UNIVERSIDAD NACIONAL SAN ANTONIO ABAD DEL CUSCO

FACULTAD DE INGENIERIA ELECTRICA, ELECTRONICA, INFORMATICA Y MECANICA

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

TESIS

IMPLEMENTACIÓN DE INGENIERÍA DE TRAFICO SOBRE MPLS-VPN EN UN ENTORNO DE LABORATORIO DE PRUEBA

PRESENTADO POR:

Br. ANDERSON VALDERRAMA PEREZ

PARA OPTAR AL TITULO PROFESIONAL DE INGENIERO ELECTRONICO

ASESOR:

Dr. JORGE LUIS ARIZACA CUSICUNA

Cusco-Perú
2025

Universidad Nacional de San Antonio Abad del Cusco

INFORME DE SIMILITUD

(Aprobado por Resolución Nro.CU-321-2025-UNSAAC)

El que suscribe, el **Asesor** JORGE LUIS ARIZACA CUSICUNA quien aplica el software de detección de similitud al trabajo de investigación/tesis titulada: IMPLEMENTACIÓN DE INGENIERÍA DE TRAFICO MPLS - VPN EN UN ENTORNO DE LABORATORIO DE PRUEBA

Presentado por: ANDERSON VALDERRAMA PEREZ DNI N° 41665677;
presentado por: ..... DNI N°: .....
Para optar el título Profesional/Grado Académico de INGENIERO ELECTRONICO

Informo que el trabajo de investigación ha sido sometido a revisión por ..... veces, mediante el Software de Similitud, conforme al Art. 6° del ***Reglamento para Uso del Sistema Detección de Similitud en la UNSAAC*** y de la evaluación de originalidad se tiene un porcentaje de 9 %.

Evaluación y acciones del reporte de coincidencia para trabajos de investigación conducentes a grado académico o título profesional, tesis

Porcentaje	Evaluación y Acciones	Marque con una (X)
Del 1 al 10%	No sobrepasa el porcentaje aceptado de similitud.	X
Del 11 al 30 %	Devolver al usuario para las subsanaciones.	
Mayor a 31%	El responsable de la revisión del documento emite un informe al inmediato jerárquico, conforme al reglamento, quien a su vez eleva el informe al Vicerrectorado de Investigación para que tome las acciones correspondientes; Sin perjuicio de las sanciones administrativas que correspondan de acuerdo a Ley.	

Por tanto, en mi condición de Asesor, firmo el presente informe en señal de conformidad y **adjunto** las primeras páginas del reporte del Sistema de Detección de Similitud.

Cusco, 15 de ENERO de 2026

Firma

Post firma JORGE LUIS ARIZACA CUSICUNA

Nro. de DNI 42348906

ORCID del Asesor 000-0003-2658-5492

Se adjunta:

1. Reporte generado por el Sistema Antiplagio.
2. Enlace del Reporte Generado por el Sistema de Detección de Similitud: **oid:** 27259:546331692

Anderson Valderrama Perez

Volumen-Tesis_Final.pdf

Universidad Nacional San Antonio Abad del Cusco

Detalles del documento

Identificador de la entrega
trn:oid:::27259:546331692

Fecha de entrega
14 ene 2026, 11:07 p.m. GMT-5

Fecha de descarga
14 ene 2026, 11:14 p.m. GMT-5

Nombre del archivo
Volumen-Tesis_Final.pdf

Tamaño del archivo
11.1 MB

224 páginas

45.322 palabras

248.905 caracteres

9% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Fuentes principales

7% Fuentes de Internet
2% Publicaciones
5% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Caracteres reemplazados
170 caracteres sospechosos en N.º de páginas
Las letras son intercambiadas por caracteres similares de otro alfabeto.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Dedicatoria

Este trabajo de tesis va dedicado a mis padres y hermanos, por su apoyo incondicional, apoyo constante. Este logro también es suyo. Gracias por estar siempre conmigo.

Agradecimientos

A mi familia, mi mayor apoyo, gracias por su amor incondicional, aliento constante y sacrificios.

Doy gracias, de forma sincera, por la aceptación y buena acogida que tuve al solicitar este proyecto a mi actual Asesor, M. Sc. Jorge Luis Arizaca Cusicuna. Su orientación fue clave para culminar este trabajo con éxito. Gracias por su tiempo y dedicación.

Agradezco sinceramente a los docentes de Escuela Profesional por proporcionarme los recursos y espacios necesarios para llevar a cabo este proyecto. Su apoyo y disposición fueron fundamentales. Gracias por su generosidad.

Índice

Índice de tablas

Índice de Figuras

Resumen

En este trabajo se describe el protocolo MPLS (IP/MPLS) y su aplicación en una implementación sobre enrutadores Mikrotik (Sistema Operativo RouterOS v7). El objetivo de este proyecto es analizar primero el funcionamiento teórico de este protocolo para finalmente, implementar en laboratorio sobre equipos físicos (Mikrotik modelo CCR2004-16G-2S+) una solución de ingeniería de tráfico para el transporte de servicios VPN L3 y VPN L2 (VPLS).

Se realizará un análisis del tráfico sobre una red IP/MPLS usando Wireshark (Software de libre licencia para el análisis de tráfico) el cual nos permitirá analizar el tráfico que viaja a través de la red IP/MPLS (conmutación de etiquetas). Esto permitirá analizar cómo se realiza la asignación, cambio y retiro de etiquetas. Como BGP realiza asignación de etiquetas de servicio para las VPN (L3 y L2). Verificar el apilamiento de etiquetas (etiquetas de transporte, etiquetas de servicio).

Se realizará un análisis de rendimiento de los servicios VPN L3 y VPN L2 implementado sobre IP/MPLS. Para lo cual se hará uso de un generador de tráfico con flujos de datos (Best Effort, Multicast, Telefonía IP) obteniendo métricas (latencia, jitter, MOS, ICPIF, perdida de paquetes) que nos permitan evaluar y realizar una comparativa entre los servicios (VPN L3 y VPN L2) implementados.

Se usará el software NETEM, que nos permita emular condiciones de red controladas donde podamos evaluar los parámetros de rendimiento de los diferentes tipos de tráfico que viajaran por la red implementada.

Palabras clave ---- MPLS, L3VPN, VPLS, Generador de tráfico, Parámetros de rendimiento.

Abstract

This paper describes the MPLS (IP/MPLS) protocol and its application in an implementation on Mikrotik routers (RouterOS v7 operating system). The objective of this project is to first analyze the theoretical operation of this protocol and then implement a traffic engineering solution for the transport of L3 VPN and L2 VPN (VPLS) services in a laboratory on physical equipment (Mikrotik model CCR2004-16G-2S+).

Traffic analysis will be performed on an IP/MPLS network using Wireshark (free software for traffic analysis), which will allow us to analyze the traffic traveling through the IP/MPLS network (label switching). This will allow us to analyze how labels are assigned, changed, and removed. How BGP performs service label assignment for VPNs (L3 and L2). Verify label stacking (transport labels, service labels).

A performance analysis of the L3 and L2 VPN services implemented over IP/MPLS will be performed. To do this, a traffic generator with data flows (Best Effort, Multicast, IP Telephony) will be used to obtain metrics (latency, jitter, MOS, ICPIF, packet loss) that will allow us to evaluate and compare the implemented services (L3 VPN and L2 VPN).

NETEM software will be used to emulate controlled network conditions where we can evaluate the performance parameters of the different types of traffic traveling through the implemented network.

Keywords ---- MPLS, L3VPN, VPLS, Traffic Generator, Performance Parameters.

Capítulo 1

Generalidades

1.1 Introducción

El presente trabajo de tesis, tiene como finalidad evaluar el rendimiento de una red IP/MPLS a través de la implementación ingeniería tráfico para el transporte de servicios de VPN (L3 y L2) en enrutadores Mikrotik del laboratorio de telemática de la escuela profesional de Ingeniería Electrónica. Si bien MPLS es un protocolo que tiene varios años, aún sigue vigente en implementaciones para brindar servicio de VPN (L3 y L2) e ingeniería de tráfico.

Es por ello que se tomó la información necesaria del protocolo MPLS sobre enrutadores Mikrotik (sistema operativo RouterOS v7), en base a sus especificaciones técnicas, recomendaciones. Se hará una evaluación de la red IP/MPLS transportando servicios de red como VPN L3, VPN L2 a través de túneles de ingeniería de tráfico, se aplicará calidad de servicio y analizaremos el comportamiento de la red con y sin calidad de servicio.

MPLS es un mecanismo de transporte que utiliza etiquetas para tomar decisiones sobre el reenvió de datos. La ingeniería de tráfico (Traffic Engineering, TE) en redes IP/MPLS permite la gestión de los recursos de los enlaces de redes. Permitiendo ejercer un control sobre las rutas que siguen los paquetes de datos, superando las limitaciones del enrutamiento tradicional basado únicamente en el camino más corto. En el contexto de servicios de Red Privada Virtual (VPN) de capa 3 y Servicios de LAN Privada Virtual (VPLS), la implementación de ingeniería de tráfico ofrece beneficios significativos en términos de optimización del ancho de banda, mejora de la calidad de servicio y garantía de acuerdos de nivel de servicios (SLA).

La Ingeniería de Trafico se integra con las L3VPN para optimizar el rendimiento y la fiabilidad de los servicios de conectividad IP ofrecidos a los clientes. Aunque el enrutamiento dentro de la VPN es manejado por los PE (Provider Edge), el tráfico entre los PE (a través de la red troncal del proveedor) puede beneficiarse enormemente de la TE (traffic Engineering). Los túneles TE pueden ser utilizados para transportar el tráfico de L3VPN a través de rutas predefinidas que eviten la congestión o que cumplan con los requisitos específicos de QoS.

La ingeniería de tráfico en VPLS se centra en la optimización del transporte de los frames Ethernet a través de la troncal MPLS. Aunque VPLS opera en la capa 2, el transporte subyacente se realiza sobre túneles MPLS, lo que permite aplicar los principios de TE (traffic

Engineering). Los túneles TE pueden ser utilizados para dirigir el tráfico de VPLS a través de la ruta específicas que cumplan con los requisitos de rendimiento o que eviten la congestión.

1.2 Planteamiento Del Problema

Las redes privadas virtuales VPN L3 y L2(VPLS) basadas en MPLS son ampliamente utilizadas por organizaciones y proveedores de servicios para conectar sitios geográficamente dispersos de forma segura y escalable. Estas redes aprovechan las ventajas de MPLS, como el transporte eficiente de paquetes mediante la conmutación de etiquetas y la separación lógica de tráfico entre clientes. La creciente demanda de aplicaciones en tiempo real (voz, video, datos) exigen redes de alta disponibilidad, baja latencia-jitter y uso óptimo de recursos. Aquí surge Ingeniería de tráfico (TE) y calidad de servicio para el transporte de los servicios VPN a través de túneles de ingeniería de tráfico.

Los enrutadores Mikrotik son equipos de red que gracias a su sistema operativo RouterOS basado en Linux y su bajo coste con respecto a otros enrutadores de otras marcas tiene mucha presencia en organizaciones públicas y privadas (Proveedores de servicio de internet medianas, instituciones gubernamentales).

En este escenario, podemos encontrar empresas que, con el fin de reducir gastos, puedan implementar la solución de red de datos con equipos MikroTik, ya que esta tecnología permite soluciones de MPLS, calidad de servicio, Firewall, IoT y VPNs bajo una única licencia, todos los enrutadores Mikrotik desde lo más básico permite implementar todos los servicios, diferenciándose en la cantidad de usuarios que puede manejar, según la capacidad de hardware.

Es importante destacar que los proveedores de servicios (ofrecer servicios de VPNs) y empresas públicas y privadas pueden implementar servicios de VPNs a través de IP/MPLS para poder interconectar sus diferentes sedes distribuidas geográficamente.

En Perú las empresas públicas y privadas tienen implementados la red basada en IP/MPLS para interconectar sus diferentes sedes tal es el caso de la SUNAT [1] o la Red dorsal Nacional de Fibra Óptica [2].

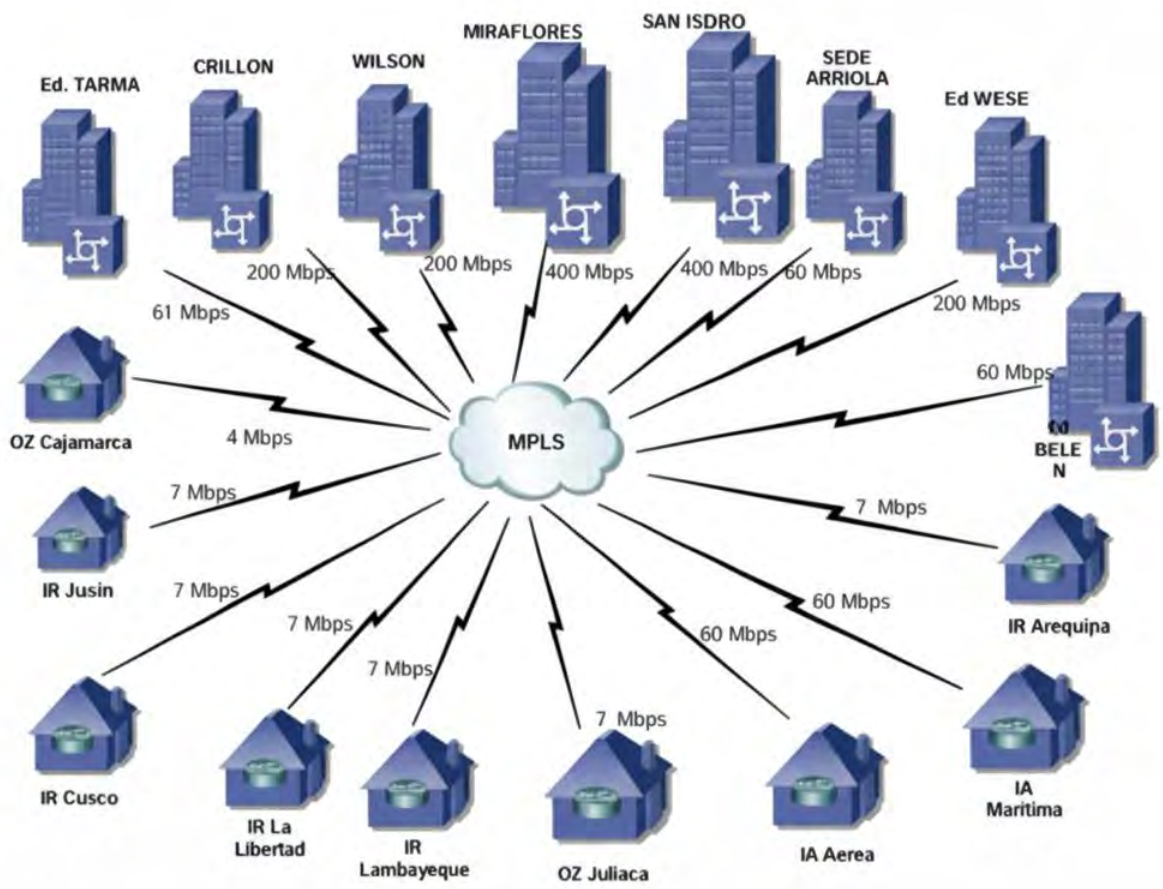


Figura 1.2.1 Topología de red SUNAT [1]

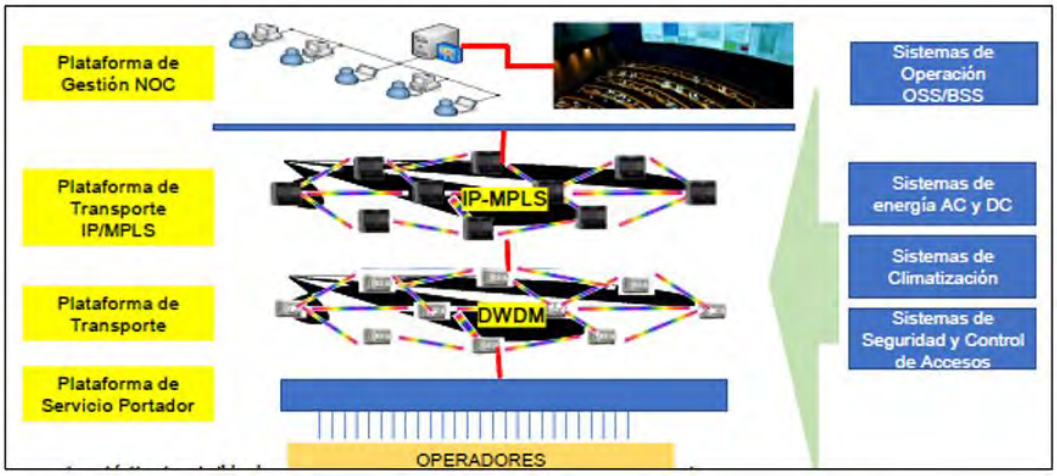


Figura 1.2.2 Esquema de la topología de red de la RDNFO [2]

A nivel de empresas o instituciones como universidades se puede implementar una red IP/MPLS para poder administrar, segmentar y dar prioridad al flujo de sus tráficos de su red interna, considerando que los recursos como ancho de banda de la LAN, conectividad a internet son recursos limitados y más hoy en día donde la demanda de tráfico en tiempo real es el tráfico de mayor demanda. Por lo mencionado anteriormente los enrutadores Mikrotik juegan un rol

importante por la funcionalidad de su sistema operativo (RouterOS), que permite implementar diferentes servicios sin depender de un licenciamiento individual que depende de cada servicio.

La demanda por conectividad sigue mostrando un crecimiento sostenido en el país. A diciembre de 2024, la dinámica de las conexiones de internet continuó su tendencia al alza, superando 14.95 % a lo registrado el año previo, informó el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).

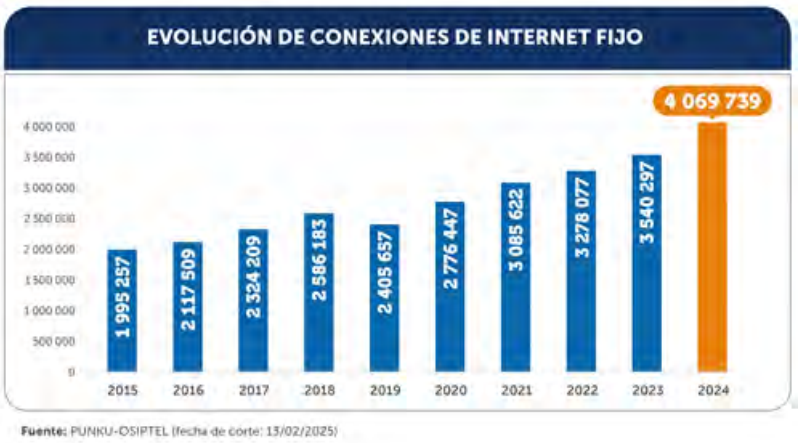
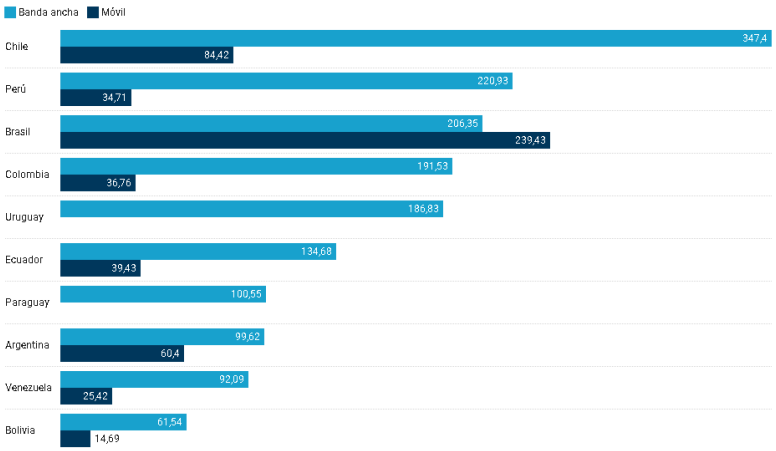


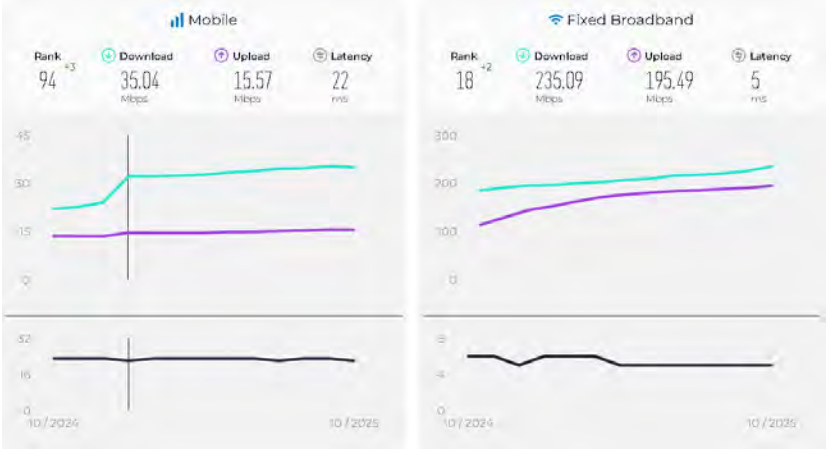
Figura 1.2.3 Evolución de la conectividad de Internet [3]

A nivel de América Latina, como se observa en la figura 1.2.4, en 2024 el Perú registra una velocidad promedio de descarga de internet móvil de 33.39 Mbps. En cuanto a banda ancha fija, el Perú destaca con una velocidad de 210 Mbps. Estos datos evidencian que, si bien el Perú mantiene una posición media en internet móvil, ha logrado posicionarse con uno de los países con mayor velocidad en banda ancha fija en la región.



Fuente: CEPLAN, https://observatorio.ceplan.gob.pe/ficha/t63

Figura 1.2.4 Velocidad promedio de descarga de internet, agosto 2025 (Mbps) [4]



Fuente: https://www.speedtest.net/global-index/peru

Figura 1.2.5 Velocidades de la mediana de país de Perú actualizadas octubre 2025 [4]

Al cierre de 2024, el 72.4 % de conexiones de internet fijo en Perú, es decir, 2 946 326 conexiones, cuenta con velocidades de bajada o descarga contratadas mayores o iguales a los 200 Mbps (megabits por segundo), más del doble de lo reportado el año previo (1 174 384 conexiones), informó el Organismo de Supervisión de Inversión Privada en Telecomunicaciones (OSIPTEL).

