

**ANÁLISIS DE MULTIPROTOCOLO LABEL SWITCHING EN REDES  
DE ÁREA METROPOLITANA**

**ANDRÉS FERNANDO PRADA SUAREZ**

**PABLO ANDRÉS BARON RUEDA**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD DE INGENIERÍAS FISICOMECAICAS  
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE  
TELECOMUNICACIONES  
ESPECIALIZACIÓN EN TELECOMUNICACIONES  
BUCARAMANGA  
2011**

**ANÁLISIS DE MULTIPROTOCOLO LABEL SWITCHING EN REDES  
DE ÁREA METROPOLITANA**

**ANDRÉS FERNANDO PRADA SUAREZ**

**PABLO ANDRÉS BARON RUEDA**

**Monografía presentada como requisito para optar al título  
de Especialista en Telecomunicaciones**

**Director**

**ING. RAUL BAREÑO**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD DE INGENIERÍAS FÍSICOMECÁNICAS  
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE  
TELECOMUNICACIONES  
ESPECIALIZACIÓN EN TELECOMUNICACIONES  
BUCARAMANGA  
2011**

## **TABLA DE CONTENIDO**

INTRODUCCIÓN .....	14
1. OBJETIVOS .....	15
2. PLANTEAMIENTO DEL PROBLEMA .....	16
3. JUSTIFICACION.....	18
4. MARCP TEÓRICO .....	19
4.1. MPLS .....	19
4.2. Arquitectura MPLS.....	23
4.3. OPERACIONES BASICAS DE ETIQUETAS .....	28
4.4. Direccionamiento MPLS .....	29
4.5. Formato Etiqueta MPLS .....	31
4.6. TIPOS DE ENRUTAMIENTO .....	36
4.7. DISTRIBUCIÓN DE ETIQUETAS Y ADMINISTRACIÓN .....	37
4.9. PHP.....	43
4.10. UBICACIÓN DE MPLS EN EL MODELO OSI .....	44
4.12. INGENIERA DE TRÁFICO .....	47
4.13. SECUENCIA DE CONFORMACIÓN DE UN TÚNEL.....	49
4.14. CLASES DE SERVICIO .....	51
5. PRÁCTICAS Y SIMULACIONES.....	53
5.1. Práctica de Laboratorio.....	58
5.2. Laboratorio .....	65
5.3. Comandos de Configuración .....	67
5.5. Generador De Tráfico .....	69
5.6. SHOW MPLS FORWARDING.....	72
7. INTERPRETACIÓN DE RESULTADOS .....	77
8. CONCLUSIONES.....	82
9. BIBLIOGRAFÍA.....	84

## TABLA DE FIGURAS

FIGURA 1 MALLA PARCIAL	FIGURA 2 MALLA COMPLETA	21
FIGURA 3 MPLS		21
FIGURA 4 COMPONENTE DE ARQUITECTURA DE UNA LSR		26
FIGURA 5 COMPONENTE DE ARQUITECTURA DE UN LSR DE BORDE		26
FIGURA 6 FUNCIONES PUSH SWAP Y POP		29
FIGURA 7 ENRUTAMIENTO EN UNA RED MPLS		30
FIGURA 8 ESTRUCTURA DE LA CABECERA MPLS		31
FIGURA 9 EJEMPLO TTL ESCENARIO UNO		33
FIGURA 10 EJEMPLO TTL ESCENARIO DOS		34
FIGURA 11 TTL EXPIRADO		36
FIGURA 12 KEEPALIVE		40
FIGURA 13 UBICACIÓN MPLS EN EL MODELO OSI		45
FIGURA 14 SIMULACIÓN RED MPLS		58
FIGURA 15 SIMULACION DE RED MPLS CON QoS		59
FIGURA 16 RESULTADO SIMULACIÓN		60
FIGURA 17 RESULTADO LSR DE ENTRADA		60
FIGURA 18 PAQUETES DE SALIDA DE UN LSR		61
FIGURA 19 PAQUETES DE UN LSR DE INGRESO		62
FIGURA 20 LSR DE SALIDA O LER		62
FIGURA 21 TRAFICO PRIORIZADO		63
FIGURA 22 TRAFICO DE ENTRADA LSR DE NÚCLEO		64
FIGURA 23 TRAFICO DE SALIDA LSR DE NÚCLEO		64
FIGURA 24 TOPOLOGÍA DE LABORATORIO		65
FIGURA 25 INTERCONEXIÓN DE DISPOSITIVOS DE LABORATORIO		65
FIGURA 26 INTERCONEXIÓN DE DISPOSITIVOS		66
FIGURA 27 CONFIGURACIÓN DE DISPOSITIVOS		66
FIGURA 28 CAPTURA CON WIRESHARK		67
FIGURA 29 CAPTURA DE TRÁFICO MPLS		77
FIGURA 30 RESULTADO PROTOCOLO EIGRP, LDP Y MPLS		78
FIGURA 31 CAPTURA TRÁFICO EIGRP		79
FIGURA 32 DATOS CAPTURA MPLS		80
FIGURA 33 DATOS CAPTURA EIGRP		80
FIGURA 34 TOPOLOGÍA MPLS Y EIGRP EN EL SIMULADOR GNS3		81

## LISTA DE TABLAS

TABLA 1 ETIQUETAMIENTO .....	74
TABLA 2 DISTANCIAS ADMINISTRATIVAS .....	76

## **ANEXOS**

1. Guía de configuración de MPLS.
2. Manual OpenSimMPLS. (Adjuntado digitalmente)
3. RFC 3031 y RFC 3036. (Adjuntados digitalmente)
4. Resultados de Captura WireShark Laboratorio (Adjuntadas digitalmente).
5. Resultado de captura de simulaciones (Adjuntadas digitalmente).

## Resumen

**Título:** Análisis de MultiProtocol Label Switching en redes de área metropolitana

**Autores:** Andrés Fernando Prada y Pablo Andrés Barón

**Palabras Claves:** MPLS, LDP, Router, Paquetes, Sesión, Tráfico Calidad-de-Servicio, Mensajes

### Contenido:

Mpls se convierte en una herramienta útil para las empresas que requieren un mejor instrumento para la convergencia de tecnologías. MPLS integra inteligencia de direccionamiento junto con los beneficios de una arquitectura IP, también permite implementar calidad de servicio, ingeniería de tráfico, con lo cual se logra mayor eficiencia a la red.

MPLS funciona a través de la inserción de una etiqueta en la cabecera de los paquetes, con el fin de que el *router* no tenga de desencapsular el paquete para saber su origen, sino que a través de esta etiqueta el router sepa su destino, sin necesidad de realizar esta operación. Para el envío de etiquetas entre los routers que utilizan MPLS, se utiliza el protocolo de distribución de etiquetas (LDP), el cual llena la base de información de etiquetas (LIB) de cada router.

Para comprobación de funcionamiento y rendimiento de una red MPLS, se realizaron varias simulaciones empleado aplicativo como: GNS3, Packet Tracer y OpenSimMPLS, junto con una práctica de laboratorio, utilizando Routers y Switchs de cisco, encontrados en el aula. Durante el desarrollo de esta actividad se utilizó para la captura de tráfico el aplicativo WareShark, el cual nos permitió comparar MPLS con otros protocolos de enrutamiento IP

Tomando como base la información recolectada tanto de libros como páginas web, junto con la experiencia del personal asesor del proyecto, se pudo apreciar el comportamiento y capacidad de implementar una red con el protocolo MPLS.

---

Proyecto de Grado Análisis de MultiProtocol Label Switching en redes de área metropolitana  
Facultad de ingenieras fisicomecanicas. Escuelas de Ingeniera Eléctrica, Electrónica y de  
Telecomunicaciones. Director Raul Bareño

## Summary

**Title:** Analysis of Multiprotocol Label Switching in metropolitan area networks

**Authors:** Andrés Fernando Prada y Pablo Andrés Baron

**Keywords:** MPLS, LDP, Router, Packets, Session, Traffic Quality-of-Service, Messages

**Content:**

MPLS has become a very helpful tool for companies that require a better way for technology convergence. MPLS integrate intelligent routing with the benefits of the actual IP architecture, plus it allows the implementation of QoS (Quality of Service), and a better flow efficiency through the network, can be obtained due to MPLS Traffic Engineering,

MPLS works through the insertion of a label on the header of the network packet, between layers 2 and 3 of the OSI model. The purpose of its location, is to avoid the decapsulation of the IP packet and to reroute it using just the information captured by the labels. For the exchange of the Labels inside between routers that are a part of the MPLS network, the Label Distribution Protocol (LDP) protocol is used. Through LDP, each router learns the labels of their peers and fills his Label Information Base (LIB), which in MPLS, represents the routing table in an IP network.

For the auditing of the operation and performance of a MPLS network, a series of test where realized, including the use of simulation software and the use of the laboratory. Software like Packet Tracer, GNS3, and OpenSimMPLS enabled the authors to understand the operation of an MPLS network from the moment a single router becomes aware of his peers, while transmitting traffic, and even the process that is carried out when a router learns that a destination becomes unreachable. During the all the activities that were carried out, the sniffer software commonly known as Wireshark, allowed the authors to capture the ongoing traffic in all the MPLS network topologies used.

Taking into account all the collected from books, webpages, the results from the simulations and the laboratories, and the personal experience of project manager, the operation and the different benefits MPLS it has to offer were appreciated are their fullest

---

Graduation Project Analysis of Multiprotocol Label Switching in metropolitan area networks  
Faculty of physical-mechanical engineers. Schools of Electrical Engineering, Electronics and  
Telecommunications. Director Raul Bareño

## **GLOSARIO**

LIB: (label información base) o tabla de conectividad

MPLS: (Multiprotocol Label Switching) tecnología de la comunicación multiprotocolo mediante etiquetas

LDP: label distribution protocol

IETF: Internet Engineering Task Force

LER (Label Edge Router): elemento que inicia o termina el túnel (agrega y quita las etiquetas). Es el punto de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router. Ambos se suelen denominar Edge Label Switch Router, ya que se encuentran en los extremos de la red MPLS.

LSR (Label Switching Router): elemento que conmuta etiquetas.

LSP (Label Switched Path): nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. Se debe tener en cuenta que un LSP es unidireccional.

LDP (Label Distribution Protocol): un protocolo para la distribución de etiquetas MPLS.

FEC (Forwarding Equivalence Class): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

QoS (Quality of Service): cualidad que permite priorizar el tráfico en una red dependiendo del servicio prestado.

OSI (Open System Interconnection): es el modelo de red descriptivo creado por la Organización Internacional de Estandarización 1984. Este modelo sirve para la creación de nuevas arquitecturas de interconexión e red.

SP (Service Provider): es el proveedor de servicio de internet.

IP (Internet Protocol): protocolo de red usado globalmente para el direccionamiento de equipos en la red. Actualmente existen dos versiones IPv4 e IPv6.

## **INTRODUCCIÓN**

Durante los últimos años los proveedores de servicios (SP) se han enfrentado a un sin número de desafíos para intentar atender la gran demanda de clientes, así como también de valores agregados. Esto ha llevado a que se busquen nuevas tecnologías que soporten los nuevos servicios que satisfagan sus requerimientos

Una necesidad actual es el envío de paquetes, esto debidos que el envío convencional, Protocolo Internet (IP) cuenta con múltiples limitaciones, por lo cual se buscan nuevos protocolos que sea lo suficientemente robustos para soportar el andamiaje tecnológico actual, con mayores prestaciones que ip.

MPLS se vislumbra como una alternativa ya que integra inteligencia de direccionamiento con el rendimiento de conmutación, y suministra beneficios importantes a la red, con una arquitectura de IP, integrando otras tecnologías de capa 2. MPLS es clave para la redes privadas virtuales escalables (VPN's) y calidad de servicio (QoS) en redes end to end, permitiendo el uso eficiente de redes existentes y posible crecimiento, también permite las corrección de fallas de enlace y fallas de nodo, ayuda a repartir y diferenciar servicios de redes ip end to end mediante configuración y direccionamiento.

# **1. OBJETIVOS**

## ***1.1. OBJETIVO GENERAL***

Presentar Multiprotocol Label Switching (MPLS) como una solución de última milla, teniendo en cuenta los resultados de las simulaciones y la prueba de laboratorio de una red MAN

## ***1.2. OBJETIVOS ESPECIFICOS***

1. Efectuar dos (2) simulaciones utilizando GNS3 Y PACKET TRACER
2. Realizar práctica de laboratorio, capturando trafico mediante el sniffer waresnark
3. Comparar y analizar, los hallazgos de la simulación y la práctica de laboratorio.
4. Exponer las bondades de implementar de MPLS, en comparación con otros protocolos.

## 2.

## PLANTEAMIENTO DEL PROBLEMA

Durante los años se ha visto un mayor crecimiento en las redes, mayor implementación de diferentes servicios (VozIP, VPN,...), y las exigencias de los clientes son cada vez mayores. Las empresas prestadoras de servicio de internet, han tenido que implementar nuevas tecnologías, nueva infraestructura y técnicas para entregarle al usuario final la disponibilidad y el acceso a estos servicios sin afectar el funcionamiento actual de la red, y que la misma sea mas escalable dándole a esta la facilidad de implementación de nuevos servicios a medida que el cliente requiera de estos.

Actualmente, algunas compañías siguen usando Protocolos como ATM o Frame Relay para manejar el backbone de sus empresas, y han sido capaces de integrar los diferentes servicios basados en IP. Este tipo de integración normalmente requiere de dos sistemas, uno que entre el tráfico y otro que maneje los diferentes servicios prestados.

MPLS nació como una solución para dicha integración. MPLS integra diferentes protocolos de capa 2 y capa 3, por eso es conocido como un protocolo de capa 2 y ½. Este protocolo implementa el uso de etiquetas agregándolas en el encapsulamiento entre la capa 2 y 3. Los routers se basan en estas etiquetas, en vez de la dirección IP, para enrutar el tráfico.

Una de las ventajas es la velocidad de enrutamiento al usar las etiquetas en vez de las direcciones IP. Además la integración de las diferentes capas, permite mayor escalabilidad para futuros nuevos usuarios o nuevos equipos que se añadan a la red.

