FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

SIMULACIÓN GRÁFICA EN GNS3 DE LA RED DE CORE IP/MPLS DE LA REGIÓN ANDINA EN LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES (CNT E.P.)

"Trabajo de titulación presentado en conformidad a los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones"

Profesor Guía:

Ing. Diego Paredes Páliz

Autores:

Natalia Elizabeth Loyos Jaramillo
Héctor Rodrigo Caizaluisa Cruz

Año
2012

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

_____

Diego Paredes Páliz
Ingeniero en Redes y Telecomunicaciones
0603014143

DECLARACIÓN DE AUTORÍA DE LOS ESTUDIANTES

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

_____	_____
Natalia Loyos	Rodrigo Caizaluisa
171827114-9	171752896-0

AGRADECIMIENTO

Agradezco a Dios por la bendición de permitirme llegar a cada meta propuesta, a mis padres por ser el impulso y apoyo que me llevó a alcanzar esas metas y a quienes hicieron posible el desarrollo de este proyecto tanto en la CNT E.P. como en la Universidad de las Américas

Natalia Loyos

AGRADECIMIENTO

Agradezco a Dios, a mi familia por estar siempre a mi lado, maestros que con sus enseñanzas nos han preparado para el futuro y amigos con los cuales he seguido este camino para alcanzar esta nueva meta

Rodrigo Caizaluisa

DEDICATORIA

El presente trabajo deseo dedicarlo a mis padres, Marco y Elizabeth por todo el apoyo que recibí durante mis estudios y aún después de ellos. Por confiar en mí y brindarme todos los medios que estuvieron a su alcance para hacerme una buena persona

Natalia Loyos

DEDICATORIA

Este trabajo está dedicado a mis padres Héctor y Yolanda, a mi hermano Diego a mí cuñada Johanna y a mi hermosa sobrina Doménica, que son la más hermosa familia.

Rodrigo Caizaluisa

RESUMEN

La Corporación Nacional de Telecomunicaciones (CNT EP) instaló en su red de transporte una solución que se basa en el protocolo de red IP/MPLS (*Internet Protocol / Multiprotocol Label Switiching)* para ofertar más y mejores servicios de transmisión de datos, sin embargo, en la actualidad esta red presenta deficiencia en cuanto al manejo de calidad de servicio. El presente proyecto de titulación tiene como fin simular en GNS3 *(Graphical Network Simulator)* la red de *core* de la región Andina de la Corporación Nacional de Telecomunicaciones y configurar reglas de QoS *(Quality of Service)*.

En el capítulo uno se expone en forma general la teoría referente a MPLS, ventajas y desventajas de su utilización así como la teoría referente a *QoS* mientras que en el segundo capítulo se describe la simulación gráfica de la cual es objeto el presente proyecto.

Para la simulación se utilizará el simulador gráfico GNS3 que entre sus funciones permite aplicar diferentes niveles de *QoS* al tráfico de una red.

Posteriormente, en el capítulo tercero, se describirán los resultados obtenidos, cabe indicar que no se realizará la instalación de ningún equipo aunque se desarrollará un escenario de prueba. El proyecto busca únicamente simular y configurar la red aplicando reglas de *QoS* definidas.

Finalmente en el cuarto capítulo se describen las conclusiones y recomendaciones que a lo largo del desarrollo del proyecto fueron encontradas y que facilitarán la comprensión del mismo.

ABSTRACT

La Corporación Nacional de Telecomunicaciones (CNT EP) installed in its transport network a solution based in the IP/MPLS (Internet Protocol/ Multiprotocol Level Switching) network protocol to offer more and better data transmission services; however, actually, this network presents deficiencies in the management of the service quality. The goal of the present project of degree is to simulate graphically in GNS3 (Graphical Network Simulator) the core network of the Andean Region of the institution and configure rules of QoS (Quality of Service).

In Chapter I, it is outlined in general way the concepts concerning to MPLS technology, the advantages and disadvantages of its use, and the theory referring to QoS while Chapter II describes the graphic simulation which is the subject of this project.

The Software GNS3 will be used to the simulation because this allows us to apply different levels of QoS.

In Chapter III, the effects will be described. It should be remarkable that it won't make the installation of any equipment because the Project is just to simulate and configure the network applying rules of QoS.

Finally, Chapter IV describes the conclusions and recommendations that has been found throughout the project development and which will facilitate its understanding.

ÍNDICE

INTRODUCCIÓN

Los avances tecnológicos, el beneficio de las comunicaciones, transporte de mayor cantidad de datos, nuevas aplicaciones entre otras, dan lugar a la necesidad de una transmisión de datos más eficiente que permita hacer uso de las telecomunicaciones.

Con el paso del tiempo nuevos métodos de comunicación se han ido desarrollando a fin de poder transmitir grandes cantidades de información, es así que se encontró que el protocolo IP *(Internet Protocol)* ya no resultaba eficiente debido a que utilizaba un gran ancho de banda para transmisiones de voz, video o datos y su velocidad de ruteo era muy lenta. A mediados de los 90's nace la tecnología ATM (*Asynchronius Transfer Mode / Modo de Transferencia Asíncrona)* la cual ofrecía velocidades de transmisión mayores y la inclusión de un nuevo concepto como es la "Ingeniería de Tráfico" que se refiere a un encaminamiento inteligente de los paquetes de datos, sin embargo esta tecnología fue más difícil tanto para configurar como para integrarla con otras tecnologías.

Para el año de 1998, un grupo de técnicos que administran tareas de ingeniería de telecomunicaciones, principalmente internet (*IETF* por sus siglas en inglés) define el estándar MPLS, el cual proporciona beneficios de ingeniería de tráfico tal como en ATM y además ofrecía la posibilidad de operar sobre cualquier tecnología, logrando que el diseño y la operación de red fuese más sencillo y ofreciendo mayor escalabilidad. Para esto se utilizó etiquetas añadidas a los paquetes y que definirían un camino virtual por la red a los cuales se les asocia un parámetro de calidad de servicio (*QoS)* determinado.

CAPÍTULO I
FUNDAMENTOS TEÓRICOS

1.1 ANTECEDENTES

La Corporación Nacional de Telecomunicaciones es una empresa que brinda una variedad de soluciones de telecomunicaciones que requiere el país, por tal motivo su sistema de comunicación debe afinarse permanentemente y adaptarse a nuevas tecnologías.

En su red de transporte a nivel nacional dispone de la tecnología IP/MPLS sobre la cual se soportan servicios de voz, video y datos, la cual es implementada en su totalidad con equipamiento CISCO de última tecnología.

Se describe a continuación las características más importantes de MPLS y *QoS* para cumplir con el objetivo del presente proyecto.

1.2 INTRODUCCIÓN A MPLS

Sobre redes existentes como ATM, Frame Relay, SDH, entre otras, se habían realizado cambios en las configuraciones con la finalidad de adaptarlas a la necesidad de ofertar calidad de servicio haciendo que sus políticas de conmutación se basen en el envío de paquetes sin embargo este método no aseguraba ningún tipo de calidad de servicio.

Ante esta necesidad los miembros de la IETF crearon un nuevo estándar de comunicación (MPLS) que proporciona escalabilidad y fácil aplicación sobre cualquier otra tecnología enfocándose principalmente en Calidad de Servicio, Ingeniería de tráfico y Redes Privadas virtuales.

Se plantea la opción de utilizar etiquetas de corto tamaño que son añadidas a los paquetes con el fin de permitir una conmutación más rápida.

1.2.1 CARACTERÍSTICAS DE MPLS

MPLS ofrece un servicio orientado a conexión y funciona sobre diferentes tecnologías. En MPLS los paquetes se etiquetan basándose en criterios de prioridad y/o calidad de servicio (QoS) del tráfico que va a pasar en la red.

MPLS opera entre la capa 2 y la capa 3 del modelo OSI representado gráficamente en la Figura 1., por lo tanto tiene características de las dos capas haciendo uso eficiente de la velocidad y el control sobre el envío de paquetes

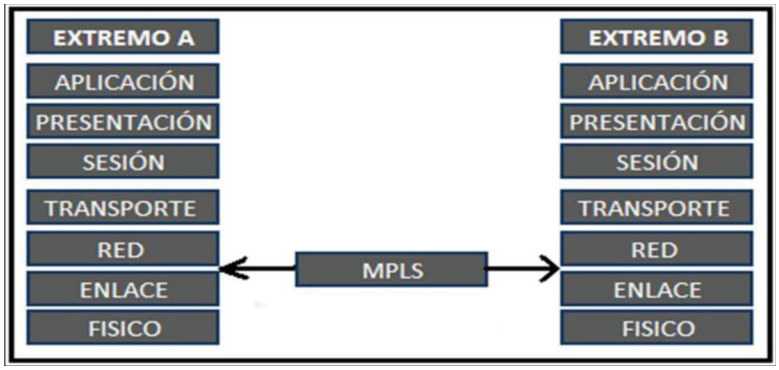


Figura 1. Representación gráfica de las capas del modelo OSI

Se dice entonces que, MPLS aprovecha dos componentes funcionales del modelo de capas OSI, la una es la conmutación rápida de capa 2 conocido como *forwarding* y la otra es el control de conmutación de la capa 3 conocido como *routing*.

1.2.2 ELEMENTOS DE MPLS

1.2.2.1 LSR *(*Label Switching Router*)*

El LSR es un router ubicado la red MPLS encargado de dirigir el tráfico interno. Este equipo es el encargado de realizar la imposición de etiquetas conocido como proceso *push* y determinación de etiquetas, conocido como proceso *pop.*

Entonces, el LSR asigna una etiqueta al paquete y lo envía al siguiente LSR del LSP (camino virtual por el que fluye el tráfico de datos). Cuando se trabaja del dominio MPLS los LSR ignoran la cabecera IP; y únicamente analizan la etiqueta de entrada, luego consultan la tabla correspondiente (tabla de conmutación de etiquetas) y remplazan la etiqueta por otra nueva, de acuerdo al algoritmo de intercambio de etiquetas. Al llegar el paquete al último LSR de cola (salida) y ve que el siguiente salto lo saca de la red MPLS; en la tabla de conmutación de etiquetas se quita ésta y se envía el paquete utilizando uno de los protocolos de ruteo por ejemplo OSPF, ISIS, etc.

Al primer router LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último LSR se le denomina de salida o de cola. Los dos están a los extremos del dominio MPLS. Los restantes equipos *router* que se encuentran entre los LSR de entrada y los LSR de salida son LSR interiores del dominio MPLS como se muestra en la Figura 2.

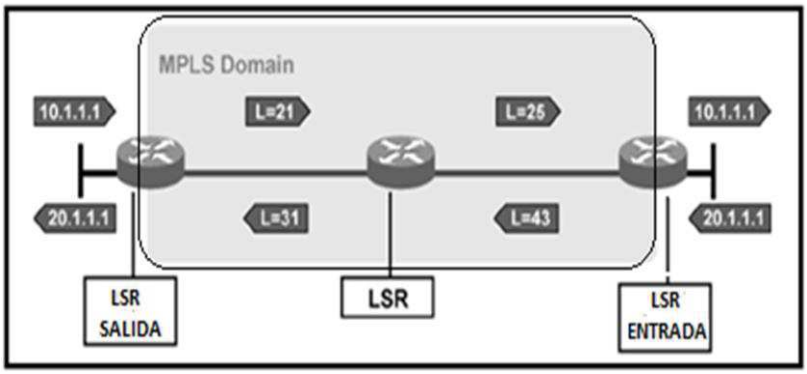


Figura 2. Representación LSR en una red MPLS

1.2.2.2 LSP *(*Label Switching Path*)*

LSP es el medio virtual por el que fluye el tráfico entre LSRs hasta alcanzar el LSR de salida, estos caminos son unidireccionales por lo tanto en cada LSR existen dos LSP. Un LSP puede ser requerido antes de que exista la transmisión de datos o una vez que se ha empezado el flujo de los mismos comportándose como un túnel ya que ignoran la cabecera de la capa de red del paquete y para el envío del mismo se basan en el algoritmo de etiquetas.

MPLS provee dos opciones para configurar un LSP, uno cuando el LSR selecciona en forma independiente el próximo salto para un FEC dado y el otro, cuando el LSR de entrada especifica el próximo salto.

1.2.2.3 FEC (Forward Equivalence Class)

FEC es un concepto básico en MPLS, es un flujo de datos cuyos paquetes comparten las mismas características para su transporte como son:

- Utilizan la misma forma de envío
- Son enviados sobre el mismo camino *Path*
- Se los envía con el mismo tratamiento

Gracias a esta agrupación, el valor de las FEC en el paquete se puede utilizar para establecer prioridades y de esta forma dar prioridad a unas FECs sobre otras sin embargo este proceso se realiza una sola vez, cuando el paquete entra en el red MPLS.

1.2.2.4 AS (*Sistema Autónomo*)

Un sistema autónomo consiste en un grupo de *routers* que comparten las mismas políticas de enrutamiento, y están bajo un mismo dominio administrativo. Puede definirse como una colección de *routers* corriendo un mismo IGP, o bien, usando variados protocolos de enrutamiento pero dichos *routers* pertenecen a una misma organización. En cualquier caso, el mundo exterior verá al sistema autónomo como una sola entidad.

Cada ruteador que utiliza BGP debe usar el número de sistema autónomo. Éstos pueden ser privados o públicos.

1.2.3 ETIQUETAS MPLS

La etiqueta es la que permite identificar un FEC dentro de la red MPLS. Cuando un paquete ingresa en una red MPLS es clasificado y asignado a un FEC específico usando etiquetas, todos los paquetes que pertenecen a un mismo FEC son renviados usando la dirección del siguiente salto. El valor de la etiqueta cambia mientras el paquete IP es transportado a través de la red, cuando el paquete etiquetado es enviado desde un LSR hacia el LSR del siguiente salto, el nuevo valor de la etiqueta del paquete es el valor que el LSR del siguiente salto asigna para representar el FEC.

- ***Header MPLS***.-La cabecera MPLS se forma de 32 bits y se inserta entre la capa 2 y capa 3 del *Stack* de comunicaciones OSI. La estructura de la cabecera se presenta en la Figura 3.

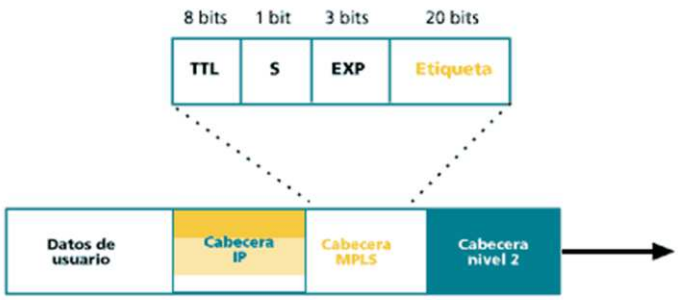


Figura 3. Cabecera MPLS

Barbera, J. (2010). Una arquitectura de backbone para la Internet del

- ***Etiqueta MPLS.-*** Se le denomina “LABEL” y es la etiqueta propiamente dicha ya que identifica una FEC, formado por 20 bits por lo tanto existen 2^{20} combinaciones, lo que equivale a 1.048.576 de las cuales las combinaciones comprendidas entre 0 y 15 se encuentran reservados. Cuando un paquete etiquetado es recibido, se establece el valor de la etiqueta con el fin conocer el siguiente salto al cual se debe re direccionar el paquete y luego se remplaza la etiqueta por una nueva.

- ***Experimental (EXP).-*** Formado por 3 bits, se usa experimentalmente para establecer calidad de servicio *(QoS)*. Maneja ocho niveles de prioridad, entre el que se destaca el código 101 (5) que representa mayor prioridad.

- ***Stack.-*** Este campo lo compone 1 bit, permite identificar si la etiqueta es la última ya que en MPLS se usan varias etiquetas principalmente para levantar servicios; entonces un 0 indica que existen más etiquetas MPLS.

- ***TTL.-*** Corresponden a una secuencia de 8 bits conocido como *Time to Life*, similar a lo utilizado en el protocolo IP. Es el tiempo máximo de vida del paquete cuyo máximo valor es 15 saltos permitidos antes de descartar un paquete.

1.2.4 PROTOCOLOS

Con la arquitectura de MPLS se maneja una variedad de protocolos cuyo uso depende de los equipos de la red así como de las políticas de administración.

A continuación se describen los protocolos para distribución de etiquetas y señalización

1.2.4.1 LDP (Label Distribution Protocol)

El protocolo LDP define procedimientos para el intercambio de etiquetas, por esa razón es imprescindible para el funcionamiento de la red MPLS. Los LSRs utilizan este protocolo para intercambiar la etiqueta FEC.

Al establecer una sesión LDP se generan diversos mensajes de modo que se pueda dar a conocer a otros LSRs qué LSR está activo.

Una sesión LDP se da entre LSRs usando TCP como transporte confiable para dichas sesiones

1.2.4.2 BGP (Border Gateway Protocol)

El protocolo BGP garantiza el intercambio de información de enrutamiento libre de lazos (conocidos como *loops)* entre sistemas autónomos (*AS*), su función no es encontrar una red específica sino proporcionar información que permita encontrar el AS en el cual se encuentra dicha red, para lo cual el encargado de encontrar la red es el protocolo de pasarela interna a utilizar, tal como RIP, IGP, EIGRP, IS-IS, OSPF etc.

