliente y los protocolos de enrutamiento corrían directamente entre los enrutador de los clientes (Lobo, 2005)

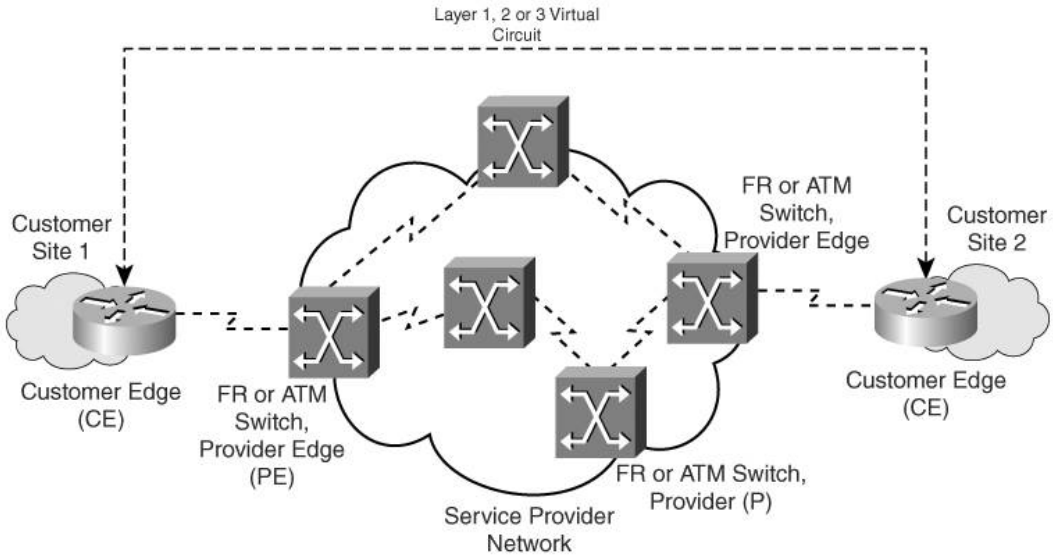

Figura 2.13: Modelo de capa superpuesta

Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

El modelo igual-igual fue desarrollado para superar las desventajas del modelo de la capa superpuesta y proveer a los clientes de una vía optima de transporte a través el backbone del proveedor de servicios.

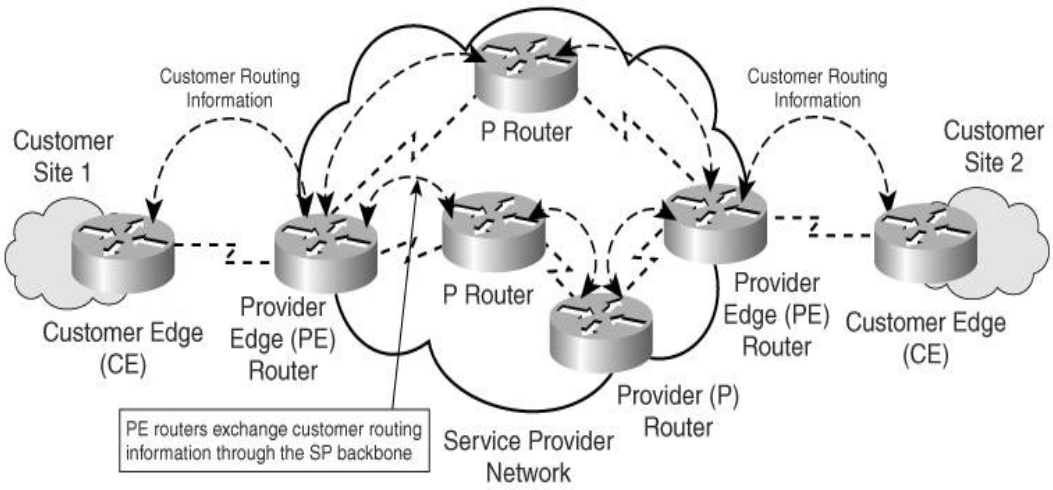

Figura 2.14: Modelo de igual a igual

Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

Por lo tanto el proveedor de servicios podría participar activamente del proceso de enrutamiento. En el modelo igual-igual la información de enrutamiento es intercambiada entre los enrutadores clientes y los enrutadores de los proveedores de servicio, en consecuencia los datos del cliente son transportados a los largo del proveedor de manera optima (Lobo, 2005)

2.6.3.5.1 Arquitectura de y terminología VPN en MPLS

El dominio MPLS VPN al igual que la tradicional VPN consiste en una red cliente y una red del proveedor, el modelo MPLS VPN es muy similar al modelo dedicado de un enrutador PE en una implementación punto a punto, sin embargo en lugar de implementar un enrutador PE dedicado por cliente, el tráfico del cliente es asignado sobre el mismo enrutador PE que establece conectividad de la red del proveedor de servicios con múltiples clientes (Lobo, 2005).

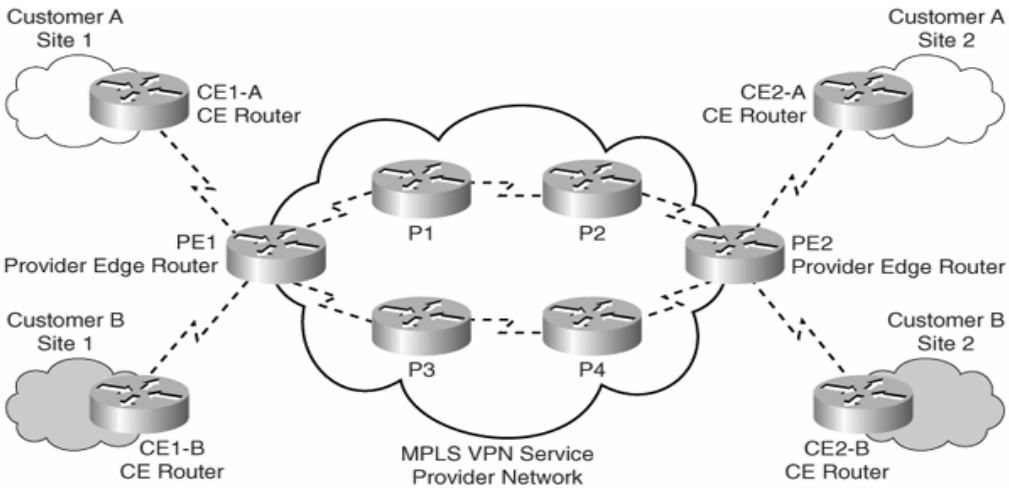

Figura 2.15: Arquitectura de red MPLS VPN
Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

Los principales componentes de una arquitectura MPLS VPN son:

- ***Red cliente (CN):*** usualmente consiste del dominio del cliente conformado por dispositivos o enrutadores que abarcan múltiples sitios pertenecientes al cliente
- ***Enrutador CE:*** son los enrutadores en la red del cliente se conectan con la red del proveedor

- ***Red del proveedor:*** es el dominio del proveedor conformado de los enrutadores extremo PE y los enrutadores de backbone que conectan sitios pertenecientes al cliente a una infraestructura compartida. El proveedor de red controla el enrutamiento del tráfico entre sitios pertenecientes al cliente
- ***Enrutadores PE***: son los enrutadores de la red del proveedor que se conectan al enrutador extremo del cliente
- ***Enrutadores P*** son los enrutadores en el núcleo de la red del proveedor que se conectan con otros enrutadores núcleo o con los extremos PE

2.6.3.5.2 Modelo de enrutamiento VPN en MPLS

La implementación de VPN MPLS es muy similar al modelo dedicado punto apunto desde la perspectiva de un enrutador cliente CE, los datos son enviados al enrutador PE. Los enrutador CE no requieren de una configuración específica para ser parte de un dominio VPN MPLS. El único requerimiento de un enrutador cliente CE es un protocolo de enrutamiento que permita el intercambio de información de ruta con el enrutador PE del proveedor (Lobo, 2005)

En la implementación de MPLS VPN, el enrutador PE lleva a cabo múltiples tareas, en primer lugar debe ser capaz de aislar el tráfico de un usuario, si más de un cliente está conectado al enrutador PE. Cada cliente por lo menos tiene asignado una tabla de enrutamiento independiente. El enrutamiento a través de la red del proveedor es llevado a cabo usando un proceso de ruta en la tabla de enrutamiento global.

Los enrutadores P permiten la conmutación de etiquetas entre los enrutadores extremo del proveedor, los enrutadores en la red del cliente no es tan consciente acerca de lo enrutador P y por lo tanto la topología de la red del proveedor es transparente al cliente. Los enrutadores P únicamente son responsables de la conmutación de etiquetas de los paquetes y no llevan rutas VPN y no participan en el enrutamiento VPN MPLS. Los enrutadores PE intercambian rutas IPv4 conectadas a los enrutadores CE usando protocolos de enrutamiento (Lobo, 2005)

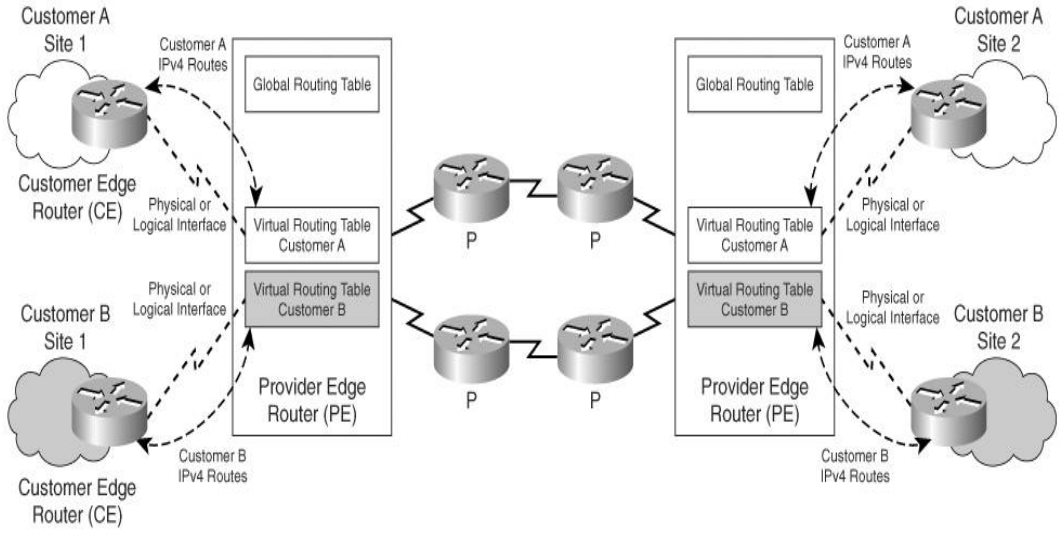

Figura 2.16: Arquitectura MPLS VPN
Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

2.7 Preparación del Penúltimo Salto

Se da en redes MPLS donde el enrutador upstream al E-LSR remueve la etiqueta tope de la pila de etiquetas y envía solo el paquete resultante para un FEC particular, este proceso es indicado por el enrutador E-LSR downstream durante la distribución de etiquetas con LDP. El enrutador E-LSR dowstream distribuye una implicit-null (POP) label hacia el enrutador upstream indicándole que debe remover la etiqueta tope y enviar el paquete resultante, entonces cuando el paquete es recibido por el enrutador E-LSR no se lleva a cabo una consulta en LIB, si el paquete que llega es un paquete IP. Por lo tanto el penúltimo salto evita un proceso de consulta a E-LSR (Lobo, 2005)

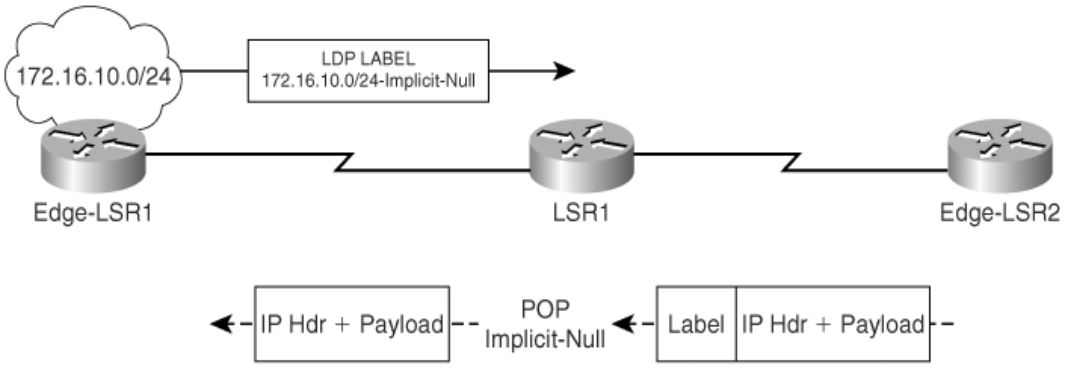

Figura 2.17: Penúltimo salto
Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

CAPITULO III
DISEÑO Y ANALISIS DE LA RED MPLS

3.1 Planteamiento del diseño de la red

La tecnología Ethernet ha evolucionado a gran escala en las últimas décadas, con las tecnologías que día a día van soportando enlaces más rápidos u otras características sobresalientes sobre la transmisión de datos. La evolución de la tecnología Ethernet ha provocado que sea la tecnología dominante en las redes de área local (LAN), lo cual hace que se establezca cada día más firme en el ámbito empresarial, con aproximadamente 95% del tráfico en todas las empresas. Las LAN con tecnología Ethernet no garantizan la mayoría de los parámetros necesarios para la obtención de calidad en el servicio tales como: disponibilidad, pérdida de tramas, reordenamiento de tramas, duplicación de tramas, retardo de tránsito y tiempo de vida de la trama. Por lo tanto, Ethernet no fue diseñada pensando en la calidad de los servicios, es aquí donde entra MPLS el cual es una tecnología de conmutación de paquetes que se encuentra entre los niveles 2 y 3 del modelo OSI, lo que posibilita mejorar la funcionalidad de capa 2 en Ethernet sin sacrificar sus prestaciones. Por este motivo, MPLS es estratégicamente importante debido a que ofrece una clasificación y conducción rápida de paquetes y que dispone de un mecanismo de túnel eficiente. En el presente capítulo se plantea el análisis y diseño de una red VPN MPLS para la Universidad de Guayaquil con la Carrera de Ingeniería en Networking, estableciendo aspectos técnicos como el tráfico de datos entre la carrera y matriz, configuraciones generales así como equipos mínimos necesarios para poder cumplir con una implementación de esta magnitud.

3.2 Equipos a usar en una red MPLS

El backbone MPLS puede estar formado por muchos equipos dependiendo de la necesidad de la implementación, situación económica o infraestructura propia de la empresa que tenga, para nuestro caso mencionaremos los más destacados que se pueden aplicar en una estructura como la que se plantea en el proyecto actual, los mismos se destacaran a nivel de capa 2 y capa 3 como los que mencionaremos a continuación:

Serie Cisco Catalyst 2950

Los switches de la serie Cisco 2950 proveen acceso Ethernet sobre redes de fibra óptica, es un modelo apilable y proporciona puertos para fastethernet y gigabit Ethernet, esta serie permite ofrecer servicios inteligentes con mayor seguridad, disponibilidad y calidad de servicio, características ideales para su ubicación al borde de la red. El software IOS ofrece funcionalidad para la transmisión de datos, video y servicios de voz mediante la configuración automática de la Calidad de Servicio mediante políticas de clasificación y discriminación de los distintos flujos de tráfico propio del software, es decir soportan DiffServ.

Figura 3.1: Cisco Catalyst 2950
Fuente: Obtenida de sitio web de proveedor Cisco

En la tabla 3.1 se mencionan algunos de los modelos de la familia cisco catalyst switch 2950 que se podrían utilizar, así como sus respectivos puertos y características más relevantes.

