ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

"EVALUACIÓN DE UNA RED MPLS USANDO DIFFSERV PARA MEJORAR EL RENDIMIENTO EN APLICACIONES CON QoS"

PAULINA FERNANDA CHACHA LLANGA

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGISTER EN SISTEMAS DE TELECOMUNICACIONES

Riobamba – Ecuador

Abril-2019

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado "Evaluación de una red MPLS usando Diffserv para mejorar el rendimiento en aplicaciones con QoS**",** de responsabilidad de la Sra. Paulina Fernanda Chacha Llanga ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Lic. Pepita Alarcon Parra M.Sc. **PRESIDENTE**	FIRMA
Ing. Oswaldo Martínez Guashima M.Sc. **DIRECTOR**	FIRMA
Lic. Raúl Lozada Yánez M.Sc. **MIEMBRO**	FIRMA
Ing. Vinicio Ramos Valencia M.Sc.	FIRMA

Riobamba, abril 2019

DERECHOS INTELECTUALES

Yo, Paulina Fernanda Chacha Llanga soy responsable de las ideas, doctrinas y resultados expuestos en este Trabajo de Titulación y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica de Chimborazo.

PAULINA FERNANDA CHACHA LLANGA

N° Cédula: 0604135483

Yo, Paulina Fernanda Chacha Llanga, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

PAULINA FERNANDA CHACHA LLANGA
N° Cédula: 0604135483

DEDICATORIA

Este trabajo va dedicado a mis padres quienes han sido el mejor ejemplo de perseverancia y dedicación, a mis suegros quienes han sido como mis segundos padres y me acogieron con amor en sus vidas, a mi esposo Fausto que ha sido mi fortaleza y a mis dos luceros: Stefanny y Valentina que son la razón de mi vida y también me la dedico a mí, a esa mujer, esposa, madre y profesional que siempre tendrá sueños por cumplir.

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios, porque en cada paso que he recorrido ha estado presente su amor infinito, demostrándome su presencia por medio de las personas buenas que he conocido y me han impulsado para hoy ver realizado uno más de mis sueños, es así que agradezco a mi tutor Ing. Oswaldo Martínez y a mis correctores los Ingenieros Raúl Lozada y Vinicio Ramos por todo el apoyo y motivación.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ABREVIATURAS

ACRÓNIMO	SIGLAS O ACRÓNIMOS
ATM	Asynchronous Transfer Mode
AToM	Any Transport over MPLS
BGP	Border Gateway Protocol
CBWFQ	WFQ basado en clases
CQ	Custom Queueing
CR-LDP	Constraint-Route Label Distribution Protocol)
DiffServ	Servicio Diferenciado
DS	Servicios Diferenciados
FEC	Forwarding Equivalence Class
FIFO	Primero en entrar, primero en salir (First-In, First-Out)
GNS3	Graphical Network Simulator
GNS3	Simulación Gráfica de Redes (Graphic Network Simulation)
IETF	Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force)
IGP	Protocolo de Compuerta Interior (Interior Gateway Protocol)
ISP	Proveedor de servicio Internet (Internet Service Provider)
LDP	Protocolo de Distribución de Etiquetas
LER	Label Edge Router
LFIB	Base de información de reenvío de etiquetas (Label Forwarding Information Base)
LIB	Label Information Base
LLQ	Low Latency Queueing
LSP	Label Switched Path
LSR	Label Switched Router
MPLS	Conmutación por etiquetas multiprotocolo (Multiprotocol Label Switching)
MTOP	Ministerio de Transporte y Obras Públicas
NS3	Network Simulator
PHBs	Per Hop Behavoir
PHP	Penultimate Hop Popping
PQ	Priority Queueing
QoS	Calidad de Servicio (Quality of Service)
RSVP-TE	Resource Reservation Protocol – Traffic Engineering

SLAs	Service Level Agreements
ToS	Tipo de Servicio (Type of Service)
VoIP	Voz sobre el Protocolo de Internet (Voice over Internet Protocol)
VPN	Red Privada Virtual (Virtual Private Network)
WFQ	Weighted Fair Queueing
ETSI	European Telecommunications Standards Institute

RESUMEN

El propósito de esta investigación fue definir y evaluar una red MPLS (Multiprotocol Label Switching) con Servicio Diferenciado para mejorar los parámetros de calidad y servicio de aplicaciones en tiempo real como: transmisión de VoIP, video conferencias, etc. Este tipo de aplicaciones requieren de bajo retardo, baja pérdida de paquetes en la transmisión de extremo a extremo para garantizar la Calidad y Servicio (QoS, Quality of Service). Esto se logró con la arquitectura MPLS y Servicio Diferenciado definida en el RFC 2474 "Definition of the Differentiated Services Field (DS Field)" donde básicamente lo que se hizo fue marcar el tráfico en la etiqueta MPLS indicando la prioridad del paquete enviado para que en caso de congestión los paquetes de mayor importancia sean los primeros en ser reenviados se aplicó 5 clases de servicio de prioridades, estas clases se denominan Premium, Oro, Plata, Bronce y mejor esfuerzo las mismas que corresponde a tráficos ordenados de acuerdo a la prioridad de llegada a su destino. Mediante el inyector de tráfico D-ITG se generó el tráfico de voz, streaming y datos y se evaluaron los parámetros de delay, jitter y pérdida de paquetes del tráfico que recorre la red MPLS con Servicio Diferenciado. Los resultados obtenidos se encuentran dentro de los umbrales adecuados según los estándares de la UIT-T G.1010, UIT Y.1541 y la IEEE 802 1.1 los mismos que son de gran aporte para las empresas que necesitan convergencia, flexibilidad y eficiencia en la transmisión de información bajo na misma plataforma. Se recomienda usar MPLS con Servicio Diferenciado en redes que requieren de un adecuado ancho de banda y garantía mínima de pérdida de paquetes para asegurar la Calidad de Servicio.

PALABRAS CLAVE: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <TELECOMUNICACIONES>, <MPLS CON SERVICIO DIFERENCIADO>, <MPLS CON QoS>, <PARÁMETROS DE QoS>, <DIFERENCIACIÓN DE SERVICIO, (DIFFSERV)>

ABSTRACT

The purpose of this research is to define and evaluate an MPLS (Multiprotocol Label Switching) network with differentiated service to improve quality parámeters and real-time application services such as: VOIP transmission (IP VOICE), video conferences, etc. This type of aplications require low delay, low packet loss in end-to-end transmission to guarantee Quality and Services (QoS, Quality of Service).This was achieved with the MPLS and Differentiated service architecture defined in RFC 2474 "Definition of the differentiated Services Field (Ds Field)" where basically what was done marking the traffic on the MPLS Label indicating the priority of the sent packet, so that in case of congestion the most importance packages are the first to be forwarded, 5 types of priority service were applied, they are: Premium, Gold, Silver, bronze and better effort, witch correspond to traffic ordered according to the priority of arrival at its destination. Through the traffic injector D-ITG to voice, streaming and data traffic was generated and the parameters of delay, jitter and packet loss of the traffic that runs the MPLS network with Diferentiated Service were evaluated. The results obtained are within the appropriate thresholds according to the standards of ITU-T G.1010, and ITU Y.1541 and IEEE 802 1.1, which are of great contribution to companies that need convergence, flexibility and efficiency in the transmission of information under the same platform. It is recommended to use MPLS with Diferentiated Service in network that requiere a bandwidth agreement and mínimum guarantee of packet loss to ensure the quality of service.

KEYWORDS: TECHNOLOGY AND SCIENCE OF ENGINEERING // TELECOMUNICATIONS // MPLS (MULTIPROTOCOL LABEL SWITCHING) WITH DIFFERENTIATED SERVICE // MPLS WITH QoS (QUALITY OF SERVICE) // PARAMETERS OF QoS // DIFFERENTIATION OF SERVICE // DIFFERENTAIATED SERVICE.

INTRODUCCIÓN

Internet crece a grandes pasos y cada vez con mayores requerimientos de nuevas aplicaciones como el uso de redes sociales, videoconferencias, transmisión VoIP. Esta demanda ha provocado el surgimiento de nuevas tecnologías como MPLS (MultiProtocol Label Switching) que acelera el encaminamiento de paquetes con la simplicidad de conmutación de nivel 2 (Ghein, 2007, pág. 482).

Las aplicaciones tradicionales de Internet como web, correo electrónico, transferencia de archivos y similares no han sido un problema en redes con limitado ancho de banda, sin embargo, la nueva generación de aplicaciones que incluyen audio, video y streaming, exigen alto rendimiento, ancho de banda y baja latencia (Nieto, 2010, p 20).

Para solucionar este problema la EITF ha definido un mecanismo de QoS denominado DiffServ, que es un mecanismo para priorizar el tráfico sobre otro menos importante y garantizar su entrega. El tráfico de VoIP es un buen ejemplo en el que se necesita QoS ya que debe ser entregado dentro de un cierto tiempo al destino, caso contrario se vuelve obsoleto.

Con esta investigación se pretende lograr un diseño que permita a los operadores de servicio gestionar el tráfico y recursos de red de la manera más eficiente posible, utilizando técnicas que ayuden a adaptar los distintos flujos de datos a los recursos de ancho de banda y hardware disponibles en el núcleo de red, de manera que obtengan las garantías necesarias para el correcto funcionamiento de las aplicaciones. Para ello se propone aprovechar MPLS con DiffServ para determinadas clases de servicio.

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1 Situación Problemática

Internet es un modelo de red pública del presente con mucha demanda de ancho de banda, sobre todo para aplicaciones de entornos corporativos, que necesitan de la red para aplicaciones y servicios críticos tales como videoconferencias, telefonía IP entre otros. Una carencia fundamental del Internet es la imposibilidad de seleccionar diferentes tipos de servicio para las diferentes aplicaciones de usuario es decir no existe diferenciación de servicios (DIIFFSERV).

El crecimiento permanente del Internet así como sus aplicaciones y la búsqueda de una mayor calidad de servicio ha permitido el desarrollo de nuevas arquitecturas como MPLS (Multiprotocol Label Switching), el cual se considera fundamental en la construcción de los nuevos cimientos para el desarrollo de la Internet actual, el cual está diseñado para poder dar servicios diferenciados según el modelo DIFFSERV del IETF, este modelo define mecanismos para poder clasificar el tráfico en un reducido número de clases de servicios, con diferentes prioridades. Según los requisitos de los usuarios, DIFFSERV permite diferenciar servicios tradicionales, tales como correo electrónico o transferencia de archivos para los cuales el retardo no es crítico, de otras aplicaciones donde el retardo es importante como son la transmisión de video y voz interactiva. MPLS con DiffServ se presenta como una solución para proveer de Calidad de Servicio (QoS) a la Internet.

1.2 Justificación.

La arquitectura MPLS permitió una conmutación de paquetes de forma más rápida y eficiente que otras tecnologías como Frame Relay, ATM. (Ghein, 2007, pág. 30)

La tecnología MPLS permite integrar voz, video y datos en una plataforma común con garantía de calidad de servicio que es necesario en la actualidad por los diferentes requerimientos como ancho de banda, jitter, latencia y disponibilidad.

La tendencia actual en las redes es la convergencia de las comunicaciones en sistemas integrados que permitan transmitir simultáneamente voz, video y datos en una red única dando beneficios de conectividad a las empresas y a sus usuarios, esto es posible gracias a las redes MPLS con Servicio Diferenciado.

Esto conlleva a realizar un estudio del impacto en su implementación, para ello se propone realizar una simulación en tiempo real de una red MPLS simple y otra de MPLS con DiffServ, de manera que mediante la comparación y análisis cuantitativo de los resultados obtenidos se llegue a un mejor conocimiento y comprensión de los beneficios y ventajas que ofrece MPLS con DiffServ para garantizar la Calidad y Servicio en tráfico de VoIP.

1.3 Objetivos

1.3.1 Objetivo General

Definir y Evaluar una Red MPLS con Servicio Diferenciado para mejorar los parámetros de Calidad y Servicio de aplicaciones en Tiempo Real.

1.3.2 Objetivos Específicos

- Estudiar los problemas asociados a las redes MPLS simples y las mejoras propuestas por MPLS con DiffServ.
- Desarrollar 2 ambientes de pruebas, uno para la red MPLS simple y otro para red MPLS con DiffServ, usando el simulador GNS3.
- Evaluar los parámetros de rendimiento en los ambientes de prueba estableciendo el mejoramiento de la QoS de extremo a extremo en uno de ellos.

1.4 Hipótesis

Mediante la definición y evaluación de una red MPLS con Servicio Diferenciado es posible mejorar los parámetros de Calidad y Servicio de aplicaciones en Tiempo Real

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Redes Multiprotocolo Label Switching (MPLS)

La tecnología MPLS ofrece una alternativa para la conmutación de paquetes ya que se basa en circuitos virtuales lo cual ofrece un mayor grado de escalabilidad, eficiencia, un alto rendimiento de la capa de red y una gran flexibilidad. MPLS no depende de ninguna tecnología a nivel inferior o superior por lo que su implementación es muy sencilla y se lo puede implementar sobre cualquier arquitectura ya establecida (Nieto, 2010, p 28).

MPLS trabaja entre la capa de red y la capa de enlace de datos, combinando el enrutamiento flexible e inteligente que ofrece la capa 3 con las funcionalidades de envio, fiabilidad y seguridad de la capa 2. En la figura 2-1 se indica la ubicación de la capa que MPLS introduce al modelo OSI (Harry, 2005, p 131).

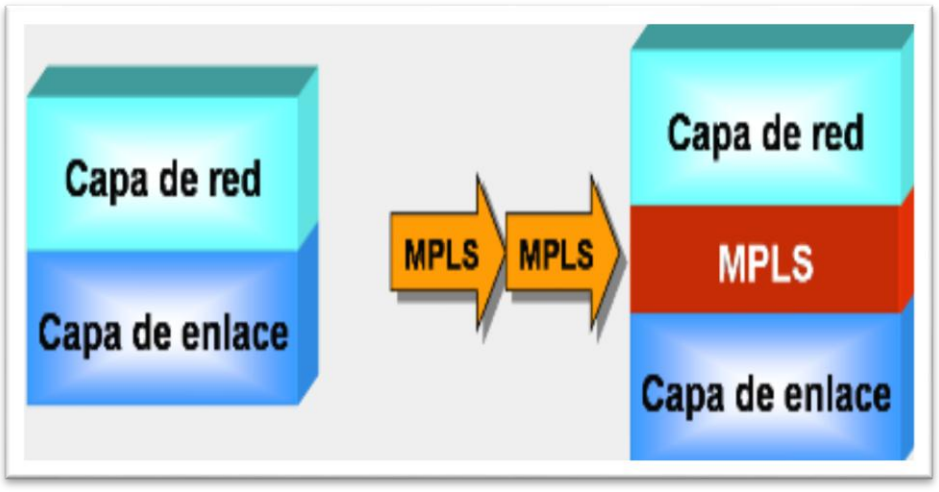

Figura 2-1 Ubicación de la Capa MPLS
Fuente: (Harry, 2005, p 131)

Dentro de una red con MPLS se emplean etiquetas que están asociadas a los paquetes IP y que facilitan enviar los datos, basándose en criterios de prioridad y calidad de servicio, permitiendo de esta manera el adecuado manejo de datos sensibles e importantes. Con la implementación de estas etiquetas, el enrutamiento de paquetes por IP´s queda de lado y se emplea la conmutación de circuitos virtuales que son mucho más rápidos y simples. Al iniciarse una red con MPLS los

routers calculan todas las rutas posibles empleando los diferentes protocolos de enrutamiento (OSPF, BGP). Una vez que se tienen todas las rutas, a través del intercambio de etiquetas se establecen los circuitos virtuales entre un origen y un destino posible (Nieto, 2010, p 41).

2.2 Beneficios de la arquitectura MPLS

MPLS presenta beneficios para los proveedores de Servicio de Internet que se detallan a continuación:

2.2.1 El uso de una red unificada

La gran ventaja de MPLS fue la idea de utilizar etiquetas, los paquetes de entrada en función de su dirección de destino u otro criterio pre-configurado, una de las razones por las que el protocolo de redes IP se convirtió en el único protocolo dominante del mundo se debe a que se puede transportar muchas tecnologías sobre él. Al agregar etiquetas al paquete le permite llevar otros protocolos además de IP, similar a lo que anteriormente era posible solo con redes Frame Raley y ATM.

MPLS puede transportar IPv4, IPv6, Ethernet, HDLS, PPP y otras tecnologías de capa 2. La característica por la cual cualquier trama de capa 2 se transporta a través de la red troncal de MPLS se llama AToM (Any Transport over MPLS), la conmutación de etiquetas MPLS es un método simple de conmutación de múltiples protocolos de red, necesita tener una tabla de reenvio que consiste en etiquetas entrantes para ser intercambiadas por etiquetas salientes y un próximo salto. En resumen, AToM permite al proveedor de servicios proporcionar el mismo envio en Capa 2 hacia el cliente, en una sola infraestructura de red unificada para trasportar todo tipo de tráfico de clientes (Lopez, 2010, p 54).

2.2.2 Núcleo de Red sin BGP

Cuando la red IP de un proveedor de servicios debe reenviar tráfico, cada enrutador debe buscar la dirección IP de destino del paquete. Si los paquetes se envían a destinos que son externos a la red del proveedor de servicios, esos prefijos IP externos deben estar presentes en la tabla de enrutamiento de cada enrutador BGP, como los prefijos del cliente o los prefijos de Internet. Esto significa que todos los enrutadores de la red del proveedor de servicios deben ejecutar BGP.

MPLS, sin embargo, permite el reenvío de paquetes en función de una búsqueda de etiqueta en lugar de una búsqueda de las direcciones IP. MPLS permite que una etiqueta se asocie con un enrutador de egreso en lugar de con la dirección IP de destino del paquete. La etiqueta es la información adjunta al paquete que le dice a cada enrutador intermedio a qué enrutador de egreso se debe reenviar. En los enrutadores principales ya no es necesario tener la información para reenviar los paquetes en función de la dirección IP de destino. Por lo tanto, los enrutadores centrales de la red del proveedor de servicios ya no necesitan ejecutar BGP. El enrutador al borde de la red MPLS aún necesita ver la dirección IP de destino del paquete y por lo tanto todavía necesita ejecutar BGP (Ghein, 2007, pág. 33) En la figura 2-2 se muestra la topología de una red BGP implementada con MPLS.

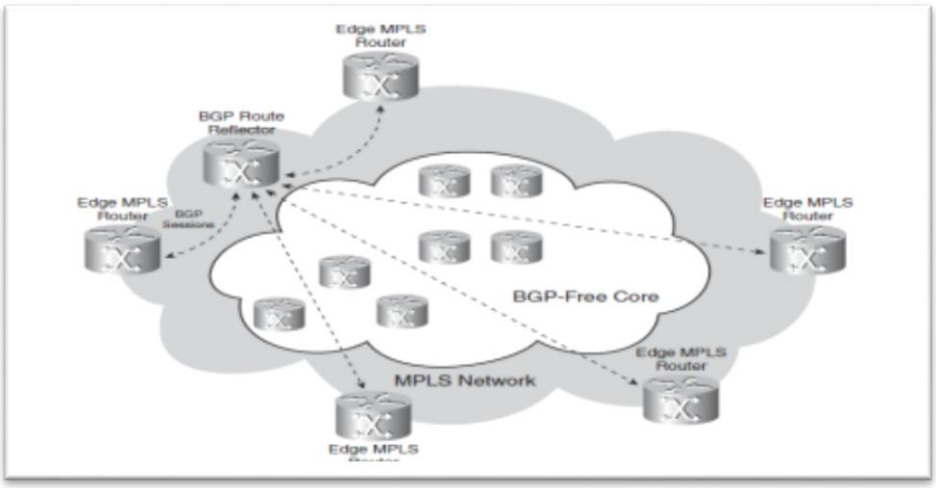

Figura 2-2: *Red MPLS con BGP en los enrutadores de borde solamente*.
Fuente: (Ghein, 2007, pág. 34)

Un proveedor de servicios de Internet (ISP) que tiene 200 enrutadores en su red central necesita tener BGP corriendo en todos los 200 enrutadores. Si se implementa MPLS en la red, solo los enrutadores de borde, que podrían ser unos 50 enrutadores, necesitan ejecutar BGP.

Todos los enrutadores en el núcleo de la red están reenviando paquetes etiquetados, sin hacer una búsqueda IP, por lo que están disminuyendo la carga de ejecutar BGP porque la tabla de enrutamiento completo para este ejemplo está muy por encima de 150,000 rutas, con MPLS no se tiene que ejecutar BGP en todos los enrutadores por lo tanto se necesitan menos memoria, sin la complejidad de tener que ejecutar BGP en los enrutadores intermedios (Ghein, 2007, p 35).

2.2.3 Modelado de VPN/MPLS punto a punto

Una Red Privada Virtual (VPN) es una red privada de datos que se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad

equivalentes a las que se obtienen con una red privada (Camacho, 2015, p 21). El objetivo de la VPN es enviar el tráfico mediante un túnel privado seguro, integrando aplicaciones multimedia de voz, datos y video, a través de una red pública compartida como Internet o en el caso de MPLS la red de un ISP.

MPLS VPN a través de un marco orientado a conexión permite a los proveedores ofrecer servicios de VPN sobre una infraestructura IP normalmente no orientado a conexión. MPLS VPN es un elegante sustituto de los circuitos virtuales permanentes de Frame Relay. La principal ventaja del modelo de MPLS VPN sobre Frame Relay es que MPLS VPN es altamente escalable (Camacho, 2015, p 25).

MPLS VPN es la más popular y extendida implementación de tecnología MPLS. Su popularidad ha crecido exponencialmente desde sus inicios, y todavía está creciendo constantemente (Ghein, 2007, p 35). Aunque la mayoría de los proveedores de servicios lo han implementado como reemplazo de los servicios Frame Relay y ATM que eran populares antes de él. MPLS VPN puede proporcionar escalabilidad y dividir la red en diferentes redes más pequeñas, hecho que a menudo es necesario en las redes empresariales más grandes, donde la infraestructura de TI tiene que ofrecer redes aisladas a departamentos individuales. Muchos de los proveedores que han ejecutado MPLS VPN durante años ahora están buscando interconectar su red a las redes MPLS VPN de otros proveedores de servicios para mejorar la escalabilidad y la facilidad de operación de su red (Ghein, 2007, p 40).

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

- En el nivel 3 del modelo OSI, mediante el protocolo IP Security (IPsec) del IETF.
- En el nivel 2 del modelo OSI, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un ISP.

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte (Bustamante, 2007, p 72)

En los túneles de nivel 2, se encapsulan paquetes de varios protocolos sobre los datagramas IP de la red del ISP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico (Bustamante, 2007, p 75)

La arquitectura MPLS tiene un modelo topológico que no se superpone, sino que se acopla a la red del proveedor, superando los inconvenientes de los túneles IP. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común", en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos Label Switched Path (LSP) (Nieto, 2010, p 70). En la figura 2-3, se muestra diferentes tunelizaciones dentro de las redes MPLS.

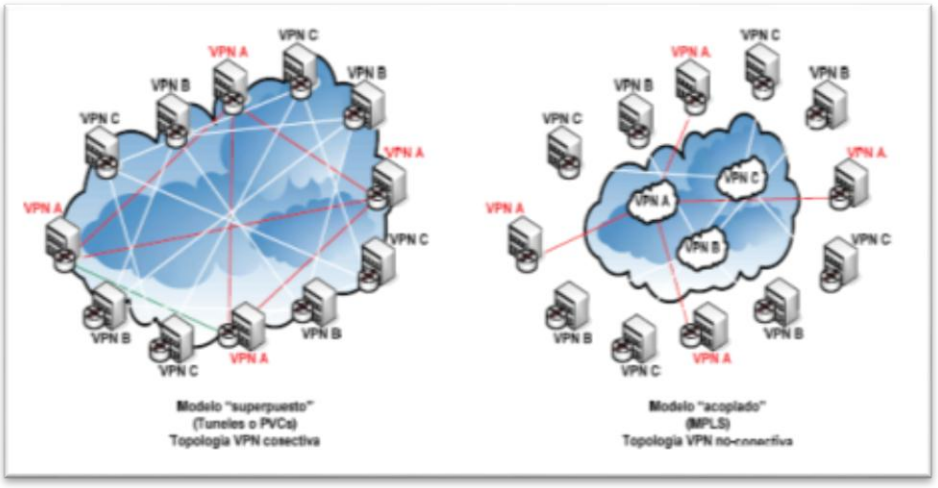

Figura 2-3: Diferencia entre túneles y MPLS
Fuente: (Nieto, 2010, p 70)

2.2.4 Ingeniería de Tráfico

La Ingeniería de Tráfico (TE) es una disciplina que procura la optimización del rendimiento de las redes operativas mediante la aplicación de tecnologías y los principios científicos en la medición, caracterización, modelado, y control del tráfico que circula por la red (Camacho, 2015, p 76). Las mejoras del rendimiento de una red operacional mediante un eficiente manejo del tráfico y modo de utilización de recursos, son los principales objetivos de TE. Una ventaja práctica de la aplicación sistemática de los conceptos de Ingeniería de Tráfico a las redes operacionales es que ayuda a identificar y estructurar las metas y prioridades en términos de mejora de la calidad de servicio dado a los usuarios finales de los servicios de la red.

El objetivo de la Ingeniería de Tráfico es adaptar los flujos de tráfico a los recursos físicos de la red, equilibrando de forma óptima la utilización de esos recursos, de manera que no hayan algunos que estén sobre-utilizados, creando cuellos de botella, mientras otros puedan estar subutilizados (Castellanos y Guzman, 2013, p 54)

MPLS con ingeniería de tráfico soluciona algunos inconvenientes con redes IP. Las redes IP se basan en el principio de enrutamiento de menor costo para calcular la ruta más corta para reenviar tráfico a través de la red, sin tener en cuenta la capacidad de ancho de banda disponible del enlace lo cual provoca que el enrutador siga enviando tráfico IP a un enlace a pesar de estar perdiendo los paquetes por falta de ancho de banda (Ortega, 2007, p.102).

El resultado de este comportamiento en el reenvío de paquetes IP es que algunos enlaces pueden ser sobreutilizados en la red, mientras que otros enlaces pueden estar infrautilizados o subutilizados (Ortega, 2007, p.103). TE puede brindar una solución manejando el tráfico de los enlaces sobrecargados de la siguiente manera:

- Proporciona una distribución eficiente del tráfico en toda la red, evitando enlaces subutilizados y sobreutilizados.
- Tiene en cuenta el ancho de banda configurado (estático) de los enlaces.
- Tiene en cuenta los atributos del enlace (por ejemplo, delay, jitter). Se adapta automáticamente al cambio de ancho de banda y atributos de enlace.
- Mover el tráfico del camino establecido por el IGP (Protocolo de Compuerta Interior) a un camino menos congestionado.
- Utilizar el exceso de ancho de banda sobre los enlaces subutilizados.
- Maximizar la utilización de los enlaces y nodos de la red.
- Aumentar la confiabilidad del servicio.

2.3 Arquitectura MPLS

Dentro de las redes MPLS se emplean dos componentes principales para garantizar su funcionalidad: control y envio.

El componente de control hace que MPLS tenga la información exacta y coherente entre todos sus elementos. Mientras que el componente de envio utiliza etiquetas con la finalidad de enrutar los diferentes paquetes dentro de una red MPLS. En la Figura 2-4 se representan los diferentes elementos que componen una red MPLS y su ubicación (Delgado, 2015, p. 64).

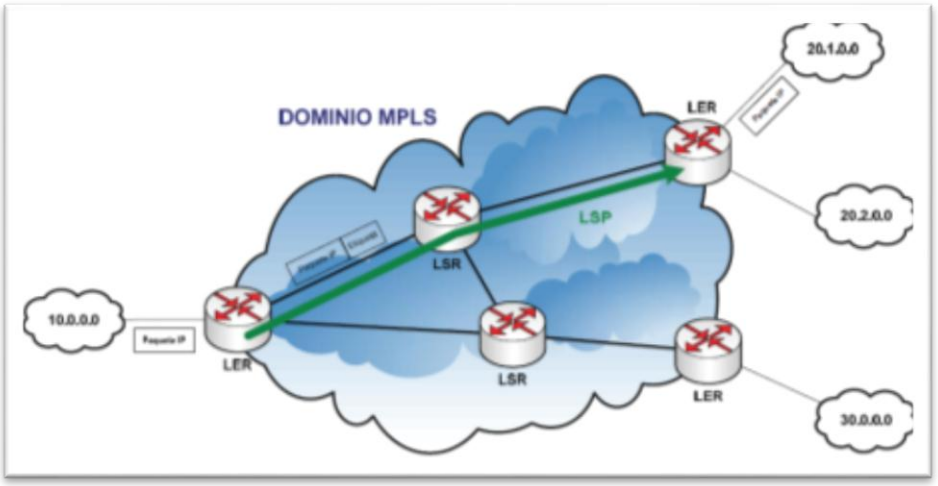

Figura 2-4: Componente en una MPLS
Fuente: (Delgado, 2015, p. 64)

2.3.1 Componentes de Envio

Se describen los conceptos que conforman los componentes de envio en MPLS como lo son: Etiquetas MPLS, Pilas de etiquetas, Encapsulamiento MPLS, Label Switching (LSR), Label Switched Path (LSP), Forwarding Equivalence Class (FEC) (Zapata, 2016, p 23).

2.3.1.1 Etiquetas MPLS

Las etiquetas MPLS tienen 32 bits divididos en cuatro campos con funciones bien definidas:

Campo 1. *Valor de la etiqueta*

Tiene un tamaño de 20 bits y define la etiqueta del paquete.

Campo 2. *EXP*

En un inicio se lo empleo para los diferentes proyectos experimentales que surgían, pero en la actualidad este campo se emplea para proveer el servicio de calidad, su tamaño es de 3 bits.

Campo 3. *BoS*

Su tamaño es de un bit e indica cuando la etiqueta es la última de la pila.

Campo 4. *TTL*

Esta sección determina el tiempo de vida que tiene el paquete, su tamaño es de 8 bits, funciona de la misma manera, como lo hace dentro de un paquete IP. Su finalidad es evitar que los paquetes creen bucles infinitos dentro de las redes.

2.3.1.2 Pilas de Etiquetas.

La pila de etiquetas son las etiquetas o etiqueta que se le coloca a un paquete por el funcionamiento en sí de MPLS, como se lo puede observar en la Figura 2-5. Para transitar dentro de estas redes, los paquetes necesitan por lo menos una etiqueta, la primera etiqueta recibe el nombre de Top

Level (Etiqueta Superior), mientras que la última se la define como Bottom Level. Esta última etiqueta es la única que va a poseer el campo BoS activo (Lopez y Pedraza, 2011, p 60).

Figura 2-5: Pila de Etiquetas
Fuente: (Lopez y Pedraza, 2011, p 60).

2.3.1.3 Encapsulado MPLS

La pila de etiquetas que está conformado por un paquete MPLS, se encuentra funcionando entre las capas 2 y 3 del modelo OSI. Por ejemplo si MPLS se encuentra funcionando dentro de una red cuyo protocolo de red sea IPv4 y el encapsulado que se emplee para el enlace de datos sea PPP, la pila de etiquetas se encuentra después del encabezado del PPP pero antes del encabezado de IPv4 (Orozco, 2017, p 43).

2.3.1.4 Label Switching Router (LSR)

Son los Routers capaces de manejar y soportar paquetes MPLS, por consiguiente tienen la habilidad de transmitir y recibir dichos paquetes. Dentro de una red MPLS se encuentran tres tipos de LRS:

LSR de Ingreso: Es el Router encargado de recibir paquetes que no poseen etiquetado MPLS, para luego enviarlos por la interfaz adecuada, sin antes introducir dichas etiquetas.

LSR de Egreso: Es el Router encargado de recibir paquetes con etiquetas MPLS, para luego enviarlos por la interfaz adecuada, sin antes haber retirado todas la etiquetas.

LSR Intermedio: Son todos los Router dentro de la red MPLS por los cuales pasan los paquetes hasta su destino, realizando la conmutación basado en las etiquetas MPLS que conllevan los paquetes.

Un LSR puede Push (colocar etiqueta), Pop (quitar etiqueta) o Swap (intercambiar una etiqueta) dependiendo de la transmisión de paquetes, por lo cual estos Routers deben ser capaces de insertar o quitar las pilas de etiquetas para garantizar su correcto funcionamiento (Orozco, 2017, p 45).

2.3.1.5 Label Switched Path (LSP)

Es el camino o ruta que toma un paquete dentro de la red MPLS, son los diferentes circuitos virtuales que atraviesa el tráfico desde su inicio hasta su final.