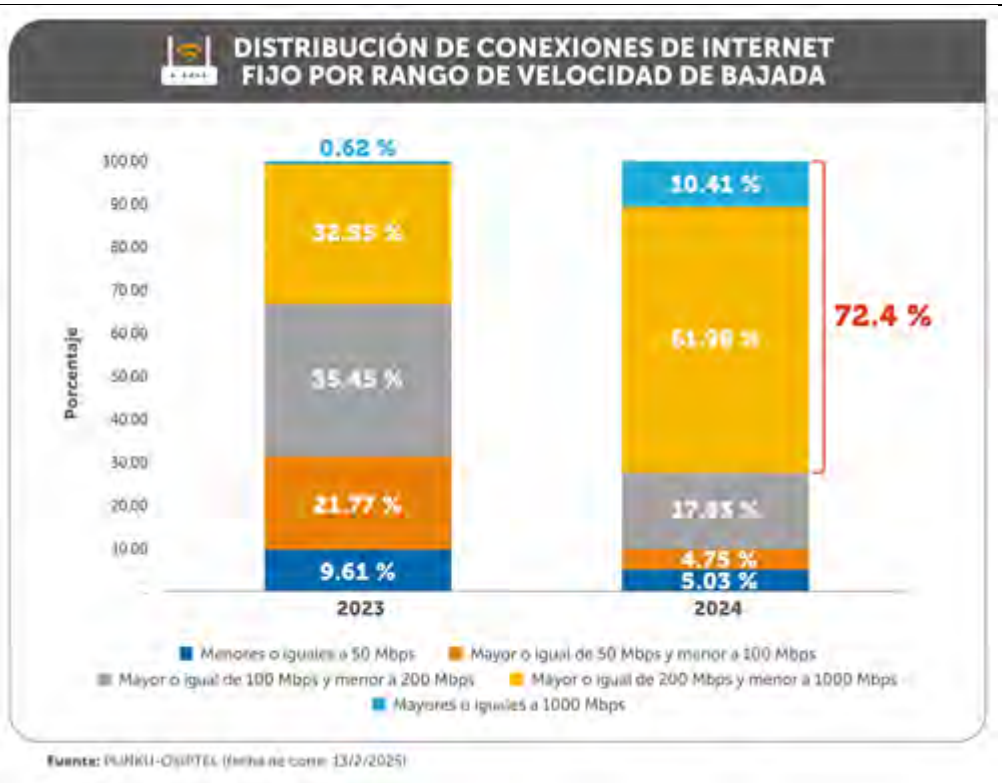


Figura 1.2.6 El 72 % de conexiones de internet contratadas esta entre los 200 Mbps [3]

Esto se podrá reflejar en una mejor gestión de estos recursos como el internet, lo cual se puede lograr con dispositivos de red con sistemas operativos de red que sean escalables como es el caso de RouterOS de Mikrotik que tiene la capacidad de poder implementar muchos tipos de servicios (firewall, Queue, VPN, MPLS) gracias a su flexibilidad.

1.2.1 Problema General

El tráfico de red IP es la predominante en la actualidad, el cual se describe como la red de “Best Effort” donde todos los paquetes de red se tratan por igual haciendo su mejor esfuerzo para la entrega de los mismos, el envío de los paquetes se basa en la IP de destino los cuales son procesados por enrutadores a través de los protocolos de enrutamiento que se basan en métricas, es decir cuando todas las métricas son iguales, el tráfico de datos toma la ruta con el menor número de saltos, lo que genera congestión por la sobreutilización de la ruta generada por el protocolo de enrutamiento a su vez dejando subutilizados otras rutas de red. El transporte de datos a través de redes sin calidad de servicio, aislamiento (privadas para cada cliente) e ingeniería de tráfico no son óptimas debido a que no existe una gestión de los recursos de red (ancho de banda de conexión a internet, ancho de banda de la red LAN, WAN, Capacidad de cómputo de los diferentes equipos de comunicaciones de la red) que son limitados. Esto es por las limitaciones de los sistemas operativos que tienen la mayoría de los dispositivos desplegados, o falta de recursos con información de análisis de rendimiento e implementación sobre cómo transportar el tráfico IP a través de IP/MPLS como en el caso de los dispositivos Mikrotik, ya que debido a la migración de sus sistema operativo a una versión más actual del core de Linux (RouterOS está basada en Linux), existe documentación muy escasa sobre las posibilidades que podría traer su implementación, esta falta de recursos se puede ver reflejado en su página web; el sistema operativo de red RouterOS de Mikrotik soporta muchos protocolos de red que permiten implementar servicios de red como L3VPN y VPLS.

Por tal motivo, el trabajo de tesis a desarrollar es la “implementación de IP/MPLS con servicios de VPN L3 y VPN L2(VPLS) que se transportarán sobre túneles de ingeniería de tráfico, permitiendo analizar su funcionamiento e implementación en equipos Mikrotik. La implementación se realizará con enrutadores Mikrotik en el laboratorio de telemática de la escuela profesional de ingeniería electrónica dentro de la UNSAAC.

1.2.2 Problemas Específicos

- El algoritmo de los protocolos de enrutamiento que consideran los saltos, estados de enlace sin ningún tipo de prioridad de tráfico, y respaldo de las rutas. No son suficientes para un óptimo transporte del tráfico IP que es la predominante en la actualidad.

- El costo de los equipos de comunicación está relacionados a los diferentes servicios que se pueden agregar según la licencia (licenciado por servicio) lo que no permite una gestión óptima de los recursos de red.
- A pesar de que el protocolo MPLS es soportado por RouterOS de MikroTik, existe una falta de información sobre la implementación de IP/MPLS que preste servicio de VPN L3, VPN L2(VPLS) e ingeniería de tráfico.
- La falta de análisis en routers Mikrotik, sobre el encapsulamiento de paquetes IP con MPLS, que nos permita implementar diferentes servicios gracias a la capacidad de apilamiento de etiquetas.

1.3 Justificación

MikroTik, con su sistema operativo RouterOS, ha evolucionado para ofrecer capacidades robustas de MPLS y, más recientemente, de Ingeniería de Tráfico. Con la versión 7 de RouterOS, MikroTik ha mejorado significativamente su soporte para MPLS-TE, permitiendo implementar soluciones de Ingeniería de Tráfico.

Ante las problemáticas expuestas, la implementación de una arquitectura de red basada en MPLS, complementada con servicios VPN de capa 3 (L3VPN), servicios de LAN Private Virtual (VPLS) para VPN de Capa 2, y la aplicación de ingeniería de tráfico (TE), emerge como una solución estratégica para su implementación para el transporte de redes IP tradicionales y así poder implementar los diferentes servicios que se pueden implementar sobre IP/MPLS (VPN de capa 2 y capa 3).

La Ingeniería de Tráfico se puede integrar con las L3VPN para optimizar el rendimiento y la fiabilidad de los servicios de conectividad IP. Aunque el enrutamiento dentro de la VPN es manejado por los enrutadores PE, el tráfico entre los PE (a través de la red IP/MPLS) puede beneficiarse enormemente de la TE. Los túneles TE pueden ser utilizados para transportar el tráfico de L3VPN a través de rutas predefinidas que eviten la congestión o que cumplan con requisitos específicos de QoS.

La Ingeniería de Tráfico en VPLS se centra en la optimización del transporte de los frames Ethernet a través de la red troncal MPLS. Aunque VPLS opera en la Capa 2, el transporte subyacente se realiza sobre túneles MPLS, lo que permite aplicar los principios de TE. Los túneles TE pueden ser utilizados para dirigir el tráfico de VPLS a través de rutas específicas que cumplan con los requisitos de rendimiento o que eviten la congestión.

El laboratorio de la escuela profesional de Ingeniería Electrónica cuenta con enrutadores Mikrotik. Esto nos permitirá realizar un análisis de rendimiento de las VPN L3 y L2 en términos de parámetros de rendimiento como la latencia, jitter, MOS, pérdida de paquetes, ICPIF.

1.4 Objetivos

1.4.1 Objetivo General

Implementar y analizar VPN (Virtual Private Network) sobre una red IP/MPLS y su transporte sobre túneles de ingeniería de tráfico.

1.4.2 Objetivos Específicos

- Estudiar a nivel conceptual los Protocolos de enrutamiento, IP/MPLS, Ingeniería de tráfico (TE), MPLS VPN L3 y L2.
- Implementar una red IP/MPLS en un entorno de laboratorio con enrutadores Mikrotik.
- Implementar L3VPN sobre IP/MPLS en un entorno de laboratorio con enrutadores Mikrotik.
- Implementar L2VPN sobre IP/MPLS en un entorno de laboratorio con enrutadores Mikrotik.
- Implementar y Evaluar el desempeño de L3VPN sobre IP/MPLS que soporte túneles de ingeniería de tráfico para el transporte de las L3VPN.
- Análisis de tráfico de la red implementada con herramientas de software libre.

1.5 Alcances

- Se realizará una descripción de una red IP/MPLS implementada en el laboratorio con enrutadores Mikrotik; realizando un análisis de tráfico con la herramienta de software Wireshark.
- Se realizará la implementación de servicios de VPN L3 y L2 sobre la red IP/MPLS, los servicios serán transportadas sobre túneles de ingeniería de tráfico. Realizando un análisis de tráfico con la herramienta de software Wireshark.
- Se establecerá un estudio comparativo, generando tráfico con y sin QoS sobre las VPN L3 y L2.
- Los resultados serán analizados a través de gráficas que nos permita visualizar el rendimiento de las VPNs.

1.6 Limitaciones

- Una de las limitaciones es Mikrotik a través de su sistema operativo RouterOS v7 que al migrar a Linux versión 5.6 está en constante actualización, lo que conlleva inestabilidades en la implementación de ingeniería de tráfico.
- Si bien la implementación de la topología de red es con equipos físicos es a nivel de laboratorio.
- La implementación de los diferentes servidores y equipos finales será sobre máquinas virtuales.
- Los parámetros de rendimiento evaluados para el análisis comparativo de las tecnologías mencionadas se obtendrán por medio de un generador de tráfico, que nos permite simular diferentes tipos de paquetes.

1.7 Metodología

Para alcanzar los objetivos planteados en este trabajo de tesis se utiliza una serie de procesos enmarcados dentro del modelo Descriptivo-Aplicativo. Los procesos incluyen:

El trabajo de tesis realiza la evaluación y cuantificación del desempeño de las VPN L3 y L2 sobre IP/MPLS con túneles de ingeniería de tráfico. Las métricas utilizadas para comparar el desempeño son: Latencia, Jitter, Pérdida de paquetes, MOS, ICPIF y poder comprarlas con valores umbrales que son establecidas en estándares internacionales.

- Implementación y Análisis: La implementación de los escenarios se dará en un entorno de laboratorio, para su análisis se inyecta tráfico modelado por un generador de tráfico.
- Se realizarán simulaciones de condiciones controladas con el software NETEM que me permite configurar los parámetros de rendimiento de red.
- Con el software Wireshark se realiza un análisis de los paquetes que viajan por las redes implementadas.

Capítulo 2

Marco Teórico

2.1 Antecedentes

Revisando repositorios digitales de universidades, de trabajos de investigación recientes con respecto a MPLS sobre router Mikrotik, el trabajo de tesis de Alvaro Andragon, Diego Marcelo [5], que desarrolla el diseño y simulación de una red MPLS utilizando equipos Mikrotik y el emulador GNS3 en entornos PYMES, en el capítulo 5 del trabajo de investigación se analiza el protocolo MPLS a través de un caso de uso, implementando de manera exitosa MPLS para el transporte de servicios de red, demostrando la funcionalidad del RouterOS en la implementación de la arquitectura MPLS.

Por otro lado, el trabajo de tesis de los autores Moreno Ibañez, Cristian; Quiñonez Pazmiño, Juan [6], que desarrollan el Diseño de una red con DMVPN sobre una red MPLS de Puntonet, en el Capítulo 5 de prueba y análisis de conectividad, se demuestra cómo la tecnología MPLS con DMVPN mejora el rendimiento de la red llegando a disminuir la latencia de red en un 70%.

El trabajo de fin de grado de Carpio Ortiz, David [7], que desarrolla un entorno MPLS en equipos Mikrotik y simulado en GNS3, el trabajo se enfoca en montar una red con equipos Mikrotik que permiten profundizar en diferentes conceptos de MPLS, etiquetado LDP de paquetes, redes Privadas Virtuales (VPN) y servicio de redes Privadas Virtuales (VPLS), en los capítulos 3 y 4 se puede ver diferentes tipos de aplicaciones que se puede implementar sobre una arquitectura de red con protocolo MPLS.

El trabajo de tesis de Escobar Poma, José [8], que desarrolla la Implementación de una infraestructura de red basada en tecnología MPLS con mejoras de Ingeniería de tráfico para el sector Industrial – Lima 2022, en el trabajo se demuestra la importancia de la Ingeniería de tráfico cuando trabaja en conjunto con la tecnología MPLS, se demuestra que gracias a la aplicación de estas tecnología el delay de la red disminuye desde un 61 % a un 8.81 %y el Jitter de un 0.016 % a un 0.00000016 %, lo que hace que la red sea más estable y con mejores indicadores.

En el trabajo de tesis de Flores Baldés, Jorge [9], titulado Análisis del desempeño de MPLS VPN L2 y L3 – Santiago de Chile 2018, en el trabajo el autor bajo un entorno simulado

en el software GNS3 usando imágenes de los router Cisco realiza una comparación de los servicios L2VPN y L3VPN. Realizando un análisis de datos de la topología implementada se afirma que la latencia y jitter del servicio L2VPN es mayor con respecto al servicio L3VPN, mientras que para tráfico multicast el retardo de L2VPN es levemente menor con respecto a L3VPN y en términos de perdida de paquetes el rendimiento de L2VPN es mejor que la de L3VPN.

2.2 MPLS (Multiprotocol Label Switching) [9]

Él envió de paquetes en una red MPLS, se basa en la conmutación de etiquetas. La asignación de las etiquetas puede estar basadas en prefijos o en otro tipo de parámetros esta asignación es generado por cada enrutador que forma la red IP/MPLS. El objeto del intercambio de etiquetas entre los enrutadores del dominio IP/MPLS es la formación de caminos o trayectorias virtuales. Estas trayectorias virtuales se denominan LSP (Label Switched Path) y es unidireccional.

En una red IP/MPLS los enrutadores se clasifican según la función que cumplen cada una dentro del dominio IP/MPLS. Los enrutadores de frontera (Tratamiento de tráfico IP y Etiquetado) son conocidos como LER (por sus siglas en inglés, Label Edge Routers) y enrutadores de conmutación de etiquetas LER (por sus siglas en inglés, Label Switching Routers) estos últimos solo conocen de la conmutación de etiquetas y no saben nada del tráfico del cliente.

PE/LER: Están ubicados en el borde del dominio MPLS, la interacción con el cliente es a nivel de capa 3 del modelo de capas de la red, estos enrutadores analizan tanto sus tablas de enrutamiento y su tabla de conmutación de etiquetas, Aquí es donde el router del cliente se conecta y hace uso de la red IP/MPLS. La función del enrutador de frontera LER en el dominio IP/MPLS es adicionar (PUSH) y retirar (POP) etiquetas dependiendo en que parte de la red está ubicado (Al inicio o al final del recorrido del tráfico).

P/LSR: Routers ubicados en el dominio IP/MPLS son los encargados de realizar la operación de conmutación de etiquetas denominado SWAP. Un enrutador LSR recibe un paquete etiquetado, realiza el procesamiento adecuado y hace el intercambio de la etiqueta y envía el paquete por la interfaz adecuada. Esta función varía según la posición del enrutador en el dominio IP/MPLS, es decir, además de intercambiar puede retirar y adicionar etiquetas.

Las operaciones que realizan los enrutadores del dominio IP/MPLS tienen nombres bien definidos, estas operaciones se realizan sobre las etiquetas de transporte y servicio en una red MPLS.

SWAP-CAMBIAR: Realiza la operación intercambiar etiquetas/s.

PUSH - PONER: Realiza la operación de añadir etiqueta/s.

POP - RETIRAR: Realiza la operación de retirar etiqueta/s.

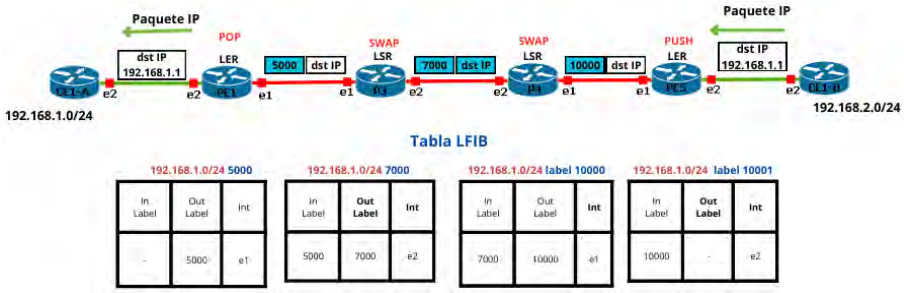


Figura 2.2.1 Enrutadores de la red IP/MPLS y sus Operaciones

2.2.1 Plano de Control en MPLS

MPLS es una red Overlay que trabaja sobre una red Underlay (protocolos de enrutamiento) MPLS utiliza los prefijos (dirección IP y sus Mascara) anunciados por los protocolos de enrutamiento IGP/EGP (Interior Gateway Protocolos/Exterior Gateway Protocols) y otros parámetros para la asignación de etiquetas. El protocolo LDP (Label Distribution Protocol) es el encargado de registrar e intercambiar las etiquetas el protocolo LDP es establecido a través de sesiones TCP para formar trayectorias LSP, caminos virtuales. Los procesos descritos anteriormente son realizados por el protocolo LDP o RSVP-TE.

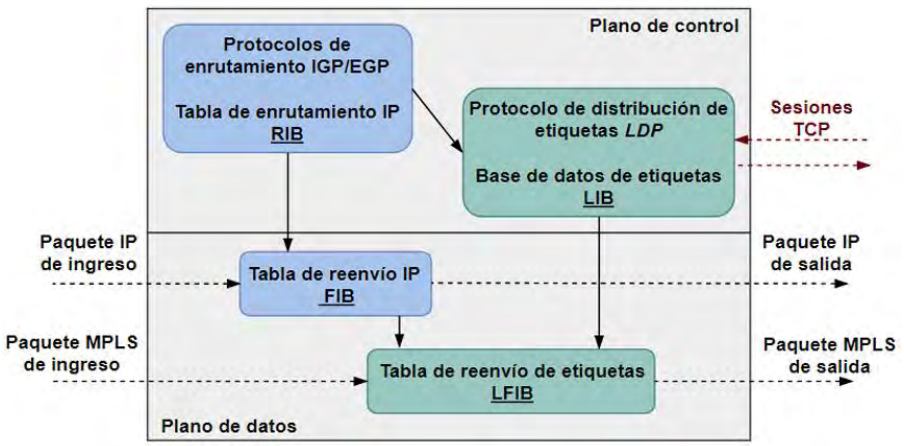


Figura 2.2.2 Plano de Control de MPLS [9]

2.2.2 Cabecera de MPLS

Los enrutadores del domino IP/MPLS (LER, LSR) procesan la pila de etiquetas que está dentro de la cabecera MPLS la misma que está compuesta por cuatro campos: Label, EXP, S y TTL.

- **Label - Etiqueta:** Campo de 20 bits; donde nos indica el valor de la etiqueta. Existen etiquetas reservadas.
- **EXP - Experimental**: Campo de 3 bits; se hace uso para definir la CoS asignada a un conjunto de paquetes que son tratados del mismo modo por el nodo (FEC por sus siglas en inglés, Forward Equivalence Class).
- **S – Apilamiento de etiquetas**: Campo de 1 bit; nos indica de la existencia de pila de etiquetas (Etiqueta de transporte, etiqueta de servicio). Cuando el valor del bit S es 1, la última etiqueta de la pila de etiquetas.
- **TTL**: Campo de 8 bits; tiene la misma funcionalidad de evitar bucles que en un paquete IP. Si el valor del TTL es 0, el paquete es descartado, de otro modo, su valor se decrementa en 1 en cada paso por un LSR, hasta un máximo de 254 saltos.

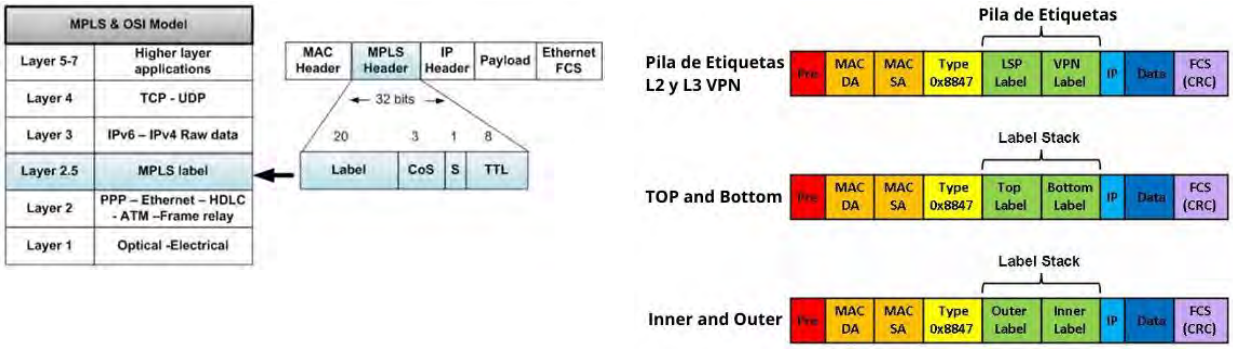


Figura 2.2.3 Cabecera MPLS

Es importante mencionar que haremos referencia a dos tipos de etiquetas. Etiquetas de transporte (LDP y RSVP) y etiquetas de servicios (VPN L3, VPN L2). Las etiquetas de transporte son procesados por los nodos del dominio MPLS (enrutadores LER, LSR) mientras que las etiquetas de servicio son las que identifican los servicios VPNs y son procesados por los enrutadores de borde (LER) del dominio MPLS.

2.2.3 VPNs en MPLS

De forma conceptual, las redes privadas virtuales permiten el acceso y compartición de información a través de túneles lógicos configurados sobre una red compartida. Según la

participación del proveedor en el enrutamiento del cliente y el número de sitios que conecta, las MPLS VPN pueden clasificarse según se muestra en la figura:

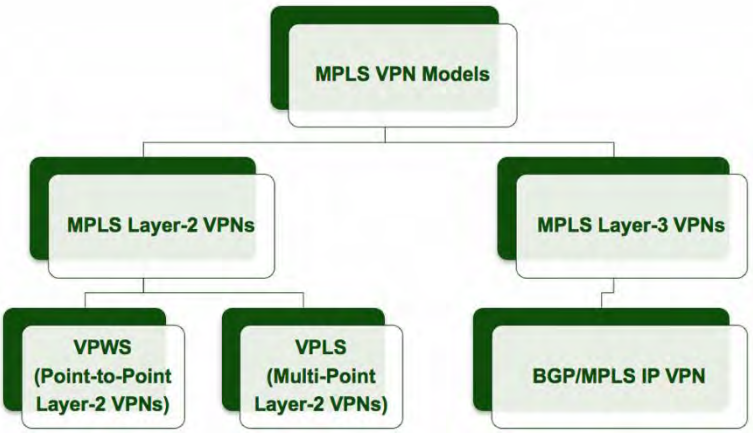


Figura 2.2.4 Clasificación de los servicios VPN MPLS [10]

2.2.4 MPLS VPLS

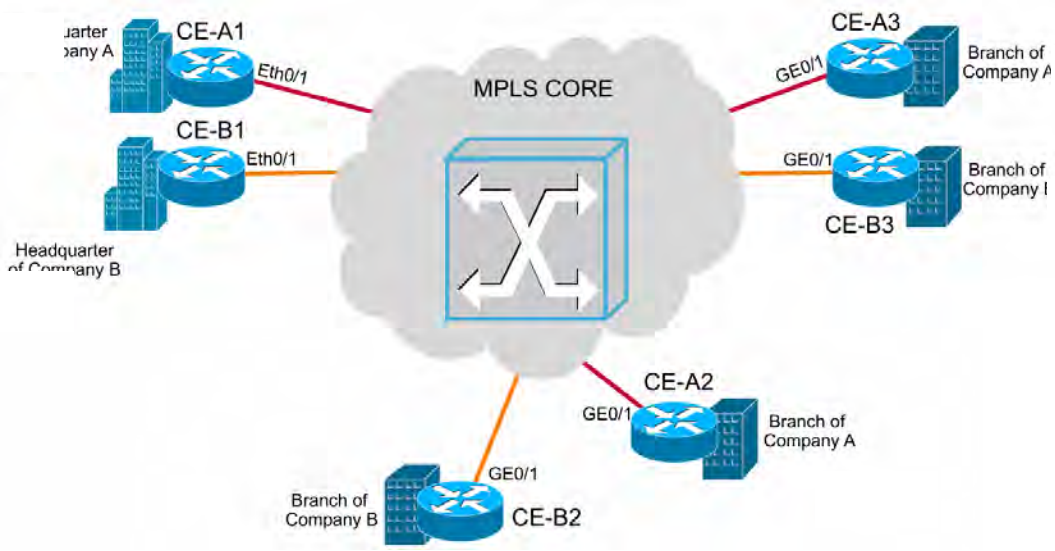


Figura 2.2.5 Topología MPLS VPLS [11]

VPLS (Virtual Private LAN Service) es una tecnología que permite a los proveedores de servicios ofrecer conectividad Ethernet multipunto a multipunto sobre una red MPLS. A diferencia de las L3VPN, VPLS emula un servicio de LAN virtual, haciendo que los sitios de los

clientes conectados a la VPLS se comporten como si estuvieran en la misma red de área local (LAN). Esto significa que el tráfico de Capa 2 (frames Ethernet) se transporta a través de la red MPLS sin necesidad de enrutamiento IP en el lado del proveedor.