Tabla 3.1: Productos de la serie 2950

Producto	Puertos	Características
WS-C2950ST-24-LRE	2 puertos 10/100/1000 BASE-T (uplink), 24 LRE y 2 SPF.	Proveen acceso a los servicios de banda ancha sobre el cableado telefónico.
WS-C2950ST-8-LRE	2 puertos 10/100/1000 BASE-T (uplink), 8 LRE y 2 SPF.	
WS-C2950-24	24 puertos 10/100 y 2 puertos 100BASE-FX (uplink)	16 MB de memoria DRAM y 8 MB de memoria Flash.

Fuente: Obtenida de sitio web de proveedor Cisco

Serie Cisco Catalyst 2960

El switch WS-C2960-24TT-L, perteneciente a la serie 2960 ofrece conectividad Fast Ethernet y Gigabit Ethernet incluyendo características de seguridad mediante ACL80 y control de admisión a la red además de QoS y soporte de servicios inteligentes mediante multidifusión, características adecuadas para su utilización al borde de la red. La seguridad de la red se garantiza con el manejo de una amplia gama de métodos de autenticación, tecnologías de encriptación de datos, puertos y direcciones MAC.

Las características más relevantes del switch WS-C2960-24TT son las siguientes:

- Posee 24 puertos Ethernet de 10/100BASE-T y dos enlaces ascendentes de 10/100/1000TX.
- Proporciona mejoras para spanning tree.
- Configuración de hasta 255 VLAN por puerto.
- La tasa de envío basada en paquetes de 64bytes es de 6.5Mpps.
- 64 MB de memoria DRAM y 32 MB de memoria Flash.
- Soporte para MPLS e IPv6.

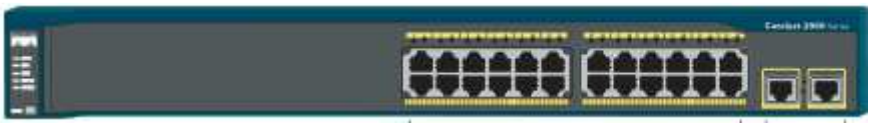

Figura 3.2: Cisco Catalyst 2960
Fuente: Obtenida de sitio web de proveedor Cisco

Serie Cisco Catalyst 3750

Entre las características más importantes de la serie 3750 están la facilidad para el despliegue de aplicaciones convergentes, proporcionan flexibilidad de configuración adaptándose al cambiante entorno tecnológico mediante el software de imagen que permite un enrutamiento IP unicast y multicast, configuraciones avanzadas para datos y video y principalmente soporte de IPv6. Para la configuración utiliza Cisco Network Assitant Software, una herramienta basada en web para una configuración rápida utilizando plantillas preestablecidas. Esta serie adicionalmente incorpora la tecnología Cisco StackWise, una arquitectura de apilamiento optimizada para Gigabit Ethernet hasta de nueve conmutadores de la serie Cisco Catalyst 3750. Una pila de la serie 3750 se gestiona como un objeto

único teniendo una dirección IP única lo que permite la administración ideal en cuanto a la seguridad, creación de VLAN y control con Calidad de Servicio.

Para el control de la seguridad tanto en la conectividad como en el control de acceso incluye ACL, autenticación y seguridad a nivel de puerto lo que ayuda a prevenir de ataques externos, principal preocupación de las empresas actualmente. Esta serie permite la configuración de hasta 1005 VLAN por pila y de hasta 12000 direcciones MAC.

Otras características de importancia se mencionan a continuación:

- Tiene funcionalidades de capa 2 y capa 3.
- 128 MB de DRAM y 16 MB de memoria FLASH.
- Enrutamiento IP unicast estático RIP.
- Enrutamiento OSPF, IGRP82, BGPv4 y IS-ISv4.
- Enrutamiento IPv6 (OSPF y EIGRP).
- Soporta MPLS y Servicios Diferenciados (DiffServ).

Figura 3.3: Serie Cisco Catalyst 3750
Fuente: Obtenida de sitio web de proveedor Cisco

Ruteador Cisco 3725

La serie Cisco 3700 para servicio de aplicaciones es una familia de enrutadores modulares que incorporan funciones de conmutación, y son la opción ideal para sucursales de baja densidad que requieren altos niveles de integración de funciones y servicios. Es un ruteador de acceso multiservicio, son modulares para la flexibilidad y escalabilidad de redes. Ofrecen una solución integrada de seguridad, telefonía IP, correo de voz, video, datos y servicios inteligentes como: QoS, IP multicast, VPN, Firewall, prevención de intrusiones y control de admisión de llamadas, todas estas cualidades sin sacrificar su rendimiento.

Figura 3.4: Ruteador Cisco 3725
Fuente: Obtenida de sitio web de proveedor Cisco

Otras características adicionales del ruteador Cisco 3725 se nombran a continuación:

• Dos puertos 10/100 integrado LAN

• Dos Integrado integración avanzada (AIM) Módulos de ranuras

• Tres tarjeta de interfaz WAN integrado (WIC) plazas

• Dos Módulo de red (NM) ranuras

• Un Módulo de Servicio de Alta Densidad ranuras (HDSM) con capacidad

• 32 MB de DRAM compacto Flash/256MB defecto

• Cisco 3725 tiene dos módulos DIMM SDRAM de 128 MB y un único módulo de 32 MB Compact Flash por defecto

• Opcional en línea de alimentación para 16 puertos EtherSwitch NM, 36 puertos HDSM EtherSwitch y puntos de acceso inalámbrico

• Soporte para los principales protocolos WAN y medios de comunicación.

3.3 Aspectos a considerarse en el diseño

Para empezar el planteamiento, es indispensable considerar dos aspectos importantes como son:

- Tamaño y localización geográfica
- Definición de los servicios a prestarse

3.3.1 Tamaño y localización geográfica

El tamaño de la red va a estar definida por la Universidad de Guayaquil y la Carrera de Ingeniería en Networking de acuerdo a su actual estructura. El diseño propuesto pretende presentar una red muy escalable mediante la aplicación de VPN basadas en MPLS, el mismo que va a estar enfocado en la carrera con

respecto a la matriz, específicamente en el centro de cómputo de cada una de las entidades mencionadas.

3.3.2 Definición de los servicios a prestarse

La red a diseñarse basada en tecnología MPLS puede soportar envío de tráfico unicast y multicast a través del backbone, de tal manera que se pueden presentar servicios de voz para una conferencia telefónica multidestino, videoconferencia, así mismo el envío de datos como emails, archivos u otro servicio adicional referente a la parte educativa que la institución crea necesaria implementar.

3.4 Desarrollo del diseño técnico

Para cumplir con el objetivo establecido de la red VPN MPLS, se brindara niveles de seguridad entre los enlaces; el diseño técnico se basará en los siguientes puntos específicos:

- Ubicación geográfica
- Estudio y análisis de tráfico
- Dimensionamiento del backbone
- Definición y elección del sistema autónomo (SA)
- Definición y elección del protocolo de enrutamiento del backbone
- Definición y elección del protocolo de enrutamiento entre CE y PE
- Designación de los equipos
- Costos referenciales del diseño

3.4.1 Ubicación geográfica

El backbone está definido para ser diseñado en la Universidad de Guayaquil la misma que se encuentra ubicada en la ciudad de Guayaquil, provincia del Guayas también conocida como la Universidad Estatal y domiciliada en la Av. Kennedy y Av. Delta. En la actualidad la universidad abarca un gran número de estudiantes cada año por tener varias extensiones en distintas parte del país y por ser una de las importantes y prestigiosas en educación superior.

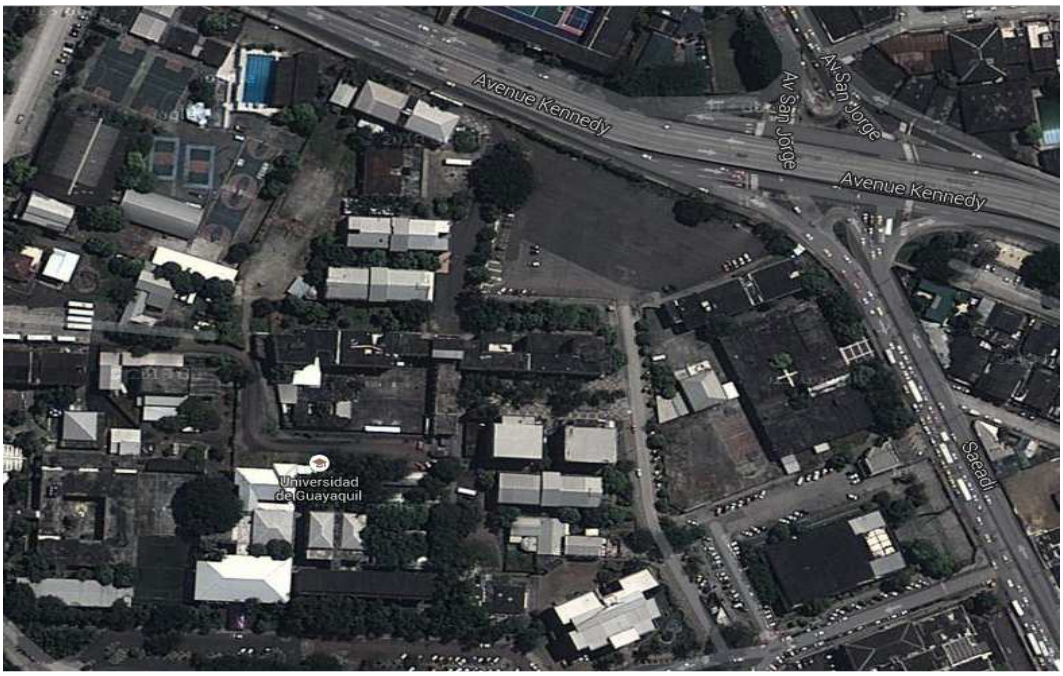

Figura 3.5: Universidad de Guayaquil
Fuente: Obtenida de google maps

Debido a que MPLS presenta muy buenas características referentes a la escalabilidad, es una arquitectura que no tendrá mayores problemas al momento de afrontar el crecimiento de una demanda futura. La VPN estará asociada a la carrera de ingeniería en Networking y Sistemas las mismas que se encuentra ubicada en Baquerizo Moreno y Víctor Manuel Rendón, edificio donde se preparan estudiantes de toda la ciudad de Guayaquil y otros cantones aledaños.

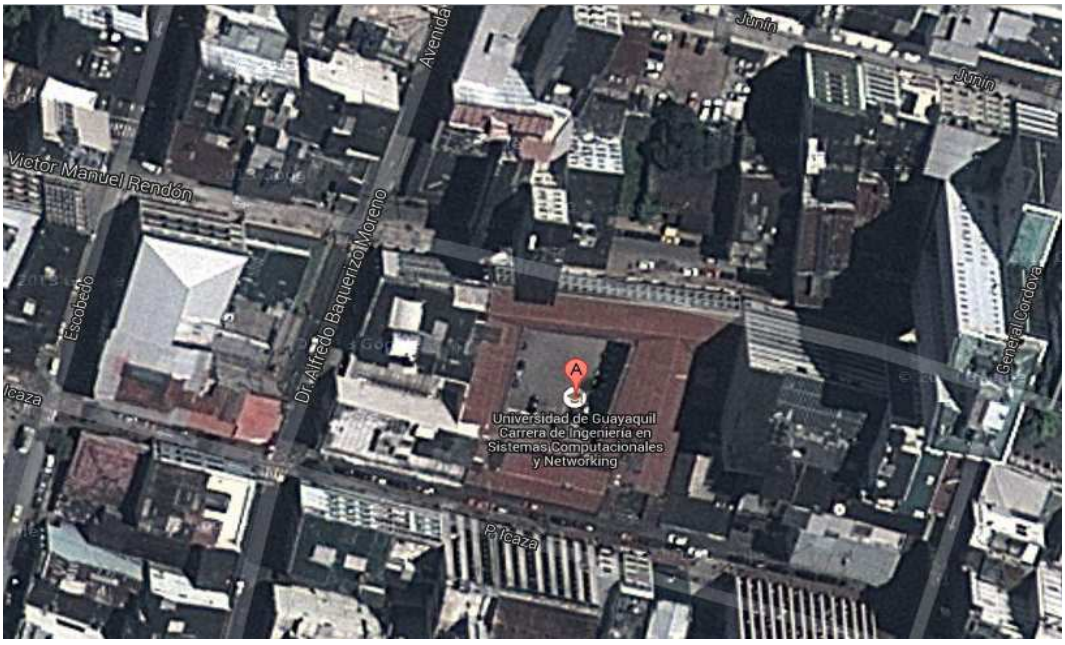

Figura 3.6: Carrera de Ingeniería en Networking
Fuente: Obtenida de google maps

3.4.2 Estudio y análisis de tráfico

En referencia al modelo jerárquico de un backbone, los enrutadores LER van a estar ubicados en las partes de concentración de tráfico hacia los usuarios, es decir, los encargados de concentrar el tráfico para su distribución a través del núcleo de la red. Así mismo, los enrutadores LSR van a ser los encargados de la conmutación del tráfico en el núcleo de la red, y serán equipos de alto rendimiento para soportar el tráfico proveniente de los LER.

Tabla 3.2: Algoritmos para codificación de voz

Codificación Estándar	Algoritmo	Velocidad de Datos
G.711	PCM	64 Kbps
G.726	ADPCM	16, 24, 32, 40 Kbps
G.728	LD-CELP	16 Kbps
G.729	CS-ACELP	8 Kbps
G.723.1	MP-MLQ ACELP	6.3 Kbps -5.3 Kbps 6.3 Kbps -5.3 Kbps

Fuente: Obtenida de sitio web de la Unión internacional de Telecomunicaciones

Los codificadores se los puede clasificar en la banda angosta y banda ancha entiendose que cuando se habla de banda ancha se hace referencia a un sistema de conexión a Internet y de transmisión de datos. Actualmente, la banda ancha es uno de las mejores opciones ya que permite disfrutar una velocidad de datos mucho más superior que lo que sucede con el acceso vía conexión por linea conmutada.

Tabla 3.3: Códec de banda ancha

Codec	Nombre	Bit rate (kb/s)	Retardo (ms)	Comentarios
G.722	Sub-band ADPCM	48,56,64	3	Inicialmente diseñado para audio y videoconferencias, actualmente utilizado para servicios de telefonía de banda ancha en VoIP [9]
G.722.1	Transform Coder	24,32	40	Usado en audio y videoconferencias
G.722.2	AMR-WB	6.6, 8.85, 12.65, 14.25, 15.85, 18.25, 19.85, 23.05, 23.85	25.9375	Estandar en común con 3GPP (3GPP TS 26.171). Los bit rates más altos tienen gran inmunidad a los ruidos de fondo en ambientes adversos (por ejemplo celulares)
G.711.1	Wideband G.711	64, 80, 96	11.875	Amplía el ancho de banda del codec G.711, optimizando su uso para VoIP
G.729.1	Wideband G.729	8 a 32 kb/s	<49 ms	Amplía el ancho de banda del codec G.729, y es "compatible hacia atrás" con este codec. Optimizado su uso para VoIP con audio de alta calidad
RtAudio	Real Time Audio	8.8, 18	40	Codec propietario de Microsoft, utilizado en aplicaciones de comunicaciones unificadas (OCS)

Fuente: Obtenida de sitio web del Grupo de trabajo de ingeniería de Internet

Las conexiones de banda estrecha hacen referencia a un tipo de conexión que utiliza un ancho de banda muy reducido. La conexión más típica de banda estrecha que existe es la conexión por módem telefónico.