### **3. JUSTIFICACION**

Este proyecto permite al estudiante aplicar lo aprendido en clases, como lo fueron: Diseño LAN y WAN, Protocolos IP y Configuración de Dispositivos de Red. Además, se presenta como una oportunidad para emplear varias de las habilidades adquiridas, aplicándolas junto con las herramientas presentadas en clase y demostrar su funcionalidad en diferentes escenarios.

De la misma manera se entiende que la aplicación de este protocolo es un proceso llevado a cabo recientemente. Por tanto, el estudio, simulación e implementación de este protocolo en un laboratorio ayuda a mantener a los estudiantes actualizados de los métodos llevados a cabo en las redes empresariales.

## **4. MARCP TEÓRICO**

Este capítulo es una presentación general de la monografía, en el cual se dará a conocer que es MPLS, como está conformado, como se aplica, que herramientas se emplearan para desarrollar las actividades propuestas, (simulaciones con los aplicativos *Packet Tracer* y *GNS3*, y la práctica de laboratorio). Las actividades propuestas se mostrarán en el capítulo II, y los análisis de los datos recolectados se revelarán en el capítulo III.

### **4.1. MPLS**

Es una nueva tecnología de transporte de datos creado por (1)ETF y definido en el RCF3031, que combina la práctica de las comunicaciones punto a punto y la factibilidad de los servicios *private line*.

Esta nueva tecnología de conmutación, puede abastecer circuitos virtuales en las redes IP. MPLS Se basa en el etiquetamiento de los paquetes sobre la base de los criterios de prioridad y claridad, en función de las etiquetas añadidas, lo cual reduce significativamente el procesamiento de los paquetes cada vez que el mismo ingresa a un enrutador en la red. Adicional a esto, MPLS es soportado sobre diversos protocolos de la capa de enlace como lo son: ATM, FRAME RELAY.

Entre sus principales características se encuentran:

- Mantiene circuitos cerrados
- Redes Privadas virtuales
- Mecanismo de protección anti fallos
- En ATM y *Frame Relay* la etiqueta MPLS ocupa el lugar del campo VPI/VCI o en el DLCI, para aprovechar el mecanismo de conmutación inherente

En una red IP tradicional, cada *router* utiliza instrucciones de búsqueda de enrutamiento, y basado en estas, el dispositivo decide hacia donde enviar los paquetes. MPLS ayuda a reducir el número de operaciones de búsqueda del enrutador, con la alternativa de cambiar el criterio de envío. Esta capacidad elimina la necesidad de utilizar un protocolo de enrutamiento especial en cada uno de los dispositivos que conforman la red.

MPLS es un mecanismo de conmutación y asignación de etiquetas, el cual usa los diferentes dispositivos de la red que implementan MPLS, por medio de ellos se permite una asignación de etiquetas de acuerdo al conocimiento de las diferentes redes mediante la estrategia de adyacencia. Estas etiquetas permiten distinguir el destino, el paquete y que ruta debe seguir. El envío dentro de la red de MPLS se basa exclusivamente en etiquetas, esto permite un envío ágil.

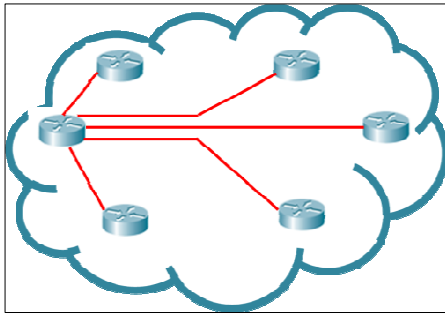


Figura 1 Malla Parcial

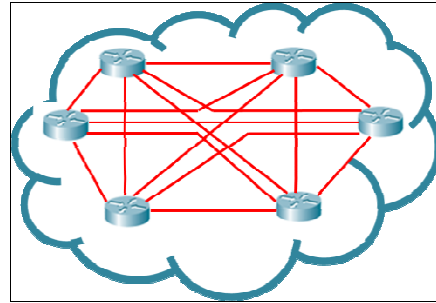


Figura 2 Malla Completa

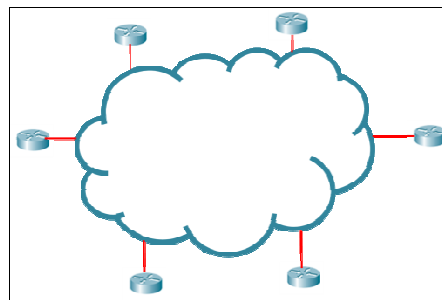


Figura 3 MPLS

En las imágenes que aparecen anteriormente, se presenta las topologías actuales (Topología Malla, Malla Parcial, MPLS). Como se puede apreciar, MPLS es un sistema más económico y proporciona enrutamiento óptimo entre los clientes, ya que solamente requiere la conexión entre el proveedor de servicio y la red MPLS.

**Topología de malla:** al igual que MPLS, proporciona un direccionamiento óptimo o entre los clientes debido a que tiene una conexión dedicada entre cada *router*, sin embargo esto resulta muy costoso ya que tendrían que existir tantos enlaces dedicados como *routers*.

**Topología malla parcial:** es una solución menos costos debido a que todos los *routers* están enlazados con un punto central en la red, esto representa un riesgo ya que dado el caso en que el *router* central falle toda la red colapsaría, otro inconveniente es que no permite un direccionamiento óptimo, al tener que pasar todos los todos los paquetes por el *router* principal, ocasionando un mayor retardo en la red.

Los dispositivos Cisco permiten tres mecanismos de conmutación

**Conmutación de procesos:** realiza una búsqueda completa en la tabla de enrutamiento del dispositivo por de cada paquete, agregando retardo en la transmisión de los datos.

**Conmutación rápida:** al recibirse el primer paquete se realiza la conmutación de procesos, la ruta se almacena en cache para que en los siguiente paquetes sigan la misma ruta.

**CEF (Cisco Express Forwarding)** permite un direccionamiento más ágil ya que se basa en los prefijos de destino, para ello utiliza dos tablas, la primera es la FIB (*Forwarding Information Base*) la cual mantiene una copia de la tabla de enrutamiento basada en IP. A través de esta tabla el *router* puede tomar la decisión del encaminamiento del paquete. Dado

el caso en el que la dirección IP no se encuentre en la FIB, el paquete es descartado.

La segunda tabla es la de adyacencia, la cual suministra una copia de la ARP de cache, donde no solo se almacena la MAC sino también el encabezado de la capa 2.

#### **4.2. Arquitectura MPLS**

Para soportar múltiples protocolo MPLS divide la arquitectura básica del *router* en dos componentes

##### ***Plano de control:***

Es el encargado del intercambio de etiquetas por medio de protocolos como LDP y RSVP, también se encarga del intercambio de información de enrutamiento para los protocolos de capa tres como son: OSPF o RIP.

##### ***Plano de datos***

Está encargado del envío de paquetes basados en las etiquetas, por medio del protocolo establecido, o de cualquier red establecida en la tabla de enrutamiento del dispositivo.

MPLS se encuentra definido en el RCF3031, de enero de 2001

En una red MPLS los dispositivos se identifican de acuerdo a su función. En el núcleo de una red que implementa MPLS se encuentran los LSRs, y en los bordes de la misma encontramos los LERs. Hay que especificar que estos nombres son una denominación de su función, más no significa que sean elementos de red diferentes a los que ya se encuentra en una red de conmutación de paquetes basada en IP

- **LSR (*Label Switching Router*)** Es el encargado de la conmutación de los paquetes, LSR se divide dos tipos, el LSR de núcleo y el LSR de borde, denominado también como un LER (*Label Edge Router*).

El LSR del núcleo se encuentra en el backbone de una red, donde se encuentran los enrutadores encargados de distribuir el tráfico. Cuando los paquetes llegan a este dispositivo, se analiza la etiqueta de llega, y según el análisis hecho en el router, se reenvía por la interfaz establecida.

El LSR de borde, como su nombre lo indica, se ubica a los bordes de una red MPLS y de acuerdo a esta cumplen una función

diferente. Un LSR de egreso es aquel que se ubica en la salida de la red MPLS y permite la interconexión con la red IP convencional. Este router se dedica a remover las etiquetas MPLS para re direccionar el paquete utilizando los protocolo de capa 3. El LSR de Ingreso hace la función opuesta del LSR, de egreso y se ubica al final de la red IP y al inicio de la red MPLS. Su principal función es recibir los paquetes IP que llegan, basados en la red de destino para designar una etiqueta que represente el destino. Esta clase de configuración permite que en el backbones solo realice el intercambio de etiquetas, por lo cual no se usa enrutamiento basado en capa 3. Solo cuando el paquete esté llegando a su destino, se realice la última revisión para el cambio a IP. Esta operación ocurre en el *router* de egreso o en el penúltimo *router* (si se usa la metodología PHP).

Como resultado, MPLS no solamente simplifica el proceso de envío de paquetes, sino también acelera la transferencia de los datos.

En las siguientes gráficas podemos apreciar más claramente las tareas de las cuales están encargados los LSRs.

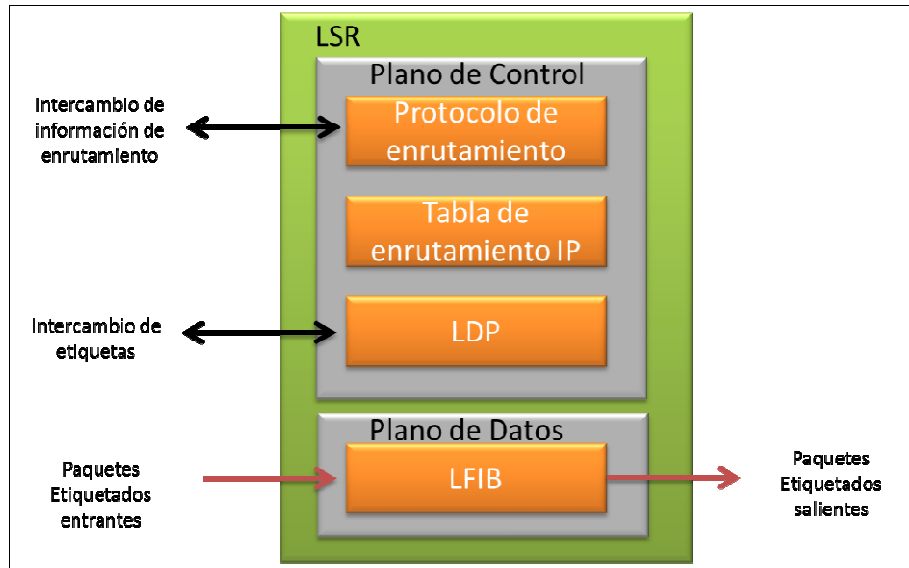


Figura 4 Componente de Arquitectura de una LSR

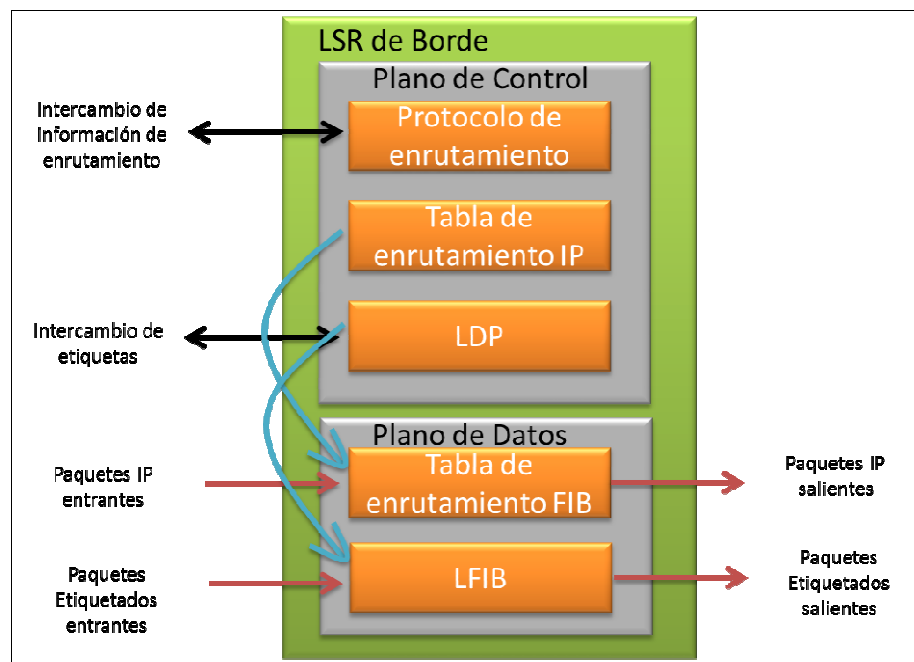


Figura 5 Componente de Arquitectura de un LSR de Borde

En comparación con la arquitectura del LSR del borde se observa que realiza más operaciones ya que se encarga de realizar el

cambio de IP a etiquetas de MPLS y viceversa dependiendo si es de ingreso o egreso respectivamente.

- **LSP (*Label Switching Path*)** A diferencia del enrutamiento de saltos de *router* a *router*, MPLS arma un camino por el cual envía sus paquetes, conocido como un LSP (Intercambio de Rutas por Etiquetas).

Un LSP debe ser establecido antes de que MPLS pueda enviar paquetes en un FEC, también se debe tener en cuenta que el camino LSP es unidireccional, es decir un paquete que sale de A a B, utiliza un camino LSP1, para que un paquete que viaja de B a A, tiene que utilizar un LSP diferente en este caso LSP2, de esta forma MPLS convierte redes no conectadas de IP a redes orientadas a conexión.

Durante todo el proceso de envío de paquetes, MPLS divide las tareas, en tres tipos de *routers* llamados LSR (*Label Switching Router*), un LSR de núcleo que se encarga de revisar las etiquetas y reemplazarlas según las una tabla de etiquetas, un LSR de ingreso que recibe el paquete IP, y le adiciona una etiqueta según el destino, y por ultimo un LSR de egreso, que es el encargado de quitar la etiqueta y enrutar según la IP.

- **LDP (*Label Distribution Protocol*)** Protocolo para la distribución de etiquetas MPLS Entre dos equipos de red.