BGP es un protocolo extremadamente complejo usado en Internet y dentro de las empresas multinacionales, permite políticas de enrutamiento y diferenciación entre el tráfico de diferentes proveedores de servicio.

1.2.4.3 EBGP (External Border Gateway Protocol)

Es un término genérico para un protocolo que funciona entre diferentes sistemas autónomos.

1.2.4.4 iBGP (Internal Border Gateway Protocol)

El protocolo *Internal* BGP se usa cuando los *routers* vecinos no son necesariamente adyacentes.

1.2.4.5 IS-IS

IS-IS es un protocolo de encaminamiento jerárquico de IGP, se basa en el uso de algoritmos que permiten encontrar el camino más fácil.

Este envía mensajes a todos los routers pertenecientes a la red de modo que cada uno de ellos conozca por completo la topología del sistema autónomo y decidir la mejor ruta para el transporte del paquete

1.2.4.6 RSVP (Protocolo de Reserva de Recursos)

RSVP es un protocolo de señalización que permite reservar la capacidad solicitada por un flujo de datos en todos los routers del camino.

Protocolo orientado a conexión, por lo tanto requiere guardar información del estado en todos los routers que conforman el trayecto lo que podría resultar un problema ya que debe guardar demasiada información pero en MPLS es un protocolo muy útil ya que en esta tecnología no se maneja números de flujos muy elevados.

1.2.5 TABLAS DE ENRUTAMIENTO MPLS

Las tablas de enrutamiento se diseñan y construyen de la información de enrutamiento que proporciona el componente de control. Mediante algoritmo de intercambio de etiquetas se realiza la clasificación de los paquetes a la entrada del dominio MPLS con lo cual se puede hacer la asignación de la cabecera.

1.2.5.1 Tabla RIB Routing Information Base

Se refiere a la tabla de enrutamiento.

1.2.5.2 Tabla LIB *Label Information Base*

En esta tabla se encuentran todas las etiquetas.

1.2.5.3 Tabla FIB *Forwarding Information Base*

Esta tabla se activa en CEF (*Cisco Express Forwarding).*

1.2.5.4 Tabla LFIB Label Forwarding Information Base

Esta tabla funciona para el *Forwarding* esto es sólo envío de paquetes. La tabla LFIB se forma al final, es decir cuando MPLS ya ha comenzado a funcionar y por esta razón contiene toda la información de envío y recepción de etiquetas.

Para llenar esta tabla, MPLS usa el protocolo LDP (*Label Distribution Protocol*) Un ejemplo se muestra en el diagrama de *Routers* de la Figura 4, donde éstos se encuentran conectados entre sí a sus interfaces Gigabit Ethernet

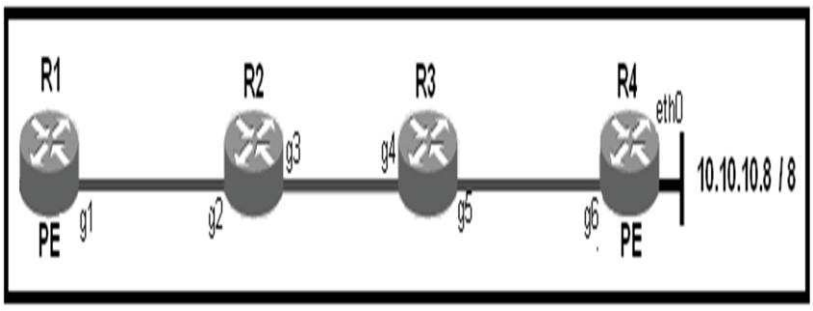


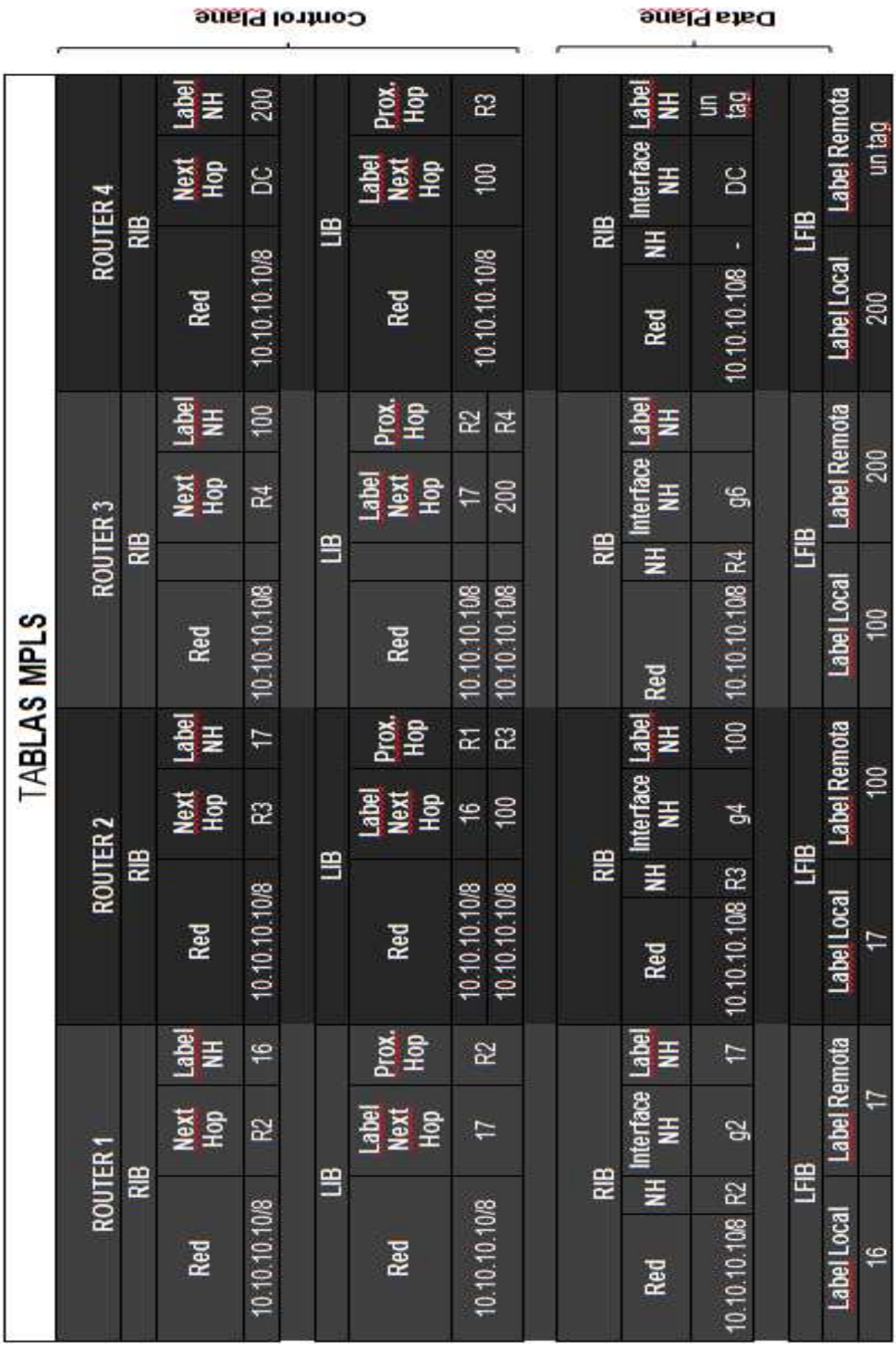
Figura 4. Diagrama de Routers

El router R1 es un LSR *(Label Switching Router)* de entrada y el R4 es un LSR de salida a la red 10.10.10.8 /8 por lo que se ubican en el exterior del dominio MPLS y se los denomina *PE (Provider Edge)*, utilizan el protocolo BGP.

Los Routers R2 y R3 son LSR's internos, también denominados *P (Provider)* como ya lo indicamos, estos Routers no se conectan a clientes y no utilizan el protocolo BGP por lo tanto podemos describirlos como el *core* de la red MPLS.Una vez configurado el protocolo MPLS en esta red, se pueden visualizar las tablas de enrutamiento en cada router.

En la Tabla 1. se muestra las tablas de enrutamiento MPLS que se deben encontrar en cada router.

Tabla 1. Formación de Tablas MPLS



1.2.6 COMPONENTES DE LA ARQUITECTURA MPLS

El protocolo MPLS presenta dos componentes principales denominados Plano de Control y Plano de Datos.

1.2.6.1 Plano de control

Es el elemento que maneja la capa 3 del modelo OSI (Red), por esta razón se le puede asociar y definir como la parte inteligente donde se tratan los protocolos OSPF, EIGRP, IS-IS y BGP para intercambiar etiquetas. El Plano de control se muestra en la Figura 5. y es la encargada del intercambio de información de enrutamiento entre los dispositivos adyacentes. El plano de control crea la tabla de enrutamiento RIB (*Routing Information Base).*

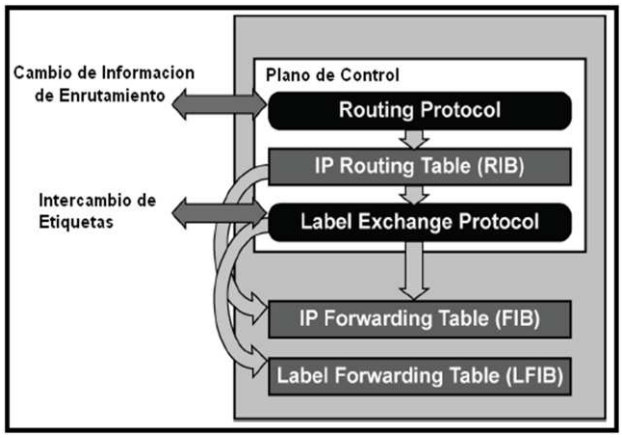


Fig. 5. Plano de Control MPLS

1.2.6.2 Plano de Datos

Hace referencia a la funcionalidad de *Switching* que se desarrolla a nivel de capa 2 (Enlace de Datos) por lo tanto sólo se envían paquetes de un *router* a otro (el paquete no se procesa, solo se envía). El plano se encarga de renviar paquetes a la interface apropiada basándose en la información proporcionada por la tabla LFIB (*Label Forwarding Information Base)*.como se puede ver en la Figura 6.

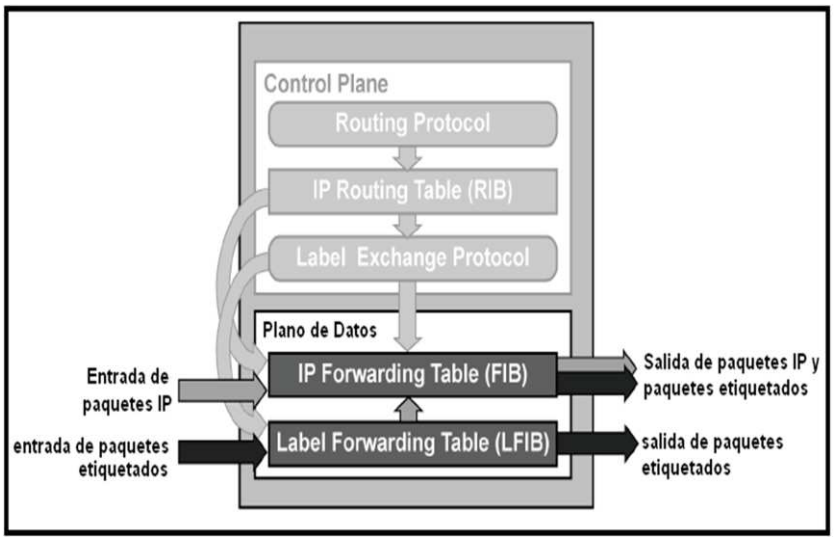


Figura 6. Plano de Datos MPLS

MPLS permite trabajar con alta granularidad (bytes por segundo), Calidad de servicio *QoS*, ingreso de diferentes tipos de tráfico sin que se mezclen entre sí para lo cual se usan las *VPN*. Los paquetes no siempre suben al plano de control gracias a que los *routers* de *core* lo hace más rápido ya que solo pasa por el plano de datos. En la Tabla 2 se resume los componentes que forman la Arquitectura MPLS.

Tabla 2. Tabla resumen de los Planos de MPLS

ARQUITECTURA MPLS			
CONTROL PLANE	Protocolos	LDP	*Label Distribution Protocol*
		TDP	*Tag Distribution Protocol*
		IGP	*Interior Gateway Protocol*
		BGP	*Border Gateway Protocol*
	Tablas	RIB	Tabla de enrutamiento normal
		LIB	Tabla de etiquetas
DATA PLANE	Forwarding		
	Tablas	FIB	Tabla RIB incluido next-hop
		LFIB	Tabla de mejores etiquetas

1.2.7 FUNCIONAMIENTO DE MPLS

El funcionamiento de MPLS está basado en el envío y control del tráfico trabajando en conjunto entre sí.

MPLS se basa en la asignación e intercambio de etiquetas lo que permite establecer los caminos LSP *(Label Switching Path)* por toda la red. Los LSP tienen la función de establecer el sentido del tráfico en la entrada en cada punto la red. Cada LSP se establece en base de concatenar uno o más saltos a los cuales se les denomina hops, donde se intercambiaran las etiquetas, de modo que cada paquete pueda ser enviado de un LSR a otro, a través del dominio MPLS.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes que se asignan a la misma FEC (*Forward Equivalence Class*). Una FEC es un conjunto de paquetes que comparten las mismas necesidades para su transporte. Como se mencionó anteriormente los LSR pueden ser de cabecera si el primer equipo o de salida si es el último LSR al resto de equipos se les denomina interiores formando así el camino LSP.

Un LSR, mostrado en la Figura 7, no es más que un *router* especializado en el envío de paquetes etiquetados por MPLS y dedicado al *Data Plane* (Componente Plano de datos) en el núcleo de la Red. A los LSR se los etiqueta con la letra “P” (*Provider*), no conectan clientes y no utilizan el protocolo de enrutamiento BGP, además se ubican en el centro *(core)* de la red MPLS y se dedican al *Forwarding* (reenvío). Por el contrario, un PE (*Provider Edge*) si utiliza el protocolo BGP, conecta clientes y estos equipos son quienes hacen *PUSH* y *POP* de Etiquetas e interactúan en el *control plane y data plane*.

La operación PUSH se refiere a apilar etiquetas, esto es cuando una etiqueta nueva es empujada encima de otra (si existe), en una operación POP la etiqueta es retirada del paquete lo cual permite revelar la etiqueta anterior.

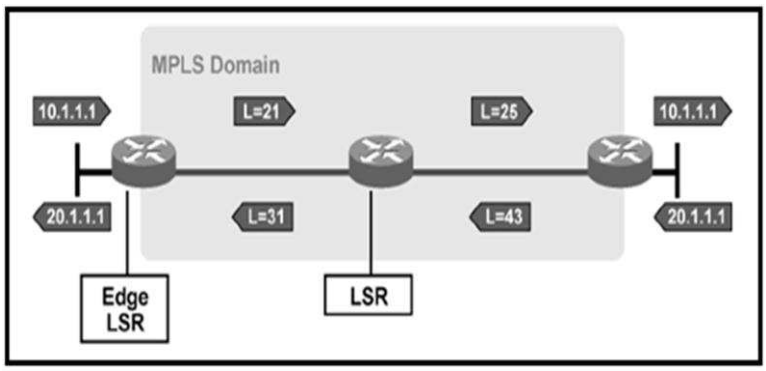


Figura 7. Representación de un LSR y PE de una red MPLS
Tomado de H3C (2012) , MPLS Operation,

En cada LSR se asigna una etiqueta y se envía el paquete al siguiente LSR del LSP, dentro del dominio MPLS ignorando la cabecera IP, logrando mayor velocidad en la red ya que solamente analizan la etiqueta de entrada, luego consultan la tabla correspondiente (tabla de conmutación de etiquetas) y remplazan la etiqueta por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas.

Las etiquetas se colocan en la cabecera MPLS, entre los niveles 2 y 3 y de acuerdo a las características del IETF, MPLS puede operar sobre cualquier infraestructura de transporte, ya sea esta PPP, LAN, ATM, FRAME RELAY, etc.

Para establecer los circuitos virtuales *LSP* el protocolo MPLS necesita información sobre los caminos de routing para la red y para esto usa la propia información de encaminamiento que manejan los protocolos internos IGP *(Interior Gateway Protocol)* (OSPF, IS-IS, RIP...) que utilizan para construir las tablas de enrutamiento.

Dicho en otras palabras, en MPLS para cada “ruta IP” de la red, crea un “camino de etiquetas” a base de concatenar las de entrada y salida en cada uno de los LSR; el protocolo interno correspondiente se encarga de pasar la información necesaria.

Siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino y para la distribución de etiquetas entre los nodos. En la actualidad la arquitectura MPLS no utiliza un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes como el protocolo RSVP (*Protocolo de reserva de recursos)* y sus diferentes extensiones *o* el caso del protocolo LDP *(Label Distribution Protocol).*

Se debe tener en cuenta que en el extremo de la nube MPLS se podría tener una red convencional de Routers IP ya que el núcleo MPLS proporciona una arquitectura de transporte permitiendo a cada par de Routers verse a una distancia de un sólo salto, como si estuvieran unidos todos en una topología tipo malla..

La diferencia con topologías reales es que en MPLS, la construcción de caminos virtuales es mucho más flexible y no existe pérdida sobre la visibilidad de los paquetes IP.

Logrando enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario.

Un ejemplo de una topología MPLS se puede ver en la Figura 8.

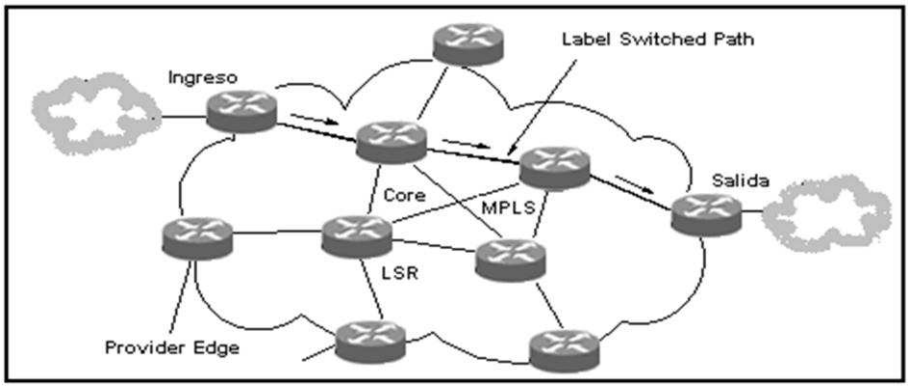


Figura 8. Representación gráfica LSP

Tomada de H3C (2012), MPLS Operation

1.2.8 VENTAJAS DE LAS REDES MPLS

En el año 1997 el IETF establece un grupo de trabajo en MPLS con el fin de obtener un estándar que unificase las soluciones propietarias de conmutación de nivel 2 para el año 1998 se establece el estándar conocido por MPLS que proporciona mayores beneficios respecto a la ingeniería de tráfico del modelo de IP sobre ATM, entre ellas:

- Flexible y escalable a las necesidades crecientes en cuanto a calidad de servicio en redes de transporte
- Comunicación de alta velocidad
- Servicio orientado a conexión
- Asignación flexible y eficaz del ancho de banda

El uso del protocolo MPLS busca corregir los problemas de IP que pueden resumirse en los siguientes:

- Tiempos muy altos de procesamiento en un *router* para analizar un paquete.
- No maneja acuse de recibo.
- Cabecera IP muy grande, de 20 bytes.
- Ruteo en capa 3 (red) lo que consume tiempo y recursos de red.
- El *Switching* que se realiza en capa 2 es más lento.
- El protocolo IP busca el camino más lento pero no siempre es el mejor.
- Además IP no toma en cuenta todas las métricas
- Con el protocolo IP se realizan varios re-cálculos, lo que demanda mayor tiempo.

MPLS evoluciona en sus presentaciones para ser el referente de las tecnologías de conmutación y cuyo gran reto es gestionar redes que son cada vez más complejas y extensas.

MPLS es un protocolo que permite asegurar un parámetro de Calidad de Servicio QoS de forma independiente y no relacionada con la red de transporte. La calidad de Servicio QoS se puede asignar dependiendo de las necesidades del tráfico ya sea a un cliente en específico o a un tipo de tráfico (FEC) a la que se asocie un LSP.

El etiquetado en capa 2 ofrece un servicio multiprotocolo y la posibilidad de ser utilizado en las diferentes tecnologías que trabajan a nivel de capa 2 o capa de enlace como: ATM, Frame Relay, líneas dedicadas, LANs.

Los LSP's son válidos para múltiples protocolos, ya que el encaminamiento de los paquetes se realiza en base a la etiqueta MPLS estándar, no a la cabecera de nivel de red.

Las decisiones de encaminamiento para los paquetes que toman los Routers MPLS se basan en la tabla LIB y las respuestas son mucho más rápidas y sencillas que las que toma un router IP ordinario sin MPLS cabe destacar que la tabla LIB es mucho más pequeña que una tabla de rutas normal. La estructuración de la red MPLS mediante etiquetas permite agregar con facilidad una mayor cantidad de flujo logrando que el sistema tenga un mecanismo muy escalable.

En lo que se refiere a la Ingeniería de Tráfico, permite optimizar los recursos y reducir congestión.

Respecto a redes privadas virtuales *(VPN)* se pueden crear caminos o LSP con gran versatilidad utilizando el protocolo MPLS y haciendo más sencilla la creación y administración de las VPN.

1.3 CALIDAD DE SERVICIO

La calidad de servicio se refiere al establecimiento de parámetros para evaluar, en redes de telecomunicaciones, adecuados niveles de priorización basadas en la elección de una política acertada para el manejo de colas de paquetes de datos. Un adecuado canal de comunicación evita el problema de retardos existentes durante la transmisión.

1.3.1 ELEMENTOS DE EVALUACIÓN DE *QoS*

1.3.1.1 Retardos

En la transmisión de paquetes existen componentes que afectan la velocidad con que llega dicho paquete desde el emisor hasta el receptor y que generan retardos que podrían afectar la calidad de servicio que se desea lograr, las causas de retardos pueden ser:

- Retardo de propagación: es el retardo que se obtiene del tiempo que le cuesta a un paquete recorrer el medio físico entre un punto y otro, en algunos casos es despreciable, excepto para grandes distancias como cuando hay comunicación satelital.
- Retardo de procesamiento o enrutamiento: Es la cantidad de tiempo que tarda un router en recibir un paquete, tomar una decisión de enrutamiento y transmitir el paquete a través de un puerto de salida no congestionado. Se mide normalmente en microsegundos.
- Retardo en colas: Es la cantidad de tiempo que espera un paquete en una cola hasta que se transmite. Durante periodos de congestión de tráfico se puede controlar el retardo en las colas mediante gestión de memorias y control de servicio de colas.
- Retardo de serialización: Este tipo de retardo aparece cuando un paquete es adaptado a un medio físico por el cual se va a transmitir. La velocidad de ese mismo medio y el tamaño del paquete son determinantes para este

retardo. En la Tabla 3 se muestra un ejemplo sobre el tiempo que se tarda en transmitir paquetes de acuerdo a la velocidad del enlace y tamaño del paquete:

Tabla 3. Tabla de Serialización

VELOCIDAD DEL ENLACE	TAMAÑO DEL PAQUETE		
	64 bytes	256 bytes	1500 bytes
64 Kbps	8 ms	32 ms	187 ms
256 Kbps	2 ms	8 ms	46 ms
512 Kbps	1 ms	4 ms	23 ms

Cálculo del retardo por serialización:

Para el caso en que se requiere transmitir un paquete de 1500 bytes por un enlace de 64 Kbps sería:

$$\frac{1500 * 8\ bits}{64000\ bps} = 0.1875\ s = 187\ ms$$

1.3.1.2 *Throughput*

El *Throughput* (*caudal*) es un término genérico que describe la capacidad de un sistema para transferir datos. El parámetro más directo que un router puede configurar para controlar el tráfico de la red es el throughput asignando diferentes anchos de banda para los diferentes tipos de paquetes.

1.3.1.3 *Jitter*

Se define como Jitter la llegada tardía de un paquete o secuencia de paquetes a su destino, lo que perjudica gravemente la transmisión de datos provocando pérdidas en la información y deteriorando el servicio prestado.

El Jitter es causado principalmente por las diferencias en los tiempos de espera en cola por los paquetes consecutivos dentro de un flujo para evitar este problema se aplica QoS en los equipos como se puede ver en la Figura 9

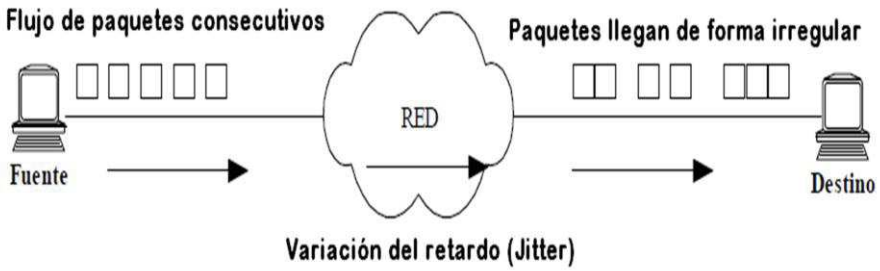


Figura 9. Jitter
Tomado de Alarcón, R. (2010). Estudio e Implementación de Mecanismos de Calidad de servicio sobre una Arquitectura de Servicios Diferenciados

1.3.1.4 Pérdida de paquetes (LOSS)

Los paquetes de datos pueden ser descartados por la red y esto puede ocurrir en determinadas circunstancias de las cuales, las más comunes son:

- Una rotura en el enlace físico
- Un paquete corrupto debido al ruido
- Desbordamiento de las memorias producidas por la congestión de la red

Hay que mencionar que en ocasiones es necesario descartar paquetes a propósito, un ejemplo de esto es cuando el *router* puede realizar el descarte selectivo de algunos paquetes para así evitar la congestión. En los últimos años se han establecido diferentes métodos para aplicar QoS en las redes de acuerdo a los diferentes tipos de tráfico que se desean transmitir.

Para esto se utiliza algoritmos avanzados de manejos de cola, modeladores de tráfico (*traffic shaping*), y mecanismos de filtrado mediante listas de acceso (*Access-list*), han hecho que elegir una estrategia de QoS sea un proceso más delicado. Cada red puede tomar ventaja de acuerdo a los distintos aspectos en el desarrollo, ejecución y evaluación de algún elemento ó parámetro que permita establecer un valor de QoS determinado, con la finalidad de obtener mayor eficiencia, ya sea para redes de pequeñas, medianas, grandes empresas o proveedores de servicios de Internet.

Una red MPLS asigna a las tramas que circulan por la red una identificación que le indique a los *routers* el camino que deben seguir los datos, está identificación sirve también para la administración de QoS.
Se definen 5 clases de servicios a los cuales se asocia una calidad de servicio definida en función del manejo de prioridades para los paquetes de datos como se describe a continuación.

- **Video**. La clase de servicio para transportar video tiene un nivel de prioridad más alto que las clases de servicio para datos, debido a que no puede existir pérdida de paquetes

- ***Voz***. La clase de servicio para transportar voz tiene un nivel de prioridad equivalente al de video, es decir, más alto que las clases de servicio para datos, ya que al igual que el video no puede existir pérdida de paquetes

- ***Datos de alta prioridad*** (D1). Ésta es la clase de servicio con el nivel de prioridad más alto para datos. Se utiliza particularmente para aplicaciones que son críticas en cuanto a necesidad de rendimiento, disponibilidad y ancho de banda.

- ***Datos de prioridad*** (D2). Esta clase de servicio se relaciona con aplicaciones que no son críticas y que tienen requisitos particulares en cuanto a ancho de banda.

- ***Los datos no prioritarios*** (D3) representan la clase de servicio de prioridad más baja y son los datos en donde generalmente no se aplica ningún tipo de calidad de servicio.

1.3.2 MODELOS DE CALIDAD DE SERVICIO

1.3.2.1 Servicio del Mejor Esfuerzo *(Best Effort)*

Como su nombre lo indica es el mejor esfuerzo que realiza la red para entregar el paquete a su destino, pero no existe garantía de que esto ocurra.

Éste modelo es utilizado por las aplicaciones de FTP y HTTP. Obviamente, no es el modelo apropiado para aplicaciones sensibles al retardo o variaciones de ancho de banda.

1.3.2.2 Servicios Integrados y Protocolo de Reserva de Recursos

En un inicio la idea de calidad de servicio en Internet se denominaba "*BEST EFFORT*" la cual no ofrecía ninguna garantía respecto a la entrega de paquetes, sin embargo, con la aparición de nuevos servicios fue necesario mejorar el sistema conocido y se le definió como Calidad de Servicio mismo que busca priorizar el tráfico y tomar acciones para evitar la congestión y pérdida de paquetes.

Esta forma de aplicar calidad de servicio garantiza una reserva de capacidad de canal en todo el trayecto, como ocurre en los circuitos ATM, para esto es necesario que cada *router* intermedio tenga conocimiento de la existencia de dicho flujo.

En el año 1995 se desarrolló el modelo *IntServ* cuyo elemento más representativo fue el protocolo *RSPV* (*Protocolo de Reserva de Recursos)* sin embargo este modelo representaba un mayor costo de instalación y desarrollo

sobre todo cuando la red se expande demasiado ya que al ser un protocolo orientado a conexión, los *routers* necesitan que la información de estado de todos los flujos activos pasan por ellos, resultando inmanejable para los *routers* de *core* porque implicaría un mayor procesamiento para soportar las grandes cantidades de conexiones activas.

Se entiende como flujo, a un tráfico continúo de datagramas relacionados entre sí que se produce como consecuencia de una acción del usuario y que requieren la misma calidad de servicio.

La arquitectura *IntServ* define tres tipos de servicio:

- **Servicio Garantizado**: garantiza un throughput mínimo y un retardo máximo. Cada *router* del trayecto debe ofrecer las garantías solicitadas, aunque a veces esto no es posible por las características del medio físico (por ejemplo en *ethernet* compartida).

- **Servicio de Carga Controlada**: este servicio debe ofrecer una calidad comparable a la de una red de datagramas poco cargada, es decir en general un buen tiempo de respuesta, pero sin garantías estrictas. Eventualmente se pueden producir retardos grandes.

- **Servicio *Best Effort*:** este servicio no tiene ninguna garantía en la entrega de paquetes ni *throughput* asignado.

1.3.2.3 Servicios Diferenciados (*Diffserv*)

Diffserv es un protocolo que garantiza cierta calidad de servicio entre extremos utilizando un conjunto reducido de calidades previstas en el núcleo donde se trata de establecer una cierta diferenciación de paquetes IP tal como se puede ver en la Figura 10.

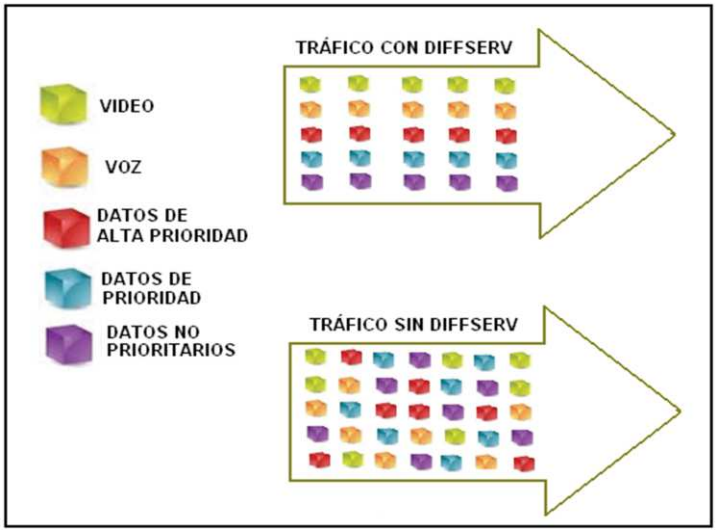


Figura 10. Diferenciación de Servicios

La calidad de servicio se percibe entre extremos (extremo A y extremo B como indica la Figura 11). En los niveles altos tenemos RSVP (*Protocolo de Reserva de Recursos)* como interfaz de programación para indicar la calidad requerida.

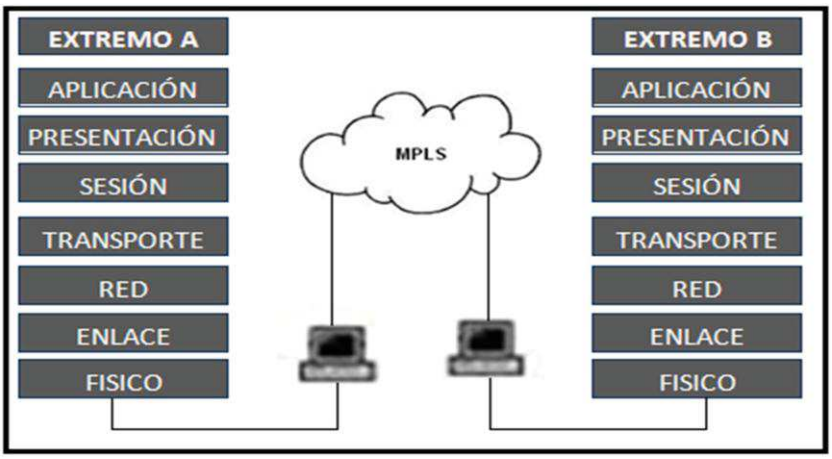


Figura 11. Capas del Modelo OSI

En MPLS cada LSP puede estar asociado a varios FEC y pueden asignarse tantos flujos de información a cada FEC como sea necesario. Esto conlleva que, a efectos prácticos, pueda elegirse qué tráfico va a ser encaminado por el LSP utilizado, pudiendo implicar con esta configuración, que la QoS sea modificada. Para especificar la clase de servicio a la que pertenece cada

paquete se utiliza en la cabecera de MPLS el campo EXP. El campo EXP es de tres bits por lo que cada paquete puede tener una de ocho posibilidades (2^3).