Tabla 3.4: Códec de Banda estrecha

Codec	Nombre	Bit rate (kb/s)	Retardo (ms)	Comentarios
G.711	PCM: Pulse Code Modulation	64, 56	0.125	Codec "base", utiliza dos posibles leyes de compresión: µ-law y A-law
G.723.1	Hybrid MPC-MLQ and ACELP	6.3, 5.3	37.5	Desarrollado originalmente para video conferencias en la PSTN, es actualmente utilizado en sistemas de VoIP
G.728	LD-CELP: Low-Delay code excited linear prediction	40, 16, 12.8, 9.6	1.25	Creado para aplicaciones DCME (Digital Circuit Multiplex Encoding)
G.729	CS-ACELP: Conjugate Structure Algebraic Codebook Excited Linear Prediction	11.8, 8, 6.4	15	Ampliamente utilizado en aplicaciones de VoIP, a 8 kb/s
AMR	Adaptive Multi Rate	12..2 a 4.75	20	Utilizado en redes celulares GSM

Fuente: Obtenida de sitio web del Grupo de trabajo de ingeniería de Internet

El tráfico más grande en una empresa correspondiente a los datos son los de correo electrónico, acceso a servidores e Internet. Cuando el servicio de correo es corporativo y el usuario tiene que validarse en un servidor que no está dentro de su LAN, el tráfico hacia fuera tiene que ser soportado por el proveedor del servicio; no siendo así cuando el servidor de correo está presente dentro de su misma red local. Para la transmisión y recepción de video existen varios estándares los mismos que se menciona a continuación:

Tabla 3.5: Normativa ITU para multimedia sobre LAN y WAN

Estándar	Descripción
G.710-G.729	Codificación de señales de voz y audio
G.730-G.739	Características principales de los equiposmúltiplex primarios
G.740-G.749	Características principales de los equiposmúltiplex secundarios
G.750-G.759	Características principales de los equipos múltiplexde orden superior
G.760-G.769	Características principales de lostranscodificadores y delos equipos de multiplicacióndigitales
G.770-G.779	Operaciones, administración y mantenimientodeequipos de transmisión
G.780-G.789	Características principales de losequipos múltiplex de lajerarquía digitalsíncrona
G.790-G.799	Otros equipos terminales
H.200-H.499	Infraestructura de los servicios audiovisuales
H.200-H.219	General

H.220-H.229	Transmisiónde multiplexacióny sincronización
H.240-H.259	Procedimientos de Comunicación
H.260-H.279	Codificación devídeo en movimiento
H.280-H.299	Aspectos de los sistemasrelacionados
H.300-H.349	Sistemas y equipos terminalespara los servicios audiovisuales
H.350-H.359	Arquitectura de serviciosde directorio para serviciosaudiovisuales y multimedia
H.360-H.369	Calidad de laarquitectura de serviciospara los servicios audiovisualesy multimedia
T.100-T.109	Videotexto
T.120-T.149	Protocolos de datos paraconferencias multimedia
T.150-T.159	Telescritura
T.170-T.189	Multimedia e hipermedia

Fuente: Obtenida de sitio web de la Unión internacional de Telecomunicaciones

3.4.3 Dimensionamiento del backbone

La meta de diseñar una red de MPLS antes de su instalación es producir una red que operará de manera confiable y óptima. De ahí, que los principales pasos a considerarse para cumplir con ese objetivo son los siguientes:

- Diseño de los puntos de presencia
- Dimensionamiento de los enlaces en el backbone
- Diseño de enrutamiento IP
- Dimensionamiento de etiquetas MPLS

3.4.3.1 Diseño de los puntos de presencia

El diseño de los puntos de presencia para una red MPLS VPN se basa en la elección del tipo de línea de acceso y el equipamiento para la red en conjunto con la localización de los puntos de presencia determinados por la ubicación de los usuarios, por lo cual podría presentarse los siguientes casos:

3.4.3.1.1 Sólo un LER (Single Edge LSR)

Cuando solo un LER es suficiente para soportar el número y el tipo de líneas de acceso en un punto de presencia, la estructura que se muestra en la figura 3.7 es un ejemplo. Numerosas líneas de acceso se reúnen en un simple LER, el cual está conectado al resto de la red MPLS VPN.

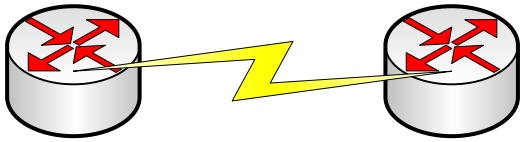

Figura 3.7: Single Edge LSR
Elaborado por: Fausto Orozco Lara

3.4.3.1.2 Múltiples LER y LSR

Un punto de presencia puede requerir más de un LER debido al gran número de líneas de acceso que tiene que soportar en determinada localización, así mismo, diferentes tipos de LER pueden ser requeridos debido a los diferentes tipos de líneas de acceso que tiene que soportar. Cuando existen varios LER en un punto de presencia tiene sentido el incluir también un LSR, el cual presenta las siguientes características:

- Conmutadores locales de tráfico que van entre diferentes LER en los puntos de presencia.
- Concentradores de tráfico que van desde un punto de presencia hacia un juego de enlaces MPLS VPN, o un conjunto separado de enlaces hacia todos los LER.
- Mejora la escalabilidad de ruteo. Solo un conjunto de protocolos de enrutamiento IP, por ejemplo OSPF los mismos que son requeridos desde un LSR a otros puntos en la red MPLS. Sin el LSR, varios protocolos de enrutamiento serían requeridos para los otros LER.

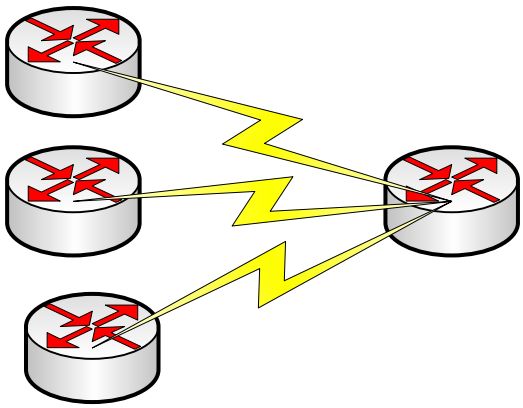

Figura 3.8: Enlaces MPLS VPN hacia LSR u otros LER
Elaborado por: Fausto Orozco Lara

Las capacidades de los enlaces se definieron partiendo de la consideración de brindar un buen servicio, en el que se toma en cuenta aplicaciones como Internet, voz, correo electrónico y videoconferencia; de donde más de 2000 usuarios aproximadamente son en la Carrera de Networking y Sistemas, es por ello necesario un enlace mínimo de 1.55 Mbps (T1) que se usa para brindar servicios unificados de voz, datos y video entre la sede central ubicada en la Universidad de Guayaquil.Tomando en cuenta estas consideraciones, a continuación se definen los puntos de presencia propuesto en este diseño y sus respectivas capacidades estimadas.

Tabla 3.6: Tráfico estimado para los puntos de presencia

Tipo	Ubicación Nodo	Tráfico (Mbps)
Local	Universidad de Guayaquil	8192
Local	Carrera de Ingeniería en Networking	4096

Elaborado por: Fausto Orozco Lara

3.4.3.2 Dimensionamiento de los enlaces en el backbone

Una vez definido el tráfico cursante por cada punto de presencia se procede a realizar el tráfico estimado de la matriz a través de la sumatoria de la capacidad de los enlaces definidos para cada LER. Además, en este cálculo está incluido el tráfico proveniente de cada concentrador ubicado junto a los LSR

Tabla 3.7: Tráfico estimado de la matriz

LSR	Trafico Estimado (Mbps)
Carrera de Ingeniería en Networking	4096
Universidad de Guayaquil	8192

Elaborado por: Fausto Orozco Lara

También se detalla los nodos y las estimaciones de requerimientos para el backbone, se ha tomado en consideración los enlaces entre LSRs y los enlaces con los concentradores LERs

Tabla 3.8: Requerimientos de nodos LSR

Nodos LSR	Requerimientos
Universidad	1 puerto STM-1 fibra monomodo para conexión al LSR con la

de Guayaquil	Universidad de Guayaquil
Carrera de Networking	2 puertos STM-1 fibra monomodo para conexión al LSR para la carrera de networking

Elaborado por: Fausto Orozco Lara

3.4.3.3 Diseño de enrutamiento IP

Para la selección de la dirección IP que un enrutador debe publicar mediante los protocolos de enrutamiento hacia sus vecinos, se lo puede hacer a través de cualquiera de las interfaces como Ethernet, Token Ring o serial. Un factor importante es la estabilidad, pues ésta depende de la dirección IP que se elija, es decir si la dirección IP elegida es de un puerto que presenta problemas de hardware que se cae a los pocos minutos, la conexión vecina y la estabilidad del sistema se verán afectadas. MPLS utiliza protocolos ordinarios de enrutamiento como OSPF o IS-IS y otros para determinar las rutas para el tráfico IP dentro de la red. Los enrutadores Cisco proporcionan particularmente la capacidad de configurar una interfaz visual denominada interfaz de bucle de prueba que está activa todo el tiempo, y en el presente diseño es posible asignar direcciones a este tipo de interfaces virtuales para asegurar que la información de enrutamiento no sufra complicaciones. De ahí que, para identificar a los LSR se podría hacer a través de una dirección de bucle de prueba por cada LSR presente en la red. Esta interfaz de loopback se debe configurar con una dirección que use una máscara de subred de 32 bits de 255.255.255.255. Se puede escoger cualquier rango de direcciones dentro de las direcciones privadas posibles, la solución se presenta con direcciones privadas tipo C y B. Se presenta la distribución de direcciones IP del backbone propuesto, en base a los puntos de presencia

Tabla 3.9: Asignación de rango de direcciones

Nodos	Hosts	Mascara	Red
Carrera de Ingeniería de Networking	300	255.255.255.0	192.168.1.0/24
Universidad de Guayaquil	2000	255.255.255.0	172.16.0.0/16

Elaborado por: Fausto Orozco Lara

El número de hosts corresponde a los usuarios potenciales que podrían estar presentes en los sectores donde están ubicados los puntos de presencia, están basados en los lugares de mayor importancia alrededor de los LERs.

3.4.3.4 Dimensionamiento de etiquetas MPLS

Siguiendo con los requerimientos para el diseño de la red VPN MPLS, un número suficiente de VC (Canales virtuales) deben reservarse para uso como LVC sobre cada enlace para completar el diseño de la red MPLS VPN. Es decir, se considera a cada LVC como un tramo del túnel LSP formado entre los enrutadores PE y está directamente relacionado con el número de etiquetas que cada LSR debe asignar para comunicarse con sus vecinos.

3.4.4 Definición y elección del sistema autónomo

Un sistema autónomo es un conjunto de redes de IP con sus propias políticas independientes de enrutamiento que realiza su propia gestión de tráfico con otros sistemas autónomos, la unión de muchos sistemas autónomos es lo que conforma el internet (Sánchez, 2012), por tanto un sistema autónomo es un componente de Internet en el máximo nivel jerárquico. Técnicamente un sistema autónomo (AS) se define como “un grupo de redes IP que poseen una política de rutas propia e independiente”.

3.4.4.1 Definición de las VRF

Para proporcionar el servicio de VPN basado en la arquitectura MPLS se deben definir las tablas VRF (VPN Routing and Forwarding). La relación entre las VPN, los sitios y las VRF se puede resumir de la siguiente manera: “Todos los sitios que comparten la misma información de enrutamiento, lo que significa que pertenecen al mismo conjunto de VPN, que tienen permiso de comunicarse entre sí y que están conectados al mismo ruteador PE pueden ser colocados en una VRF común”. En la arquitectura MPLS VPN una VPN puede ser vista como una comunidad de intereses, en la que los miembros de una VPN comparten la misma información de enrutamiento que se coloca en la VRF específica.

3.4.5 Definición y elección del protocolo de enrutamiento del backbone

La función del enrutamiento es una función de la Capa tres del modelo OSI, es unesquema de organización jerárquico que permite que se agrupen direcciones individuales que son tratadas como unidades únicas hasta que se necesita la dirección destino para la entrega final de los datos. El enrutamiento es el proceso de hallar la ruta más eficiente desde un dispositivo a otro. Dentro de las opciones que se manejan como protocolo de enrutamiento en el backbone de la red está OSPF, otra opción puede ser EIGRP pero esto limitaría a la red de funcionar con Ingeniería de Tráfico, ésta aplicación requiere de un protocolo basado en el algoritmo de estado de enlace tal como OSPF que tiene la capacidad de funcionar con extensiones que son utilizadas por MPLS-TE (MPLS-Traffic Engineering). OSPF permite manejar hasta 500 rutas dentro de un mismo sistema autónomo y dado que el backbone que se propone tiene apenas 8 puntos de presencia, no se supera el valor máximo de restricción para utilizar el protocolo OSPF, por estas razones OSPF será el protocolo a usarse para el enrutamiento en el backbone además de la aplicación de MPLS-TE.

3.4.6 Definición y elección del protocolo de enrutamiento entre CE y PE

El enlace entre PE y CE corresponde a la última milla, los protocolos de enrutamiento de este enlace pueden ser mediante RIP, EBGP o enrutamiento estático. Debido a que la red se considera un solo sistema autónomo, los enlaces a partir de los equipos LER se consideran sistemas autónomos diferentes y se toman en cuenta al momento del establecimiento y configuración de las VRF en los equipos de frontera. Cualquiera de las opciones mencionadas puede ser válida para el enrutamiento de última milla y satisfacer las necesidades de interconexión entre PE y CE. Para redes de datos de pequeño tamaño y con una estructura topológica en estrella, la configuración mediante enrutamiento estático puede ser suficiente, sin descartar el enrutamiento dinámico como EBGP u OSPF, que se pueden usar en sectores donde las redes de los usuarios sean más grandes y así publicar las rutas hacia la red MPLS VPN.

3.4.6.1 Protocolo de información de enrutamiento RIP

RIP (Protocolo de enrutamiento de la Información) es un protocolo de enrutamiento que usa la métrica de saltos para indicar la distancia hacia un

destino, teniendo la posibilidad de un conteo de saltos infinito si se llega a presentar un bucle, de ahí que se ha limitado el número de saltos a 16, cuando una entrada llega a esta distancia se considera no accesible. Entre las características se puede mencionar que si no se reciben actualizaciones de una determinada ruta por un tiempo se da de baja la ruta, mantienen solamente la mejor ruta para un determinado destino, no soporta máscaras variables y realiza actualizaciones cada 30 segundos.

3.4.6.2 Protocolo de frontera de borde externo EBGP

Es un protocolo extremadamente complejo utilizado a través de internet y dentro de empresas multinacionales. La función de un protocolo de routing de pasarela externa (eBGP) no es encontrar una red específica sino proporcionar información que permita encontrar el sistema autónomo en cual se encuentra dicha red. Entre sus características principales podemos mencionar que soporta VLSM, CIDR, sumarización, mantiene keepalives periódicos, tiene su propia tabla de enrutamiento, asegura la fiabilidad del transporte llevando sus actualizaciones de enrutamiento y sincronizando las actualizaciones de enrutamiento, entre otras. (Cabeza, 2009)

3.4.6.3 Enrutamiento estático

El conocimiento de las rutas estáticas se gestiona manualmente por el administrador de red, que lo introduce en la configuración de un ruteador. El administrador debe actualizar manualmente cada entrada de ruta estática siempre que un cambio en la estructura de la red requiera una actualización. Los enrutadores no tienen que descubrir ni propagar nuevas rutas a través de la red. Existe una relación entre la dirección destino de un paquete y el interfaz por el cual debe ser enviado dicho paquete. Esta relación es la que se programa de forma estática en los enrutadores, y no variará con el paso del tiempo. Un paquete dirigido a una dirección determinada se enviará siempre por la misma interfaz.