La asignación de etiquetas para la formación de la VPLS (L2VPN) puede ser realizada a través de los protocolos LDP o MP-BGP (señalización BGP).

LDP: Ambos enrutadores de frontera LER asignan una etiqueta de servicio VPLS (L2VPN) previamente configurada y envían un mensaje de asignación de etiqueta a su par a través de una sesión LDP o una sesión MP-BGP. El enrutador LER receptor mapea este mensaje con el servicio VPLS y si hay coincidencia utiliza la etiqueta generando la relación y codificación en el mensaje de asignación para enviar los paquetes hacia su par.

MP-BGP: Es una extensión del protocolo BGP y además de anunciar prefijos IPv4 permite anunciar prefijos IPv6, L2VPN, VPNV4, por mencionar algunos. En el contexto de las VPN L2 y VPN L3, MP-BGP es utilizado para anunciar prefijos L2VPN e intercambiar etiquetas de VPN L2 con sus pares. En este trabajo de tesis se usará MP-BGP para la asignación de las etiquetas de servicio.

En ambos casos el protocolo LDP o RSVP-TE es el encargado de asignar la etiqueta de transporte de la cabecera MPLS.

La figura 2.2.6 muestra lo expuesto; los routers PE1 y PE5 distribuyen la etiqueta de servicios L3VPN y VPLS a través de MP-BGP.

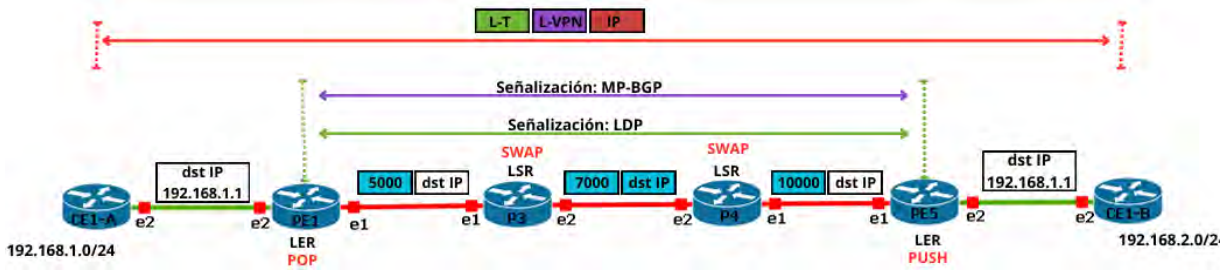


Figura 2.2.6 Intercambio de etiquetas por LDP y MP-BGP

2.2.5 MPLS VPN L3

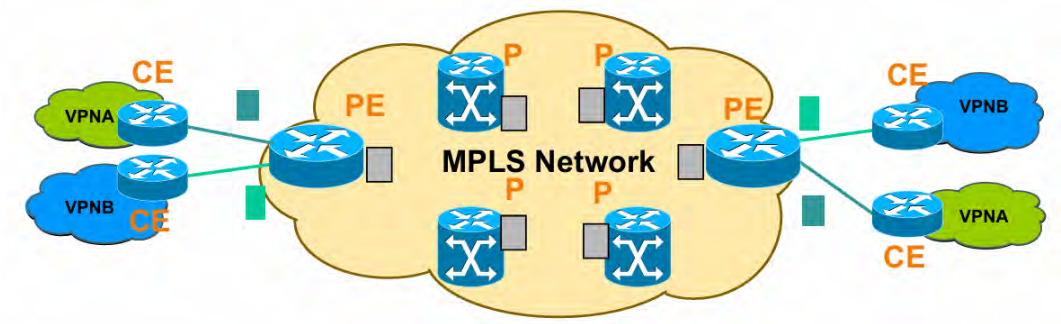


Figura 2.2.7 Topología MPLS L3VPN [10]

Las VPN de Capa 3 (L3VPN) son una de las aplicaciones más extendidas de MPLS, permitiendo a los proveedores de servicios ofrecer conectividad IP segura y escalable a múltiples clientes sobre una infraestructura de red compartida. En una L3VPN, el enrutamiento entre los sitios del cliente es manejado por los routers del proveedor de servicios (Provider Edge, PE), que mantienen tablas de enrutamiento separadas para cada cliente utilizando instancias de enrutamiento virtual y reenvío (VRF).

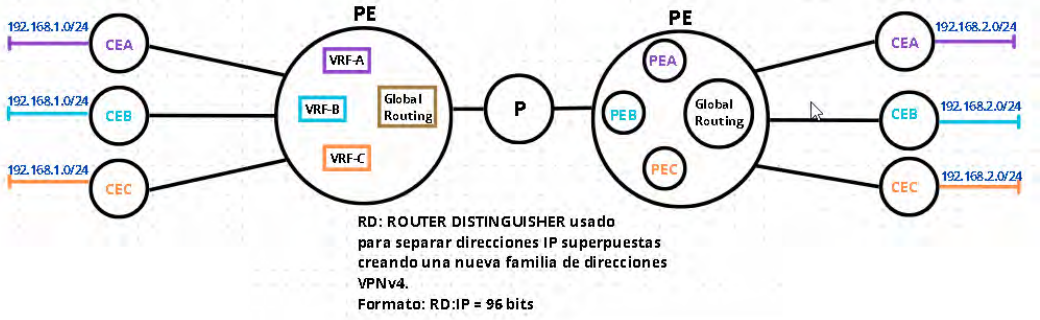


Figura 2.2.8 Tabla de enrutamiento Virtual - VRF

En este modelo de VPN se genera un intercambio de información de enrutamiento entre el cliente y el proveedor (interacción a nivel de capa 3 entre cliente y proveedor). Las rutas entregadas por el cliente son anunciadas entre los nodos LER a través de sesiones MP-BGP y la privacidad de la red se da a través de tablas de enrutamiento virtuales denominadas VRF. Cada VRF posee parámetros relevantes que deben ser configurados según cliente especifico:

Route Distinguisher: Valor de 64 bits. Que junto con la cabecera IP forman un paquete de 96 bits denominado prefijos VPNV4. Al ser únicos en la red permite el solapamiento de direcciones IPv4. Por ejemplo, es posible interconectar a través de una misma infraestructura IP/MPLS dos clientes que usan los mismos segmentos de redes.

Route Target: Valor de 64 bits. Permite realizar las operaciones de importaciones y exportaciones de tráfico VPNV4 que cada LER aprende o publica a través de MP-BGP. Esto nos permite controlar la redistribución de rutas entre diferentes VPN.

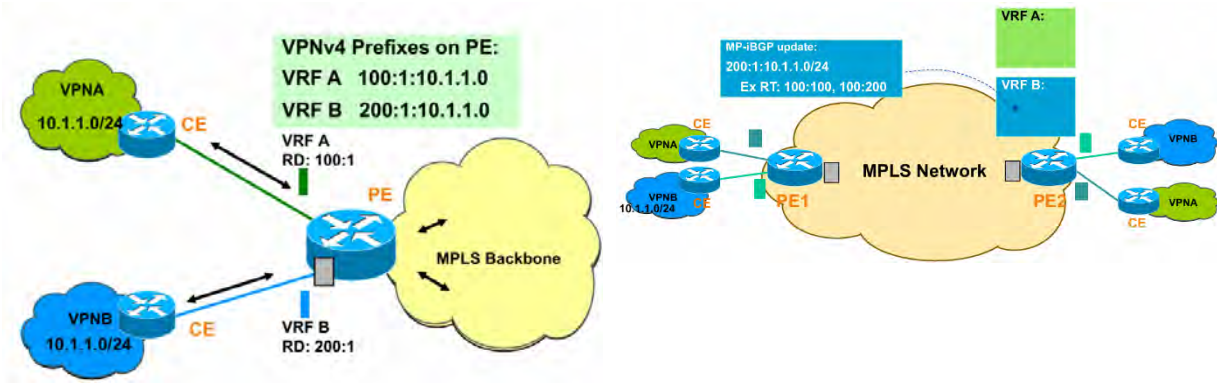


Figura 2.2.9 RD (Route Advertisement) y RT (Route Advertisement) [10]

Al igual que en VPLS, MP-BGP se utiliza para anunciar prefijos VPNV4 e intercambiar etiquetas de servicio L3VPN. El protocolo LDP o RSVP se encarga de asignar la etiqueta externa (etiquetas de transporte) de la cabecera MPLS.

Es necesario recalcar que la compartición de rutas entre el cliente y el proveedor puede ser a través de rutas estáticas, o protocolos de enrutamiento.

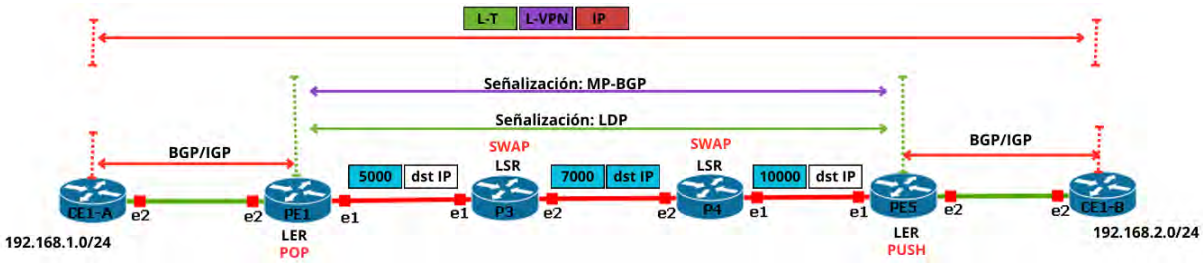


Figura 2.2.10 Señalización de etiquetas en servicios de MPLS VPN L3

2.2.6 MPLS – Ingeniería de Trafico (TE)

Ingeniería de tráfico en MPLS, permite el manejo de congestiones inesperadas, mejor utilización del ancho de banda disponible, reenrutamiento sobre nodos o enlaces caídos, capacidad de planificación.

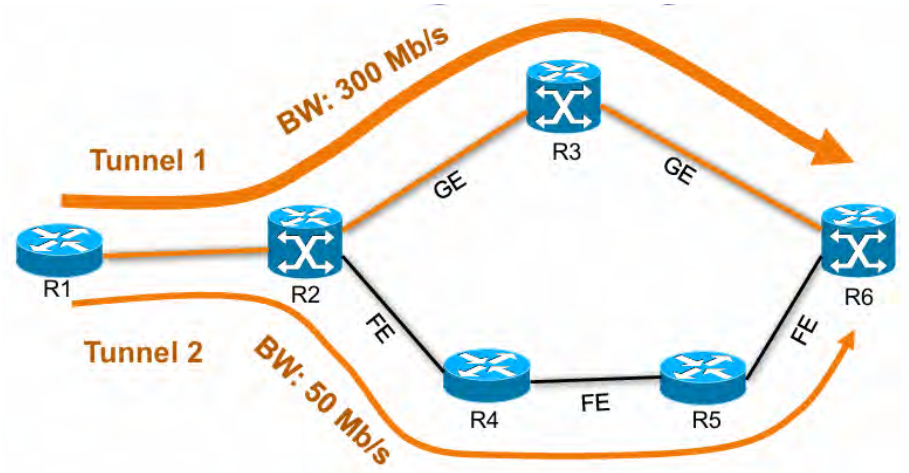


Figura 2.2.11 Túneles de ingeniería de trafico [12]

2.3 Calidad de Servicio – QoS [9]

QoS es un mecanismo que permite clasificar y propagar políticas sobre los diferentes tipos de tráfico que recorren una red, en nuestro caso una red IP/MPLS. Los enrutadores Mikrotik tienen la capacidad de poder aplicar calidad de servicio al tráfico que pasa a través de este.

Clasificación**:** Nos permite marcar y clasificar los paquetes en función del tipo de tráfico que estos transportan El marcado de paquetes se pueden establecer en varios niveles según el modelo TCP/IP utilizando los campos COS, DSCP y EXP de los *header* correspondientes.

Tabla 2.3.1 Reglas de QoS en función del tipo de trafico [9]

Aplicación	*IPP*	*PHB*	*DSCP*	*COS/EXP*
Enrutamiento IP	*6*	*CS6*	*48*	*6*
Voz	*5*	*EF*	*46*	*5*
Video interactivo	*4*	*AF41*	*34*	*4*
Streaming de video	*4*	*CS4*	*32*	*4*
Datos de misión critica	*3*	*-*	*25*	*3*
Señalización de llamadas	*3*	*AF31/CS3*	*26/24*	*3*
Datos transaccionales	*2*	*AF21*	*18*	*2*
Gestión de red	*2*	*CS2*	*16*	*2*
Datos masivos	*1*	*AF11*	*10*	*1*
Scavenger	*1*	*CS1*	*8*	*1*
Mejor esfuerzo	*0*	*0*	*0*	*0*

2.4 Métricas de Desempeño en Redes IP [9]

Para verificar el desempeño de una red se hace a través de la evaluación de las métricas de rendimiento, sus servicios y las políticas de QoS configuradas sobre ella. En redes IP, estas métricas están estandarizadas por organismos internacionales como la IETF y la ITU-T.

2.4.1 Métricas Según la IETF

Las métricas IETF se agrupan en términos de disponibilidad, perdida, retardo y utilización. Y están especificadas en los RFCs 2678, 2679, 2680, 2681 y 3393

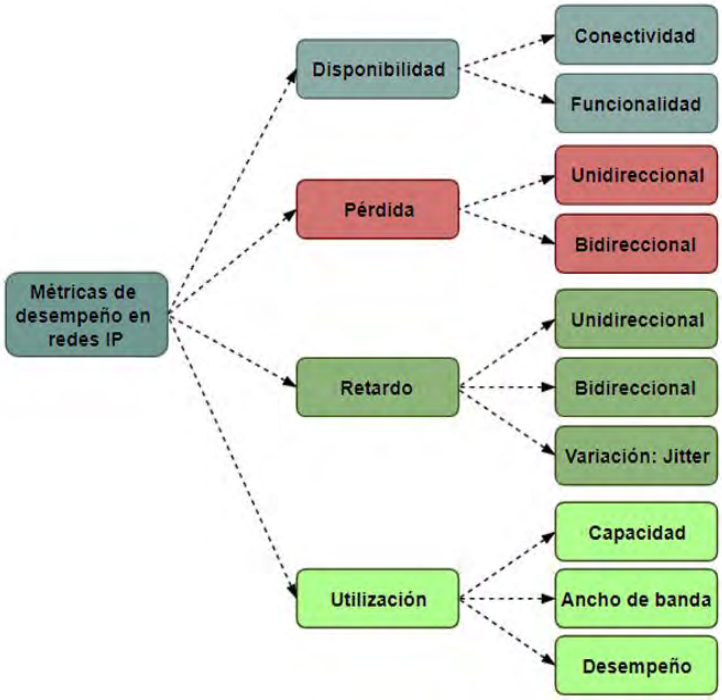


Figura 2.4.1 Métricas de desempeño en redes IP [9]

- **Disponibilidad:** Expresada en términos porcentuales y nos indica la disponibilidad de la mismo dentro de una ventana temporal.
- **Conectividad:** Nos indica la disponibilidad de la conexión física de los nodos de una determinada red.
- **Funcionalidad:** Es la calidad de servicio provista de la red.
- **Pérdida de paquetes:** Cantidad de paquetes perdidos el cual puede ser determinado en una sola dirección o en ambas direcciones del tráfico de red.
- **Retardo:** Es el tiempo que tarda un paquete en viajar desde un origen a un destino, a sus variaciones delta entre cada retardo se le denomina jitter.

- **Utilización:** Es la capacidad de utilización de un sistema o red que este sujeto a la capacidad máxima del sistema. Aquí podemos incluir errores de nodo y protocolos.

2.4.2 Métricas Según la ITU-T

Nos permiten evaluar la calidad y degradación en redes IP.

E-Model (MOS, Mean Opinion Score): Valor numérico entre 1 y 5. Permite indicar la calidad de una sesión de voz en función de varios parámetros como perdida de paquetes, retardo, jitter. En la ITU-T G.107 se describe a detalle como estimarla.

Impairment / Calculated Planning Impairment Factor (ICPIF): Valor numérico entre 5 y 55. Indica el nivel de degradación en función de parámetros como perdida de paquetes, retardo. La ITU-T G.113 describe a detalle como estimarla.

2.5 Protocolos de Enrutamiento Multicast

2.5.1 Protocolo de Gestión de Grupo (GMP)

Este protocolo permite que cualquier interfaz se convierta en receptor para el flujo de multicast. Permite probar las configuraciones de enrutamiento y conmutación multicast sin usar clientes IGMP dedicados.

2.5.2 IGMP Snooping

Permite al switch escuchar comunicación multicast y tomar decisiones de reenvió para tráfico multicast basados en la información recibida. Por defecto los switches inundan la red con tráfico multicast lo que no es eficiente por lo que el IGMP snooping se encarga de que él envió se realice a los dispositivos registrados a una dirección de grupo multicast

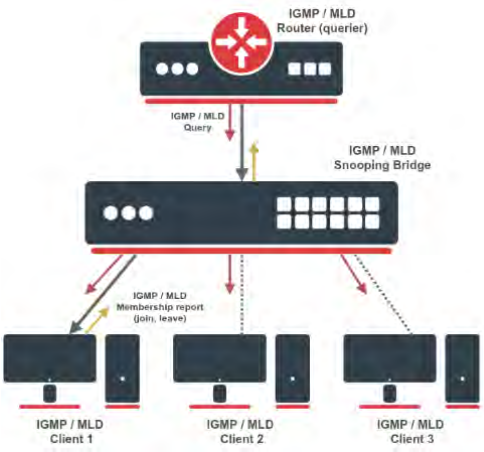


Figura 2.5.1 Protocolo IGMP Snooping

2.5.3 PIM-SM

Es una tecnología que permite compartir datos de forma eficiente con muchos destinatarios a través de la red. Los remitentes transmiten sus datos a una dirección IP multicast especifica, y los receptores indican su interés en recibir los datos enviados a esa dirección. La red se encarga entonces de entregar los datos de los emisores a los receptores.

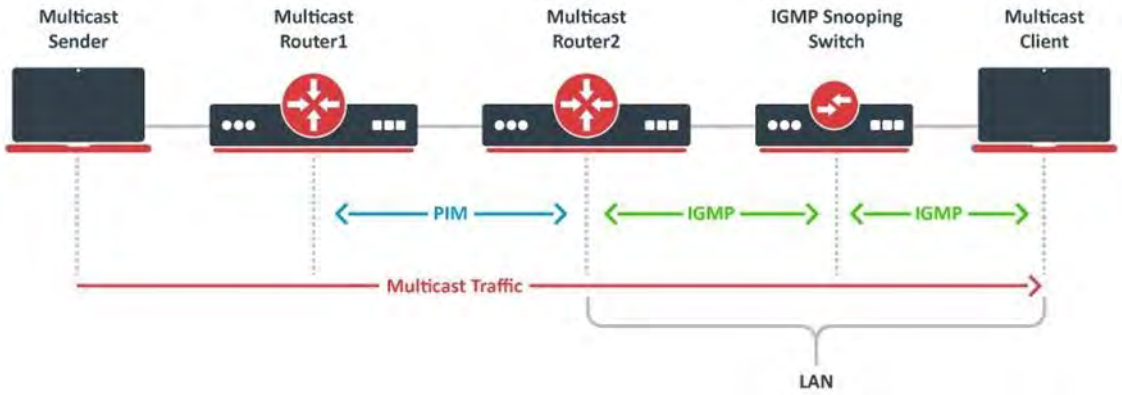


Figura 2.5.2 Protocolo PIM-SM

2.6 Técnicas de Monitoreo Activo y Pasivo de una Red

Las técnicas de monitoreo activo inyectan tráfico en la red y al final de su ejecución despliegan reportes que incluyen métricas más complejas como índices de calidad de llamada o video. En este trabajo de tesis se utilizará el generador de tráfico de MikroTik. En contraparte, las técnicas de monitoreo pasivo no inyectan tráfico a la red y utilizan sondas o gestores de monitoreo SNMP para recopilar información. Una herramienta de software para este trabajo puede ser Zabbix.

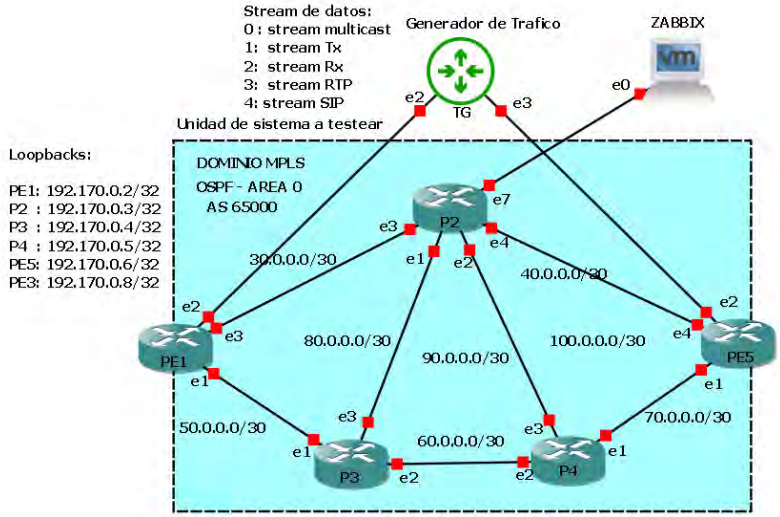


Figura 2.6.1 Monitoreo activo con generador de trafico

Capítulo 3

Descripción y Evaluación de Entornos de Prueba

En este capítulo se describen los procesos de diseño, implementación y simulación de los escenarios de laboratorio. La tabla 3.1.1 muestra una visión general de cada proceso.

3.1 Descripción de los Laboratorios

Tabla 3.1.1 Description de la implementación y Análisis

Diseño	Implementación	Análisis
• La topología de red de los escenarios IP/MPLS. • Preparación de las plantillas de paquete de datos y Stream para el generador de tráfico. • Condiciones Iniciales y restricciones. • Herramientas.	• Configuración de nodos y servidores. • Implementación de los servicios L3VPN y L2VPN sobre el dominio IP/MPLS. • Configuración del generador de tráfico. • Implementación de túneles de ingeniería de tráfico para el trasporte de VPN IP/MPLS. • Simular entornos de rendimiento controlado con NETEM	• Análisis y monitoreo de parámetros de rendimiento. • Análisis del comportamiento de los diferentes Stream de datos, en dominios de IP/MPLS con y sin calidad de servicio.