Fundamentalmente la diferencia que se establece entre IntServ y DiffServ es que la información para aplicar calidad de servicio es establecida en los datagramas (no en los routers) lo cual permite un servicio muy escalable permitiendo manejar una mayor cantidad de flujos de información.
En la arquitectura DiffServ se define tres tipos de servicio:

- ***Expedited Forwarding*** **"EF"**
  Cuyo valor de DSCP es '101110', ofrece la mayor prioridad en lo que se refiere a QoS, garantizando un máximo caudal, disminuyendo la tasa máxima de pérdida de paquetes, retardo medio y *jitter*.

- ***Best Effort*** **"BE"**
  Se caracteriza por tener en cero los tres primeros bits del DSCP. En este caso los dos bits restantes pueden utilizarse para marcar una prioridad, dentro del grupo 'best effort'. En este servicio no existe ninguna seguridad para saber si los paquetes serán entregados.

- ***Assured Forwarding*** **"AF"**
  AF asegura un trato diferente pero no garantiza el ancho de banda ni retardos. Se definen cuatro clases de servicio AF posibles, asignándose a cada clase una cantidad de recursos en los routers como ancho de banda, espacio en buffers, como se puede ver en la Tabla 4.
  La clase es determinada en los tres primeros bits del campo DSCP. Para cada clase se definen tres categorías de descarte de paquetes (probabilidad alta, media y baja) que se especifican en los dos bits siguientes (cuarto y quinto). Existen por tanto 12 valores de DSCP diferentes asociados con este tipo de servicio.

Tabla 4. Códigos usados en AF

	Precedencia de descarte		
Clase	**Baja**	**Media**	**Alta**
4	10001	10010	10011
3	01101	01110	01111
2	01001	01010	01011
1	00101	00110	00111

Estructura Diffserv

Para insertar la información de QoS en cada datagrama se utiliza un campo de tamaño de un byte (8bits) denominado DS, este campo a su vez se subdivide en dos subcampos como se indica en la Tabla 5

Tabla 5. Estructura de Campo Diffserv

Subcampo	Longitud (bits)
DSCP (*Differentiated Service Code Point)*	6
ECN *(Explicit Congestion Notification)*	2

DSCP (2^6) ofrece 64 posibles categorías de tráfico

ECN tiene que ver con la notificación de situaciones de congestión

El uso de los servicios diferenciados DS es la solución del IETF para los problemas asociados a los servicios integrados (IntServ). Esta solución básicamente agrupa los flujos de tráfico IP, para que los paquetes agrupados sean tratados de la misma forma en cada nodo.

A este proceso o trato realizado salto a salto se le denomina Per-hop forwarding behavior *(PHB).* Para cada uno de los grupos *PHB* al que pertenecen los paquetes se codifica el campo *DS* y su valor determinará el tratamiento que se le debe dar a ese paquete en cada tramo de la red.

Un *PHB* se refiere a la planificación del paquete, el encolamiento, la política, de un nodo en cualquier paquete dado perteneciente a un BA *(Behavior Aggregate).* Existen cuatro estándares disponibles de PHB's:

- Default PHB (PHB por defecto, RFC 2474)
- Class-Selector PHB (PHB selector de clases, RFC 2474)
- Assured Forwarding (AFny) PHB (RFC 2597)
- Expedited Forwarding (EF) PHB (RFC 2598)

En este proyecto de simulación se tomó el estándar AF *(Assured Forwarding)* y EF *(Expedited Forwarding)* ya que nos permite dividir el tráfico en las siguientes clases como se puede ver en la Tabla 6:

Tabla 6. Clasificación del tráfico:

CLASE DE TRÁFICO	***TIPO DE TRÁFICO***	***VALOR DSCP***	**ESTÁNDAR**
I	VOZ	46	EF
II	VIDEO	46	EF
III	FTP	22	AF1
	SMTP	20	AF22
	TELNET	18	AF21
IV	WWW	26	AF3

El Estándar AF de PHB define cuatro clases.

A cada una de estas clases se le asigna un específico ancho de banda de la interfaz y se pueden especificar tres valores de precedencia tal como se puede ver en la tabla 7.

Tabla 7. Valores DSCP en clase AF PHB

VALOR DE PRECEDENCIA	***CLASE1***	***CLASE2***	***CLASE3***	***CLASE4***
Bajo	001010	010010	011010	100010
Medio	001100	010100	011100	100100
alto	001110	010110	011110	100110

El estándar EF corresponde a una clase de prioridad estricta, por lo que este tráfico se retransmite antes que cualquier otro flujo de otra clase.

Diffserv utiliza 6 bits del paquete IP para codificar el tratamiento de transmisión. El encabezado del paquete IP traía, en su especificación original, un campo llamado *Type of Service (TOS, tipo de servicio),* compuesto por 3 bits de precedencia, 3 bits para especificar el servicio y dos bits reservados (siempre son cero) como se indica en la Tabla 8. Los bits de precedencia representaban prioridades para el tráfico, mientras que los bits de servicio especificaban la preferencia por throughput, delay y pérdida.

Tabla 8. Campo IP TOS

Precedencia			**D**	**T**	**R**	**0**	**0**
1	2	3	4	5	6	7	8

DiffServ redefine el campo IP TOS, denominado ahora campo DS (ver tabla 9). Los primeros 6 bits se usan ahora como punto de codificación de servicios diferenciados *(DiffServ code point, DSCP*) donde se codifica el PHB para un paquete en cada nodo DS. Los 2 bits restantes se ocupan para señalar congestión.

El DSCP es un índice a una tabla de PHBs, y el mapeo correspondiente debe ser configurable

Tabla 9. Campo DS

DSCP						0	0
1	2	3	4	5	6	7	8

Beneficios de Diffserv

La utilización de DiffServ como QoS de extremo a extremo proporciona los siguientes beneficios:

- Reduce la carga de los dispositivos de red y escala fácilmente cuando la red crece.
- Permite priorizar paquetes
- Alivia los cuellos de botella mediante la gestión eficiente de los recursos de la red.

1.3.2.4 Métodos de Calidad de Servicio que soporta Diffserv

PQ *(Priority Queuing)*

Este tipo de encolamiento consiste en clasificar el conjunto de colas desde la prioridad alta a la prioridad baja. Cada uno de los paquetes se asigna a una de estas colas, las mismas que serán atendidas en estricto orden de prioridad.

Si los paquetes de una cola de menor prioridad está siendo transmitida e ingresa un paquete de una cola de mayor prioridad, ésta será atendida inmediatamente.

Este mecanismo se utiliza en condiciones donde existe un tráfico muy relevante y debe ser transmitido inmediatamente, el inconveniente es que puede causar la total falta de atención de colas de menor prioridad (*starvation*).

WFQ (*Weighted Fair Queuing)*

WFQ soporta flujos con diferentes requerimientos de ancho de banda. Esto lo logra dándole a cada cola un peso que le asigna un porcentaje diferente del ancho de banda de salida, también soporta paquetes de longitud variable de forma que los flujos con paquetes mayores no dispongan de un ancho de banda mayor que los flujos cuyos paquetes sean de menor tamaño. Esto añade una mayor complejidad a los algoritmos de servicio de colas. Por ello, estas disciplinas de servicio de colas funcionan mejor con paquetes de longitud fija (redes ATM basadas en celdas) que con paquetes de longitud variable (redes IP)

Class-Based WFQ (CBWFQ)

Cuando se utiliza WFQ se tienen diversas limitaciones de escalamiento, ya que el algoritmo que utiliza éste se ve afectado a medida que el tráfico que cruza por enlace aumenta por cual existe la posibilidad de que el enlace se caiga debido al gran número de flujos que se requiere analizar. CBWFQ se desarrolló con el fin de evitar este tipo de limitaciones, basándose en el algoritmo de WFQ y expandiéndolo, lo que permitió crear clases definidas por el usuario, obteniendo mayor control sobre las diferentes colas de tráfico, asignando el ancho de banda específico y garantizando una determinada tasa de transmisión para cierto tipo de tráfico, lo cual no es posible mediante WFQ.

Cada clase es separada en una cola y cada uno de los paquetes que cumplen el criterio definido para una clase en particular se asocia a dicha cola. Establecido los criterios para las diferentes clases, es posible determinar cómo se manejarán los paquetes pertenecientes a dicha clase. Si cualquiera de las clases no utiliza su ancho de banda, podrán ser usadas por otras clases.

En cada clase que se pueden configurar diferentes parámetros como el ancho de banda y límite de paquetes máximos (profundidad de cola) para cada clase.

El tamaño asignado a la cola de cada clase se determina mediante el ancho de banda asignado a ésta.

LLQ (*Low Latency Queuing*)

Esta técnica de encolamiento de baja latencia clasifica el tráfico de acuerdo al protocolo, interfaz o lista de acceso, reuniendo las características de los métodos PQ y CB-WFQ.

En la actualidad es el método de encolamiento recomendado para Voz sobre IP (VoIP), Telefonía IP y Videoconferencias.
Mediante LLQ se puede definir colas de prioridad personalizadas, basadas en las clases de tráfico que se pueda manejar junto con una cola de prioridad, la cual tendrá preferencia absoluta sobre las otras colas.

Si existe tráfico en la cola de prioridad, ésta será atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su determinada prioridad. Por este comportamiento es necesario configurar un ancho de banda límite de reserva para la cola de prioridad, evitando que el resto de las colas no puedan transmitir.
En la cola de prioridad con LLQ se configura un máximo retardo para garantizar a los paquetes entrantes en esta cola, mediante el cálculo del tamaño del MTU dividida para la velocidad del enlace.

1.3.4 CALIDAD DE SERVICIO Y MPLS

Como se explicó anteriormente, la configuración de una red MPLS permite asignar a la red parámetros de calidad de servicio y lograr de este modo una transmisión de datos de mayor calidad y por lo tanto una comunicación eficiente, entre las ventajas que ofrece se había indicado la posibilidad de configurar VPNs *(Virtual Private Network)*

1.3.4.1 Redes Virtuales Privadas

Una VPN interconecta múltiples sitios sobre una infraestructura de red pública proveyendo las mismas políticas de seguridad de una red privada. Puede soportar distintos tipos de topologías como malla completa, malla parcial. *Hub* and *Spoke* y puede escalar a cientos y miles de sitios. Ésta a la vez puede proveer calidad de servicio QoS que el cliente requiera extremo a extremo.

Con una VPN en MPLS se pueden exigir niveles de *jitter* y pérdida de paquetes según la configuración del administrador de la red. Los servicios VPN pueden satisfacer los requerimientos de privacidad, flexibilidad, escalabilidad y QoS.

Las VPN tradicionales eran configuradas estableciendo líneas emuladas entre los sitios o usando túneles y *software* que se ejecutaban en el CPE (Equipo cliente). Estas tecnologías desde el punto de vista de costos no son efectivas para pequeñas empresas y no son escalables para grandes empresas. En lugar de esto los clientes pueden utilizar todo el potencial del SP (proveedor de servicios) sin la necesidad de desplegar aplicaciones VPN como servidores de autenticación, integridad y seguridad delegando estos servicios al SP.

La VPN en MPLS es configurada utilizando el protocolo BGP y por lo tanto recibe el nombre de VPN MPLS MP-BGP definida en la RFC2547 como un tipo de PPVPN *(Provider Provisioned Virtual Private Network)* propuesta por la IETF.

La operación con VPN MPLS MP-BGP tiene muchas ventajas, por ejemplo con una VPN MPLS MP-BGP el cliente que solicita la VPN tiene una topología de malla completa lo cual implica que todos sus sitios tienen comunicación directa entre ellos, esto añade redundancia, otra ventaja muy importante es la capacidad de añadir QoS extremo a extremo en la VPN, al configurar una VPN MPLS MP-BGP si tiene mayor escalabilidad ya que, en otros casos, agregar un nuevo sitio requiere configurar el correspondiente PE.

1.3.5 CALIDAD DE SERVICIO Y PROVEEDORES DE SERVICIO

En el caso de ser un proveedor de servicio o un cliente de servicio de datos es importante definir las necesidades del cliente para establecer los parámetros de calidad de servicio *QoS.*

1.3.5.1 SLA (Service Level Agreement)

El Acuerdo de Nivel de Servicio (SLA) es un contrato escrito que se realiza por proveedor de servicio y el cliente a fin de fijar el nivel acordado para la calidad de dicho servicio.

Este acuerdo permite a ambas partes llegar a un consenso en los términos de los niveles de calidad del servicio prestado, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc. Para establecer un SLA se deben tener en cuenta las siguientes consideraciones:

- Disponibilidad: se refiere al tiempo mínimo que la red se encuentra en funcionamiento y cuya responsabilidad depende el proveedor de servicios, se mide en cantidades porcentuales por ejemplo 99.99% de disponibilidad.
- Ancho de Banda: se refiere al ancho de banda mínimo que el proveedor ofrece al cliente, se mide en Bits por segundo. Por ejemplo Ancho de banda de 2 Mb/s.
- Pérdida de Paquetes: se refiere al máximo de paquetes perdidos cuya medición es porcentual y responsabilidad del proveedor de servicios siempre y cuando el cliente no exceda el ancho de banda ofrecido dentro del mismo SLA. Por ejemplo 0.1%

  Retardo: generalmente referido al retarde de ida y vuelta medio de los paquetes y medido en milisegundos.
- Jitter: referente a la variación que se produce en el retardo y medido en milisegundos.

1.4 SIMULADOR GRÁFICO GNS3

El programa GNS3 corresponde a un simulador grafico de redes que permite diseñar topologías de red y luego ejecutar simulaciones en él. GNS3 soporta IOS de routers, ATM/Frame Relay/switches Ethernet y PIX firewalls.

1.4.1 COMPONENTES DE GNS3

1.4.1.1 Dynamips

Entre los simuladores gráficos, Dynamips es un emulador de routers Cisco desarrollado por Christophe Fillot. Emula a las plataformas 1700, 2600, 3600, 3700, 7200 ejecutando imágenes de IOS estándar.

El emulador Dynamips hace uso intensivo de memoria RAM y capacidad de procesamiento del CPU es así que si se requiere ejecutar una imagen de IOS de 256 MB de RAM en un router 7200 real el GNS3 utilizará esos 256 MB de memoria RAM.
El emulador Dynamips también hace uso intensivo de CPU, porque está emulando el procesador CPU de un router instrucción por instrucción. En principio no tiene manera de saber cuándo el *router* virtual está en estado de espera (*idle*), por esa razón ejecuta diligentemente todas las instrucciones que constituyen las rutinas de idle del IOS, igualmente que las instrucciones que conforman el “real” funcionamiento. Pero una vez que haya ejecutado el proceso de “*Idle-PC*” para una determinada imagen de IOS, la utilización de CPU decrecerá en forma drástica.

1.4.1.2 Dynagen

Dynagen es una interfaz dentro de GNS3 basado en texto para Dynamips y que permite a los usuarios listar los dispositivos suspender y recargar instancias entre otros.

En la Figura 12 se muestra la ventana principal del Simulador GNS3 donde:

1. Corresponde al área donde se encuentran los dispositivos que pueden ser usados en la creación de una topología
2. Corresponde al área donde se ejecuta Dynagen, aquí se construye la red
3. Corresponde al área de Dynamips donde es posible iniciar o detener *Routers*
4. En esta área se encuentra la lista de todos los dispositivos presentes en la topología creada así como el estado en el que se encuentran y las conexiones que poseen

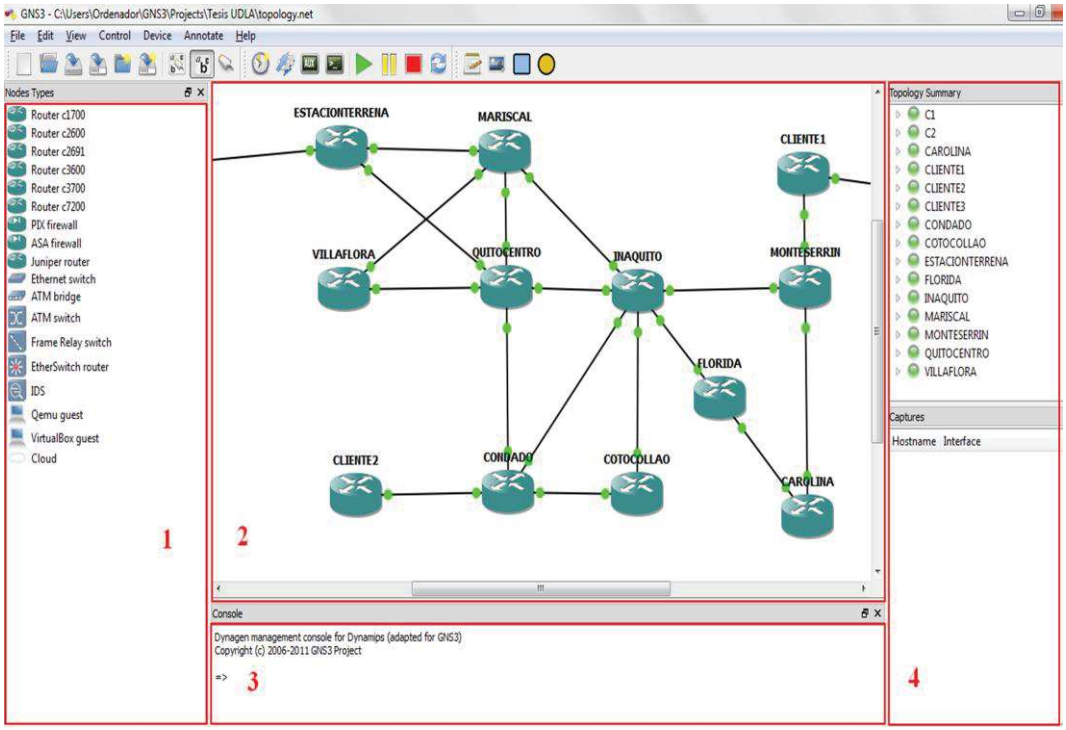


Figura 12. Ventana Principal del GNS3

CAPÍTULO II
PARÁMETROS PARA EL PROCESO DE SIMULACIÓN

En el presente proyecto se utiliza el simulador gráfico de redes *GNS3* versión 0.8.2. La simulación consta de un total de 13 ruteadores, cada uno ejecuta como sistema operativo el IOS de cisco 7200 elegidos porque estos ofrecen la capacidad de ejecutar MPLS y el protocolo IS-IS.