- **FEC (*Forwarding Equivalence Classes*)** es un grupo de paquetes IP que son enviados por el mismo camino con el mismo tratamiento de la red. Cada FEC posee una ruta determinada a seguir en una red MPLS. La asignación de paquetes a una FEC, es basado solamente en subred de destino, derivado de la Cabecera de un paquete IP, en el caso de MPLS aparte de la información de cabecera del paquetes, el asignamiento de una FEC puede ser influenciado por otros criterios de calificación como lo son: combinación de la red origen y destino, identificador VLAN, identificador VPN, QoS, entre otros.
- **LFIB (*Label Forwarding Instance Base*)** Es la tabla de conmutación utilizada por enrutadores para el envío y recepción de los paquetes.

#### **4.3. OPERACIONES BASICAS DE ETIQUETAS**

En los LSR´s se pueden llevar a cabo diferentes operaciones: PUSH, POP y SWAP

**PUSH:** Es la función que realiza el router para agregar una nueva etiqueta a la pila de etiquetas MPLS, ya sea sobre un paquete IP o sobre otra etiqueta de la pila.

**SWAP:** Es la operación que realiza el router para intercambio de etiquetas según la tablas de etiquetas, es decir que remueve la etiqueta con que llega al router y se agrega la nueva etiqueta para el envío.

**POP:** Es la operación que realiza el router para remover la etiqueta del nivel superior de la pila. Si este proceso ocurre en el router de egreso significa que ha salido de la red MPLS a una red IP.

A continuación se presenta una imagen en cual se ilustran los tres diferentes operaciones

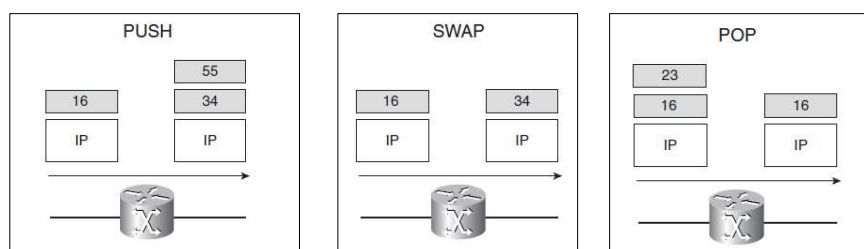


Figura 6 Funciones PUSH SWAP y POP

#### 4.4. Direccionamiento MPLS

Cuando un paquete IP llega al LSR de ingreso de una red MPLS, este examina el paquete para verificar la red de destino, posteriormente se examina la tabla LFIB (Label Forwarding Information Base), buscando una etiqueta para dicha red. Si existe una etiqueta, al paquete se le agrega dicha etiqueta. Tomando como referencia el modelo OSI, esta

etiqueta se ubica entre la capa 2 y capa 3. Una vez establecida la etiqueta el paquete se re-envía por la interfaz correspondiente al siguiente salto. Una vez el paquete haya ingresado a la red MPLS, se realiza el intercambio de etiquetas en cada salto, teniendo en cuenta que siempre se examina la tabla LFIB para saber qué operación realizar con la etiqueta recibida y hacia donde se debe re direccionar. Al llegar al router de egreso las etiquetas son removidas y el paquete se re direcciona utilizando la tabla de enrutamiento del router.

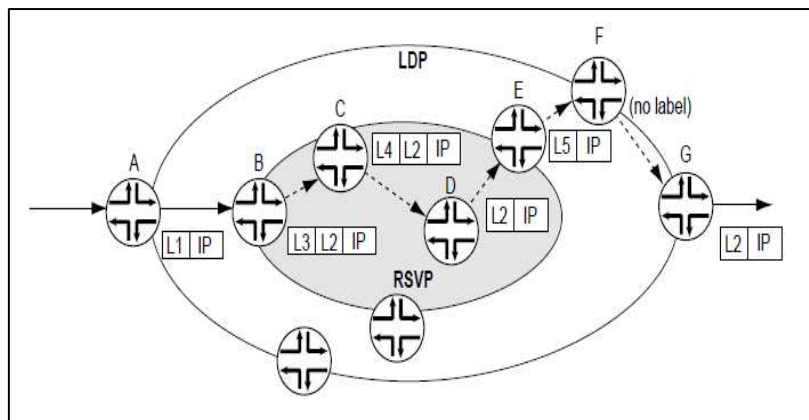


Figura 7 Enrutamiento En Una Red MPLS

En la gráfica anterior se resume el proceso de redireccionamiento de un paquete, desde el ingreso hasta el egreso de la red MPLS. Como se puede apreciar, en el *router* de ingreso se establece la etiqueta delante de la cabecera IP del mismo. Al viajar dentro de la red MPLS, se hace las operaciones respectivas de remoción, intercambio y superposición de etiquetas (*POP*, *SWAP* y *PUSH*). Al llegar al *router* de egreso de la red, las

etiquetas que se contengan en el paquete, son removidas, y el mismo es re-direccionando fuera de la red MPLS hacia una red basada en IP.

#### 4.5. Formato Etiqueta MPLS

La etiqueta MPLS se encuentra conformada por 32 Bits, divididos de la siguiente manera:

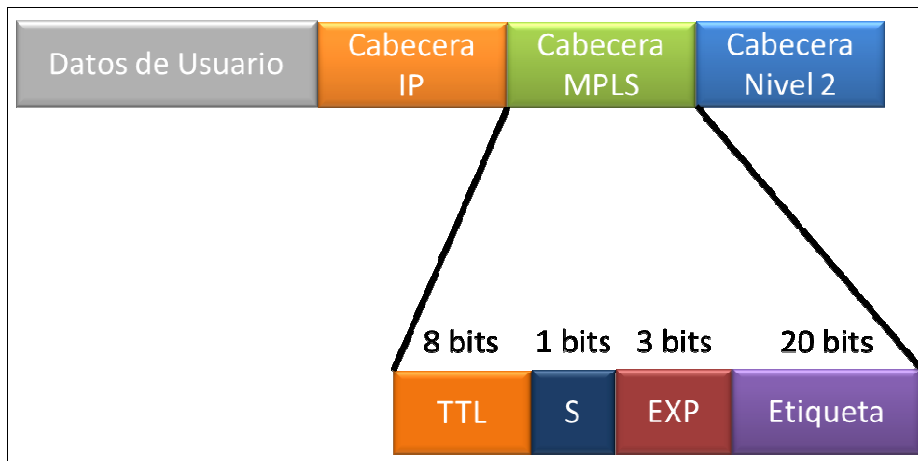


Figura 8 Estructura de la Cabecera MPLS

- El valor de la etiqueta tiene un tamaño de 20 bits. Este valor puede variar entre 0 y 1048575, teniendo en cuenta que los primeros 16 valores son reservados.
- Exp: tiene un tamaño de 3 bits y es para uso experimental. Estos bits son usados únicamente para calidad de servicio QoS

- S: es el bit de posición de la pila.
  - Cuando es 1 indica que es la entrada más antigua en la pila
  - Cuando es 0 indica cualquier otra entradas

La pila es la colección de etiquetas que se encuentran encima de los paquetes. La cantidad de etiquetas que pueden encontrarse en una pila van desde 1 hasta N, aunque lo más común es encontrar pilas de 4 o más etiquetas.

- TTL son los últimos 8 bits del paquete y se utiliza para codificar el valor de conteo de saltos o tiempo de vida

Como se comentó anteriormente las primeras 16 etiquetas no se estableces para el direccionamiento ya que cumplen una función diferente. Los valores reservados para el campo de la etiqueta que se añade al paquete, son nombrados a continuación.

- Label = 0, paquete descende de una red IPv4
- Label = 2, paquete descende de una red IPv6
- Label 4 – 15, reservado para uso futuro por la agencia de asignación de números de internet (IANA)

TTL es el acrónimo en inglés de Time To Live, que representa un mecanismo altamente usado en las redes IP. Este indica el tiempo de vida de un paquete en una red antes de ser desechado. El TTL tiene un tamaño de 8 bits, y un valor inicial de 255, el cual va decreciendo de uno en uno por cada salto en la red, si el valor TTL llega a cero, el datagrama

se desecha y se envía un mensaje de error al emisor del paquete a través del protocolo ICMP, advirtiéndole al emisor que no se encontró el dispositivo destino.

Al igual que en una red basada en IP, en MPLS las etiquetas cuentan con una campo TTL el cual funciona de la misma manera. Cada vez que se realice un salto el valor del TTL disminuye en uno (1). Existen dos escenarios en el cual se puede analizar el comportamiento del campo TTL:

Escenario uno: de IP a etiqueta o etiqueta a IP (ingreso y egreso de la red)

Escenario dos: de etiqueta a etiqueta (Núcleo de la red MPLS).

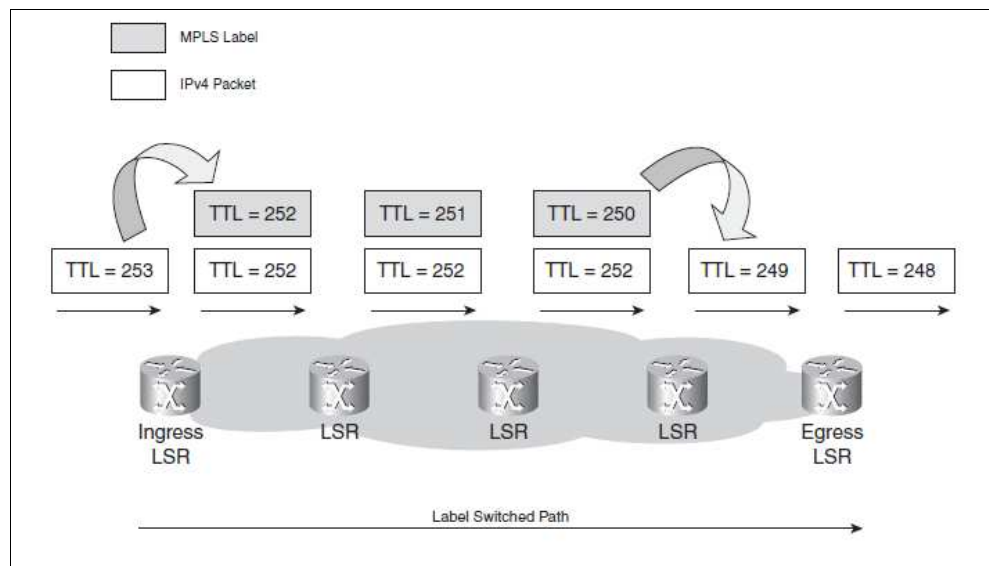


Figura 9 Ejemplo TTL Escenario Uno

**ESCENARIO UNO:** Al llegar un paquete al router de Ingreso de una red MPLS, se copia el TTL del mismo en el TTL de la etiqueta, a medida que la información pasa por la red, el TTL de la etiqueta va disminuyendo de uno en uno dependiendo de la cantidad de salto que tenga que realizar. Durante este proceso el TTL del paquete IP no es modificado. Al llegar al router de egreso de la red MPLS, el TTL de la última etiqueta disminuye uno por el salto y este es copiado en el TTL del paquete IP. Este comportamiento lo podemos apreciar en la gráfica anterior donde se aprecia el proceso de etiquetamiento en los diferentes routers

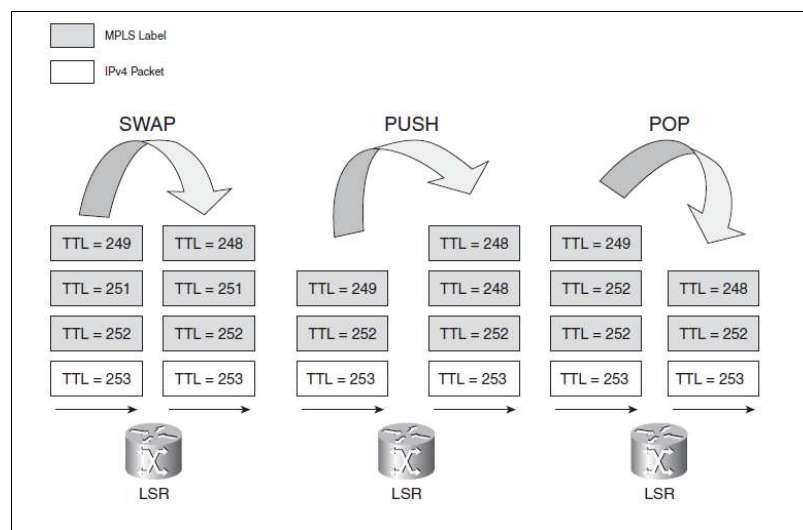


Figura 10 Ejemplo TTL Escenario Dos

**ESCENARIO DOS:** El intercambio de etiquetas se puede contemplar ampliamente en el núcleo de la red MPLS, que es donde podemos ver su comportamiento. Es decir se trabaja tan solo en las etiquetas de MPLS utilizando las funciones SWAP PUSH Y POP. Al utilizar la función SWAP el

campo TTL de la etiqueta disminuye en uno en cada salto, de la misma manera como funciona en IP, realizando la copia del TTL a la etiqueta que se intercambia con la anterior. Si la función que ocurre es un PUSH de una o más etiquetas, el valor del TTL -1 es copiado a la nueva etiqueta (similar al proceso de ingreso a la red MPLS). Si la función es POP el TTL de la etiqueta removida -1 es copia a la siguiente etiqueta de la pila (similar al proceso de egreso de una red MPLS). En la gráfica anterior podemos apreciar con mayor claridad las funciones POP SWAP Y PUSH

En una red basada en IP cuando el campo TTL de un paquete llega a cero, este es desechado y se envía por medio de ICMP un mensaje de tiempo expirado al origen de la transmisión. En una red basada en MPLS cuando un router recibe una etiqueta que en el campo TTL tiene un valor en uno (1), el datagrama es desechado y se envía un mensaje ICMP de tiempo excedido, el cual debe llegar hasta el final del camino LSP y devolverse por otro camino LSP a su origen con un mensaje de tiempo excedido. El motivo por el cual el paquete llega a su destino y de ahí devuelve es debido a que:

1. El LSP es unidireccional
2. MPLS no modifica la cabecera de los paquetes IP.
3. Tanto el router donde ocurre el evento, como los adyacentes, desconocen el origen del datagrama.