Para realizar el trabajo de tesis, se describe la zona de estudio, así como los equipos con la que se implementará los diferentes escenarios de laboratorio. Los laboratorios a implementar serán con los equipos de red del laboratorio de Telemática de la Escuela Profesional de Ingeniería Electrónica de la UNSAAC. Con la implementación y diseño de las diferentes topologías se analizará el desempeño de los servicios MPLS VPN que se pongan a prueba. En base a esto se plantea: nodos de borde y políticas de QoS comunes para los servicios MPLS VPN. La topología *backbone* IP/MPLS base será la misma para las L3VPN y L2VPN.

3.2 Diseño de la Topología de Laboratorios

La topología base del core IP/MPLS de los diferentes escenarios de red será como se describe en la Fig. 3.2.1, el dominio IP/MPLS está compuesto por 5 routers de los cuales PE1 y PE5 son equipos de borde que interconecta la parte usuario hacia el core de la red MPLS, estos equipos deben trabajar tanto en el dominio IP a través de protocolos de enrutamiento con el router del cliente, y en el dominio IP/MPLS a través de la conmutación de etiquetas. Mientras tanto los equipos del core IP/MPLS (P2, P3 y P4), conocidos como LSR (Label Switching Router) solo trabajan a través de la conmutación de etiquetas, estos equipos no conocen del tráfico generado por los routers de los clientes.

El conexionado de los enlaces en la topología de la Fig. 3.2.1 refleja varias posibles rutas para el tráfico en la red, los mismos que serán administrados a través de la configuración de túneles de ingeniería de tráfico. La ruta que el protocolo OSPF (Implementado en el core IP/MPLS) generaría para el tráfico seria a través de PE1 – P2 - PE5 (considerando que todos los enlaces tienen las mismas características), mientras tanto que con ingeniería de tráfico de MPLS podemos hacer que el tráfico vaya por la ruta PE1-P3-P4-PE5 (Una ruta subutilizada).

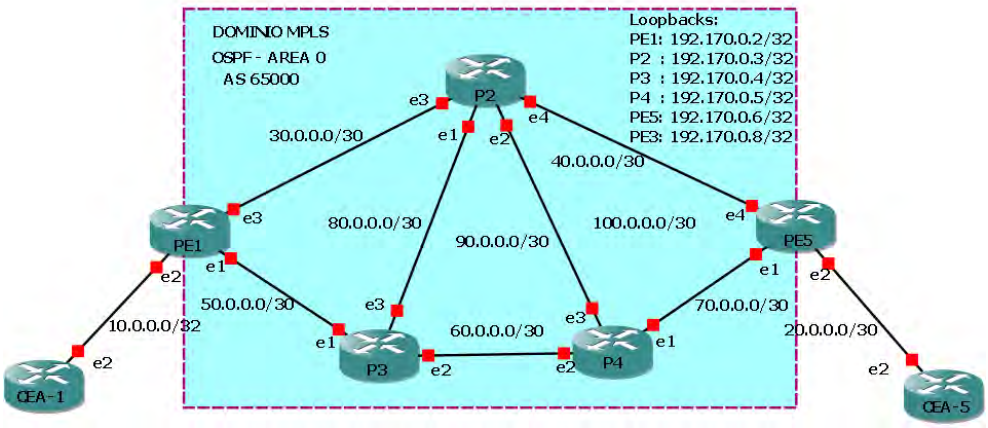


Figura 3.2.1 Topología IP/MPLS base a implementar

Otras consideraciones:

a) Los nodos CEA-1 y CEA-5 pueden ser router o switch según la VPN (L3VPN y L2VPN) a implementar.
b) Capacidad de inyección de tráfico por la herramienta de generación de tráfico de Mikrotik.
c) Capacidad de monitoreo y almacenamiento de métricas.

d) Capacidad de análisis de tráfico para analizar la interacción de los diferentes protocolos de redes.

Los escenarios para tráfico unicast, multicast y telefonía IP poseen las mismas características, los cuales serán generados a través de un generador de tráfico, armando la estructura de paquetes a transmitir, estructurando el stream para cada tipo de paquete La figura 3.3.1 muestra la topología planteada, la Figura 3.3.2 muestra la plantilla de paquetes y el flujo de stream del paquete de datos.

El escenario con aplicaciones reales en este caso servidor Multicast (IPTV) con el software VLC Media Player, servidor PBX con el software Issabel, servidor Iperf3. Los cuales generan los diferentes tipos de tráfico que luego serán consumidos por los clientes (usuarios finales) como un cliente de VLC Media Player (consumo de IPTV), cliente de telefonía IP (softphone de PC o aplicaciones) y cliente de Iperf3. Serán implementados sobre una infraestructura de L3VPN MPLS que serán transportados sobre túneles de ingeniería de tráfico.

3.3 Análisis y Monitoreo

Para el análisis y monitoreo se hará uso de un generador de tráfico, una herramienta de software del sistema operativo de red RouterOS, el cual nos permitirá generar diferentes tipos de tráfico (Multicast, Telefonía IP, Datos Generales). Para el procesamiento de los datos obtenidos del generador de tráfico se hará uso de librerías del lenguaje de programación Python, que nos permitirá generar gráficas que luego podamos analizar y evaluar los diferentes laboratorios implementados.

En una segunda instancia para la implementación con servidores (Multicast, Telefonía IP y Iperf3) se hará uso de la herramienta de software NETEM, el cual nos permitirá generar escenarios de red controlados (configurar, un retardo, Jitter, etc.). Para su análisis y monitoreo se hará uso de herramientas como un script que permita procesar y generar gráficos que el Iperf3 genera.

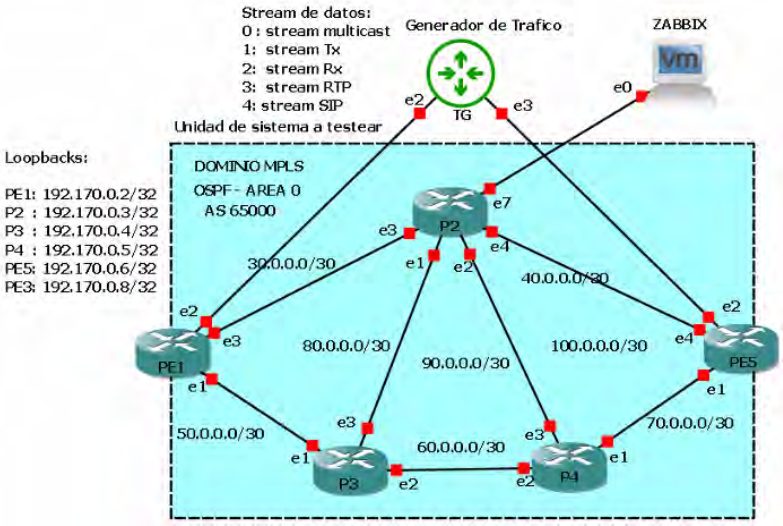


Figura 3.3.1 Topología del escenario IP/MPLS a implementar y monitorear

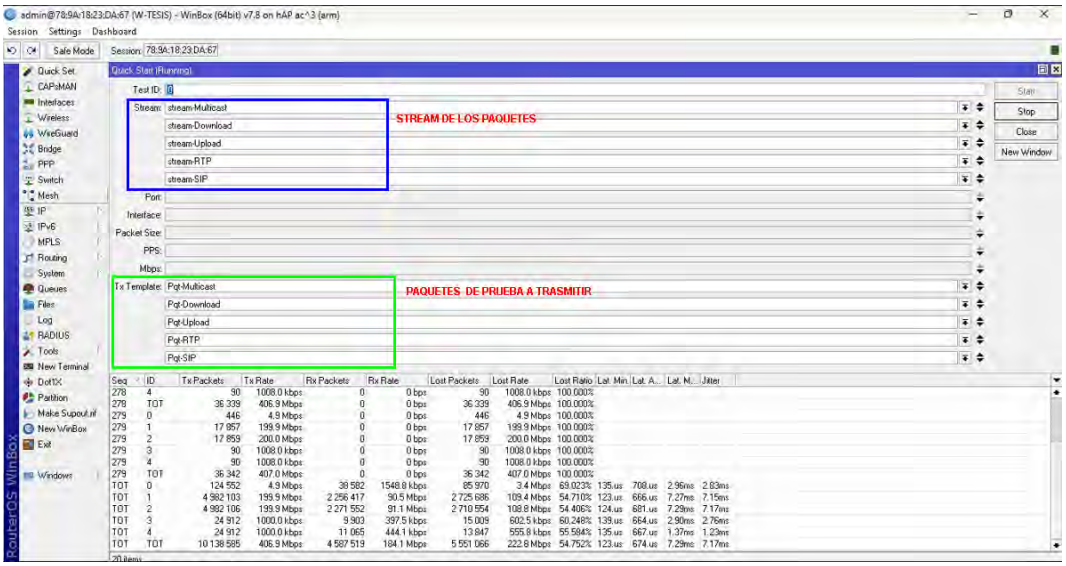


Figura 3.3.2 Generador de trafico de Mikrotik

3.3.1 Métricas de Desempeño

Las métricas utilizadas para comparar el desempeño de los servicios MPLS L2 y L3 son: pérdida de paquetes, retardos, jitter, disponibilidad, ICPIF y MOS.

3.3.2 Condiciones Iniciales

Identifica problemas en cada tipo de tráfico comparando métricas con valores umbrales según estándares internacionales:

- Latencia promedio > 150 ms
- Jitter promedio > 30 ms

- Pérdida de paquetes > 1%
- MOS < 3.5
- ICPIF > 20

3.4 Implementación

3.4.1 Recursos y Herramientas

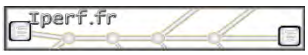
Para desplegar los escenarios se utilizan enrutadores Mikrotik con sistema operativo RouterOS versión 7.19. La herramienta para el análisis de tráfico a usar será Wireshark. La herramienta para generar tráfico unicast, multicast y telefonía IP, será a través de la herramienta generadora de tráfico de Mikrotik. Uso del software NETEM que funciona bajo en sistema operativo Linux, que nos permitirá simular entornos de red controlados pudiendo configurar retardos, jitter, pérdida de paquetes.

Tabla 3.4.1 Características de los Software

Aplicación	Herramienta
Sistema Operativo de Red	RouterOS
Generación de tráfico	Generador de tráfico Mikrotik
Procesamiento de datos	Script de Python
Análisis de tráfico	Software Wireshark
Entornos controlados	Software NETEM
Monitoreo de Métricas	Generador de tráfico Mikrotik, script de Python.
Implantación de aplicaciones reales: IPTV, Telefonía IP y otros tráficos.	• Software VLC Media Player. • Issabel PBX y Softphone. • Generador de tráfico de Mikrotik. • Iperf3 • NETEM

Tabla 3.4.2 Aplicaciones de la Implementación

Equipos	Descripcion	Referencia
MikroTik CCR2004-16G-2S+	• Procesador- AL32400 de 4 núcleos a 1.7GHz • Arquitectura ARM 64 bits • 16GB de RAM • Licencia RouterOS 6 • Sistema operativo RouterOS (v7.19.3) • Almacenamiento 128 MB • 16 Puertos Ethernet 10/100/1000	

	• https://mikrotik.com/product/ccr2004_16g_2splus	
CSS326-24G-2S+RM	• Switch Chip Model: 98DX3216 • Sistema operativo RouterOS (v7.12) • Almacenamiento 2 MB • 24 Puertos Ethernet 10/100/1000 • https://mikrotik.com/product/CSS326-24G-2SplusRM	
hAP ax³	• Procesador- IPQ-6010 de 4 núcleos auto (864 - 1800) MHz • Arquitectura ARM 64 bits • 1GB de RAM • Licencia RouterOS 6 • Sistema operativo RouterOS (v7.8) • Almacenamiento 128 MB • Wireless 2.4 GHz standards: 802.11b/g/n/ax • 5 Puertos Ethernet 10/100/1000 • https://mikrotik.com/product/hap_ax3	
Servidor Multicast	• VLC Media Player: https://www.videolan.org/ • Sistema Operativo: Ubuntu Server 24.04: https://ubuntu.com/download/server • VMWare WorkStation 17: https://www.vmware.com/	
Servidor PBX	• Issabel PBX: https://www.issabel.org/ • Rocky Linux: https://rockylinux.org/es-ES/download • VMWare WorkStation 17: https://www.vmware.com/	
Servidor y Cliente Iperf3	• Iperf3: https://iperf.fr/	
Clientes Telefonia IP	• Softphone: linphone (Instalado en Pc y App en Android): https://www.linphone.org/en/linphone-softphone/ • Sistema Operativo Parrot Security OS: https://www.parrotsec.org/ • Oracle VirtualBox: https://www.virtualbox.org/	
Clientes Multicast	• VLC Media Player (Instalado en Pc y App en Android): https://www.videolan.org/ • Sistema Operativo Parrot Security OS: https://www.parrotsec.org/ • Oracle VirtualBox: https://www.virtualbox.org/	

3.4.2 Restricciones

El rendimiento de los router Mikrotik, no cuenta con todas las características para poder implementar ingeniería de tráfico. La implementación a nivel simulación con el software GNS3 tiene muchas limitaciones para casos de uso en tiempo real, la imagen del sistema operativo RouterOS tiene limitaciones a 1 Mbps en ancho de banda. La implementación de la solución será a nivel de laboratorio con los equipos que están ubicados en el laboratorio de Telemática de escuela profesional de Ingeniería Electrónica. Los servidores de IPTV, Telefonía IP serán a través de máquinas virtuales implementados bajo un laptop que será anfitrión de estas máquinas virtuales.

3.4.3 Equipos Router Mikrotik Modelo CCR2004-16G-2S+

Este router tiene 16 puertos Giga Ethernet y dos puertos SFP+ de 10 G, tiene una carcasa blanca de montaje en rack de 1U. Cuenta con un procesador de 4 núcleos modelo ARMv8-A-Cortex-A57 de 64 bits que funciona a 1.7 GHz. Su capacidad de este equipo permite su implementación en pequeñas y medianas empresas.

Tabla 3.4.3 Características del Router [13]

Detalle	Característica
Código de producto	CCR2004-16G-2S+
Arquitectura	ARM 64 bit
CPU	AL 32400
Recuento de núcleos de CPU	4
Frecuencia nominal de la CPU	1700 MHz
Cambiar modelo de chip	88E6191X
Dimensiones	443 x 210 x 44 mm
Licencia de RouterOS	6
Sistema operativo	RouterOS v7
Tamaño de la RAM	4 GB
Tamaño de almacenamiento	128 MB
Tipo de almacén	NAND
MTBF	Aproximadamente 200.000 horas a 25C
Temperatura ambiente probada	De -20 °C a 60 °C
Aceleración de hardware IPsec	Sí

3.4.4 Herramientas de Análisis de Trafico

Wireshark es una herramienta grafica de análisis de paquetes, T-shark es su version de línea de comandos, tcpdump es una herramienta de línea de comandos tradicional y SolarWinds Network Traffic Analyzer es una solución comercial completa y más avanzada. Wireshark y T-shark son gratis, mientras que SolarWinds es de pago. T-shark y tcpdump usan la sintaxis de filtros de Berkely, mientras que Wireshark tiene su propio filtro de visualización.

Tabla 3.4.4 Comparativa de analizadores de trafico

Característica	**Wireshark**	**tcpdump**	**t-shark**	**SolarWinds Network Traffic Analyzer**
Interfaz	Gráfica (GUI) y de línea de comandos	Solo línea de comandos (CLI)	Solo línea de comandos (CLI)	Gráfica y de línea de comandos
Uso principal	Análisis detallado y diagnóstico de problemas de red, auditorías de seguridad	Captura de paquetes en entornos sin GUI	Análisis de paquetes en línea de comandos.	Monitoreo de tráfico de red, análisis de rendimiento y seguridad.
Tipos de filtros	Sintaxis de filtros de visualización de Wireshark	Filtros de captura al estilo BPF (Berkeley Packet Filter)	Sintaxis de filtros de visualización de Wireshark y de captura BPF	Filtros de captura y análisis, con GUI para la configuración
Capacidad de análisis	Desglose de protocolos y contenido de paquetes muy detallado	Más limitado en el análisis detallado de paquetes	Similar a Wireshark, pero en formato de línea de comandos	Ofrece análisis de tráfico de alto nivel, monitoreo de ancho de banda
Licencia	Gratuito y de código abierto	Gratuito	Gratuito (se puede instalar de forma independiente o junto a Wireshark)	Comercial, con licencia de pago

3.4.5 Análisis y Captura de Paquetes con Wireshark

Wireshark es una herramienta de software que nos permite capturar paquetes que viajan a través de una red (IP/MPLS en nuestro caso), estas capturas nos muestran la disgregación de los diferentes protocolos por capas según el modelo TCP/IP. Nos permitirá analizar como los protocolos que participan en la implementación de nuestras topologías interactúan entre ellos (por ejemplo, como el paquete IP es encapsulado por MPLS). A través de la red pasaremos tráficos como Telefonía IP, Multicast (IPTV) y datos generales, Wireshark nos permitirá analizar de manera muy granular según el tipo el tipo de tráfico que uno quiere analizar o capturar. También nos permitirá ver estadísticas, gráficas, la jerarquía de protocolos de nuestras implementaciones.

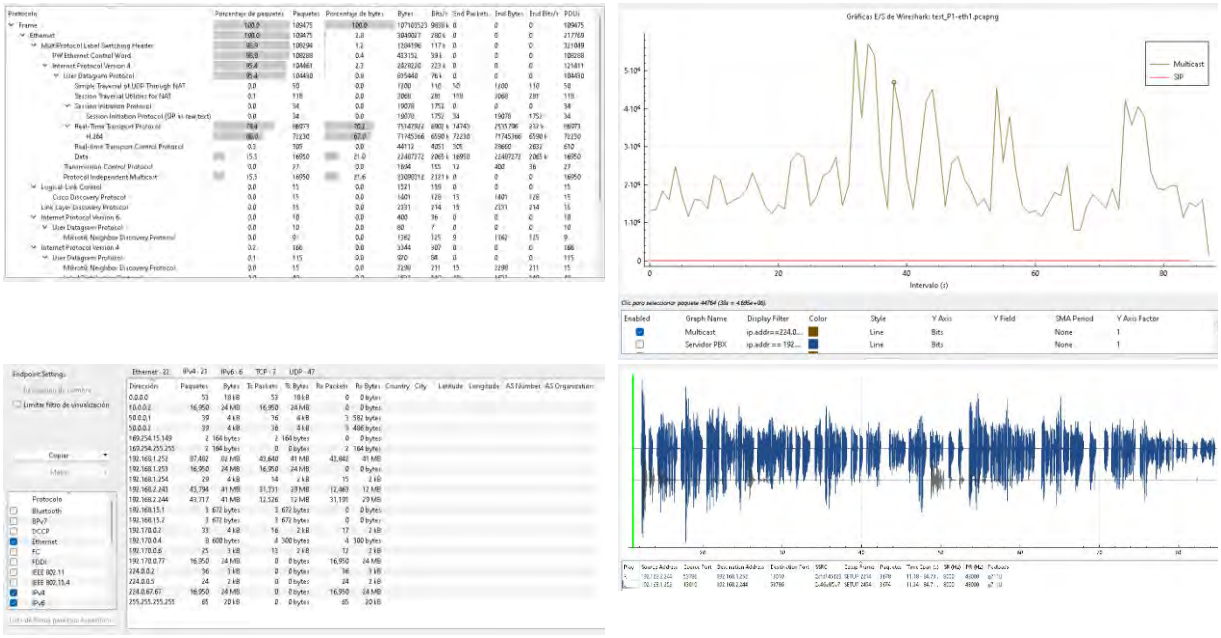


Figura 3.4.1 Captura de Paquetes con Wireshark

3.4.6 Simulación de Entornos Controlados con NETEM

NETEM nos permitirá simular entornos con escenarios controlados, que nos permitan configurar retardos, jitter, pérdida de paquetes, etc. y así poder evaluar como es el comportamiento de nuestra red evaluando el rendimiento de nuestras aplicaciones bajo diferentes condiciones creadas con NETEM. Es una herramienta de línea de comandos integrada en el Kernel de Linux para simular (retardos, pérdida de paquetes, duplicaciones, etc). [14]

sudo tc qdisc add dev enp7s0 root netem delay 250 ms

El comando agrega 250 ms de retraso a los paquetes que salen de la interfaz: enp7s0

3.4.7 Medir el Rendimiento de Ancho de Banda de Red con Iperf3

Iperf3 es una herramienta cliente servidor que nos permite medir el throughput de nuestra red. Es una aplicación de código abierto, multiplataforma que se usa para medir el throughput entre dos dispositivos. La salida que nos generará Iperf3 estará en formato JSON en cual lo procesaremos, e interpretaremos sus resultados.

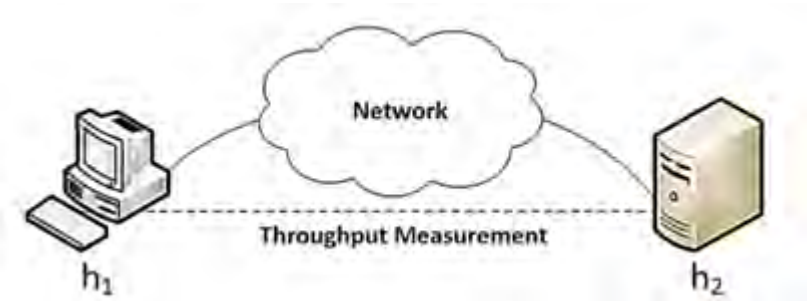


Figura 3.4.2 Medición del throughput con Iperf3 [14]

3.4.8 Generación de Tráfico con Mikrotik.

El generador de tráfico es una herramienta que nos permite evaluar el rendimiento de DUT (Device Under Test) o SUT (Sistema bajo test). El generador puede generar y enviar paquetes sobre puertos específicos. Esto permite registrar valores latencia, jitter, tasas de transmisión y recepción de paquetes, registrar la pérdida de paquetes. [15]

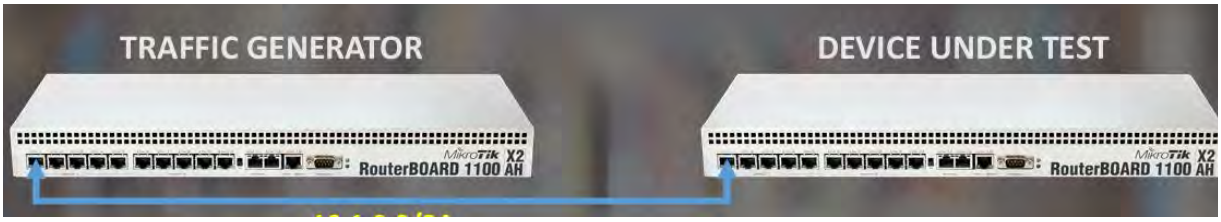


Figura 3.4.3 Simple Generador de trafico [15]

3.4.9 ITU-T Y.1564 - Ethernet Service Activation Test

Estándar de la ITU (International Telecomunicación Union) diseñado específicamente para validar servicios Ethernet y SLAs (Service Level Agreements) en redes de producción.