2.1 DIAGRAMA DE RED

En la Figura 13 se indica el diagrama de red del Core IP/MPLS de la Región Andina de la Corporación Nacional de Telecomunicaciones y que será simulada en GNS3.

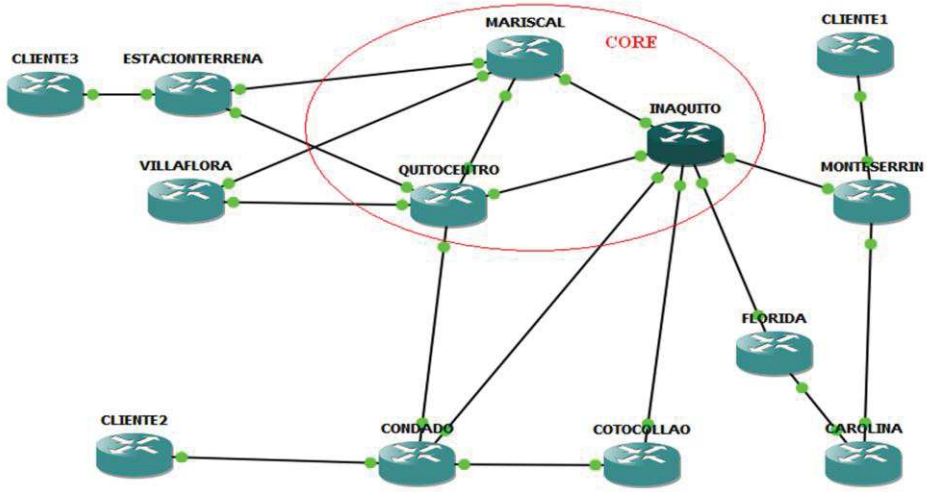


Figura 13. Diagrama de Red del Core de la Región Andina de la CNT E.P.

2.2 DIRECCIONAMIENTO

En la Figura 14 se muestra la conexión de los equipos por interfaces. De esta manera se tiene una clara visión del direccionamiento. En las Tabla 10 y Tabla 11 se muestra el subneteo y direccionamiento de la red.

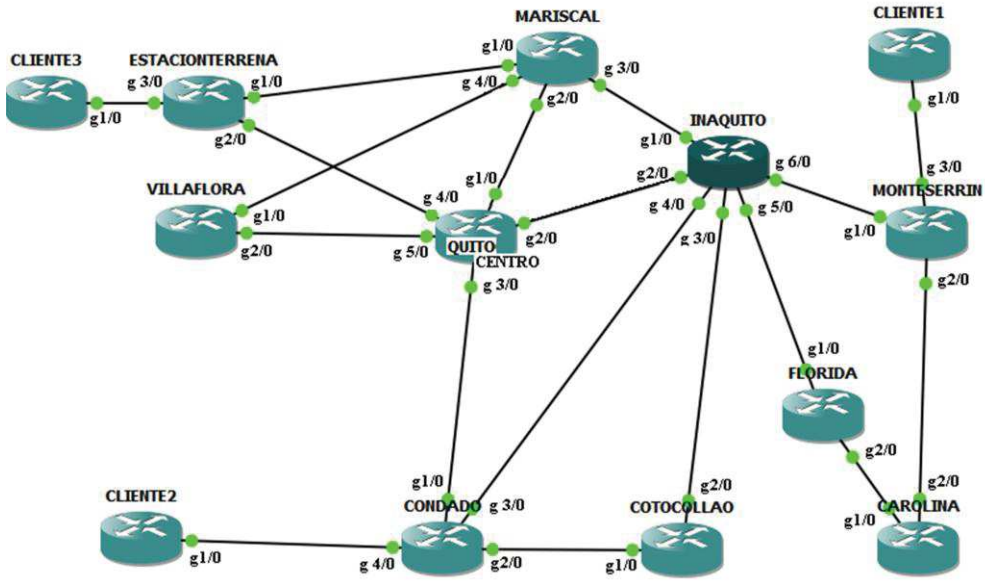


Figura 14. Interfaces por Router

Tabla 10 Tabla de Subneting

TABLA SUBNETEO		
Dirección de subred	**Dirección de broadcast**	**Máscara / 30**
192.168.1.0	192.168.1.3	255.255.255.252
192.168.1.4	192.168.1.7	255.255.255.252
192.168.1.8	192.168.1.11	255.255.255.252
192.168.1.12	192.168.1.15	255.255.255.252
192.168.1.16	192.168.1.19	255.255.255.252
192.168.1.20	192.168.1.23	255.255.255.252
192.168.1.24	192.168.1.27	255.255.255.252
192.168.1.28	192.168.1.31	255.255.255.252
192.168.1.32	192.168.1.35	255.255.255.252
192.168.1.36	192.168.1.39	255.255.255.252
192.168.1.40	192.168.1.43	255.255.255.252
192.168.1.44	192.168.1.47	255.255.255.252
192.168.1.48	192.168.1.51	255.255.255.252
192.168.1.52	192.168.1.55	255.255.255.252
192.168.1.56	192.168.1.59	255.255.255.252
192.168.1.60	192.168.1.63	255.255.255.252
192.168.1.64	192.168.1.67	255.255.255.252

Tabla 11 Tabla de Direccionamiento

TABLA DE DIRECCIONAMIENTO								
Router	**G1/0**	**G2/0**	**G3/0**	**G4/0**	**G5/0**	**G6/0**	**MSK**	**Loopback 0**
Mariscal	192.168.1.6	192.168.1.17	192.168.1.21	192.168.1.13	----------	----------	/30	10.20.1.100
Quito Centro	192.168.1.18	192.168.1.25	192.168.1.29	192.168.1.10	192.168.1.33	----------	/30	10.20.2.100
Iñaquito	192.168.1.22	192.168.1.26	192.168.1.41	192.168.1.38	192.168.1.45	192.168.1.49	/30	10.20.3.100
Estación Terrena	192.168.1.5	192.168.1.9	192.168.2.1	----------	----------	----------	/30	10.20.4.100
Villafora	192.168.1.14	192.168.1.34	----------	----------	----------	----------	/30	10.20.5.100
Condado	192.168.1.30	192.168.1.61	192.168.1.37	192.168.4.1	----------	----------	/30	10.20.6.100
Cotocollao	192.168.1.62	192.168.1.42	----------	----------	----------	----------	/30	10.20.7.100
Florida	192.168.1.46	192.168.1.58	----------	----------	----------	----------	/30	10.20.8.100
Monteserrín	192.168.1.50	192.168.1.53	192.168.3.1	----------	----------	----------	/30	10.20.9.100
Carolina	192.168.1.57	192.168.1.54	----------	----------	----------	----------	/30	10.20.10.100

2.3 COMANDOS DE CONFIGURACIÓN

2.3.1 Comandos de Configuración MPLS

- **Router(config)# ip cef**
  Este comando habilita la conmutación CEF (Cisco Express Forwarding), es de carácter obligatorio para habilitar MPLS.
  CEF es una plataforma de los procesos de conmutación de los paquetes transportados por la red a su destino. Se basa en la tabla FIB que contiene una completa información de conmutación IP. El ruteador usa la información de esta tabla para los envíos de los paquetes.

- **Router(config)# mpls label protocol ldp**
  Este Comando habilita LDP (Label Distribution Protocol), se configura en forma global y en cada interfaz. Es de carácter obligatorio para habilitar MPLS.

- **Router(config)# interface serial 1/1**
  Este comando nos permite ingresar a la interfaz para posterior mente habilitar LDP con el comando que a continuación se indica.

- **Router(config-if)# mpls label protocol ldp**
  Este protocolo habilita LDP (Label Distribution Protocol), dentro de la interfaz.

- **Router(config-if)# ip mpls**
  Este comando permite habilitar la conmutación de etiquetas (Swapping) e iniciar el protocolo LDP

- **Router(config-if)# mpls ldp router-id loopback 0**
  Este comando define una interfaz específica, en este caso la interfaz de loopback e identificará al ruteador dentro de la nube MPLS

2.3.2 Comandos de Configuración MP-BGP

- **Router(config)# Router bgp 28006**
  Este comando crea un proceso BGP en el router definiendo el número de sistema autónomo al que pertenece. En este caso el AS es 28006.

- **Router(config-router)# bgp router-id 10.20.9.100**
  Este comando especifica el router ID *(identificador del router),* en este caso es la direcci{on IP de la loopback.

- **Router(config-router)# neighbor 10.20.6.100 remote-as 28006**
  Este comando especifica la dirección IP de la interfaz de loopback en el PE del otro extremo. El sistema autónomo es el mismo ya que se tiene la misma sesión iBGP

- **Router(config-router)# address-family vpnv4**

- **Router(config-router-af)# neighbor 10.20.6.100 activate**
  Estos dos comandos seguidos permiten ingresar parámetros específicos VPN versión 4. Por defecto siempre se activa.

- **Router(config-router-af)# neighbor 10.20.6.100 send-community both**
  Este comando se usa para habilitar el transporte de comunidades estándar y extendidas a través de la sesión IBGP

- **Router(config-router)# neighbor 10.20.6.100 update-source loopback0**
  Este comando se configura ya que siempre es necesario realizar las actualizaciones BGP desde la interfaz identificada como el origen de toda actualización.

- **Router(config-router)# address-family vpn4**

- **Router(config-router-af)# neighbor 10.15.200.39 next-hop-self**
  Estos dos comandos seguidos se configuran debido a que en la tabla de enrutamiento del BGP, es importante que se defina como próximo salto *(next-hop)* al neighbor MPLS donde se originó la ruta

2.3.3 Comandos de configuración de VRF's

- **Router(config)# ip vrf datos1**
  Este comando nos permite crear la tabla VRF, en nuestro proyecto, denominada datos1 o permite ingresar a la configuración de una VRF ya existente

- **Router(config-vrf)# rd 28006:100**
  Este comando crea un RD *(router distinguisher)* que permite identificar a una tabla VRF, el número del RD fue configurado con el número del Sistema autónomo configurado en BGP, un número decimal de 32 bits.

- **Router(config-vrf)# route-target both 28006:100**
  Este comando crea especificar qué comunidad se añadirá a la dirección IPv4por medio de la opción export y también especifica las comunidades que ingresan a la tabla VRF por medio de la opción import.

- **Router(config)# router bgp 28006**
  Este comando permite ingresar al bgp que ya creamos anteriormente

- **Router(config-router)# address family ipv4 vrf datos1**

- **Router(config-router-af)# redistribute connected**

- **Router(config-router-af)# redistribute static1**
  La configuración de estos comandos permite propagar los prefijos locales al resto de equipos PE para que éstos sepan encaminar los paquetes hacia dichos prefijos

- **Router(config)# interface G3/0**

- **Router(config-if)# ip vrf forwarding datos1**

- **Router(config-if)# ip aadd 192.168.3.1 255.255.255.0**
  Estos comandos nos permiten configurar el “forwarding” en las interfaces de los routers “PE” que están conectados a los routers “CE”:

2.3.4 Comandos de configuración de calidad de servicio

- **Router(config)#access-list 101 permit udp any any range 16384 32768**

- **Router(config)# access-list 102 permit tcp any any eq www**

- **Router(config)# access-list 103 permit tcp any any eq telnet**

- **Router(config)# access-list 104 permit tcp any any eq smtp**

- **Router(config)# access-list 105 permit tcp any any eq ftp**

- **Router(config)# access-list 107 permit ip any any**

Estos comandos nos permiten configurar listas de accesos para poder filtrar el tráfico de la manera deseada, en este caso las listas de acceso fueron configuradas de acuerdo a la Tabla 12:

Tabla 12. Listas de acceso configuradas

LISTA DE ACCESO	TRÁFICO
101	Voz
102	Web
103	telnet
104	correo
105	transferencia de archivos
106	video
107	el resto de paquetes

- **Router(config)# class-map match-all EF**
- **Router(config-cmap)# match access-group 101**
- **Router(config-cmap)# exit**
- **Router(config)# class-map match-all AF1**
- **Router(config-cmap)# match access-group 105**
- **Router(config-cmap)# exit**
- **Router(config)# class-map match-all AF21**
- **Router(config-cmap)# match access-group 103**
- **Router(config-cmap)# exit**
- **Router(config)# class-map match-all AF22**
- **Router(config-cmap)# match access-group 104**
- **Router(config-cmap)# exit**

- **Router(config)# class-map match-all AF3**

- **Router(config-cmap)# match access-group 102**
  Estos comandos crean clases en las que se clasifican los paquetes en la entrada de los routers *PE*.

- **Router(config)# policy-map SETDSCP**

- **Router(config-pmap)# class EF**

- **Router(config-pmap-c)# set ip dscp 4**

- **Router(config-pmap)# class AF1**

- **Router(config-pmap-c)# set ip dscp 22**

- **Router(config-pmap)# class AF21**

- **Router(config-pmap-c)# set ip dscp 18**

- **Router(config-pmap)# class AF22**

- **Router(config-pmap-c)# set ip dscp 20**

- **Router(config-pmap)# class AF3**

- **Router(config-pmap-c)# set ip dscp 26**

  Estos comandos permiten configurar una política de tráfico en el que se especifica en nombre de la política, y a la que se asocian clases de tráfico, definidas previamente. Todo el tráfico que no se equipara con los criterios de las clases, pertenecen a la clase de tráfico por defecto.

- **Router(config)# class-map match-all “Prioridad1”**
- **Router(config-cmap)# match ip dscp 46**
- **Router(config)# class-map match-all “Prioridad2”**
- **Router(config-cmap)# match ip dscp 22**
- **Router(config)# class-map match-all “Prioridad3”**
- **Router(config-cmap)# match ip dscp 18 20**
- **Router(config)# class-map match-all “Prioridad4”**
- **Router(config-cmap)# match ip dscp 26**
- **Router(config)# policy map VoIP**
- **Router(config-cmap)# class “Prioridad1”**
- **Router(config-cmap-c)# priority 500**
- **Router(config-cmap)# class “Prioridad2”**
- **Router(config-cmap-c)# bandwidth percent 35**
- **Router(config-cmap)# class “Prioridad3”**
- **Router(config-cmap-c)# bandwidth percent 25**
- **Router(config-cmap)# class “Prioridad4”**

- **Router(config-cmap-c)# bandwidth percent 15**

  Estos comandos nos permiten marcar las clases de tráfico con los valores indicados de DSCP así como los diferentes comportamientos que tendrán los paquetes al salir del router PE,

CAPÍTULO III
SIMULACIÓN DE LA RED

3.1 SIMULACIÓN DE LA RED IP/MPLS

En base a lo establecido en el capítulo anterior donde se indican los parámetros que se usaron en la simulación de la Red IP/MPLS, se presenta a continuación el trabajo realizado en el simulador gráfico GNS3.

La instalación del programa GNS3 incluye en paquete Dynamips, cuyo software es necesario para correr GNS3 y WinPCAP que es un conjunto de librerías que se utilizan para trabajar con protocolos de red.

Una vez instalado el simulador, se construye la red tal como se muestra en la Figura 15 y se configura los r*outers* con los comandos mencionados en el capítulo 2.