2.3.1.6 Forwarding Equivalence Class (FEC)

Representan a un conjunto de paquetes que toman el mismo LSP y que son tratados de la misma manera, es decir, tienen las mismas políticas de calidad de servicio. Todos los paquetes de un mismo FEC poseen la misma etiqueta. Para la agrupación de los paquetes dentro de un mismo FEC se lo realiza a través de los siguientes criterios:

- Paquetes con direcciones de origen IP similares.
- Paquetes con direcciones de destino IP que sean parte del mismo prefijo BGP.
- Paquetes multicast.
- Paquetes que son recibidos y tratados por la misma sub-interfaz.
- Paquetes que son tratados dependiendo del DSCP.

2.3.2 Componentes de Control

La finalidad de este componente es mantener una coherencia entre los elementos de la red MPLS, es decir, que posean una misma información de ruteo para lo cual se crean uniones o relaciones entre la información de capa 3 y las etiquetas y dichas relaciones son transmitidas a los diferentes elementos empleando un protocolo de distribución.

2.3.2.1 Distribución de etiquetas.

La distribución de etiquetas se realiza entre los Routers vecinos con la finalidad de conocer que etiqueta colocar a cada paquete que va a reenviar a la red MPLS, para lo cual se utilizan los protocolos de distribución.

Estos protocolos pueden utilizar protocolos de enrutamientos pre-existentes para la distribución de etiquetas o emplear un protocolo independiente de los primeros, que se encarguen solamente de hacer esta tarea (Zapata, 2016, p 21).

2.3.2.2 Protocolos de distribución de etiquetas

Un protocolo de distribución de etiquetas se define como un conjunto de procedimientos mediante el cual un enrutador informa a otro sobre el significado de las etiquetas utilizadas para reenviar tráfico entre ellos. Actualmente existe una amplia variedad de protocolos utilizados para la distribución de etiquetas. La arquitectura MPLS no especifica uno de estos en particular, sino que, más bien recomienda su elección dependiendo de los requerimientos específicos de la red. Los protocolos utilizados pueden agruparse en dos grupos: Protocolos de enrutamiento explícito

y Protocolos de enrutamiento implícito. El enrutamiento explícito es idóneo para ofrecer Ingeniería de Tráfico y permite la creación de túneles. El enrutamiento implícito, por el contrario, permite el establecimiento de LSPs pero no ofrece características de Ingeniería de Tráfico (Nieto, 2010, p 43).

Protocolos de enrutamiento implícito:

- Protocolo de Distribución de Etiquetas (LDP)

Protocolos de enrutamiento explícito:

- LDP de Ruta Restringida (CR-LDP)
- Protocolo de Reservación de Recursos con Ingeniería de Tráfico (RSVP-TE).

2.3.2.3 1.- Protocolo de distribución de etiquetas (LDP)

LDP es el protocolo encargado de la distribución de etiquetas para rutas internas. Todos los LSRs directamente conectados deben establecer una sesión LDP entre ellos. Los pares LDP intercambian mensajes de asignación de etiquetas durante el período de sesión LDP. Una etiqueta es un enlace a una determinada FEC (Nieto, 2010, p 45). LDP tiene cuatro funciones principales:

- Descubrir LSRs que ejecuten LDP.
- Establecer y mantener una sesión.
- Anunciar los enlaces de etiquetas.
- Notificar errores y advertencias.

Establecimiento de la sesión LDP: Es un proceso que consta de dos pasos que son: establecimiento de la conexión TCP llevado a cabo por el LSR activo (identificador con el LSR más alto), e inicio de sesión donde luego de establecida la conexión TCP se negocian los parámetros de la sesión intercambiando mensajes de inicialización. Dos LSRs pueden enviar mensajes de inicialización, el LSR que recibe el mensaje contesta con un mensaje KeepAlive, si los parámetros son aceptados. Si los parámetros son inaceptables, el LSR envía un mensaje de notificación de error rechazando la sesión y cerrando la conexión (Nieto, 2010, p 46). En la Figura 2-6 se observa diferentes mensajes del mecanismo LDP.

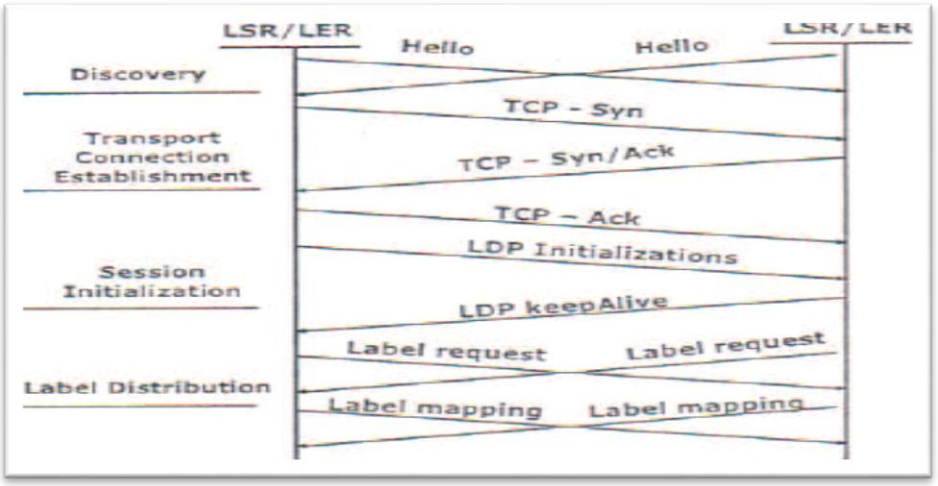

Figura 2-6: Intercambio de mensajes en el mecanismo LDP
Fuente: (Nieto, 2010, p 46).

Cuando un LSR asigna una etiqueta a una FEC, éste necesita informar a sus vecinos acerca de esta etiqueta y su significado, LDP define cuatro tipos de mensajes:

Discovery.- Se ejecuta sobre UDP y usa mensajes multicast Hello para aprender acerca de otro LSR con quien tiene una conexión directa LDP.

Adjacency.- Se ejecuta sobre TCP y provee la inicialización mediante mensajes Initialization al comienzo de una sesión LDP. EL mensaje KeepAlive es enviado periódicamente para monitorear mediante timers la sesión LDP.

Label Advertísement.- Provee mensajes de asociación de etiquetas utilizando mensajes Label Mappíng, Label Withdrawalm y Label Reléase.

Notification.- Este mensaje provee información de errores entre un par de LSR que tienen una sesión LDP establecida (Zapata., Pacheco, De la Torre y Vallejo, 2017, p 3).

Protocolo CR-LDP (Constraint-Route Label Distribution Protocol)

EL grupo de trabajo IETF documentó en el RFC 3212 el desarrollo del protocolo de señalización CR-LDP el mismo que provee mecanismos para el establecimiento de rutas explicitas LSPs, estos mecanismos son definidos como una extensión de LDP. Debido a que LDP es un protocolo basado en el establecimiento y mantenimiento de sesiones TCP por tanto se tienen los siguientes beneficios:

Los mensajes CR-LDP son entregados confiablemente por el protocolo TCP y la información de estado asociada con los LSP enrutados explícitamente no requiere actualización periódica (Hesselbach, Huerta y Calderón, 2014, p 3).

Los mensajes CR-LDP están controlados por flujos a través de TCP. CR-LDP se define con el propósito específico de establecer y mantener LSP enrutados explícitamente y ofrecer capacidades opcionales y/o adicionales para la negociación de servicios LSP y la gestión de tráfico más allá de la entrega del paquete con best-effort. CR-LDP permite que estos parámetros como asignación de ancho de banda, configuración y prioridades de mantenimiento sean modificados dinámicamente sin interrupción del LSP operacional. Este conjunto de parámetros, son adecuados y lo suficientemente potentes para describir, caracterizar y parametrizar una amplia variedad de escenarios con servicios QoS (Hesselbach, Huerta y Calderón, 2014, p 4).

En particular, CR-LDP y RSVP-TE son dos protocolos de señalización que realizan funciones similares en redes MPLS con extensión para ingeniería de tráfico. Internet Engineering Task Force (IETF), llegó a un consenso de centrar sus esfuerzos en el desarrollo de RSVP-TE y paró el desarrollo de CR-LDP, esto se encuentra documentado en el RFC 3468 (Zapata, 2016, p 150).

Resource Reservation Protocol (RSVP-TE)

El grupo de trabajo IETF, enfoca sus esfuerzos en el protocolo de señalización con reserva de recursos para aplicaciones de ingeniería de tráfico RSVP-TE mediante el RFC 3209.

RSVP es un protocolo de señalización, fue originalmente diseñado para la señalización de servicios integrados (Int-Serv) y actualmente es usado para señalizar los túneles de TE (Traffic Engineering). En otras palabras, RSVP señaliza calidad de servicio (QoS) en toda la red.

- RSVP utiliza mensajes PATH y RESV para señalizar una ruta. El router que se encuentra en la cabecera TE, envía los mensajes PATH hacia el router de cola, mientras que, los mensajes RESV son enviados por la misma ruta, pero en sentido opuesto. El router de cabecera de un túnel TE se encarga de calcular la mejor ruta que el túnel TE debe tomar de la base de datos TE, teniendo en cuenta el ancho de banda y otras limitaciones (Ortega, 2007, p.120).

2.4 Funcionamiento de MPLS

Con el enrutamiento IP los paquetes avanzan de “salto en salto” a través de la red, es decir que en cada router se encamina el paquete hacia el siguiente salto en función de su dirección IP destino y de la tabla de enrutamiento. En MPLS, los LSR también encaminan los paquetes “salto a salto”

pero simplemente basándose en la etiqueta de longitud fija, lo que significa que no usan la información de la cabecera IP (Delgado, 2015, p. 27).

La base de MPLS está en la asignación e intercambio de etiquetas, que permiten el establecimiento de los LSP por la red. Cada LSP se crea a base de concatenar uno o más saltos en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Swiching Router) a otro, a través de la red MPLS (Nieto, 2010, p 45).

2.4.1 Recorrido de paquete MPLS en la red

Primero, llega un paquete sin etiquetar a un router LER de ingreso. El router entonces decide a que FEC pertenece y le asigna las etiquetas correspondientes (push). El proceso de asignar un paquete a un FEC solo se hace una vez, a diferencia de lo que ocurriría con un paquete IP tradicional, que se evalúa en cada nodo.

Una vez que el paquete ya está etiquetado, se envía al siguiente salto LSR usando la tabla LIB (Label Information Base). Este paquete va saltando de LSR en LSR basándose en la tabla LIB de cada router.

Normalmente lo que hacen estos routers es hacer un intercambio (swap) de la etiqueta. Finalmente, el paquete llega al router LER de salida, el cual es el encargado de quitar la última etiqueta (pop) y enviar el paquete hacia su destino por routing convencional. En este punto, el paquete ya no es del tipo MPLS porque ya no tiene etiquetas. Este último paso suele realizarlo en el penúltimo router de la red (Penultimate Hop Popping).

La razón de esto es para liberar al último router del trabajo, ya que este tiene que enrutar un paquete IP y si además tuviera que eliminar la etiqueta, tendría dos trabajos. De esta forma, el penúltimo router de la red MPLS hace un pop en el momento de enviar el paquete al interfaz que le indica la tabla LIB y el último router ya recibe un paquete IP convencional (Orozco, 2017, p 19).

2.4.2 Creación de la tabla LIB en cada LSR

Cada LSR construye una tabla de etiquetas LIB (Label Information Base) a medida que va recibiendo las etiquetas con el protocolo LDP. En las tablas LIB se especifica el mapeo de cada etiqueta con una interfaz, tanto de entrada como de salida. Esta tabla se actualiza cada vez que se

efectúa una renegociación de las uniones de etiquetas (Castellanos y Guzmán, 2013, p 16). En la Figura 7-2 se aprecia el ejemplo de una tabla LIB.

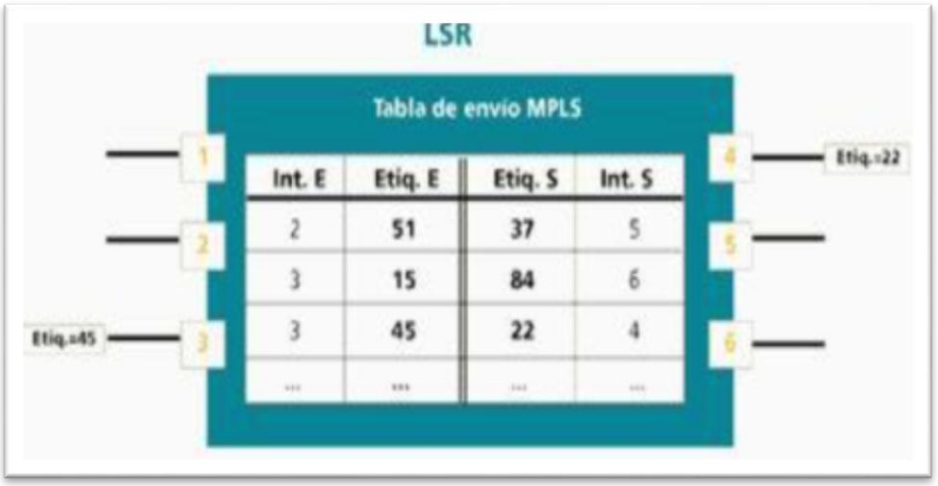

Figura 2-7: Tabla LIB (Label Information Base)
Fuente: (Castellanos y Guzmán, 2013, p. 17)

Esta tabla guía al LSR cuando tiene que realizar un swap de etiquetas, indicándole a que interfaz tiene que dirigir el paquete. En el ejemplo de la Figura 2-7, un paquete de entrada por la interfaz 2 con la etiqueta 51, se redirigiría a la interfaz 5 con la etiqueta 37.

2.4.3 Creación de los LSP

Un LSP se crea en orden inverso a la trayectoria del paquete. Lo que significa que el LSP se crea desde el nodo destino hacia el nodo origen (Buñay, 2013, p. 44).

El nodo origen, al recibir un paquete del cual no tiene etiqueta en la tabla LIB, solicita mediante un paquete "request" la ruta que necesita. Este paquete "request" se irá propagando hasta llegar al nodo LER de salida. Una vez recibido este paquete, el LER enviará un paquete de "mapping" en dirección upstream. Este paquete, al pasar por los nodos hacia el Nodo Origen, irá completando la tabla LIB relacionada con el LSP que se está creando (Buñay, 2013, p. 49). En la Figura 2-8 se muestra el sentido y los nodos por los cuales va a pasar el tráfico dentro de la red MPLS.

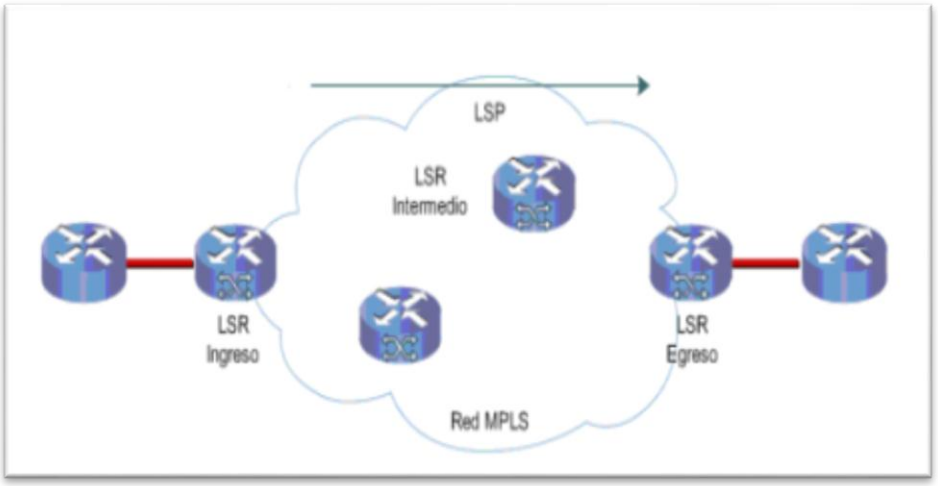

Figura 2-8: Creación de un LSP
Fuente: (Buñay, 2013, p. 44).

2.5 Calidad de Servicio (QoS)

Debido a la gran convergencia que se está presentando en la actualidad a nivel mundial, donde todos los servicios de telecomunicaciones necesitan una conectividad global, están afectando a la calidad en la transmisión de datos. Al inicio de las redes no importaba el tipo de dato que se transmitía porque se disponía de un canal con un ancho de banda lo suficientemente grande para soportar el tráfico y los únicos inconvenientes que se necesitaba resolver eran la confidencialidad y la garantía de que los datos lleguen a su destino. Hoy en día se tiene mucho más tráfico circundando dentro de las redes a nivel mundial, lo cual está ocasionando problemas a las aplicaciones o datos que son susceptibles a los retardos, pérdidas de paquetes, un Jitter muy alto, etc. De esta manera se establecen los parámetros necesarios para garantizar que todas las aplicaciones cumplan las condiciones necesarias para su correcto funcionamiento, a lo cual se lo determina como Calidad de Servicio (QoS).

La QoS no es otra cosa que la combinación de esfuerzos colectivos y globales que se establecen para la prestación de distintos servicios tecnológicos con la finalidad de brindar una experiencia satisfactoria al usuario (Ortega, 2007, p.110).

2.5.1 Parámetros de Calidad de Servicio.

La ITU-T, define que para cada distinta aplicación son necesarios diferentes parámetros de QoS, estos parámetros varían dependiendo del tipo de tráfico, el tipo de cliente y los aspectos técnicos de la red, a pesar de ello, se establecen que los siguientes parámetros pueden ser utilizados para

la evaluación de la calidad de servicio en diferentes áreas (Recomendación UIT-T G.1010, 2001, p. 11)

Retardo de transferencia de paquetes: es el tiempo que le toma a un paquete IP en ser transmitido desde su origen hasta un destino específico. Para su cálculo intervienen parámetros como el número de nodos que tiene que atravesar el paquete, el protocolo de enrutamiento, el tráfico presente en la red, etc.

Las aplicaciones que más se ven afectadas por este parámetro son los basados en tiempo real y multimedia como son: videoconferencia, voz, etc.

Ancho de Banda: es el espacio suministrado para la transmisión de datos dentro de un canal de comunicación, cuando mayor sea este espacio más cantidad de información se podrá enviar, pero el inconveniente se encuentra en los altos costos que tiene para contratar un ancho de banda más grande y en los cambios tecnológicos que se deben realizar para implementar estos cambios. Por tal motivo se debe realizar una administración adecuada del ancho de banda garantizando prioridades para los datos más sensibles.

Jitter o Varianza de retardo de los paquetes de información: es originado por el tráfico que se presenta dentro de una red, por la pérdida de paquetes o por las diferentes rutas que puede tomar un paquete para llegar a su destino. Este problema se presenta en las aplicaciones multimedia, tiempo real, telefonía IP, radio, etc.

Tasa de pérdida del paquete IP: es el porcentaje de paquetes descartados con relación al número total de paquetes transmitidos, este efecto se presenta por el alto grado de congestión en las colas de los nodos, tiempo de vida de los paquetes (Recomendación UIT-T G.1010, 2001, p. 11).

2.5.2 Modelos para implementar QoS

La habilidad para diferenciar diversas clases de servicio y asignarles prioridades sobre cada enrutador es el trabajo que tiene que realizar un modelo de calidad de servicio. Todos los modelos de QoS llevan a cabo una serie de pasos que les permite manipular un determinado tráfico de datos, el primer paso para la implementación de QoS es identificar las distintas clases de tráfico que la red va a soportar. El tráfico puede ser clasificado basado en el tipo como voz, aplicaciones, datos, etc., y sobre las propiedades de patrones de tráfico, luego de que el tráfico ha sido clasificado, el próximo paso es identificar que operaciones de QoS serán llevadas a cabo para cada uno de esos tipos sobre el enrutador local. Debemos notar que, aunque QoS es una implementación extremo-extremo, debe ser configurada sobre cada enrutador en el camino desde el origen al destino, sin embargo, varias secciones de la red pueden ser configuradas con diferentes esquemas de QoS para mejorar distintos tipos de tráfico. Este proceso de definir las operaciones

de QoS para un cierto tipo de tráfico se denominan Políticas de Servicio (Zapata, Pacheco, De la Torre y Vallejo, 2017, p. 89).

Existen 3 modelos para implementar calidad y servicio (QoS) sobre una red (Cisco System, 2004, vol 2, p 291). El modelo Best-Effort fue diseñado para entregar paquetes sin garantías, este modelo sigue predominando hoy en día. El modelo Integrated Services (IntServ) se introdujo para complementar el modelo Best-Effort al reservar ancho de banda para aplicaciones que requieren garantías de retardo. El modelo DiffServ se crea para proveer gran escalabilidad al proporcionar QoS a los paquetes. La principal diferencia entre IntServ y DiffServ en que DiffServ no requiere señalización.

> *Modelo Best-Effort:* en este modelo no se aplica QoS a los paquetes, no es importante cuando ni como lleguen los paquetes. No hay diferenciación entre tipos de tráfico todos los paquetes son tratados de igual manera. Utiliza el tipo de cola FIFO (Primero en entrar primero en salir). A todos los usuarios se les proporciona el ancho de banda que se tenga disponible sin importar su prioridad o importancia. Por este motivo se lo denomina QoS deficiente y es el modelo por defecto de todo el tráfico (Cisco System, 2004, vol 2, p 293).
>
> *Modelo IntServ:* se lo llama flujo continuo de datagramas, el cual es unidireccional y permite definir tres tipos de servicio: *servicio garantizado* garantiza un caudal mínimo con un máximo retardo; *servicio de carga controlada* ofrece la capacidad de carga de una red con pocos datagramas aunque en algunas ocasiones se producen retardos grandes; *servicio del mejor esfuerzo* no se tiene ninguna garantía ni QoS, lo único que realiza es reservar recursos para el flujo de datos sin ningún control de pérdidas de paquetes ni prioridades (Cisco System, 2004, vol 1, p 67).
>
> *DiffServ:* proporciona la mayor escalabilidad y flexibilidad en la implementación de QoS en una red. Realiza una clasificación del tráfico lo que permite proporcionar diferentes niveles de QoS a cada clase de tráfico. Se usa en aplicaciones de misión crítica. Una clase de tráfico se define como los requisitos de QoS y las garantías que se proporcionan a una colección de paquetes.
> DiffServ mantiene la interoperabilidad con dispositivos que no son compatibles con este modelo debido a lo cual DiffServ se puede implementar gradualmente en grandes redes preexistentes o de la nueva generación (Cisco System, 2004, vol 2, p 300).

Estos tres modelos de implementación o administración de la calidad de servicio son los que se utilizan hoy en día para administrar el tráfico de las redes globales, pero el modelo de servicio

diferenciado está ganando mucho terreno en los últimos años gracias a sus prestaciones y fácil implementación en redes pre-existentes con internet, sin la necesidad de realizar cambios costosos y garantizando su funcionalidad, por tal motivo en la siguiente sección se detalla al servicio diferenciado Diff-Serv sobre la red MPLS (Cisco System, 2004, vol 2, p 310).

2.6 Servicio Diferciado sobre MPLS

Servicio diferenciado (Diff-Serv) es un conjunto de tecnologías que permiten a los proveedores de servicios ofrecer diferentes niveles de calidad de servicio para distintos clientes y tráfico de datos. Se basa únicamente en el marcado de paquetes, no hay reserva de recursos por flujo, no hay protocolo de señalización ni tampoco información del estado de los routers (Ghein, 2007, p 484).

La diferenciación de servicios se lleva a cabo en cada uno de los dispositivos de interconexión, a este hecho se le conoce como Comportamiento por Salto (PHB). El PHB indica el tráfico que corresponde a un determinado paquete a través del campo DSCP, además, específica la prioridad del enrutamiento de los paquetes en los routers, conservando la clasificación estándar de BE (Mejor Esfuerzo), CS (Selector de clase), EF (Encaminamiento expedido) y AF (Encaminamiento asegurado) (Ghein, 2007, p 490).

En este modelo de manejo de tráfico cada uno de los Routers de la red MPLS debe analizar y definir el tratamiento adecuado al tráfico, es decir, da un trato diferenciado a cada flujo de datos. Se puede establecer caminos predefinidos para que dicho tráfico fluya por una determinada zona dependiendo de su prioridad (Lopez, 2009, 103).

2.6.1 Elemento de la arquitectura DIFFSERV

El servicio diferenciado consta de los siguientes elementos (Buñay, 2013, p. 70):

Clasificador: Guía a los paquetes que tienen características similares por un camino especifico.

Medidor: envía la información necesaria para que se lleve a cabo para asignar el recurso pertinente a dicho tráfico.

Marcador: marca los paquetes con un código DS con la finalidad de seleccionar el PHB adecuado.

Acondicionador: controla las colas de almacenamiento descartando los paquetes cuando la cola está llena.

Descartador: descarta paquetes para prevenir la congestión dentro de la red.

2.6.2 DiffServ en paquetes Ip

La Figura 2-9 describe el formato básico del campo DSCP y describe el propósito de éste dentro de la cabecera IP.

La cabera IP, dispone del campo TOS, para proveer de niveles de priorización de paquetes, como se observa en la Figura 2-10 este campo de 1 byte está dividido en 3 bits de precedencia, 4 bits TOS y un bit MBZ (Cisco System, 2004, vol 1, p 82).

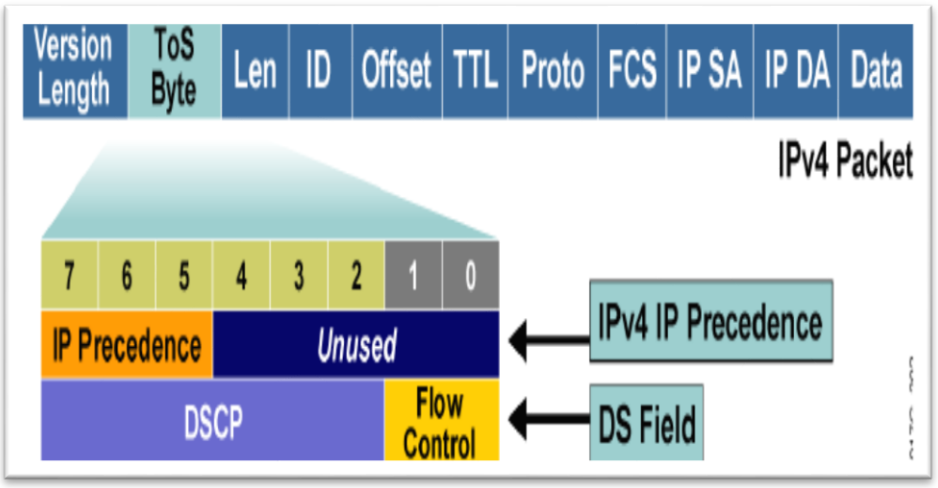

Figura 2-9: Campo de la Cabecera IP
Fuente: (Cisco System, 2004, vol 1, p 82).

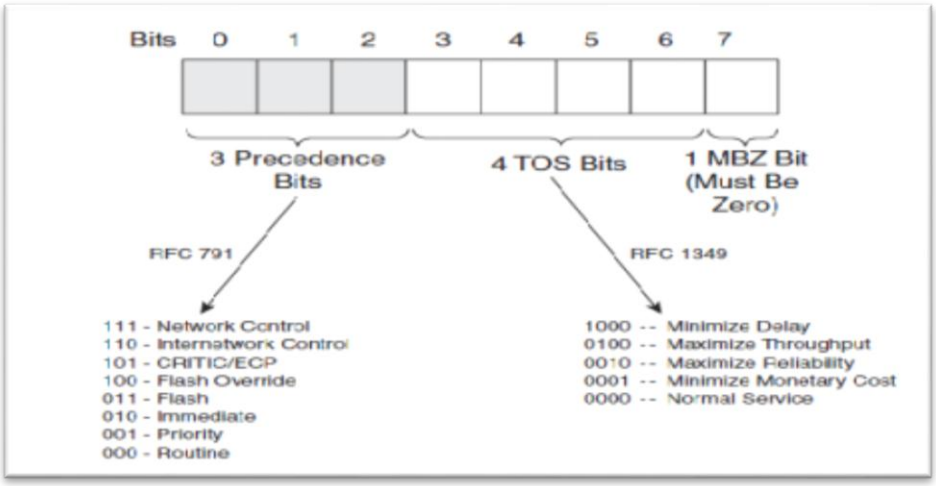

Figura 2-10: Byte de TOS de la cabecera IP definida por los 3 bits de precedencia.
Fuente: (Ghein, 2007, p 490).

El uso de los bits de precedencia para QoS ahora se usa ampliamente en todo el mundo para muchas redes. El inconveniente de los bits de precedencia, sin embargo, es que solo existen tres

bits, lo que significa que puede tener solo ocho niveles de servicio. Por lo tanto, el IETF decidió dedicar más bits para QoS.

Para aplicar DiffSev se asignó una nueva distribución del campo TOS incluyendo a los cuatro bits de TOS que estaban en desuso anteriormente. De acuerdo en la RFC 2474, se asignaron 6 bits, proporcionando niveles más que suficientes de QoS. La Figura 2-11 muestra qué bits del byte TOS se usan para DiffServ.

Campo DSCP

Cada valor de DSCP identifica un BA (Behavior Aggregates). Cada BA tiene asignado un PHB. Cada PHB está implementado utilizando el mecanismo de QoS apropiado o un conjunto de mecanismos de QoS. (Ghein, 2007, p 501).

Per-Hop Behaviors

El campo DSCP selecciona los siguientes PHB a través de la red, definidos por el estándar ETF

- Default PHB (FIFO, tail drop)
- EF PHB
- AF PHB

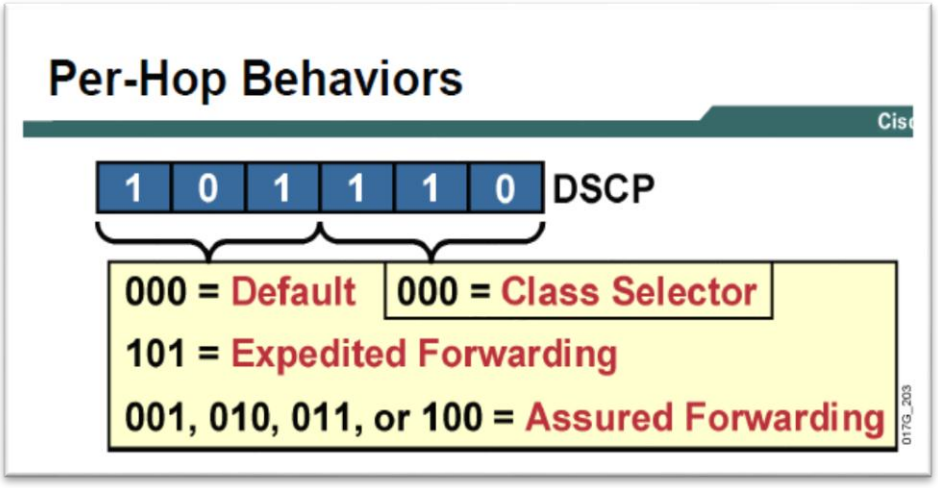

Figura 2-11: Per Hop Behaviors del campo DSCP
Fuente: (Cisco System, 2004, vol 2, p 88).

Default PHB

Usa el servicio de mejor esfuerzo Best-Effort (los bits 5 al 7 de DSCP = “000”

Expedited Forwarding (EF)

Es un envio acelerado con baja pérdida, baja latencia, baja jitter, asegurado ancho de banda extremo a extremo, a través del dominio DiffServ. Los bits del 5 al 7 de DSCP = “101”.

Assured Forwarding (AF)

Define diferentes servicios de reenvío seguro. Se definen cuatro clases de AF, cada una con tres precedencias de descarte. Las clases de AF se anotan como AFij, siendo i de 1 a 4 para la clase j de 1 a 3 para la precedencia de descarte. (Cisco System, 2004, vol 2, p 90).

Los tres primeros bits de los 6 bits definidos en el campo DSCP corresponden a la clase, los siguientes dos bits definen la precedencia de descarte, y el último bit está reservado. Cuanto mayor sea la precedencia de descarte dentro de una clase, es más probable que el paquete se elimine cuando ocurre congestión en relación con los otros paquetes con menor precedencia de descarte. Existen cuatro clases para el tráfico, y existen tres niveles para la precedencia de descarte. En la Figura 2-12 se pueden observar los diferentes tipos de codificación para el tráfico.