A continuación se presenta una gráfica explicativa

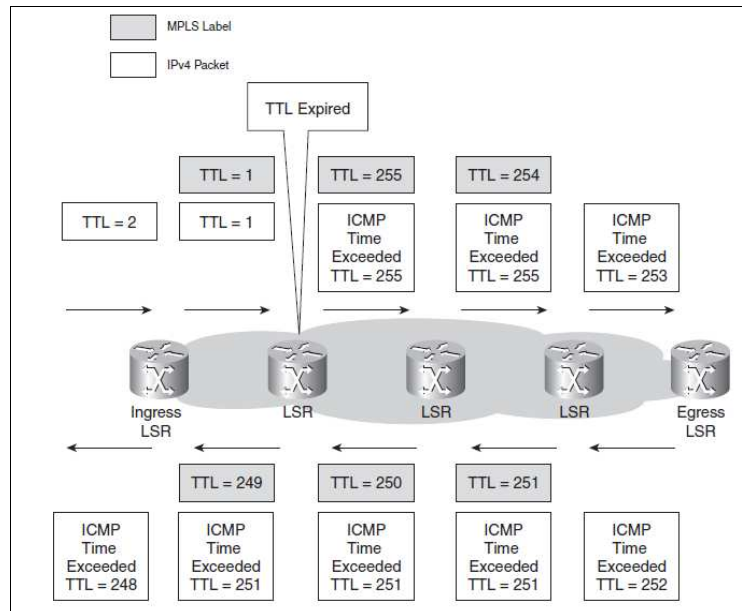


Figura 11 TTL Expirado

#### 4.6. TIPOS DE ENRUTAMIENTO

MPLS maneja tres estrategias para la selección rutas a tomar por los LSP dentro de un FEC específico:

1. **Enrutamiento Salto a Salto:** cada LSR elige el siguiente salto para cada FEC, sin tener en cuenta los demás LSRs, en esta alternativa se utiliza OSPF, infortunadamente no suministra ingeniería de tráfico ni políticas de ruteo para el manejo QoS.
2. **Enrutamiento explícito:** el LSR de entrada define varios o todos los LSRs por los que van a pasar el LSP, dentro de un FEC explícito. Cuando el LER define todos los LSRs se cumple completamente el ruteo explícito si solo se definen algunos, el

ruteo explícito es parcial. Esto no implica que no se pueda contar con todas las características y prestaciones de MPLS. De igual manera las ruta explícitas se definir anticipadamente o dinámicamente. Si se decide adopta dinámicamente se mejora la eficacia. Para que sea funcional el LER debe poseer información de la topología de la red y de los requisitos de QoS del dominio.

3. **Enrutamiento Mediante Algoritmo:** se encuentra basado en restricciones, donde se tienen en cuenta los requisitos del flujo de diversos paquetes y recursos disponibles en cada salto y en diferentes nodos.

#### **4.7. DISTRIBUCIÓN DE ETIQUETAS Y ADMINISTRACIÓN**

Para realizar la distribución de las etiquetas es necesario conocer la red desde el inicio hasta el final; este procedimiento requiere de un protocolo de enrutamiento previamente establecido.

Un LSP debe estar asociado a un FEC específico para poder enviar un paquete, para ello se emplea la técnica de conocimiento del vecino.

El etiquetamiento se efectúa desde el router de egreso al router de ingreso y los paquetes se envían desde el router de ingreso hasta el router de egreso.

#### **4.7.1. PROTOCOLO DE DISTRIBUCIÓN DE ETIQUETAS**

El protocolo de distribución permite establecer la comunicación de los FEC a las etiquetas y comentar a los SLRs a los Vecinos, esto con el fin de establecer el LSP de ingreso al destino.

El MPLS soporta diferentes protocolos como son: RSVP-T y LDP.

**RSVP-TE:** Es una extensión del protocolo RSVP, el cual fue concebido para realizar la distribución de las etiquetas. RSVP soporta la asignación de ruta explícitas con o sin reserva de recursos, también permite el re-enrutamientos de los túneles LSP, para soportar los inconvenientes frente a caídas de red, congestiones y cuellos de botella.

**LDP:** El protocolo LDP mantiene MPLS en correlación, entre las etiquetas y las relaciones que puedan tener con los FECs en la red.

Para llevar los paquetes a través de un LSP en una red MPLS, los LSRs deben correr un protocolo de distribución de etiquetas e intercambiar sus asociaciones. LDP es usado en conjunto con los protocolos de enrutamiento de capa de red, para distribuir la información de las etiquetas entre los LSR; también permite a un LSR distribuir sus etiquetas usando el puerto TCP 646, se asegura un envío confiable de la información de las etiquetas gracias a las características de este protocolo de la capa de transporte.

LDP tiene cuatro funciones principales:

**Descubrimiento de LSRs** que tiene activado el LDP, los LSRs que tiene activado LDP envían mensajes de HELLO en todos enlaces donde se encuentra activado el protocolo, los mensajes HELLO son mensajes UDP que son enviados a la dirección IP de multicast 224.0.0.2, usando el puerto 646.

El LSR que recibe los mensajes UDP de la interface, se encuentra alerta ante la presencia de routers adyacentes que estén usando LDP, de esta forma se podría establecer una sesión y hacer el intercambio respectivo de etiquetas. El mensaje HELLO tiene un tiempo de espera; si ningún mensaje es recibido antes que el tiempo expire, el LSR remueve el otro LSR de la lista de vecinos (LDP descubiertos). Si el LSR1 recibe un mensaje HELLO del LSR2 se crea una adyacencia entre los dos LSRs que tengan LDP activo.

El tiempo de espera del HELLO es de 15 segundos y el intervalo de envío es de 5 segundos, de igual manera estos valores pueden ser modificados, teniendo presente de que los mismos no sean tan pequeños como para que se caiga la conexión, ni tan grandes y ocasione que la conexión se mantenga activa por demasiado tiempo, afectando el direccionamiento.

**Sesión y Mantenimiento:** Si dos LSRs se descubre mediante mensajes HELLO, los LSRs intentan crear una sesión entre los dos mediante el protocolo TCP utilizando el puerto 646.

Después de que la sesión es estable, se mantiene ya sea por los paquetes que se reciben o por los mensajes periódicos KEEPALIVE. Cada vez que el vecino recibe un paquete LDP o un mensaje KEEPALIVE el temporizador de KEEPALIVE es reseteado para el vecino (los mensajes KEEPALIVE y de sesión también son parametrizables). En la imagen que aparece a continuación se presenta un mensaje KEEPALIVE de la captura realizada en el laboratorio

c2:0b:1c:00:00:01	CDP/VTP/DTP/PAGP/UDL/CDP	342 Device ID: R5 Port ID: FastEthernet0/1
172.16.6.1	172.16.5.1	LDP 72 Keep Alive Message
172.16.5.1	172.16.6.1	TCP 60 ldp > 56790 [ACK] Seq=378 Ack=402 win=3727 Len=0
172.16.15.2	224.0.0.10	EIGRP 74 Hello
172.16.5.1	172.16.6.1	LDP 72 Keep Alive Message
172.16.6.1	172.16.5.1	TCP 60 56790 > ldp [ACK] Seq=402 Ack=396 win=3733 Len=0

Label Distribution Protocol

- Version: 1
- PDU Length: 14
- LSR ID: 172.16.6.1 (172.16.6.1)
- Label Space ID: 0
- Keep Alive Message
  - 0... .. = u bit: unknown bit not set
  - Message Type: Keep Alive Message (0x201)
  - Message Length: 4

Figura 12 Keepalive

Existen cuatro tipos de mensajes que permiten el intercambio de información entre los diferentes LSR:

**Descubrimiento:** UDP envía mensajes HELLO multicast con el fin de aprender sobre los otros LSRs, posteriormente se establece una

conexión TCP y una sesión LDP con sus vecinos. Los LSR pueden establecer o solicitar asociaciones

**Adyacencia:** Los mensajes de adyacencia viajan usando el protocolo TCP y suministran los datos de inicio de sesión LDP. Este mantiene los temporizadores, rangos de etiquetas, entre los dos LSRs distintos. Keepalive envía mensajes periódicamente para mantener la sesión activa, ya que las sesiones se cierran si durante un periodo de tiempo predeterminado no se recibe un mensaje keepalive.

**Advertencia de etiquetas:** Los mensajes suministran la información sobre las asociaciones a los FEC y las etiquetas establecidas para cada uno. Se utilizan mensajes label mapping para distribuir esta asociación, de igual manera los mensajes labelwithdrawal, es cual tiene como finalidad deshacer el proceso de asociación. Los mensajes Label reléase tiene como objetivo liberar las etiquetas que ya no son requeridas después de haber sido realizada una asociación.

**Mensajes de notificación:** Estos mensajes suministran información de advertencia e información de errores entre los vecinos LSRs que tiene una sesión LDP entre ellos. Todos los mensajes LDP corren por TCP salvo Discovery que viaja por UDP

#### **4.7.2. CONTROL DE DISTRIBUCIÓN DE ETIQUETAS**

Para el control de distribución de etiquetas, MPLS plantea dos alternativas:

*Modo De Control Independiente:* En este modo de control cuando se identifica un FEC, el LSR decide si asocia una etiqueta a este FEC y la envía a sus vecinos. Dado el caso en que se reciba un paquete etiquetado pero que no tenga una etiqueta de salida para este paquete, automáticamente él pasa a Capa 3 en busca del destino y en el siguiente salto se decidirá si continúa en IP o si se etiqueta en MPLS.

*Modo Ordenado:* En este modo de control un LSRs solo asocia una etiqueta a un FEC si es el enrutador de egreso del FEC, o si fue recibida una asociación para ese FEC. De otra forma se debe solicitar una etiqueta al siguiente salto. Esto garantiza que el tráfico de un FEC específico continúe en una ruta particular, con un conjunto de atributos definidos, lo cual no se consigue con el modo de control independiente.

#### **4.8. RETENCIÓN DE ETIQUETAS**

Existen dos modos de retención de etiquetas:

*Modos De Retención De Conservación:* En este modo las etiquetas retenidas son guardadas si y solo si, se encuentran directamente conectadas con el router del siguiente salto. En el caso contrario en cual no se encuentran asociadas, la etiqueta es desechada y por consiguiente no es guardada. Si por alguna razón algún vecino que pertenece a un FEC en particular se convierte en el siguiente salto, tendría que solicitar nuevamente la etiqueta para ser guarda.

*Modo de retención Liberal:* En este modo un LSR retiene las etiquetas de todos los vecinos sin importa si pertenece o no a un FEC en particular; dado el caso en el que algún vecino se convierta en el siguiente salto no es necesario que se solicite la etiqueta, ya que él mismo la tiene almacena. Mientras un LSR en modo de retención de conservación tiene un tiempo un tiempo de convergencia más largo utiliza menos memoria al almacenar menos etiquetas lo cual es inversamente proporcional al modo de retención liberal.

#### **4.9. PHP**

PHP (*Penúltimate Hop Popping*) permite que el penúltimo LSR elimine la etiqueta, en lugar del router de egreso, lo cual agiliza los procesos del router de egreso para el cambio de la red MPLS a IP. Un ejemplo del funcionamiento de PHP cuando existe una etiqueta en la pila y si no se encuentra presente PHP, el router de egreso realiza una doble búsqueda, la primera en la tabla de etiquetas y la segunda en la tabla de IP. Para el caso cuando PHP se encuentra activo, se elimina la etiqueta en el

penúltimo router, lo cual disminuye la cantidad de búsquedas ha realizar router de egreso permitiendo al router de egreso que solo realice una busqueda en la tabla de IP.

#### **4.10. UBICACIÓN DE MPLS EN EL MODELO OSI**

La pila de etiquetas de MPLS, no se encuentra en la capa 2 (Enlace de datos) ni en la capa 3 (Red); se puede decir que MPLS conforma la capa 2.5 debido a que el esta se encuentra en medio de la capa 2 y 3.

La capa dos establece el formato de las tramas dependiendo de la tecnología (*HDLC, Ethernet y Frame Relay*) que se esté utilizando para la comunicación de los datos entre los dispositivos.

La capa tres está encargada de la conectividad y la selección de ruta que debe seguir un paquete para llegar a su destino aunque estos no tengan conexión directa Algunos protocolos encontrados en esta capa son IPv4, IPv6, OSPR, RIP, entre otros.

Mpls se encuentra en medio de las la capa dos y tres debido a que trabaja basado con diferentes tecnologías, sin importan el protocolo de capa 3 (*IP, IPX*) utilizado para el enrutamiento de paquetes,

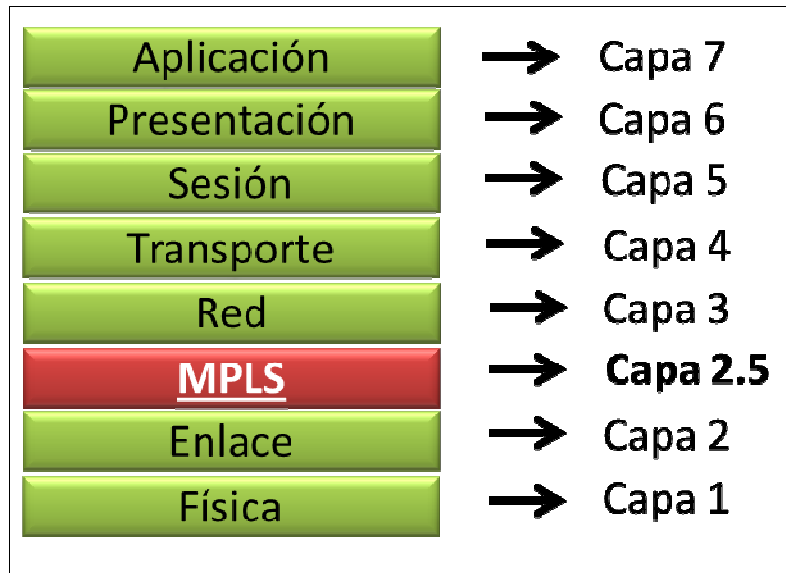


Figura 13 Ubicación MPLS En El Modelo OSI

#### **4.11. DISPOSITIVOS EN UNA RED MPLS**

En una red MPLS los enrutadores son denominados *Label Switch Router* (LSR), ellos son capaces de entender el tráfico MPLS, así como también realizar las operaciones de recepción y de reenvío de paquetes. En MPLS podemos encontrar tres tipos de LSRs categorizados según su funcionalidad: *Router* de Ingreso, *Router* de Egreso, y *Router* intermedio o de núcleo

**Router de Ingreso:** El *router* de ingreso es aquel que recibe un paquete de la red IP, lo etiqueta y lo envía al núcleo de la red MPLS

**Router de Núcleo:** El *router* de núcleo es el encargado de transportar los paquetes dentro de la red, utilizando la tabla de etiquetas MPLS.