Fases de Prueba

Fase 1: Prueba de Configuración

- Duración mínima: 15 minutos
- Duración recomendada: 2-4 horas
- Objetivo: Verificar que cada servicio cumple con sus parámetros de SLA individuales
- Características:
    - Prueba cada servicio de manera independiente
    - Mide Frame Loss Ratio (FLR)
    - Mide Frame Transfer Delay (FTD)
    - Mide Frame Delay Variation (FDV - Jitter)

Parámetros medidos por servicio:

- Throughput: Capacidad real vs comprometida
- Latencia: Delay unidireccional y bidireccional
- Jitter: Variación del delay
- Pérdida de frames: Porcentaje de frames perdidos

Fase 2: Prueba de Rendimiento

- Duración mínima: 15-30 minutos
- Duración recomendada: 2-24 horas
- Objetivo: Validar que todos los servicios funcionan correctamente de manera simultánea bajo carga sostenida
- Características:
    - Todos los servicios se prueban simultáneamente
    - Simula condiciones reales de operación
    - Valida que no hay interferencia entre servicios
    - Prueba la estabilidad a largo plazo

Escenarios típicos:

- Mezcla de tipos de tráfico (datos, voz, video)
- Diferentes tamaños de frame

Ventajas sobre RFC 2544

- Multiservicio: Prueba múltiples servicios simultáneamente
- QoS: Valida diferentes clases de servicio
- No disruptivo: Puede ejecutarse en redes de producción
- Orientado a SLA: Mide parámetros contractuales específicos
- Tráfico realista: Simula patrones de tráfico más cercanos a la realidad

Métricas de Y.1564

FLR (Frame Loss Ratio)

- Porcentaje aceptable de pérdida de frames
- Típicamente < 0.01% para servicios críticos
- < 0.1% para servicios estándar

FTD (Frame Transfer Delay)

- Latencia máxima permitida
- Crítico para aplicaciones en tiempo real
- Típicamente < 10ms para enlaces metropolitanos

FDV (Frame Delay Variation - Jitter)

- Variación aceptable en la latencia
- Crítico para VoIP y videoconferencia
- Típicamente < 1ms para voz

Casos de Uso

Servicios de Voz (VoIP)

Requisitos especiales Duración de pruebas

- Latencia <150ms (ITU-T G.114)
- Jitter <30ms
- Pérdida de paquetes <1%
- MOS score >4.0
- Pruebas de calidad: 30 minutos mínimo
- Llamadas de prueba: 100+ llamadas
- Duración por llamada: 2-5 minutos

Video Streaming

Requisitos especiales y Duración de pruebas

- Throughput sostenido
- Baja variabilidad
- Soporte para multicast
- Streaming continuo: 2-4 horas
- Cambio de canal: 1 hora (múltiples cambios)
- Calidad de imagen: Evaluación subjetiva + objetiva

Consideraciones de Seguridad

Pruebas en Entornos de Producción Precauciones

- Usar Y.1564 en lugar de RFC 2544
- Limitar tráfico de prueba
- Horarios de bajo tráfico

- Notificar a stakeholders

Generación de Tráfico Riesgos y Mitigaciones

- Puede parecer ataque DDoS
- Activar sistemas de seguridad
- Consumir ancho de banda crítico
- Coordinar con equipo de seguridad
- Whitelist de IPs de prueba
- Patrones de tráfico identificables
- Monitoreo paralelo

Tabla 3.4.5 Resumen de tiempos recomendadas para una prueba

Tipo de Prueba	**Mínimo**	**Recomendado**	**Óptimo**
RFC 2544 Throughput	60s	5 min	10 min
RFC 2544 Latency	120s	5 min	10 min
Y.1564 Fase 1	**15 min**	**1-2 hr**	**2-4 hr**
Y.1564 Fase 2	**15 min**	**2-4 hr**	**24 hr**
Burn-in Testing	24 hr	48 hr	72 hr
Service Acceptance	2 hr	4 hr	8 hr
Troubleshooting	30s	15 min	1 hr

3.4.10 Implementación de un Sistema de Telefonía IP con Issabel.

Se hará uso del Software Issabel como servidor PBX y Linphone como cliente softphone SIP. Se usará un servidor basado en Linux para el software Issabel y dispositivo cliente (PC o móvil) con Linphone. Se configuró un sistema de telefonía IP funcional, escalable y listo para su uso en la red implementada en esta tesis de grado.

Figura 3.4.4 Telefonía IP

3.4.11 Implementación de un Sistema Multicast (IPTV) con VLC Media Player.

Aquí se configurará un equipo emisor, para enviar el contenido multimedia a una dirección multicast. Esto permite que múltiples clientes se unan al stream sin necesidad de conexiones individuales.

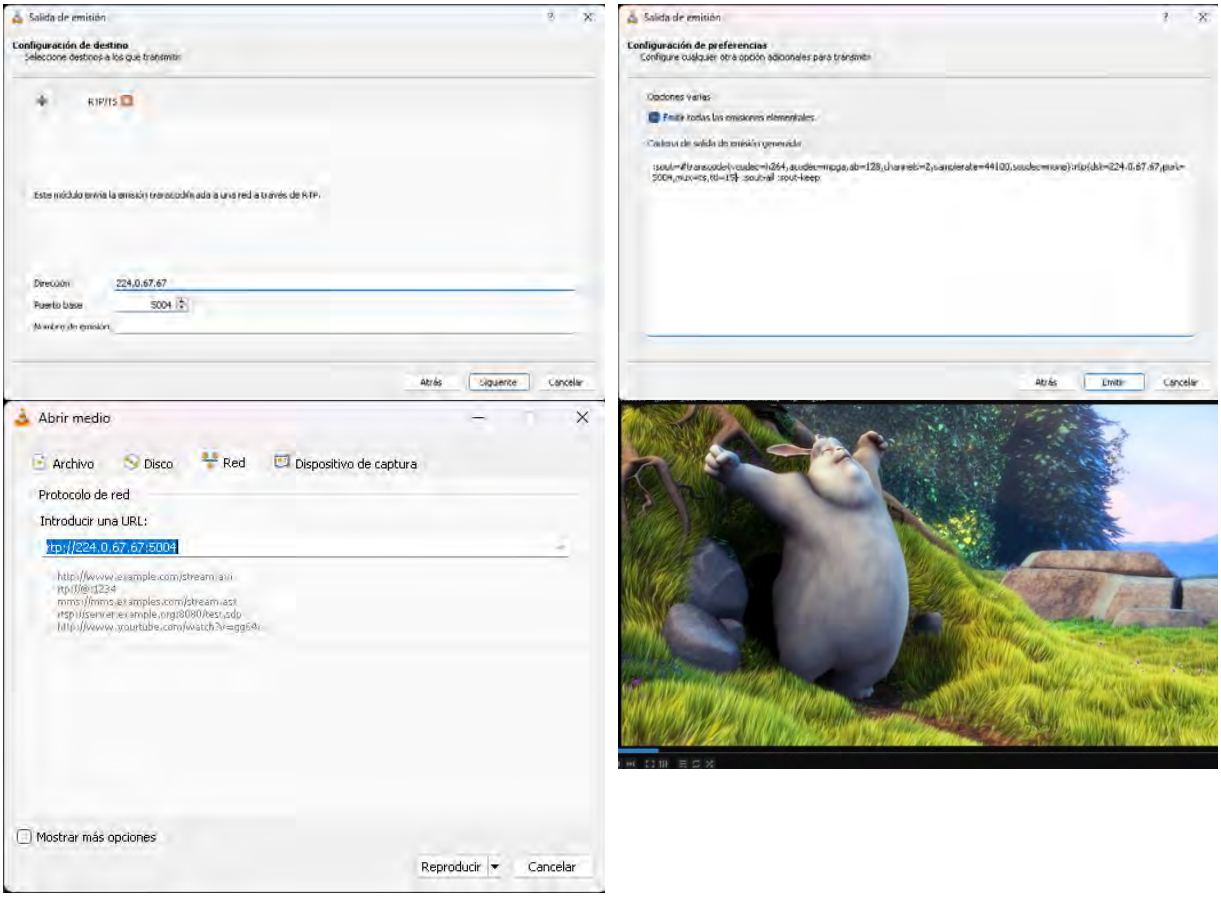


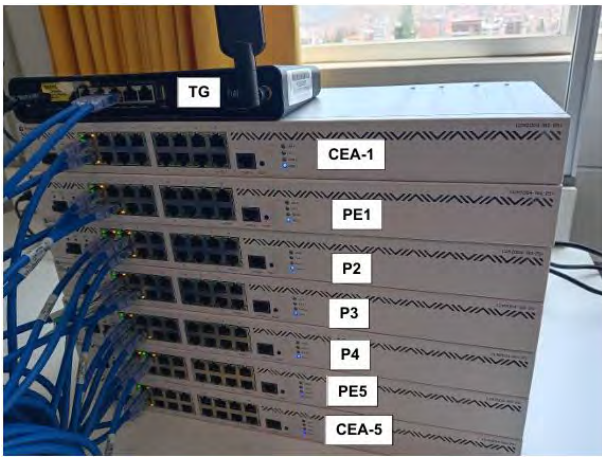
Figura 3.4.5 IPTV con VLC media Player

Capítulo 4

Implementación y Configuración de Routers Mikrotik

4.1 Implementación de una Red IP/MPLS

a) Laboratorio de Telemática



b) Router Mikrotik

Figura 4.1.1 Equipos Mikrotik a configurar

Configurar IP/MPLS en RouterOS v7 para la topología implementada implica establecer una red MPLS básica sobre IP, utilizando OSPF como protocolo de enrutamiento interior (IGP) y LDP para la distribución de etiquetas. Esto permite el transporte eficiente de tráfico IP a través del dominio MPLS (PE1, PE3, PE5 como routers de borde, y P2, P3, P4 como routers de tránsito). A continuación, se detalla los pasos genéricos, sin especificar IPs explícitamente para mantener flexibilidad ya que se adjuntará la configuración de todos los equipos en los anexos del presente trabajo.

4.1.1 Recursos Utilizados en la Implementación

- En el laboratorio de Telemática se cuenta con equipos MikroTik modelo **CCR2004-16G-2S+** que cuentan con el sistema operativo de red RouterOS v7. El mismo soporta los requerimientos para implementar IP/MPLS.
- Conectividad física y asignación de direcciones IP en las interfaces según la tabla 4.1.1 de direcciones IP.
- Acceso administrativo a todos los routers (PE1, PE3, PE5, P2, P3, P4), a través de la aplicación WinBox de MikroTik.

4.1.2 Topología de Red IP/MPLS en RouterOS v7

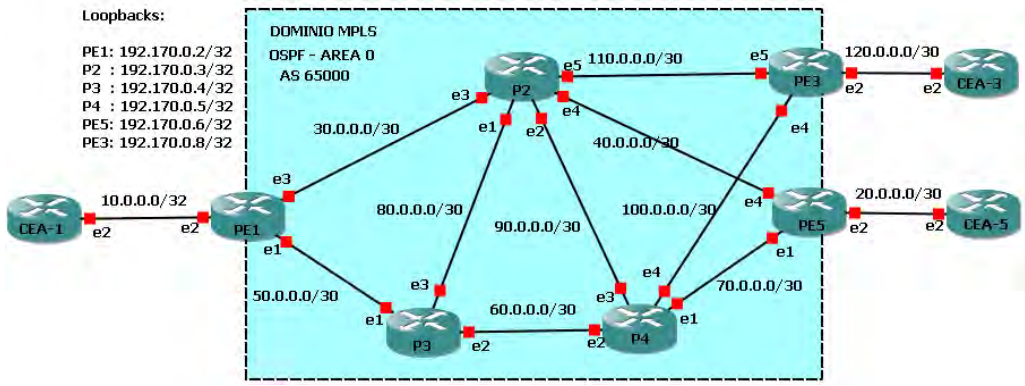


Figura 4.1.2 Dominio IP/MPLS Implementado

4.1.3 Asignación de Direcciones IP en la red

Tabla 4.1.1 Direcciones IP de la topología IP/MPLS

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway
PE1	Ether1	30.0.0.1	255.255.255.252	-
	Ether2	10.0.0.1	255.255.255.252	-
	Ether3	50.0.0.1	255.255.255.252	-
	Loopback 0	192.170.0.2	255.255.255.255	-
P2	Ether1	80.0.0.1	255.255.255.252	-
	Ether2	90.0.0.1	255.255.255.252	-
	Ether3	30.0.0.2	255.255.255.252	-
	Ether4	40.0.0.1	255.255.255.252	-
	Ether5	110.0.0.1	255.255.255.252	-
	LoopBack 0	192.170.0.3	255.255.255.255	-
P3	Ether1	50.0.0.2	255.255.255.252	-
	Ether2	60.0.0.1	255.255.255.252	-
	Ether3	80.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.4	255.255.255.255	-
P4	Ether1	70.0.0.1	255.255.255.252	-
	Ether2	60.0.0.2	255.255.255.252	-
	Ether3	90.0.0.2	255.255.255.252	-
	Ether4	100.0.0.1	255.255.255.252	-
	LoopBack 0	192.170.0.5	255.255.255.255	-
PE5	Ether1	70.0.0.2	255.255.255.252	-
	Ether2	20.0.0.1	255.255.255.252	-
	Ether4	40.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.6	255.255.255.255	-
PE3	Ether2	120.0.0.1	255.255.255.252	-
	Ether4	110.0.0.1	255.255.255.252	-
	Ether5	100.0.0.1	255.255.255.252	-
	LoopBack 0	192.170.0.8	255.255.255.255	-

4.1.4 Protocolos Configurados en IP/MPLS

La topología de red con IP/MPLS necesitará diferentes protocolos de red para su funcionamiento los cuales se listan en la tabla 4.1.2.

Tabla 4.1.2 Protocolos configurados en la topología IP/MPLS

Configuración\Equipo	PE1	P2	P3	P4	PE5
Interfaz LoopBack	✓	✓	✓	✓	✓
Interfaces Fisicas	✓	✓	✓	✓	✓
OSPF	✓	✓	✓	✓	✓
MPLS	✓	✓	✓	✓	✓

Los comandos para configurar los diferentes equipos en la red son similares solo variando en valores específicos que se le asigna a cada router de la topología IP/MPLS, en esta sección generamos las plantillas para cada configuración necesaria, en los anexos de este trabajo de tesis se adjuntan las configuraciones de todo los routers para la topología IP/MPLS.

4.1.4.1 Configuración de las Interfaces y Direcciones IP

Asigna direcciones IP a las interfaces de core (entre PEs y Ps) y loopbacks en todos los routers según la tabla 4.1 de direcciones IP.

```
/ip address
add address=<loopback-ip> interface=loopback
add address=<mpls-link-ip1> interface=<core-interface1>
add address=<mpls-link-ip2> interface=<core-interface2>
```

Plantilla de configuración de direcciones IP sobre las interfaces de red IP/MPLS

4.1.4.2 Configuración de OSPF como IGP

El protocolo de enrutamiento OSPF será utilizado para el enrutamiento dentro de la red MPLS, es decir se configurará en los routers PE1, P2, P3, P4, PE3 y PE5. Este nos permitirá interconectar los routers del dominio MPLS para que se puedan formar los LSP (Label Switching Path) que serán usados para transportar los datos a través de la conmutación de etiquetas, también nos permitirá configurar los túneles de ingeniería de tráfico que transporta las VPN de capa 2 y 3 que se implementara en capítulos posteriores.

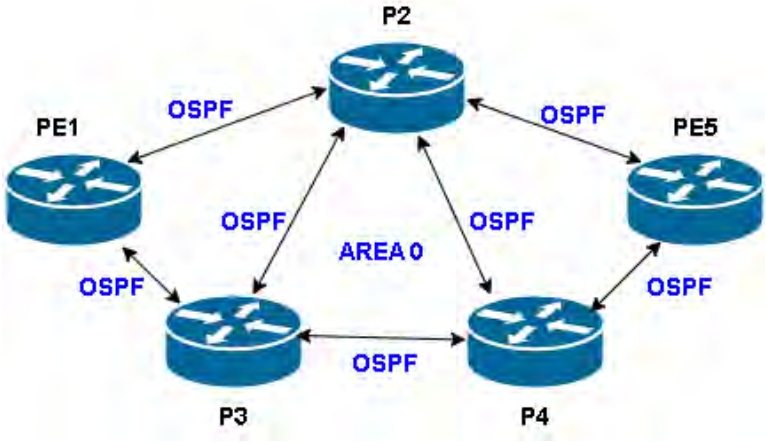


Figura 4.1.3 Protocolo OSPF en el core IP/MPLS

```
/routing ospf instance
add name=ospf-instance router-id=<loopback-ip> distribute-default=never
/routing ospf area
add name=backbone instance=ospf-instance
/routing ospf interface
add interface=<core-interface1> network-type=point-to-point area=backbone
add interface=<core-interface2> network-type=point-to-point area=backbone
add interface=loopback network-type=point-to-point area=backbone passive=yes
```

Plantilla Genérica para la configuración del protocolo OSPF sobre el dominio IP/MPLS

```
[admin@P2] > routing/ospf/neighbor/print
Flags: V - virtual; D - dynamic
 0  D instance=ospf-instance-1 area=ospf-area-1 address=80.0.0.2
      router-id=192.170.0.4 state="Full" state-changes=6 adjacency=1m23s
      timeout=32s

 1  D instance=ospf-instance-1 area=ospf-area-1 address=90.0.0.2
      router-id=192.170.0.5 state="Full" state-changes=5 adjacency=1m13s
      timeout=39s

 2  D instance=ospf-instance-1 area=ospf-area-1 address=30.0.0.1
      router-id=192.170.0.2 state="Full" state-changes=6 adjacency=1m23s
      timeout=39s

 3  D instance=ospf-instance-1 area=ospf-area-1 address=40.0.0.2
      router-id=192.170.0.6 state="Full" state-changes=6 adjacency=1m13s
      timeout=31s
[admin@P2] >
```

Figura 4.1.4 Verificación de la conectividad OSPF

4.1.4.3 Habilitar MPLS y el Protocolo LDP

La configuración de MPLS se realizará en todos los routers que pertenecen al dominio IP/MPLS (PE1, P2, P3, P4, PE3, PE5); en los routers de borde (PE1, PE3 y PE5) se configura en las interfaces con vista al dominio IP/MPLS. El protocolo nos permitirá distribuir las etiquetas

y así poder formar los LSP (Label Switching Path), que son los túneles preestablecidos, que usará MPLS para transportar los datos a través de la conmutación de etiquetas.

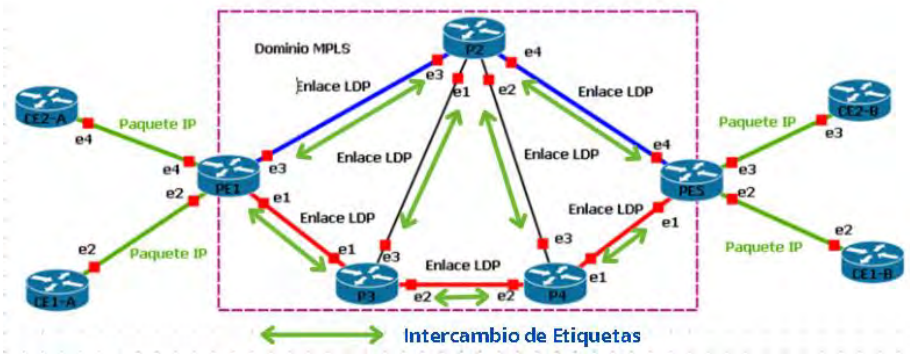


Figura 4.1.5 MPLS y LDP en las interfaces de los routers del dominio IP/MPLS

```
/mpls
set enabled=yes
/mpls ldp
set enabled=yes lsr-id=<loopback-ip> transport-address=<loopback-ip>
/mpls ldp interface
add interface=<core-interface1>
add interface=<core-interface2>
```

Plantilla para habilitar MPLS y LDP en las interfaces de red

4.1.4.4 Verificar las Configuraciones

Estos comandos nos permitirán verificar que LDP esté funcionando y las etiquetas se distribuyan correctamente.

```
[admin@PE1] > mpls/ldp neighbor/print
Flags: D - DYNAMIC; O - OPERATIONAL; t - SENDING-TARGETED-HELLO; v - VPLS; p - PASSIVE
Columns: TRANSPORT, LOCAL-TRANSPORT, PEER, ADDRESSES
#       TRANSPORT     LOCAL-TRANSPORT  PEER            ADDRESSES
0 DOtvp 192.170.0.6   192.170.0.2      192.170.0.6:0   40.0.0.2
                                                       70.0.0.2
                                                       192.168.10.2
                                                       192.170.0.6
1 DO  p 192.170.0.3   192.170.0.2      192.170.0.3:0   30.0.0.2
                                                       40.0.0.1
                                                       80.0.0.1
                                                       90.0.0.1
                                                       192.168.137.8
                                                       192.170.0.3
2 DO  p 192.170.0.4   192.170.0.2      192.170.0.4:0   50.0.0.2
                                                       60.0.0.1
                                                       80.0.0.2
                                                       192.170.0.4
```

a) */mpls ldp neighbor print*

```
[admin@PE1] > mpls forwarding-table/print
Flags: L - LDP, P - VPN, V - VPLS
Columns: LABEL, VRF, PREFIX, NEXTHOPS, VPLS
 #   LABEL  VRF       PREFIX         NEXTHOPS                                                  VPLS
 0 P  1001  VRF-CE2
 1 P  1002  VRF-CE1
 2 L  1003  main      40.0.0.0/30    { label=impl-null; nh=30.0.0.2; interface=ether3 }
 3 L  1004  main      80.0.0.0/30    { label=impl-null; nh=50.0.0.2; interface=ether1 }
                                     { label=impl-null; nh=30.0.0.2; interface=ether3 }
 4 L  1005  main      90.0.0.0/30    { label=impl-null; nh=30.0.0.2; interface=ether3 }
 5 L  1006  main      192.170.0.3    { label=impl-null; nh=30.0.0.2; interface=ether3 }
 6 L  1007  main      192.170.0.6    { label=impl-null; nh=192.168.10.2; interface=vpls15 }
 7 L  1008  main      70.0.0.0/30    { label=6002; nh=50.0.0.2; interface=ether1 }
                                     { label=3002; nh=30.0.0.2; interface=ether3 }
 8 V  1000                                                                                    vpls15
 9 L  1011  main      192.170.0.5    { label=6006; nh=50.0.0.2; interface=ether1 }
                                     { label=3007; nh=30.0.0.2; interface=ether3 }
10 L  1009  main      192.170.0.4    { label=impl-null; nh=50.0.0.2; interface=ether1 }
11 L  1010  main      60.0.0.0/30    { label=impl-null; nh=50.0.0.2; interface=ether1 }
[admin@PE1] >
```

b) */mpls forwarding-table print*

Figura 4.1.6 Verificar la configuración de MPLS

```
[admin@PE1] > ip route/print
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, s - STATIC, o - OSPF; + - ECMP
Columns: DST-ADDRESS, GATEWAY, ROUTING-TABLE, DISTANCE
#      DST-ADDRESS       GATEWAY           ROUTING-TABLE  DISTANCE
  DAc  192.168.10.0/24   vpls15            main                  0
  DAc  30.0.0.0/30       ether3            main                  0
  DAo  40.0.0.0/30       30.0.0.2%ether3   main                110
  DAc  50.0.0.0/30       ether1            main                  0
  DAo  60.0.0.0/30       50.0.0.2%ether1   main                110
  DAo+ 70.0.0.0/30       50.0.0.2%ether1   main                110
  DAo+ 70.0.0.0/30       30.0.0.2%ether3   main                110
  DAo+ 80.0.0.0/30       50.0.0.2%ether1   main                110
  DAo+ 80.0.0.0/30       30.0.0.2%ether3   main                110
  DAo  90.0.0.0/30       30.0.0.2%ether3   main                110
  DAc  192.170.0.2/32    lo                main                  0
  DAo  192.170.0.3/32    30.0.0.2%ether3   main                110
  DAo  192.170.0.4/32    50.0.0.2%ether1   main                110
  DAo+ 192.170.0.5/32    50.0.0.2%ether1   main                110
  DAo+ 192.170.0.5/32    30.0.0.2%ether3   main                110
0  As  192.170.0.6/32    192.168.10.2      main                  1
  D o  192.170.0.6/32    30.0.0.2%ether3   main                110
  DAc  10.0.0.0/30       ether2@VRF-CE1    VRF-CE1               0
  DAc  10.0.2.0/30       ether4@VRF-CE2    VRF-CE2               0
  DAc  192.170.0.11/32   loop@VRF-CE2      VRF-CE2               0
[admin@PE1] >
```