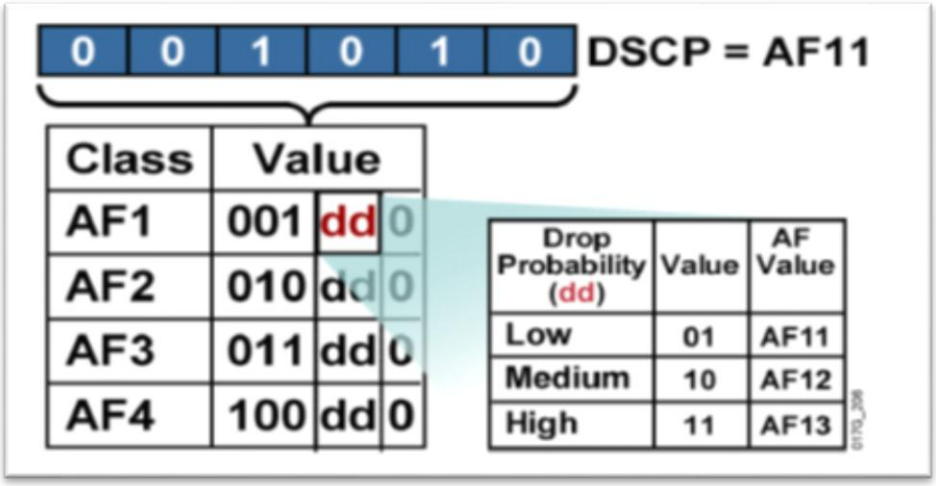

Figura 2-12: Clases del campo DSCP
Fuente: (Cisco System, 2004, vol 1, p 30).

AF23, por ejemplo, denota la clase 2 y descarta la precedencia 3. La Tabla 2-1 muestra los valores para las cuatro clases de reenvío seguro

Tabla 2-1: Cuatro clases AF cada una con 3 precedencias de descarte

AF CLASS	Drop Probability		DSCP Value	DSCP-DEC
AF Class 1	Low	AF11	001 01 0	10
	Medium	AF12	001 10 0	12
	HIGH	AF13	001 11 0	14
AF Class 2	Low	AF21	010 01 0	18
	Medium	AF22	010 10 0	20
	HIGH	AF23	010 11 0	22
AF Class 3	Low	AF31	011 01 0	26
	Medium	AF32	011 10 0	28
	HIGH	AF33	011 11 0	30
AF Class 4	Low	AF41	100 01 0	34
	Medium	AF42	100 10 0	36
	HIGH	AF43	100 11 0	38

Fuente: (Ghein, 2007, p 482)
Realizador por: Chacha, Paulina, (2019)

2.6.3 DiffServ con paquetes MPLS

La arquitectura MPLS provee el campo EXP de la cabecera destinada a aplicar QoS. La Figura 2-13 muestra la sintaxis de la etiqueta MPLS

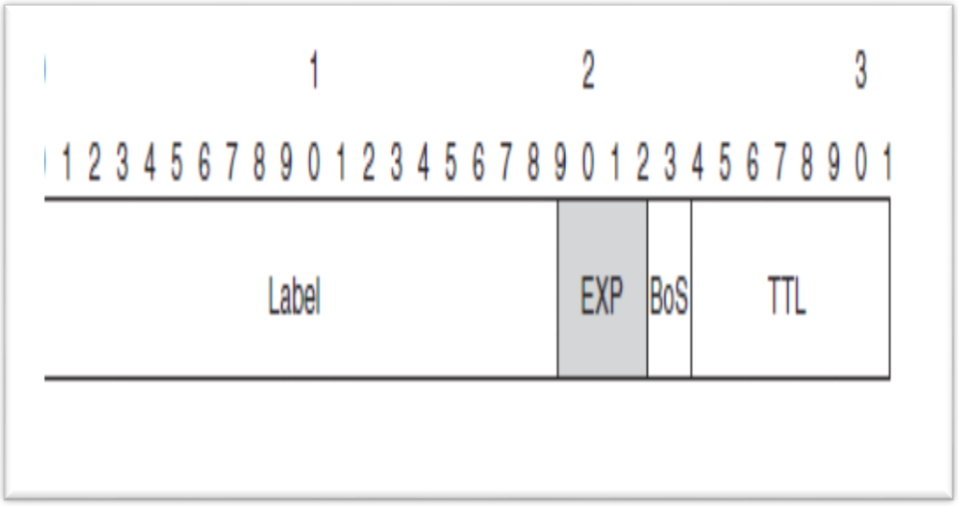

Figura 2-13: Sintaxis de una etiqueta MPLS
Fuente: (Nieto, 2010, p 30).

Como se observa en la Figura 2-13, hay tres bits EXP. Se llaman experimentales, pero son realmente usados solo para QoS.

Cuando un LSR reenvía un paquete etiquetado, solo necesita buscar la etiqueta superior en su tabla de reenvío (LFIB) para decidir dónde reenviar el paquete. Lo mismo es para la transmisión con QoS. El LSR solo necesita mirar los bits EXP de la etiqueta superior para determinar cómo tratar este paquete (Ortega, 2007, p.102).

2.6.4 Modelos de tunelización aplicados a MPLS con QoS

Servicio diferenciado proporciona a los proveedores de internet (ISP) una herramienta para administrar la calidad de servicio a través de modelos de tunelización. La tunelización es la capacidad para hacer transparentes las comunicaciones desde un borde al otro borde de una red.

A través de la utilización de etiquetas se configura los túneles de esta manera, un túnel comienza donde se coloca una etiqueta al paquete y finaliza donde se la extrae, normalmente esto ocurre en los router de borde denominados Label Switch Router PE (LSR). Los modos de tunelización o formas de transmitir los datos a través de la red son: (Cisco, 2012, p. 6).

- Modo Uniforme
- Modo Tubería
- Modo Tubería corta

2.6.4.1 Modo Uniforme

En el modo de tunelización uniforme solamente se considera una capa de calidad de servicio, es decir, los paquetes son tratados uniformemente en las redes IP y MPLS, tanto el valor de la IP como el valor EXP de MPLS son idénticos. Sin embargo, un router puede cambiar o reescribir el valor de PHB de un paquete, este cambio debe ser reflejado tanto en el campo del paquete IP como del paquete MPLS.
Este modo de tunelización funciona de la siguiente manera:

- El valor de PHB es copiado en una nueva capa superior o en el campo del DSCP, esto ocurre tanto en las redes MPLS-MPLS como en las MPLS-IP.
- El campo del PHB es de 3 bits (8 posibles tipos de PHB)
- Si el campo PHB sobrepasa los 3 bits se debe realizar una tabla de mapeo desde el valor DSCP a MPLS justo a la entrada de la red MPLS
- De la misma manera, cuando el paquete sale de la red MPLS se debe volver a mapear el campo PHB para volver a tener el valor del campo DSCP en lugar del valor del EXP.

Como se puede observar en la Figura 2-14, el funcionamiento del modo de tunelización uniforme empieza desde el Router PE1, el cual copia el valor del campo DSCP desde el paquete IP que está ingresando desde el Router CE1, en el campo EXP de MPLS. EL Router P1 modifica el campo EXP de la etiqueta superior. En el Router P2 el valor del campo EXP se copia al campo EXP inferior en el penúltimo salto del paquete. Finalmente, el Router PE copia el campo EXP al campo DSCP del paquete IP (Cisco, 2012, p. 10).

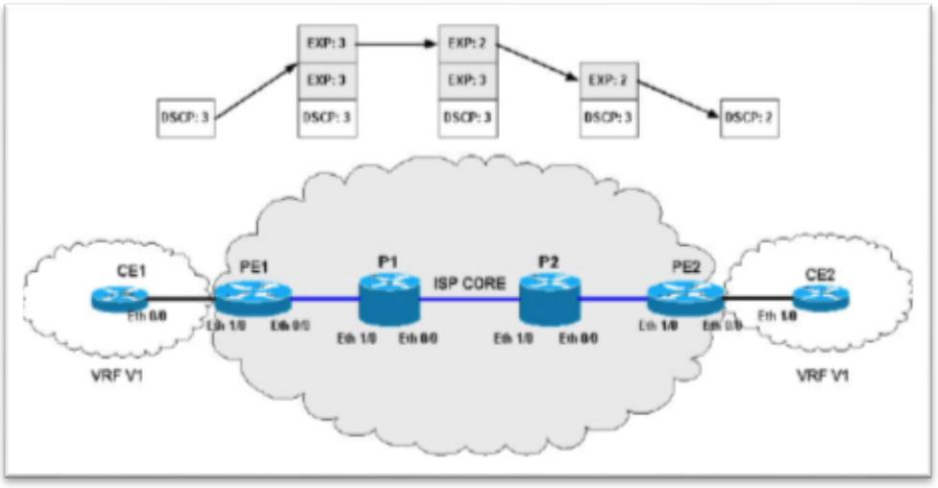

Figura 2-14: Modo Uniforme dentro de MPLS
Fuente: (Cisco, 2012, p. 10).

2.6.4.2 Modo Tubería

El modo tubería brinda una QoS en la interfaz de salida del LER de egreso, basada en el campo EXP de la cabecera MPLS recibida, aun cuando una o más etiquetas MPLS hayan sido removidas. El subcampo precedencia del paquete IP, los bits del campo EXP y el subcampo DSCP no son alterados cuando el paquete es transmitido por la red MPLS.

Cualquier cambio en el marcado de los paquetes en el interior de la red MPLS no es permanente ni propagado cuando el paquete deja la red. El LER de egreso usa el marcado que fue usado por los LSRs. Sin embargo, este LER debe remover las etiquetas impuestas al paquete original, después de guardar una copia interna del marcado para clasificar el paquete en la interfaz de salida. La figura 2-15 indica un ejemplo del comportamiento de los *routers* configurados con el modo tubería (Nieto, 2010, p 169).

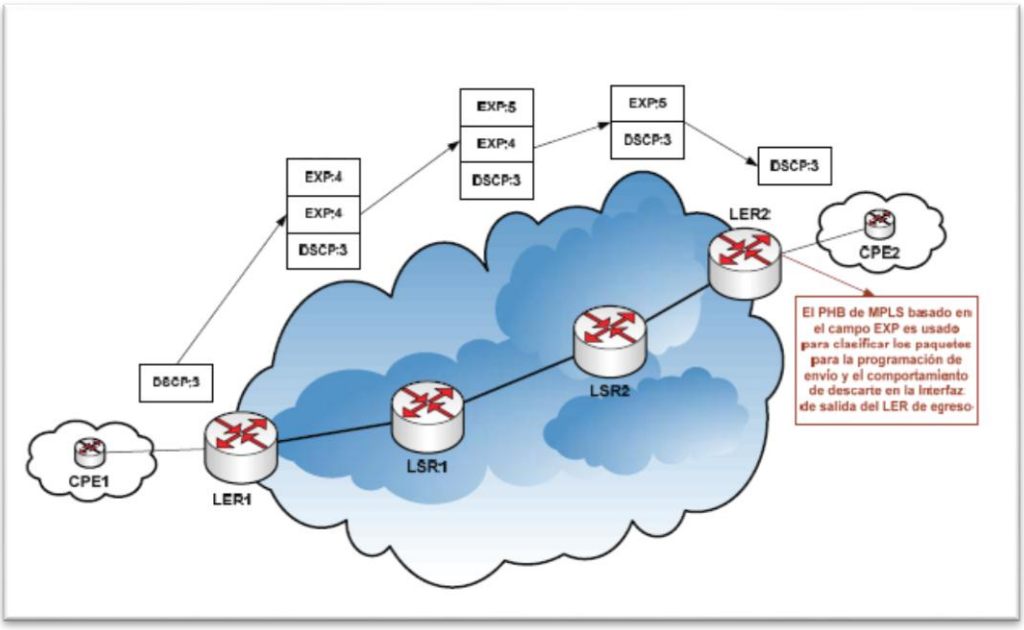

Figura 2-15: Modo de tunelización tubería
Fuente: (Nieto, 2010, p 169).

2.6.4.3 Modo de Tubería Corta

Posee la misma funcionalidad que un modelo de tubería normal con la única diferencia que las políticas de calidad de servicio, son aplicadas basándose en el valor del campo DSCP con el que llegue al destino el paquete.

Como se observa en la Figura 2-16, la transmisión del paquete es similar a un modelo de túnel, en la trayectoria hacia el destino los valores del campo EXP de las etiquetas pueden ser cambiadas, pero al final de la transmisión se utiliza el campo del DSCP para aplicar las políticas de QoS (Cisco, 2012, p. 14).

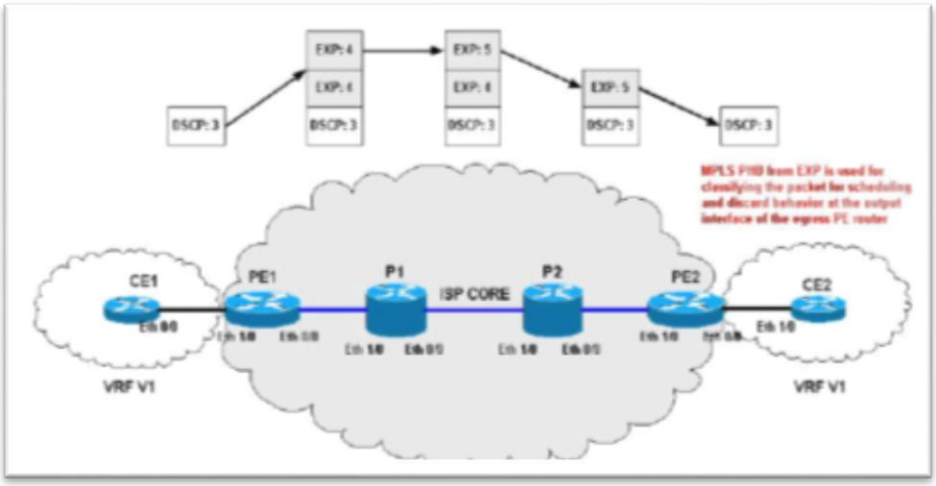

Figura 2-16: Modo de tunelización tubería corta
Fuente: (Cisco, 2012, p. 14)

2.6.5 Ventajas de una red MPLS con servicio diferenciado

Uno de los principales beneficios de los servicios basados en MPLS reside en su capacidad para aplicar calidades de servicio (QoS) mediante la priorización del tráfico en tiempo real, una prestación clave cuando se quiere introducir voz y video en las redes de datos.

Asignación eficiente de los recursos mediante métodos de gestión de cola se asigna ancho de banda de tal modo que garantiza un porcentaje de ancho de banda para el tráfico de la red.

Diferenciación de paquetes.- Cuando los paquetes IP atraviesan una red MPLS, los paquetes son diferenciados mapeando los bits de precedencia IP de los paquetes IP con los bits CoS del campo EXP de los paquetes MPLS. Este Mapeo de bits permite al proveedor de servicios mantener la garantía de extremo a extremo de la red y proveer al cliente acuerdos de niveles de servicio (SLAs).

El tráfico de VoIP, es un buen ejemplo en el que se necesita QoS. El tráfico de VoIP debe ser entregado dentro de un cierto tiempo al destino o se vuelve obsoleto. Por lo tanto, la QoS debería priorizar el Tráfico VoIP para garantizar que se entregue dentro de un determinado tiempo. Para lograr esto, el IOS de Cisco hace posible poner en cola VoIP con una prioridad más alta que el tráfico FTP o HTTP para asegurarse de que si se produce congestión, el tráfico FTP o HTTP caiga antes que el tráfico de VoIP (Ghein, 2007, p 482).

2.6.6 Desventajas de una red MPLS simple

MPLS por si solo no provee QoS, se debe implementar el mecanismo de Servicio Diferenciado para evitar los siguientes problemas:
El incremento de la cantidad de personas que trabajan de forma remota, hace que las aplicaciones en tiempo real como: VoIP, videoconferencias, videollamdas, etc tengan problemas de retardo y pérdida de paquetes.

2.7 Mecanismo de Gestión de Colas

El término “control de congestión” se usa para nombrar los distintos tipos de estrategias de encolamiento que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red.

El control de congestión involucra la creación de colas, asignación de paquetes a dichas colas basándose en la clasificación de los paquetes y la planificación de los paquetes en la cola para su transmisión (Cisco System, 2004, p 9).

Los mecanismos de gestión de colas se dividen en:

- FIFO (First-In, First-Out)
- WFQ (Weighted Fair Queueing)
- CBWFQ (WFQ basado en clases)
- CQ (Custom Queueing)
- PQ (Priority Queueing)
- LLQ (Low Latency Queueing).

2.7.1 FIFO (First-In, First-Out)

Es el tipo más simple de encolamiento, se basa en el concepto de que el primer paquete en entrar a la interfaz es el primero en salir, como se indica en la Figura 2-17. La ventaja clave de FIFO es que requiere la menor cantidad de recursos del *router*. Sin embargo, su naturaleza simplista es también su desventaja principal, ya que como los paquetes salen por la interfaz en su orden de llegada, no es posible asignar prioridades al tráfico, ni evitar que una aplicación o usuario utilice en exceso el ancho de banda disponible (Zapata, 2016, p 77)

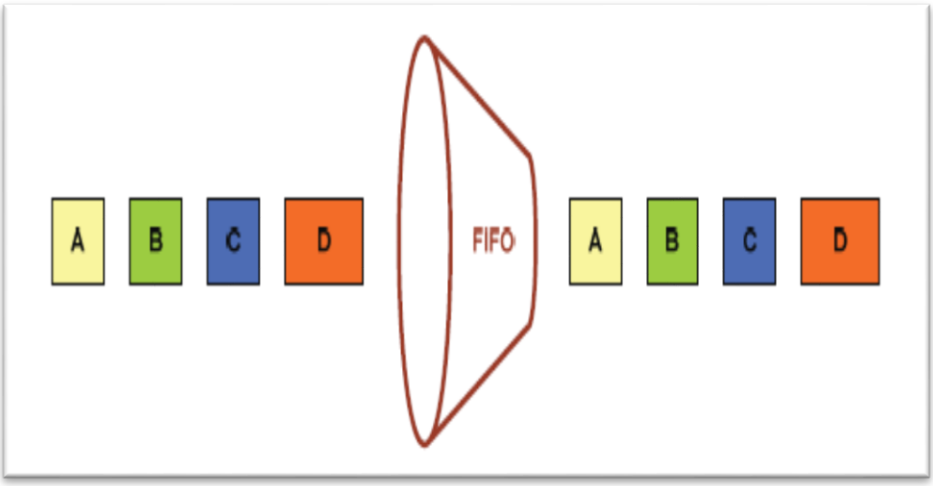

Figura 2-17: Tipo de encolamiento FIFO
Fuente: (Zapata, 2016, p 77)

2.7.2 WFQ (Weighted Fair Queueing)

WFQ es un algoritmo de encolamiento basado en flujos, que realiza dos cosas simultáneamente, programar el tráfico interactivo al frente de la cola para reducir el tiempo de respuesta y compartir equitativamente el ancho de banda remanente entre flujos de gran ancho de banda. En la Figura 2-18 se observa un esquema del encolamiento del método WFQ (Zapata, 2016, p 78).

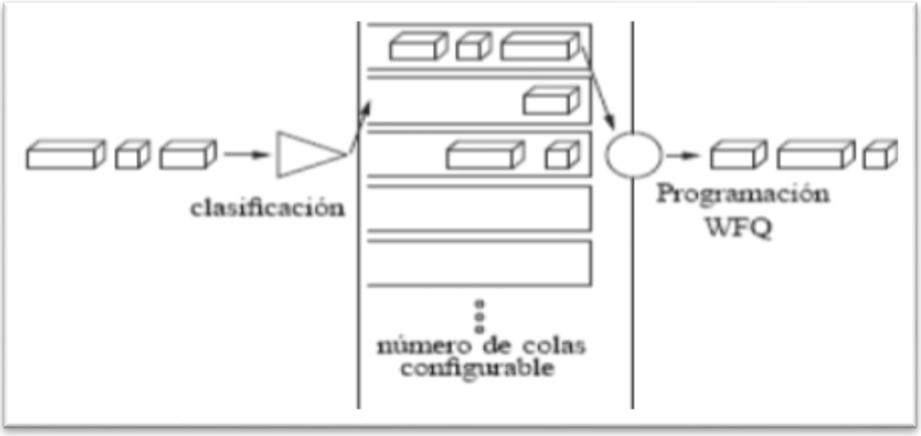

Figura 2-18: Esquema del encolamiento WFQ
Fuente: (Zapata, 2016, p 78)

WFQ proporciona un reparto equitativo del ancho de banda para cada flujo, y proporciona una planificación justa de sus colas, WFQ no puede proporcionar ancho de banda garantizado ni baja latencia para seleccionar aplicaciones. Por ejemplo, el tráfico de voz aún puede competir con otros flujos agresivos en el sistema de colas WFQ porque carece de programación de prioridad para las clases de tráfico de tiempo crítico (cisco system, 2004, vol 2, p 71).

2.7.3 CBWFQ (WFQ basado en clases)

CBWFQ permite la creación de clases definidas por el usuario, que permiten un mayor control sobre las colas de tráfico y asignación del ancho de banda.

Cada clase posee una cola separada y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase (Zapata, 2016, p 79).

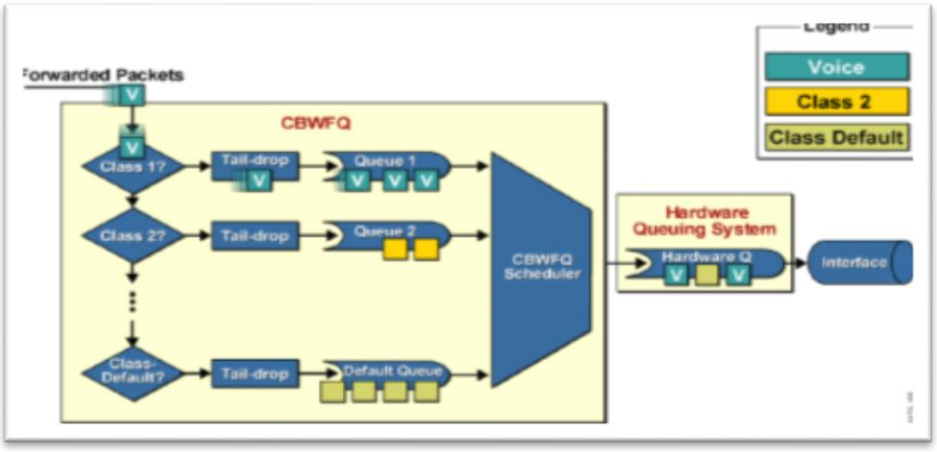

Figura 2-19: Esquema de encolamiento CBWFQ
Fuente: (Zapata, 2016, p 77).

CBWFQ extiende la funcionalidad de WFQ estándar para proporcionar soporte para clases de tráfico definidas por el usuario. Con CBWFQ, se definen clases de tráfico basadas en criterios de coincidencia que incluyen protocolos, listas de control de acceso (ACL) e interfaces de entrada para satisfacer los criterios de coincidencia de una clase. Una cola está reservada para cada clase, y el tráfico perteneciente a una clase se dirige a dicha cola.

CBWFQ admite mapas de clases múltiples para clasificar tráfico en sus colas FIFO correspondientes. Trail drop es el esquema de eliminación predeterminado de CBWFQ, aunque se puede combinar con WRED.

El esquema CBWFQ se utiliza para garantizar el ancho de banda que se basa en los pesos configurados. Un ejemplo del encolamiento CBWFQ está en la Figura 2-19.

Inserción de políticas

Cada cola tiene un número máximo de paquetes que puede contener (tamaño de cola).

- El tamaño máximo de cola depende de la plataforma.
- Después que un paquete se clasifica en una de las colas, el enrutador encolará el paquete si el límite de cola ha sido alcanzado (Tail drop dentro de cada clase).
- WRED se puede usar en combinación con CBWFQ para evitar la congestión de la clase.

CBWFQ garantiza ancho de banda de acuerdo con los pesos asignado a las clases de tráfico. Los pesos pueden definirse especificando:

- Ancho de banda (en kbps)
- Porcentaje de ancho de banda (porcentaje de disponibilidad de ancho de banda de la interfaz)

- Porcentaje del ancho de banda restante disponible. Una política de servicio no puede tener pesos asignados de diferentes tipos. (Nieto, 2010, 43).

CBWFQ le permite definir clases de tráfico y luego asignar características a esa clase. Por ejemplo, puede designar el mínimo ancho de banda entregado a la clase durante la congestión.

Para CBWFQ, el peso para un paquete que pertenece a una clase específica se determina por el ancho de banda que asignó a la clase. Por lo tanto, el ancho de banda asignado a los paquetes de una clase determina el orden en que se envían los paquetes. Todos los paquetes son atendidos justamente en base al peso; ninguna clase de paquetes puede tener prioridad absoluta. Este esquema plantea problemas para el tráfico de voz, que es en gran medida intolerante a los retardos.

2.7.4 CQ (Custom Queueing)

En CQ, el ancho de banda es asignado proporcionalmente para cada clase de tráfico diferente. CQ permite especificar el número de bytes o paquetes que serán sacados de la cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo round-robin. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles. La gestión de colas CQ permite especificar qué porcentaje de ancho de banda se dedica a cada tipo de tráfico (Cisco System, 2004, vol 2, p 59). En la Figura 2 se observa el diagrama del encolamiento CQ.

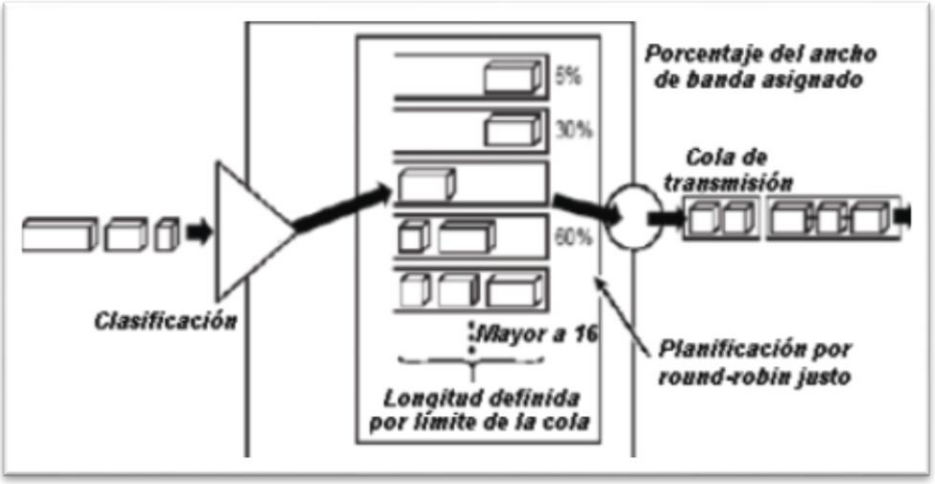

Figura 2-20: Esquema del encolamiento CQ
Fuente: (Cisco System, 2004, vol2, p 59).

2.7.5 PQ (Priority Queueing)

PQ consiste en un conjunto de cuatro colas, clasificadas desde alta, hasta baja prioridad. Cada paquete es asignado a una de estas colas, las cuales son servidas en estricto orden de prioridad. Las colas de mayor prioridad son siempre atendidas primero, luego la siguiente de menor prioridad y así. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente (Nieto, 2010, p. 82). En la Figura 2-21, se observa el esquema de encolamiento PQ.

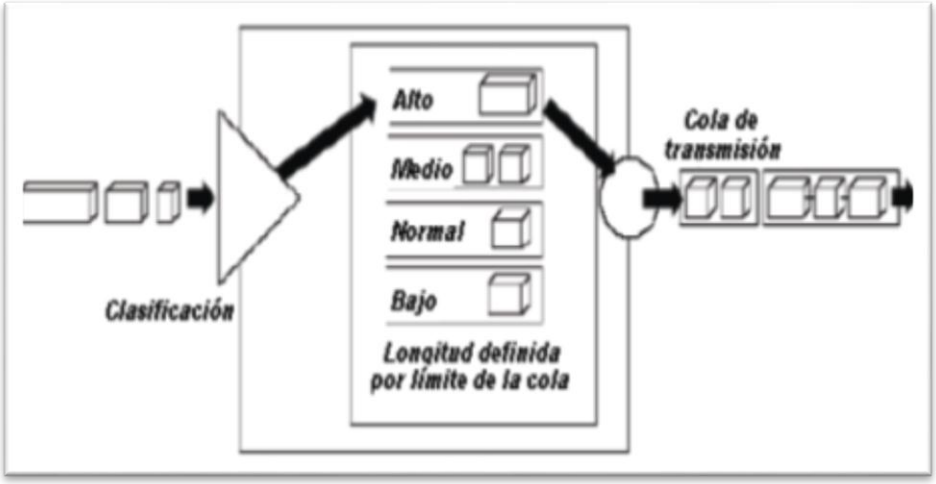

Figura 2-21: Encolamiento PQ
Fuente: (Nieto, 2010, p. 82).

2.7.6 LLQ (Low Latency Queueing)

LLQ es una mezcla entre los métodos PQ y CBWFQ y es actualmente el método de encolamiento recomendado para VoIP y telefonía IP, por lo que también trabajará apropiadamente con tráfico de videoconferencia. LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas. Si existe tráfico en la cola de prioridad, ésta es 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 prioridad. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad.

La función LLQ proporciona colas de prioridad estricta para CBWFQ, lo que reduce la inestabilidad en las conversaciones de voz. Configurado por el comando priority, LLQ habilita el uso de una simple cola de prioridad. Si LLQ se usa dentro del sistema CBWFQ, crea una cola de prioridad adicional en el sistema WFQ, que es atendido por un planificador de prioridad estricta. Por lo tanto, cualquier clase de tráfico puede ser adjunto a una política de servicio, que utiliza la

programación de prioridad, y por lo tanto se puede priorizar sobre otras clases (Cisco System, 2004, vol 2, p 293).

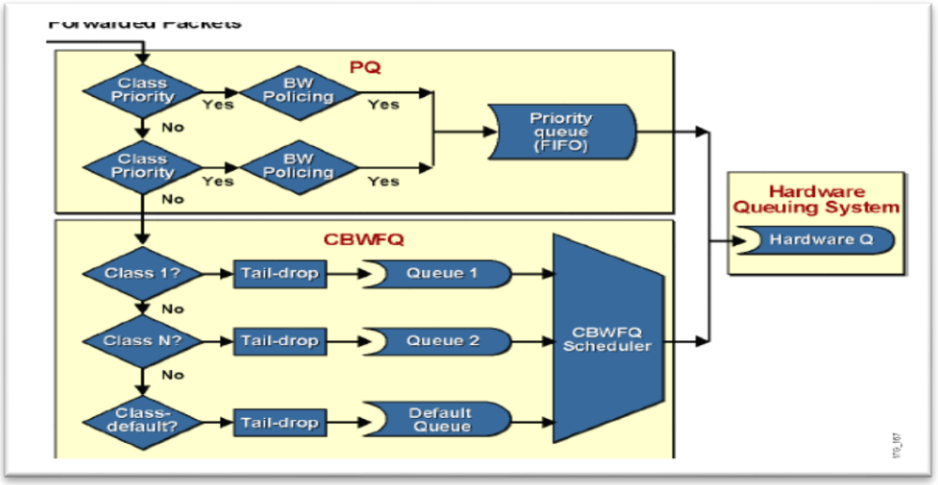

Figura 2-22: Arquitectura LLQ
Fuente: (Cisco System, 2004,vol 2, p 295).

2.8 Evasión de la congestión

Las técnicas de evasión de congestión monitorean la carga de tráfico en la red en un esfuerzo por anticipar y evitar la congestión en los "cuellos de botella" comunes. La evasión de congestión se logra mediante el descarte de paquetes. Los mecanismos de evasión de congestión se basan en la manera que los protocolos operan, con el fin de no llegar a la congestión de la red. Entre los mecanismos de evasión de congestión más usados está Random Early Detection (RED) y Weighted Random Early Detection (WRED). Si no se configura ninguno de los dos, el router usa el mecanismo de descarte de paquetes por defecto llamado tail drop (Buñay, 2013, p. 76).

2.8.1 Tail drop

Tail drop trata todo el tráfico de igual forma y no hace diferencias entre clases de servicio. En una situación de congestión las colas se llenan; cuando la cola de salida está llena y este mecanismo entra en acción, los paquetes que llegan son descartados hasta que la congestión es eliminada y la cola no está muy llena (Ortega, 2007, p.158).

2.8.2 Random Early Detection (RED)

Con este mecanismo, la eliminación de paquetes en la cola se realiza de forma aleatoria y antes de que se produzca la congestión del interfaz. De esta forma se fuerza a que conexiones TCP

aleatorias reduzcan su tasa de envío de datos, evitando que la congestión se produzca (Nieto, 2010 p. 109).