Entre sus principales ventajas se puede mencionar que es el de menor consumo de recursos de la red y el ruteador ahorra ancho de banda en cada uno de sus enlaces al no necesitar información proveniente de la red para construirse las tablas de enrutamiento, ayuda a crear redes más seguras puesto que solo existe un camino

para entrar o salir de este tipo de redes haciendo más fácil la monitorización. En base a estas definiciones, se puede brindar los tres tipos de enrutamiento dependiendo de las aplicaciones y requerimientos del usuario, para ejemplo en el proyecto planteado será usado el protocolo BGP.

3.5 Designación de los equipos

Para la selección de los equipos, hay que tomar en cuenta algunos factores como la oferta en el mercado y la disposición de actualización de software y hardware que puedan tener, es importante considerar que MPLS proviene de una iniciativa derivada de la conmutación de etiquetas propuesta en marzo de 1998 por Cisco a la IETF, siendo partícipe activo en la actualización del estándar, la tecnología MPLS Cisco se ve como una plataforma de lanzamiento para ofrecer servicios como VPN. Deben ser equipos que estén liderando la entrega de soluciones MPLS que se han adoptado por proveedores de servicio globales debido a la escalabilidad que esta tecnología presenta,por ello se debe tomar en cuenta el precio, disponibilidad y soporte en el momento de seleccionar los equipos.

3.5.1 Selección del equipo de frontera Edge LSR

Hay que tomar en cuenta cuatro consideraciones para la selección del equipo de frontera:

- El tipo de servicios que se ofrece
- El tipo de líneas de acceso como G.SHDSL y Frame Relay
- El número de líneas de acceso.
- Requisitos para la redundancia y la confiabilidad, las cuestiones clave son: si el equipo puede reducir al mínimo o prevenir completamente la interrupción en el caso de fallas de hardware o software; o si los componentes individuales, tales como las tarjetas de los puertos pueden ser cambiadas en caliente, es decir, sin necesidad de apagar el equipo.

Tabla 3.10: Características LER para nodos de menor y mayor congestión

Nodo	Descripción de equipo
Carrera de Ingeniería en Networking	Concentrador de acceso universal, servicio ip+atm con líneas de acceso e3t3, puede soportar enlaces full dúplex de 150 mbps, puertos para tarjetas Ethernet.

	Soporte de puertos Ethernet (8 por slot), soporte de NAT, VPN, soporte de MPLS, enlaces E1/T1, Ethernet y Fast Ethernet a 10 Mbps, ISDN BRI, E3, T3 o OC-3/STM-1 ATM.

Elaborado por: Fausto Orozco Lara

3.5.2 Selección del equipo del núcleo LSR

Se pueden considerar los siguientes aspectos importantes para la selección del equipo LSR:

- Tipo de enlaces: en el núcleo de la red la mayoría de los enlaces serán a través de interfaces seriales, con enlaces basados en fibra monomodo con un alcance de 4 a 8 Km.
- Numero de enlaces
- Número de conexiones soportadas

En base a estas consideraciones se puede considerar idóneo al equipo que se presente las siguientes características, cabe recalcar que los nodos LSR deben ser equipos muy confiables debido a que por éstos circula todo el tráfico generado por los puntos de presencia, y además, son los responsables de la conmutación de las etiquetas en el núcleo de la red.

Tabla 3.11: Características LSR presentes en el backbone

Nodo	Descripción de equipo
Universidad de Guayaquil	Puertos de conmutación que soportan 800/1600 Mbps, 200 Mhz de procesador, 16 MB de Flash, puerto Fast Ethernet, slots PCMCIA, puerto de consola y puerto auxiliar, soporte fibra multimodo con distancias superiores a los 2 Km y fibra monomodo con distancias superiores a los 20 Km, puertos T3/E3 ATM, soporta VC Merge, alimentación 48 VDC

Elaborado por: Fausto Orozco Lara

3.5.3 Esquema de configuración de los equipos

Los esquemas de configuración están basados en la función que van a desempeñar los equipos dentro de la red, debido a que existen los equipos de frontera o LER y los equipos de conmutación del núcleo o LSR, dando importancia a la descripción general de la forma de configurar la red para desempeñar MPLS. Una de las

principales aplicaciones de la arquitectura MPLS son las VPN, cuya configuración posible se verá más adelante. Por motivos de seguir un orden en los pasos de configuración, se propone continuar de la siguiente manera:

3.5.3.1 Configuración de niveles de control MPLS y definición del VRF

Se pueden presentar tres casos posibles, el primero que presenta los pasos necesarios para incrementar y desplegar MPLS a través de la red asumiendo que los paquetes hacia todos los destinos deben ser conmutados por etiquetas, el segundo que propone que los paquetes sean conmutados hacia un conjunto específico de destinos, y el tercer método por el cual se puede controlar de mejor manera la distribución de etiquetas dentro de la red. En la siguiente tabla se muestran los comandos de la posible configuración de los equipos LER, siguiendo el orden determinado, tomando en cuenta la asociación de una VRF a una FEC.

Tabla 3.12: Configuración de niveles de control MPLS y definición de VRF

COMANDO	PROPÓSITO
Router# ***configuration terminal***	Ingreso al modo de configuración global
Router (config)# ***ip cef distributed***	
Router (config)# ***ip vrf <vrf-name>***	Ingresa al modo de configuración VRF y especifica una VRF
Router (config-vrf)# ***rd <route-distinguisher>***	Configura el distinguidor de ruta y a continuación se configura las route targets para la VRF
Router (config-vrf)# ***route target {import |export | both} route-target-ext-community***	Crea una lista de las comunidades route target de importación y/o exportación para una VRF específica
Router (config-if)# ***ip vrf <forwarding vrfname>***	Asocia una VRF con una interfaz
Router (config-router)# ***address-family ipv4 vrf <vrf-name>***	Crea la familia de direcciones para la VRF determinada.
Router (config-router)# ***address-family ipv4 vrf<vrf-name>***	Configura los parámetros RIP para ser usados entre PE y VRF Ces
Router (config-router-af)# ***exit-address-family***	Sale del modo de configuración address-family

Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

3.5.3.2 Configurando sesiones de enrutamiento BGP

Para la configuración general de sesiones BGP en los enrutadores LER, se pueden aplicar las siguientes configuraciones en el modo de configuración.

Tabla 3.13: Configuración de sesiones de enrutamiento BGP en ruteador PE

COMANDO	PROPÓSITO
Router (config-router)# ***address-family {ipv4 | vpnv4} [unicast | multicast]***	Configura la familia de direcciones BGP
Router (config-router-af)# ***neighbor {address|peer-group}remote-asas-num***	Define una sesión iBGP con otro ruteador PE
Router (config-router)# ***no bgp default ipv4- activate***	Activa una sesión BGP, previene los anuncios de las familias de direcciones IPv4 a todos los vecinos
Router (config-router)# ***neighbor address remote-as as-number***	Configura iBGP para intercambiar VPNv4
Router (config-router)# ***neighbor address update-source interface***	Define una sesión iBGP
Router (config-router-af***)# neighbor address activate***	Activa los anuncios de VPNv4

Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

Para la configuración de la información de las rutas de importación y exportación, y definir una VPN MPLS, los pasos a seguir en el ruteador PE son.

Tabla 3.14: Configuración rutas de importación y exportación

COMANDO	PROPÓSITO
Router (config)# ***ip vrf vrf_name***	Definir un nombre para VRF
Router (config-vrf)# ***route-target import community-distinguisher***	Importa información de enrutamiento para una comunidad extendida
Router (config-vrf)# ***route-target export community-distinguisher***	Exporta información de enrutamiento para una comunidad extendida.
Router (config-vrf)# ***import map route-map***	Asocia el mapa de ruta específica con una VRF

Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

3.5.3.3 Configurando las sesiones de enrutamiento entre PE y CE

Para realizar la configuración de las sesiones de enrutamiento entre los equipos de frontera de la red PE y los equipos del lado del usuario, se lo puede hacer mediante enrutamiento EBGP, RIP o enrutamiento estático. A continuación la configuración en caso que el protocolo escogido sea RIP

Tabla 3.15: Configuración de sesiones de enrutamiento RIP

COMANDO	PROPÓSITO
Router # ***configure terminal***	Ingresar a modo de configuración global
Router (config)# ***router rip***	Habilita RIP
Router (config-router-af)# ***address-family ipv4 [unicast] vrf vrf_name***	Define parámetros RIP para sesiones de enrutamiento entre PE y CE
Router(config-router-af)#***network prefix***	Habilita RIP en el enlace PE – CE

Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

Si el protocolo BGP fuese usado, se definen comandos que ejecutan la activación y sesión entre los enrutadores, los mismos que pueden ser los siguientes:

Tabla 3.16: Configuración de sesiones de enrutamiento EBGP

COMANDO	PROPÓSITO
Router(config-router)# ***address family ipv4 [unicast] vrf vrf_name***	Define parámetros EBGP para sesiones de enrutamiento entre PE y CE
Router (config-router-af)# ***neighbor address remote-as as number***	Define una sesión EBGP entre los enrutadores PE y CE
Router (config-router-af)# ***neighbor address activate***	Activa los anuncios de la familia de direcciones IPv4

Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

Y en caso de no configurar enrutamiento dinámico se puede usar enrutamiento estático con los comandos que se detalla en la tabla 3.17

Tabla 3.17: Configuración de sesiones de enrutamiento estático

COMANDO	PROPÓSITO
Router (config)# ***ip route vrf*** *vrf_name*	Define los parámetros de una ruta estática para cada sesión PE-CE
Router (config-router)# ***address-family ipv4 [unicast] vrf*** *vrf_name*	Define los parámetros de una ruta estática para cada sesión de enrutamiento BGP entre PE y CE
Router (config-router-af)# ***redistribute estatic***	Redistribuye las rutas estáticas VRF dentro de una tabla VRF BGP
Router (config-router-af)# ***redistribute estatic connected***	Redistribuye directamente las redes conectadas dentro de la tabla CRF BGP

Fuente: Configuración MPLS de Cisco IOS Software por Lancy Lobo

3.6 Equipos referenciales del diseño

Se presenta un marco referencial de los equipos que podrían utilizarse como LER y LSR teniendo en cuenta las tarjetas que se pueden usar para la interconexión entre LSR y las tarjetas con las interfaces físicas de conexión de última milla. Se realiza una comparación entre las marcas Cisco, 3COM y Alcatel, con la finalidad de justificar la elección de los equipos que satisfagan los requerimientos mencionados.

Solución mediante equipos de marca Cisco

La serie se equipos Cisco 6400, son enrutadores IP+ATM que provee servicios de banda ancha en ATM y QoS en ATM, el IOS (Sistema Operativo Internetwork) permite proveer servicios de MPLS como Ingeniería de tráfico, QoS y MPLS VPN. La cantidad de tarjetas estimadas en los equipos LER se basan en el número de puertos que tiene cada tarjeta, el tipo de enlace con el usuario y la tecnología de transporte. Se estima que el mayor número de enlaces serán E1 o T1 Se presenta también 30 tarjetas con 4 puertos cada una, con interfaces físicas como Frame Relay, X.21 y enlaces seriales. Estas características se pueden manifestar en los enlaces de última milla, no es propósito del presente diseño profundizar en tecnologías de enlace con el usuario, pero se presentan debido al dimensionamiento de los equipos LER que se exponen.

Los equipos que se presentan son de marca CISCO

Tabla 3.18: Resumen de equipos CISCO

Número Parte	Descripción
BPX8650	BPX IP+ATM switch: BPX w/BCC-4, ASM, backcards, Cisco7204TSC
C7206VXR4002FE	Cisco 7206VXR with NPE-400 and I/O Controller with 2 Fe/E PORT
C6400-CHAS-AC/RRF	Cisco Universal Access Concentrator 6400
MGXMMF4155BRF	Cisco Expansión Module ATM Sonet OC-3/STM-1 155Mbps 4-Ports
NM1E2W	Cisco Interface Module 3600 EN ISDN 10Mbps 1-Port
NM4BU	Cisco ISDN Terminal Adapter WAN 128Kbps 4-Ports
701000468-00	Cisco WAN Adapter 3600 8Mbps 4-Ports NM4T
S4KL3EK9112218EW	Cisco IOS Enhanced Layer 3 and Voice Software
AXAUSM4T1	Cisco ATM Uni Service Module T1 4-Ports

Elaborado por: Fausto Orozco Lara

Solución mediante equipos de marca 3COM (HP)

3COM también se ha destacado en desarrollar equipos de conectividad, si bien es cierto la mayoría de ellos no son compatibles con la tecnología MPLS, se tiene como referencia los equipos de la serie 3000, 5000 y 6000. A continuación se enlista equipos de marca 3Com como segunda alternativa.

Tabla 3.19: Resumen de equipos 3COM

Número Parte	Descripción
3C13804	3Com Ruteador 6000 Processing Unit Ethernet
3C13840US	3Com Ruteador 6040 Modular Expansión Base 3 U
3C200700	3Com Module ATM 155Mbps 1-Port
w/SW 3C12067	3Com Expansión Module Ethernet 10Mbps FO 1-Port
3C13769	3Com Module T1 1.544Mbps 2-Ports
3C13775	3Com Multi-Function Interface Module Serial T3 1-Port
3C421800	3Com SuperStack II RAS 1500 2PT ISDN BRI I/O 128 Kbps
3C35410	3Com Expansión Module 100Mbps 6-Ports 100 Mbps
3C13764	3Com Expansión Module Serial 2Mbps 4-Ports

Elaborado por: Fausto Orozco Lara

De las familias de equipos mencionados, solamente la correspondiente a la serie 6000 cumple con los requerimientos del diseño, que son soporte de ATM, VPNs, MPLS, entre otras; además, la diferencia en precios es muy notoria respecto del planteado con equipos Cisco. Otro aspecto importante es que no han desarrollado tarjetas de expansión con la misma escalabilidad que Cisco, de ahí que no se encuentren disponibles tarjetas con tecnologías como Frame Relay o con conectores BNC para permitir conexión mediante cable coaxial. Al no tener escalabilidad en la capacidad de las tarjetas se tomaron en cuenta aquellas de capacidades superiores para suplir y cubrir a las de menores capacidades.

Solución mediante equipos de marca Alcatel

Alcatel proporciona una familia completa de productos con grado operador que permiten trabajar sin problemas en las redes actuales de grandes capacidades.Mediante el uso de MPLS y las funciones permitidas por la mediación ATM/MPLS, Alcatel es capaz de proporcionar una migración sin saltos de los servicios de datos a través del núcleo de paquetes. A continuación se presenta una tabla con los precios de equipos Alcatel.

Tabla 3.20: Resumen de equipos Alcatel

Número Parte	Descripción
90818101	New Alcatel 7470/7670 1 Port Stm1-2m Adapter Card New Open Box
90718202	New Alcatel 7270 1 Port Stm1-2m Adapter Card
OS6600GNIU2	Alcatel Expansión Module E1 120PRI CFR Quad Mod. (R2.2) 2- Ports
OS7540CNIH2	Module Alcatel Multi-Function Interface Serial T3 Port
OS6820NHER9	Alcatel Expansión Module Interface T1 4-Ports
90-4463-01	3-Port DS3/E3 BNC I/O Mod.
90-4672-01	36170: IMA Module-T1/E1 ATM CR
90-7569-02	7670 8-Port OC3c/STM1 IR I/O Mod.
OS6770CNHJ1	Alcatel Expansión Module Ethernet 10Mbps Fibre Optic 2-Port

Elaborado por: Fausto Orozco Lara

El concentrador multiservicio Alcatel 7270 MSC junto a la plataforma multiservicio Alcatel 7470 RSP, son usados por operadores de todo el mundo para brindar servicios de datos rentables, incluyendo Frame Relay, líneas alquiladas y X.25. De igual forma, no posee escalabilidad en cuanto a sus módulos de expansión como tarjetas con puertos de cobre o cable coaxial. La cantidad de dispositivos está en función del número de puertos que tiene cada módulo.