**Router de Egreso:** El *router* de egreso es el encargado recibir los paquetes etiquetados, sustraer cualquier etiqueta MPLS que contenga, y enrutarlo a la red IP convencional.

#### **4.12. INGENIERA DE TRÁFICO**

La ingeniería de tráfico se basa en la optimización y la adaptación del flujo de tráfico y los recursos físico de la red. Al balancear cargas se busca que los recursos que se encuentren saturados o sobrecargados, disminuyan su carga al trasladar el trabajo a otros recursos que se encuentren libres o con baja carga.

El flujo de tráfico tiene la instrucción de seguir el camino más corto, el cual es dado por el algoritmo IGP. Cuando se presenta congestión de uno o varios enlaces, se añaden más enlaces, sin importar que no sea la ruta más corta. Esta operación se realiza de manera dinámica

La ingeniera de tráfico en MPLS permite establecer rutas detallando el camino de un LSP; además provee estadísticas de uso de LSP, el cual es muy útil a la hora de realizar planificaciones de la red, proyecciones futuras, análisis cargas de enlaces, entre otros.

Utilizando MPLS y configurando los anchos de bandas de cada enlace, se pueden establecer túneles entre el origen y destino para los enlaces que manejen grandes volúmenes de datos. Para establecer los túneles, se realiza mediante RSVP, el cual envía mensajes PATH que viajan de salto a salto, estableciendo las reservas de ancho de banda. En cada salto por donde viaja el mensaje, se almacena el estado del túnel. Después de que el mensaje PATH llega a su destino, se realiza un control para

determinar si se cumple con los requisitos de ancho de banda, si el enlace supera los requerimientos de ancho de banda, el ancho de banda requerido se reserva, se coloca una etiqueta de mensaje de reservado, y se envía al origen con la etiqueta. En cada salto se realiza la misma verificación y reservación.

Existen diferentes alternativas de mapear un túnel, ya sea a través de un enrutamiento estático, dinámico, o por póliza.

**Enrutamiento estático:** Este enrutamiento se presenta cuando se establece previamente una ruta entre el origen y el destino, el cual es definido por el administrador de la red.

**Enrutamiento dinámico:** Se crea cuando un *router* aprende una dirección de una red ubicada en otro *router*, por medio de un protocolo de enrutamiento establecido entre los dispositivos. El *router* aprende por cual enlace tiene que enviar los paquetes para que lleguen a la red destino y la métrica establecida por el protocolo.

**Enrutamiento por pólizas:** Este ocurre dependiendo de la priorización del tráfico, definiendo el uso del túnel. Por ejemplo si el tráfico de voz pasa por un enlace, se puede enrutar por un túnel previamente establecido.

Entre los beneficios de la ingeniería de tráfico se destacan:

- Optimiza el ruteo de tráfico IP
- Utiliza la ruta más corta que cumpla con las especificaciones ancho de banda, medio y prioridad
- Permite el análisis de los enlaces así como también la escalabilidad de la red.
- Permite una mejor QoS
- permite establecer rutas detalladas al camino exacto de un LSP.

#### **4.13. SECUENCIA DE CONFORMACIÓN DE UN TÚNEL**

Para la conformación de un túnel, es necesario contar con un conjunto de pasos los cuales se describen a continuación:

1. Se establece una ruta desde el origen hasta el fin por medio del protocolo de interior IGP, tal como lo es OSPF o ISIS.
2. El administrador define los anchos de banda disponibles y activa la opción de ingeniería de tráfico MPLS.
3. Al habilitarse la ingeniería de tráfico, se activa el envío de la información de las características del enlace en la red, incluyendo el ancho de banda disponible configurado por el administrador.

4. El administrador configura el ancho de banda, inicio, destino y tiene la opción para establecer la forma para encontrar el camino hacia el destino, este puede ser: explícito o dinámica (El camino explícito es definido por el administrador, mientras el dinámico se define tan solo el destino y la ruta es establecida de salto a salto).
5. Se envía un PATH al siguiente salto, en el cual se incluye el camino, ya sea explícito o dinámico
6. Los router de núcleo almacenan la información del Id del túnel y ancho de banda y pasan el mensaje PATH al siguiente salto, hasta llegar a su destino.
7. Una vez cuando el mensaje PATH llega a la red destino, el *router* acepta el túnel, si cumple los requisitos de ancho de banda solicitados. El *router* destino envía un mensaje con una etiqueta de reservado al origen.
8. El mensaje reservado es devuelto por todo el camino, en cada salto se realiza un control de admisión, para revisar si el enlace tiene el ancho de banda solicitado. Si se presenta un inconveniente con el control de admisión se envía un mensaje de error al destino y otro al origen; por consiguiente el túnel no se establece. Si el mensaje de control

9. Es aceptado, se establece una etiqueta y se envía un mensaje de reservado al origen.
10. Cuando el mensaje de reservado llega al inicio, se proyectan las etiquetas quedando establecida la configuración del túnel.
11. El administrador debe definir diferentes tipos de tráfico que pasaran por este túnel
12. Una vez completado el paso 10, el tráfico puede ser enviado por el túnel, adicionando la etiqueta para ser enviado.
13. El tráfico es re direccionado por los dispositivos que conforman el núcleo de la red MPLS, hasta llegar a la red destino.
14. En el último o penúltimo *router*, se elimina la etiqueta y se envía por la red basada en IP.

#### **4.14. CLASES DE SERVICIO**

Las etiquetas MPLS contiene el campo EXP con el fin de propagar la clase de servicio CoS en el LSP. Esto permite que MPLS soporte el transporte de diferentes clases de tráfico ya que el tráfico que pasa por un LSP determinado se puede asignar a diferentes colas de salidas en los distintos saltos o LSR.

En cada par de LSR exteriores (más conocidos como LSR de Ingreso/Egreso o LSR de Borde), se pueden provisionar múltiples LSPs, cada uno de ellos con diferentes prestaciones y garantías de ancho de banda.

## 5. PRÁCTICAS Y SIMULACIONES

En este capítulo se presentan las simulaciones realizadas, la práctica de laboratorio, y las imágenes del análisis de los mismos. Los análisis de estos datos se presentan de una manera muy gráfica lo cual permite desde el inicio una interpretación y comprensión casi intuitivas de los mismo, de igual manera las mismas cuentan con un explicación con un lenguaje adecuado y sencillo.

### **GNS3**

(2) Es un simulador gráfico de redes que permite la simulación de redes, dando la posibilidad de experimentar las características de: CISCO IOS, JUNOS, Juniper. Lo cual nos brinda la oportunidad de realizar configuraciones extensas con todas las características permitidas por las IOS, nada diferente a un ambiente real de trabajo.

#### *Generalidades*

- Diseños de alta calidad y topologías complejas
- Emulación de diferentes plataformas de *CISCO IOS Router, IPS, Cortafuegos PIX, ASA, Jun.*
- Simulación de *Ethernet* sencillas, ATM e Interruptores de *Frame Relay*.
- Conexión de cable de red simulada.
- Captura de tráfico en los enlaces usando el software *WireShark*.

## **Packet Tracer**

(3) Es una herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta permite crear topologías de red, configurar dispositivos, insertar paquetes y simular una red de múltiples representaciones visuales.

### *Generalidades*

- Entre sus principales funcionalidades se destacan
- Soportes para Windows (2000, Xp, Vista) Linux (Ubuntu y fedora)
- Permite configurar múltiples usuarios y colaborativas en tiempo real.
- Soporte Ipv6, OSPF multi área, redistribución de rutas, RSTP, SSH y Switchs multicapa
- Soporta los siguientes protocolos.
- HTTP, TCP/IP, TELNET, SSH, TFTP, DHCP y DNS
- TCP/UDP, IPV4, IPV6, ICMP4 e ICMP6
- RIP, EIGRP, OSPF multi área, enrutamiento estático, y redistribución de rutas
- Ethernet 802.3 y 802.11, HDLC, FRAME RELAY y PPP
- ARP, CDP, STP, STP, 802.1 q VTP Y DTP, Polly Mkt, VLAN'S Spanning tree Mike mtk etc.

## **Wireshark**

(4) Es un analizador de protocolos utilizado para realizar análisis y solución de problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación.

Cuenta con todas las características estándar de un analizador de protocolos.

Además permite examinar los datos sobre el tráfico de una red usando capturas en tiempo real o de un archivo de captura previamente guardado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos

## **OPENSIMMPLS**

Es una herramienta que nos permite simular de forma rápida y sencilla un escenario en la cual se puede ver el funcionamiento del protocolo MPLS. Por medio de este aplicativo, podemos hacer simulación de varios escenarios sin necesidad de conocer los comandos de configuración.

Una bondad de esta herramienta, es que nos permiten generar gráficos cuando una red funciona normalmente utilizando LDP y el inicio del envío de las etiquetas para transmitir paquetes entre los diferentes LSRs dentro del núcleo de la red MPLS.

Una utilidad que nos ofrece este aplicativo es la simulación de QoS, el cual nos permite priorizar el tráfico, dándole mayores privilegios en el

momento de direccionamiento de tráfico a uno o más servicios específicos, frente a los otros servicios soportados por la red.

A continuación se expondrán los diferentes elementos utilizados en el simulador al momento de hacer un montaje de un escenario MPLS.

**Emisor de tráfico:** Es el dispositivo que generara el tráfico. Este flujo constante de paquetes, permite ver como viajan los paquetes IP por la red y el momento cuando ingresan a la red MPLS, se les establece una etiqueta, viajan según los LSP predeterminados, y por ultimo llegan al *router* de egreso de la red MPLS y se vuelve a enviar usando IP en vez de las etiquetas. Para poder insertar un emisor, en primer lugar se tiene que agregar un receptor al escenario que estamos montando; de otra manera no podremos agregar el emisor, ya que al momento de agregar el emisor, el simulador nos obliga a escoger un receptor inmediatamente.

**Receptor:** Es el dispositivo al cual va dirigido todo el tráfico generado por el emisor; este receptor puede ser el destino de diferentes emisores.

**Label Edger Router:** (LER) Como su nombre lo indica es el *router* del borde ya sea el de entrada o de salida de la red MPLS. Este dispositivo marca el inicio y salida de la red MPLS, en este *router* se hace una

operación PUSH (en el *router* de Ingreso) o una operación POP (en el *router* de egreso).

**Label Edger Router Activo:** (LERA) Al igual que un LER, es un *router* de borde ya sea en la entrada o en la salida de la red MPLS. La diferencia consiste en que este dispositivo viene con la configuración para especificar los parámetros de QoS dentro de la red MPLS.

**Label Switch Router:** (LSR) Es el *router* encargado de re direccionar el tráfico MPLS dentro del núcleo de la red MPLS.

**Label Switch Router:** (LSRA) Al igual que el LSR, es un *router* dedicado a conmutar el tráfico dentro del núcleo de la red MPLS, la diferencia consiste en que este dispositivo viene con la configuración para especificar los parámetros de QoS dentro de la red MPLS.

**Link:** Es el enlace que existe entre los diferentes *routers*. Se especifica el origen y destino.

## 5.1. Práctica de Laboratorio

Para demostrar el funcionamiento de MPLS en una red normal se realiza una primera simulación en la cual utilizamos un emisor, un receptor, 2 LER y 4 LSR, los interconectamos entre sí como muestra la siguiente gráfica.

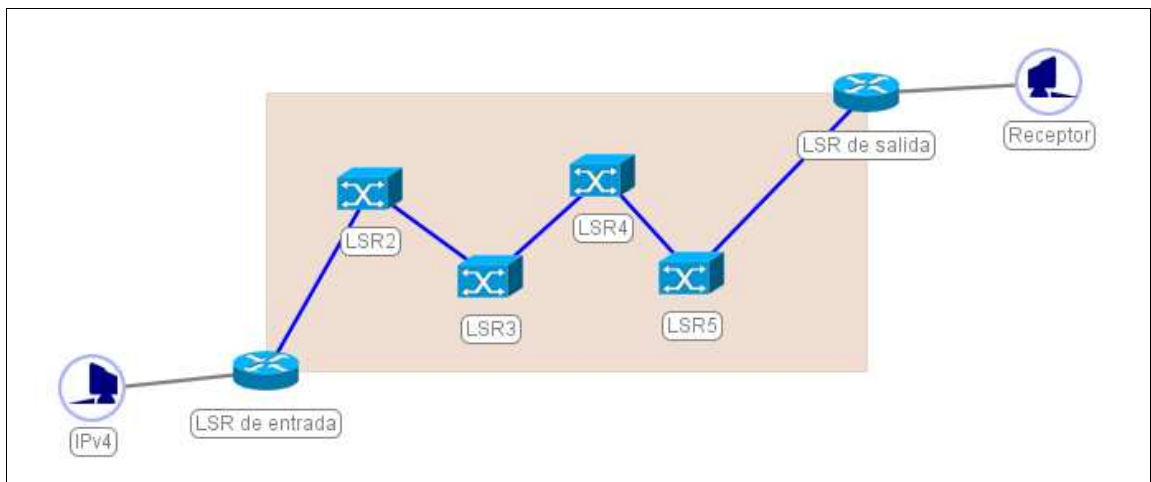


Figura 14 Simulación Red MPLS

Con el emisor generamos tráfico HTTP hacia el receptor. Con la simulación observamos cómo se establece el LSP, que es el camino que debe seguir el paquete MPLS para llegar a su destino. Posteriormente que se establece el LSP, se envía el tráfico MPLS con la etiqueta establecida (en el simulador no se puede apreciar la identificación de las etiquetas puesta sobre el paquete, solamente se puede identificar el tráfico IP normal del tráfico MPLS).

Al realizar una simulación con un enlace caído, podemos observar como LDP envía a los routers vecinos la información de la ruta fallida y como se detiene el tráfico. al volver a subir el enlace, se advierte de la nueva adyacencia a los demás routers, para que se vuelva a establecer el LSP y continua con el envío de tráfico a su destino.