2.8.3 Weighted Random Early Detection (WRED)

WRED evita la congestión asegurándose que la cola no se llene, calculando constantemente la longitud media de la cola y comparándola con dos umbrales o límites. Si el tamaño de la cola se encuentra por debajo del umbral mínimo no se descarta ningún paquete, si es mayor que el máximo entonces todos los paquetes nuevos que lleguen serán descartados y si el tamaño se encuentra entre los dos umbrales, entonces los paquetes se descartan de acuerdo a un cálculo de probabilidad obtenido del tamaño mínimo de la cola; es decir, a medida que el tamaño medio de la cola se va acercando al umbral máximo, se va descartando un número cada vez mayor de paquetes. La probabilidad de descarte de paquetes será mayor en conexiones que utilicen un mayor ancho de banda (López y Gálvez, 2009, p. 23).

2.9 Resumen de los mecanismos de colas

En la Tabla 2-2 se muestra un resumen de los diferentes métodos de encolamiento.

Tabla 2-2: Mecanismos de colas

Mecanismo de Encolamiento	**WFQ basado en Flujo**	**CBWFW**	**CQ**	**PQ**
Número de Colas	Tiene un configurable número de colas 256 Asegura igualdad entre todo el tráfico basándose en pesos	Puede configurarse una cola por clases, hasta 64 clases Proporciona garantía de ancho de banda para las clases de tráfico definidas por el usuario	16 colas de Usuarios	4 colas
Tipo de Servicio	La prioridad estricta del encolamiento está disponible a través del uso de características de prioridad el encolamiento	El encolamiento estricto de prioridad está disponible a través de Características como LLQ	Servicio Round Robin	Colas de Alta Prioridad. Son servidas primero

Fuente: (Nieto, 2010, p. 87).
Realizador por: Chacha, Paulina, 2019

2.10 Políticas de QoS con modular QOS CLI (MQC)

MQC proporciona un enfoque modular para la configuración de mecanismos de QoS. Los administradores de red pueden introducir nuevos mecanismos de QoS y reutilizar todas las opciones de clasificación disponibles. Primero construye módulos definidos de clases de tráfico. Ver Figura 2-23. Luego define políticas de QoS y asigna clases a las políticas. Finalmente asigna módulos de políticas a las interfaces.

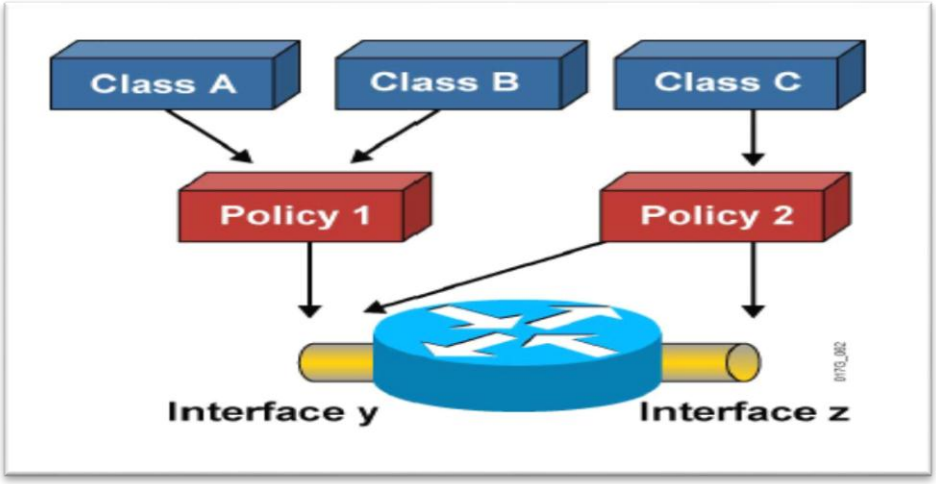

Figura 2-23: Clases de QoS
Fuente: (Cisco System, 2004, vol 2, p 320)

MQC fue introducido para permitir el soporte de clasificación que será usado con algún mecanismo de QoS. Un importante beneficio de configuración de MQC es la reusabilidad ya que permite que alguna política de QoS sea aplicable a múltiples interfaces (Cisco System, 2004, vol 2, p. 325). Para implementar QoS usando MQC se sigue estos 3 pasos:

- Configura la clasificación usando el comando class-map
- Configurar políticas de tráfico para asociar la clase de tráfico con uno o más características de QoS usando el comando policy-map.
- Fijar la política de tráfico en la entrada y salida de la interfaz o subinterfaz usando el comando service-policy.

2.10.1 Class Maps

Los class maps son usados para crear plantillas de clasificación que serán usados posteriormente en policy maps donde los mecanismos de QoS están ligados a las clases.

Un router puede configurar un gran número de class maps (límite actual 257). El class map es identificado por un nombre y cada uno contiene uno o más condiciones que determinan si un paquete pertenece a la clase. Hay dos maneras de proceder cuando existe más de una condición en la clase:

- Match all: Se debe cumplir todas las condiciones para vincular un paquete a la clase.
- Match any: Se debe cumplir al menos una condición para vincular el paquete a la clase.

Por defecto la estrategia del match de un class maps es match all. El comando match es usado para especificar varios criterios de clasificación de paquetes. Si un paquete no concuerda con ninguno de los criterios especificados Cada criterio match es evaluado para determinar el paquete se clasifica como miembro de la clase de tráfico "class-default" (Zapata, 2016, p 83).

2.10.2 Policy Maps

El policy map es usado para asignar políticas de QoS a una clase de tráfico. El comando policy-map permite configurar una política de tráfico con características de QoS que puede ser asociado con una clase, 256 clases pueden ser usadas con una policy-map (Camacho, 2015, p 54).

2.11 Códec de VOIP

Un Codec, viene del inglés coder-decoder, convierte una señal de audio analógico en un formato de audio digital para transmitirlo y luego convertirlo nuevamente a un formato descomprimido de señal de audio para poder reproducirlo. Los codecs realizan esta tarea de conversión tomando muestras de la señal de audio miles de veces por segundo.

Los códecs pueden ser clasificados en base a distintos factores que los caracterizan, como pueden ser su tasa de bits, la calidad del audio codificado, su complejidad, el tipo de tecnología que usan o el retardo que introducen (Telefonía Voz IP., 2012, p. 76).

2.11.1 Standares de Códecs

Originariamente, los códecs fueron diseñados para ser usados en el rango de frecuencias donde se concentra la mayor parte de energía, entre los 300 Hz y los 3,4 KHz. Estos códecs se conocen como de banda estrecha (NB, NarrowBand).

Con posterioridad, se han incluido códecs capaces de trabajar en rangos más amplios, entre 50 Hz y 7 KHz, considerados de banda ancha (WB, WideBand). Actualmente, la ITU-T ha estandarizado códecs de banda "superancha" (SWB, SuperWideBand), para el rango comprendido entre 50 Hz y 14 KHz, y de banda completa (FB, FullBand), para el intervalo de frecuencias de 50 Hz a 20 KHz.

En las tablas 2-3, 2-4 y 2.5 se muestran los códecs de voz más representativos pertenecientes a cada tipo de códec, según la clasificación establecida. En ellas se recoge las tasas de bit y el retraso generado en la codificación, y su aplicación básica en las comunicaciones. (Castellanos y Guzmán, 2013, p 34).

Tabla 2-3 Códec de Banda Estrecha

Codec	Nombre	Tasa de Bits (Kbps)	Retardo (ms)	Comentarios
G.711	PCM: Pulse Code Modulation	64/56	0,125	Utiliza dos posibles leyes de compresio: u-law y A-law
G.723.1	Hybrid MPC-MLQ and ACELP	6,3/5,3	37,5	Desarrollando inicialmente para videoconferencias en la PSTN. SE utiliza actualmente e VoIP
G.728	LD-CELP: Low-Delay Code Excited Linear Prediction	40/16/12,8/9,6	1,25	Diseñado para aplicaciones DCME (digital Circuit Multiplex encoding)
G.729	CS-ACELP: Conjugate Structure Algebraic Codebook Excited Linear Prediction	11,8/8/6,4	15	Ampliamente utilizado en aplicaciones de VoIP, a 8 KHz
AMR	Adaptive Multi rate	12,2 a 4,75	20	Utilizado en redes celulares GSM
iLBC	Internet Low Bitrate Codec	15,2/13,33	20/30	Utilizado en VoIP por su robustez ante pérdida de paquetes

Fuente: (Castellanos y Guzmán, 2013, p 35)
Realizador por: Chacha, Paulina, 2019

Tabla 2-4: Códec de Banda Ancha

Codec	Nombre	Tasa de Bits (Kbps)	Retardo (ms)	Comentarios
G.722	Sub-band ADPCM	64/56/48	3	Originalmente creado para audios y videoconferencias. Actualmente utilizado en servicios de telefonía de banda ancha en VoIP
G.722.1	Transform Coder	32/24	40	Usado en audio y videoconferencias
G.711.1	WideBand G.711	96/80/64	11,875	Amplia el ancho de banda del códec G.711, optimizando su uso para VoIP
G.729.1	WideBand G.729	8 a 32	49	Amplia el ancho de banda del códec G.729, optimizando su uso para VoIP con audio de alta calidad
G.722.2	AMR-WB	23,85 a 6,6,	25,375	Estándar común con 3GPP

Fuente: (Castellanos y Guzman, 2013, p 36).
Realizador por: Chacha, Paulina, 2019

Tabla 2-5: Códec de Banda Súper Ancha

Codec	Nombre	Tasa de Bits (Kbps)	Retardo (ms)	Comentarios
G.711.1 SWB	G.7.11.1 Superwideband	128 a 96	12,8125	Extensión interoperabilidad con G711 y G711.1
G.722 SWB	G.722 Superwideband	96/80/64	12,3125	Extensión interoperabilidad con G.722
G.722.1C	G.722.1	48/32/24	40	Optimizado para su uso en tiempo real
SILK	SILK	8 a 24	25	Utilizado por SKYPE

Fuente: (Castellanos y Guzman, 2013, p 37)
Realizador por: Chacha, Paulina, 2019

2.12 Simuladores de Redes de Comunicaciones

2.12.1 Graphical Network Simulator (GNS3).

Graphical Network Simulator o GNS3 es una herramienta de simulación de redes potente y muy útil para el estudio y emulación de topologías de red complejas, GNS3 se distribuye bajo licencia OpenSource y su uso es totalmente gratuito. Puede ejecutarse tanto en Linux como en Windows o MAC. GNS3 tiene una interfaz gráfica llamada Dynagen. Dynamips es el motor que permite la emulación de los IOS exactamente igual como en los equipos físicos, Dynagen se ejecuta sobre Dynamips para crear un entorno más amigable. Mediante Virtualbox y WMware también se hace posible la emulación de varios sistemas operativos sobre un PC en un ambiente virtual como Windows, Ubuntu y Linux (López y Pedraza, 2011, p 102).

2.12.2 Dynamips y Dynagen

Dynamips es el motor de emulación utilizado en GNS3 para la simulación de dispositivos Cisco y Juniper. Para efectuar las emulaciones, Dynamips utiliza una gran cantidad de RAM y de CPU.

Para asignar la memoria virtual de los routers, Dynamips utiliza archivos mapeados de memoria. Esto hará que el sistema operativo almacene en caché en la RAM las secciones de los archivos mmap que se estén utilizando. El hecho de que además, Dynamips tenga un consumo tan alto de CPU, es porque simula la CPU del router "instrucción-a-instrucción". Para optimizar la CPU, GNS3 y Dynamips utilizan el parámetro Idle-PC, que consiste en un valor que permite disminuir la ocupación de la CPU, durmiendo los procesos dynamips mientras que no se requiera que estén activos, y despertándolos y pasándolos a la CPU cuando la ejecución de la imagen IOS así lo requiere (Zapata, Pacheco, De la Torre y Vallejo, 2017, p. 64).

2.12.3 Network Simulator (NS3)

El NS3 es un simulador de redes basado en eventos discretos. Se emplea, principalmente, en ámbitos educativos y de investigación. La infraestructura software NS3 fomenta el desarrollo de modelos de simulaciones que son lo suficientemente realistas como para ser usados como un emulador de redes a tiempo real.
NS3 es una librería C++ que proporciona modelos de simulación de redes implementados como objetos C++ y con interfaces en Phyton. Los usuarios interaccionan con esta librería mediante aplicaciones C++ o Phyton que instancian unos modelos de simulación para montar el escenario de interés (Delgado, 2015, p. 18)

2.12.4 Virtual Networks over Linux (VNX)

VNX es una herramienta de código abierto, que permite la creación de escenarios de prueba virtuales, donde puedan interactuar de forma más real con escenarios de red, de forma similar a los programas GNS3, NetKit, entre otros. En base a ficheros de configuración XML permite la creación y despliegue automático de escenarios virtuales de red de una forma sencilla.

Ventajas y desventajas:
Integración de nuevas plataformas de virtualización que permiten otros sistemas operativos como Windows, Linux. Entre los hipervisores que soporta están KVM/QEMU, virtualBox, XEN, etc.

Además, se integra el uso de Dynamips y Olive, el primero es el emulador de router Cisco y el segundo de Juniper

VNX: es capaz de emular de forma limitada las funcionalidades de routers Cisco o Juniper.

VNX: es que está en constante evolución introduciendo mejoras y nuevas funcionalidades, por lo que al ser un proyecto vivo les da ventajas frente a otros (Orozco, 2017, p 43).

2.12.5 Packet Tracer

El Packet Tracer es un simulador de entorno de Redes de comunicaciones de fidelidad media, que permite crear topologías de Red, utilizando una interfaz gráfica. Ofrece el análisis de cada proceso que se ejecuta en el programa de acuerdo a la capa de modelo OSI que interviene en dicho proceso; a raíz de eso se dice que es una herramienta de gran ayuda en el estudio y aprendizaje del funcionamiento y configuración de Redes de comunicaciones.

Ventajas y desventajas:

El enfoque pedagógico de este simulador hace que sea una herramienta muy útil como complemento de los fundamentos teóricos sobre redes de comunicaciones. Packet Tracer soporta un conjunto de Protocolos de capa de aplicación simulados, al igual que enrutamiento básico con RIP, OSPF, y EIGRP, utiliza solo un pequeño número de características encontradas en el hardware real. No permite crear topologías de Red que involucren la implementación de tecnologías diferentes a Ethernet tales como Frame Relay, ATM, XDSL, Satelitales, telefonía celular entre otras (Orozco, 2017, p 77).

2.12.6 Tabla Comparativa entre los simuladores de estudio.

En la Tabla 2-6 se presenta un resumen de las características más relevantes que poseen los softwares de simulación que existen en el mercado.

Tabla 2-6: Comparación de softwares de simulación

Herramienta	**GNS3**	**Packet Tracer**	**VNX**
Licencia	GNU	Prop	GNU
S.O	Linux, Windows, Mac Os X	Linux, Windows	Linux, Windows
Facilidad	SI	SI	NO
Cisco IOS	SI	NO	SI
GUI	SI	SI	SI

Fuente: (Orozco, 2017, p 77).
Realizador por: Chacha, Paulina, 2019

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Tipo de Investigación

Por la naturaleza investigativa y experimental del proceso se define a este estudio como un compendio de diferentes métodos y técnicas a través de las cuales se conseguirán tanto las bases teóricas de fundamento, así como las métricas de resultados. Entre las utilizadas se definen las siguientes:

Exploratoria

Se desarrollará en las fases iniciales de la investigación, en la recolección de la información sobre mejores métodos de gestión de cola para una correcta aplicación de Servicio Diferenciado para lograr parámetros de rendimiento adecuado en una transmisión de voz, streaming y datos.

Descriptiva

Este tipo de investigación se utilizará específicamente en la fase de evaluación de parámetros para determinar la eficiencia de una red MPLS con servicio Diferenciado frente a una red MPLS simple.

3.2 Diseño de la Investigación

El presente trabajo de investigación es cuasi-experimental. En donde se propone simular un sistema de red MPLS con servicio diferenciado para evaluar los parámetros de QoS como son jitter, retardo y pérdida de paquetes. Los diseños cuasi-experimentales, los sujetos no se asignan al azar a los grupos ni se emparejan, sino que dichos grupos ya estan formados antes del experimento.

3.3 Métodos de Investigación

Los métodos de investigación a utilizar son los siguientes:

Método Científico

Desde un punto de vista científico y para obtener un conocimiento válido consta de 6 etapas: pregunta, observación, hipótesis, experimento, análisis y conclusiones. Se plantea la investigación basada en la evaluación de los parámetros de rendimiento de una red MPLS aplicando el mecanismo de Servicio Diferenciado. Cabe mencionar las preguntas que se pretente responder:

¿La utilización de DiffServ mejorará el rendimiento de una red MPLS?
¿Que parámetros influyen en la calidad de servicio en tiempo real?
Estas preguntas justifican los motivos por los cuales se propone realizar esta investigación, Para desarrollar el objetivo propuesto en este trabajo es necesario elaborar un marco teórico que ayude a adquirir una visión general de los criterios más relevantes dentro de esta investigación.
Se plantea una hipótesis la cual es una respuesta al problema planteado y posee una íntima relación entre el problema y el objetivo.
Se realiza la recolección de datos, y se observa el comportamiento de las variables de los dos ambientes de pruebas con el fin de determinar cuál es la solución más adecuada.
Se realiza la prueba de la hipótesis con los resultados obtenidos.
Se elabora las conclusiones y recomendaciones, producto del desarrollo de esta investigación.

Método Comparativo

Después del estudio general se deberá comparar cada uno de los parámetros de rendimiento obtenidos en una red MPLS simple versus una red MPLS con DiffServ.

3.3.1 Enfoque de la Investigación

El presente trabajo investigativo tomará un enfoque cuantitativo ya que las métricas empleadas para medir la incidencia de Diffserv en el mejoramiento de Calidad y Servicio de extremo a extremo en la transmisión de tráfico en tiempo real se conseguirán mediante D-ITG 2.61 GUI 0.92: (Distributed Internet Traffic Generator), software que mide estos parámetros de rendimiento como jitter, latencia y pérdida de paquetes.

3.3.2 Alcance Investigativo

El alcance de la presente investigación y propuesta es de tipo descriptivo que especifican las características de una red MPLS con Servicio Diferenciado y los beneficios en cuanto a Calidad y Servicio en una transmisión de aplicaciones en tiempo real.

3.3.3 Población de estudio

La población es el conjunto de todos los elementos a ser evaluados, en la presente investigación tenemos una red MPLS con DiffServ y el tráfico en tiempo real.
Los tipos de tráfico son: Voz, streaming, datos de transacción, transferencia de archivos.
Los estándares de VoIP son: G.711: bit-rate de 56 o 64 Kbps, G.722: bit-rate de 48, 56 o 64 Kbps, G.723: bit-rate de 5,3 o 6,4 Kbps, G.728: bit-rate de 16 Kbps, G.729: bit-rate de 8 o 13 Kbps.

3.3.4 Selección de la muestra

De estas poblaciones se seleccionó las muestras dirigidas para el tráfico en tiempo real basada en los siguientes criterios:
Los paquetes de VoIP deben recibir un trato especial, son muy sensibles a retardos y necesitan un ancho de banda garantizado. Es necesario ofrecer cierta QoS para disminuir el retardo.
Los datos son los paquetes que más se envían en la red.
En la empresa pública como lo es el MTOP se tiene como políticas priorizar el tráfico de VoIP y de datos, al ser los más utilizados e importantes.
Para los estándares de VoIP se tiene los más utilizados según la ITU-T G (Series: Transmission systems and media, digital systems and networks) son: G.711, G.729 y G.723.1.

3.3.5 Tamaño de la muestra

Se trabajará con toda la muestra establecida.

3.3.6 Validación de Instrumentos

Los routers usados en la simulación son cisco 7200 y C3640
Los IOS de Cisco que se emplearon para la implementación del escenario fue i86bi-linux-l3-adventerprisek9-15.5.2T que representa a un router 7200.

Los requerimientos mínimos para la ejecución del simulador GNS3 son:

- Sistema Operativo Windows 8 o Superior de 64 bits
- 2 o más núcleos lógicos
- Habilitar la función de virtualización en la BIOS
- 6 Gb de memoria RAM
- 20 Gb de Espacio Libre

3.4 Técnica de Recolección de Datos Primarios y Secundarios

La recolección de datos se obtuvo de libros, paper, tesis relacionads al tema de investigación. Para determinar si aplicando la tecnología DiffServ sobre las redes MPLS se tendrá una adecuada QoS extremo a extremo en la transmisión en tiempo real se realizaron los siguientes escenarios:

- Redes MPLS: con la configuración básica del protocolo de distribución de etiquetas (LDP) y el adecuado protocolo de enrutamiento para redes IP en este caso se uso OSPF, posteriormente se inyecta tráfico de voz, streaming y datos y se evalúan los parámetros de calidad y servicio tomando las mediciones de jitter, latencia y pérdida de paquetes.
- Redes MPLS con DiffServ: En este escenario se configurará las políticas de entrada y salida para las interfaces que se aplicarán sobre redes MPLS, midiendo los indicadores de QoS.

Todos estos datos son organizados en tablas de valoración, y posteriormente se comparará con valores de umbrales permitidos en los parámetros de QoS.

3.5 Escenario de Pruebas

3.5.1 Topología completa del Escenario de Prueba

El esquema presentado en la Figura 3-1 es un modelo de red de conectividad basado en la infraestructura que posee el Ministerio del Transporte y Obras Públicas de las provincias de la ZONA 3, el cual está constituido por las redes de las provincias de Tungurahua, Chimborazo y Cotopaxi interconectadas con la matriz en Quito. Para el presente análisis se optó por seleccionar la sede en la ciudad de Ambato para obtener los datos necesarios con los cuales se configuraron las simulaciones en el emulador GNS3. Como se puede observar en la Figura 3-1 tenemos los Router de borde PE1, PE2, PE3 y PE4 que se encuentran en el borde del proveedor, en este caso

el proveedor de internet es CNT. En el otro lado de la red están los Routers CE1, CE2, CE3, CE4 que corresponde a los Router de borde del cliente (Customer Edge).

La red MPLS se encuentra usando un protocolo IGP como es el protocolo de enrutamiento OSPF, que generará las tablas de enrutamiento y será aprovechado por el protocolo LDP (Label Distribution Protocol) para generar el intercambio de etiquetas.

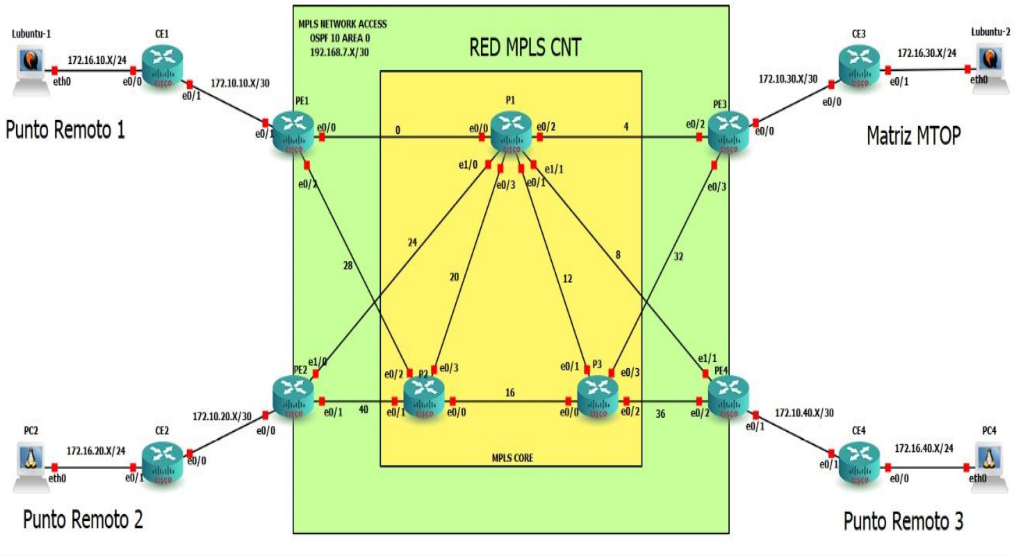

Figura 3-1: Escenario de Pruebas
Elaborado por: Chacha, Paulina. 2019

El Ministerio de Transporte utiliza tecnología IP, su proveedor de Servicio de Internet es CNT que mantiene tecnología IP/MPLS y está diseñada bajo el modelo jerárquico de tres capas. La capa core está formada por 3 nodos que concentran la mayor cantidad de tráfico, Los equipos de estos nodos trabajan como LSRs y son denominados como P1, P2 y P3 y corresponden al router C7200.

Adicionalmente, la capa core tiene otros equipos que distribuyen el tráfico a grandes velocidades y trabajan como LERs a la vez, para permitir el paso entre las tecnologías IP y MPLS. Estos nodos enrutan el tráfico entrante a la red MPLS, usando un protocolo de señalización de etiquetas y distribución de tráfico saliente. Estos equipos son denominados como: PE1, PE2, PE3 y PE4 y corresponden al router C7200.

Los routes PE forman parte de la capa de distribución debido a las funciones que realizan como la implementación de políticas de ruteo y de red, filtrado de paquetes, seguridad entre otras. La capa de distribución implementa enlaces redundantes para casos de fallas.

La capa de acceso es la capa que permite la interconexión de los clientes de la red del MTOP con la red de CNT, estos equipos son denominados CE1, CE2, CE3, CE4 y corresponden al router C3640.

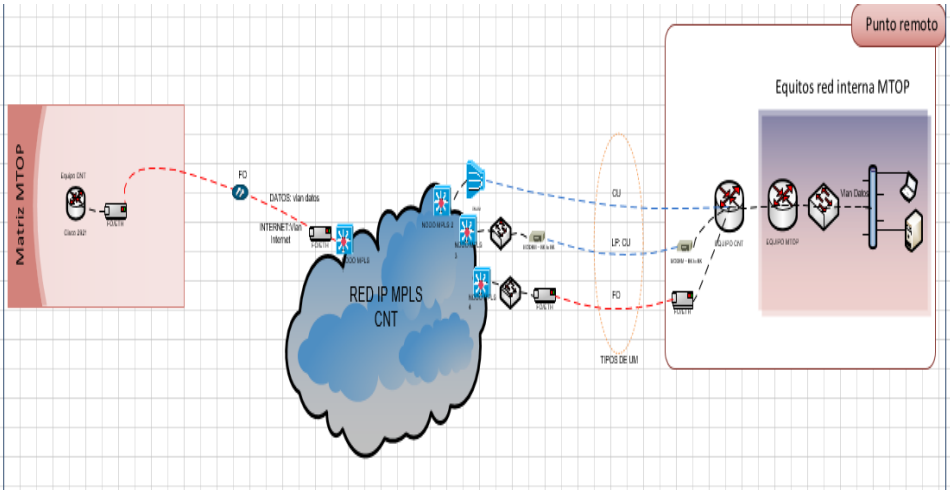

Figura 3-2: Diagrama General del Ministerio de Transporte y Obras Públicas
Elaborado por: Chacha, Paulina. 2019.

3.5.2 Asignación de Direcciones y Equipos.

Por tratarse de una red MPLS, fue preciso realizar adaptación del valor de MTU soportado. El valor por default de MTU en redes IP convencionales en de 1500 bytes, pero MPLS agrega una cabecera adicional de 4 bytes por etiqueta. Por lo tanto, se decidió establecer un valor de MTU de 1700 bytes en todos los enlaces que son parte del núcleo de red MPLS. En la Tabla 3-1 se detalla el direccionamiento de los diferentes equipos de la red.

Tabla 3-1: Asignación de direcciones IP a las interfaces de los Routers

Equipo	Interfaz	Dirección de red
PE1	ethernet 0/0 ethernet 0/1 ethernet 0/2 Loopback 0	192.168.7.1 172.10.10.2 192.168.7.29 1.1.1.1
PE2	ethernet 0/0 ethernet 0/1 ethernet 1/0 Loopback 0	192.168.7.17 192.168.7.42 192.168.7.26 2.2.2.2
PE3	ethernet 0/0 ethernet 0/2 ethernet 0/3 Loopback 0	172.10.30.1 192.168.7.6 192.168.7.33 3.3.3.3
PE4	ethernet 0/1	172.10.40.1

	ethernet 0/2 ethernet 1/1 Loopback 0	192.168.7.38 192.168.7.10 4.4.4.4
CE1	ethernet 0/0 ethernet 0/1	172.16.10.1 172.10.10.1
CE2	ethernet 0/0 ethernet 0/1	172.10.20.1 172.16.20.1
CE3	ethernet 0/0 ethernet 0/1	172.10.30.2 172.16.30.1
CE4	ethernet 0/0 ethernet 0/1	172.16.40.1 172.10.40.2
PC1	Ethernet 0	172.16.10.10
PC2	Ethernet 0	172.16.20.0
PC3	Ethernet 0	172.16.30.10
PC4	Ethernet 0	172.16.40.10

Realizador por: Chacha, Paulina, 2019

3.5.3 Elección de modelo de gestión de Colas

La medida para control de congestión seleccionada será el modelo Low Latency Queueing (LLQ) que brindará prioridad al tráfico de voz para la clase EF, adicionalmente se incluye CBWFQ con esto se podrá especificar la cantidad de ancho de banda para cada una de las clases de servicio AF.

LLQ aplica colas de prioridad estricta a CBWFQ. Las colas de prioridad estricta permiten transmitir datos sensibles al retardo, como la voz para ser enviados primero, dando un tratamiento preferencial a los datos sensibles al retraso sobre otro tráfico.

Con el propósito de evitar la congestión, se configurará el mecanismo Weighted Random Early Detection (WRED) para proporcionar un descarte aleatorio en base a los diferentes valores de AF con sus diferentes preferencias de descarte.

3.5.4 Modelamiento del servicio diferenciado (DIFFSERV)

Según la calidad y servicio de extremo a extremo del sistema de Telecomunicaciones y protocolos de internet armonizados sobre redes (TIPHON). Se define 5 clases de servicios: Premium, Oro, Plata, Bronce y Best Effort para priorizar el tráfico. La clase premium tendrá el campo DSCP con el valor EF (Expedited Forwarding) que corresponde a la prioridad más alta cuyo valor es igual a 101110 y que manejará el tráfico de voz que es muy sensible a retardos. A las clases Oro, Plata y Bronce se le asignará los valores de AF (Asured Forwarding) y todo el tráfico que no coincida en algunas de estas clases será tratado como Best Effort o mejor esfuerzo, esta clasificación se la

toma como base del proyecto realizado por (Nieto, 2010, p 196). Esta clasificación de la realiza tal como se observa en la tabla 3-2.

Tabla 3-2: Clasificación y Asignación de valores DSCP al tráfico de red

CoS	Valor DSCP	Tipo de aplicación
Premium	EF=46	VoIP (TDMoIP, RTP, Skype, Net2Phone, UniqueFone, SIP, H.323)
Oro	AF11=10	Videoconference (RSTP)
	AF13=14	Applications streaming personalized
Plata	AF21=18	Base de datos, SSL, IPSec, GRE, L2TP
	AF23=22	Transacciones web (HTTPS), SFTP
Bronce	AF31=26	SNMP, TELNET, SSH
	AF33=30	SMTP, POP3, IMAP4, VNC, Syslog, DHCP, ICMP
Mejor Esfuerzo	BE=0	P2P, juegos, HTTP, Facebook, FTP, NFS, DNS y el resto de aplicaciones que cursan por la red y que no recibirán ninguna garantía de QoS

Fuente: (ETSI, 2000, p. 8, **Recomendación** UIT-T G.1010, 2001, p. 14)
Realizador por: Chacha, Paulina, 2019

La clase Premium implementará un encolamiento LLQ para controlar la congestión ya que requiere parámetros de rendimiento en jitter, latencia y pérdida de paquetes muy bajos y un ancho de banda asegurado en aplicaciones en tiempo real.

Las clases Oro, Plata y Bronce que dispone de valores de AF (Asure Forwarding) en el campo DSCP, empleará el encolamiento CBWFQ. Si no se especifica mecanismos de evasión de la congestión se usará el que viene por defecto, conocido como tail drop.

La clase mejor esfuerzo (Best Effors) tiene un valor en el campo DSCP igual a cero y no recibirá ningún tratamiento de QoS. En la Tabla 3-2 se presenta clasificación y asignación de los valores DSCP que puede llegar a tener el tráfico.

3.5.5 Expedited Forwarding (EF) PHB

Definido en el RFC 2598, el EF PHB tiene un valor de DSCP igual a 101110 y ofrece un servicio de bajas pérdidas, baja latencia, bajo jitter y un ancho de banda asegurado para aplicaciones en tiempo real. Esta clase de servicio se la ha denominado Premium por requerir un servicio con mejores prestaciones en sus parámetros de calidad de servicio.

El tipo de encolamiento que se utilizará en este PHB para controlar la congestión será Low Latency Queueing (LLQ), ya que tiene preferencia absoluta sobre las colas del mecanismo

CBWFQ configurado en el AF PHB, de manera que el tráfico asignado sea atendido de forma inmediata y en caso de que no exista tráfico en la cola, el resto de colas sean atendidas, evitando el desperdicio de recursos.