a) */ip route print*

```
[admin@PE1] > ip route/print where ospf
Flags: D - DYNAMIC; A - ACTIVE; o - OSPF; + - ECMP
Columns: DST-ADDRESS, GATEWAY, ROUTING-TABLE, DISTANCE
    DST-ADDRESS       GATEWAY           ROUTING-TABLE  DISTANCE
DAo  40.0.0.0/30      30.0.0.2%ether3   main                110
DAo  60.0.0.0/30      50.0.0.2%ether1   main                110
DAo+ 70.0.0.0/30      50.0.0.2%ether1   main                110
DAo+ 70.0.0.0/30      30.0.0.2%ether3   main                110
DAo+ 80.0.0.0/30      50.0.0.2%ether1   main                110
DAo+ 80.0.0.0/30      30.0.0.2%ether3   main                110
DAo  90.0.0.0/30      30.0.0.2%ether3   main                110
DAo  192.170.0.3/32   30.0.0.2%ether3   main                110
DAo  192.170.0.4/32   50.0.0.2%ether1   main                110
DAo+ 192.170.0.5/32   50.0.0.2%ether1   main                110
DAo+ 192.170.0.5/32   30.0.0.2%ether3   main                110
D o  192.170.0.6/32   30.0.0.2%ether3   main                110
[admin@PE1] >
```

b) */ip route print where ospf*

Figura 4.1.7 Verificar el enrutamiento OSPF

```
[admin@PE1] > interface/monitor-traffic interface=ether3
                          name:    ether3
       rx-packets-per-second:         7
          rx-bits-per-second:   6.6kbps
    fp-rx-packets-per-second:         6
       fp-rx-bits-per-second:   5.9kbps
         rx-drops-per-second:         0
        rx-errors-per-second:         0
       tx-packets-per-second:        11
          tx-bits-per-second:  19.8kbps
    fp-tx-packets-per-second:         0
       fp-tx-bits-per-second:      0bps
         tx-drops-per-second:         0
   tx-queue-drops-per-second:         0
        tx-errors-per-second:         0
-- [Q quit|D dump|C-z pause]
```

a) *interface/monitor-traffic interface=ether3*

Figura 4.1.8 Monitorear el tráfico MPLS

Consideraciones

- Topología: Todas las interfaces de core son configuradas con OSPF y MPLS. Los routers P (P2, P3, P4) solo necesitan OSPF y MPLS, mientras que los PEs (PE1, PE3, PE5) pueden incluir VRFs por cada cliente CE dependiendo del servicio implementado.
- Escalabilidad: En un despliegue de L3VPN y L2VPN en capítulos posteriores usaremos BGP entre PEs para poder escalar nuestra implementación.
- Pruebas: Se realizó a través del comando ping entre las direcciones IPs de las interfaces loopbacks de PEs (PE1 a PE5) que nos permite enviar paquetes ICMP para confirmar la conectividad MPLS.

```
[admin@PE1] > ping 192.170.0.6 src-address=192.170.0.2
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 192.170.0.6                                56  64 10ms744us
    1 192.170.0.6                                56  64 14ms761us
    2 192.170.0.6                                56  64 11ms53us
    3 192.170.0.6                                56  64 12ms305us
    4 192.170.0.6                                56  64 15ms915us
    5 192.170.0.6                                56  64 15ms969us
    6 192.170.0.6                                56  64 4ms7us
    7 192.170.0.6                                56  64 13ms337us
    8 192.170.0.6                                56  64 11ms611us
    sent=9 received=9 packet-loss=0% min-rtt=4ms7us avg-rtt=12ms189us max-rtt=15ms969us
```

Figura 4.1.9 Conectividad entre PE1 y PE5

- Tráfico IP desde PE1 a PE5 será encapsulado a través de LSP (Label Switching Path) de MPLS, usando etiquetas distribuidas por LDP y rutas calculadas por OSPF.
- Los routers P (P2, P3, P4) actúan como tránsito, intercambiando etiquetas (operación de SWAP).

4.2 Implementación de L3VPN

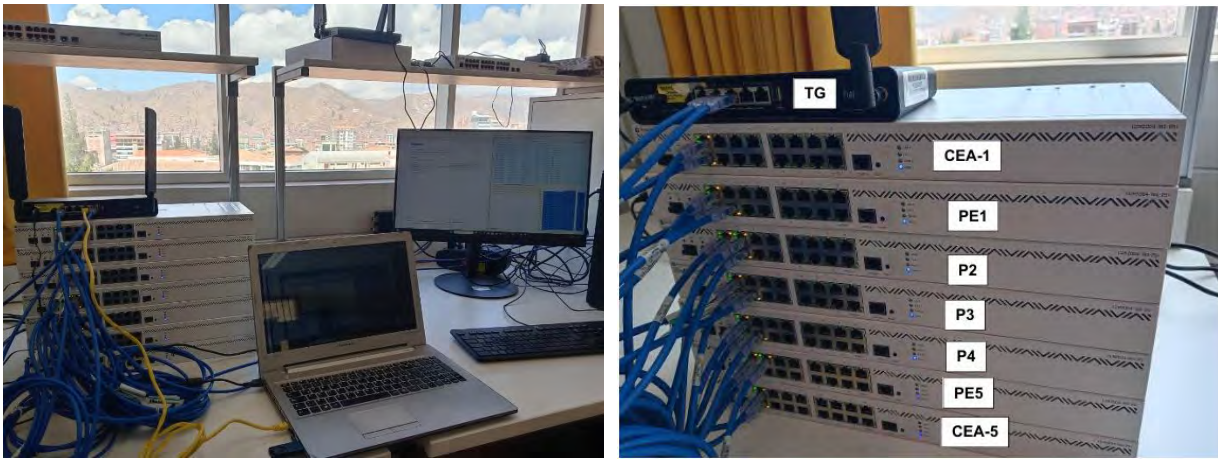


Figura 4.2.1 Routers del Core IP-MPLS y Cliente-L3VPN

Implementar una VPNL3 (VPNv4) sobre un túnel de ingeniería de tráfico (Traffic Engineering, TE) en routers MikroTik con RouterOS v7 es factible gracias al soporte mejorado para MPLS y protocolos como RSVP-TE (Resource Reservation Protocol for Traffic Engineering). En esta sección se detalla los pasos clave para su implementación, la implementación se basa en la implementación de IP/MPLS y enrutamiento que se implementó en el *capítulo 4: Implementación de IP/MPLS*. La configuración requiere múltiples componentes: IP/MPLS, RSVP-TE para el túnel TE, VRFs (Virtual Routing and Forwarding) para la VPN L3, y BGP para distribuir VPNv4.

4.2.1 Recursos Utilizados en la Implementación

- **Hardware**: Se hace uso del router Mikrotik modelo ccr2004-16g-2s+ en cual cumple con los requerimientos para la implementación de la solución.
- **RouterOS v7 actualizado**: Se usa el sistema operativo de red RouterOS versión 7.19.3 el cual soporta MPLS.
- **Conocimientos necesarios**: Para la implementación de la solución se hace necesario conocer de MPLS, RSVP-TE (distribución de etiquetas para el túnel de ingeniería de tráfico), VRF (tablas de enrutamiento individuales para cada cliente), VPLS (para relacionar el túnel VPLS hacia el tunnel TE) y BGP (específicamente MP-BGP para VPNv4).
- **Topología de red**: la Figura 4.2.2 describe los nodos de la topología de red (por ejemplo, P, PE, CE), interfaces, direcciones IP, y el tráfico que se desea priorizar en el túnel TE.

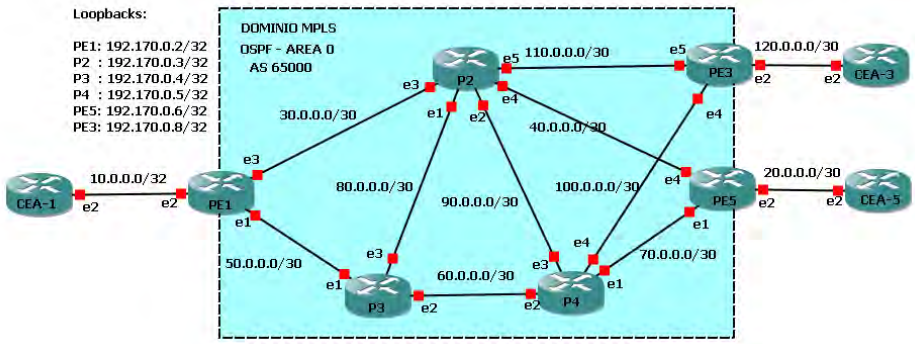


Figura 4.2.2 Dominio IP/MPLS Implementado

4.2.2 Direccionamiento IP de la Red Implementada

Tabla 4.2.1 Direcciones IP asignadas

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway
CEA-1	Ether1	192.168.1.1	255.255.255.0	-
	Ether2	10.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.1	255.255.255.255	-
	LoopBack 1	192.170.100.1	255.255.255.255	-
PE1	Ether1	30.0.0.1	255.255.255.252	-
	Ether2	10.0.0.1	255.255.255.252	-
	Ether3	50.0.0.1	255.255.255.252	-
	Loopback 0	192.170.0.2	255.255.255.255	-
	Loopback 1	192.170.100.2	255.255.255.255	-
P2	Ether1	80.0.0.1	255.255.255.252	-
	Ether2	90.0.0.1	255.255.255.252	-

	Ether3	30.0.0.2	255.255.255.252	-
	Ether4	40.0.0.1	255.255.255.252	-
	LoopBack 0	192.170.0.3	255.255.255.255	-
P3	Ether1	50.0.0.2	255.255.255.252	-
	Ether2	60.0.0.1	255.255.255.252	-
	Ether3	80.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.4	255.255.255.255	-
P4	Ether1	70.0.0.1	255.255.255.252	-
	Ether2	60.0.0.2	255.255.255.252	-
	Ether3	90.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.5	255.255.255.255	-
PE5	Ether1	70.0.0.2	255.255.255.252	-
	Ether2	20.0.0.1	255.255.255.252	-
	Ether4	40.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.6	255.255.255.255	-
	LoopBack 1	192.170.100.6	255.255.255.255	-
PE3	Ether2	120.0.0.1	255.255.255.252	-
	Ether4	100.0.0.2	255.255.255.252	-
	Ether5	110.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.8	255.255.255.255	-
	LoopBack 1	192.170.100.8	255.255.255.255	-
CEA-3	Ether1	192.168.3.1	255.255.255.0	-
	Ether2	120.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.9	255.255.255.255	-
	LoopBack 1	192.170.100.9	255.255.255.255	-
CEA-5	Ether1	192.168.2.1	255.255.255.0	-
	Ether2	20.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.7	255.255.255.255	-
	LoopBack 1	192.170.100.7	255.255.255.255	-

4.2.3 Configuración de Equipos

Tabla 4.2.2 Protocolos configurados

Configuración\Equipo	CEA-1	PE1	P2	P3	P4	PE5	CEA-5	CEA-3
Interfaz LoopBack	✓	✓	✓	✓	✓	✓	✓	✓
Interfaces Físicas	✓	✓	✓	✓	✓	✓	✓	✓
OSPF	✓	✓	✓	✓	✓	✓	✓	✓
BGP		✓				✓		
MPLS		✓	✓	✓	✓	✓		
VPNv4		✓				✓		
RD		✓				✓		
RT		✓				✓		
VPLS		✓				✓		
MPLS-TE (RSVP)		✓	✓	✓	✓	✓		

4.2.3.1 Configuración de las Interfaces y el Enrutamiento

Asignar direcciones IP a las interfaces de los routers (P, PE, CE).

```
# Configuración de interfaces y direcciones IP (genérica)
/interface bridge
add name=bridge-local
/ip address
add address=<customer-ip> interface=bridge-local
add address=<loopback-ip> interface=loopback
add address=<mpls-link-ip> interface=<core-interface>
```

Plantilla para la asignación de direcciones IP sobre las interfaces de red

Configurar un protocolo de enrutamiento IGP para la red MPLS interna. OSPF para MPLS-TE.

```
# Configuración de OSPF para IGP
/routing ospf instance
add name=ospf-instance router-id=<loopback-ip> distribute-default=never
/routing ospf area
add name=backbone instance=ospf-instance
/routing ospf interface
add interface=<core-interface> network-type=point-to-point area=backbone
add interface=loopback network-type=point-to-point area=backbone passive=yes
```

Plantilla de configuracion del protocolo OSPF en el dominio IP/MPLS

Por Ejemplo: El router P2 tiene una vecindad OSPF con los routers PE1, P3, P4 y PE5 como se muestra en la Figura 4.2.3.

```
[admin@P2] > routing/ospf/neighbor/print
Flags: V - virtual; D - dynamic
 0  D instance=ospf-instance-1 area=ospf-area-1 address=80.0.0.2
      router-id=192.170.0.4 state="Full" state-changes=6 adjacency=1m23s
      timeout=32s

 1  D instance=ospf-instance-1 area=ospf-area-1 address=90.0.0.2
      router-id=192.170.0.5 state="Full" state-changes=5 adjacency=1m13s
      timeout=39s

 2  D instance=ospf-instance-1 area=ospf-area-1 address=30.0.0.1
      router-id=192.170.0.2 state="Full" state-changes=6 adjacency=1m23s
      timeout=39s

 3  D instance=ospf-instance-1 area=ospf-area-1 address=40.0.0.2
      router-id=192.170.0.6 state="Full" state-changes=6 adjacency=1m13s
      timeout=31s
[admin@P2] >
```

Figura 4.2.3 Vecindades del router P2

4.2.3.2 Habilitación de MPLS y LDP en la Red

- Activamos MPLS en todos los routers (P y PE) y configuramos LDP (Label Distribution Protocol) para la distribución de etiquetas base, para la formación LSP (Label Switching Path).

```
# Habilitar MPLS y LDP
/mpls
set enabled=yes
/mpls ldp
set enabled=yes lsr-id=<loopback-ip> transport-address=<loopback-ip>
/mpls ldp interface
add interface=<core-interface>
```

Habilitacion de MPLS en los nodos del dominio IP/MPLS

4.2.3.3 Configuración RSVP-TE para el Túnel de Ingeniería de Tráfico

- Habilitamos RSVP-TE en las interfaces de los routers del core IP/MPLS.
- Definimos la ruta que los túneles usarán. La configuración se realizará en los routers de borde PE1, PE3 y PE5.
- Definimos los túneles y luego asignamos las rutas creadas. La configuración se realizará en los routers de borde PE1, PE3 y PE5.
- En los routers del core IP/MPLS como P2, P3 y P4 se habilitará RSVP en las interfaces del dominio IP/MPLS.
- Se habilitará en todos los router del dominio IP/MPLS el protocolo OSPF (CSPF) para ingeniería de tráfico.

```
/routing ospf instance
add disabled=no mpls-te-address=192.170.0.2 mpls-te-area=0.0.0.0 name=ospf-instance-1
/mpls traffic-eng interface
add bandwidth=100Mbps disabled=no interface=ether1
add bandwidth=100Mbps disabled=no interface=ether3
/mpls traffic-eng path
add disabled=no
hops=50.0.0.2/strict,60.0.0.1/strict,60.0.0.2/strict,70.0.0.1/strict,70.0.0.2/strict name=R-
Principal record-route=yes
add disabled=no
hops=30.0.0.2/strict,90.0.0.1/strict,90.0.0.2/strict,70.0.0.1/strict,70.0.0.2/strict
name=Respaldo record-route=yes use-cspf=no
add disabled=no name=D-CFS record-route=yes use-cspf=yes
/mpls traffic-eng tunnel
add bandwidth=15Mbps disabled=no from-address=192.170.0.2 name=tunnel15 primary-
path=R-Principal secondary-paths=Respaldo,D-CFS to-address=192.170.0.6
```

Configuración de túneles de ingeniería de tráfico en PE1, PE3 y PE5

- Configuramos RSVP en los routers intermedios (P) y en PE5 para soportar el túnel:

```
/mpls traffic-eng interface
add bandwidth=100Mbps disabled=no interface=ether1
add bandwidth=100Mbps disabled=no interface=ether3
```

Configuración de RSVP en los enrutadores del dominio IP/MPLS

4.2.3.4 Configuración VRFs para la VPN L3

En los routers PE (PE1 y PE2), se crea VRFs (Virtual Route Forwarding) para aislar el tráfico del cliente.

```
/ip vrf
add interfaces=ether2 name=VRF-CE1
```

Configuración VRF en los router de borde PE1 y PE5

4.2.3.5 Configuración MP-BGP para VPNv4

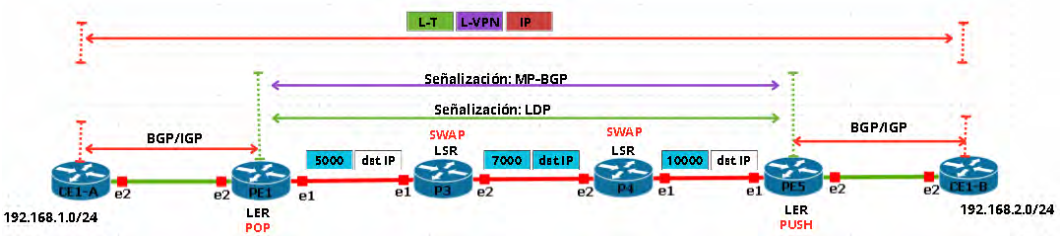


Figura 4.2.4 Señalización LDP y MP-BGP para L3VPN

- Habilitar BGP con soporte para VPNv4 entre los routers PE (PE1 y PE5), esto permitirá asignar y transportar las etiquetas a través del protocolo BGP a través de su extensión MP-BGP.
- Configurar el identificador único de 64 bit RD (Route Distinguisher) que añadido al IPv4 hacen a este único globalmente evitando el solapamiento de direcciones IP entre diferentes clientes que hacen uso de la red IP/MPLS para transportar sus VPNs.
- Configurar el RT (Route Target) que se usa como una etiqueta para distribuir (importar o exportar) las VPNs.

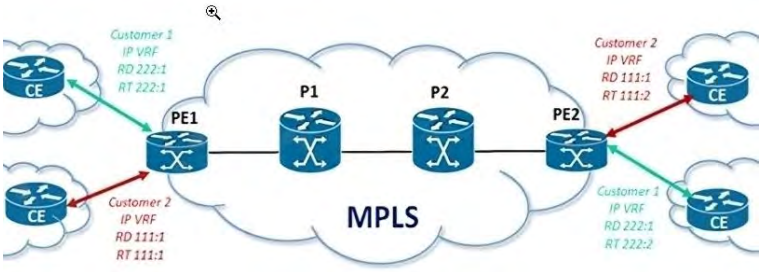


Figura 4.2.5 RD (Route-Distinguisher) y RT (Route-Target)

```
/routing bgp vpn
add disabled=no export.redistribute=bgp .route-targets=10:1 import.route-targets=10:1
.router-id=VRF-CE1 label-allocation-policy=per-vrf name=bgp-mpls-vpn-1 \
   route-distinguisher=10:1 vrf=VRF-CE1
add disabled=no export.redistribute=ospf .route-targets=20:1 import.route-targets=20:1
.router-id=VRF-CE2 label-allocation-policy=per-vrf name=bgp-mpls-vpn-2 \
   route-distinguisher=20:1 vrf=VRF-CE2add vrf=vrf-customer1
/routing bgp vpn
set vpnv4=export
```

Configuración MP-BGP en PE1 y PE5 del dominio IP/MPLS

- Los peers BGP entre PE1 y PE5 hacen uso de las direcciones de loopback.
- Las interfaces Loopback nos permite una mejor estabilidad ya que está interfaz es implementada en los enrutadores a nivel software, por lo que si cae una interfaz físicamente esta puede mantenerse estable.

4.2.3.6 Dirigir el Tráfico VPNv4 al Túnel TE

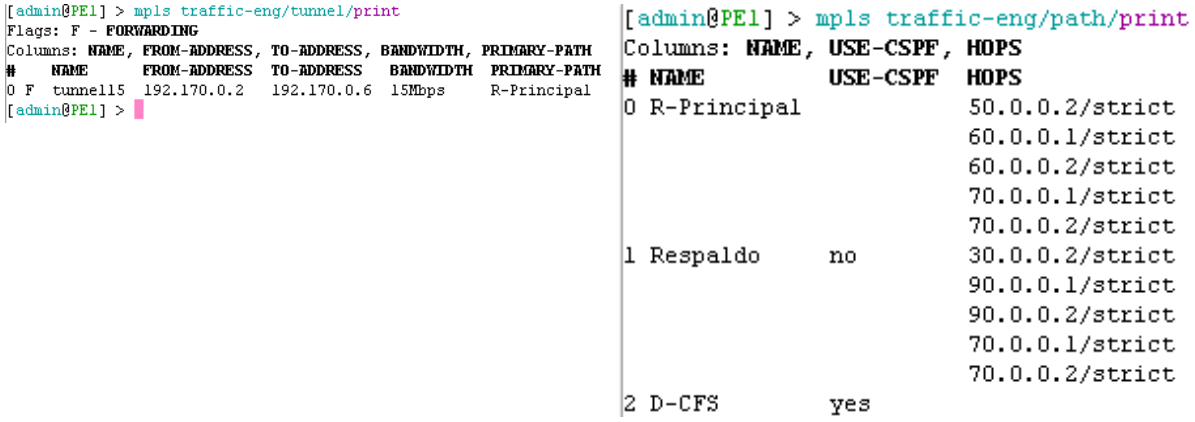
Asociaremos el tráfico de la VRF al túnel VPLS el cual está asociado automáticamente al túnel de ingeniería de tráfico y así L3VPN podrá usar el túnel de ingeniería de tráfico, se producirá un apilamiento de etiquetas (Etiqueta VPN3, Etiqueta VPLS y Etiqueta TE).

```
/ip route
add dst-address=192.170.0.6 gateway=192.168.10.2
[admin@PE1] > interface/vpls/monitor vpls15
  remote-label: 9000
   local-label: 1000
 remote-status:
    te-tunnel: tunnel15
     nexthops: { label=6009; nh=50.0.0.2; interface=ether1 }
```

VRF por el túnel de VPLS el cual usa el túnel TE

4.2.3.7 Verificación y Monitoreo

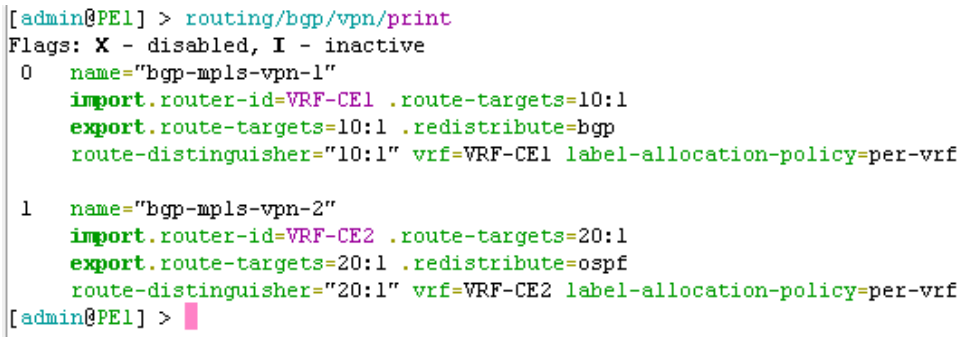
- Verificar que el túnel TE esté activo:



a) /mpls traffic-eng tunnel print b) */mpls traffic-eng/path/print*

Figura 4.2.6 Monitoreo del túnel de ingeniería de trafico

- Comprobar que las rutas VPNv4 se distribuyan correctamente:



a) /routing bgp VPNV4 print

Figura 4.2.7 Monitoreo de la VPNV4 configurada

Parámetros genéricos: Los valores <core-interface>, <loopback-ip>, <mpls-link-ip>, <customer-ip>, <customer-vrf-ip>, <rd-value>, <PE2-loopback>, <next-hop1>, <next-hop2>, etc., se reemplazan con los valores específicos de la topología.