### 5.1.1. Simulación QoS:

Se realizó una simulación de calidad de tráfico usando el software OpenSimMPLS, al igual que en la simulación anterior, primero se establece el LSP, y luego se inicia el envío de tráfico correspondiente. Para esta simulación se utilizaron dos generadores de tráfico, uno lo configuramos con calidad de servicio, y otro sin calidad de servicio. Después del establecimiento del LSP, se aprecia como el tráfico con QoS se prioriza sobre el tráfico sin QoS.

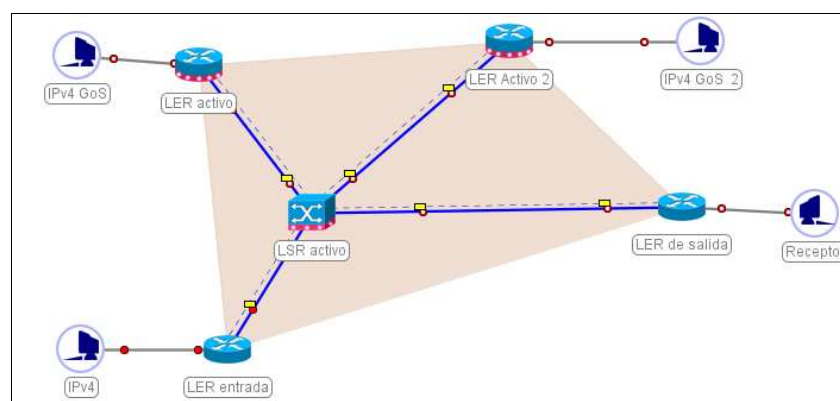


Figura 15 Simulación de red MPLS con QoS

A continuación se presenta el análisis gráfico de la simulación anterior.

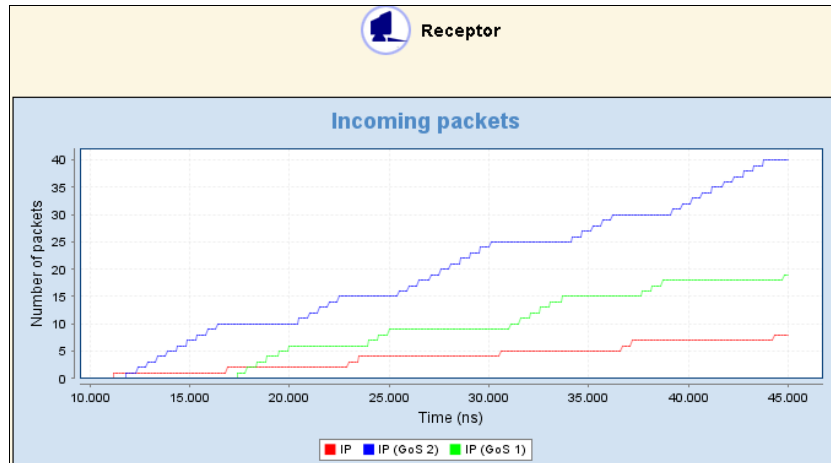


Figura 16 Resultado Simulación

En esta gráfica se puede apreciar el tráfico IP sin calidad de servicio de color rojo, y el color azul y verde representan la cantidad de paquetes IP con calidad de servicio. Además podemos apreciar que los paquetes recibidos que vienen con calidad de servicio están en mayor proporción que los paquetes sin calidad de servicio.

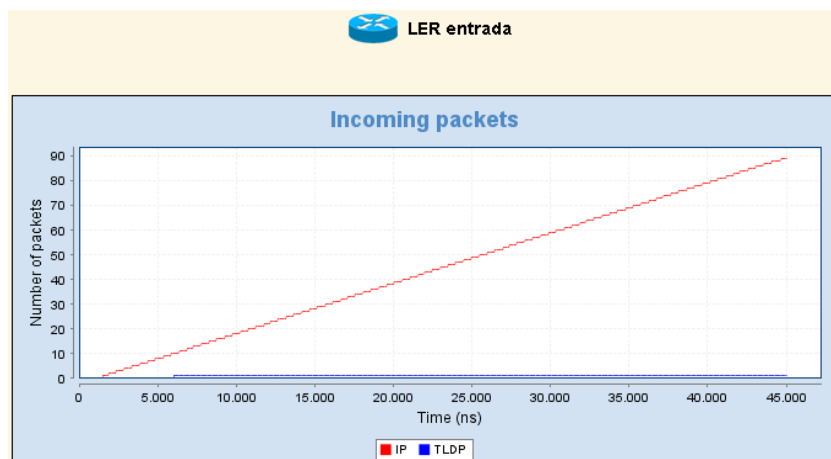


Figura 17 Resultado LSR de Entrada

En la gráfica anterior podemos apreciar el LSR de entrada el cual es el encargado de recibir los paquetes IP y le agrega la etiqueta MPLS para

reenvíalos por toda la red al LSR vecino. En la siguiente gráfica apreciamos el tráfico de salida de este router, es reenviado basado en las etiquetas MPLS.

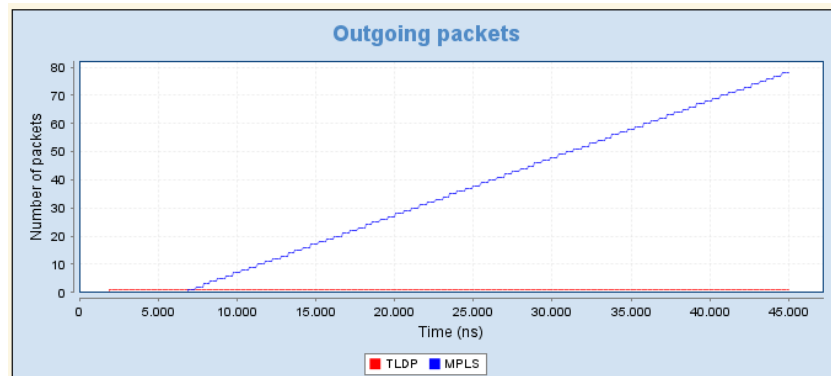


Figura 18 Paquetes de Salida de un LSR

De la misma manera MPLS permite implementar QoS para la priorización de tráfico, en este punto los LSR funcionan de igual manera con o sin calidad de servicio con respecto a la conmutación de paquetes. El administrador define en cada LSR la prioridad de tráfico (*Este tema fue abordado en un capítulo anterior*).

En la siguiente gráfica podemos apreciar el LSR de entrada el cual es el encargado de recibir los paquetes IP y le agrega la etiqueta MPLS para reenvíalos por toda la red al LSR vecino, con calidad de servicio.

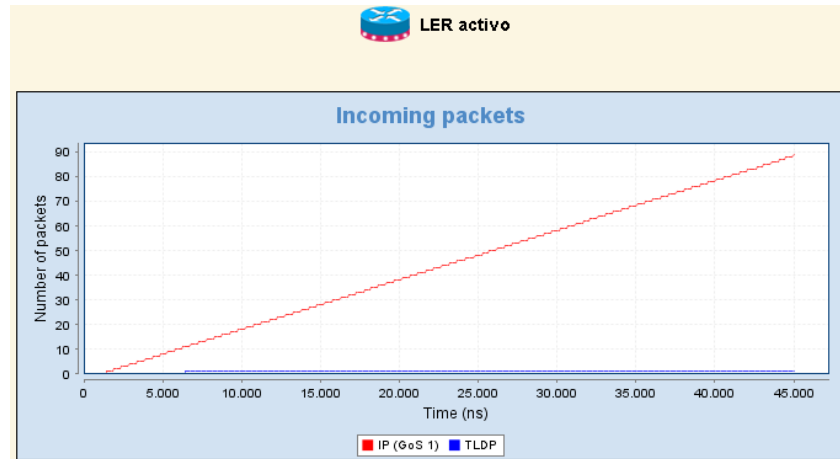


Figura 19 Paquetes de un LSR de Ingreso

Al igual que en las gráficas anteriores, este dispositivo es también un *LSR* de ingreso a la red MPLS, pero viene con la opción de Calidad de servicio activada. En los dos casos anteriores se aprecia que hay una demora inicial para el envío de los paquetes, ya que antes de enviarlos, los LSR deben aprender las etiquetas de los vecinos con el fin de saber la ruta (LSP) para llegar a su destino.

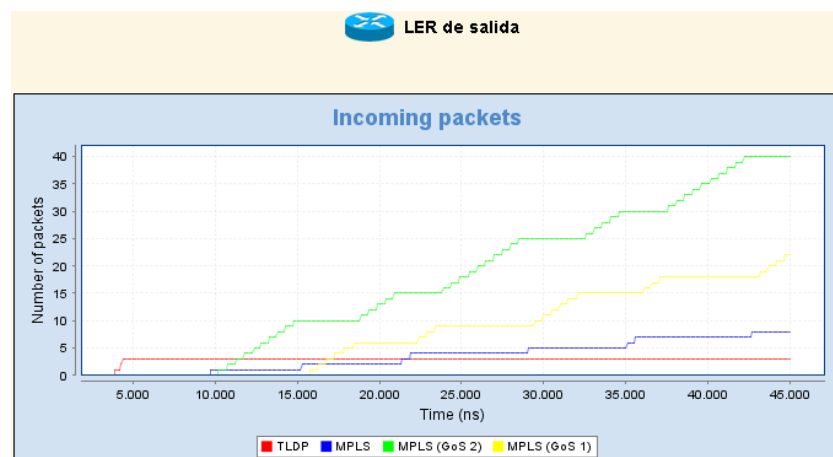


Figura 20 LSR de Salida o LER

Este dispositivo es un *LSR* de Egreso, el cual es el *router* que se encuentra al borde de la red MPLS e IP. Este a diferencia del LSR de

ingreso recibe el tráfico MPLS de la red, este le remueve las etiquetas que tenga y lo reenvía según la tabla de enrutamiento basada en IP. De la misma manera hay que entender que el servicio de QoS está activo en la red y como se puede apreciar en estas dos gráficas, este tráfico es priorizado ante el tráfico que no tiene QoS.

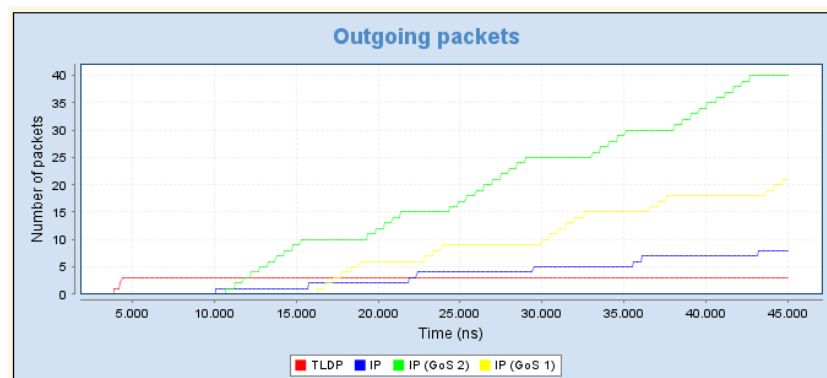


Figura 21 Trafico Priorizado

Este dispositivo es el *router* de egreso de la red MPLS, como se observa, el tráfico entrante de MPLS viene con priorización de tráfico, y sale al igual con la misma configuración de priorización de tráfico. De la misma forma se observa que la proporción de tráfico con Calidad de Servicio es mayor que el que viene son calidad de servicio activada.

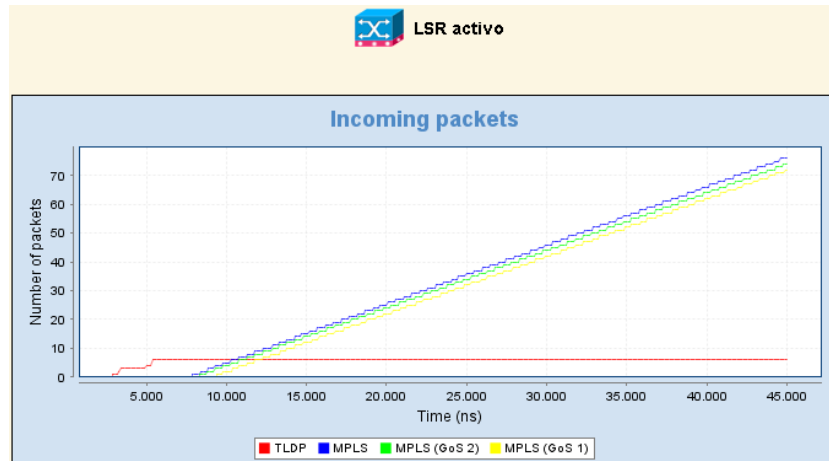


Figura 22 Trafico de Entrada LSR de Núcleo

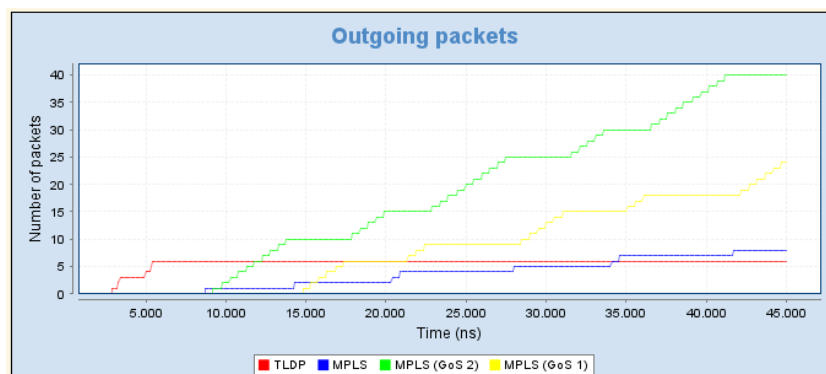


Figura 23 Trafico de Salida LSR de Núcleo

Por ultimo podemos ver en la gráfica de la topología que este router es un LSR perteneciente al núcleo de la red MPLS como vemos todo el tráfico llega a este router y de aquí es enviado a su destino específico. En la topología vemos que el tráfico llega de diferentes orígenes, pero van hacia el mismo destino pasando por este dispositivo, todos llegan al mismo tiempo al router pero debido a la priorización de tráfico por medio de la Calidad de Servicio, se envían más paquetes pertenecientes a un tipo de tráfico que a otro.