3.5.6 Assured Forwarding (AF) PHB

El comportamiento por salto (PHB) de Assured Forwarding se manejará con 3 clases: clase 1, clase 2, clase 3 que van a corresponder a las clases de servicio Oro, Plata y Bronce respectivamente, definidas en los Services Level Agreements (SLAs) que la empresa desea ofrecer, con 2 categorías de preferencia de descarte, bajo y alto. La Tabla 3-3 indica los valores DSCP asignados a las clases de servicio de los SLAs. Se creará 3 clases de colas con el mecanismo CBWFQ.

Tabla 3-3: Valores DSCP para las clases de servicio Asured Forwarding (AF)

% de descarte	ORO	PLATA	BRONCE
Bajo	AF11=001010	AF21=010010	AF31=011010
Alto	AF13=001110	AF23=010110	AF33=011110

Fuente: (Cisco System, 2004, vol 2, p 200)
Realizador por: Chacha, Paulina, 2019

3.5.7 Default PHB

El default PHB tiene un valor de DSCP igual a 000000 según el RFC 2474 y el servicio ofrecido es igual al tradicional "mejor esfuerzo". El tráfico perteneciente a este PHB no recibirá ningún tipo de tratamiento y será atendido luego de los PHBs EF y AF.

3.5.8 Asignación de parámetros de QoS aceptables para las clases de Servicio

Los acuerdos de niveles de servicios (SLAs) ofrecidos por los ISP, las clses de servicios pueden variar de acuerdo a las necesidades de las empresas; para nuestro estudio se trabajará con 4 clases de servicios que son Premium, Oro, Plata y Bronce, de acuerdo a parámetros que se detallan en la Tabla 3-4 con respecto a paquetes entregados, latencia y jitter.

Tabla 3-4: Parámetros comprometidos por CoS

Parámetro	Clase de Servicio (CoS)			
	Premium	**Oro**	**Plata**	**Bronce**
Paquetes entregados	99,9%	99,5%	99,0	-
Latencia	28 ms	68 ms	-	-
Jitter	15 ms	-	-	-

Fuente: (Nieto, 2010, p 199).
Realizador por: Chacha, Paulina, 2019

3.6 Correspondencias de valores del campo DSCP y EXP.

La Tabla 3-5 indica la correspondencia entre los valores DSCP definidos en los PHBs descritos para clasificar el tráfico transmitido a través de la red IP y los valores exp7, exp 0 del campo EXP, que serán mapeados en los nodos de borde LERs de la red MPLS

Tabla 3-5: Mapa de Correspondencia entre el subcampo DSCP y el campo EXP

CoS	Valor DSCP	Valor EXP
Premium	EF	exp7
Oro	AF11	exp6
	AF13	exp5
Plata	AF21	exp4
	AF23	exp3
Bronce	AF31	exp2
	AF33	exp1
Mejor esfuerzo	BE	exp0

Fuente (Nieto, 2010, p 196).
Realizador por: Chacha, Paulina, 2019

3.7 Configuración de equipos en la red MPLS

3.7.1 Configuración ***de direcciones IP de las interfaces en de red IP/MPLS***

En el anexo A.1 muestra los comandos necesarios para asignar las direcciones IP a todas las interfaces de la red MPLS y red IP de acuerdo a la Tabla 3-1.

3.7.2 Configuración del Protocolo de enrutamiento IGP en la red IP /MPLS

El comando necesario para implementar un protocolo de enrutamiento interno (IGP) se observa en el anexo A.2. Dentro de la red MPLS se ha escogido el protocolo IGP conocido como OSPF porque es un protocolo de enrutamiento dinámico que detecta rápidamente los cambios producidos en la topología de un sistema autónomo y calcula las nuevas rutas sin bucles de enrutamiento, luego de un periodo rápido de convergencia.

La conexión entre la red IP que se encuentra en lado del customer y la red MPLS que corresponde al proveedor de servicios se la realiza por medio de una enrutamiento estático.

3.7.3 Configuración básica de MPLS

Para activar la funcionalidad de MPLS se habilita primero ip cef (Cisco express forwarding) para permitir el modo de procesamiento de paquetes de cisco con funciones de MPLS. Especificando el rango de etiquetas que se usará en cada router y también se activará el protocolo de distribución de etiquetas LDP para activar la comunicación de etiquetas dentro de la nube MPLS. Los comandos de configuración se encuentran en el anexo A.3

3.7.4 Configuración de calidad de servicio con DIFFSERV

3.7.4.1 Configuración de mapas de clases para el router PE en la red MPLS

El mecanismo DiffServ consiste en clasificar el tráfico entrante o saliente en diferentes mapas de clases y realizar el marcaje para posteriormente aplicar mapas de políticas de tráfico de acuerdo a los requerimientos de la empresa.

En este punto se realizará mapas de clases para agrupar los paquetes IP de acuerdo al campo DSCP, por ejemplo cuando el campo DSCP del paquete IP tenga un valor de AF11, se creará una clase de nombre IP-AF11. Toda la configuración detallada se encuentra en el anexo A.4.

3.7.4.2 Configuración de política en el router PE

En esta sección se configura un mapa de política de nombre DSCP-EXP, aplicado al ingreso del router PE para definir el comportamiento del campo EXP en la red MPLS, se realiza un mapeo del campo DSCP con su correspondiente valor para el campo EXP, la configuración se encuentra en el anexo A.5.

3.7.4.3 Aplicar políticas sobre las interfaces de entrada y/o Salida

La política denominada DSCP-EXP se aplicará a las interfaces de entrada del router PE ya que consiste en un agrupamiento de los campos DSCP a su respectivo valor de campo EXP, que servirá para aplicar modelos de gestión de cola. Ver anexo A.6.

3.7.4.4 Creación de los mapas de clases Premium, Oro, Plata y Bronce

Se crea las clases de mapas denominadas MPLS-premium, MPLS-Oro, MPLS-Plata, MPLS-Bronce, la configuración se encuentra en anexo A.7

3.7.4.5. Configuración de gestión de cola CBWFQ en Router Cisco

El método de gestión de cola CBWFQ, se aplicará en las 4 clases de servicio que se han elegido para clasificar el tráfico según el grado de prioridad es así que contamos con los 4 grupos como son: MPLS-Premium, MPLS-Oro, MPLS-Plata y MPLS-Bronce, se asignará un porcentaje de ancho de banda a cada clase del 29%, 21%, 15% y 10% respectivamente, estos valores fueron extraídos del trabajo previo de (Delgado H., 2015).

La gestión de colas se encuentra configurada por defecto como WFQ para interfaces menores de 2Mbps. El comando para desplegar todas las políticas de servicio aplicados a una interfaz se visualiza con el comando show policy-map interface. La configuración se encuentra en el anexo A.8.

3.7.4.6. Configuración de Low-Latency Queuing

A la clase MPLS-premium se le aplicará la característica de LLQ que es proporcionar una cola de prioridad estricta para CBWFQ. Las cola de estricta prioridad permite trabajar con datos sensible al retardo como voz, otorgando un trato preferencial sobre otro tráfico. Sin LLQ la característica de CBWFQ proporciona colas equitativas basadas en pesos y se define clases sin estrictas prioridades disponibles para el tráfico en tiempo real.

La función LLQ proporciona colas de prioridad estricta para CBWFQ, lo que reduce la inestabilidad en las conversaciones de voz. LLQ permite el uso de una única y estricta cola de prioridad dentro de CBWFQ. Para enrutar el tráfico de clase a la cola de prioridad estricta, se configura el comando priority para la clase después de que se especifique el nombre de la clase

dentro de un mapa de políticas. Un mapa de políticas, puede otorgarle a una o más clases el estado de prioridad. Los comandos para su configuración se pueden revisar en el anexo A.9.

3.7.4.7. Aplicar políticas de QoS a la salida del router PE

En los anexos A.10 se aplica las políticas de nombre política_MPLS-PHBs a las interfaces de salida del router PE que concierne con el comportamiento transparente que se llevará dentro de la nube MPLS.

3.7.4.8. Configuración de políticas a la salida de la red MPLS hacia la red del Customer

Se crea un mapa de políticas denominada política_IP-PHBs que está conformado por 4 clases como son: IP-premium, IP-oro, IP-plata. IP-bronce, este comando vuelve a modificar el campo DSCP para determinar comportamiento dentro de la red IP. Esta configuración se encuentra en el anexo A.11

3.7.4.9. Aplicar las políticas a la salida de la red MPLS hacia la red del Customer

En el anexo A.12 se encuentra la configuración para aplicar a las interfaces de salida las politicas de PHB que se aplicará de acuerdo a las Clases de Servicio.

3.7.5 Configuración del generador de tráfico D-ITG

La configuración de la instalación del inyector de tráfico D.ITG se encuentra en el anexo A.13

3.8 Características de los Servicios requeridos.

Los servicios que más se utiliza dentro del Ministerio de Transportes y Obras Públicas y que necesitan ser gestionados son:

- Servicios de Telefonía IP (Voz)
- Servicio de Videoconferencia (Streaming)
- Servicios Web y de Email (Datos)

Las características o parámetros que se emplearon para configurar cada uno de los tráficos se resumen en la Tabla 3-6. Para la transmisión del servicio de telefonía IP (Voz) se utilizó el estándar G.711 que es el más utilizado según (López y Gálvez, 2009, p. 23), el tiempo para la obtención de la muestra se determinó en 2 minutos (120000 ms). De igual manera para el servicio de Videoconferencia (Streaming) se determinó 5 minutos (300000 ms) con tráfico UDP. Para los

Servicios Web y de Email se simuló un tráfico TCP con requerimientos y respuestas (tráfico ida-vuelta), el tiempo de muestreo se determinó en 100 segundos (100000 ms).

Tabla 3-6: Características de los flujos de datos

	Tamaño de Paquete (Byte)	Nº Paquetes / Segundo	Ancho de Banda (kb/s)	Tiempo Simulación (ms)
Tráfico de Voz	120 (G. 711)	100	96.1	120000
Tráfico Streaming	1024	4000	33664	300000
Tráfico de Datos	512	2000	4416	100000

Elaborado por: Chacha, Paulina, 2019

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1 Proceso para la evaluación de la arquitectura MPLS

Para la evaluación de la arquitectura MPLS se extrajo parámetros (Delay, Jitter y Paquetes Perdidos) de la red con la finalidad de cuantificar y valorar su rendimiento dentro de un marco de Servicios Diferenciados (DiffServ). Para la obtención de estos parámetros se empleó la topología de red anteriormente presentada, adicionalmente se le configuró los servicios (tráficos) que más se utilizan dentro de la red del Ministerio de Transporte y Obras Públicas (Datos, Streaming y Voz), a través del generador de tráfico D-ITG.

4.1.1 Parámetros de Rendimiento

4.1.1.1 Latencia (Delay)

La latencia o retardo es la demora o tiempo que se tarda un paquete en transferirse de un origen a un destino. La Tabla 4-1 resume los valores del retardo para cada una de los servicios en sus diferentes niveles de prioridad, basándose en los estándares o recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p.

Tabla 4-1: Valores de la Latencia para los diferentes servicios.

Nivel de Calidad de Servicio	Servicio	Valor del Retardo (ms)
0	Tiempo real, alta interacción, sensible al retardo (Voz y video en tiempo real)	100
1	Tiempo real, interactivo, sensible al retardo (Voz y Video en tiempo real de menor calidad)	150
2	Datos de alta prioridad (Transaccionales altamente interactivos)	200
3	Datos de media prioridad (Datos transaccionales interactivos)	225
4	Datos de baja prioridad (transacciones cortas, datos en grandes cantidades, flujo continuo de video streaming)	250
5	Datos de mejor esfuerzo	300

Fuente: (Nieto, 2010, p 196).
Elaborado por: Chacha, Paulina, 2019

En base a los valores que se tiene en la Tabla 4-1, se resumió y estableció los rangos del Retardo (Delay) para cada uno de los servicios o tráfico de datos que se utilizaron para el presente análisis, los cuales se resumen en la Tabla 4-2.

Tabla 4-2: Valoraciones cualitativas de la Latencia.

Tipo de Servicio	Excelente	Bueno	Malo
Voz	<100ms	>100ms y <150ms	>150ms
Streaming	<=100ms	>100ms y <=250ms	>250ms
Datos	<250ms	>250ms y <300ms	>300ms

Fuente: (Buñay, 2013, p 104)
Elaborado por: Chacha, Paulina, 2019

4.1.1.2 Jitter.

Debido al retardo que se produce en los flujos de datos se genera un problema llamado Jitter que aparece por la congestión de la red, especialmente por una incorrecta sincronización de bits entre los elementos de red.

En la Tabla 4-3 se resume los valores del Jitter para cada uno de los servicios en sus diferentes niveles de prioridad, basándose en los estándares o recomendaciones de la UIT-T, G.1010, Y.1541 y la IEEE 802.1p.

Tabla 4-3: Valores del Jitter para los diferentes servicios.

Nivel de Calidad de Servicio	Servicio	Valor del Jitter (ms)
0	Tiempo real, alta interacción, sensible al retardo (Voz y video en tiempo real)	45
1	Tiempo real, interactivo, sensible al retardo (Voz y Video en tiempo real de menor calidad)	50
2	Datos de alta prioridad (Transaccionales altamente interactivos)	55
3	Datos de media prioridad (Datos transaccionales interactivos)	N/A
4	Datos de baja prioridad (transacciones cortas, datos en grandes cantidades, flujo continuo de video streaming)	N/A
5	Datos de mejor esfuerzo	N/A

Fuente: Fuente: (Buñay, 2013, p 104)
Elaborado por: Chacha, Paulina, 2019

En base a los valores que se tiene en la Tabla 4-3, se resumió en la Tabla 4-4 los rangos del Jitter para cada uno de los servicios o tráfico de datos que se utilizaron para el presente análisis.

Tabla 4-4: Valoraciones cualitativas del JITTER.

Tipo de Tráfico	Excelente	Bueno	Malo
Voz	<40ms	>40ms y <50ms	>50ms
Streaming	<=35ms	>35ms y <=65ms	>65ms
Datos	<55ms	>55ms y <70ms	>70ms

Fuente: (Buñay, 2013, p 105)
Elaborado por: Chacha, Paulina, 2019

4.1.1.3 Paquetes Pérdidos.

Tomando las referencias de las recomendaciones UIT-T G.1010, Y. 1541 IEEE 802.1p se resume en la Tabla 4-5 los valores del porcentaje de la pérdida de paquetes para cada uno de los servicios en sus diferentes niveles de prioridad.

Tabla 4-5: Porcentaje de la Pérdida de Paquetes para los diferentes servicios.

Nivel de Calidad de Servicio	Servicio	Pérdida de Paquetes (%)
0	Tiempo real, alta interacción, sensible al retardo (Voz y video en tiempo real)	1%
1	Tiempo real, interactivo, sensible al retardo (Voz y Video en tiempo real de menor calidad)	3%
2	Datos de alta prioridad (Transaccionales altamente interactivos)	3%
3	Datos de media prioridad (Datos transaccionales interactivos)	5%
4	Datos de baja prioridad (transacciones cortas, datos en grandes cantidades, flujo continuo de video streaming)	5%
5	Datos de mejor esfuerzo	5%

Fuente: (Buñay, 2013, p 106)
Elaborado por: Chacha, Paulina, 2019

Conforme a los valores que se tiene en la Tabla 4-5, se resumió en la Tabla 4-6 los rangos del porcentaje de pérdida de paquetes para cada uno de los servicios o tráfico de datos que se utilizaron para la simulación.

Tabla 4-6: Valoraciones cualitativas de los Paquetes Perdidos

Tipo de Tráfico	Excelente	Bueno	Malo
Voz	<1%	>1% y <3%	>3%
Streaming	<=2%	>2% y <=5%	>5%
Datos	<3%	>3% y <5%	>5%

Fuente: (Buñay, 2013, p 104)
Elaborado por: Chacha, Paulina, 2019

4.2 Análisis de las muestras del escenario Sin Calidad de Servicio

4.2.1 Análisis del Tráfico de Voz sin QoS

En la Tabla 4-7 se resume los promedios del Retardo, Jitter y Paquetes perdidos obtenidos de la simulación de la trasmisión de Voz IP sin Calidad de Servicio. El valor del Retardo (Delay) en este escenario es de ochocientos doce punto quince mili segundos (812.15 ms), el valor del Jitter es de catorce punto noventa y ocho mili segundos (14.98 ms) y el promedio de los paquetes perdidos es de seis punto ochenta por ciento (6.80%).

Tabla 4-7: Promedio de los parámetros del Tráfico de Voz sin QoS

Promedio Retardo (Delay)	Promedio Jitter	Paquetes Pérdidos
812.15 ms	14.98 ms	6.80%

Elaborado por: Chacha, Paulina, 2019

En la Figura 4-1, Figura 4-2 y Figura 4-3 se aprecian los valores obtenidos del retardo, jitter y pérdida de paquetes con el tráfico de voz en un escenario sin calidad de servicio respectivamente

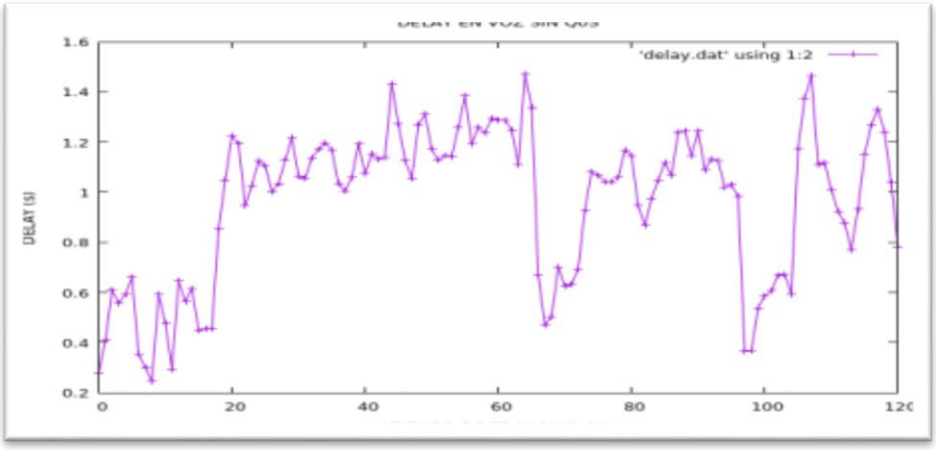

Figura 4-1: Retardo en la transmisión de Voz sin QoS
Elaborado por: Chacha, Paulina, 2019

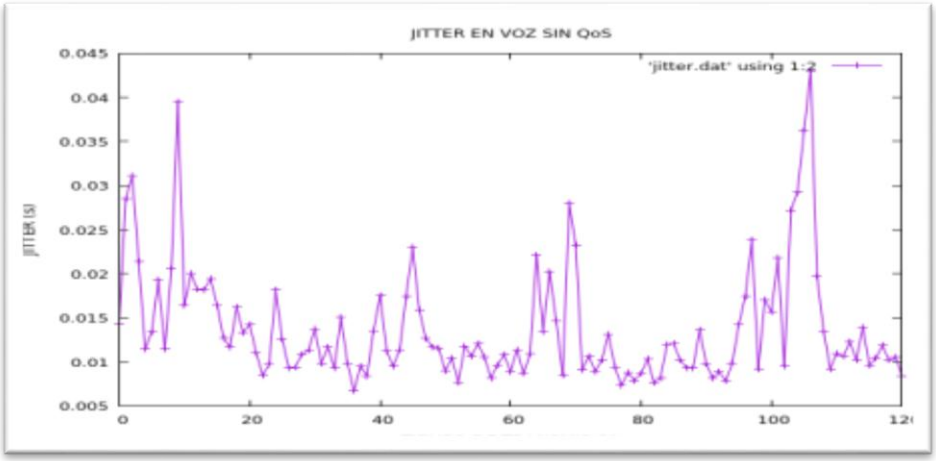

Figura 4-2: Jitter en en la transmisión de Voz sin QoS
Elaborado por: Chacha, Paulina, 2019

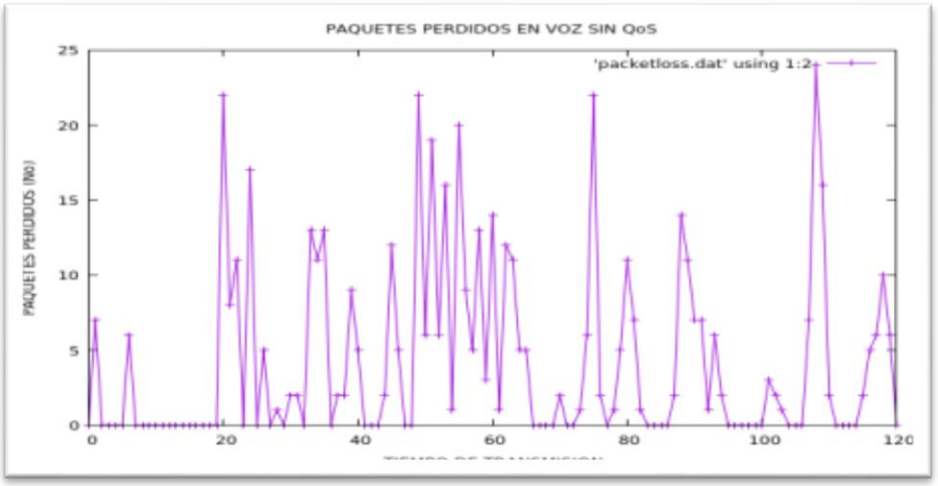

Figura 4-3: Paquetes pérdidos en la transmisión de Voz sin QoS
Elaborado por: Chacha, Paulina, 2019

4.2.2 Tráfico de Streaming sin QoS

Se observa en la Tabla 4-8 el resume de los promedios del Retardo, Jitter y Paquetes Perdidos obtenidos de la simulación de la trasmisión del Streaming sin Calidad de Servicio. El valor del Retardo (Delay) en este escenario es de seiscientos ochenta punto setenta y tres mili segundos (680.73 ms), el valor del Jitter es de nueve punto cuarenta y tres mili segundos (9.43 ms) y el promedio de los paquetes pérdidos es de doce punto diez por ciento (12.10%).

Tabla 4-8: Promedio de los parámetros del Tráfico de Streaming sin QoS

Promedio Retardo (Delay)	Promedio Jitter	Paquetes Pérdidos
680.73 ms	9.43 ms	12.10 %

Elaborado por: Chacha, Paulina, 2019

En la Figura 4-4, Figura 4-5 y Figura 4-6, se oberva los valores obtenidos del retardo, jitter y pérdida de paquetes para el tráfico de Streaming en un escenario sin calidad de servicio respectivamente.

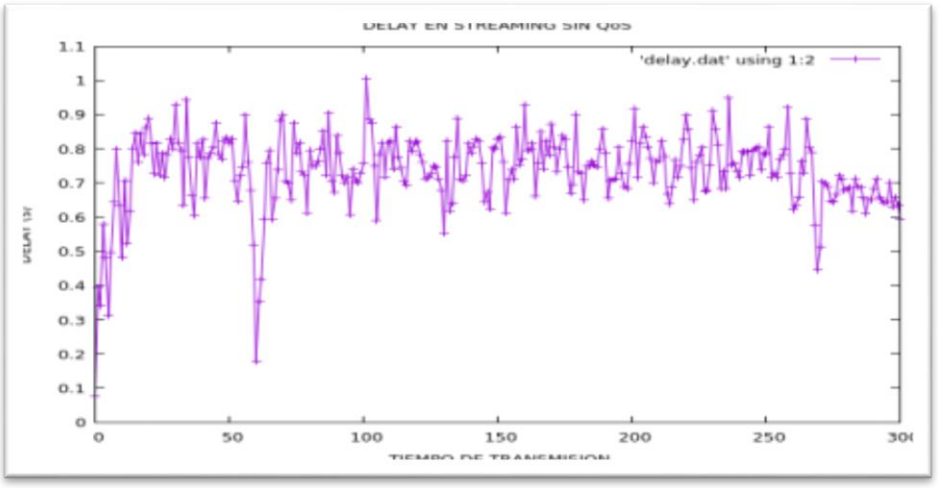

Figura 4-4: Retardo en la transmisión de Streaming sin QoS
Elaborado por: Chacha, Paulina, 2019

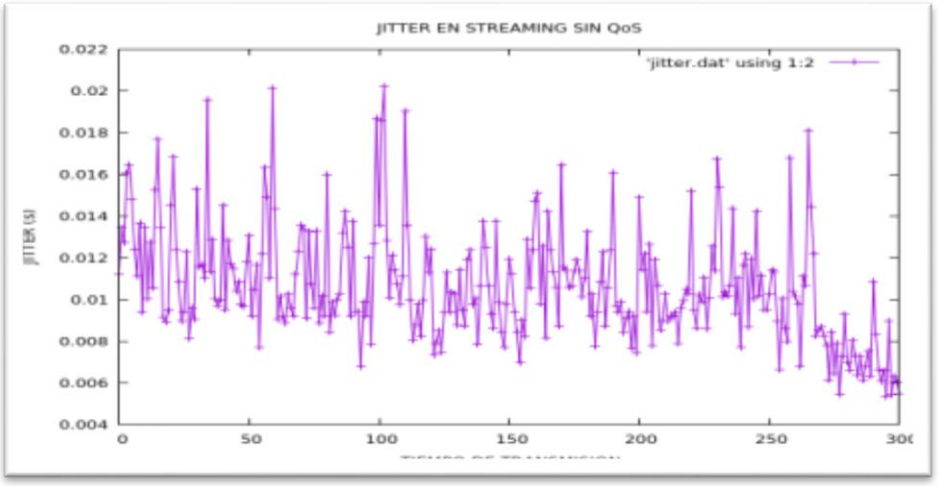

Figura 4-5: Jitter en la transmisión de Streaming sin QoS
Elaborado por: Chacha, Paulina, 2019

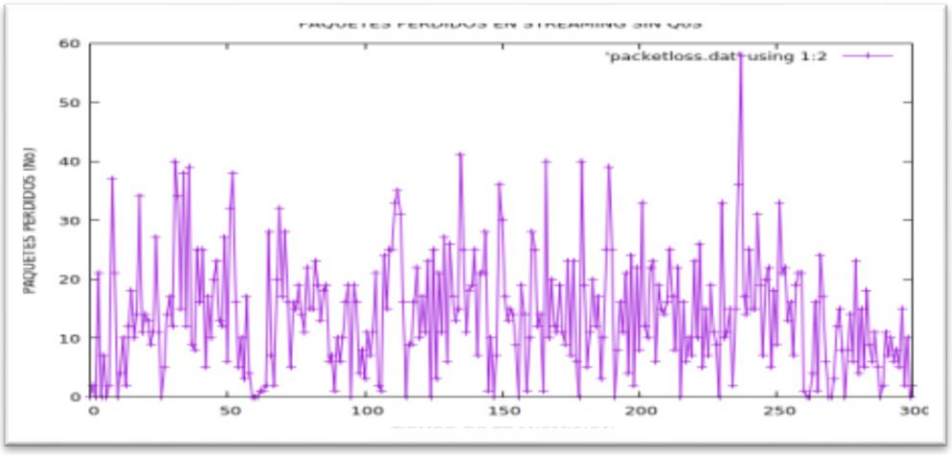

Figura 4-6: Paquetes pérdidos en la transmisión de Streaming sin QoS
Elaborado por: Chacha, Paulina, 2019

4.2.3 Tráfico de Datos sin QoS

En la Tabla 4-9 se visualiza el resume de los promedios del Retardo, Jitter y Paquetes Perdidos obtenidos de la simulación de la trasmisión de Datos sin Calidad de Servicio. El valor del Retardo (Delay) en este escenario es de trescientos ochenta y siete punto catorce mili segundos (387.14 ms), el valor del Jitter es de veinte y cinco punto cero dos mili segundos (25.02 ms) y el promedio de los paquetes pérdidos es de cinco punto noventa y cuatro por ciento (5.94%).

Tabla 4-9: Promedios de los parámetros de Tráfico de Datos sin QoS

Promedio Retardo (Delay)	Promedio Jitter	Paquetes Pérdidos
387.14 ms	25.02 ms	5.94%

Elaborado por: Chacha, Paulina, 2019

Se aprecia en la Figura 4-7, Figura 4-8 y Figura 4-9 los valores obtenidos del retardo, jitter y pérdida de paquetes con el tráfico de datos en un escenario sin calidad de servicio respectivamente.

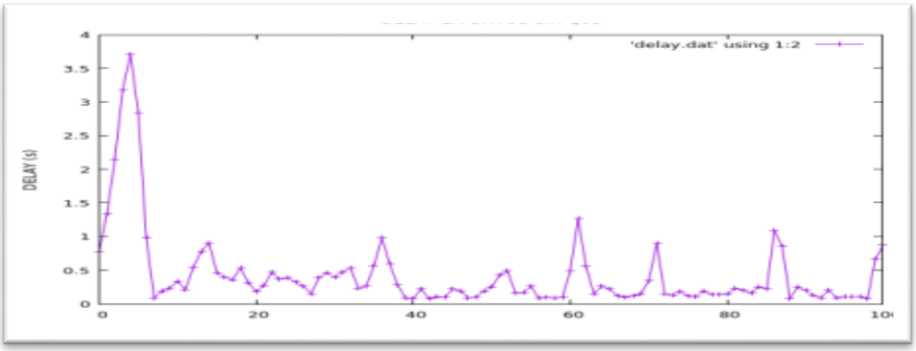

Figura 4-7: Retardo en la transmisión de datos sin QoS
Elaborado por: Chacha, Paulina, 2019

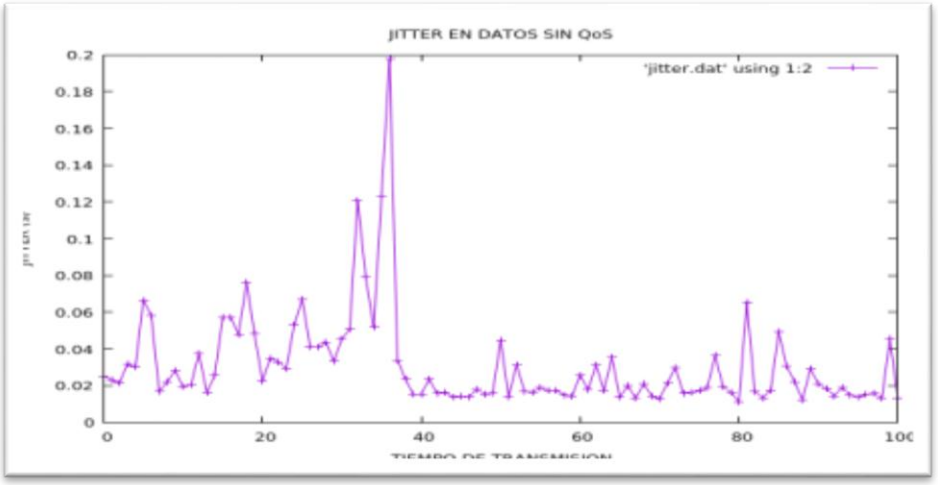

Figura 4-8: Jitter en la transmisión de datos sin QoS
Elaborado por: Chacha, Paulina, 2019

Figura 4-9: Paquetes pérdidos en la transmisión de datos sin QoS
Elaborado por: Chacha, Paulina, 2019

4.3 Análisis de las muestras del escenario con Calidad de Servicio

4.3.1 Tráfico de Voz con QoS

La Tabla 4-10 muestra el resume de los promedios del Retardo, Jitter y Paquetes Pérdidos obtenidos de la simulación de la trasmisión de voz con Calidad de Servicio. El valor del Retardo (Delay) en este escenario es de dos punto sesenta y un mili segundos (2.61 ms), el valor del Jitter es de uno punto noventa mili segundos (1.90 ms) y el promedio de los paquetes pérdidos es del cero por ciento (0.00%).

Tabla 4-10: Promedio de los parámetros del Tráfico de Voz con QoS

Promedio Retardo (Delay)	Promedio Jitter	Paquetes Pérdidos
2.61 ms	1.90 ms	0.00%

Elaborado por: Chacha, Paulina, 2019

En la Figura 4-10, Figura 4-11 y Figura 4-12 se aprecian los valores obtenidos del retardo, jitter y pérdida respectivamente de paquetes con el tráfico de voz en un escenario con calidad de servicio.