Traffic Engineering: La configuración de tunnel15 en PE1 asume que el túnel se dirige a otro PE (PE5). Ajustar <PE5-loopback> y los hops (<next-hop1>, <next-hop2>) según la ruta deseada.

Escalabilidad: Los routers P (como P3) no requieren túneles TE específicos a menos que sean puntos de inicio o fin, pero se habilita TE en todas las interfaces <core-interface> por compatibilidad.

La topología con dos routers PE (PE1 y PE5) y los enrutadores P2, P3 y P4 intermedios:

- PE1 (loopback 192.17.0.2) conectado a P2 y P3 (loopbacks 192.170.0.3 y 192.170.0.4 respectivamente) vía ether1 y ether3 (50.0.0.1/30 y 30.0.0.1/30)

- P3 conectado a P4 (loopback 192.170.0.5) vía ether2 (60.0.0.1/30).
- P4 conectado a PE5 (loopback 192.170.0.6) vía ether1 (70.0.0.1/30).
- Cliente en VRF CEA-1 con red 10.0.0.0/30.

Los pasos que se siguieron para la configuración son:

1. Configurar OSPF y LDP en todos los routers.
2. Crear un túnel TE de PE1 a PE5 con RSVP-TE, reservando 200 Mbps.
3. Configurar VRFs en PE1 y PE5 para el cliente.
4. Habilitar MP-BGP entre PE1 y PE5, asegurando que las rutas VPNv4 se distribuyan.
5. Dirigir el tráfico de CEA-1 al túnel TE.

4.3 Implementación de VPLS

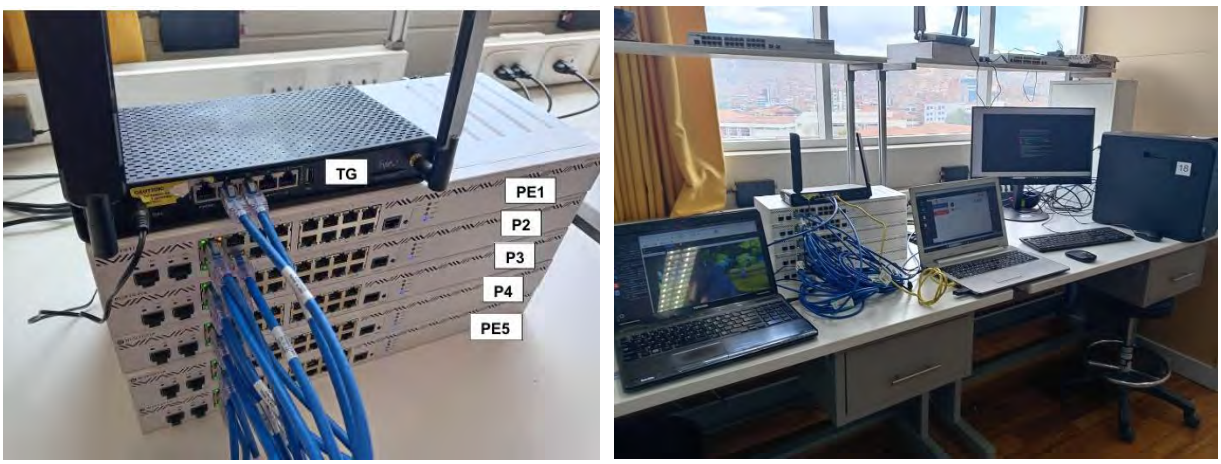


Figura 4.3.1 Configuración de VPLS sobre IP/MPLS

Configurar VPLS (Virtual Private LAN Service) que será transportado por un túnel de ingeniería de tráfico (Traffic Engineering, TE) en RouterOS v7 utilizando la topología propuesta implica combinar MPLS, RSVP-TE para el túnel TE, y la configuración de VPLS para conectar los sitios CE (como CEA-1, CEA-3, CEA-5) a través de los routers PE (PE1, PE3, PE5). A continuación, se detalla los pasos, adaptados a la topología IP/MPLS de capítulos anteriores.

4.3.1 Requisitos y Topología de Red

- RouterOS v7 instalado en dispositivos Mikrotik modelo ccr2004-16g-2s+ del laboratorio de telemática de escuela profesional de ingeniería Electrónica.
- Configuración básica de MPLS, MP-BGP y OSPF.

- Conocimiento de la topología: PE1, PE3, PE5 como routers de borde (PE), P2, P3, P4 como routers de tránsito (P).

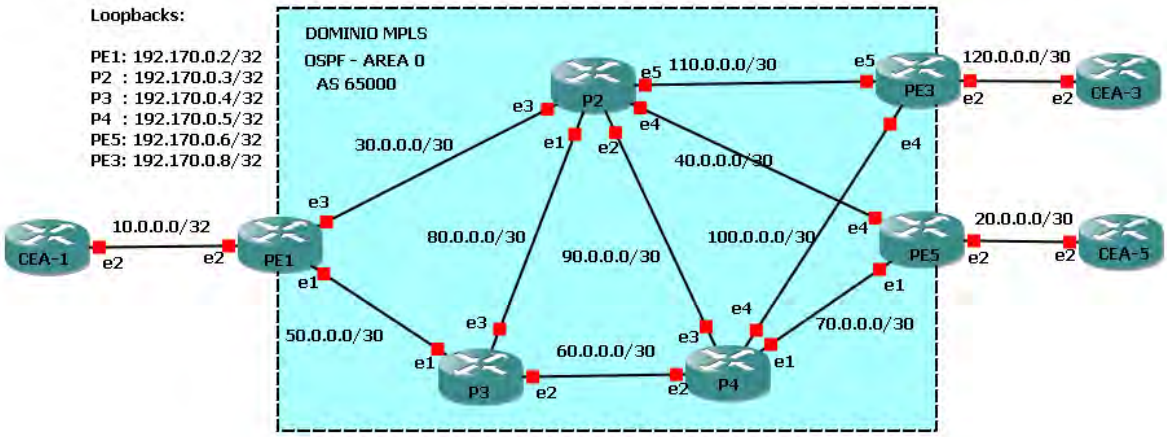


Figura 4.3.2 Dominio IP/MPLS Implementado

4.3.2 Direccionamiento IP de la Red Implementada

Tabla 4.3.1 Direcciones IP asignadas

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway
PE1	Ether1	30.0.0.1	255.255.255.252	-
	Ether2	Bridge con VPLS	-	-
	Ether3	50.0.0.1	255.255.255.252	-
	Loopback 0	192.170.0.2	255.255.255.255	-
P2	Ether1	80.0.0.1	255.255.255.252	-
	Ether2	90.0.0.1	255.255.255.252	-
	Ether3	30.0.0.2	255.255.255.252	-
	Ether4	40.0.0.1	255.255.255.252	-
	LoopBack 0	192.170.0.3	255.255.255.255	-
P3	Ether1	50.0.0.2	255.255.255.252	-
	Ether2	60.0.0.1	255.255.255.252	-
	Ether3	80.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.4	255.255.255.255	-
P4	Ether1	70.0.0.1	255.255.255.252	-
	Ether2	60.0.0.2	255.255.255.252	-
	Ether3	90.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.5	255.255.255.255	-
PE5	Ether1	70.0.0.2	255.255.255.252	-
	Ether2	Bridge con VPLS	-	-
	Ether4	40.0.0.2	255.255.255.252	-

	LoopBack 0	192.170.0.6	255.255.255.255	-
SW - Servidores	Ether1	-	-	-
	Ether2	-	-	-
	Ether3	-	-	-
	Ether4	-	-	-
SW -Clientes	Ether1	-	-	-
	Ether2	-	-	-
	Ether3	-	-	-
	Ether4	-	-	-

4.3.3 Configuración de Equipos

Tabla 4.3.2 Protocolos configurados

configuración\Equipo	CEA-1	PE1	P2	P3	P4	PE5	CEA-5
Interfaz LoopBack	✓	✓	✓	✓	✓	✓	✓
Interfaces Físicas	✓	✓	✓	✓	✓	✓	✓
OSPF		✓	✓	✓	✓	✓	
BGP		✓				✓	
MPLS		✓	✓	✓	✓	✓	
VPLS		✓				✓	
RD		✓				✓	
RT		✓				✓	
MPLS-TE (RSVP)		✓	✓	✓	✓	✓	

4.3.4 Configuración del Túnel TE (Traffic Engineering)

El túnel TE se configura en los routers PE para crear un camino explícito con RSVP-TE. Esto asegura que el tráfico VPLS pase por la ruta optimizada con túnel de ingeniería de tráfico.

En PE1 (inicio del túnel hacia PE3 o PE5):

```
/mpls traffic-eng interface
add interface=<core-interface> bandwidth=100M
/mpls traffic-eng tunnel
add name=te-tunnel1 to-address=<remote-PE-loopback> primary-path=path1
/mpls traffic-eng path
add name=path1 dynamic=no
add hop address=<next-hop1> loose=no
add hop address=<next-hop2> loose=no
```

Configuración de la ruta y tunnel de Ingeniería de tráfico.

- *<remote-PE-loopback>:* Loopback del PE destino (PE3 o PE5).
- *<next-hop1> y <next-hop2>:* Direcciones de los routers intermedios (P2 o P3).

En routers P intermedios (P2, P3, P4):

```
/mpls traffic-eng interface
add interface=<core-interface1> bandwidth=100M
add interface=<core-interface2> bandwidth=100M
```

Habilitar el protocolo RSVP en los enrutadores del dominio IP/MPLS

Configurar todas las interfaces del camino TE, habilitando RSVP en cada interfaz.
En PE3 o PE5 (fin del túnel):

- No es necesario configurar un túnel de salida explícito, pero se habilita RSVP-TE en las interfaces:

```
/mpls traffic-eng interface
add interface=<core-interface> bandwidth=100M
```

Habilitar el protocolo RSVP en PE3 o PE5

4.3.5 Configura VPLS en los Routers PE

VPLS requiere la creación de instancias de bridge y la asociación con túneles TE o LSPs (Label Switched Paths).

En PE1:

```
/interface bridge
add name=bridge-vpls
/interface vpls
add name=vpls1 remote-peer=<remote-PE-loopback> bridge=bridge-vpls vpls-id=<vpls-id>
/ip address
add address=<customer-ip> interface=bridge-vpls
```

Configuración de túneles VPLS en los router de borde PE.

- <vpls-id>: Identificador único para la instancia VPLS (100:1).
- La asociación con el túnel TE (tunnel15) es automático en el sistema operativo RouterOS.

En PE3 y PE5:

```
/interface bridge
add name=bridge-vpls
/interface vpls
add name=vpls1 remote-peer=<PE1-loopback> bridge=bridge-vpls vpls-id=<vpls-id>
/ip address
add address=<customer-ip> interface=bridge-vpls
```

Configuración de túneles VPLS en los router de borde PE3 y PE5.

El túnel VPLS se asocia al túnel TE de manera automática o usa el LSP predeterminado si el túnel termina.

4.3.6 Conectar las Interfaces al Bridge VPLS

En nuestra topología las interfaces Ether2 de los enrutadores de borde (PE1, PE3 y PE5) deben estar en el mismo bridge que la VPLS configurada en cada router PE. Por qué la interfaz Ether2 es la que conecta a los clientes los mismos se conectan a través de switches, la interconectividad es a nivel de capa 2, una extensión de la LAN del cliente que atraviesa el dominio IP/MPLS.

En PE1 (con CEA-1), En PE3 (con CEA-3), En PE5 (con CEA-5):

```
/interface bridge port
add bridge=bridge-vpls interface=<ce-interface>
```

Comando para asociar la interfaz a un Bridge que interconecta al cliente

4.3.7 Verificar Configuración

Confirmar con los siguientes comandos que el túnel TE está activo:

```
[admin@PE1] /mpls/traffic-eng/tunnel> print
Flags: X - DISABLED, I - INVALID, F - FORWARDING
Columns: NAME, FROM-ADDRESS, TO-ADDRESS, BANDWIDTH, PRIMARY-PATH
#    NAME                  FROM-ADDRESS  TO-ADDRESS   BANDWIDTH  PRIMARY-PATH
0 F  tunnel-gold-PE5       192.170.0.2   192.170.0.6  512kbps    R-Gold-Hacia-PE5
1 X  tunnel-clientB-silver-PE5 192.170.0.2 192.170.0.6 10Mbps    R-Silver-Hacia-PE5
2 X  tunnel-clientC-bronze-PE5 192.170.0.2 192.170.0.6 5Mbps     R-CSPF
3 X  tunnel-clientC-bronze-PE3 192.170.0.2 192.170.0.7 5Mbps     R-CSPF
4 X  tunnel-clientB-silver-PE3 192.170.0.2 192.170.0.7 10Mbps    R-Silver-Hacia-PE3
5 F  tunnel-gold-PE3       192.170.0.2   192.170.0.7  512kbps    R-Gold-Hacia-PE3
[admin@PE1] /mpls/traffic-eng/tunnel>
```

a) /mpls traffic-eng tunnel print

b) /mpls traffic-eng tunnel

Figura 4.3.3 Verificar la configuración del túnel de TE

Con el siguiente comando verificamos el establecimiento del túnel VPLS.

```
[admin@PE1] > interface/vpls/print
Flags: R - RUNNING; D - DYNAMIC
Columns: NAME, PEER, BGP-VPLS
#     NAME   PEER          BGP-VPLS
0 RD  vpls1  192.170.0.7  vpls-clientA-gold
1 RD  vpls2  192.170.0.6  vpls-clientA-gold
[admin@PE1] >
```

Figura 4.3.4 Verificar la configuración de VPLS

El siguiente comando nos ayuda a Monitorear el tráfico en el bridge:

```
[admin@PE1] > interface/bridge/monitor VPLS
                  state: enabled
    current-mac-address: 02:7C:24:E6:48:3F
              bridge-id: 0x8000.02:7C:24:E6:48:3F
            root-bridge: yes
       root-bridge-id: 0x8000.02:7C:24:E6:48:3F
       root-path-cost: 0
            root-port: none
           port-count: 3
  designated-port-count: 3
          fast-forward: no
-- [Q quit|D dump|C-z pause]
```

Figura 4.3.5 Verificar el tráfico en el bridge-VPLS

El ancho de banda del túnel TE es ajustable si es necesario (bandwidth=200M puede modificarse según el tráfico).

Consideraciones que se debe tomar al configurar los túneles de TE

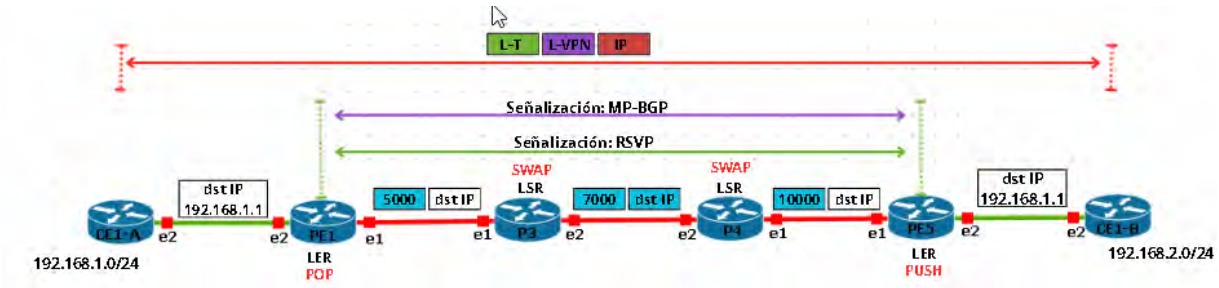


Figura 4.3.6 Protocolos de señalización para VPLS sobre túnel TE

- Topología: Configurar los túneles TE entren PE1-PE3, PE1-PE5, y PE3-PE5 según las rutas deseadas (se puede necesitar múltiples túneles o un diseño de malla).
- Escalabilidad: Para una topología completa, configurar VPLS con todos los PEs como peers (PE1-PE3, PE1-PE5, PE3-PE5) usando el mismo <vpls-id>, si se usa la señalización LDP y diferentes si usamos señalización MP-BGP, como es el caso de nuestra implementación.

```
[admin@PE1] > routing/bgp/vpls/print detail
Flags: X - disabled, I - inactive
 0   name="vpls-clientA-gold" rd=65000:100 site-id=100 import-route-targets=65000:105,65000:103 export-route-targets=65000:100 bridge=VPLS bridge-horizon=1

 1 X name="vpls-clientC-bronze" rd=65000:300 site-id=300 import-route-targets=65000:300 export-route-targets=65000:300 bridge=VPLS3

 2 X name="vpls-clientB-silver" rd=65000:200 site-id=200 import-route-targets=65000:203,65000:205 export-route-targets=65000:200 bridge=VPLS2 bridge-horizon=1
[admin@PE1] >
```

Figura 4.3.7 VPLS con señalización MP-BGP.

- Rendimiento: Los túneles TE y VPLS aumentan la carga de la CPU.

- Pruebas: Realizamos ping entre las interfaces de cliente (CEA-1 a CEA-3, CEA-5) para verificar la conectividad L2.

```
[admin@CE1-A] > ping 172.10.102.254 src-address=172.10.102.1
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 172.10.102.254                             56  64 20ms705us
    1 172.10.102.254                             56  64 18ms143us
    2 172.10.102.254                             56  64 14ms931us
    3 172.10.102.254                             56  64 13ms727us
    4 172.10.102.254                             56  64 16ms756us
    5 172.10.102.254                             56  64 15ms248us
    6 172.10.102.254                             56  64 18ms903us
    sent=7 received=7 packet-loss=0% min-rtt=13ms727us avg-rtt=16ms916us max-rtt=20ms705us

[admin@CE1-A] >
```

Figura 4.3.8 Prueba de conectividad de extremo a extremo

4.3.8 Flujo de Datos

- Tráfico desde CEA-1 (conectado a PE1) a CEA-3 (conectado a PE3) usará el túnel TE tunnel-gold-PE3 desde PE1 a PE3, transportado sobre MPLS con etiquetas VPLS.

```
[admin@PE1] > mpls traffic-eng/tunnel/print
Flags: X - DISABLED, I - INVALID, F - FORWARDING
Columns: NAME, FROM-ADDRESS, TO-ADDRESS, BANDWIDTH, PRIMARY-PATH
#    NAME                       FROM-ADDRESS  TO-ADDRESS   BANDWIDTH  PRIMARY-PATH
0 F  tunnel-gold-PE5            192.170.0.2   192.170.0.6  512kbps    R-Gold-Hacia-PE5
1 X  tunnel-clientB-silver-PE5  192.170.0.2   192.170.0.6  10Mbps     R-Silver-Hacia-PE5
2 X  tunnel-clientC-bronze-PE5  192.170.0.2   192.170.0.6  5Mbps      R-CSPF
3 X  tunnel-clientC-bronze-PE3  192.170.0.2   192.170.0.7  5Mbps      R-CSPF
4 X  tunnel-clientB-silver-PE3  192.170.0.2   192.170.0.7  10Mbps     R-Silver-Hacia-PE3
5 F  tunnel-gold-PE3            192.170.0.2   192.170.0.7  512kbps    R-Gold-Hacia-PE3
[admin@PE1] >
```

Figura 4.3.9 Túnel de Ingeniería de tráfico PE1-PE3

- Los routers P (P2, P3, P4) actúan como tránsito, sin necesidad de procesar VPLS, solo MPLS -TE.

```
[admin@P4] > mpls traffic-eng tunnel print

[admin@P4] > mpls traffic-eng tunnel print detail
Flags: X - disabled, I - invalid, F - forwarding
[admin@P4] > mpls traffic-eng path print detail
Flags: X - disabled
[admin@P4] >
```