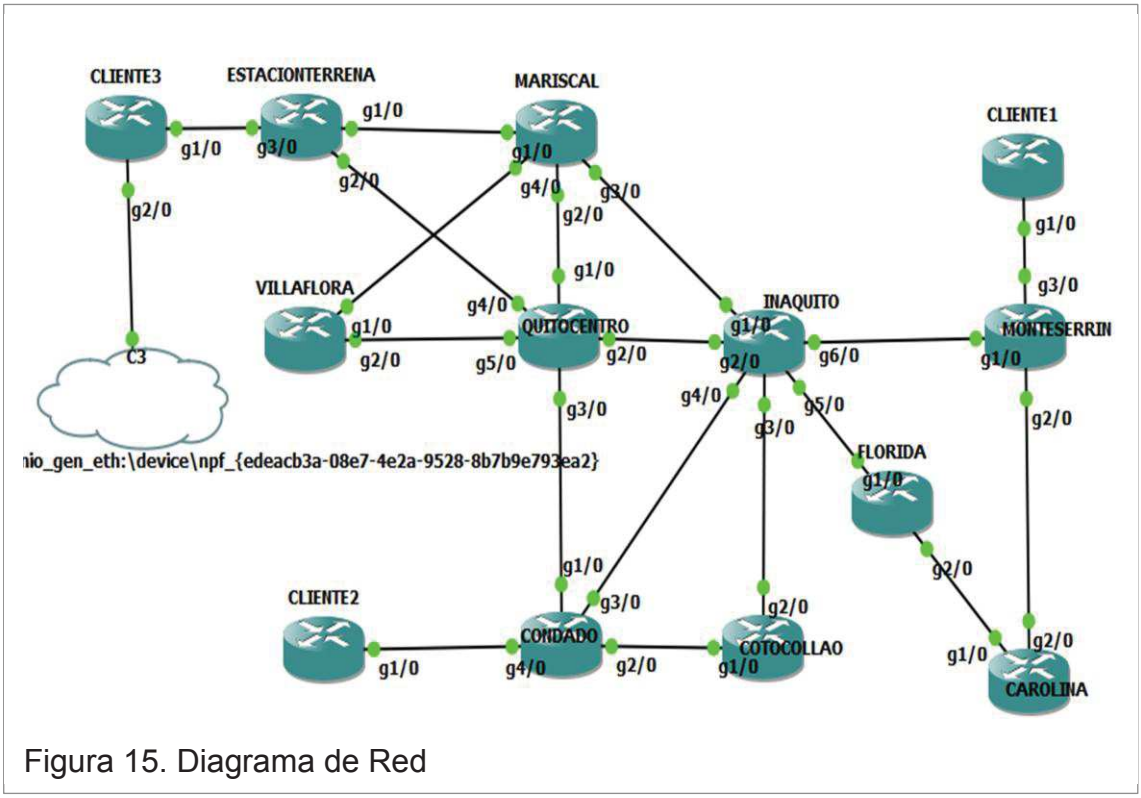


Figura 15. Diagrama de Red

A diferencia de la Figura 13, esta incluye una nube de red cuyo propósito se explica más adelante.

En los r*outers:* Estación Terrena, Villaflora, Condado, Cotocollao, Florida, Carolina, Monteserrín, Mariscal, Quito Centro e Iñaquito se configuró el protocolo MPLS.

En los r*outers* Estación Terrena, Condado y Monteserrín además se configuró la *VRF* datos1 la cual permite la comunicación entre los clientes 1, 2 y 3 así como también calidad de servicio *QoS* por ser los equipos que conectan los routers CE

Para tener una visión más gráfica de la configuración de los equipos se puede ejecutar los comandos de monitoreo en cada uno de los *routers* a fin de saber, por ejemplo, cuáles son las interfaces configuradas con el protocolo *MPLS*.

En Figura 16 se muestra la información que se despliega en el *router* Quito Centro y se puede observar que las interfaces Gigabit Ethernet de la 1/0 a la Gigabit Ethernet 5/0 están configuradas con el protocolo LDP que, como mencionamos anteriormente es importante en MPLS ya que este es el que permite la distribución de etiquetas.

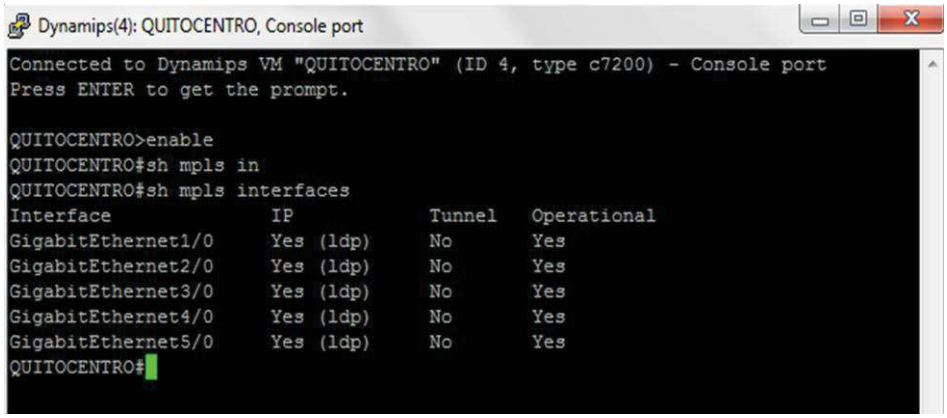


Figura 16. Interfaces MPLS del router QUITOCENTRO

Para conocer si el protocolo *MPLS* configurado está funcionando, se debe revisar si los r*outers* vecinos están siendo reconocidos, para esto se ejecuta el comando *show mpls ldp discovery* como se muestra en la Figura 17 con lo cual se obtiene el detalle de los vecinos que el *router* denominado Quito Centro ha encontrado, aquí se puede observar como resultado la dirección de loopback del vecino encontrado por LDP.

Es así que se puede deducir que el router Quito Centro tiene cinco equipos denominados “Vecinos” y cuyas direcciones de loopback son:
10.20.1.100, 10.20.3.100, 10.20.6.100, 10.20.4.100 y 10.20.5.100 y que son detectados por las interfaces Gigabit Ethernet 1/0, 2/0, 3/0, 4/0 y 5/0 respectivamente

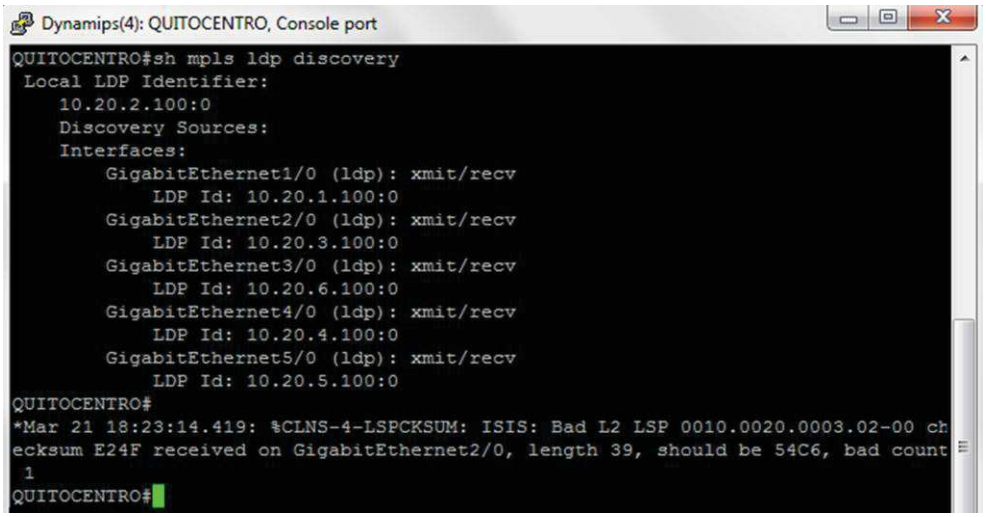


Figura 17. Routers vecinos del router QUITOCENTRO

Lo que indica el comando es correcto ya que coincide con nuestro modelo de red que se simula y se indicado en la Figura 15.

Sin embargo, si se ejecuta el comando Show mpls ldp neighbor en alguno de los *routers* que se muestra en la Figura 15 podemos observar, (para el ejemplo que tomamos router QUITOCENTRO) con mayor detalle los vecinos del mismo.

La Figura 18 muestra la información de los r*outers* que QUITOCENTRO encuentra como vecinos así como las direcciones IP que aprende a través de ellos.

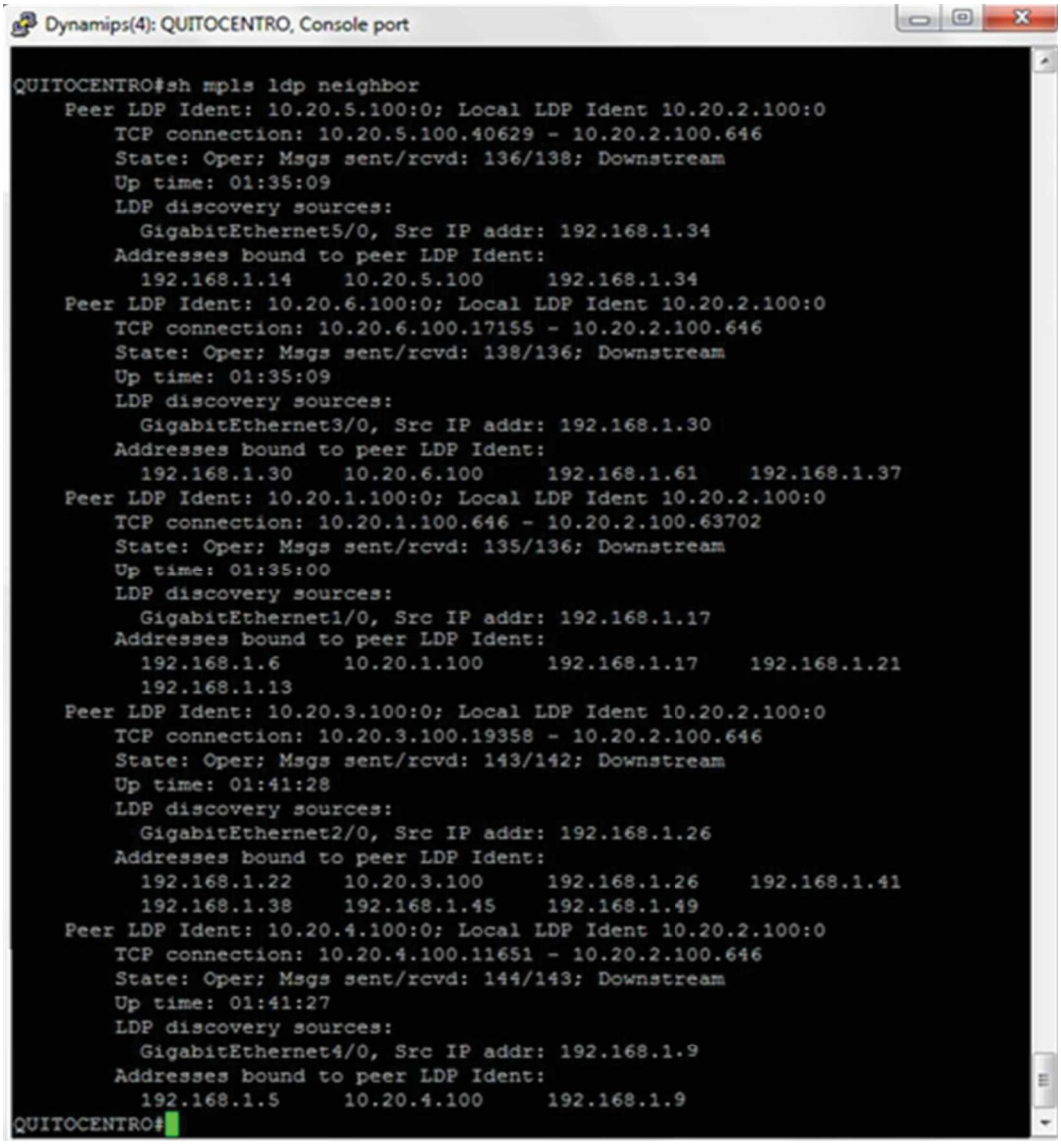


Figura 18. Detalle de routers vecinos del router QUITOCENTRO

Con este comando se puede observar además de la interfaz y la dirección de loopback de los *router* vecinos, la dirección IP que el router Quito Centro conoce a través de estos por ejemplo a través de la interfaz Gigabit Ethernet 4/0 está aprendiendo la dirección IP 192.168.1.9.

Para conocer las etiquetas en las interfaces de loopback la Figura 19 muestra el comando que se debe ejecutar

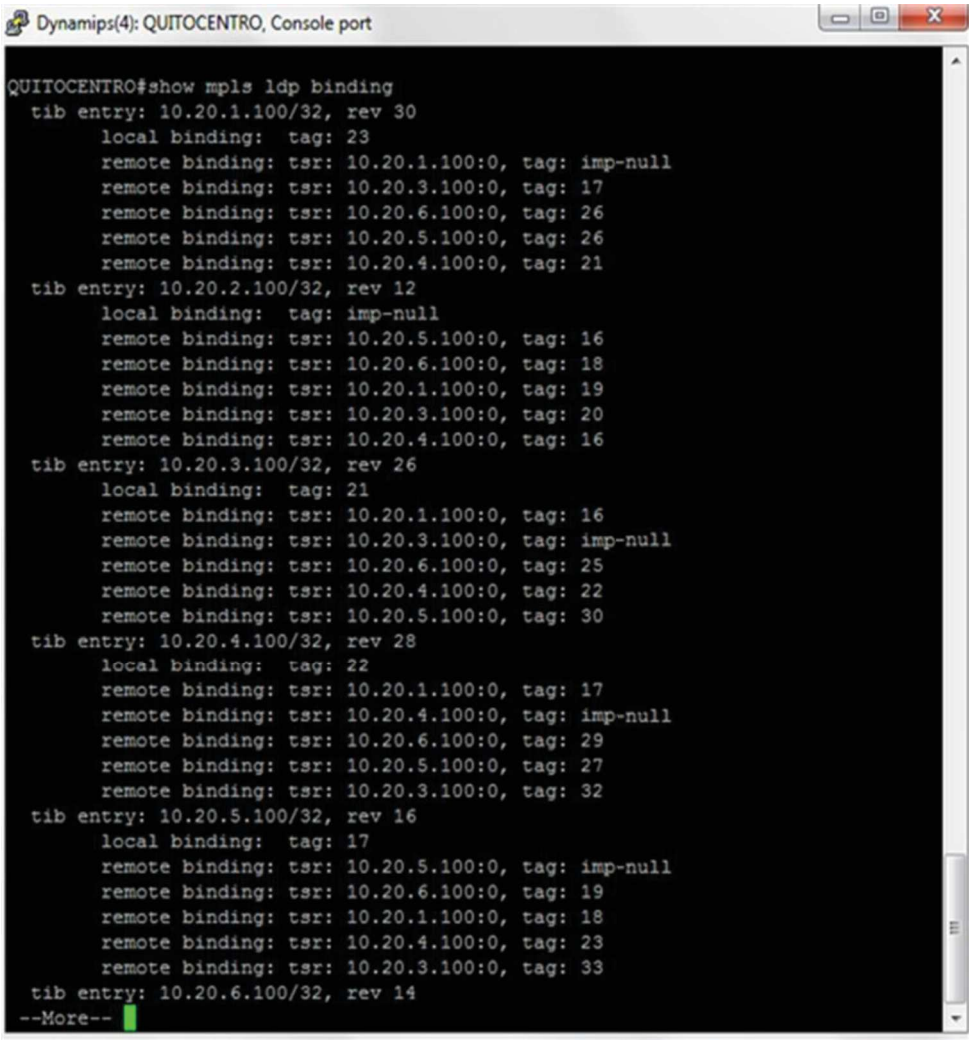


Figura 19. Detalle etiquetas

Una vez armada la red en el simulador gráfico *GNS3,* configurado el protocolo *MPLS* y configurado *VRF,* se procede a configurar calidad de servicio *QoS* en los *routers* a los que se conectan los clientes.

La noción de calidad de servicio se hace indispensable cuando nacen nuevos servicios, debido a que *TCP/IP* (*Protocolo de Control de transmisión / Protocolo de Internet*) no puede ofrecer servicios de Voz o video conferencias dado que

su funcionamiento es *Best Effort (mejor esfuerzo)* esto quiere decir que en el encabezado de los paquetes se marca el valor *DSCP* como “000000” e implica que para el transporte de estos paquetes no existe ninguna pre asignación de recursos como tampoco garantía de la entrega de dichos paquetes, por esta razón se aplican mecanismos que permitan ofrecer un trato diferenciado a los diferentes paquetes de la red y a esto llamamos Calidad de Servicio *QoS*.

Para poder dar este tratamiento diferenciado de paquetes se debe hacer uso de la prioridad y gestión de tráfico por medio de colas, por lo tanto distinguimos dos tipos de *routers* en la Figura 15:

***Routers* de Frontera:**

Estación Terrena
Condado
Monteserrín

***Routers* del Interior:**

Mariscal
Quito Centro
Iñaquito
Villaflora
Florida
Cotocollao
Carolina

Los *routers* de frontera son los encargados de la clasificación y marcado de los paquetes y por lo tanto en estos tres configuramos *QoS.*

El marcado de paquetes está relacionado con la clasificación ya que al ingresar un paquete, la marcación del mismo definirá la clase a la cual se dirigirá dicho paquete.