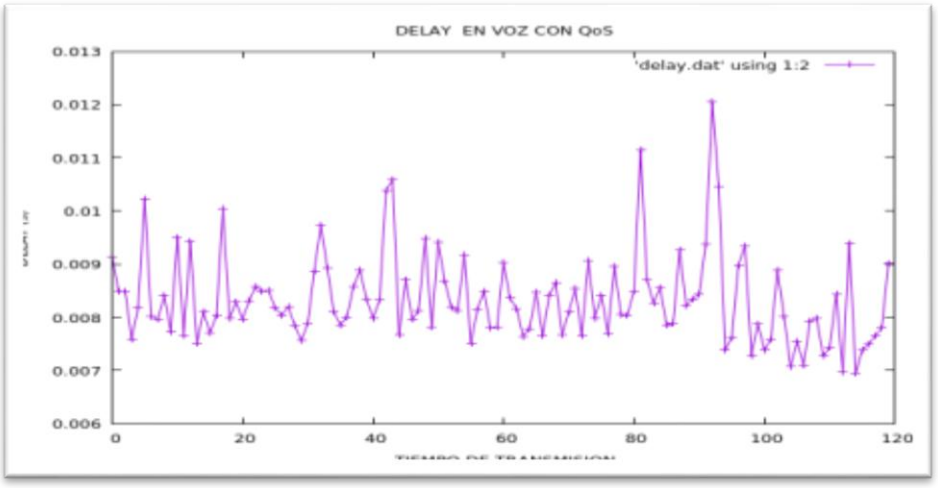

Figura 4-10: Retardo en la transmisión de voz con QoS
Elaborado por: Chacha, Paulina, 2019

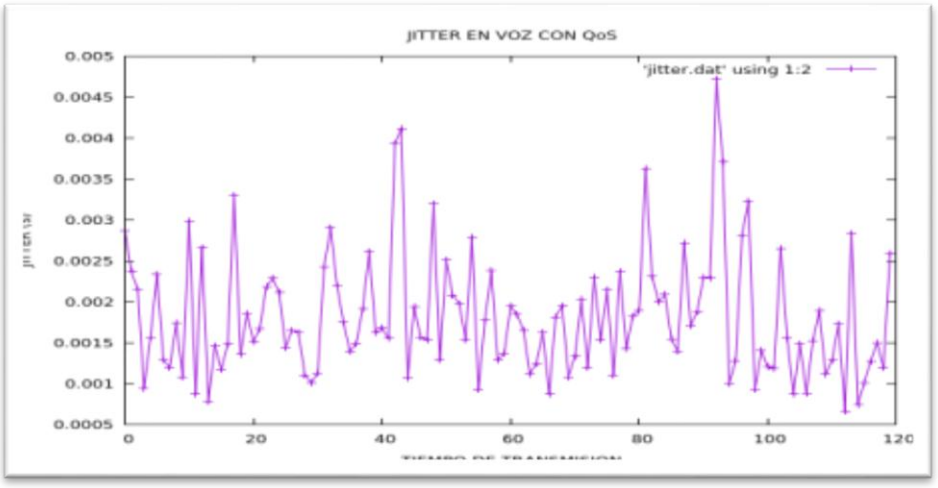

Figura 4-11: Jitter en la transmisión de voz con QoS
Elaborado por: Chacha, Paulina, 2019

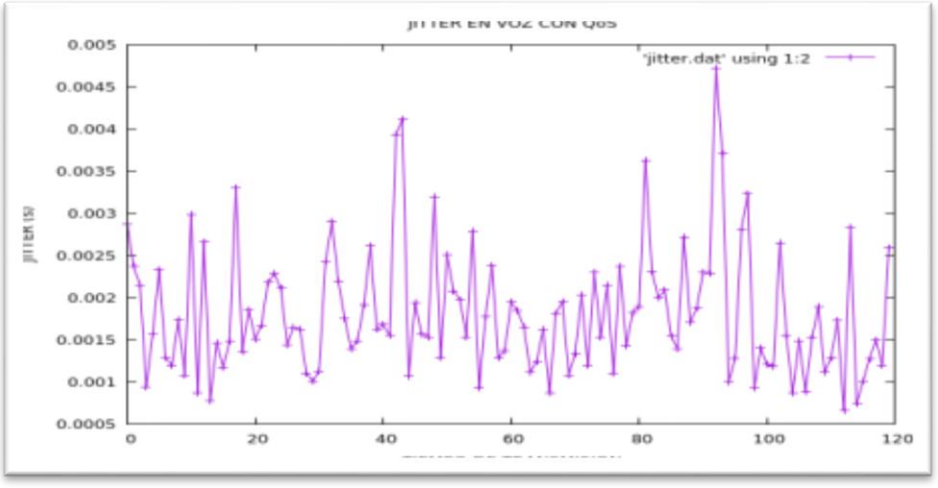

Figura 4-12: Paquetes pérdidos en la transmisión de voz con QoS
Elaborado por: Chacha, Paulina, 2019

4.3.2 Tráfico de Streaming con QoS

En la Tabla 4-11 se resume los promedios del Retardo, Jitter y Paquetes Prdidos obtenidos de la simulación de la trasmisión de streaming con Calidad de Servicio. El valor del Retardo (Delay) en este escenario es de catorce punto ochenta y dos mili segundos (14.82 ms), el valor del Jitter es de tres punto diez y nueve mili segundos (3.19 ms) y el promedio de los paquetes pérdidos es uno punto veinte y siete por ciento (1.27%).

Tabla 4-11: Promedio de los parámetros del Tráfico Streaming con QoS

Promedio Retardo (Delay)	Promedio Jitter	Paquetes Pérdidos
14.82 ms	3.19 ms	1.27 %

Elaborado por: Chacha, Paulina, 2019

En la Figura 4-13, Figura 4-14 y Figura 4-15 se aprecian los valores obtenidos del retardo, jitter y pérdida de paquetes con el tráfico de streaming en un escenario con calidad de servicio respectivamente.

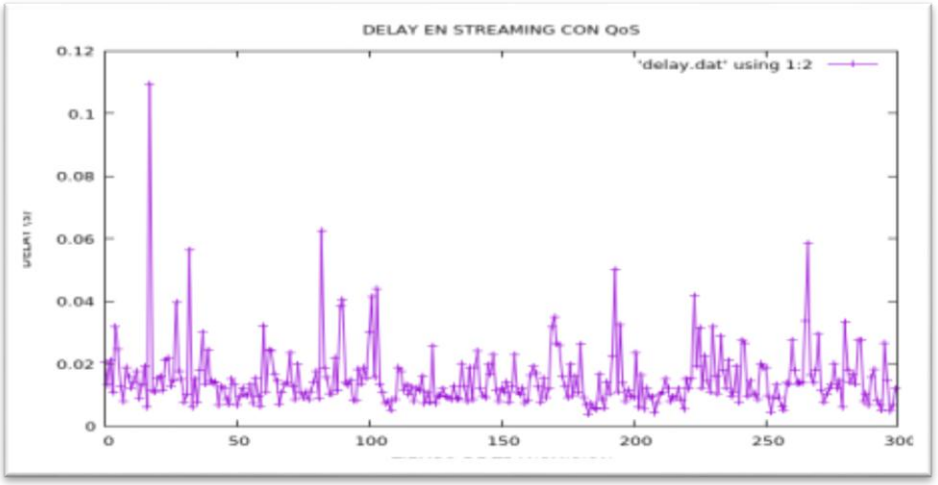

Figura 4-13: Retardo en la transmisión de streaming con QoS

Elaborado por: Chacha, Paulina, 2019

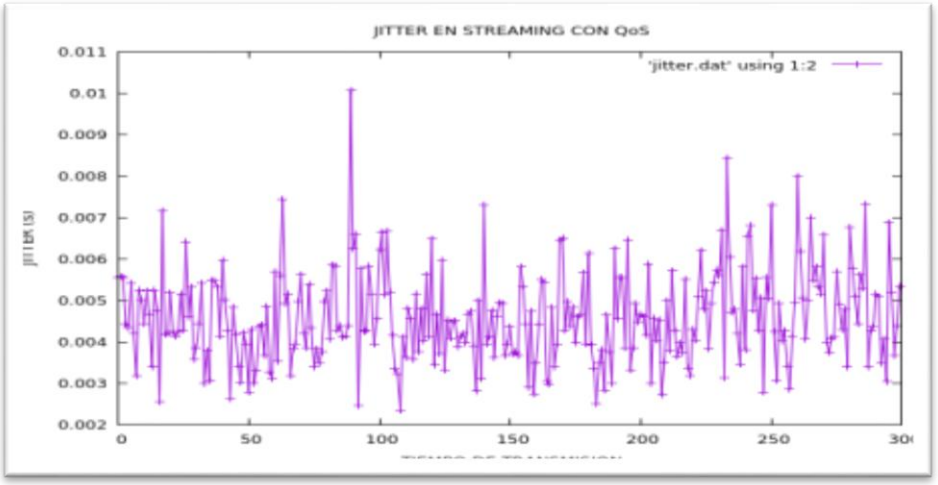

Figura 4-14: Jitter en la transmisión de streaming con QoS
Elaborado por: Chacha, Paulina, 2019

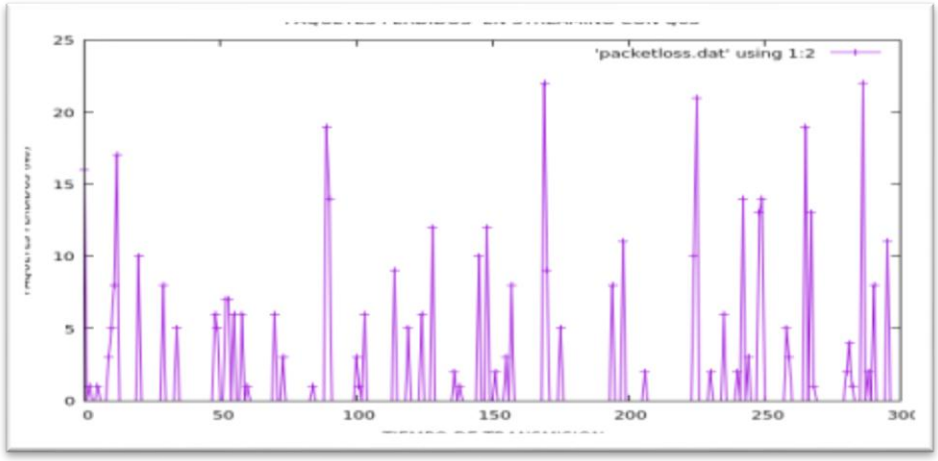

Figura 4-15: Paquetes pérdidos en la transmisión de streaming con QoS
Elaborado por: Chacha, Paulina, 2019

4.3.3 Tráfico de Datos con QoS

Los resultados se resumen en la Tabla 4-12 de los promedios del Retardo, Jitter y Paquetes Pérdidos obtenidos de la simulación de la trasmisión de Datos con Calidad de Servicio. El valor del Retardo (Delay) en este escenario es de veinte y cuatro punto veinte y dos mili segundos (24.22 ms), el valor del Jitter es de seis punto cincuenta y tres mili segundos (6.53 ms) y el promedio de los paquetes pérdidos es del cero por ciento (0.00%).

Tabla 4-12: Promedio de los parámetros de Tráfico de Datos con QoS

Promedio Retardo (Delay)	Promedio Jitter	Paquetes Pérdidos
24.22 ms	6.53 ms	0.00 %

Elaborado por: Chacha, Paulina, 2019

En la Figura 4-16, la Figura 4-17 y la Figura 4-18 se aprecian los valores obtenidos del retardo, jitter y pérdida de paquetes con el tráfico de datos en un escenario con calidad de servicio respectivamente.

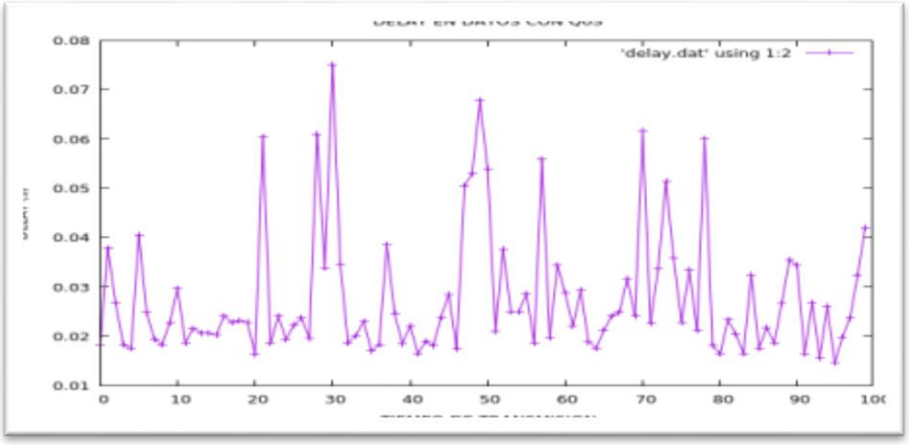

Figura 4-16: Retardo en la transmisión de datos con QoS
Elaborado por: Chacha, Paulina, 2019

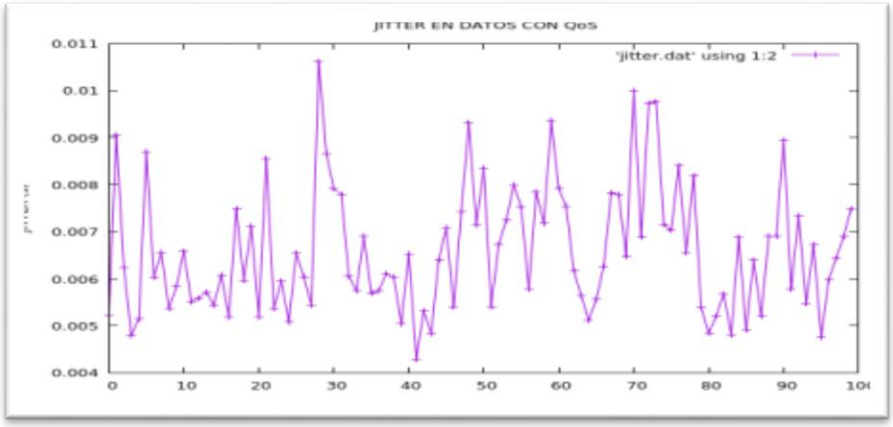

Figura 4-17: Jitter en la transmisión de datos con QoS
Elaborado por: Chacha, Paulina, 2019

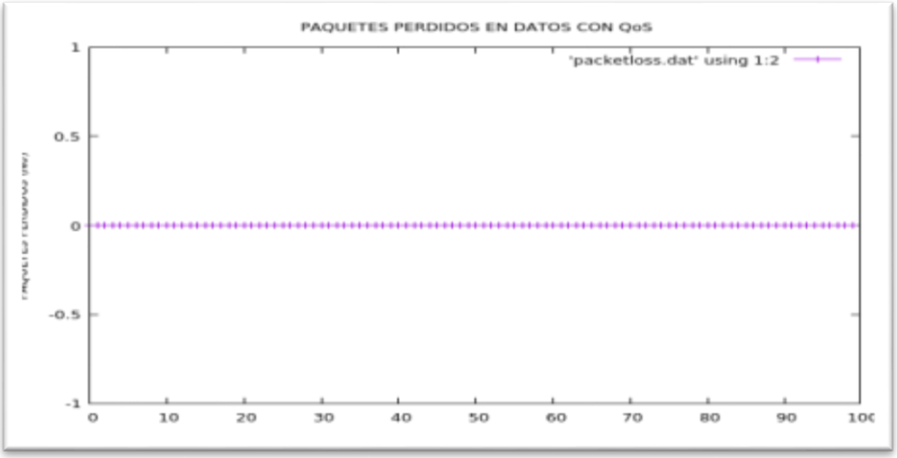

Figura 4-18: Paquetes pérdidos en la transmisión de datos con QoS
Elaborado por: Chacha, Paulina, 2019

4.3.4 Resumen de los resultados obtenidos.

En la Tabla 4-13 se resumen los promedios obtenidos de los parámetros de rendimiento en cada uno de los servicios (tráficos) que se utilizaron en el presente proyecto (anexo A.14 y anexo A.15).

Tabla 4-13: Comparación de los parámetros de calidad de los servicios

		Retardo (ms)	Jitter (ms)	Paquetes Perdidos (%)
VOZ	SIN QoS	812.15	14.98	6.80%
	CON QoS	2.61	1.90	0.00%
STREAMING	SIN QoS	680.73	9.43	12.10 %
	CON QoS	14.82	3.19	1.27 %
DATOS	SIN QoS	387.14	25.02	5.94%
	CON QoS	24.22	6.53	0.00 %

Elaborado por: Chacha, Paulina, 2019

Como se puede observar en la Figura 4-19 los valores del Retardo (Delay) con el servicio de voz, obtenidos en el escenario sin ningún tipo de calidad de servicio son valores mucho más grandes que los resultados obtenidos en el escenario aplicando calidad de servicio.

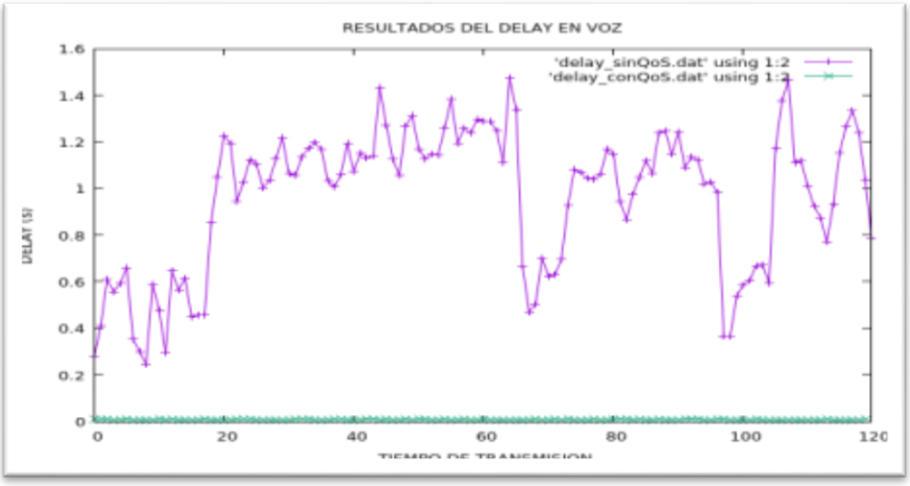

Figura 4-19: Resumen del Delay en el tráfico de voz

Elaborado por: Chacha, Paulina, 2019

La Figura 4-20 muestra los valores del Jitter con el tráfico de voz, obtenidos en el escenario sin ningún tipo de QoS y se aprecia valores mucho más grandes que los resultados obtenidos en el escenario aplicando QoS mediante DiffServ.

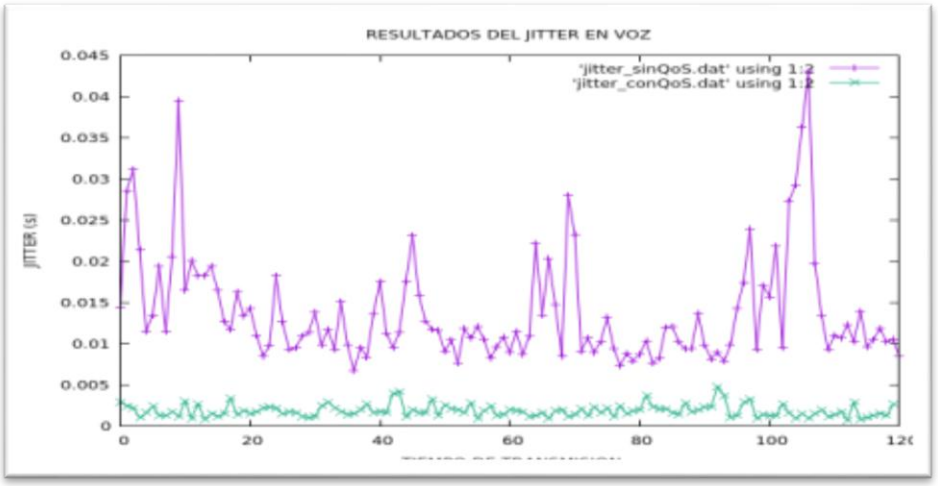

Figura 4-20: Resumen del Jitter en el tráfico de Voz
Elaborado por: Chacha, Paulina, 2019

Mediante la Figura 4-21 se puede apreciar que los valores de los paquetes pérdidos con el tráfico de voz, obtenidos en el escenario sin ningún tipo de QoS son valores mucho más grandes que los resultados obtenidos en el escenario aplicando QoS mediante DiffServ.

Figura 4-21: Resumen de los paquetes pérdidos en el tráfico de voz
Elaborado por: Chacha, Paulina, 2019

Como se puede observar en la Figura 4-22 los valores del Retardo (Delay) con el tráfico de streaming, obtenidos en el escenario sin ningún tipo de QoS son valores mucho más grandes que los resultados obtenidos en el escenario aplicando QoS con DiffServ.

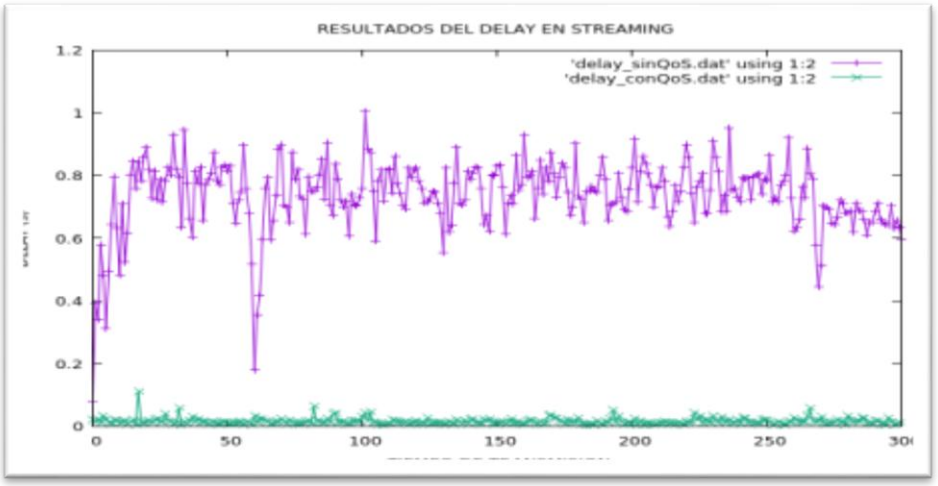

Figura 4-22: Resumen del delay en el tráfico de streaming
Elaborado por: Chacha, Paulina, 2019

La Figura 4-23 muestra los valores del Jitter en la transmisión de streaming, obtenidos en el escenario sin ningún tipo de QoS que son más grandes que los resultados obtenidos en el escenario aplicando QoS con DiffServ.

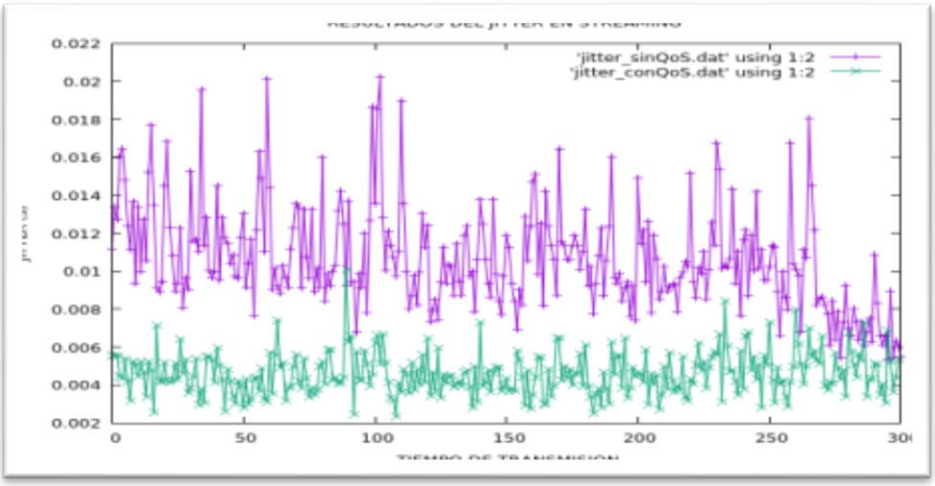

Figura 4-23: Resumen del Jitter en el tráfico de streaming
Elaborado por: Chacha, Paulina, 2019

Se puede apreciar en la Figura 4-24 que los paquetes pérdidos con el tráfico de streaming, obtenidos en el escenario sin ningún tipo de QoS son mucho mayor que los resultados obtenidos en el escenario aplicando QoS con DiffServ.

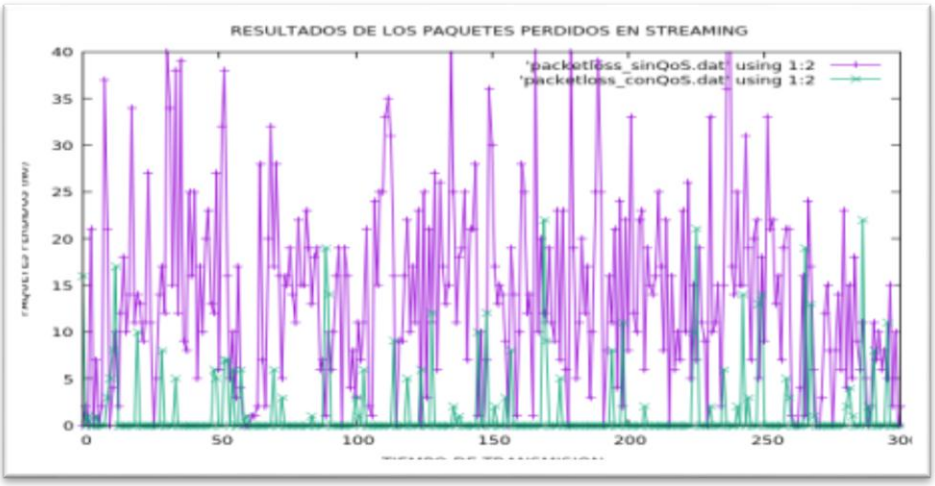

Figura 4-24: Resumen de los Paquetes Pérdidos en el tráfico de streaming
Elaborado por: Chacha, Paulina, 2019

Como se puede observar en la Figura 4-25 los valores del Delay con el tráfico de datos, obtenidos en el escenario sin ningún tipo de QoS es más significativo que los resultados obtenidos en el escenario aplicando QoS con DiffServ.

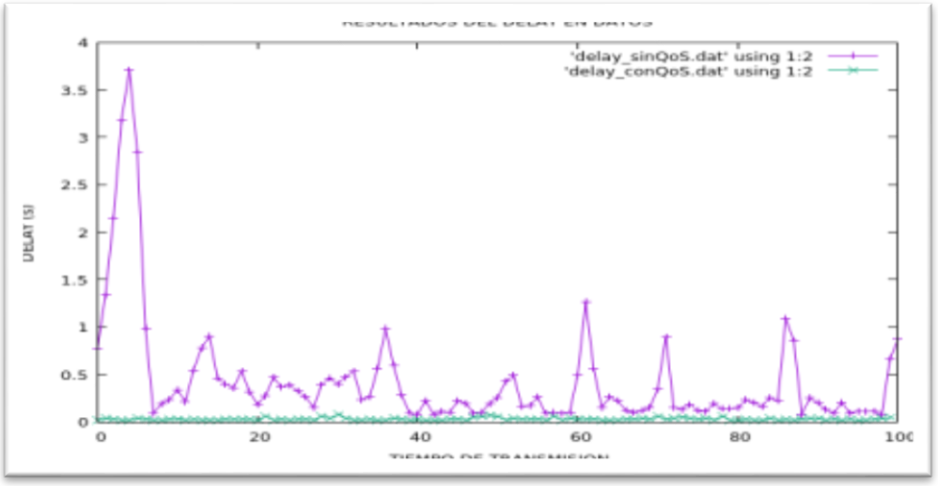

Figura 4-25: Resumen del Delay en el tráfico de Datos
Elaborado por: Chacha, Paulina, 2019

La Figura 4-26 presenta los valores del Jitter en el tráfico de datos, obtenidos en el escenario sin ningún tipo de QoS son más significativos que los resultados obtenidos en el escenario aplicando QoS con DiffServ.

Figura 4-26: Resumen del Jitter en el tráfico de Datos
Elaborado por: Chacha, Paulina, 2019

Mediante la Figura 4-27 se observa que los paquetes pérdidos con el tráfico de datos sin ningún tipo de QoS son mucho mayor que los resultados obtenidos en el escenario aplicando QoS con DifServ.

Figura 4-27: Resumen de los Paquetes Perdidos en el tráfico de Datos
Elaborado por: Chacha, Paulina, 2019

El Grafico 1-4 muestra un resumen global donde se puede apreciar que el retardo aplicando DiffServ al tráfico de voz es cien veces mejor que no aplicar ningún concepto de QoS, de la misma manera con el tráfico de streaming con DiffServ el retardo es cincuenta veces mejor que al no tener ningún tipo de QoS. Para el tráfico de datos ocurre lo mismo, con DiffServ es veinte veces mejor que solamente tener una red MPLS sin ningún tipo de QoS.

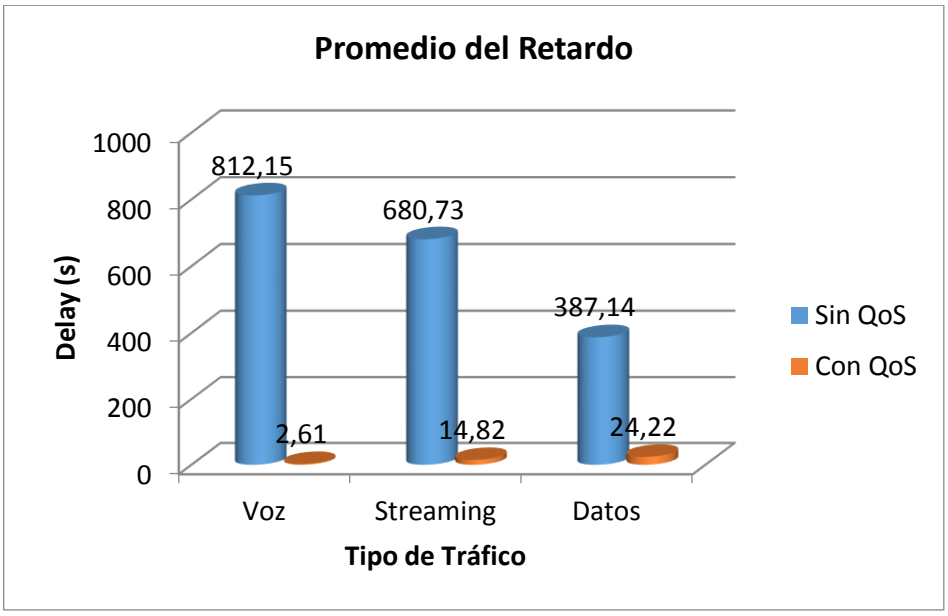

Gráfico 1-4: Promedio del Retardo
Elaborado por: Chacha, Paulina, 2019

Mediante el Grafico 2-4 se resume que los valores del Jitter aplicando DiffServ al tráfico de voz se reduce aproximadamente a una décima parte que al no aplicar ningún concepto de QoS, con el tráfico de streaming con DiffServ el Jitter se reduce aproximadamente a la mitad que cuando no se tiene ningún parámetro de QoS. Para el tráfico de datos aplicando DiffServ, el Jitter se reduce a la cuarta parte que cuando solo se tiene una red MPLS sin ninguna implementación de QoS.

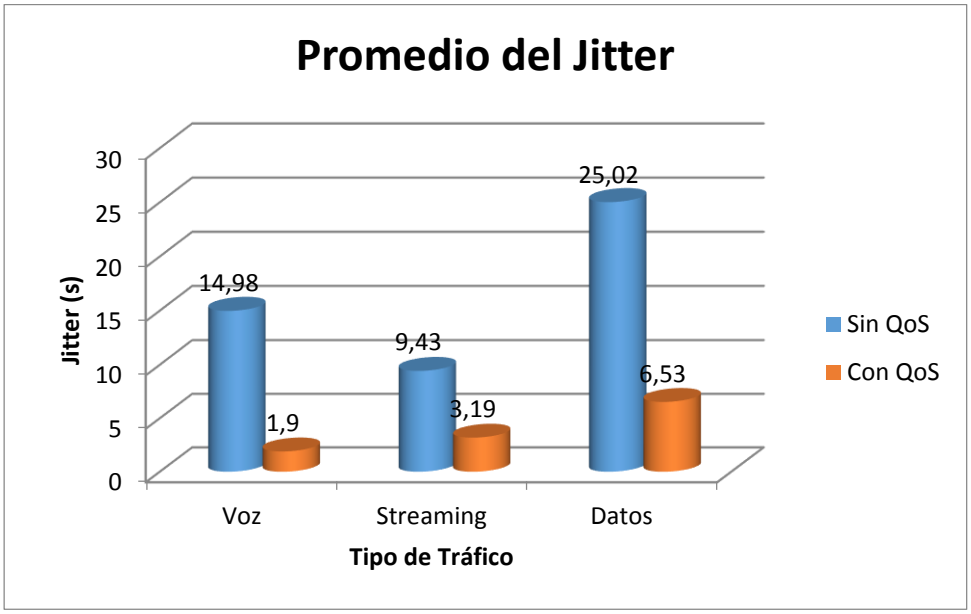

Gráfico 2-4: Promedio del Jitter
Elaborado por: Chacha, Paulina, 2019

Se observa en el Grafico 3-4, que los paquetes pérdidos aplicando QoS mediane DiffServ al tráfico de voz se reduce aproximadamente a un doscientos por ciento que al no aplicar ningún

concepto de QoS. Los paquetes pérdidos con el tráfico de streaming con DiffServ se reduce aproximadamente en un noventa por ciento por ciento que cuando no se aplica QoS. Para el tráfico de datos con QoS mediante DiffServ los paquetes pérdidos se reduce a cero que cuando solo se tiene una red MPLS sin QoS.