Una vez presentadas tres posibles alternativas de equipos de marcas diferentes, hay que resaltar mucho el factor económico, como se puede apreciar la diferencia en los precios de equipos 3COM y Alcatel respecto de equipos Cisco es muy notoria. Desde el punto de vista técnico los equipos Alcatel y 3COM son bastante aceptados por los operadores de servicios, pero a pesar de dicha aceptación, los equipos de marca Cisco son los que actualmente dominan el mercado debido a su demanda y a su facilidad de actualización en software y hardware; además, es muy importante considerar que MPLS proviene de una iniciativa derivada de la conmutación de etiquetas propuesta en marzo de 1998 por Cisco a la IETF, siendo partícipe activo en la actualización del estándar. MPLS dentro del software Cisco IOS, hace que las VPN sean más fáciles de desplegar y actualmente están liderando la entrega de soluciones MPLS que han sido adoptadas por proveedores de servicio debido a la escalabilidad que presenta.Por estas razones, a pesar de existir una diferencia en costos, Cisco va a ser la marca de equipos a usarse tanto para los equipos de frontera como del núcleo sabiendo además que presentan una gran escalabilidad en las capacidades de los módulos de expansión.

3.7 Simulación en el software GNS3

Las simulaciones de sistemas utilizando equipos informáticos son en la actualidad de gran aplicación en las ingenierías, en ellas podemos observar la evolución de un sistema en concreto con sus características principales. El objetivo de las mismas es recrear un modelo lo más fiable posible a la realidad, para poder estudiar los resultados obtenidos mediante la simulación, es por eso para poder realizar el proyecto se ha escogido un simulador de red que ofrece características potentes como es el GNS3, con el objetivo de diseñar un modelo datos lo más fiable posible. GNS3 es un software de código abierto es decir bajo licencia GPL que simulan redes complejas siendo lo más cerca posible a la forma en redes

reales que se realizan. Todo esto sin haber dedicado hardware de red tales como enrutadores y switches., el software ofrece una interfaz gráfica de usuario intuitiva para diseñar y configurar redes virtuales, se ejecutan en hardware de PC tradicionales y se puede utilizar en múltiples sistemas operativos, incluyendo Windows, Linux y MacOS X. (GNS3, 2013)

3.7.1 Dynamips

Dynamips es un software que emula IOS Cisco en un PC tradicional, fue creado por Christop he Fillot quien comenzó su trabajo en agosto de 2005 La última versión oficial de Dynamips soporta Cisco 7200, 3600 series 3620, 3640 y 3660, serie 3700, 3725, 3745, 2600 series 2610 a 2650XM , 2691 y la serie 1700. GNS3 se basa en Dynamips y Dynagen un front-end basado en texto para Dynamips, para crear una red Cisco virtual completo, añadiendo muchas características adicionales y lo más importante por lo que es fácil de crear, cambiar y guardar sus topologías de red. (GNS3, 2013)

3.7.2 Configuración de IOS en GNS3

Una vez instalado en GNS3, se procede con la configuración IOS de los modelos de enrutadores que se va a usar, ya que en el aplicativo no viene ningún IOS por defecto. Para subir alguna IOS nos vamos al menú principal en la opción de **Edit** y seleccionamos **IOS imagen and hypervisos**.

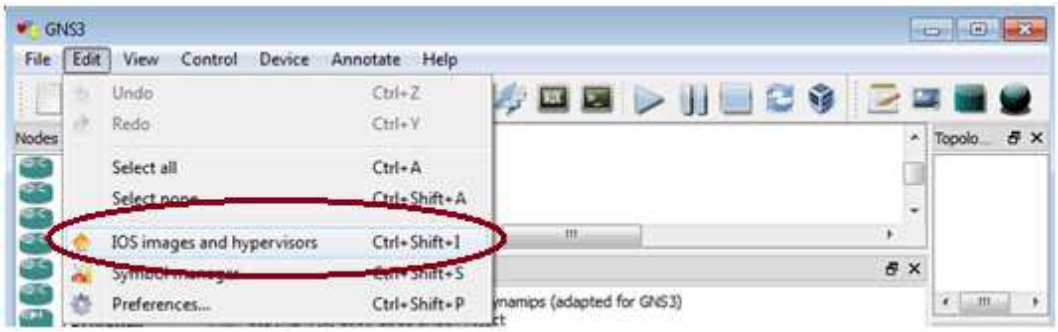

Figura 3.9: Configuración de IOS en GNS3
Fuente: Obtenida de aplicativo GNS3

Pulsada la opción anterior nos saldrá la figura 3.10 en la cual seleccionamos el archivo de imagen del IOS correspondiente al modelo de ruteador que deseamos trabajar en nuestro caso un modelo 3700.

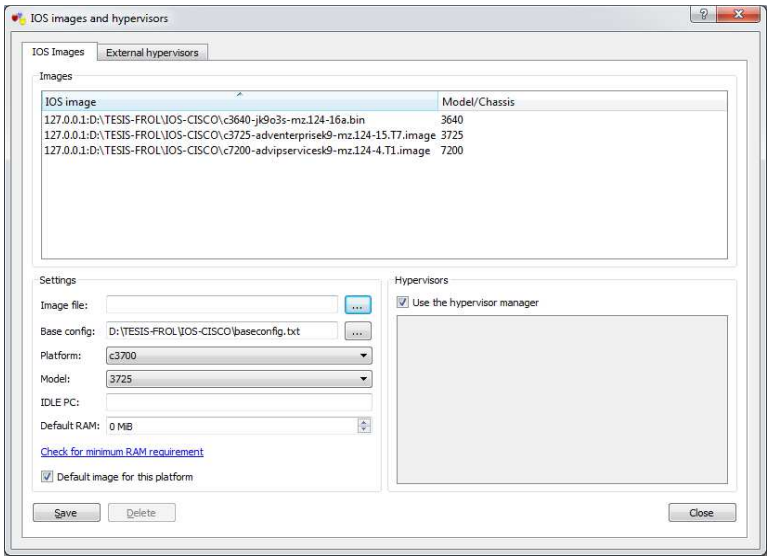

Figura 3.10: Inserción de IOS en GNS3
Fuente: Obtenida de aplicativo GNS3

Una vez configurado las imágenes del IOS de los enrutadores a trabajar podemos seleccionar los equipos que deseemos para nuestro diseño. Estos equipos lo encontramos en Node types y bastara seleccionar un elemento y llevarlo

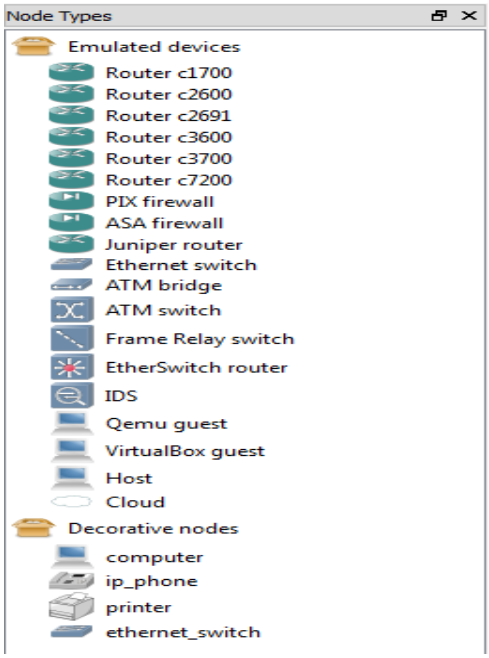

Figura 3.11: Tipos de equipos en GNS3
Fuente: Obtenida de aplicativo GNS3

3.7.3 Barras de herramientas de GNS3

Dentro del aplicativo GNS3 tenemos algunas barras de herramientas, entre las cuales podemos mencionar las siguientes:

Barra general

En esta barra de herramienta podemos tener muchas opciones de trabajo como:

- Crear nuevos diseños
- Abrir nuevos proyectos
- Guardar proyectos
- Guardar topologías
- Mostrar etiquetas a las interfaces
- Conexión a interfaces LAN/WAN

Figura 3.12: Barra de herramientas General
Fuente: Obtenida de aplicativo GNS3

Barra simulación

Esta barra nos permite ver opciones de inicio y parada de emulación así como también el acceso a consola para la administración de los equipos

Figura 3.13: Barra de herramientas de Simulación
Fuente: Obtenida de aplicativo GNS3

Barra de dibujo

Esta barra nos permite agregar notas en el diseño topológico así como también insertar imágenes prediseñadas como figuras geométricas como cuadrado y círculos para agrupar algunos equipos que identifiquen alguna área específica.

Figura 3.14: Barra de herramientas de Dibujo
Fuente: Obtenida de aplicativo GNS3

Barras de menús de GNS3

Al igual que la mayoría de aplicaciones dentro del menú principal encontramos muchas de las opciones que se realiza en las barras de herramientas, destacándose las de edición como la de control

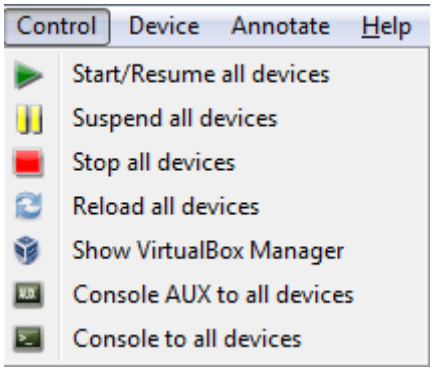

Figura 3.15: Barra de herramientas de Menús
Fuente: Obtenida de aplicativo GNS3

3.8 Diseño topológico de Universidad de Guayaquil con la Carrera de Ingeniería en Networking

La Universidad de Guayaquil como se mencionó anteriormente está constituida por varias extensiones ubicadas en distintos lugares del país, así como una diversidad de facultades y carreras, por lo cual necesita tener almacenada toda su información en un lugar específico como lo es la matriz, la misma que tiene las aplicaciones vía web para el uso de sus estudiantes de todas las facultades y otros servicios educativos que brinda. A continuación de manera macro se muestra la estructura actual.

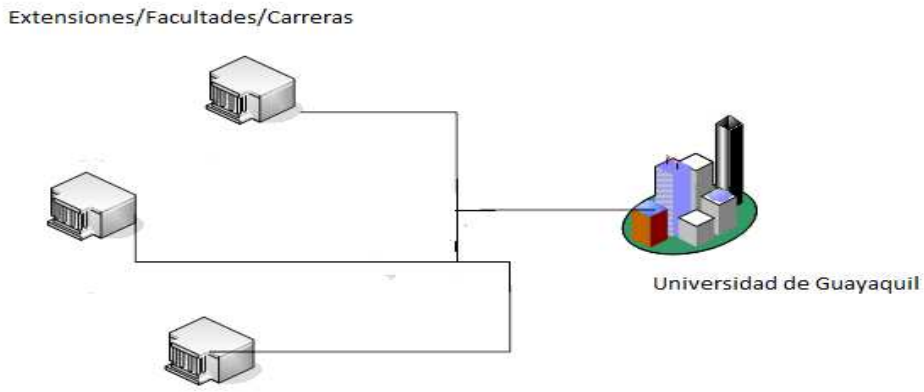

Figura 3.16: Estructura de la Universidad de Guayaquil
Elaborado por: Fausto Orozco Lara

La propuesta involucra comunicación usando tecnología MPLS VPN desde la Carrera de Ingeniería en Networking hacia la matriz, para lo cual será imperante la configuración de los equipos de comunicación tanto en la carrera como en el

centro de cómputo central, para lo cual nos vamos ayudar con la herramienta de simulación GNS3 para realizar las configuraciones básicas para cumplir con el bosquejo del diseño.

Figura 3.17: Diseño Propuesto de red MPLS VPN
Elaborado por: Fausto Orozco Lara

3.9 Desarrollo de diseño

Para el desarrollo del diseño se detallara la configuración de todos los componentes a nivel del esquema de MPLS propuestos para la Universidad como los equipos C, CE, PE y el backbone con los enrutadores principales, por ello podemos visualizar en el ***anexo 1*** la propuesta de diseño planteada para este proyecto.

3.9.1 ConfiguracióndeenrutadoresCE R1 y R8

La configuración del cambio de ruta entre PE y CE enrutadores consiste en la implementación de un protocolo de enrutamiento en los enrutadores CE, no hay ninguna configuración específica con excepción de la configuración habitual del protocolo de enrutamiento que se requiere en los enrutadores CE. En los enrutadores PE, se requiere que los contextos de enrutamiento VRF para el intercambio de rutas entre el PE y la CE. A continuación se detalla la configuración de los mismos:

Paso 1: Configuración de interfaz loopback10

```
R1# configure terminal
R1(config)# interface loopback 10
R1(config-if)# ip address 192.168.100.100 255.255.255.0
R8(config)# interface loopback 10
R8(config-if)# ip address 192.168.200.200 255.255.255.0
```

Paso 2: Configuración de interfaz fastethernet 0/0

```
R1# configure terminal
R1(config)# interface fastEthernet 0/0
R1(config-if)#  ip address 10.10.100.1 255.255.255.252

R8(config)# interface fastEthernet 0/0
R8(config-if)#  ip address 10.10.100.5 255.255.255.252
```

Paso 3: Configuración de reenvío de paquetes

```
R1# configure terminal
R1(config)#ip forward-protocol nd
R1(config)#ip route 10.10.100.4 255.255.255.252 10.10.100.2
R1(config)#ip route 192.168.200.0 255.255.255.0 10.10.100.2 name toUG

R8(config)#ip forward-protocol nd
R8(config)#ip route 10.10.100.0 255.255.255.252 10.10.100.6
R8(config)#ip route 192.168.100.0 255.255.255.0 10.10.100.6 name toCINT
```

3.9.2 Configuración de BGP PE -PE rutas en PE enrutadores

La configuración de enrutamiento BGP PE -PE entre los enrutadores PE es el siguiente paso en una implementación de MPLS VPN. El propósito de este paso es asegurar que las rutas VPNv4 pueden ser transportados a través de la columna vertebral proveedor de servicio usando MP- iBGP. La configuración la podemos detallar de la siguiente manera:

Paso 1: Configurar BGP routing en enrutadores PE

```
R2(config)#router bgp 6500
R7(config)#router bgp 6500
```

Paso 2: Configurar los vecinos MP-iBGP

```
R2(config-router)#neighbor  192.168.23.37  remote-as 65000
R2(config-router)#neighbor 192.168.23.37  update-source loopback 155

R7(config-router)#neighbor  192.168.23.32  remote-as 65000
R7(config-router)#neighbor 192.168.23.32  update-source loopback 155
```

Paso 3: Configurar dirección para VPNv4 family bajo proceso de BGP

```
R2(config-router)#address-family vpn4
R2(config-router-af)# neighbor  192.168.23.37  activate
R2(config-router-af)# neighbor  192.168.23.37  send-community extended

R7(config-router)#address-family vpn4
```

R7(config-router-af)# neighbor 192.168.23.32 activate
R7(config-router-af)# neighbor 192.168.23.32 send-community extended

Paso 4: Configurar la IPv4 address family

R2(config-router)# address-family ipv4 vrf CINT
R2(config-router-af)# redistribute connected
R2(config-router-af)# exit-address-family

R7(config-router)# address-family ipv4 vrf CINT
R7(config-router-af)# redistribute connected
R7(config-router-af)# exit-address-family

3.9.3 Implementación de BGP PE-CE para sitios VPN con único SA

Lospasos para configurarel enrutamientoBGPPE-CE en enrutadores PEson los siguientes:

Paso1. ConfigurarporcontextoenrutamientoVRFBGP enenrutadoresPE

R2(config)#router bgp 65000
R2(config-router)#address-family ipv4 vrf CINT

Paso 2. Definir y activar BGP en los vecinos CE

R2(config-router-af)#neighbor 192.168.23.37 remote-as 65000
R2(config-router-af)#neighbor 192.168.23.37 activate

3.9.4 Configuracióndeenrutadores P

En los enrutadores P no hayconfiguraciones especiales que se deben realizaren los equipos parasoporte de MPLSVPN, esto debido a que losenrutadoresPsólo participan enMPLS en el reenvío de paquetesetiquetados,los únicos requisitosson los de unLSRen una redMPLS, a saber, laIGPpara el intercambioNLRIyLDPpara la asignaciónydistribución de etiquetas. Como siempre, CEF debe estar habilitadoen todas las interfacesconfiguradaspara el reenvío deMPLS.