Se utiliza entonces, el valor de *DSCP (Differentiated Services CodePoint)* para realizar el marcado de los paquetes, en el encabezado del protocolo de Internet *IP* existe el campo *Type of Service* (tipo de servicio*)* el cual nos ofrece la posibilidad de jugar con los valores de *DSCP*. La Figura 20 muestra la cabecera *IP* y dónde se ubica el valor de *DSCP.*

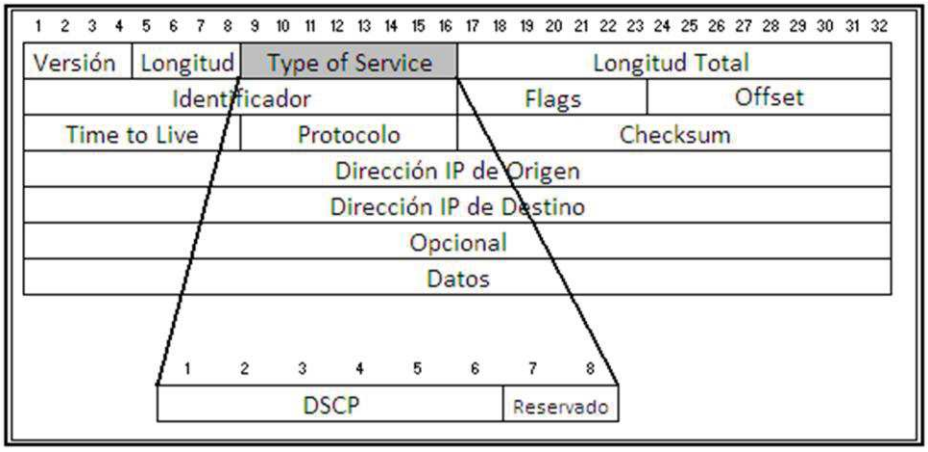


Figura 20. Cabecera IP

Donde los seis bits de mayor peso se conocen como DSCP *(Differentiated Services CodePoint)* y cuyo valor es empleado por el *router* para determinar el tratamiento que recibirá un paquete y los dos últimos bits conocidos como CU *(Currently Unused)* están reservados para usos futuros.

3.2 ANÁLISIS

Una vez que se han realizado las configuraciones y ejecutado la simulación de la red, se debe comprobar que los paquetes están siendo marcados tal como se configuró la calidad de servicio.

Para cumplir este objetivo, se incluye en el diagrama una nube de red que permita enlazar dentro del GNS3, la tarjeta de red física del computador (cuya

dirección IP es 192.168.6.2) con la finalidad de conectar a la interfaz Ethernet un equipo generador de tráfico tal como se puede ver en la Figura 21.

Figura 21. Conexión equipo IXIA

Gracias a la herramienta Wireshark se puede comprobar el paso del tráfico por el *router* Estación Terrena, para esta prueba se incluye el direccionamiento de los *routers* Cliente1, Cliente2 y Cliente3 tal como se indica en la Tabla 13.

Tabla 13 Direccionamiento Routters Cliente

ROUTER	G1/0	MSK
Cliente1	192.168.3.2	255.255.255.0
Cliente2	192.168.4.2	255.255.255.0
Cliente3	192.168.2.2	255.255.255.0

En la simulación se configura DiffServ en los routers del borde PE y de esta forma son ellos quienes realizan los trabajos de clasificación de paquetes y de acondicionamiento de tráfico; es decir, identifican a qué clase pertenece un paquete y se monitoriza si un flujo cumple con un acuerdo de servicio previo, cuyo incumplimiento llevará en algunos casos al descarte de los paquetes.

La Figura 22 es la captura de la ventana de Wireshark donde se puede apreciar que los paquetes se están marcando de acuerdo al criterio establecido en el capítulo 2,

La dirección IP de la fuente es 192.168.6.2 (dirección de red de la nube a la cual conectamos el generador de tráfico IXIA) y la dirección IP destino es 192.168.4.2 (cliente2), para el caso de transportar paquetes SMTP *(Protocolo de Simple Transferencia de Correo)* se ha marcado Assured Forwarding 22. Al comparar con la configuración realizada en el capítulo anterior tenemos que el tráfico SMTP fue clasificado en la lista de acceso 104 (comando *access-list 104 permit tcp any any eq smtp*) y esta lista de acceso marcada en el AF22 (commandos *class-map match-all AF22*, *y match access-group 104*), con lo cual se ha podido clasificar el tráfico y se ha podido establecer QoS a la red MPLS simulada.

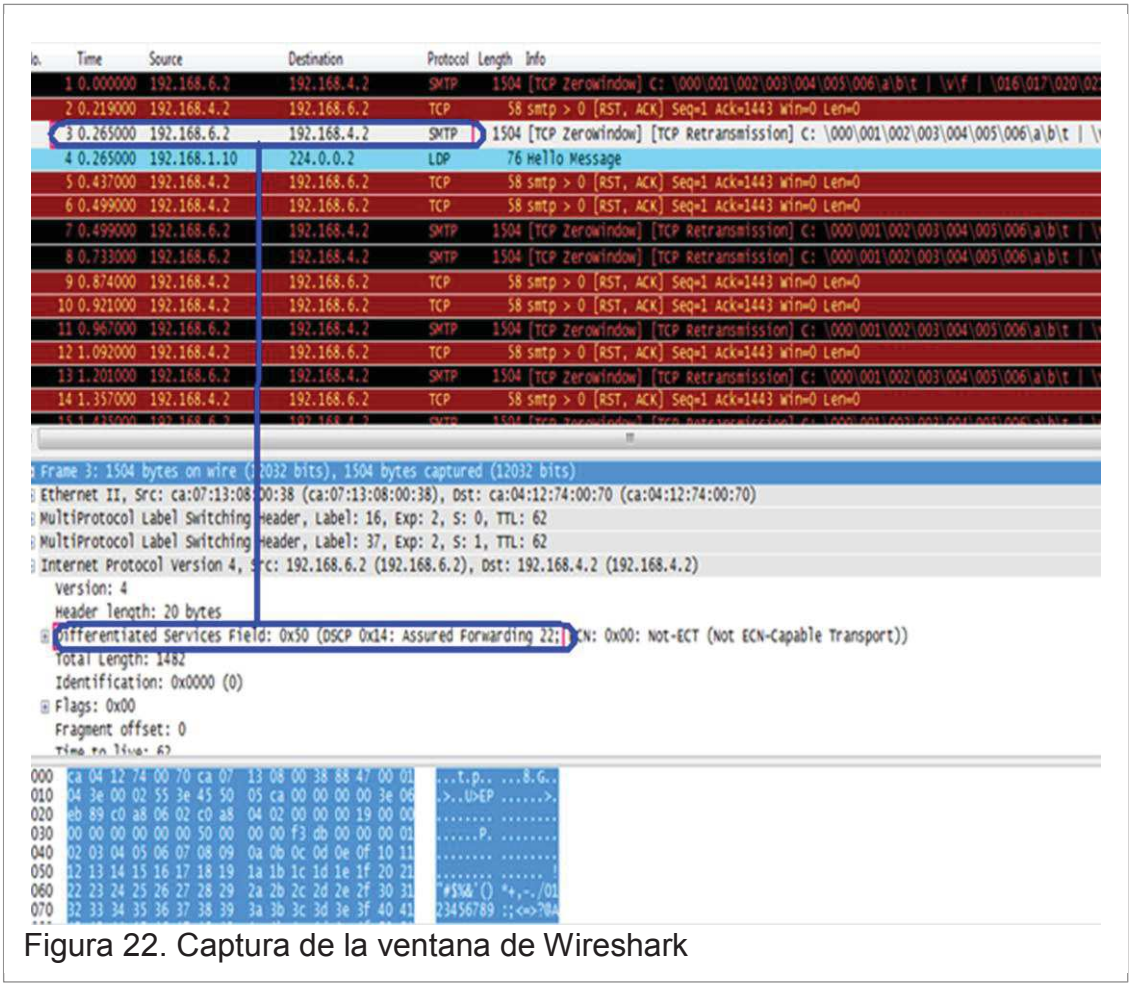


Figura 22. Captura de la ventana de Wireshark

Una vez comprobado que los paquetes están siendo marcados y debido a que se cuenta con una sola tarjeta de red se hace uso de un software generador de

tráfico (Ostinato). Este software generador de tráfico permite inyectar dos tipos de tráfico diferentes hacia la red en GNS3 a través de una única tarjeta de red. La diferencia con el equipo utilizado anteriormente para generar tráfico (IXIA) es que el IXIA necesita dos tarjetas de red para inyectar tráfico y al momento de ingresar un solo tráfico consumía grandes recursos tanto de memoria como procesador de la máquina por lo cual se continuó las pruebas con el software generador de tráfico.

Ostinato es un software generador de tráfico que trabaja en la modalidad cliente – servidor permitiendo generar el tráfico por la interfaz Ethernet hacia el GNS3. Para esto se vuelve a utilizar la nube a la cual se hace referencia en el capítulo anterior del diagrama de red.

La Figura 23 muestra la configuración del Ostinato, donde la fuente del generador de tráfico es la dirección IP fuente (donde se genera el tráfico) 192.168.6.4 y la dirección destino (hacia donde se está destinando el tráfico) 192.168.3.2 correspondiente al router Cliente1

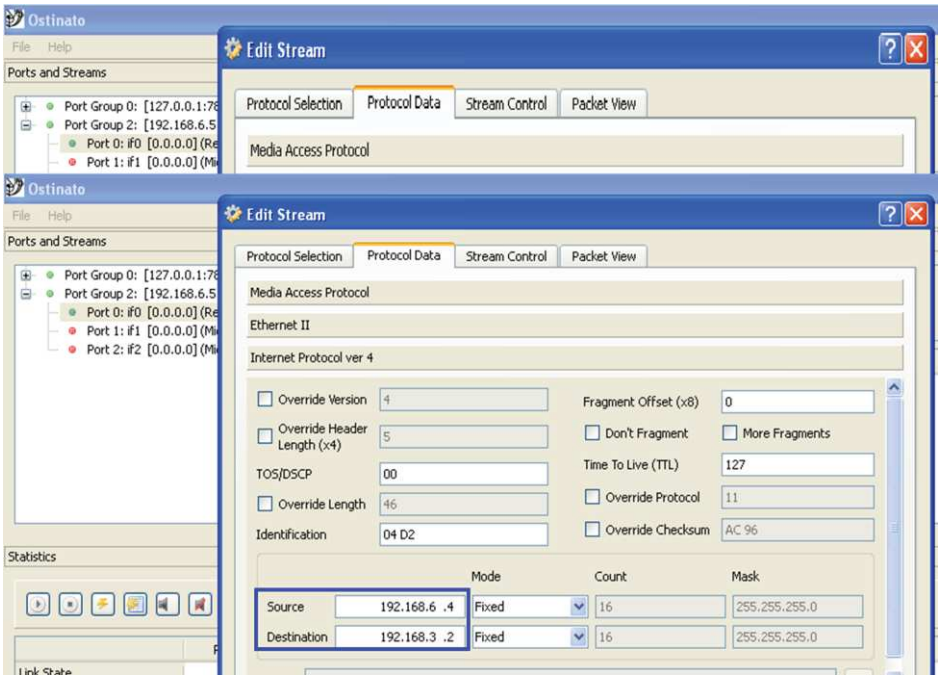


Figura 23. Configuración Ostinado

Luego se configura en Ostinato el envío de paquetes UDP hacia la dirección IP de destino y a la vez se ejecuta un ping extendido como se muestra en la Figura 24 hacia la misma dirección, de manera que al router cliente1 le lleguen paquetes ICMP y UDP simulando la generación de dos tráficos distintos cada uno con diferente trato en lo que se refiere a QoS. Los paquete UDP serán tratados como Expedited Forwarding “EF” con la más alta prioridad y el ICMP con un tráfico de menos prioridad

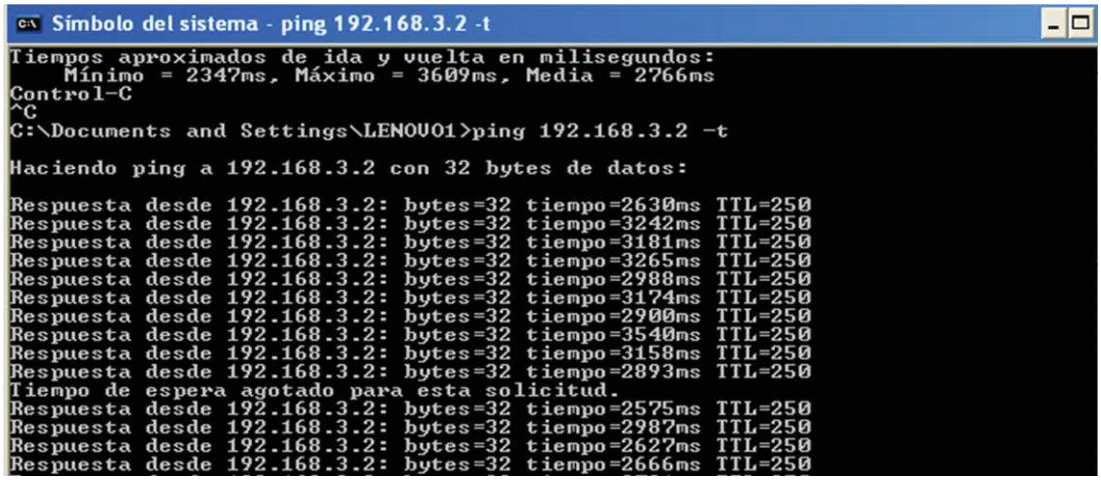


Figura 24. Ping extendido hacia la dirección destino

Con la finalidad de observar que los paquetes UDP tienen prioridad sobre los paquetes ICMP (configuración de QoS), se utiliza la herramienta wireshark donde se captura los paquetes. Se observa que los paquetes ICMP están llegando en forma continua, sin embargo al enviar un paquete UDP, este es tratado con la más alta prioridad y se antepone a los de ICMP, comprobando la simulación tal como se muestra en la Figura 25.

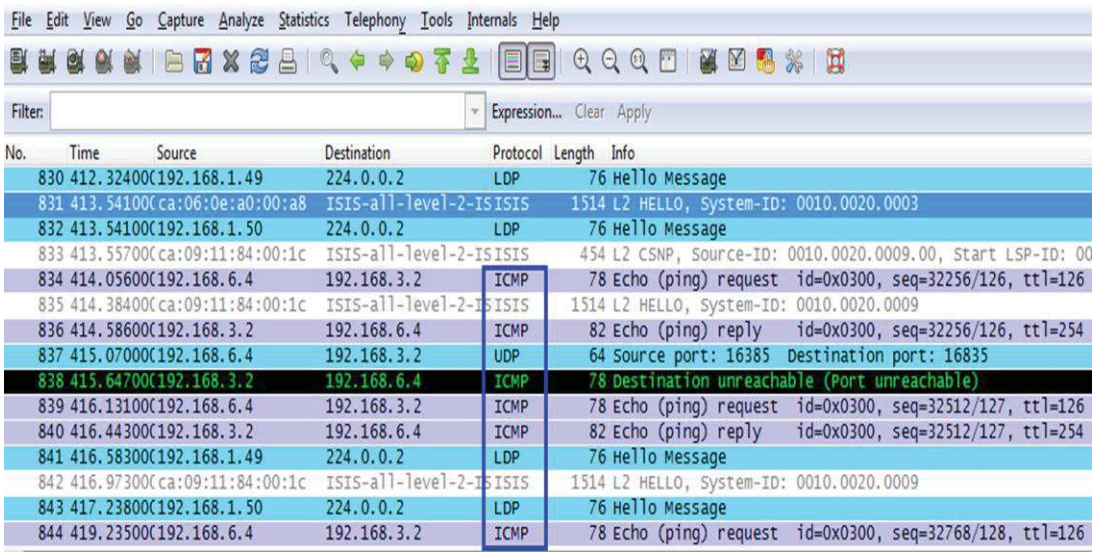


Figura 25. Captura paso de tráfico ICMP-UDP

CAPÍTULO IV
CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Se concluye que en una red MPLS al ser enviados los paquetes en función de las etiquetas permite un transporte de paquetes más rápido debido a que no es necesario examinar completamente la cabecera de red. Es importante aclarar que el protocolo MPLS no remplaza al protocolo IP. En el trasporte de paquetes, cada un es clasificado en base a las clases de tráfico denominadas FEC (Forwarding Equivalence Class).

- Se concluye que la operación con VPN MPLS MP-BGP tiene muchas ventajas sobre una VPN normal, por ejemplo con una VPN MPLS MP-BGP el cliente que solicita la VPN tiene una topología de malla completa lo cual implica que todos los sitios tienen comunicación directa entre ellos, esto añade redundancia, otra ventaja muy importante es la capacidad de añadir QoS extremo a extremo en la VPN, al configurar una VPN MPLS MP-BGP se tiene mayor escalabilidad ya que, en otros casos, agregar un nuevo sitio requiere configurar el correspondiente PE.