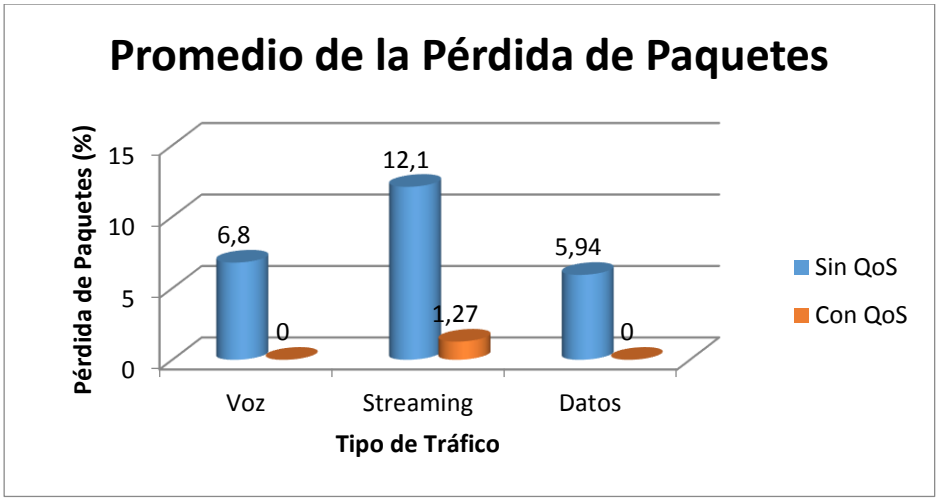

Gráfico 3-4: Promedio de la pérdida de paquetes.
Elaborado por: Chacha, Paulina, 2019

4.4 Comprobación de Hipótesis

Para la comprobación de la Hipótesis planteada en el presente trabajo de investigación se empleó la prueba estadística de T de Student para evaluar cada uno de los parámetros de rendimiento en el escenario planteado. Para utilizar esta prueba estadística se utilizó la herramienta estadística IBM SPSS que posee un paquete estadístico completo que incluye la prueba T de Student y que facilitó la realización de los distintos cálculos que se emplean para la comprobación de la hipótesis.

Se usa T de Student para comparar una muestra en 2 circunstancias diferentes porque interesa comparar la diferencia entre los parámetros de QoS (delay, jitter y pérdida de paquetes) antes de aplicar Servicio Diferenciado y después de aplicarla en una red MPLS.

En primer lugar para poder utilizar la prueba de T de Student se debe tener muestras normalizadas, para corroborar esta condición se utilizó la prueba de normalidad Shapiro-Wilk que está incluido en software SPSS.

4.4.1 Prueba Shapiro Wilk

4.4.1.1 Prueba Shapiro Wilk aplicado a las muestras del Retardo (Delay)

En la Tabla 4-14, se presenta el resultado de la prueba Shapiro Wilk que se aplicó a las muestras del Retardo (Delay) del tráfico de voz, en el cual podemos observar que el valor de significancia "Sig", tanto para las muestras que se extrajeron con QoS aplicando el mecanismo DiffServ, como para las muestras sin ningún mecanismo de QoS se obtuvieron valores de cero punto cuarenta y ocho (0.48) y cero punto treinta (0.30) respectivamente, los mismos que son mayores a cero punto cero cinco (0.05) lo que determinó que las muestras son normalizadas.

Tabla 4-14: Prueba Shapiro Wilk del Delay de las muestras de Voz.

Prueba Shapiro-Wilk del Delay de Voz			
	Estadístico	gl	Sig.
Sin QoS	0.945	20	0.303
Con QoS	0.957	20	0.481

Elaborado por: Chacha, Paulina, 2019

La Tabla 4-15 presenta el resultado de la prueba Shapiro Wilk que se aplicó a las muestras del Retardo (Delay) del tráfico de Streaming, en el cuál podemos observar que el valor de significancia "Sig", tanto para las muestras que se extrajeron con QoS aplicando el mecanismo DiffServ, como para las muestras sin ningún mecanismo de QoS se obtuvieron valores de cero punto diez y seis (0.16) y cero punto cuarenta y siete (0.47) respectivamente, los mismos que son mayores a cero punto cero cinco (0.05) lo que determinó que las muestras son normalizadas.

Tabla 4-15: Prueba Shapiro Wilk del Delay de las muestras del Streaming

Prueba Shapiro-Wilk del Delay de Streaming			
	Estadístico	gl	Sig.
Sin QoS	0.956	20	0.470
Con QoS	0.932	20	0.167

Elaborado por: Chacha, Paulina, 2019

En la Tabla 4-16, se presenta el resultado de la prueba Shapiro Wilk que se aplicó a las muestras del Retardo (Delay) del tráfico de datos, en el cual podemos observar que el valor de significancia "Sig", tanto para las muestras que se extrajeron con QoS aplicando el mecanismo DiffServ, como para las muestras sin ningún mecanismo de QoS, se obtuvieron valores de cero punto cincuenta y seis (0.56) y cero punto cuarenta y siete (0.47) respectivamente, los mismos que son mayores a cero punto cero cinco (0.05) lo que determinó que las muestras son normalizadas.

Tabla 4-16: Prueba Shapiro Wilk del Delay de las muestras de Datos

Prueba Shapiro-Wilk del Delay de Datos			
	Estadístico	gl	Sig.
Sin QoS	0.957	20	0.477
Con QoS	0.961	20	0.569

Elaborado por: Chacha, Paulina, 2019

4.4.1.2 Prueba Shapiro Wilk aplicado a las muestras del Jitter

La Tabla 4-17 presenta el resultado de la prueba Shapiro Wilk que se aplicó a las muestras del Jitter del tráfico de Voz, en el cual podemos observar que el valor de significancia "Sig", tanto para las muestras que se extrajeron con QoS aplicando DiffServ, como para las muestras sin ningún mecanismo de QoS, se obtuvieron valores de cero punto treinta (0.30) y cero punto noventa y nueve (0.99) respectivamente, los mismos que son mayores a cero punto cero cinco (0.05) lo que determinó que las muestras son normalizadas.

Tabla 4-17: Prueba Shapiro Wilk del Jitter de las muestras de Voz

Prueba Shapiro-Wilk del Delay de Voz			
	Estadístico	gl	Sig.
Sin QoS	0.987	20	0.990
Con QoS	0.946	20	0.307

Elaborado por: Chacha, Paulina, 2019

La Tabla 4-18 muestra el resultado de la prueba Shapiro Wilk que se aplicó a las muestras del Jitter del tráfico de Streaming, en el cual podemos observar que el valor de significancia "Sig", tanto para las muestras que se extrajeron con QoS aplicando DiffServ, como para las muestras sin ningún mecanismo de QoS, se obtuvieron valores de cero punto setenta y nueve (0.79) y cero punto doce (0.12) respectivamente, los mismos que son mayores a cero punto cero cinco (0.05) lo que determinó que las muestras son normalizadas.

Tabla 4-18: Prueba Shapiro Wilk del Jitter de las muestras de Streaming

Prueba Shapiro-Wilk del Delay de Streaming			
	Estadístico	gl	Sig.
Sin QoS	0.925	20	0.124
Con QoS	0.972	20	0.797

Elaborado por: Chacha, Paulina, 2019

La Tabla 4-19 presenta el resultado de la prueba Shapiro Wilk que se aplicó a las muestras del Jitter del tráfico de datos, en el cual podemos observar que el valor de significancia "Sig", tanto para las muestras que se extrajeron con QoS aplicando el mecanismo DiffServ, como para las muestras sin ningún mecanismo de QoS, se obtuvieron valores de cero punto quince (0.15) y cero punto cero nueve (0.09) respectivamente, los mismos que son mayores a cero punto cero cinco (0.05) lo que determinó que las muestras son normalizadas

Tabla 4-19: Prueba Shapiro Wilk del Jitter de las muestras de Datos

Prueba Shapiro-Wilk del Delay de Datos			
	Estadístico	gl	Sig.
Sin QoS	0.920	20	0.099
Con QoS	0.930	20	0.156

Elaborado por: Chacha, Paulina, 2019

4.4.1.3 Prueba Shapiro Wilk aplicado a las muestras de los Paquetes Pérdidos

En el caso de los paquetes pérdidos tanto en el tráfico de voz como de datos se obtuvo valores de cero cuando se aplicó DiffServ a la red MPLS lo que significa que no existió ningún paquete pérdido que es lo ideal para la trasmisión de datos y por ser muestras constantes no es necesario aplicar algún tipo de prueba estadística. Para el caso de las muestras del tráfico de Streaming si fue necesario aplicar la prueba estadística, de esta manera se obtuvo que el resultado de la prueba Shapiro Wilk que se aplicó a las muestras del Jitter del tráfico de Datos, en el cual podemos observar que el valor de significancia "Sig", tanto para las muestras que se extrajeron con calidad de servicio aplicando el mecanismo DiffServ, como para las muestras sin ningún mecanismo de QoS, se obtuvieron valores de cero punto cero seis (0.06) y cero punto diez y ocho (0.18) respectivamente, los mismos que son mayores a cero punto cero cinco (0.05) lo que determinó que las muestras son normalizadas, estos datos están resumidos en la Tabla 4-20.

Tabla 4-20: Prueba Shapiro Wilk de los paquetes perdidos de Streaming

Prueba Shapiro-Wilk de los paquetes perdidos de Streaming			
	Estadístico	gl	Sig.
Sin QoS	0.934	20	0.182
Con QoS	0.909	20	0.062

Elaborado por: Chacha, Paulina, 2019

4.4.2 Correlación de muestras

El siguiente paso fue determinar la correlación en las muestras obtenidos con el fin de identificar que tipo de prueba de T de Student se aplicaría. Para esto se utilizó la Correlación de Pearson cuyo valor oscila entre -1 y 1, cuando el resultado es cero indica que las muestras no tienen ningún punto de correlación, mientras que los valores diferentes a cero indican que las muestras tienen una correlación. De la misma manera se utilizó el software SPSS para calcular esta condición.

4.4.2.1 Correlación de Pearson de las muestras del tráfico de Voz.

En la Tabla 4-21 se observa el resultado de la prueba de correlación de Pearson de las muestras del Retardo (Delay) presente en el tráfico de Voz. El resultado obtenido, indica un valor de Correlación de Pearson de cero punto cero setenta y cinco (0.075) entre las muestras obtenidas con QoS aplicado DiffServ y las muestras sin ningun tipo de QoS. Este valor es diferente a cero, con lo cual se determinó que las muestras son correlacionadas.

Tabla 4-21: Correlación de Pearson del Delay en el tráfico de Voz

		Sin QoS	**Con QoS**
Sin QoS	Correlación de Pearson	1	**0.075**
	Sig. (bilateral)		0.753
	N	20	20
Con QoS	Correlación de Pearson	**0.075**	1
	Sig. (bilateral)	0.753	
	N	20	20

Elaborado por: Chacha, Paulina, 2019

Mediante la Tabla 4-22 se presenta el resultado de la prueba de correlación de Pearson de las muestras del Jitter presente en el tráfico de Voz. El resultado obtenido indica un valor de Correlación de Pearson de menos cero punto once (-0.11), entre las muestras obtenidas con QoS aplicado DiffServ y las muestras sin ningún mecanismo de QoS. Este valor es diferente a cero, con lo cual se determinó que las muestras son correlacionadas.

Tabla 4-22: Correlación de Pearson del Jitter en el tráfico de Voz

		Sin QoS	Con QoS
Sin QoS	Correlación de Pearson	1	**-0.118**
	Sig. (bilateral)		0.619
	N	20	20
Con QoS	Correlación de Pearson	**-0.118**	1
	Sig. (bilateral)	0.619	
	N	20	20

Elaborado por: Chacha, Paulina, 2019

En el caso de los paquetes perdidos en el tráfico de voz se obtuvo valores de cero cuando se aplicó DiffServ a la red MPLS, lo que representa que no existió ningún paquete pérdido que es lo ideal para una trasmisión y por ser muestras constantes no es necesario aplicar algún tipo de prueba estadística.

4.4.2.2 Correlación de Pearson de las muestras del tráfico de Streaming.

En la Tabla 4-23 se presenta el resultado de la prueba de correlación de Pearson de las muestras del Retardo (Delay) presente en el tráfico de Streaming. El resultado obtenido, indica un valor de Correlación de Pearson de menos cero punto veinte (-0.20), entre las muestras obtenidas con QoS aplicado Servicio DiffServ y las muestras sin ninguna tipo de QoS. Este valor es diferente a cero, con lo cual se determinó que las muestras son correlacionadas.

Tabla 4-23: Correlación de Pearson del Delay en el tráfico de Streaming

		Sin QoS	Con QoS
Sin QoS	Correlación de Pearson	1	**-0.206**
	Sig. (bilateral)		0.385
	N	20	20
Con QoS	Correlación de Pearson	**-0.206**	1
	Sig. (bilateral)	0.385	
	N	20	20

Elaborado por: Chacha, Paulina, 2019

Medinate la Tabla 4-24 se presenta el resultado de la prueba de correlación de Pearson de las muestras del Jitter presente en el tráfico de Streaming. El resultado obtenido indica un valor de Correlación de Pearson de cero punto cero cinco (0.05), entre las muestras obtenidas con QoS aplicado DiffServ y las muestras sin ninguna tipo de QoS. Este valor es diferente a cero, con lo cual se determinó que las muestras son correlacionadas.

Tabla 4-24: Correlación de Pearson del Jitter en el tráfico de Streaming

		Sin QoS	Con QoS
Sin QoS	Correlación de Pearson	1	**0.058**
	Sig. (bilateral)		0.809
	N	20	20
Con QoS	Correlación de Pearson	**0.058**	1
	Sig. (bilateral)	0.809	
	N	20	20

Elaborado por: Chacha, Paulina, 2019

Se observa en la Tabla 4-25 que el resultado de la prueba de correlación de Pearson de las muestras de los paquetes perdidos presente en el tráfico de Streaming. Se tiene un valor de Correlación de Pearson de menos cero punto trece (-0.13), entre las muestras obtenidas con QoS aplicado DiffServ y las muestras sin ningún mecanismo de QoS. Este valor es diferente a cero, con lo cual se estableció que las muestras son correlacionadas.

Tabla 4-25: Correlación de Pearson de los Paquetes perdidos en el tráfico de Streaming

		Sin QoS	Con QoS
Sin QoS	Correlación de Pearson	1	**-0.131**
	Sig. (bilateral)		0.581
	N	20	20
Con QoS	Correlación de Pearson	**-0.131**	1
	Sig. (bilateral)	0.581	
	N	20	20

Elaborado por: Chacha, Paulina, 2019

4.4.2.3 Correlación de Pearson de las muestras del tráfico de Datos.

Se observa en laTabla 4-26 el resultado de la prueba de correlación de Pearson de las muestras del Retardo (Delay) presente en el tráfico de datos. El resultado obtenido indica un valor de Correlación de Pearson de cero punto uno (0.1), entre las muestras obtenidas con QoS aplicado DiffServ y las muestras sin ningún tipo de QoS. Este valor es diferente a cero, con lo cual se estableció que las muestras son correlacionadas.

Tabla 4-26: Correlación de Pearson del Delay en el tráfico de Datos

		Sin QoS	Con QoS
Sin QoS	Correlación de Pearson	1	**0.100**
	Sig. (bilateral)		0.675
	N	20	20
Con QoS	Correlación de Pearson	**0.100**	1
	Sig. (bilateral)	0.675	
	N	20	20

Elaborado por: Chacha, Paulina, 2019

En la Tabla 4-27 se presenta el resultado de la prueba de correlación de Pearson de las muestras del Jitter presente en el tráfico de Datos. El resultado obtenido indica un valor de Correlación de Pearson de menos cero punto cero cinco (-0.05), entre las muestras obtenidas con QoS aplicado DiffServ y las muestras sin ningún mecanismo de QoS. Este valor es diferente a cero, con lo cual se determinó que las muestras son correlacionadas.

Tabla 4-27: Correlación de Pearson del Jitter en el tráfico de Datos

		Sin QoS	Con QoS
Sin QoS	Correlación de Pearson	1	**-0.052**
	Sig. (bilateral)		0.827
	N	20	20
Con QoS	Correlación de Pearson	**-0.052**	1
	Sig. (bilateral)	0.827	
	N	20	20

Elaborado por: Chacha, Paulina, 2019

Los paquetes pérdidos que se obtuvieron con el tráfico de datos aplicado DiffServ a la red MPLS son de cero por lo que representa que no existió ningún paquete pérdido que es lo ideal para la trasmisión de datos y por ser muestras constantes no es necesario aplicar algún tipo de prueba estadística.

4.4.3 Prueba T de Student para Muestras Relacionadas

Una vez que se determinó que los datos tienen una distribución normalizada y además tienen correlación se procedió aplicar la prueba estadística T de Student para muestras correlacionadas. Para la aplicación de esta prueba se establecieron dos hipótesis específicas, una nula y una alternativa para cada parámetro de rendimiento.

El grado de error o nivel de confiabilidad que se escogió para realizar la prueba se lo determinó en 5% (0.05) el mismo que es un estándar para las investigaciones científicas.

4.4.3.1 Prueba T de Student para las muestras del Retardo (Delay)

Las hipótesis específicas para este parámetro son:

- Hipótesis Nula (Ho): No hay diferencia significativa en el parámetro de Delay en una arquitectura MPLS con Servicio Diferenciado y una red MPLS sin Servicio Diferenciado.
- Hipótesis alternativa (Ha): Si hay diferencia en el parámetro de Delay en una arquitectura MPLS con Servicio Diferenciado y una red MPLS sin Servicio Diferenciado.

En la Tabla 4-28 se presenta el resultado obtenido de la prueba T de Student aplicado a las muestras del Retardo (Delay) que se obtuvieron en el escenario de pruebas. De dicha tabla el valor más relevante es "Sig Bilateral" que en este caso es cero para todos los tipos de tráfico (Voz-Streaming-Datos), este valor es menor que el nivel de confiabilidad (0.05) por lo cual los valores del Retardo obtenidos con QoS aplicado DiffServ y los valores sin ningún tipo de QoS son diferentes completamente, por lo cual se acepta la hipótesis alternativa que indica que si hay diferencia en el parámetro de Delay en una arquitectura MPLS con Servicio Diferenciado y una red MPLS sin Servicio Diferenciado.

Tabla 4-28: Prueba T de Student del Delay

	Diferencias emparejadas					**T**	**Gl**	**Sig Bilateral**
	Media	**Desviación Estándar**	**Media de error estándar**	**95 % de Intervalo de confianza de la diferencia**				
				Inferior	**Superior**			
VOZ Con QoS – Sin QoS	-809.53	109.25	24.43	-860.66	-758.39	-33.13	19	**0.0**
STREAMING Con QoS – Sin QoS	-665.91	97.367	21.77	-711.48	-620.34	-30.58	19	**0.0**
DATOS Con QoS – Sin QoS	-362.91	10.686	2.38	-367.91	-357.91	-151.80	19	**0.0**

Elaborado por: Chacha, Paulina, 2019

4.4.3.2 Prueba T de Student para las muestras del Jitter

Las hipótesis específicas para este parámetro son:

- Hipótesis Nula (Ho): No hay diferencia significativa en el parámetro de Jitter en una arquitectura MPLS con Servicio Diferenciado y una red MPLS sin Servicio Diferenciado.
- Hipótesis alternativa (Ha): Si hay diferencia en el parámetro de Jitter en una arquitectura MPLS con Servicio Diferenciado y una red MPLS sin Servicio Diferenciado.

La Tabla 4-29 muetra el resultado obtenido de la prueba T de Student aplicado a las muestras del Jitter que se obtuvieron en el escenario de pruebas. De dicha tabla el valor más relevante es "Sig Bilateral", que en este caso es cero para todos los tipos de tráfico (Voz-Streamins-Datos), este valor es menor que el nivel de confiabilidad (0.05) por lo cual los valores obtenidos del Jitter con QoS aplicado DiffServ y sin ninguna tipo de QoS son diferentes completamente. Por lo cual se acepta la hipótesis alternativa que indica que si hay diferencia significativa en el parámetro de Jitter en una arquitectura MPLS con Servicio Diferenciado y una red MPLS sin Servicio Diferenciado.

Tabla 4-29: Prueba T de Student del Jitter

	Diferencias emparejadas					**T**	**Gl**	**Sig Bilateral**
	Media	**Desviación Estándar**	**Media de error estándar**	**95 % de Intervalo de confianza de la diferencia**				
				Inferior	**Superior**			
VOZ Con QoS – Sin QoS	-13.079	2.227	0.498	-14.121	-12.036	-26.26	19	**0.00**
STREAMINS Con QoS – Sin QoS	-6.239	1.034	0.231	-6.723	-5.754	-26.97	19	**0.00**
DATOS Con QoS – Sin QoS	-18.496	2.400	0.536	-19.61	-17.372	-34.45	19	**0.00**

Elaborado por: Chacha, Paulina, 2019

4.4.3.3 Prueba T de Student para las muestras de los Paquetes Perdidos

Las hipótesis específicas para este parámetro son:

- Hipótesis Nula (Ho): No hay diferencia significativa en el parámetro de pérdida de paquetes en una arquitectura MPLS con Servicio Diferenciado y una red MPLS sin Servicio Diferenciado.
- Hipótesis alternativa (Ha): Si hay diferencia en el parámetro de pérdida de paquetes en una arquitectura MPLS con Servicio Diferenciado y una red MPLS sin Servicio Diferenciado.

En la Tabla 4-30 se presenta el resultado obtenido de la prueba T de Student aplicado a las muestras de los paquetes perdidos que se obtuvieron del escenario con el tráfico de Streaming, de dicha tabla el valor más relevante es "Sig Bilateral", que en este caso es cero, este valor es menor que el nivel de confiabilidad (0.05) lo que significa que los valores obtenidos de pérdida de paquetes con QoS aplicado DiffServ y sin ningún mecanismo de QoS son diferentes.

Tabla 4-30: Prueba T de Student de los Paquetes Perdidos

	Diferencias emparejadas					**T**	**Gl**	**Sig Bilateral**
	Media	**Desviación Estándar**	**Media de error estándar**	**95 % de Intervalo de confianza de la diferencia**				
				Inferior	**Superior**			
STREAMING Con QoS – Sin QoS	-10.831	1.191	0.266	-11.38	-10.27	-40.6	19	**0.00**

Elaborado por: Chacha, Paulina, 2019

Como se determinó anteriormente las muestras que se obtuvieron con el tráfico de voz y de datos son constantes y cuyo valor de cero es el mejor resultado que se puedo obtener, se puede aceptar directamente la hipótesis alternativa, por ende se puede decir si hay diferencia significativa en el parámetro de pérdida de paquetes en una arquitectura MPLS con Servicio Diferenciado y una red MPLS sin Servicio Diferenciado.

Una vez que se aplicó la prueba estadística T de Student se corroboró que los resultados que se obtuvieron aplicando Calidad de Servicio con un mecanismo de DiffServ son distintos y mejores que los resultados obtenidos sin ningún tipo de Calidad de Servicio.

En base a la Tabla 4-2 de Valoración Cuantitativas de Latencia, se pudo afirmar que el promedio de Retardo (Delay) obtenido en un escenario con QoS es "EXCELENTE", de la misma manera en la Tabla 4-4 de Valoración Cuantitativas del Jitter, se pudo afirmar que el promedio de Retardo (Delay) obtenido en un escenario con QoS mediante Diffserv es "EXCELENTE" y finalmente, en base en la Tabla 4-6 de Valoración Cuantitativas de los paquetes perdidos, se concluye que el promedio de porcentaje de paquetes pérdidos obtenidos en un escenario con QoS mediante DiffServ es "EXCELENTE".

Por lo antes mencionado se puede afirmar que al aplicar QoS mediante DiffServ en una red con MPLS se garantizan mejores resultados en los parámetros de retardo, jitter y pérdida de paquetes con lo cual se cumplió con la hipótesis de investigación.

CONCLUSIONES

- Las redes MPLS con el mecanismo DiffServ ofrece garantías de calidad de servicio para los diferentes tipos de tráfico como son VoIP, Streaming y Datos esta afirmación se comprobó mediante las mediciones de los valores de los parámetros de rendimiento como: jitter, retardo y pérdida de paquetes que se encuentran dentro de los umbrales adecuados según los estándares de la UIT-T G.1010, UIT Y.1541 y la IEEE 8021.1.

- El indicador de retardo sin el mecanismo de DiffServ y con el mecanismo DiffServ se obtuvo un promedio respectivamente de 970.18 ms y 8.32 ms para el tráfico de Voz, 731.017ms y 15.28 ms para el tráfico de Streaming, 401.34ms y 28.01 ms para el tráfico de Datos, como se puede observar sin aplicar el mecanismo de DiffServ no son valores adecuados mientras que aplicando el mecanismo de DiffServ los valores trabajan en el rango recomendado por los estándares antes mencionados.

- El indicador de Jitter para las redes MPLS sin el mecanismo de DiffServ y aplicando el mecanismo de DiffServ se obtiene respectivamente 13.035ms y 1.797ms para VoIP, 10.506ms y 4.568ms para Streaming, 23.950ms y 6.03ms para Datos, se observa que los valores disminuyen con el mecanismo de DiffServ porque se maneja prioridades de tráfico. El tráfico de voz tiene valores menores de retardo y jitter que el tráfico de streaming y datos porque se le garantizó más reservas de ancho de banda que el resto de tráfico por medio de los mecanismos de gestión de colas.

- La comprobación de la hipótesis se realizó con la prueba de T de Student, aplicando a las muestras de retardo, jitter y pérdida de paquetes, mediante el cual se ha aceptado la hipótesis alternativa que indica que si hay diferencia en el parámetro de retardo, jitter y pérdida de paquetes en una arquitectura MPLS con servicio Diferenciado y una red MPLS sin servicio Diferenciado.

RECOMENDACIONES

- Se recomienda usar una red MPLS por la velocidad de conmutación de paquetes ya que no requiere ingresar a analizar la cabecera de cada router como lo hace una red IP.

- En aplicaciones que se desea transmitir en tiempo real con buenas prestaciones de QoS se debe aplicar Servicio Diferenciado para dar prioridad a este tráfico frente a otros menos susceptibles al retardo.

- Dado el consumo de recursos requeridos por el emulador GNS3 y D-ITG en una plataforma robusta de equipos Ciscos se recomienda mínimo 6GB de memoria RAM y un procesador de 4GHz

- El administrador de red debe realizar un análisis del tráfico para aplicar las políticas de entrada y salida a las interfaces de acuerdo a sus necesidades de prioridad.

BIBLIOGRAFÍA

Buñay, P. (2013). *Aplicación de la arquitectura DIFFSERV sobre redes MPLS para la provisión de QoS punto a punto en la transmisión de tráfico en tiempo real* (Tesis de Postgrado). Escuela Superior Politécnica de Chimborazo. Riobamba.

Bustamante, A. (2007). *Contribución en el análisis y simulación de una red MPLS con la internet de servicios diferenciados DIFFSERV* (Tesis de Postgrado). Universidad Nacional Mayor de San Marcos, Lima.

Camacho, T. (2015). *Estudio de la Ingeniería de Tráfico en Redes MPLS mediante Casos de uso Práctico con la herramienta VNX* (Tesis de Postgrado). Universidad Politécnica de Madrid, Madrid-España.

Castellanos, M., y Guzmán, J. (2013). *Implementación de Calidad de Servicio sobre una red MPLS en la región metropolitana de Guatemala* (Tesis de Pregrado). Universidad Galileo, Guatemala.

Cisco (sf). *MPLS Quality of Service (QoS*). USA: Cisco IOS Release 12.0 (22)S

Cisco System, (2004). (vols 1-2). *Implementing Cisco Quality of Service*. (s.l): (s.n)

Cisco. (2012). *MPLS DiffServ Tunneling Modes. Cisco IOS Release 15M&T*.

Delgado, H. (2015). *Construcción de una red MPLS y validación de GNS3 para su simulación* (Tesis de Pregrado). Universidad Politécnica de Cartagena, Cartagena-Colombia.

ETSI TR 101 329-6, V1.1, (2000). *End to End Quality of Service in TIPHON (Telecommunications and Internet Protocol Harmonisation over Networks) Systems, Definition of Quality of Service (QoS) Classes*. Francia:etsi.fr

Ghein, L. (2007). *MPLS Fundamentals.* USA: Karen A. Gill

Harry, P. (2005). *The Multi-Protocol Label Switching (MPLS) Architecture. En Connection-Oriented Networks* (pp 131-179). *Inglaterra:* John Wiley & Sons Ldt.

Hesselbach, X., Huerta, M. y Calderón, O. (2014). Problemas abiertos en MPLS. Migración, Protección, Gestión de Recursos y Balanceo de Carga. Barcelona. Recuperado de https://www.researchgate.net/publication/261635186.

Lopez, D, Gelvez, N. (2009). Ingeniería de tráfico en redes de conmutación de etiquetas Traffic Engineering Label Switched Networks. *Visión Electrónica. 85-89.* Doi: 10.23919/OCEANS.2009.5422081.

Lopez, D., Pedraza., L., y Hernandez, C. (2011). *MPLS y ATM como tecnologías backbone para la transferencia de videoconferencia.* Tecnura. 53-71.

Nieto, L. B. (2010). *Diseño y configuración de Calidad de Servicio en la tecnología MPLS para un proveedor de servicios de Internet* (Tesis de Pregrado). Universidad Politécnica Nacional, Quito.

Orozco, F. (2017). *Diseño de una Red Privada Virtual con tecnología MPLS para la carrera de Ingeniería de Networking de la Universidad de Guayaquil* (Tesis de Pregrado) Guayaquil.

Ortega, R. (2007). *Mecanismos de protección en escenarios IP-MPLS multidominio* (Tesis de postgrado). Universidad Carlos III de Madrid, Madrid-España.

Recomendación UIT-T G.1010. (2001). *Categorías de calidad de servicio para los usuarios de extremo de servicios multimedios*. (pp 11-16). Ginebra: UIT.

Recomendación UIT-T Y.1541. (2006). *Objetivos de calidad de funcionamiento de red para servicios basados en el protocolo Internet.* (pp 16-18). Ginebra: UIT

Telefonía Voz IP. (2012). *Codecs en la Telefonía IP, Codecs VoIP*. Recuperado de http://www.telefoniavozip.com/voip/codecs-voip.htm

Zapata, M. A. (2016). *Evaluación de parámetros de Calidad de Servicio (QoS) para el diseño de una red VPN con MPLS* (Tesis de Postgrado). Pontificia Universidad Católica del Ecuador, Quito.

Zapata, M., Pacheco, F., De la Torre, A., y Vallejo, M. (2017). *QoS Parameters Evaluation in a VPN-MPLS Diffserv Network under a Complete Free Software Emulation Environment.* Directory of Open Access Journals. 74-82. doi: https://doi.org/10.26423/rctu.v4i3.285.

ANEXOS

Anexo A Configuración de equipos en la red MPLS

Anexo A.1 Configuración de direcciones IP en las interfaces de red IP/MPLS

PE1#configure terminal
PE1(config)# interface Ethernet0/0
PE1(config-if)#ip address192.168.7.1 255.255.255.252
PE1(config-if)# clock rate 6400
PE1(config-if)# no shutdown

Anexo A.2 Configuración de protocolo IGP

El comando necesario para implementar un protocolo de enrutamiento interno (IGP) conocido como OSPF con el proceso 10 y área 0 esto se configura en todos los router de la nube MPLS.