Paso 1: Configuración de interfaz loopaback
R3#configure terminal
R3(config)# interface Loopback 155
R3(config-if)# ip address 192.168.23.33 255.255.255.255

R4(config)# interface Loopback 155
R4(config-if)# ip address 192.168.23.34 255.255.255.255

R5(config)# interface Loopback 155
R5(config-if)# ip address 192.168.23.35 255.255.255.255

```
R6(config)# interface Loopback 155
R6(config-if)# ip address 192.168.23.36 255.255.255.255
```

Paso 2: Configuración de interfaz serial

```
R3#configure terminal
R3(config)# interface Serial 0/0
R3(config-if)# ip address 200.200.10.2 255.255.255.0
R3(config-if)# mpls label protocol ldp
R3(config-if)# ip ospf authentication-key ugcint
R3(config-if)# mpls ip

R3#configure terminal
R3(config)# interface Serial 0/1
R3(config-if)# ip address 200.200.20.1 255.255.255.0
R3(config-if)# clock rate 64000
R3(config-if)# mpls label protocol ldp
R3(config-if)# mpls ip

R3#configure terminal
R3(config)# interface Serial 0/2
R3(config-if)# ip address 200.200.30.1 255.255.255.0
R3(config-if)# clock rate 64000
R3(config-if)# mpls label protocol ldp
R3(config-if)# mpls ip

R4#configure terminal
R4(config)# interface Serial 0/0
R4(config-if)# ip address 200.200.20.2 255.255.255.0
R4(config-if)# mpls label protocol ldp
R4(config-if)# mpls ip

R4#configure terminal
R4(config)# interface Serial 0/1
R4(config-if)# ip address 200.200.40.1 255.255.255.0
R4(config-if)# clock rate 64000
R4(config-if)#mpls label protocol ldp
R4(config-if)#mpls ip

R5#configure terminal
R5(config)# interface Serial 0/0
R5(config-if)# ip address 200.200.40.2 255.255.255.0
R5(config-if)# mpls label protocol ldp
R5(config-if)# mpls ip

R5#configure terminal
R5(config)# interface Serial 0/1
R5(config-if)# ip address 200.200.50.2 255.255.255.0
R5(config-if)# mpls label protocol ldp
```

```
R5(config-if)# mpls ip

R5#configure terminal
R5(config)# interface Serial 0/2
R5(config-if)# ip address 200.200.60.1 255.255.255.0
R5(config-if)# clock rate 64000
R5(config-if)# mpls label protocol ldp
R5(config-if)# mpls ip
R3(config-if)# ip ospf authentication-key ugcint

R6#configure terminal
R6(config)# interface Serial 0/0
R6(config-if)# ip address 200.200.30.2 255.255.255.0
R6(config-if)# mpls label protocol ldp
R6(config-if)# mpls ip

R6#configure terminal
R6(config)# interface Serial 0/1
R6(config-if)# ip address 200.200.50.1 255.255.255.0
R6(config-if)# clock rate 64000
R6(config-if)# mpls label protocol ldp
R6(config-if)# mpls ip
```

Paso 3: Configuración de protocolo de enrutamiento OSPF

```
R3(config)#router ospf 1
R3(config-router)# network 192.168.23.33 0.0.0.0 area 0
R3(config-router)# network 200.200.10.0 0.0.0.255 area 0
R3(config-router)# network 200.200.20.0 0.0.0.255 area 0
R3(config-router)# network 200.200.30.0 0.0.0.255 area 0

R4(config)#router ospf 1
R4(config-router)# network 192.168.23.34 0.0.0.0 area 0
R4(config-router)# network 200.200.20.0 0.0.0.255 area 0
R4(config-router)# network 200.200.40.0 0.0.0.255 area 0

R5(config)#router ospf 1
R5(config-router)# network 192.168.23.35 0.0.0.0 area 0
R5(config-router)# network 200.200.40.0 0.0.0.255 area 0
R5(config-router)# network 200.200.50.0 0.0.0.255 area 0
R5(config-router)# network 200.200.60.0 0.0.0.255 area 0
R6(config)#router ospf 1
R6(config-router)# network 192.168.23.36 0.0.0.0 area 0
R6(config-router)# network 200.200.30.0 0.0.0.255 area 0
R6(config-router)# network 200.200.50.0 0.0.0.255 area 0
```

Paso 4: Especificar el router-id

```
R3(config)#mpls ldp router-id Loopback 155
R4(config)#mpls ldp router-id Loopback 155
```

R5(config)#mpls ldp router-id Loopback 155
R6(config)#mpls ldp router-id Loopback 155

Paso 5: Configuración de reenvío de paquetes

R3(config)#ip forward-protocol nd
R4(config)#ip forward-protocol nd
R5(config)#ip forward-protocol nd

3.9.5 Configuraciónde enrutamiento estáticoPE-CE

1. Configurarel enrutamiento estáticoPE-CE

Definir VRF estático en PE Enrutadores R2 and R2
R2(config)#ip vrf CINT
R2(config-vrf)# rd 1:100
R2(config-vrf)#route-target both 1:100
R2(config-vrf)#interface FastEthernet0/0
R2(config-if)# ip vrf forwarding CINT
R2(config-if)# ip address 10.10.100.2 255.255.255.252

2. Configurar ruta estática VRFen losenrutadoresPE

Paso 1. Configurar VRF por ruta estáticaenlosenrutadoresPE

R2(config)#ip route vrf CINT 192.168.100.0 255.255.255.0 10.10.100.1 name toCINT

Paso 2. Configurar dirección IPv4Family yRedistribucióndeBGP

R2(config)#router bgp 65000
R2(config-router)#address-family ipv4 vrf CINT
R2(config-router-af)#network 10.10.100.0 255.255.255.252
R2(config-router-af)#redistribute static
R2(config-router-af)#redistribute connected

3.9.6 ConfiguraciónMPLS reenvío yVRFdefinición enPEenrutadores

Para la configuración dereenvíoMPLS se le aplicara a los enrutadores PE que a su vez esel primer paso parael suministrobackboneMPLSVPNdel proveedor de servicios. Con esta configuración se asegura la disposición delproveedor de serviciospara proporcionarservicios relacionados conMPLS a los clientes potenciales. Los pasos para configurarel reenvío deMPLSen los enrutadoresPE son:

Paso1.HabilitarCEF

```
R2(config)# ip cef distributed
R2(config)# do show running-config interface s0/0 | include cef  no ip route-cache cef
R2(config)# interface s0/0
R2(config-if)#ip route-cache cef
```

Paso 2. Configurar el protocolo de enrutamiento IGP en el router PE.

```
R2(config)#router ospf 1
R2(config)#network 192.168.23.32 0.0.0.0 area 0
R2(config)#network 200.200.10.0 0.0.0.255 area 0
```

Paso 3. Configurar MPLS en las interfaces de PE conectados a P.

```
R2(config)#mpls ldp router-id loopback 155
```

Paso 4. Habilitar IPv4 MPLS o de envío de etiquetas en la interfaz

```
R2(config)#interface serial 0/1
R2(config-if)#mpls ip
```

VRF definición en PE Enrutadores: pasos de configuración

Paso 1. Configurar VRF en PE router

```
R2(config)#ip vrf  CINT
```

Paso 2. Configurar RD

```
R2(config-vrf)#rd  65000:100
```

Paso 3. Configurar la política de importación y exportación

```
R2(config-vrf)#route-target both 65000:100
```

Paso 4. Asociar VRF con la interface

```
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 10.10.100.2 255.255.255.252
R2(config-if)#ip  vrf forwarding CINT
R2(config-if)# ip address 10.10.100.2 255.255.255.252
```

3.10 Validación de configuración y análisis de Pruebas

Para la validación y funcionalidad del proceso MPLS VPN se analizara por partes cada proceso ya sea BGP en los PE como las VPN de la carrera con la Universidad y de igual manera el envío de etiquetas usando el wireshark con los equipos involucrados en el diseño.

3.10.1 Verificacióny monitoreo deBGPPE-PE

Para la verificación del protocolo BGP en los enrutadores PE se verifica la relación BGP al igual que la vpn como se muestra a continuación:

Paso 1: Verificar relación BGP

```
R2#show ip bgp vpnv4 all summary
BGP router identifier 192.168.23.32, local AS number 65000
BGP table version is 9, main routing table version 9
4 network entries using 560 bytes of memory
4 path entries using 272 bytes of memory
4/3 BGP path/bestpath attribute entries using 496 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1384 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.23.37   4 65000      47      49        9    0    0 00:42:01        2
```

```
R7#show ip bgp vpnv4 all summary
BGP router identifier 192.168.23.37, local AS number 65000
BGP table version is 9, main routing table version 9
4 network entries using 560 bytes of memory
4 path entries using 272 bytes of memory
4/3 BGP path/bestpath attribute entries using 496 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1384 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.23.32   4 65000      53      51        9    0    0 00:46:39        2
```

Paso 2: Verificar la tabla de enrutamiento VRF en los PE

```
R2#show ip route vrf CINT bgp
B    192.168.200.0/24 [200/0] via 192.168.23.37, 00:43:18
     10.0.0.0/30 is subnetted, 2 subnets
B       10.10.100.4 [200/0] via 192.168.23.37, 00:43:18
```

```
R7#show ip route vrf  CINT bgp
     10.0.0.0/30 is subnetted, 2 subnets
```

```
B       10.10.100.0 [200/0] via 192.168.23.32, 00:49:07
B    192.168.100.0/24 [200/0] via 192.168.23.32, 00:49:07
```

Paso 3: Verificar la tabla de enrutamiento BGP VPNv4 en los PE

```
R2#show ip bgp vpnv4 all
BGP table version is 9, local router ID is 192.168.23.32
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: 65000:100 (default for vrf CINT)
*> 10.10.100.0/30   0.0.0.0                  0         32768 i
*>i10.10.100.4/30   192.168.23.37            0    100      0 ?
*> 192.168.100.0    10.10.100.1              0         32768 ?
*>i192.168.200.0    192.168.23.37            0    100      0 ?
```

R7#show ip bgp vpnv4 all

```
BGP table version is 9, local router ID is 192.168.23.37
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: 65000:100 (default for vrf CINT)
*>i10.10.100.0/30   192.168.23.32            0    100      0 i
*> 10.10.100.4/30   0.0.0.0                  0         32768 ?
*>i192.168.100.0    192.168.23.32            0    100      0 ?
*> 192.168.200.0    10.10.100.5              0         32768 ?
```

Paso 4: Verificar conectividad de extremo a extremo

```
R1#ping 10.10.100.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/157/316 ms

R8#ping 10.10.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/67/108 ms
```

3.10.2 Verificación de enrutamiento estático PE-CE

Para la validación del enrutamiento estático se valida la tabla de rutas tanto BGP como las VPN de los enrutadores involucrado como se visualiza a continuación:

Paso 1. BGP VPNv4 Routing Table

```
R2#show ip bgp vpnv4 vrf CINT

BGP table version is 9, local router ID is 192.168.23.32
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: 65000:100 (default for vrf CINT)
*> 10.10.100.0/30   0.0.0.0                  0         32768 i
*>i10.10.100.4/30   192.168.23.37            0    100      0 ?
*> 192.168.100.0    10.10.100.1              0         32768 ?
*>i192.168.200.0    192.168.23.37            0    100      0 ?
```

Paso 2. Verificar la tabla de enrutamiento VRF en R2

```
R2# show ip route vrf CINT

Routing Table: CINT
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
       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

B    192.168.200.0/24 [200/0] via 192.168.23.37, 01:37:07
     10.0.0.0/30 is subnetted, 2 subnets
B       10.10.100.4 [200/0] via 192.168.23.37, 01:37:07
C       10.10.100.0 is directly connected, FastEthernet0/0
S    192.168.100.0/24 [1/0] via 10.10.100.1
```

Paso 3. Verificar conectividad extremo a extremo usando el ping

```
R1#ping 192.168.200.200 source 192.168.100.100
Sending 5, 100-byte ICMP Echos to 192.168.200.200, timeout is 2 seconds:
Packet sent with a source address of  192.168.200.100
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

3.10.3 Verificación de la configuración VRF paraenrutadores PE

La validación de la VPN en los enrutadores PE se la puede realizar con los comandos show ip vrf o show ip vrf interfaces como se muestra a continuación:

R2#show ip vrf

Name	Default RD	Interfaces
CINT	65000:100	Fa0/0

R2#show ip vrf interfaces

Interface	IP-Address	VRF	Protocol
Fa0/0	10.10.100.2	CINT	up

3.10.4 Verificación básica delfuncionamiento MPLS

La verificación de funcionalidad de MPLS se la puede resumir en 5 pasos como se muestra a continuación:

Paso 1: Verificación de CEF

R1#show ip cef

Prefix	Next Hop	Interface
0.0.0.0/0	drop	Null0 (default route handler entry)
0.0.0.0/32	receive	
10.10.100.0/30	attached	FastEthernet0/0
10.10.100.0/32	receive	
10.10.100.1/32	receive	
10.10.100.2/32	10.10.100.2	FastEthernet0/0
10.10.100.3/32	receive	
10.10.100.4/30	10.10.100.2	FastEthernet0/0
192.168.100.0/24	attached	Loopback10
192.168.100.0/32	receive	
192.168.100.100/32	receive	
192.168.100.255/32	receive	
192.168.200.0/24	10.10.100.2	FastEthernet0/0
224.0.0.0/4	drop	
224.0.0.0/24	receive	
255.255.255.255/32	receive	

R2# show ip cef

Prefix	Next Hop	Interface
0.0.0.0/0	drop	Null0 (default route handler entry)
0.0.0.0/32	receive	
192.168.23.32/32	receive	
192.168.23.33/32	200.200.10.2	Serial0/1
192.168.23.34/32	200.200.10.2	Serial0/1
192.168.23.35/32	200.200.10.2	Serial0/1
192.168.23.36/32	200.200.10.2	Serial0/1
192.168.23.37/32	200.200.10.2	Serial0/1
200.200.10.0/24	attached	Serial0/1
200.200.10.0/32	receive	
200.200.10.1/32	receive	

```
200.200.10.255/32   receive
200.200.20.0/24     200.200.10.2        Serial0/1
200.200.30.0/24     200.200.10.2        Serial0/1
200.200.40.0/24     200.200.10.2        Serial0/1
200.200.50.0/24     200.200.10.2        Serial0/1
200.200.60.0/24     200.200.10.2        Serial0/1
224.0.0.0/4         drop
224.0.0.0/24        receive
255.255.255.255/32  receive
```