## 5.2. Laboratorio

En las instalaciones de las Unidades Tecnológicas de Santander se llevaron a cabo los laboratorios de esta monografía. En el siguiente gráfico podemos apreciar la topología implementada. Como podemos observar usamos un *switch* conectado entre cada enlace de *router* a *router*, en el *switch* configuramos un puerto para monitorear el tráfico que pasaba por el enlace usando un computador con el *sniffer Wireshark*.

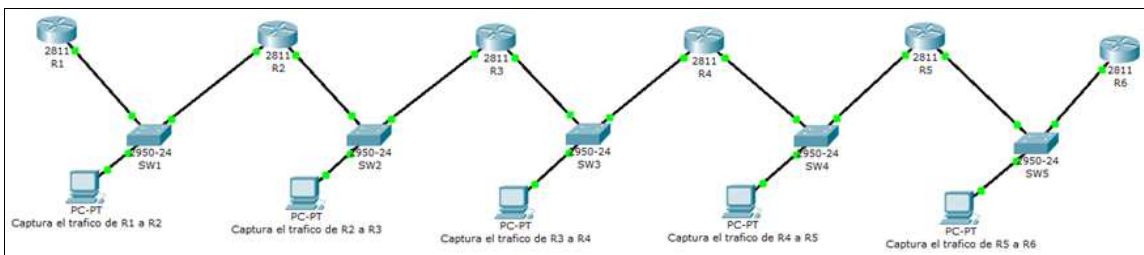


Figura 24 Topología de Laboratorio

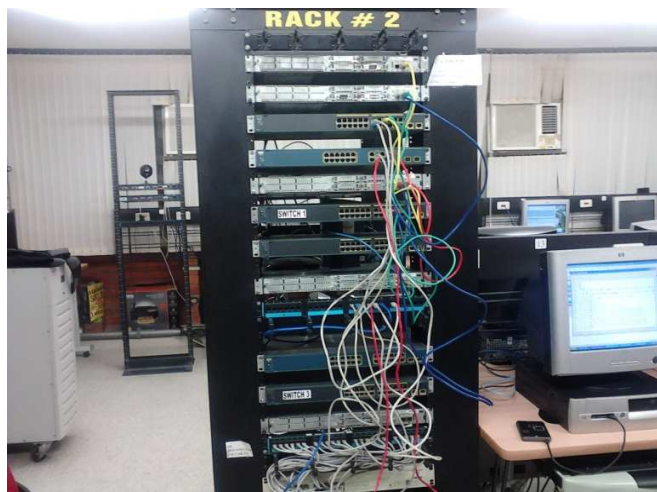


Figura 25 Interconexión de Dispositivos de Laboratorio

En estos Rack se puede apreciar los *Router* y *switchs* utilizados en el laboratorio. Como se comentó anteriormente, los *switchs* fueron usados para capturar todo el tráfico entrante y saliente de cada *router* de la red.

Las siguientes fotografías muestran los equipos de cómputo usados para capturar el tráfico, como se puede ver, se usó un equipo por cada enlace.



Figura 26 Interconexión De Dispositivos

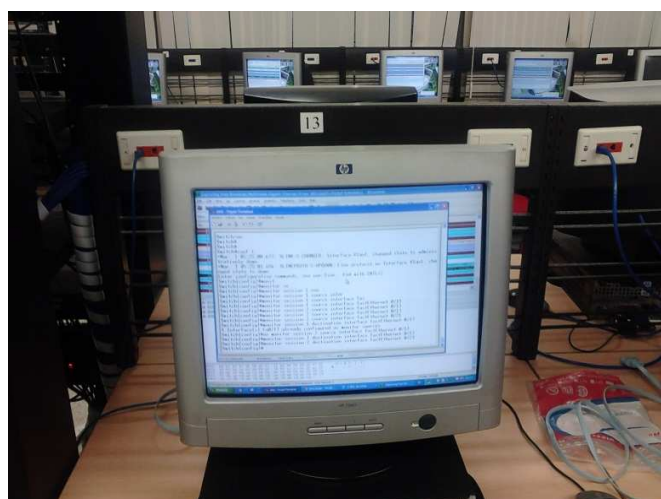


Figura 27 Configuración de Dispositivos

En la siguiente imagen se puede apreciar el momento cuando se está realizando la configuración de los dispositivos (*Routers* y *Switchs*). En cada *router* se realizó la captura mediante el *sniffer Wireshark*.



Figura 28 Captura con WireShark

En esta imagen podemos apreciar el instante en el cual se realiza la captura con el *Wireshark*.

### **5.3. Comandos de Configuración**

#### ***Comando Configuración MPLS***

A continuación se presenta la configuración del router 3, ya que en esencia es la misma configuración utilizada en los demás dispositivos.

ip cef

MPLS ip

MPLS label protocol ldp

Los dos últimos comandos se deben configurar en las interfaces en las cuales vamos a trabajar con MPLS. El comando MPLS IP, nos permite decirle a la interfaz que en esa red directamente conectada, vamos a trabajar con MPLS, y con el comando MPLS LABEL PROTOCOL LDP, le decimos al router con que protocolo vamos a distribuir las etiquetas a los demás routers. El Comando IP CEF es un comando característico de CISCO, que significa Cisco Express Forwarding (CEF), que permite una aceleración en la transmisión de paquetes, sin, este comando, no se puede configurar MPLS en la red.

#### 5.4. Metodología

Debido a que los routers solo tenían 2 puertos de FastEthernet, se hizo necesario utilizar un Switch intermedio. Por medio de este interconectamos los routers. El objetivo final del switch era poder configurar una sesión de monitoreo para poder ver el tráfico que viajaba entre los routers. De esta forma pudimos ver que MPLS fue activado exitosamente en la red. Aparte de esto, Activamos 4 sesiones de generadores de tráfico (2 en cada punta de la red), para poder hacer análisis estadísticos de los paquetes de la red.

Debido al procesamiento que conlleva el monitoreo de un puerto específico, en los dispositivos CISCO, se permiten un máximo de dos sesiones por dispositivo, cada una con su puerto de origen (puerto por donde pasa el tráfico que queremos monitorear), y un puerto de destino (puerto donde tenemos conectado un dispositivo con el cual queremos capturar el tráfico). Para el laboratorio solamente usamos, una sesión por dispositivo. Usando los siguientes comandos, monitoreamos el tráfico por medio de los switches intermedio, como se comentó anteriormente, se usan dos puertos un origen y un destino.

```
monitor session 1 source interface
```

```
monitor session 1 destination interface
```

## **5.5. Generador De Tráfico**

Mediante los comandos que aparecen a continuación, se establecen sesiones en las cuales se envía tráfico desde un router de origen a un router destino.

```
! ICMP Echo
```

```
ip sla monitor 1
```

```
type echo protocol ipIcmpEcho 172.16.6.1
```

```
timeout 0
```

```
frequency 9
ip sla monitor schedule 1 start-time now life forever
```

```
! DNS Request
ip sla monitor 2
type dns target-addr www.gns3vault.com name-server 172.16.5.1
timeout 0
frequency 9
ip sla monitor schedule 2 start-time now life forever
```

```
! HTTP GET Traffic
ip sla monitor 5
type http operation get url http://172.16.2.1
frequency 60
ip sla monitor schedule 5 start-time now life forever
```

```
! TCPConnect to FTP
ip sla monitor 8
type tcpConnect dest-ipaddr 172.16.3.1 dest-port 21 control disable
timeout 1000
frequency 60
ip sla monitor schedule 8 life forever start-time now
```

En estas sesiones se puede configurar la IP destino, el tipo de tráfico que se envía, la frecuencia mínima para el envío de paquetes, y el tiempo de inicio y fin. En nuestro caso se decidió envía tráfico desde que

se activó la sesión hasta que se decidió detenerlo mediante el apagado de los dispositivos de red. Para este laboratorio se generó un tráfico desde el router 1, a varios routers del núcleo y lo mismo en sentido contrario desde el router final a router inicial.

Se configura el protocolo para hacer el enrutamiento de tráfico entre toda la red. Con el protocolo activo y los router conociendo todas las rutas posibles, se puede empezar a enviar tráfico, y el router envía los paquetes a los destinos específicos. De igual manera solo denotaremos la configuración de un solo router ya que para todos los demás tiene una configuración similar.

```
hostname R1
!
no ip domain lookup
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 172.16.11.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
router eigrp 1
 no auto-summary
```

```
network 172.16.1.0
network 172.16.11.0
```

## 5.6. SHOW MPLS FORWARDING

Muestra que subredes están asociadas a que etiquetas en el *router*. Las etiquetas son locales en cada *router*, así que una red A con la etiqueta X en el *router* R1, en el *router* R2, la etiqueta de envío puede ser una etiqueta Y para la misma red A, pero en su tabla LFIB identifica con que etiqueta llega el paquete (etiqueta remota), en otras palabras se puede decir que la tabla LFIB de MPLS, representa la tabla de enrutamiento de los protocolos de enrutamiento basado en IP. Estas etiquetas son enviadas gracias al protocolo LDP.

```
R1#show MPLS ldp bindings
tib entry: 172.16.1.0/24, rev 2
    local binding: tag: imp-null
    remote binding: tsr: 172.16.2.1:0, tag: 16
tib entry: 172.16.2.0/24, rev 6
    local binding: tag: 16
    remote binding: tsr: 172.16.2.1:0, tag: imp-null
tib entry: 172.16.3.0/24, rev 10
    local binding: tag: 18
    remote binding: tsr: 172.16.2.1:0, tag: 17
tib entry: 172.16.4.0/24, rev 16
    local binding: tag: 21
    remote binding: tsr: 172.16.2.1:0, tag: 20
```

tib entry: 172.16.5.0/24, rev 21  
    local binding: tag: 22  
    remote binding: tsr: 172.16.2.1:0, tag: 21

tib entry: 172.16.6.0/24, rev 25  
    local binding: tag: 24  
    remote binding: tsr: 172.16.2.1:0, tag: 23

tib entry: 172.16.11.0/24, rev 4  
    local binding: tag: imp-null  
    remote binding: tsr: 172.16.2.1:0, tag: imp-null

tib entry: 172.16.12.0/24, rev 8  
    local binding: tag: 17  
remote binding: tsr: 172.16.2.1:0, tag: imp-null

tib entry: 172.16.13.0/24, rev 12  
    local binding: tag: 19  
    remote binding: tsr: 172.16.2.1:0, tag: 18

tib entry: 172.16.14.0/24, rev 19  
    local binding: tag: 20  
    remote binding: tsr: 172.16.2.1:0, tag: 19

tib entry: 172.16.15.0/24, rev 23  
    local binding: tag: 23  
remote binding: tsr: 172.16.2.1:0, tag: 22

Si se observa la lista nos damos cuenta que todo paquete que tenga una etiqueta 16 O 17, se les debe hacer operación POP con la cual quitamos la etiqueta trabajamos solo en IP. En los otros casos a las etiquetas les hacemos la operación SWAP e intercambiamos las etiquetas, además nos dice cuales la interfaz de salida.

R1#show MPLS forwarding-table

Tabla 1 Etiquetamiento

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	NextHop
16	Pop tag	172.16.2.0/24	0	Fa0/0	172.16.11.2
17	Pop tag	172.16.12.0/24	0	Fa0/0	172.16.11.2
18	17	172.16.3.0/24	0	Fa0/0	172.16.11.2
19	18	172.16.13.0/24	0	Fa0/0	172.16.11.2
20	19	172.16.14.0/24	0	Fa0/0	172.16.11.2
21	20	172.16.4.0/24	0	Fa0/0	172.16.11.2
22	21	172.16.5.0/24	0	Fa0/0	172.16.11.2
23	22	172.16.15.0/24	0	Fa0/0	172.16.11.2
24	23	172.16.6.0/24	0	Fa0/0	172.16.11.2

Los resultados anteriores muestran la misma información que el comando show Mpls ldp bindings, pero de forma más resumida, igual nos muestra la etiqueta entrante, que se debe hacer para cada paquete que llegue con esa etiqueta y la red que representa la etiqueta, cual es la interfaz de salida y por último la IP del siguiente salto.

A continuación se muestra la tabla de enrutamiento basada en IP, en la cual se pueden ver los diferentes protocolos de enrutamiento activados en la red, además se puede ver porque interfaz se recibió que métrica existe hacia la red destino, y por último el protocolo usado y la distancia administrativa del protocolo.

```
R1#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       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
```

```
172.16.0.0/24 is subnetted, 11 subnets
```

```
D 172.16.12.0 [90/30720] via 172.16.11.2, 00:30:07, FastEthernet0/0
```

```
D 172.16.13.0 [90/33280] via 172.16.11.2, 00:23:24, FastEthernet0/0
```

```
D 172.16.14.0 [90/35840] via 172.16.11.2, 00:14:35, FastEthernet0/0
```

```
D 172.16.15.0 [90/38400] via 172.16.11.2, 00:12:55, FastEthernet0/0
```

C 172.16.11.0 is directly connected, FastEthernet0/0  
 D 172.16.4.0 [90/161280] via 172.16.11.2, 00:22:31, FastEthernet0/0  
 D 172.16.5.0 [90/163840] via 172.16.11.2, 00:14:34, FastEthernet0/0  
 D 172.16.6.0 [90/166400] via 172.16.11.2, 00:12:26, FastEthernet0/0  
 C 172.16.1.0 is directly connected, Loopback0  
 D 172.16.2.0 [90/156160] via 172.16.11.2, 00:33:31, FastEthernet0/0  
 D 172.16.3.0 [90/158720] via 172.16.11.2, 00:29:26, FastEthernet0/0

La distancia administrativa es la confianza que se debe tener en un protocolo, es decir una red conecta directamente tiene un valor de distancia administrativa de 0, lo cual implica que es más confiable que una red aprendida por medio de un protocolo de enrutamiento cuya distancia administrativa siempre es mayor que 0.

La tabla que se muestra a continuación, denota las diferentes distancias administrativas que existen.

Tabla 2 Distancias Administrativas

Origen de la ruta	Distancia administrativa
Conectado	0
Estático	1
Resumen de ruta EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

## 7. INTERPRETACIÓN DE RESULTADOS

En este capítulo presenta los hallazgos de la simulación y del laboratorio realizado, así como también análisis de los mismos, con el fin de exponer las bondades comparativas de MPLS frente a los protocolos OSPF y EIGRP.

Al realizarse el laboratorio y la captura de MPLS obtuvo el siguiente tráfico.