PE1(config)#router ospf 10 area 0

Anexo A.3 Configuración básica de MPLS

PE1(config)#ip cef
PE1(config)# mpls ldp router-id loopback 0
PE1(config)# interface Ethernet 0/1
PE1(config-if)# mpls ip
PE1(config-if)# mpls label protocol ldp

Anexo A.4 Configuración de mapas de clases para el router PE en la red MPLS

PE1(config)#class-map IP-EF
PE1(config-cmap)#match ip dscp ef
PE1(config-cmap)#exit
PE1(config)#class-map IP-AF11
PE1(config-cmap)#match ip dscp af11
PE1(config-cmap)#exit
PE1(config)#class-map IP-AF13
PE1(config-cmap)#match ip dscp af13
PE1(config-cmap)#exit
PE1(config)#class-map IP-AF21
PE1(config-cmap)#match ip dscp af21
PE1(config-cmap)#exit
PE1(config)#class-map IP-AF23
PE1(config-cmap)#match ip dscp af23
PE1(config-cmap)#exit
PE1(config)#class-map IP-AF31
PE1(config-cmap)#match ip dscp af31
PE1(config-cmap)#exit
PE1(config)#class-map IP-AF33
PE1(config-cmap)#match ip dscp af33
PE1(config-cmap)#exit

Anexo A.5 Políticas de comportamiento en la nube MPLS

Se crea la política de nombre DSCP-EXP, sobre el comportamiento de los paquetes dentro de la nube MPLS.

```
PE1(config)#policy-map DSCP-EXP
PE1(config-pmap)#class IP-EF
PE1(config-cmap)#set mpls experimental imposition 7
PE1(config-cmap)#exit
PE1(config)#class IP-AF11
PE1(config-cmap)#set mpls experimental imposition 6
PE1(config-cmap)# exit
PE1(config)#class IP-AF13
PE1(config-cmap)#set mpls experimental imposition 5
PE1(config-cmap)#exit
PE1(config)#class IP-AF21
PE1(config-cmap)#set mpls experimental imposition 4
PE1(config-cmap)#exit
PE1(config)#class IP-AF23
PE1(config-cmap)#set mpls experimental imposition 3
PE1(config-cmap)#exit
PE1(config)#class IP-AF31
PE1(config-cmap)#set mpls experimental imposition 2
PE1(config-cmap)#exit
```

Anexo A.6 Configuración de política a una interfaz

Para aplicar una política a un interfaz se utiliza el siguiente comando:

```
PE1#conf t
PE1(config)#interface Ethernet 0/1
PE1(config-if)#service-policy input DSCP-EXP
PE1(config-if)#exit
```

Anexo A.7 Creación de los mapas de clases

```
PE1(config)#class-map MPLS-premium
PE1(config-cmap)#match mpls experimental topmost 7
PE1(config-cmap)#exit
PE1(config)#class-map match-any MPLS-oro
PE1(config-cmap)#match mpls experimental topmost 6 5
PE1(config-cmap)#exit
PE1(config)#class-map match-any MPLS-plata
PE1(config-cmap)#match mpls experimental topmost 4 3
PE1(config-cmap)#exit
PE1(config)#class-map match-any MPLS-bronce
PE1(config-cmap)#match mpls experimental topmost 2 1
PE1(config-cmap)#exit
```

Anexo A.8 Configuración de gestión de cola CBWFQ

Router(config-pmap-c)# Bandwith bandwidth

Permite asignar cantidades de ancho de banda a una clase, coloca los valores en kbps

Router(config-pmap-c)# bandwidth percent percent

Permite asignar un porcentaje de ancho de banda a la clase

Router(config-pmap-c)# Bandwidth remaining percent percent

Asigna un porcentaje disponible de ancho de banda a la clase.

Se aplicará las políticas de comportamiento de QoS en las interfaces de salida de los router de borde. Se realizará un control de políticas aplicando el método de gestión de colas LLQ + CBWFQ y el método de descarte de paquete de baja prioridad WRED

```
PE1(config)#policy-map politica_MPLS-PHBs
PE1(config-cmap)#class MPLS-premium
PE1(config-cmap)#priority percent 29
PE1(config-cmap)#exit
PE1(config)#class MPLS-oro
PE1(config-cmap)#bandwidth percent 21
PE1(config-cmap)#random-detect
PE1(config-cmap)#exit
PE1(config)#class MPLS-plata
PE1(config-cmap)#bandwidth percent 15
PE1(config-cmap)#random-detect
PE1(config-cmap)#exit
PE1(config)#class MPLS-bronce
PE1(config-cmap)#bandwidth percent 10
PE1(config-cmap)#random-detect
PE1(config-cmap)#exit
```

El comando de configuración de clase del mapa de política de ancho de banda se usa para especificar o modificar el ancho de banda asignado para una clase que pertenece a un mapa de políticas. Todas las clases que pertenecen a un mapa de políticas deben usar el mismo tipo de ancho de banda por ejemplo en kbps, porcentaje del ancho de banda de la interfaz o porcentaje de ancho de banda disponible.

Anexo A.9 Configuración de Low-Latency Queuing

Router(config-pmap-c)# priority bandwidth [burst]

Permite fijar ancho de banda en kbps a una clase y asegurar un envio EF (expedited forwarding) o envio acelerado. Si el tráfico excede el ancho de banda especificado es eliminado si existe congestión.

Router(config-pmap-c)# priority percent percentage [burst]

Permite configurar un porcentaje de ancho de banda de una clase y asegurar el envio EF (expedited forwarding). Si el tráfico excede el ancho de banda especificado es eliminado si existe congestión

Anexo A.10 Aplicar políticas de QoS a la salida del router PE

```
PE1(config)#interface Ethernet 0/0
PE1(config.if)#service-policy output politica_MPLS-PHBs
PE1(config-if)#exit
PE1(config)#interface Ethernet 0/2
PE1(config-if)#service-policy output politica_MPLS-PHBs
```

Anexo A.11 Configuración de QoS para la salida de la red MPLS hacia la red IP

```
PE1(config)#class-map IP-premium
PE1(config-cmap)#match dscp ef
PE1(config-cmap)#exit
PE1(config)#class-map match-any IP-oro
PE1(config-cmap)#match dscp af11 af13
PE1(config-cmap)#exit
PE1(config)#class-map match-any IP-plata
PE1(config-cmap)#match dscp af21 af23
PE1(config-cmap)#exit
PE1(config)#class-map match-any IP-bronce
PE1(config-cmap)#match dscp af31 af33
PE1(config-cmap)#exit
```

Anexo A.12 Configuración de políticas a la salida de la red MPLS

Aplicar las políticas a la salida de la red MPLS hacia la red del Customer, se aplica a las interfaces de salida las policías de PHB que se aplicará de acuerdo a las Clases de Servicio.

```
PE1(config)#interface Ethernet 0/0
PE1(config-if)#service-policy output politica_MPLS-PHBs
PE1(config-if)#exit
PE1(config)#interface Ethernet 0/2
PE1(config-if)#service-policy output politica_MPLS-PHBs
```

Anexo A.13 Instalación y configuración del generador de tráfico D-ITG

D-ITG, esta soportado sobre los siguientes Sistemas Operativos Linux (Ubuntu, Debian, Fedora, CentOS, OpenWRT, Snapgear, Montavista, uClinux) Windows (XP, Vista, 7), OSX (Leopard) FreeBSD.

Se ha escogido el sistema Lubuntu versión 18.1.1.1 por ser muy liviano y su requerimiento mínimo de RAM es de 256 MB. Los pasos para su instalación de detallan a continuación:

- Descargar el paquete," D-ITG-2.8.1-r2058M-src.zip" en algún lugar de su sistema de archivos.
- Abrir un terminal para instalar complementos como g++ que es el programa compilador:
- $ sudo apt-get install g++
- Mediante línea de comando descomprimir el archivo e ingresamos al directorio "D-ITG-2.8.1-r2058M/src":
- $ sudo unzip D-ITG-2.8.1-r2058M-src.zip
- $ cd D-ITG-2.8.1-r2058M-src/src
- Una vez el directorio SRC tipiar make para construir el binario.
- $ make

Para mayor facilidad se ha instalado el modo GUI (interfaz gráfica de Usuario) que se puede observar en la Figura 1-A y se lo activa del siguiente modo:

- Descargar el D-ITG en modo grafico **D-ITG GUI 0.92 (253 kB)** de la página http://www.semken.com/projekte/index.html.
- Ingresamos a la carpeta que contiene el programa D-ITG GUI 0.92.
- En un terminal ejecutar $java –jar ITGGUI.jar y se despliega la siguiente ventana

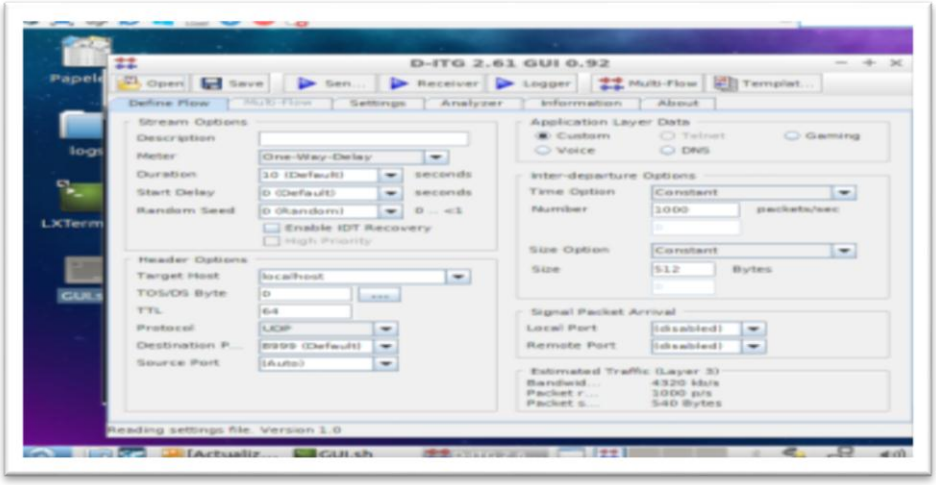

Figura 1-A: Interfaz gráfica del inyector de tráfico D-ITG
Elaborado por: Chacha, Paulina, 2019

Configuración de parámetros del inyector de tráfico

Se debe configurar tanto en el host transmisor como en el host receptor para sincronizar la transmisión y obtener los archivos de jitter, pérdida de paquetes y delay. En las Figuras 2-A y 3-A se ha resaltado los parámetros más importantes que se deben configurar en el transmisor: como la dirección IP de destino, el tiempo de duración, la aplicación, y la ubicación de los directorios para almacenar los archivos .log

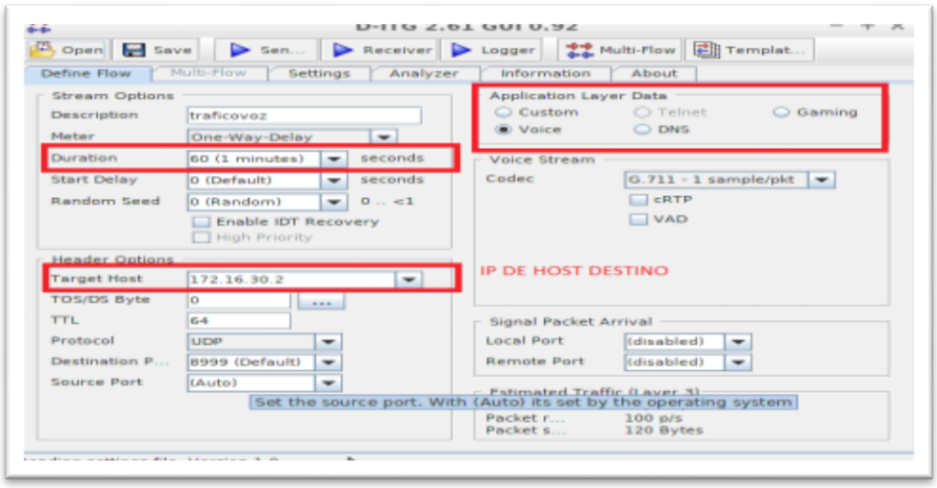

Figura 2-A: Parámetros de configuración en el transmisor
Elaborado por: Chacha, Paulina, 2019

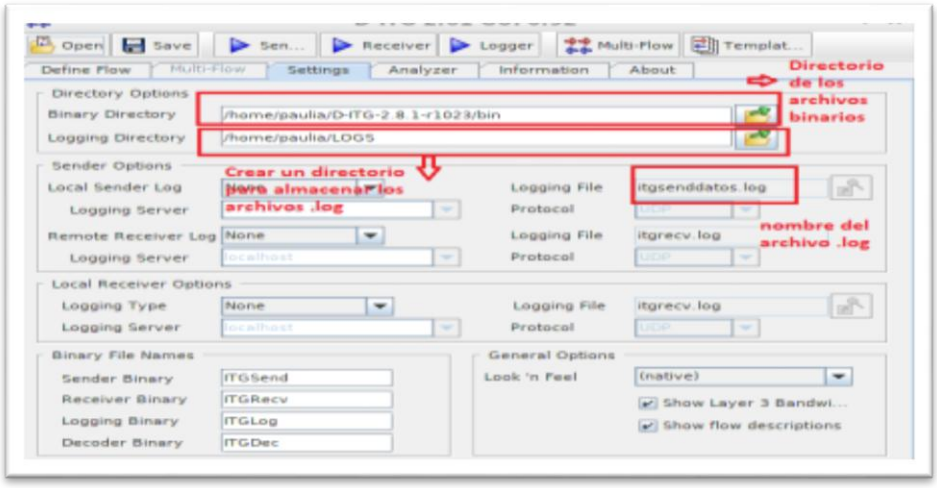

Figura 3-A: Parámetros de configuración en el transmisor
Elaborado por: Chacha, Paulina, 2019

En la figura 4-A, se encuentras todos los parámetros de configuración del receptor del inyector de tráfico

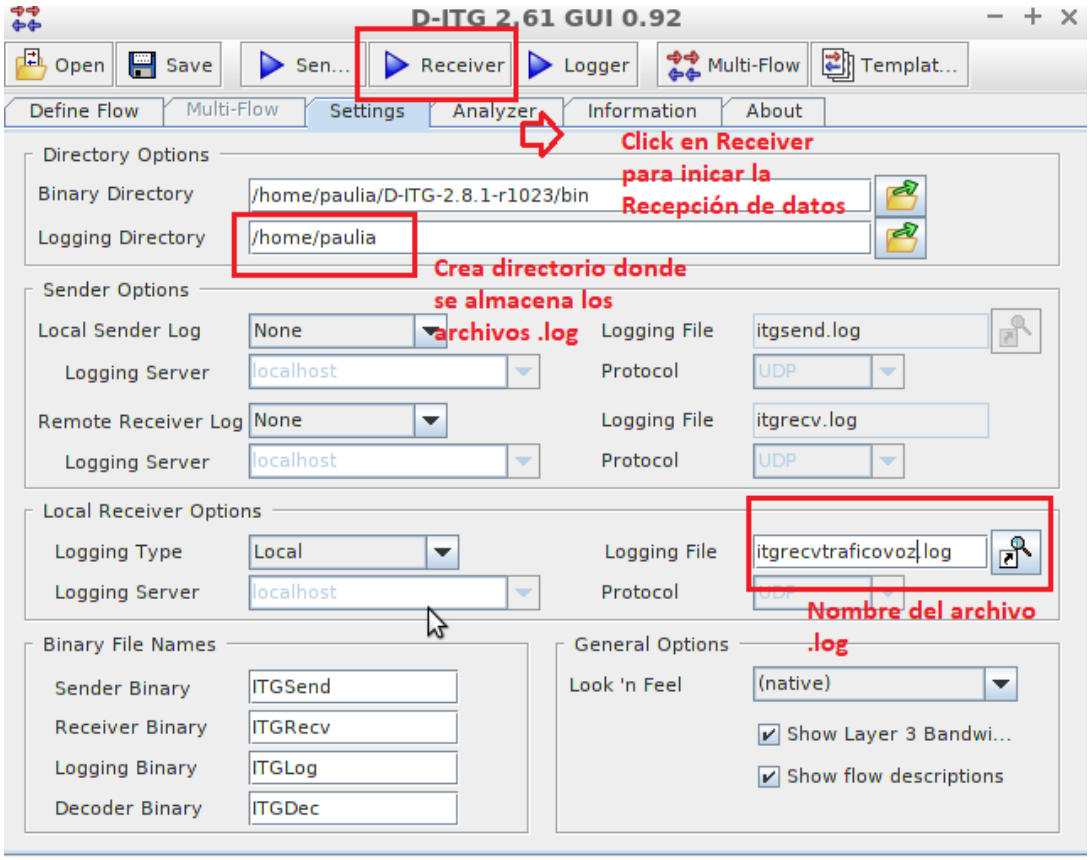

Figura 4-A: Parámetros de configuración en el Receptor
Elaborado por: Chacha, Paulina, 2019

.

Anexo A.14 Cuadro de Resultados sin Mecanismo de Servicio Diferenciado

Resultados de Delay, jitter y pérdida de paquetes para tráfico de voz, streaming y datos sin mecanismo de Servicio Diferenciado.

VOZ				STREAMING				DATOS			
N° Muestra	**Delay (ms)**	**Jitter (ms)**	**Paquetes Perdidos (%)**	**N° Muestra**	**Delay (ms)**	**Jitter (ms)**	**Paquetes Perdidos (%)**	**N° Muestra**	**Delay (ms)**	**Jitter (ms)**	**Paquetes Perdidos (%)**
1	852,26	10,25	8,56	1	625,4	9,23	12,69	1	380,3	20,56	4,56
2	965,25	18,36	7,56	2	598,8	8,26	12,48	2	395,7	24,89	5,23
3	754,23	12,36	8,59	3	589,5	9,45	12,34	3	385,5	23,56	5,69
4	957,58	15,98	7,56	4	769,5	10,6	13,65	4	392,6	24,58	5,23
5	632,25	13,56	8,45	5	705,2	10,2	12,85	5	398,6	24,69	7,45
6	796,56	14,85	6,59	6	769,5	9,56	13,59	6	402,6	24,32	8,26
7	865,21	19,56	5,59	7	658,5	9,28	13,57	7	386,5	26,56	4,52
8	698,45	13,56	7,69	8	698,3	9,65	13,59	8	398,6	24,51	4,58
9	769,25	14,56	8,56	9	539,8	10,5	13,52	9	375,3	24,69	5,59
10	658,36	12,35	7,98	10	694,4	9,57	12,58	10	366	25,89	6,89
11	912,35	12,56	6,58	11	619,9	9,23	12,59	11	398,2	25,69	6,45
12	869,36	17,25	6,45	12	539,9	10,6	11,58	12	378,3	24,57	4,69
13	768,69	14,36	9,12	13	617,3	8,56	12,59	13	389,6	24,53	5,69
14	825,45	18,25	8,26	14	759,2	9,57	15,69	14	388,3	26,58	8,56
15	698,45	16,25	5,89	15	856,5	9,61	11,67	15	395,4	28,36	6,25
16	926,15	13,25	6,57	16	698,6	9,54	12,58	16	376	25,64	4,69
17	896,45	15,36	4,65	17	847	8,56	12,54	17	386,5	26,24	4,25
18	625,89	16,39	3,25	18	798,7	7,95	12,53	18	394,4	28,26	6,58
19	958,36	14,89	5,69	19	659,9	9,45	13,56	19	375,6	24,86	5,12
20	812,36	15,78	2,56	20	569,2	9,48	13,58	20	379,6	29,58	8,56
PROMEDIO	812,146	14,99	6,8075	PROMEDIO	680,7	9,44	12,9885	PROMEDIO	387,1	25,43	5,942

Fuente: Simulación con GNS3, para diferentes tipos de tráfico sin QoS

Anexo A.15 Cuadro de Resultados con Mecanismo de Servicio Diferenciado

Resultados de Delay, jitter y pérdida de paquetes para tráfico de voz, streaming y datos con mecanismo de Servicio Diferenciado.

VOZ

N° Muestra	Delay (ms)	Jitter (ms)	Paquetes Perdidos (%)
1	4.745	1,28	0
2	4.157	1,86	0
3	9.607	3,09	0
4	2.691	1,51	0
5	3.488	1,64	0
6	1.194	2,27	0
7	2.439	2,74	0
8	1.046	1,88	0
9	1,72	1,43	0
10	1.412	4,69	0
11	3,88	2,99	0
12	5,95	2,14	0
13	2,65	1,77	0
14	2,86	2,05	0
15	1,73	1,54	0
16	1,33	1,32	0
17	1,84	1,74	0
18	2,86	2,34	0
19	2,38	2,04	0
20	2,27	1,83	0
PROMEDIO	1.540	2,108	0

STREAMING

N° Muestra	Delay (ms)	Jitter (ms)	Paquetes Perdidos (%)
1	14,03	2,94	0
2	10,56	3,44	0
3	20,41	3,8	16
4	15,15	3,35	2,65
5	16,23	4,55	2,24
6	16,74	3,94	0
7	15,01	3,7	0,42
8	20,34	3,2	0
9	23,35	3,72	0,23
10	9,34	2,96	0
11	32,62	4,39	0
12	6,74	2,9	0,18
13	8,34	3,32	0
14	4,58	2,2	0,23
15	10,27	3,2	0,37
16	14,24	2,25	0
17	12,41	1,68	0
18	16,65	4,05	3,02
19	15,05	2,06	0
20	14,34	2,34	3,34
PROMEDIO	14,82	3,2	1,434

DATOS

N° Muestra	Delay (ms)	Jitter (ms)	Paquetes Perdidos (%)
1	35,16	7,06	0
2	23,24	8,48	0
3	26,21	7,38	0
4	28,36	7,91	0
5	41,57	6,44	0
6	25,34	5,45	0
7	22,56	6,56	0
8	21,67	3,45	0
9	27,56	7,45	0
10	24,26	3,56	0
11	24,67	4,67	0
12	19,45	6,57	0
13	28,47	8,54	0
14	18,25	6,223	0
15	21,78	8,45	0
16	26,56	3,24	0
17	28,45	8,56	0
18	23,8	4,56	0
19	21,87	8,65	0
20	25,34	7,43	0
PROMEDIO	25,73	6,532	0

Fuente: Simulación con GNS3, para diferentes tipos de tráfico sin QoS

Anexo B *Configuraciones de los Routers*

PE1 (Provider Edge Entrada CE1)

==========

```
enable
configure terminal
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
ip ospf 10 area 0
exit
interface Ethernet0/0
ip address 192.168.7.1 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/1
ip address 172.10.10.2 255.255.255.252
no shutdown
exit
interface Ethernet0/2
```

```
ip address 192.168.7.29 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
ip route 172.16.10.0 255.255.255.0 172.10.10.1
ip route 172.16.100.0 255.255.255.0 172.10.10.1
router ospf 10
redistribute static subnets
exit
mpls label protocol ldp
mpls ldp router-id Lo0
interface Ethernet0/0
mpls ip
interface Ethernet0/2
mpls ip
class-map IP-EF
match ip dscp ef
exit
class-map IP-AF11
match ip dscp af11
exit
class-map IP-AF13
match ip dscp af13
exit
class-map IP-AF21
match ip dscp af21
exit
class-map IP-AF23
match ip dscp af23
exit
class-map IP-AF31
match ip dscp af31
exit
class-map IP-AF33
match ip dscp af33
exit

policy-map DSCP-EXP
class IP-EF
set mpls experimental imposition 7
exit
class IP-AF11
set mpls experimental imposition 6
exit
class IP-AF13
set mpls experimental imposition 5
exit
class IP-AF21
set mpls experimental imposition 4
exit
```

```
class IP-AF23
set mpls experimental imposition 3
exit
class IP-AF31
set mpls experimental imposition 2
exit
class IP-AF33
set mpls experimental imposition 1
exit
class class-default
set mpls experimental imposition 0
exit
exit
interface Ethernet 0/1
service-policy input DSCP-EXP
exit
class-map MPLS-premium
match mpls experimental topmost 7
exit
class-map match-any MPLS-oro
match mpls experimental topmost 6 5
exit
class-map match-any MPLS-plata
match mpls experimental topmost 4 3
exit
class-map match-any MPLS-bronce
match mpls experimental topmost 2 1
exit
policy-map politica_MPLS-PHBs
class MPLS-premium
priority percent 29
exit
class MPLS-oro
bandwidth percent 21
random-detect
exit
class MPLS-plata
bandwidth percent 15
random-detect
exit
class MPLS-bronce
bandwidth percent 10
random-detect
exit
exit
interface Ethernet 0/0
service-policy output politica_MPLS-PHBs
exit
interface Ethernet 0/2
service-policy output politica_MPLS-PHBs
```

```
exit

PE2     (Provider Edge Entrada CE2)
====================================
enable
configure terminal
interface LoopBack0
ip address 4.4.4.4 255.255.255.255
ip ospf 10 area 0
exit

interface Ethernet0/0
ip address 172.10.20.2 255.255.255.252
no shutdown
exit
interface Ethernet0/1
ip address 192.168.7.41 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet1/0
ip address 192.168.7.26 255.255.255.252
no shutdown
ip ospf 10 area 0
exit

ip route 172.16.20.0 255.255.255.0 172.10.20.1

router ospf 10
redistribute static subnets
exit
mpls label protocol ldp
mpls ldp router-id Lo0
interface Ethernet0/1
mpls ip
interface Ethernet1/0
mpls ip

PE3     (Provider Edge Salida CE3)
====================================
enable
configure terminal
interface LoopBack0
ip address 3.3.3.3 255.255.255.255
ip ospf 10 area 0
exit
interface Ethernet0/0
ip address 172.10.30.2 255.255.255.252
no shutdown
exit
```

```
interface Ethernet0/2
ip address 192.168.7.6 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/3
ip address 192.168.7.33 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
ip route 172.16.30.0 255.255.255.0 172.10.30.1
router ospf 10
redistribute static subnets
exit
mpls label protocol ldp
mpls ldp router-id Lo0
interface Ethernet0/2
mpls ip
interface Ethernet0/3
mpls ip
class-map match-any MPLS-bronce
 match mpls experimental topmost 1  2
class-map match-any MPLS-plata
 match mpls experimental topmost 3  4
class-map match-all MPLS-premium
 match mpls experimental topmost 7
class-map match-any MPLS-oro
 match mpls experimental topmost 5  6
policy-map politica-entrada
class IP-premium
set dscp ef
exit
class IP-oro
set precedence 5
exit
class IP-plata
set precedence 3
exit
class IP-bronce
set precedence
exit
exit
interface Ethernet 0/2
service-policy output politica_entrada
exit
class-map IP-premium1
match dscp ef
exit
class-map match-any IP-oro1
match dscp af11 af13
```

```
exit
class-map match-any IP-plata1
match dscp af21 af23
exit
class-map match-any IP-bronce1
match dscp af31 af33
exit
policy-map politica_salida
class IP-premium1
priority percent 29
exit
class IP-oro1
bandwidth percent 21
random-detect dscp-based
exit
class IP-plata1
bandwidth percent 15
random-detect dscp-based
exit
class IP-bronce1
bandwidth percent 10
random-detect dscp-based
exit
exit
interface Ethernet 0/0
service-policy output politica_salida
exit
```

PE4 (Provider Edge Salida CE4)

==========

```
enable
configure terminal
interface LoopBack0
ip address 7.7.7.7 255.255.255.255
ip ospf 10 area 0
exit
interface Ethernet0/1
ip address 172.10.40.2 255.255.255.252
no shutdown
exit
interface Ethernet0/2
ip address 192.168.7.38 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet1/1
ip address 192.168.7.10 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
ip route 172.16.40.0 255.255.255.0 172.10.40.1
```

```
router ospf 10
redistribute static subnets
exit
mpls label protocol ldp
mpls ldp router-id Lo0
interface Ethernet0/1
mpls ip
interface Ethernet1/1
mpls ip
```

P1

```
=====================================
enable
configure terminal
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
ip ospf 10 area 0
exit
interface Ethernet0/0
ip address 192.168.7.2 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/1
ip address 192.168.7.13 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/2
ip address 192.168.7.5 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/3
ip address 192.168.7.21 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet1/0
ip address 192.168.7.25 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet1/1
ip address 192.168.7.9 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
mpls label protocol ldp
mpls ldp router-id Lo0
```

```
interface Ethernet0/0
mpls ip
interface Ethernet0/1
mpls ip
interface Ethernet0/2
mpls ip
interface Ethernet0/3
mpls ip
interface Ethernet1/0
mpls ip
interface Ethernet1/1
mpls ip
```

P2

```
========================================
enable
configure terminal
interface LoopBack0
ip address 5.5.5.5 255.255.255.255
ip ospf 10 area 0
exit

interface Ethernet0/0
ip address 192.168.7.17 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/1
ip address 192.168.7.42 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/2
ip address 192.168.7.30 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/3
ip address 192.168.7.22 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
mpls label protocol ldp
mpls ldp router-id Lo0
interface Ethernet0/0
mpls ip
interface Ethernet0/1
mpls ip
interface Ethernet0/2
mpls ip
```

```
interface Ethernet0/3
mpls ip
```

P3

==========

```
enable
configure terminal
interface LoopBack0
ip address 6.6.6.6 255.255.255.255
ip ospf 10 area 0
exit

interface Ethernet0/0
ip address 192.168.7.18 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/1
ip address 192.168.7.14 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/2
ip address 192.168.7.37 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
interface Ethernet0/3
ip address 192.168.7.34 255.255.255.252
no shutdown
ip ospf 10 area 0
exit
mpls label protocol ldp
mpls ldp router-id Lo0
interface Ethernet0/0
mpls ip
interface Ethernet0/1
mpls ip
interface Ethernet0/2
mpls ip
interface Ethernet0/3
mpls ip
```

CE1

==========

```
enable
configure terminal
interface Ethernet0/0
ip address 172.16.10.1 255.255.255.0
no shutdown
```

```
exit
interface Ethernet0/1
ip address 172.10.10.1 255.255.255.252
no shutdown
exit
interface Ethernet0/2
ip address 172.16.100.1 255.255.255.0
no shutdown
exit
ip route 0.0.0.0 0.0.0.0 172.10.10.2
class-map IP-premium1
match dscp ef
exit
class-map match-any IP-oro1
match dscp af11 af13
exit
class-map match-any IP-plata1
match dscp af21 af23
exit
class-map match-any IP-bronce1
match dscp af31 af33
exit
policy-map politica_salida
class IP-premium1
priority percent 29
exit
class IP-oro1
bandwidth percent 21
random-detect dscp-based
exit
class IP-plata1
bandwidth percent 15
random-detect dscp-based
exit
class IP-bronce1
bandwidth percent 10
random-detect dscp-based
exit
exit
interface Ethernet0/1
service-policy output politica_salida
exit
```

CE2

```
=====================================
enable
configure terminal
interface Ethernet0/0
ip address 172.10.20.1 255.255.255.252
no shutdown
```

```
exit
interface Ethernet0/1
ip address 172.16.20.1 255.255.255.0
no shutdown
exit

ip route 0.0.0.0 0.0.0.0 172.10.20.2
CE3
====================================
enable
configure terminal
interface Ethernet0/0
ip address 172.10.30.1 255.255.255.252
no shutdown
exit
interface Ethernet0/1
ip address 172.16.30.1 255.255.255.0
no shutdown
exit
ip route 0.0.0.0 0.0.0.0 172.10.30.2
class-map IP-premium1
match dscp ef
exit
class-map match-any IP-oro1
match dscp af11 af13
exit
class-map match-any IP-plata1
match dscp af21 af23
exit
class-map match-any IP-bronce1
match dscp af31 af33
exit
policy-map politica_salida
class IP-premium1
priority percent 29
exit
class IP-oro1
bandwidth percent 21
random-detect dscp-based
exit
class IP-plata1
bandwidth percent 15
random-detect dscp-based
exit
class IP-bronce1
bandwidth percent 10
random-detect dscp-based
exit
exit
interface Ethernet0/1
```

service-policy output politica_salida
exit

CE4
==========
enable
configure terminal
interface Ethernet0/0
ip address 172.16.40.1 255.255.255.0
no shutdown
exit
interface Ethernet0/1
ip address 172.10.40.1 255.255.255.252
no shutdown
exit
ip route 0.0.0.0 0.0.0.0 172.10.40.2

Generador-Tráfico
==========
ifconfig eth0 172.16.10.10 netmask 255.255.255.0
route add default gw 172.16.10.1

PC1
==========
ifconfig eth0 172.16.10.11 netmask 255.255.255.0
route add default gw 172.16.10.1

PC (Emisor FTP)
==========
ifconfig eth0 172.16.100.10 netmask 255.255.255.0
route add default gw 172.16.30.1

Receptor Tráfico
==========
ifconfig eth0 172.16.30.10 netmask 255.255.255.0
route add default gw 172.16.30.1

PC2
==========
ifconfig eth0 172.16.30.12 netmask 255.255.255.0
route add default gw 172.16.30.1

Ubuntu (Servidor FTP)
==========
ifconfig eth0 172.16.30.11 netmask 255.255.255.0
route add default gw 172.16.30.1