```
R2#show cef interface serial 0/1

Serial0/1 is up (if_number 7)
  Corresponding hwidb fast_if_number 7
  Corresponding hwidb firstsw->if_number 7
  Internet address is 200.200.10.1/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  Interface is marked as point to point interface
  Hardware idb is Serial0/1
  Fast switching type 4, interface type 185
  IP CEF switching enabled
  IP CEF Fast switching turbo vector
  Input fast flags 0x0, Input fast flags2 0x0, Output fast flags 0x0, Output fast
flags2 0x0
  ifindex 5(5)
  Slot 0 Slot unit 1 Unit 1 VC -1
  Transmit limit accumulator 0x0 (0x0)
IP MTU 1500
```

Paso 2: Validar reenvío de MPLS si se encuentra habilitado en las interfaces

```
R2#show mpls interfaces

Interface              IP            Tunnel      Operational
Serial0/1              Yes (ldp)     No          Yes
```

Paso 3: Verificar el estado del protocolo de distribución de etiquetas (LDP)

```
R2#show mpls ldp discovery

Local LDP Identifier:
    192.168.23.32:0
    Discovery Sources:
    Interfaces:
        Serial0/1 (ldp): xmit/recv
LDP Id: 192.168.23.33:0
```

Paso 4: Validar el estado de los LDP vecinos

R2#show mpls ldp neighbor

Peer LDP Ident: 192.168.23.33:0; Local LDP Ident 192.168.23.32:0
TCP connection: 192.168.23.33.58538 - 192.168.23.32.646
State: Oper; Msgs sent/rcvd: 439/438; Downstream
Up time: 06:11:33
LDP discovery sources:
Serial0/1, Src IP addr: 200.200.10.2
Addresses bound to peer LDP Ident:
200.200.10.2 192.168.23.33 200.200.20.1 200.200.30.1

Verificación panel de control y datos de reenvíoenMPLS

R2#show mpls ldp bindings

tib entry: 192.168.23.32/32, rev 2
local binding: tag: imp-null
remote binding: tsr: 192.168.23.33:0, tag: 20
tib entry: 192.168.23.33/32, rev 14
local binding: tag: 20
remote binding: tsr: 192.168.23.33:0, tag: imp-null
tib entry: 192.168.23.34/32, rev 12
local binding: tag: 19
remote binding: tsr: 192.168.23.33:0, tag: 19
tib entry: 192.168.23.35/32, rev 10
local binding: tag: 18
remote binding: tsr: 192.168.23.33:0, tag: 18
tib entry: 192.168.23.36/32, rev 8
local binding: tag: 17
remote binding: tsr: 192.168.23.33:0, tag: 17
tib entry: 192.168.23.37/32, rev 6
local binding: tag: 16
remote binding: tsr: 192.168.23.33:0, tag: 16
tib entry: 200.200.10.0/24, rev 4
local binding: tag: imp-null
remote binding: tsr: 192.168.23.33:0, tag: imp-null
tib entry: 200.200.20.0/24, rev 24
local binding: tag: 25
remote binding: tsr: 192.168.23.33:0, tag: imp-null
tib entry: 200.200.30.0/24, rev 22
local binding: tag: 24
remote binding: tsr: 192.168.23.33:0, tag: imp-null
tib entry: 200.200.40.0/24, rev 20
local binding: tag: 23
remote binding: tsr: 192.168.23.33:0, tag: 23
tib entry: 200.200.50.0/24, rev 18
local binding: tag: 22