- Los paquetes pueden ser transportados por un router dentro de la red sin que todas las interfaces estén configuradas con el protocolo mpls sin embargo no siempre sucede y no es efectivo por lo que los comandos "*mpls ip"* y *"mpls label protocol lsp"* deben ser ejecutados en todas las interfaces de cada router de esta manera se habilita el protocolo LDP *(Label Distribution Protocol)* y comienza el intercambio de etiquetas entre los routers vecinos.

- Las interfaces a las cuales se conectan los clientes CE (*Customer Edge)* de los Routers PE como son: Estación Terrena, Condado y Monteserrín no

deben ser configuradas con MPLS ya que este modo de transporte es transparente para el cliente.

- En MPLS los paquetes son enviados en base a una consulta de etiqueta MPLS y no en base a la consulta de la cabecera IP del paquete.

- Cualquier enrutador equipo Provider que esté dentro del LSP no tendrá conocimiento de las tablas de enrutamiento IP ni de las etiquetas VPN entre los enrutadores Provider Edge.

- Para obtener el servicio de VPN *(Vittual Private Network)* se debe primero configurar una VRF *(Virtual Routing and Forwarding)*. La VRF es una tabla de enrutamiento y envío VPN que se configuran en los routers PE. Dependiendo a que PEs se conecte cada sitio se tendrá el número de VRFs a configurar.

- La función del protocolo BGP *(Border Gateway Protocol)* es permitir la interconexión de dos sistemas autónomos mediante el uso de una conexión TCP *(Transmission Control Protocol)* establecida entre dos ruteadores de borde. Se puede dar un giro al uso de BGP en contexto de las redes VPN basadas en MPLS de modo que permita intercambiar rutas dentro de las mismas VPN's en otras palabras, el BGP permite intercambiar rutas de un PE a otro PE y cuando trabaja de esta manera, se denomina MP-BGP *(Multiprotocol BGP).*

- Las etiquetas que encontramos en la tabla LIB se generan por las etiquetas remotas de los vecinos, las etiquetas de la tabla LFIB se generan por una etiqueta local y una remota, al caer uno de los enlaces, las tablas MPLS cambian.

- Las sesiones MP-BGP deben ser ejecutados entre las interfaces de loopback ya que estas siempre se encuentran en un estado "UP" sin

riesgos de mal funcionamiento debido a interfaces caídas o dañadas ya que la interfaz loopback es una interfaz lógica.

- Se concluye que DiffServ se configura sólo en los routers del borde PE ya son ellos quienes realizan los trabajos de clasificación de paquetes y de acondicionamiento de tráfico; es decir, identifican a qué clase pertenece un paquete y se monitoriza si un flujo cumple con un acuerdo servicio previo, cuyo incumplimiento llevará en algunos casos al descarte de los paquetes fuera del acuerdo.

- La aplicación del protocolo *MPLS* es transparente para el usuario ya que, como se muestra en la simulación, es configurada únicamente por el proveedor de servicio de datos. El cliente únicamente se conecta al *router PE* del proveedor y este se encarga de proporcionar la ruta hacia el destino.

- Se concluye que la Calidad de Servicio puede ser aplicada de diferentes formas como Servicios Integrados usando el protocolo de reserva RSVP que aunque ofrecen mayor garantía necesitan de un protocolo de reserva para los diferentes flujos, lo cual en una red grande arrastra problemas de escalabilidad ó Servicios Diferenciados los cuales se basan en marcado y encolamiento y es la que hemos utilizado en esta simulación ya que ofrece mayor flexibilidad y escalabilidad, y al hablar de Flexibilidad y escalabilidad en las redes de comunicaciones nos referimos a la capacidad que otorgamos a la red de tal manera que cuando se incremente la capacidad no se interrumpa los servicios existentes en ella así como evitar que se pierda la calidad de transporte que se ofrece en ella y la configuración al momento de extender la red.

- Se concluye que es necesario en MPLS la configuración de BGP *(Border Gateway Protocol)* para poder levantar VPN (*Virtual Private Network)*

- La simulación de la red IP/MPLS de la Corporación Nacional de Telecomunicaciones con QoS permitirá mejorar el rendimiento de la red y por lo tanto, mejorar la eficiencia en los actuales servicios que brinda esta empresa. Por ejemplo mejorar los servicios de internet, telefonía IP, o desarrollo de nuevos servicios basándose en el protocolo de internet, como el ya creciente video sobre IP.

- Es conveniente indicar que GNS3 es solo un software de emulación por lo cual es necesario un sistema operativo IOS que emular. Este software puede ser descargado mediante una cuenta Cisco.

- Se concluye que BGP facilita el tráfico en esquemas de redistribucion y exportación de rutas desde y hacia inter-conectividad entre VRFs de proveedores de servicios

4.2 RECOMENDACIONES

- Una vez que se han definido los diferentes métodos para configurar Calidad de servicio, se recomienda el modelo diffserv por las condiciones analizadas en la Tabla 14:

Tabla 14 Cuadro comparativo de Modelos de QoS

Modelo de *QoS*	**Características**		**Calificación**
Best Effort	todo tráfico tiene la misma importancia Gran escalabilidad Fácil implementación Sin garantía para el tráfico	X √ √ X	no
Servicios Integrados	Usa protocolo de señalización Provee garantías de ancho de banda Control end to end modelo no escalable Mayor complejidad de instalación Gran garantía de QoS Cada flujo necesita señalización	X √ √ X X √ X	no
Servicios Diferenciados	Menor garantía de QoS que Servicios Integrados Diferenciación de tráfico No requiere señalización Usa técnicas de control y admisión Implementación menos compleja Permite escalabilidad	X √ √ √ √ √	si

Además de que la arquitectura DiffServ satisface requisitos como proporcionar altas prestaciones, escalabilidad, permitir el crecimiento sostenido del tamaño de las redes y su ancho de banda, etc.

- Para un mejor control de tráfico se recomienda crear listas de acceso (a*ccess list)* asignando un rango de puertos de entrada, tal como en la simulación, usando el comando *access-list* de esta manera se consigue filtrar el tráfico que entra en el *router* para que pueda ser clasificado.

- Se recomienda tener enlaces redundantes en El core (*Núcleo)* de la red.

- Más que una recomendación es imprescindible que los ruteadores Provider *P* se conecten solamente con ruteadores Provider Edge *Pe* y con otros enrutadores Provider *P*, los ruteadores *PE* pueden conectarse con ruteadores *P, PE y CE*, los ruteadores Customer Edge *CE* pueden conectarse solamente a enrutadores PE, los ruteadores CE no ejecutan por sí mismo ningún tipo de proceso de conmutación de etiquetas por lo que MPLS no se configura en estos *Routers*.

Para aclarar este punto se analiza la Figura 26, objeto de simulación de este proyecto, donde se indica la ubicación de estos routers. En un dominio MPLS a los ruteadores de borde se les llama PE *(Provider Edge)* y a los ruteadores de núcleo P (Provider). Los PE son los encargados de añadir la cabecera MPLS a cada paquete IP que ingrese a la WAN, los P conmutan las etiquetas contenidas en las cabeceras MPLS.

Esto significa que por cada P que atreviese un paquete IP el valor de la etiqueta cambia, esta conmutación de etiquetas a lo largo de la ruta de un flujo de paquetes IP crea lo que se conoce como ruta conmutada por etiquetas.

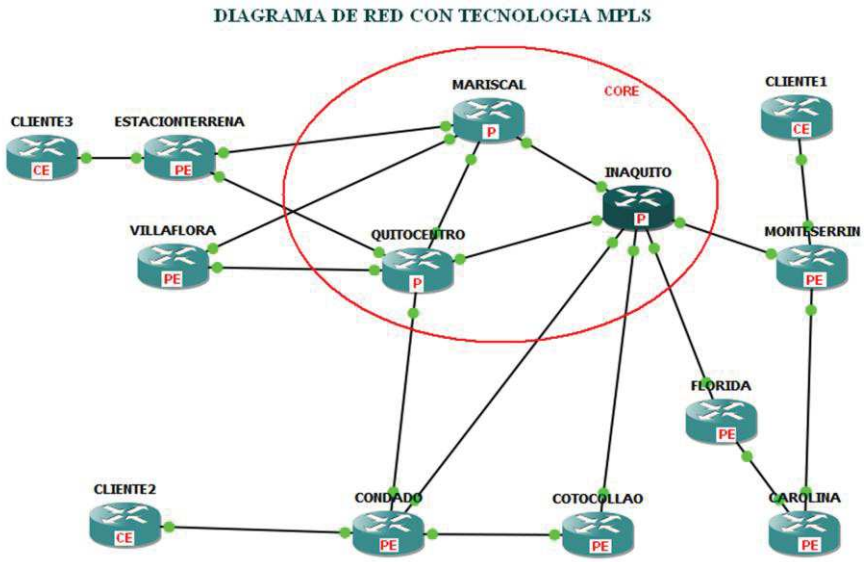


Figura 26. Diagrama de Red del Core de la Región Andina de la CNT E.P

- Se recomienda habilitar LDP por interfaz ya que existen interfaces en los PE *(Provider Edge)* que salen del dominio de la WAN y por ende no requieren ser habilitadas para MPLS/LDP.

- Se recomienda configurar las interfaces de loopback en cada router porque esto permite mayor convergencia ya que siempre se encuentra en estado "*up"* es decir activo.

REFERENCIAS

Alarcón, R. (2010). Estudio e Implementación de Mecanismos de Calidad de servicio sobre una Arquitectura de Servicios Diferenciados. Recuperado el 17 de enero de 2012.de http://repositorio.bib.upct.es/dspace/bitstream/10317/184/1/pfc908.pdf,

Álvarez, G. (2005). Estudio y configuración de calidad de servicio para protocolos ipv4 e ipv6 en una red de fibra óptica WDM. Recuperado el 16 de enero de 2012 de http://www.scielo.cl/pdf/rfacing/v13n3/art15.pdf,

Angulo, M. (2008). MPLS. Recuperado el 11 de Agosto de 2011 de http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml.

Barberá, J. (2010). Una arquitectura de backbone para la Internet del siglo XXI. Recuperado el 17 de febrero de 2011 de http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

H3C, (2012). MPLS OPERATION. Recuperado el 20 de enero de 2012 de http://www.h3c.com/portal/Technical_Support_Documents/Technical-_Documents/Security_Products/H3C_SecPath_F100-M/Configuration/Operation_Manual/H3C_SecPath_Series_Security_Prod-ucts_OM(V1.04)/200706/207235_1285_0.htm.

Icaran, (2011). Estudio y configuración de una VPN MPLS MP-BGP, recuperado el 20 de enero de 2012 de http://www.google.com.ec/url?sa=t&rct=j&q=configuracion%20mpbgp&source=web&cd=1&ved=0CCEQFjAA&url=http%3A%2F%2Fprofesores.elo.utfsm.cl%2F~agv%2Felo323%2F2s10%2Fprojects%2FMauricioIcaran%2FVPN%2520publiF.doc&ei=QdYZT9C2G8_qtgfc0uG5Cw&usg=AFQjCNGVhTIwB3Gp1nOMn0fzbqIsJ2wsng.

Jeff, (2008). Conmutación de etiquetas multiprotocolo**.** Recuperado el 10 de Agosto de 2011 de http://es.kioskea.net/contents/internet/mpls.php3.

Jiménez, G., González, R. (2011). Integración de MPLS y DiffServ en una Arquitectura para la Provisión de QoS. Recuperado el 18 de agosto de 2011.de http://docs.google.com/viewer?a=v&q=cache:3tH-qFbjFqIJ:gitaca.es/javiercg/uploads/ES/jimenez05jitel.pdf+diffserv+qos+en+mpls&hl=es&gl=ec&pid=bl&srcid=ADGEESgC81cXVYzXNuyhrygWHDiApYb8drDUnILujDBe-SsrBrlvJJZ-yfDksjvJAa_xl-RZgvcBP8lFg4MPF7sPwvVWdWqEO693xLFdPOJTe2dGGl-Oou0fVSvzpiqkujPtIq_c_Je7&sig=AHIEtbTgH5JLtMwPClB4WWot76p8EbQz-g

Montaña, R. (2011). CALIDAD DE SERVICIO (QOS). Recuperado el 18 de agosto de 2011.de http://www.securisite.org/biblioteca/seguridad/Ingenieria%20Telematica-curso/TELE_16-Calidad%20de%20Servicio/ampli_3.pdf.

Tanenbaum, A. (Eds.) (2003). Redes de Computadoras. (4a. ed.). México, México: Prentice Hall.

Valencia, F. (2011), Cisco Certified Internetwork Expert. Recuperado el 2 de abril de 2012 de http://es.scribd.com/doc/76603077/201/LLQ-LOW-LATENCY-QUEUING,

ANEXOS

MODOS DE CONFIGURACIÓN DE UN ROUTER

Modo	Permite	Símbolo
USUARIO	Consulta de Información	Router >
PRIVILEGIADO	Visualizar el estado del router	Router #
CONFIGURACIÓN GLOBAL	Utilizar comandos generales de configuración	Router (config) #
CONFIGURACIÓN DE INTERFACES	Utilizar comandos de configuración de interfaces	Router (config-if) #

COMANDOS BÁSICOS Y DE INICIALIZACIÓN

Comando	Función
Router> enable	Permite ingresar al modo privilegiado del router
Router# configure terminal	Permite ingresar el modo de configuración global del router
Router(config)# hostname ESTACIONTERRENA	Permite cambiar el nombre que se asignará al router, para el ejemplo el nombre es ESTACIONTERRENA

COMANDOS DE CONFIGURACIÓN DE INTERFACES

Comando	Función
Router(config)# interface giga 1/0	Permite ingresar al modo de configuración de interfaces, en este caso se ingresará a la interfaz Giga Ethernet 1/0 del router
Router(config-if)# ip address 192.168.1.37 255.255.255.252	Permite asignar una dirección IP y una máscara de red a la interfaz.
Router(config-if)# no shutdown	Este comando levanta la interfaz.
Router(config-if)# exit	Permite salir del modo de configuración de interfaz.
Router# write	Permite grabar la configuración realizada en el router.
Router(config)# interface loopback 0	Permite ingresar en la interfaz de loopback.
Router(config-if)# ip add 10.20.10.100 255.255.255.255	Permite asignar la IP de loopback

COMANDOS DE MONITOREO

Comando	Función
Router# show mpls ldp parameters	Despliega los parámetros LPD en el ruteador local, muestra las interfaces en las cuales está funcionando el protocolo MPLS.
Router# show mpls interfaces	Despliega el estado de MPLS en cada interfaz.
Router# show mpls ldp discovery	Despliega todos los neighbors descubiertos.
Router# show mpls ldp neighbor	Despliega información sobre los neighbors LDP.
Router# show mpls ldp bindings	Despliega la Base de Información de Etiqueta (LIB)
Router# show mpls forwarding-table	Despliega el contenido de la LFIB
Router# show ip cef	Despliega las entradas en la FIB
Router# show ip bgp vpnv4 all summary	Despliega la información de bgp configurada
Router# show class-map	Despliega la información de todas las clases de tráfico configuradas en el router.
Router# show policy-map	Muestra todas las políticas de tráfico configuradas
Router# show class-map	Muestra las clases que se han configurado

GLOSARIO DE TÉRMINOS

SIGLA	DEFINICIÓN
ATM	*Modo de Transferencia Asíncrono*
BGP	*Border Gateway Protocol*
CE	*Customer Edge*
CEF	*Cisco Express Forwarding*
	(proceso de conmutación más rápido, propietario Cisco)
CEF	*Cisco Express Forwarding*
DIFFSERV	*Diferenciación de Servicio*
DS	*Diffserv*
DSCP	*Differentiated Service CodePoint*
ECN	*Explicit Congestion Notification*
FEC	*Forwarding Equivalence Class*
FORWARDING	*Reenvío de paquetes*
GNS3	*Simulador Gráfico de Redes*
IEFT	*Internet Engineering Task Force*
IGP	*Internal Gateway Protocol*
IOS	*Internetworking Operating System*
IP	*Protocolo Internet*
IS-IS	*Intermediate System To Intermediate System*
LAN	*Red de Área Local*
LDP	*Label Distribution Protocol*
LIB	*Label Information Base*
LLQ	*Low Latency Queuing / Encolamiento de baja latencia*
LSP	*Label Switching Path*
LSP	*Label Switching Path*
LSR	*Label sitching Router*
LSR	*Label Switching Router*
MP-BGP	*Multiprotocol BGP*
MPLS	*Multiprotocol Label Switching*

OSPF	*Open Shortest Path First*
P	*Provider*
PE	*Provider Egde*
PHB	*Per-hop forwarding behavior*
PIX FIREWALL	*Private Internet eXchange*
PQ	*Priority Queuing*
QoS	*Quality of Service*
RIP	*Routing Information Protocol*
ROUTING	*Control de Paquetes*
RSVP	*Protocolo de Reserva de Recursos*
SLA	*Service Level Agreement*
TCP	*Transmission Control Protocol*
TDP	*Tag Distribution Protocol*
TTL	*Time to Live*
VPN	*Vitual Private Network*
VRF	*VPN Routing and Forwarding*
WFQ	*Weighted Fair Queuing / Espera Equitativa Ponderada*