Source	Destination	Protocol	Length	Info
172.16.11.1	172.16.5.1	DNS	81	Standard query A www.gns3vault.com
c2:00:11:28:00:00	c2:00:11:28:00:00	LOOP	60	Reply
172.16.14.2	172.16.11.1	ICMP	74	Destination unreachable (Port unreachable)
172.16.6.1	172.16.11.1	ICMP	82	Echo (ping) reply id=0x0000, seq=0/0, ttl=255
172.16.13.2	224.0.0.10	EIGRP	74	Hello
172.16.13.1	224.0.0.2	LDP	76	Hello Message
172.16.13.2	224.0.0.2	LDP	76	Hello Message
172.16.13.1	224.0.0.10	EIGRP	74	Hello
c2:03:11:28:00:01	c2:03:11:28:00:01	LOOP	60	Reply
⊕ Frame 781: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)				
⊕ Ethernet II, Src: c2:00:11:28:00:00 (c2:00:11:28:00:00), Dst: c2:03:11:28:00:01 (c2:03:11:28:00:01)				
⊖ MultiProtocol Label Switching Header, Label: 16, Exp: 0, S: 1, TTL: 253				
MPLS Label: 16				
MPLS Experimental Bits: 0				
MPLS Bottom Of Label Stack: 1				
MPLS TTL: 253				
⊕ Internet Protocol Version 4, Src: 172.16.6.1 (172.16.6.1), Dst: 172.16.11.1 (172.16.11.1)				
⊕ Internet Control Message Protocol				

Figura 29 Captura de Tráfico MPLS

En esta gráfica se pueden observar los mensajes que viaja por la red: EIGRP, LDP e ICMP, con lo cual se denota que ya que encuentra activo MPLS. También podemos observar los campos MPLS explicados en el capítulo uno: etiqueta = 16, exp=0, TTL = 253, y bottom of label Stack =1, los cuales son valores normales en MPLS.

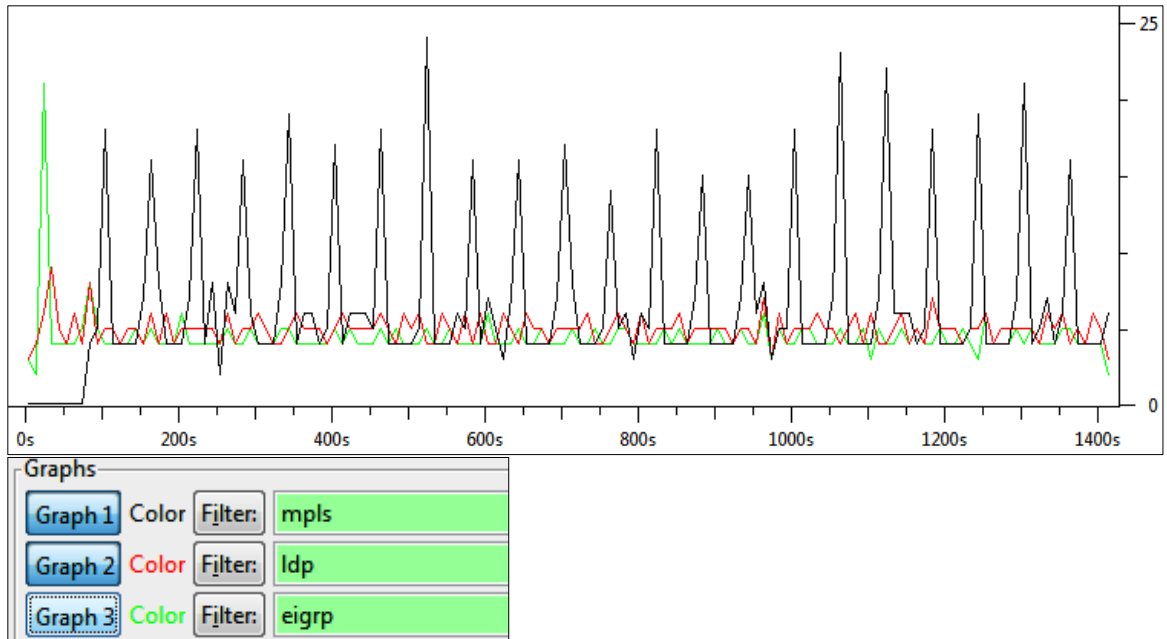


Figura 30 Resultado Protocolo EIGRP, LDP y MPLS

En este gráfico se muestra EIGRP, LDP y MPLS. Como podemos observar LDP se encuentra siempre activo, y el consumo de ancho de banda es bajo. EIGRP tiene un pico al iniciar la transmisión pero posteriormente decrece. MPLS inicia más tarde que EIGRP y LDP, ya que primero se tiene que establecer todas las adyacencias antes de enviar los paquetes.

Source	Destination	Protocol	Length	Info
c2:03:11:28:00:01	c2:03:11:28:00:01	LOOP	60	Reply
172.16.11.1	172.16.6.1	ICMP	78	Echo (ping) request id=0x0000, seq=0/0, ttl=253
172.16.11.1	172.16.5.1	DNS	77	Standard query A www.gns3vault.com
c2:00:11:28:00:00	c2:00:11:28:00:00	LOOP	60	Reply
172.16.14.2	172.16.11.1	ICMP	70	Destination unreachable (Port unreachable)
172.16.6.1	172.16.11.1	ICMP	78	Echo (ping) reply id=0x0000, seq=0/0, ttl=253
172.16.13.1	224.0.0.10	EIGRP	74	Hello
172.16.13.2	224.0.0.10	EIGRP	74	Hello
172.16.13.1	224.0.0.10	EIGRP	74	Hello
172.16.13.2	224.0.0.10	EIGRP	74	Hello
172.16.11.1	172.16.6.1	ICMP	78	Echo (ping) request id=0x0000, seq=0/0, ttl=253
172.16.6.1	172.16.11.1	ICMP	78	Echo (ping) reply id=0x0000, seq=0/0, ttl=253
c2:03:11:28:00:01	c2:03:11:28:00:01	LOOP	60	Reply
172.16.11.1	172.16.5.1	DNS	77	Standard query A www.gns3vault.com
c2:00:11:28:00:00	c2:00:11:28:00:00	LOOP	60	Reply
172.16.14.2	172.16.11.1	ICMP	70	Destination unreachable (Port unreachable)
172.16.13.1	224.0.0.10	EIGRP	74	Hello
c2:03:11:28:00:01	CDP/VTP/DTP/PagP/UDLCCDP		342	Device ID: R3 Port ID: FastEthernet0/1

Figura 31 Captura Tráfico EIGRP

Se observan los mensajes *hello* enviados por *EIGRP*, y la respuesta a través de un ping enviado por *ICMP*

### Escenario GNS3 - MPLS y EIGRP 1

En la siguiente gráfica se aprecian los mismos datos de paquetes enviados, tiempo entre el primer y último paquetes, paquetes por segundo, tamaño de los paquetes, Bytes, bytes por segundo mediante EIGRP.

Traffic	Captured	Displayed	Marked
Packets	2697	2697	0
Between first and last packet	1415,230 sec		
Avg. packets/sec	1,906		
Avg. packet size	79,208 bytes		
Bytes	213624		
Avg. bytes/sec	150,946		
Avg. MBit/sec	0,001		

Figura 32 Datos Captura MPLS

En la siguiente gráfica se puede apreciar los mismos datos de paquetes enviados, tiempo entre el primer y último paquetes, paquetes por segundo, tamaño de los paquetes, Bytes, bytes por segundo, mediante

Traffic	Captured	Displayed	Marked
Packets	2472	2472	0
Between first and last packet	2083,703 sec		
Avg. packets/sec	1,186		
Avg. packet size	84,034 bytes		
Bytes	207733		
Avg. bytes/sec	99,694		
Avg. MBit/sec	0,001		

Figura 33 Datos Captura EIGRP

En conclusión, podemos apreciar que MPLS, envía más paquetes, en menos tiempo

En esta gráfica se muestra la topología simulada en GNS3 para los protocolos MPLS y EIGRP, utilizando seis *routers*.

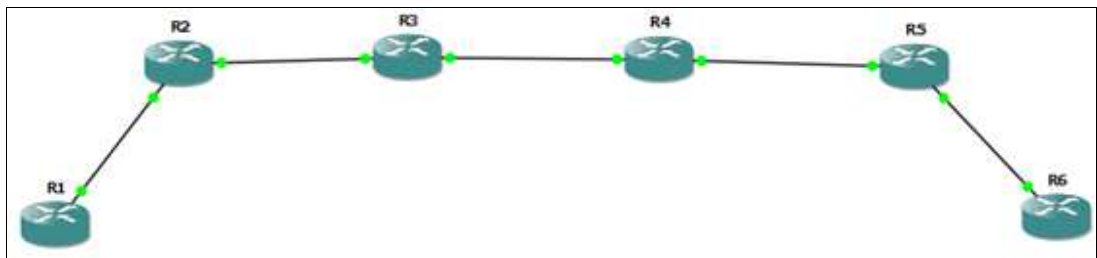


Figura 34 Topología MPLS y EIGRP en el Simulador GNS3

Como se pudo apreciar tanto en las simulaciones con los aplicativos, Packet Tracer, GNS3 y OpenSimMPLS, como en el laboratorio, y sobre la base de los resultados presentado, se puede apreciar que MPLS es más eficiente comparándolo frente a los protocolo EIGRP y OSPF, como se puede observar en las figuras 32 y 33 donde se observa que hay un mayor velocidad de envío de paquetes, el procesamiento de los mismo se realizó con una mayor rapidez; adicional a esto permite utiliza ingeniera de tráfico y QoS.

Para implementar MPLS tan solo se requiere que los sistemas operativos de los dispositivos de red tengan la opción de implementar MPLS

## **8. CONCLUSIONES**

MPLS es una nueva herramienta que no solo es importante para un SP, sino también a organizaciones que tienen un core diferente pero que requieren un tráfico de información importante, e incluso priorizar tipos de tráfico como es el caso de la video conferencias, la cual requiere un gran flujo de tráfico, en comparación con una llamada convencional.

En la práctica de laboratorio, las simulaciones, y el análisis del tráfico, se puede concluir que activando MPLS en una red IP, se observa una mejora importante en tiempo para el envío de paquetes desde su origen hasta su destino; aprovechando las características del protocolo como es el caso QoS e ingeniería de tráfico, da una ventaja comparativa frente a otros protocolos, que no integran todas las bondades que posee MPLS.

La implementación de MPLS tiene un costo bajo debido a que se puede efectuar en cualquier red basada en IP (IPv4 o IPv6), y que en la gran mayoría los dispositivos Hardware actuales (router Cisco) soportan esta tecnología. Además las redes que implementen Calidad de Servicio, podrán migrar estas reglas a MPLS ya que este protocolo también permite QoS y otros beneficios como lo son la ingeniería de Tráfico.

MPLS presenta un sinnúmero de posibilidades y de beneficios integrados de otros protocolos, y las ventajas anteriormente descritas lo convierten en una alternativa viable para su implementación en redes MAN, WAM, LAN.

## 9. BIBLIOGRAFÍA

1. **IETF.** IETF. [En línea] NGN and Enterprise Virtualization cisco, 6 de 11 de 2006. [Citado el: 4 de 10 de 2011.] [www.ietf.org/rfc/rfc3031.txt](http://www.ietf.org/rfc/rfc3031.txt). 3031.
2. GNS3. [En línea] [Citado el: 07 de 04 de 2011.] [www.gns3.net](http://www.gns3.net). ISBN/ISSN.
3. cisco. [En línea] 2009. [http://www.cisco.com/web/offer/emea/3217/docs/packet\\_tracer.pdf](http://www.cisco.com/web/offer/emea/3217/docs/packet_tracer.pdf).
4. wikipedia. [En línea] <http://es.wikipedia.org/wiki/Wireshark>.
5. **Gonzales A., Sindy Marjenny y Hernandez, Sergio Andres.** *Academia Local de Cisco UTS Gia de Estudio: IPsec VPN y MPLS.*
6. *MPLS interdominio en Internet: Aplicaciones Y Retos.* Madrid España : Dpto. de Ingenieria Telemática.
7. *MPLS (Multiprotocolo Label Switching.* **Huidoro Moya, José M y Millan Tejedor, Ramón J.** 4, 2002.
8. **Dorado, Manuel Dominguez.** Soporte de Garantias de Servicio QoS Sobre MPLS Mediante Técnicas Activas. 2004.
9. **Canalis, Maria Sol.** MPLS “Multiprotocol Label Switching”. *una Arquitectura de Backbone para la Internet del Siglo XXI.*
10. **Gejin, Luc De.** *MPLS Fundamental.* s.l. : Cisco Press, 2007.
11. **Alwayn, Vivek.** *Advanced MPLS Desing and Implementation.* s.l. : Cisco Press, 2001.
12. **Lobo, Lancy.** *MPLS Configuration on Cisco IOS Software.* s.l. : Cisco Press, 2005.
13. **Tan, Kee.** *MPLS fopr Metropolitan Area Network.* s.l. : Auerbach Publication, 2005.
14. **AbginYA, Johnson I.** *Multiprotocolo Label Switching.* s.l. : Auerbach Publication, 2010.
15. **Statti, Albert.** *JUNOS Internet Software for J-Series. and T-Series Routing Plataforms MPLS Applications Configuration Guide, Release 7.0.* 2004 : Juniper Networks Inc.

16. **Lucek, Ina Minei And Julian.** *MPLS Enabled Applications : Emerging Developments and New Technologies, 3rd Edition.* s.l. : John Wiley & Sons Ltd, UK.

17. **Yamanaka, Kohei Shimoto Eiji Oki y Naoaki.** *GMPLS Technologies.* s.l. : CRC Press, 2006.

18. **Feldman, N.** [En línea] IBM Corporation, Enero de 2001. [www.ietf.org/rfc/rfc3036.txt](http://www.ietf.org/rfc/rfc3036.txt). 3036.

19. **Dominguez, Manolo.** Manolo Dominguez. [En línea]  
[www.manolodominguez.com/projects/opensimmppls/index.php](http://www.manolodominguez.com/projects/opensimmppls/index.php).

20. MPLS Resource Center. [En línea] [www.mplsrc.com](http://www.mplsrc.com)