```
        remote binding: tsr: 192.168.23.33:0, tag: 22
  tib entry: 200.200.60.0/24, rev 16
        local binding:  tag: 21
remote binding: tsr: 192.168.23.33:0, tag: 21
```

Paso 5: Asignaciónde etiquetas y verificación de distribuciónen R2

R2#show mpls forwarding-table

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	16	192.168.23.37/32	0	Se0/1	point2point
17	17	192.168.23.36/32	0	Se0/1	point2point
18	18	192.168.23.35/32	0	Se0/1	point2point
19	19	192.168.23.34/32	0	Se0/1	point2point
20	Pop tag	192.168.23.33/32	0	Se0/1	point2point
21	21	200.200.60.0/24	0	Se0/1	point2point
22	22	200.200.50.0/24	0	Se0/1	point2point
23	23	200.200.40.0/24	0	Se0/1	point2point
24	Pop tag	200.200.30.0/24	0	Se0/1	point2point
25	Pop tag	200.200.20.0/24	0	Se0/1	point2point
26	Aggregate	10.10.100.0/30[V]	0		
27	Untagged	192.168.100.0/24[V]	0	Fa0/0	10.10.100.1

3.11 Análisis de resultados usando Wireshark

Para la validación de la configuración en el esquema planteado en la presente tesis se ha necesitado la ayuda de la aplicación de un sniffer como wireshark para así visualizar las capturas de paquetes del backbone, de los equipos CE, PE y P respectivamente así como el tráfico respectivo de cada equipo de comunicación involucrado en el diseño.

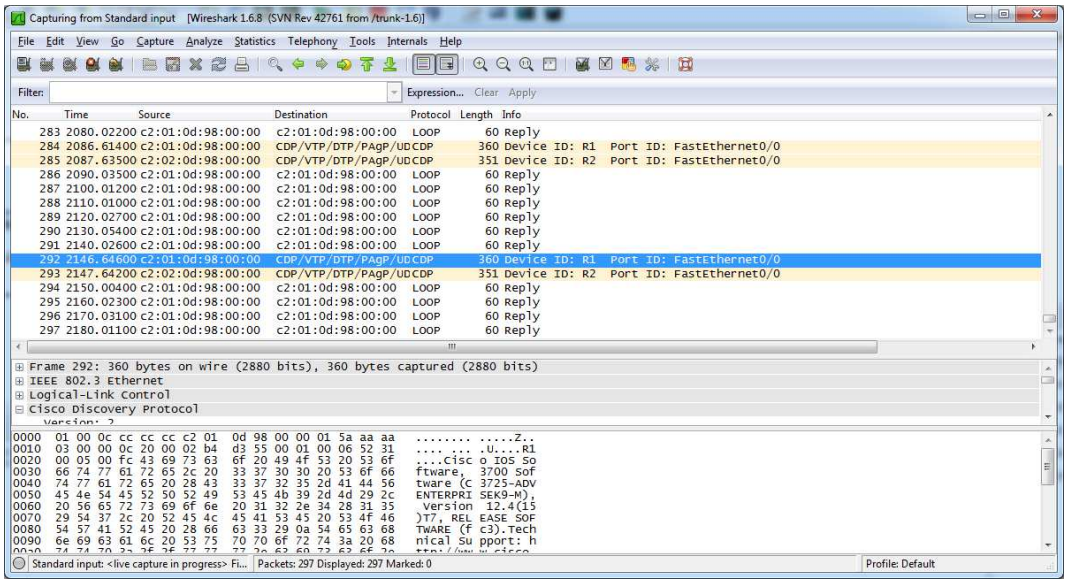

Figura 3.18: Validación de paquetes de CE - R1

Fuente: Obtenida de aplicativo Wireshark

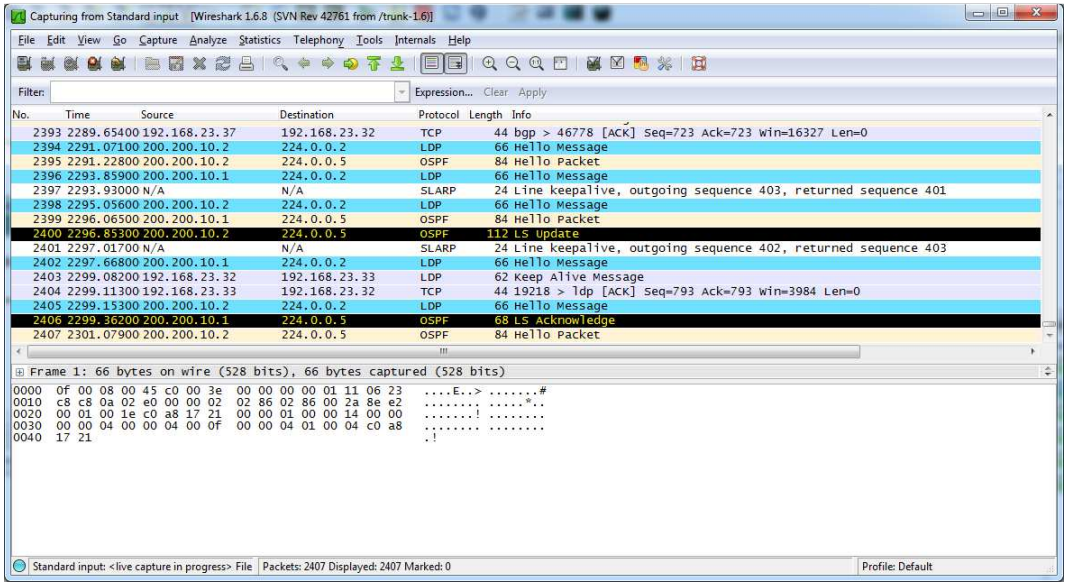

Figura 3.19: Validación de paquetes de PE – R2

Fuente: Obtenida de aplicativo Wireshark

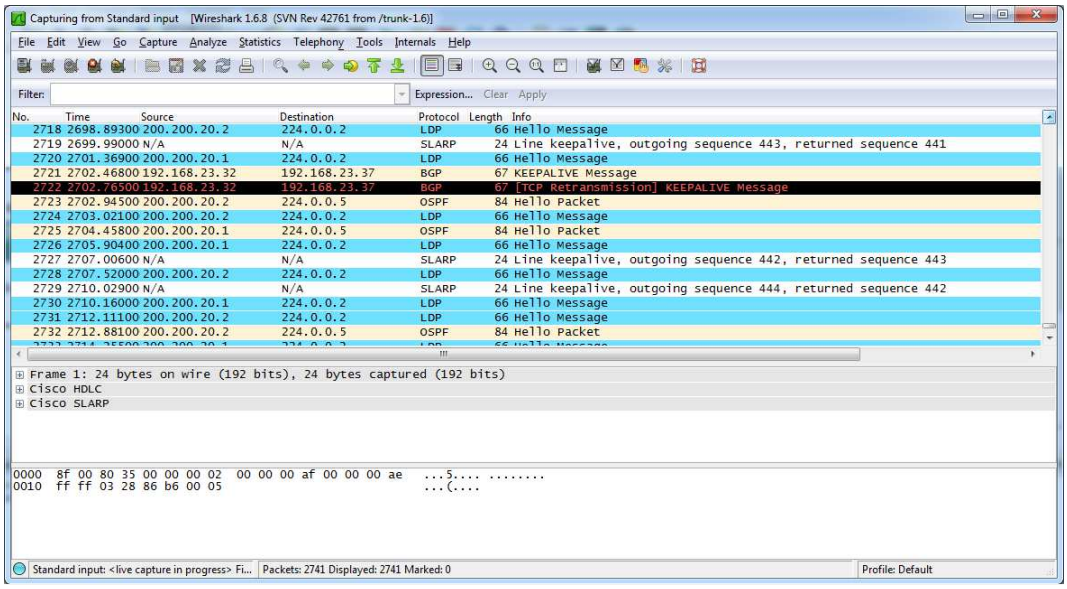

Figura 3.20: Validación de paquetes de P – R4
Fuente: Obtenida de aplicativo Wireshark

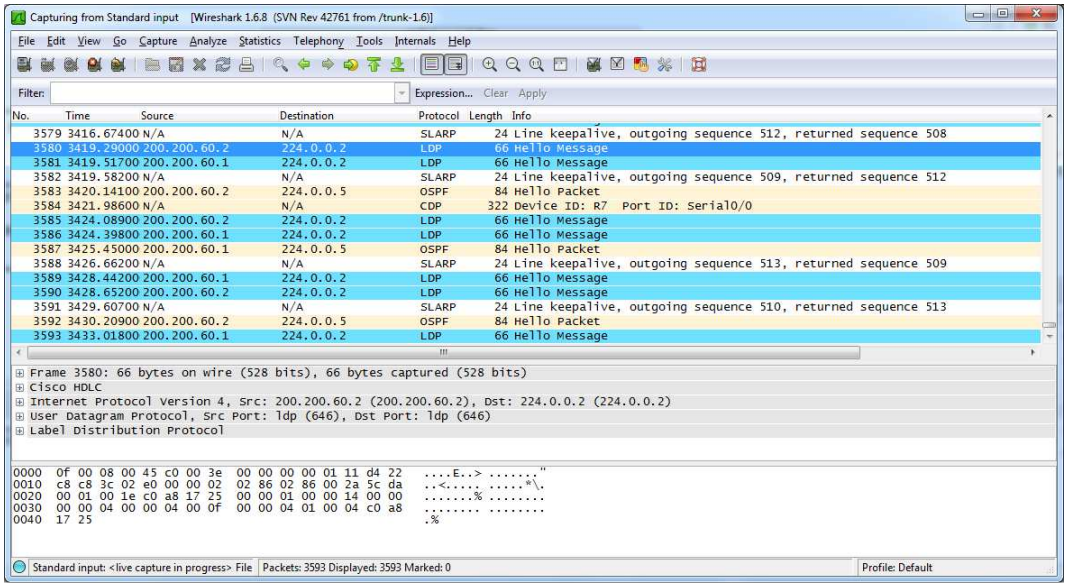

Figura 3.21: Validación de paquetes de P – R5
Fuente: Obtenida de aplicativo Wireshark

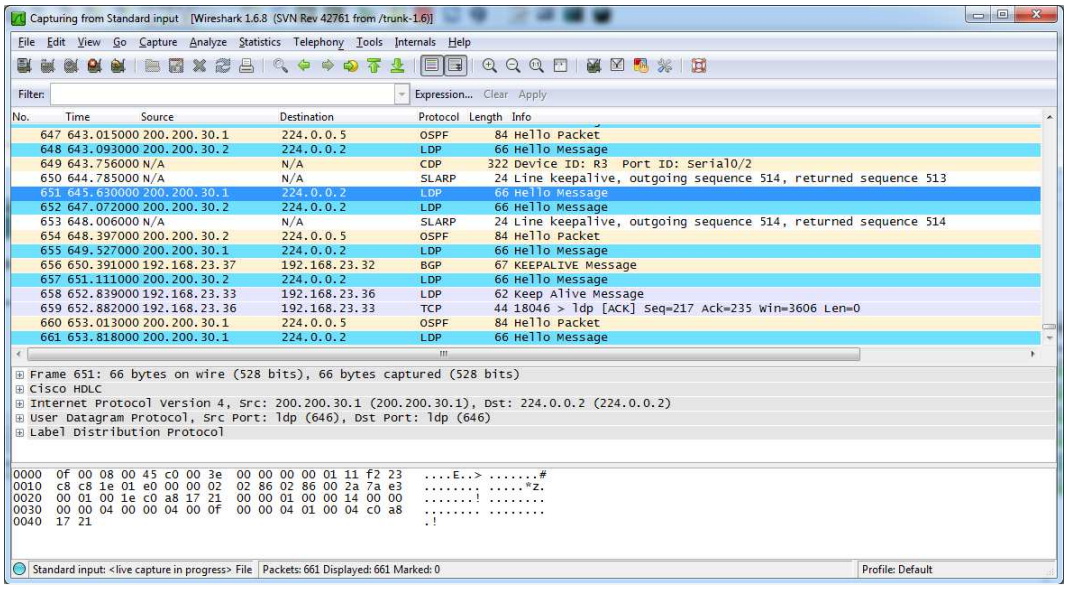

Figura 3.22: Validación de paquetes de P – R6
Fuente: Obtenida de aplicativo Wireshark

CAPÍTULO IV
CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

En el presente trabajo de tesis se detalla las características generales de MPLS así como también la arquitectura para realizar ingeniería de tráfico, la misma que se puede definir como viable en un tiempo de mediano a largo plazo según la estructura organizacional, para poder definir el diseño se necesitó un emulador de configuración de enrutadores como GNS3 que nos facilitó realizar la configuración específica para un posterior análisis de resultados ayudados con la herramienta del wireshark.

La tecnología MPLS permite a los ISP incrementar la fiabilidad y confianza en sus redes por lo que beneficia al reducir tiempos en su transmisión de información y brinda seguridad requerida por el cliente. Cabe indicar que pueden ser usados varios protocolos de enrutamiento dinámico como RIP, EIGRP, OSPF o inclusive enrutamiento estático, pero por las bondades que tiene cada uno de ellos se prefiere trabajar con OSPF por sus ventajas con respecto a los otros protocolos

MPLS VPN con su implementación en la Universidad de Guayaquil con la carrera de Ingeniería de Networking ayudará a la comunicación entre las mismas así también a la especialización de la tecnología para los estudiantes de la carrera de manera tal que podrían tener mejor aprendizaje y posiblemente las mejoras de velocidades se verán incrementadas en los próximos años y estarán en un nivel de poder hacer las respectivas actualizaciones si ameritan.

MPLS VPN va permitir que las demás facultades o carreras que no se encuentran radicadas físicamente en la universidad matriz utilicen la tecnología en un futuro para así poder tener las comunicaciones online de manera segura con calidad de servicio.

La implementación de una red basada MPLS VPN en Guayaquil revolucionará el mercado tecnológico, ya que con la capacidad diseñada se podrá transportar muchos servicios de diferentes formatos, permitiendo ser a la Universidad una

entidad que brinda calidad de servicio así como una red segura para la transmisión de data a nivel MAN.

4.2 Recomendaciones

Con respeto a los equipos que pueden usarse hay distintos proveedores como 3COM ahora de HP, Alcatel, Cisco, sin embargo por todas las bondades así como el soporte del mismo se recomienda los equipos Cisco ya es una solución completa e integra para cualquier entorno de comunicaciones. Sus dispositivos de comunicación tanto router como switches poseen calidad y operatividad que se adaptan a cualquier esquema topológico y mucho mejor usando la tecnología MPLS VPN prueba de ello los escenarios de resultados que se evaluó configuración y soporte de la tecnología mencionada. Adicional a ello se recoge que son de fácil implementación y tienen el soporte necesario en caso de necesitar alguna referencia.

Por todo lo mencionado es importante recalcar que la implementación de esta solución es de suma importancia por la seguridad y calidad de servicio al transmitir información confidencial entre lugares distantes y más aún en la parte educativa como lo es la Universidad de Guayaquil.

BIBLIOGRAFÍA

Alcatel. (2013, Junio 20). Retrieved from http://www3.alcatel-lucent.com/alcatel/

Alwayn., V. (2002). *Advanced MPLS Design and Implementation.*Cisco System.

Cabeza, E. C. (2009). *Fundamentos de Routing.*

CISC. (2012, Diciembre 1). Retrieved from http://www.cisc.ug.edu.ec/cisc/index.html

Cisco. (2006). *Implementing Cisco MPLS volumen 1 versión 2.2 Student guide.* Cisco Systems.

Cisco. (2006). *Implementing Cisco MPLS volumen 2 versión 2.2 Student guide.* Cisco Systems.

Cisco. (2008). *Guia de configuracion Cisco IOS Multiprotocol Label Switching.*San Jose: Cisco Systems.

Cisco. (2012, Enero 15). Retrieved from http://www.cisco.com

Cisco-Router. (2013, Septiembre 16). Retrieved from http://www.cisco.com/en/US/prod/collateral/routers/ps282/product_data_sheet09186a008009203f.html

CiscoRouterS. (2013, Septiembre 16). Retrieved from http://www.cisco.com/web/ES/solutions/smb/products/routers_switches/

CiscoSwitches. (2013, Septiembre 16). Retrieved from http://www.cisco.com/en/US/products/hw/switches/index.html

CiscoTech. (2013, Septiembre 12). Retrieved from http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a00800a6c11.shtml

Cisco-VPN. (2013, Agosto 5). Retrieved from http://www.cisco.com/web/ES/solutions/es/vpn/index.html

Coimbraweb. (2013, Mayo 10). Retrieved from http://www.coimbraweb.com/documentos/telecom/9.8_mpls.pdf

COIT. (2013, Mayo 14). Retrieved from ttp://www.coit.es/publicac/publbit/bit109/quees.htm

Datatracker. (2013, Octubre 14). Retrieved from http://datatracker.ietf.org/wg/mpls/charter/

Farrel., B. S. (2008). *MPLS: Next Steps.* Morgan Kaufmann series in Networking.

Fengnet. (2013, Mayo 10). Retrieved from http://fengnet.com/book/MPLS%20Configuration%20on%20Cisco%20IOS%20Software/ch09lev1sec4.html

Frankel, S. (2011, Febrero). *RFC6071.* Retrieved from http://tools.ietf.org/html/rfc6071

Gallaher, R. (2003). *MPLS Training Guide, Building Multi Protocol Label Switching Networks.* Syngress Publishing.

Ghein, L. d. (2007). *Fundamentos de MPLS* . Cisco Systems.

GNS3. (2013, Diciembre 2). Retrieved from http://www.gns3.net

Gómez, M. M. (2006). *Introducción a la metodología de la investigación científica 1ra edición.*Córdoba : Editorial Berujas .

GoogleMaps. (2013, Septiembre 18). Retrieved from https://maps.google.com.ec/

Guichard, I. P. (2003). *MPLS and VPN Architectures Volume II.* Cisco Systems .

HP. (2013, Diciembre 16). Retrieved from http://h17007.www1.hp.com/us/en/networking/index.aspx

IETF. (2013, Octubre 14). Retrieved from http://datatracker.ietf.org/wg/mpls/charter/

IIE. (2013, Julio 10). Retrieved from http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Codificacion%20de%20voz%20y%20video.pdf

ITU. (2013, Octubre 10). Retrieved from http://www.itu.int/es/Pages/default.aspx

K. Hamzeh, G. P. (1999, Julio). *RFC2637.* Retrieved from http://www.ietf.org/rfc/rfc2637.txt

Lobo, L. (2005). *Configuración MPLS de Cisco IOS Software.*Cisco Press.

Lucek, I. M. (2011). *MPLS -Enabled Applications, Emerging Developments and New Technologies Third Edition.* John Wiley & Sons.

Monografias. (2013, Septiembre 10). Retrieved from http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml

Monrique Morrow, A. S. (1997). *MPLS y redes de proxima Generacion: Fundamentos de las NGN y virtualizacion empresarial.*Indianapolis, USA: Cisco Press.

Nadeau, T. D. (2003). *MPLS Network Management, MIBs. Tools, and techniques.* Morgan Kaufmann.

Namakforoosh, M. N. (2005). *Metodología de la Investigación 2da edición* . México: Limusa Noriega Editores.

Nethumans. (2013, Agosto 5). Retrieved from http://www.nethumans.com/solutions/itSecurity/VPN.aspx

Pegaso. (2013, Octubre 6). Retrieved from http://pegaso.ls.fi.upm.es/servicios/transparencias3/sld041.htm

Pickavance, C. L. (2006). *Selecting MPLS VPN services.* Cisco Systems.

Reddy, K. (2005). *Building MPLS-Based Broadband Access VPNs.* Cisco Systems.

Rediris. (2013, Agosto 5). Retrieved from http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

Salkind, N. J. (1999). *Métodos de investigación.* México : Editorial Prentice Hall.

Sánchez, E. R. (2012). *Tecnologías de la información y la comunicación para la innovación educativa.* Mexico: Diaz de Santos.

Scott, C. W. (1999). *Virtual Private Networks.*O'Reilly & Associates.

Simha., E. O. (2003). *Traffic Engineering with MPLS.* Cisco Systems.

SW-LIBRE. (2013, Agosto 6). Retrieved from http://sw-libre.blogspot.com/2011/11/configurar-una-vpn-de-acceso-remoto-con.html

Tamayo, M. T. (2004). *El proceso de la investigación científica, 4ta edición* . México: Editorial Limusa.

Universidad Guayaquil. (2012, Diciembre 1). Retrieved from http://www.ug.edu.ec/SitePages/historia.aspx

Valencia, A. T. (1999, Agosto). *RFC 2661.*Retrieved from http://www.ietf.org/rfc/rfc2661.txt

VPN. (2013, Agosto 5). Retrieved from http://redprivadavirtualiut.wikispaces.com/Tipos+de+VPN

Wikipedia. (2014, 08 13). *WikipediaL2TP*. Retrieved from http://es.wikipedia.org/wiki/L2TP

Wikipedia-UniversidadGuayaquil. (2012, Diciembre 1). Retrieved from http://es.wikipedia.org/wiki/Universidad_de_Guayaquil

Wireshark. (2013, Diciembre 2). Retrieved from http://www.wireshark.org

Wordpress. (2013, Agosto 5). Retrieved from http://fundamentosderedesespe.wordpress.com/2012/01/27/tecnologias-mpls/

WordpressMpls. (2013, 08 19). Retrieved from http://omar1985.wordpress.com/

GLOSARIO DE TÉRMINOS

ATM	Asynchronous Transfer Mode: Modo de Transferencia Asincrónico.
AH	Authentication Protocol: Protocolo de autenticación
AIM	Advanced Integration Module: Modulo avanzado de integración
ATM	Asynchronous Transfer Mode: Modo de transferencia asíncrona
BACKBONE	Se refiere a las principales conexiones troncales de Internet. Está compuesta por enrutadores comerciales, gubernamentales de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.
BGP	Border Gateway Protocol: Protocolo de gateway fronterizo
CE	Customer Edge: Router de cliente
CN	Customer Network: Red cliente
CoS	Quality of Service: Calidad de Servicio
DIFFSERV	Servicios diferenciados
DSL	Digital Subscriber Line: Línea de Abonado Digital.
EIGRP	Enhanced Interior Gateway Routing Protocol: Protocolo de enrutamiento de gateway interior mejorado
ETHERNET	Estándar de redes de área local para computadores con acceso al medio por detección de la portadora con detección de colisiones
FEC	Forward Error Correction: Corrección de errores
FIB	Forwarding information base: Base de información de envío
FIFO	First In First Out que indica que las posiciones se cierran en el orden que fueron abiertas.
FO	Fiber optic: Fibra Óptica.
FRAME RELAY	Frame-mode Bearer Service: técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual
IEEE	Institute of Electrical and Electronics Engineers: Instituto de ingenieros eléctricos y electrónicos

IETF	Internet Engineering Task Force: Grupo de trabajo de Ingeniería de Internet
IGP	Interior Gateway Protocol: Protocolo de pasarela interno
IOS	Internetwork Operating System: es el software utilizado en los enrutadores y switches
IP	Internet Protocol: Protocolo de Internet.
IPSEC	Internet Protocol security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando cada paquete en un flujo de datos.
IPV6	Internet Protocol versión 6: Protocolo de Internet versión 6, es una versión del protocolo Internet Protocol (IP) y diseñada para reemplazar a Internet Protocol versión 4 (IPv4)
IS-IS	Intermediate System to Intermediate System: Sistema intermedio a Sistema intermedio
ISP	Internet service Provider: Proveedor de servicios de Internet
ITU	Internacional Telecommunications Unión: Unión Internacional de Telecomunicaciones.
L2TP	Layer 2 Tunneling Protocol: Protocolo de túnel de capa 2
LAN	Local Area Network: Red de Área Local.
LDP	Label Distribution Protocol: Protocolo de Distribución de Etiquetas
LER	Label Edge Router - Enrutadores de Etiquetas de Borde
LFIB	Label Forwarding Instance Base: Base de información de envío de etiquetas
LIB	Label Information Base: Base de información de etiquetas
LSP	Label Switched Path: Caminos conmutados mediante etiquetas
LSR	Label Switching Router - Enrutadores Conmutadores de Etiquetas
MAC	Media Access Control: Control de Acceso al Medio.
MAN	Metropolitan Área Network: Red de Área Metropolitana.
MPLS	Multiprotocol Label Switching: Conmutación Multi-Protocolo mediante Etiquetas

MULTICAST	Método para transmitir datagramas IP a un grupo de receptores interesados.
OSI	Open Systems Interconnection: Interconexión de Sistemas Abiertos.
OSPF	Open Shortest Path First: El camino más corto primero
PDU	Packet data unit: Unidad de datos de protocolo se utilizan para el intercambio de datos entre unidades disparejas, dentro de una capa del modelo OSI.
PE	Provider Edge: Router de proveedor
PHP	Remoción en el penúltimo salto
POP	Es una operación donde la etiqueta es retirada del paquete lo cual puede revelar una etiqueta interior.
PPP	Point-to-point Protocol: Protocolo punto a punto
PPTP	Point-To-Point Tunneling Protocol: Protocolo punto a punto de túnel
PUSH	Es una operación de aplicar nueva etiqueta la que es empujada encima de otra si existe.
RAS	Servidor de acceso remoto, se utiliza para conectarse a las LAN o WAN mediante internet, modem, vpn.
RDSI	Integrated Services Digital Networks: Red Digital de Servicios Integrados
RFC	Request For Comments: Petición de comentarios
RIB	Routing Information Base: Base de información de ruteo
RIP	Routing Information Protocol: Protocolo de Información de enrutamiento
ROUTER	Es un dispositivo que proporciona conectividad a nivel de red en el modelo OSI, su función principal consiste en encaminar paquetes de datos de una red a otra
RSVP	Resource Reservation Protocol: Protocolo de reserva de recursos
SA	Autonomous System: Sistema Autónomo, es definido como un grupo de redes IP que poseen una política de rutas propia e independiente

SOHO	Small Office-Home Office: Pequeña Oficina-Oficina en Casa, es un término que se aplica para denominar a los aparatos destinados a un uso profesional o semiprofesional pero que, a diferencia de otros modelos, no están pensados para asumir un gran volumen de trabajo.
SPANNING TREE	Spanning Tree Protocol, es un protocolo de red de nivel 2 del modelo OSI, su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes
STACK	Pila, sirve para el apilado jerárquico de etiquetas
SUPERTEL	Superintendencia de telecomunicaciones, Organismo Estatal de Control de las Telecomunicaciones
SWAP	Es una operación que intercambia una etiqueta por otra y el paquete es enviado en el camino asociado a esta nueva etiqueta.
SWITCH	Es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red.
TCP	Transmission Control Protocol: Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet.
TLV	Time To Live: Tiempo de Vida, contador en el interior de los paquetes multicast que determinan su propagación.
UNICAST	Es el envío de información desde un único emisor a un único receptor.
UPSTREAM	Se refiere a la velocidad con que los datos pueden ser transferidos de un cliente a un servidor, lo que podría traducirse como velocidad de carga:
BER	Bits Error Rate: Tasa de Bits Erróneo. La tasa de errores de desempeño
VLAN	Virtual Local Area Network: Red de Area Local Virtual.
VPN	Virtual Private Network: Red Privada Virtual supone una tecnología de red que, por razones de costo y comodidad, brinda la posibilidad de conectarse a una red pública generando una extensión a nivel de área local.

VRF	Virtual Routing and Forwarding, permite múltiples tablas de rutas separadas las cuales pueden coexistir en el mismo router y al mismo tiempo.
WAN	Wide Area Network: Red de Area Amplia.

ANEXOS

Anexo #1: Diseño de Red MPLS VPN de la Universidad De Guayaquil y Carrera de Ingeniería en Networking