Figura 4.3.10 Ninguna configuración de rutas y túnel en P4

4.4 Implementación L3VPN con Tráfico Real

Figura 4.4.1 Topología física Implementada

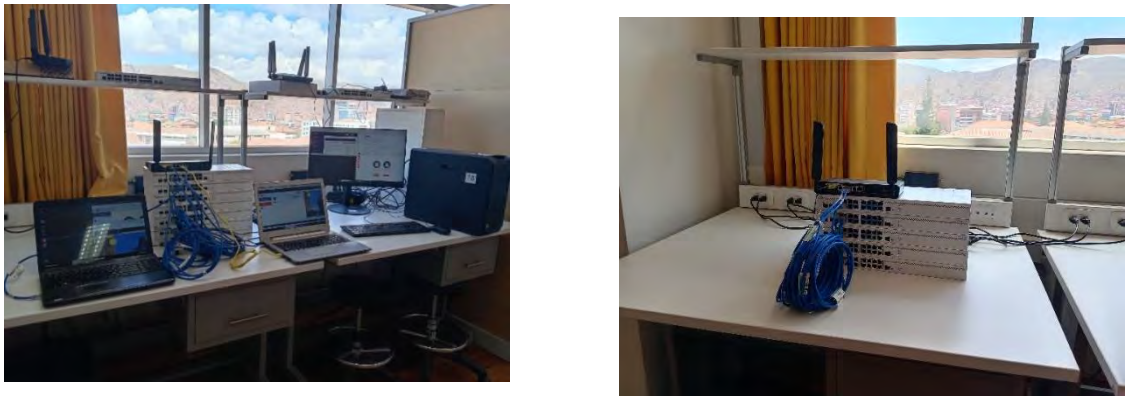


Figura 4.4.2 Laboratorio Implementado

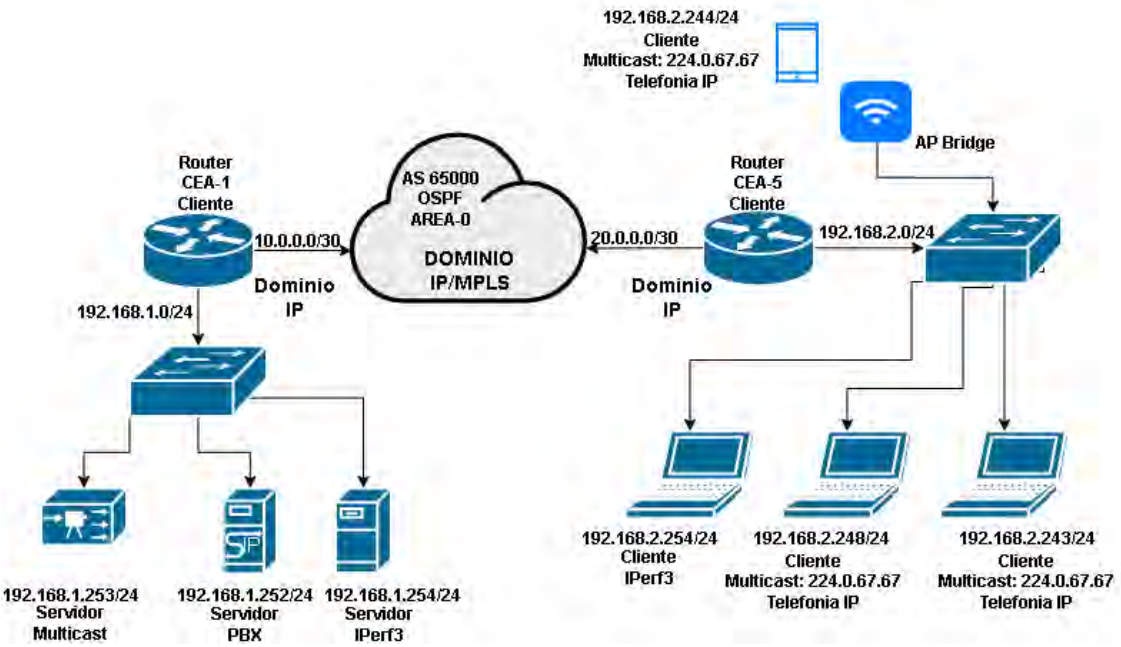


Figura 4.4.3 Topología lógica de la implementación IP/MPLS

4.4.1 Direccionamiento IP

Tabla 4.4.1 Asignación de direccionamiento IP

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway
CEA-1	Ether1	192.168.1.1	255.255.255.0	-
	Ether2	10.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.1	255.255.255.255	-
	LoopBack 1	192.170.100.1	255.255.255.255	-
PE1	Ether1	30.0.0.1	255.255.255.252	-
	Ether2	10.0.0.1	255.255.255.252	-
	Ether3	50.0.0.1	255.255.255.252	-
	Loopback 0	192.170.0.2	255.255.255.255	-
	Loopback 1	192.170.100.2	255.255.255.255	-
P2	Ether1	80.0.0.1	255.255.255.252	-
	Ether2	90.0.0.1	255.255.255.252	-
	Ether3	30.0.0.2	255.255.255.252	-
	Ether4	40.0.0.1	255.255.255.252	-
	LoopBack 0	192.170.0.3	255.255.255.255	-
P3	Ether1	50.0.0.2	255.255.255.252	-
	Ether2	60.0.0.1	255.255.255.252	-
	Ether3	80.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.4	255.255.255.255	-
P4	Ether1	70.0.0.1	255.255.255.252	-
	Ether2	60.0.0.2	255.255.255.252	-
	Ether3	90.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.5	255.255.255.255	-
PE5	Ether1	70.0.0.2	255.255.255.252	-
	Ether2	20.0.0.1	255.255.255.252	-
	Ether4	40.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.6	255.255.255.255	-
	LoopBack 1	192.170.100.6	255.255.255.255	-
CEA-5	Ether1	192.168.2.1	255.255.255.0	-
	Ether2	20.0.0.2	255.255.255.252	-
	LoopBack 0	192.170.0.7	255.255.255.255	-
	LoopBack 1	192.170.100.7	255.255.255.255	-
SW - Servidores	Ether1	-	-	-
	Ether2	-	-	-
	Ether3	-	-	-
	Ether4	-	-	-
SW -Clientes	Ether1	-	-	-
	Ether2	-	-	-
	Ether3	-	-	-

	Ether4	-	-	-
Serv. Multicast	Ether0	192.168.1.253	255.255.255.0	192.168.1.1
Servidor PBX	Ether0	192.168.1.252	255.255.255.0	192.168.1.1
Servidor Iperf3	Ether0	192.168.1.254	255.255.255.0	192.168.1.1
Cliente 1 Multicast	Ether0/Vlc Player	192.168.2.248 224.0.67.67	255.255.255.0	192.168.2.1
Cliente 2 Multicast	Ether0/Vlc Player	192.168.2.243/ 224.0.67.67	255.255.255.0	192.168.2.1
Cliente 3 Multicast	Ether0/Vlc Player	192.168.2.244/ 224.0.67.67	255.255.255.0	192.168.2.1
Cliente 1 Telefonía IP	Ether0	192.168.2.248	255.255.255.0	192.168.2.1
Cliente 2 Telefonía IP	Ether0	192.168.2.243	255.255.255.0	192.168.2.1
Cliente 3 Telefonía IP	Ether0	192.168.2.244	255.255.255.0	192.168.2.1
Cliente Iperf3	Ether0	192.168.2.254	255.255.255.0	192.168.2.1

4.4.2 Configuracion de Equipos

Tabla 4.4.2 Protocolos configurados

Configuración\Equipo	CEA-1	PE1	P2	P3	P4	PE5	CEA-5
Interfaz LoopBack	✓	✓	✓	✓	✓	✓	✓
Interfaces Físicas	✓	✓	✓	✓	✓	✓	✓
OSPF	✓	✓	✓	✓	✓	✓	✓
BGP		✓				✓	
MPLS		✓	✓	✓	✓	✓	
VPNv4		✓				✓	
RD		✓				✓	
RT		✓				✓	
VPLS		✓				✓	
MPLS-TE (RSVP)		✓	✓	✓	✓	✓	
PIM-SM (PIM v2)	✓	✓				✓	✓
IGMP Snooping						✓	✓

La configuracion de los equipos de laboratorio esta desarrollado en las secciones Implemetacion de L3VPN y Implementacion de VPLS. Aquí se desarrollara la configracion de multicast para el trafico de IPTV. Para esta configuracion habilitaremos el protocolo de enrutamiento para multicast en los enrutadores del cliente (CEA1 y CEA5) y los enrutadores de borde (PE1 y PE2) en el dominio IP/MPLS. El protocolo de enrutamiento para multicast que soporta Mikrotik es PIM-SM y el protocolo para multicast a nivel capa 2 que soporta Mikrotik es IGMP Proxy y IGMP Snooping estos protocolos se habilitaran de lado de los clientes que consumen los recursos de los servidores (Telefonia IP, Multicast y datos generales). La

configuraion del protocolo de enrutamiento solo se hara en la implemetacion del servicio L3VPN por que aquí la interaccion a nivel de red es en la capa 3 del modelo de capas de red. Mientras tanto que en la configuracion del servicio VPLS la interaccion entre la red IP/MPLS y la red del cliente es a nivel de capa 2 del modelo de capas de red, por lo que los protocolo a configrar seria IGMP Proxy y IGMP Snooping.

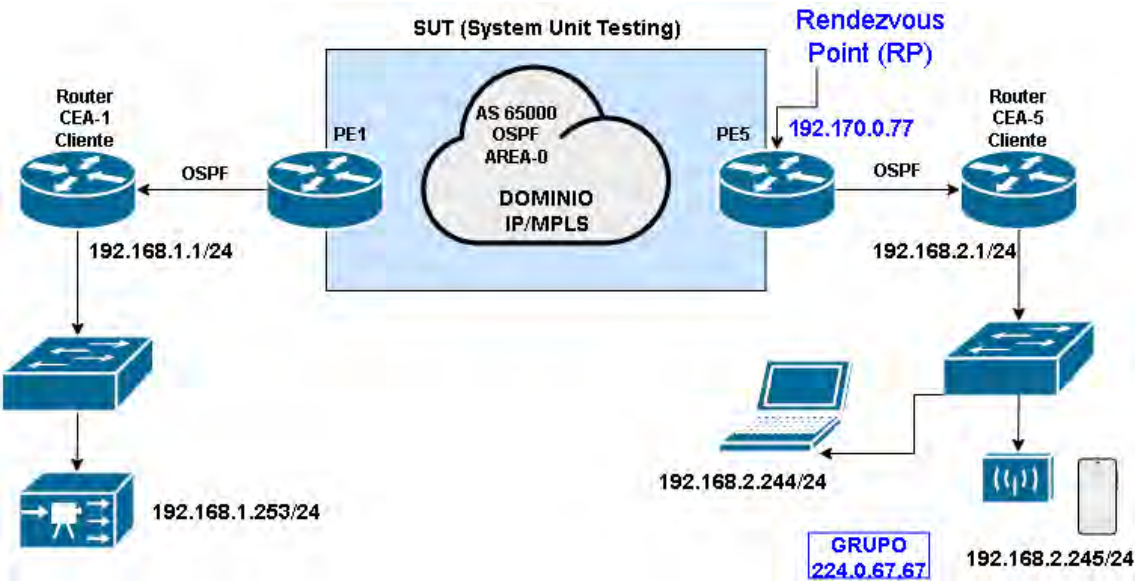


Figura 4.4.4 Multicast sobre L3VPN

```
/routing pimsm instance
add disabled=no name=instancia1 vrf=main
/routing pimsm interface-template
add disabled=no instance=instancia1 interfaces=lom,ether1,ether2
/routing pimsm static-rp
add address=192.170.0.77 instance=instancia1
```

Configuración de PIM-SM en router CEA1

```
/routing pimsm instance
add disabled=no name=instancia1 vrf=vrf-ce1
/routing pimsm interface-template
add disabled=no instance=instancia1 interfaces=ether2,lom,vrf-ce1
/routing pimsm static-rp
add address=192.170.0.77 instance=instancia1
```

Configuración de PIM-SM en router PE1

```
/routing pimsm instance
add disabled=no name=instancia1 vrf=vrf-ce5
/routing pimsm interface-template
add disabled=no instance=instancia1 interfaces=ether2,lom,vrf-ce5
/routing pimsm static-rp
add address=192.170.0.77 instance=instancia1
```

Configuración de PIM-SM en router PE5

```
/routing pimsm instance
add disabled=no name=instancia1 vrf=main
/routing pimsm interface-template
add disabled=no instance=instancia1 interfaces=lom,ether2,ether1
/routing pimsm static-rp
add address=192.170.0.77 instance=instancia1
```

Configuración de PIM-SM en router CEA5

Figura 4.4.5 Configuración Multicast L3VPN

Capítulo 5

Análisis y Evaluación

5.1 Análisis de Paquetes con Wireshark – L3VPN

La captura de paquetes se realizará en la ruta marcada de color rojo que es el túnel entre los routers PE1 y PE5, Fig. 5.1.2. Wireshark es una herramienta de software que permite analizar los protocolos de las diferentes capas del modelo TCP/IP. En este caso analizaremos como se da la conmutación de etiquetas a través del dominio IP/MPLS de la topología implementada.

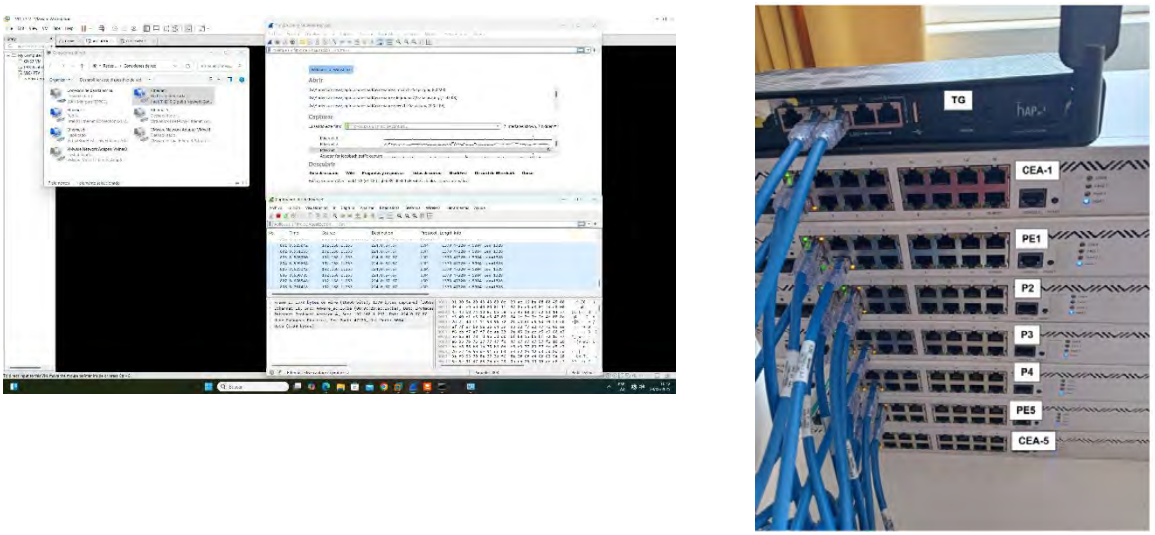


Figura 5.1.1 Captura de paquetes, IP MPLS – L3VPN

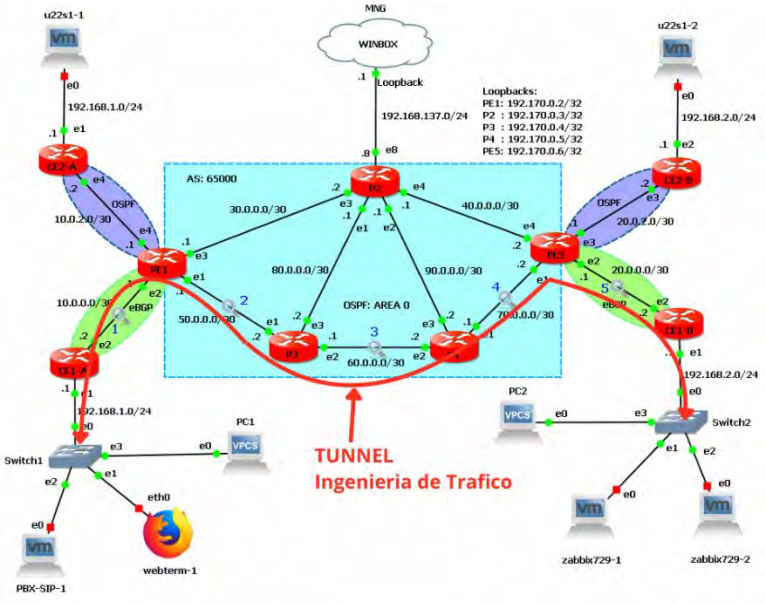


Figura 5.1.2 Topología de red L3VPN con Ingeniería de trafico

5.1.1 Ruta de Túnel de Ingeniería de Trafico

La ruta del túnel de ingeniería de tráfico en la imagen de la topología de red se encuentra resaltada con la línea roja (PE1, P3, P4 y PE5), Fig.5.1.2.

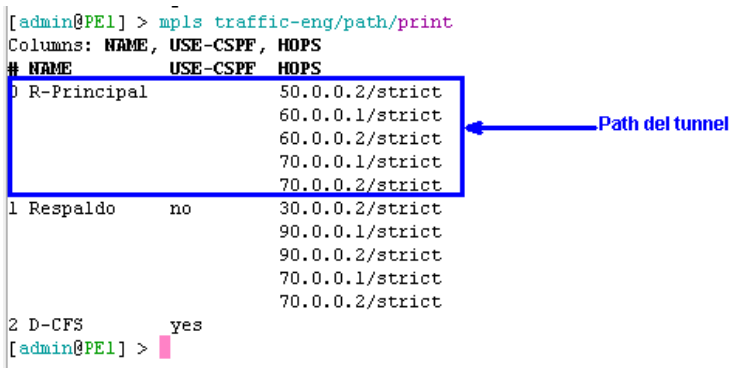


Figura 5.1.3 Path Principal de túnel de ingeniería de tráfico desde PE1 hacia PE5

Puntos de Captura de paquetes con Wireshark: Las capturas se realizarán como se detalla a continuación.

1. CE1-A (ether2) ←→ PE1 (ether2) - Entrada al dominio MPLS – Trafico IP.
2. PE1 (ether1) ←→ P3 (ether2) - Trafico etiquetado en el dominio IP/MPLS.
3. P3 (ether2) ←→ P4 (ether2) - Trafico etiquetado en dominio IP/MPLS.
4. P4 (ether1) ←→ PE5 (ether1) - Trafico etiquetado en el dominio IP/MPLS.
5. PE5 (ether2) ←→ CE1-B (ether2) - Salida del dominio MPLS – Trafico IP.

5.1.2 Captura de paquetes entre CE1A (eth2) - PE1 (eth2)

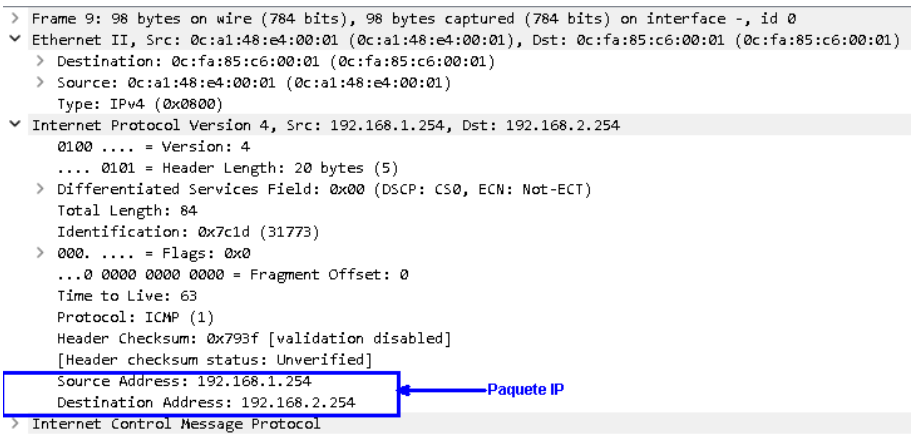


Figura 5.1.4 Paquetes capturados entre CE1-A y PE1

Análisis del Frame 9: CE1-A → PE1

Capa 2 (Ethernet)

- Src MAC: 0c:a1:48:e4:00:01 (CE1-A).
- Dst MAC: 0c:fa:85:c6:00:01 (PE1).

Tipo: IPv4 (0x0800) – Indica el tipo de protocolo que está transportando la capa 2 (ethernet), en este caso es IP, ya que la interacción entre el router cliente y router de borde del dominio IP/MPLS es por IP.

- Versión: IPv4.
- Src IP: 192.168.1.254 (CE1-A)
- Dst IP: 192.168.2.254 (CE1-B)
- Protocolo: ICMP (ping)
- TTL: 63
- DSCP: CS0 (sin QoS marcado)

Protocolo ICMP

- Tipo: Echo Request (ping)
- Tamaño total: 98 bytes

Observaciones

1. Tráfico IP Puro: En este punto no hay etiquetas MPLS - es tráfico IPv4 normal
2. Punto de Ingreso: Este es el tráfico antes de ingresar al dominio MPLS
3. Comunicación VPN: El tráfico va de una red (192.168.1.0/24) a otra (192.168.2.0/24)

Siguiente Salto; En el siguiente punto de captura es entre PE1 (ether1) y P3 (ether2), se vera la:

- Encapsulación MPLS con las etiquetas de VPN3, VPLS y MPLS-TE
- Stack de etiquetas múltiples
- Preservación del paquete IP original

5.1.3 Captura de Paquetes entre PE1 (eth1) - P3 (eth2)

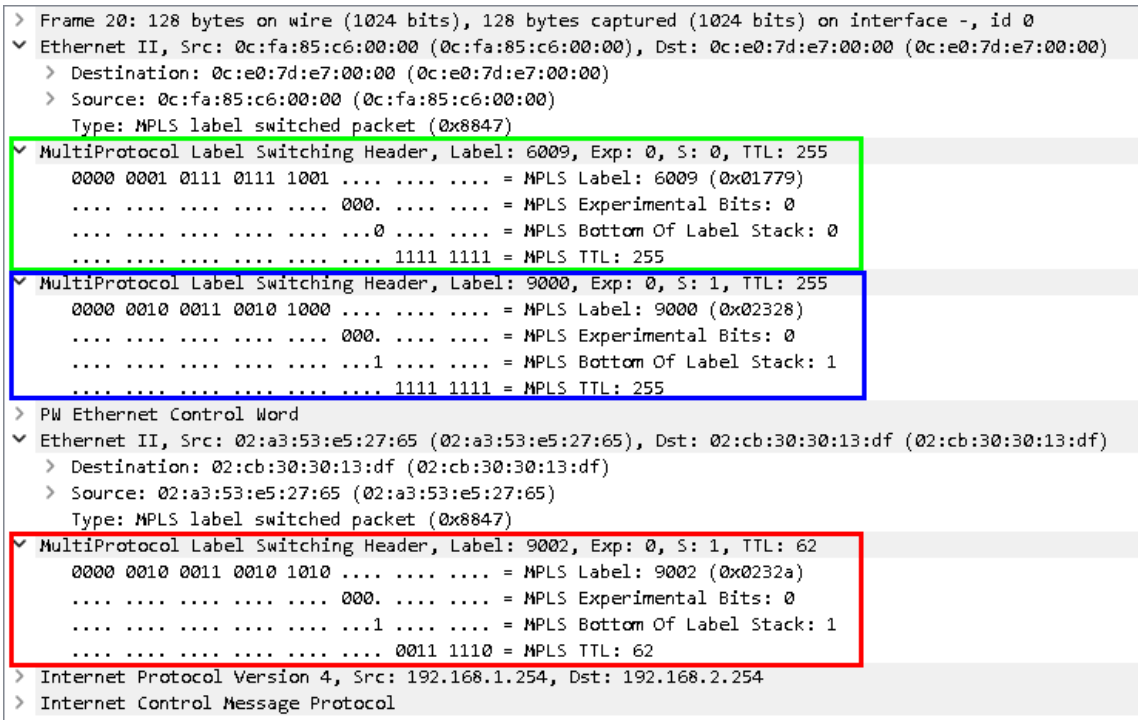


Figura 5.1.5 Captura de paquetes entre PE1 y P3

Análisis del Frame 20: Entre enrutadores PE1 → P3

El tráfico ahora tiene una pila (Stack) de etiquetas MPLS implementado, la etiqueta del rectángulo verde es la de ingeniería de tráfico cuyo valor es 6009, la etiqueta del rectángulo azul es la etiqueta del túnel VPLS cuyo valor es 9000 y por último la etiqueta del rectángulo rojo es la etiqueta de servicio (en este caso L3VPN) cuyo valor es 9002.

Primera Etiqueta MPLS (Exterior):

- Label: 6009 (0x1771) – túnel de ingeniería de tráfico.
- Exp: 0 (sin QoS)
- S: 0 (Indica que no es la última etiqueta de la pila)
- TTL: 255

Segunda Etiqueta MPLS (Interior):

- Label: 9000 (0x2328) – túnel VPLS construido a través de LDP.
- Exp: 0 (sin QoS)

- S: 1 (Etiqueta interior de la pila)
- TTL: 255

Tercera Etiqueta MPLS (Etiqueta de servicio):

- Label: 9002 (0x232a) – servicio L3VPN
- Exp: 0 (sin QoS)
- S: 1 (Ultima etiqueta de la pila)
- TTL: 62

Jerarquía de Túneles Identificada

[Ethernet] → [MPLS-TE: 6009] → [VPLS: 9000] → [VPN3: 9002] → [IP Original]

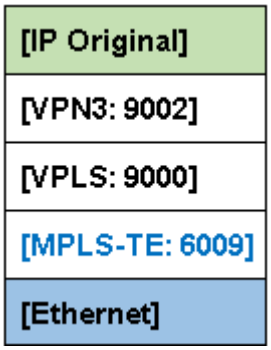


Figura 5.1.6 Pila de Etiquetas entre PE1 y P3

Se presenta la siguiente encapsulación:

1. VPN3 (Etiqueta 9002): Identifica el servicio L3VPN específico
2. VPLS (Etiqueta 9000): Túnel de transporte VPLS (Virtual Private LAN Service)
3. MPLS-TE (Etiqueta 6009): Ingeniería de tráfico para optimización de ruta

En la captura del paquete podemos notar lo siguiente.

- El TTL del IP original (63→62) se mantiene en la etiqueta VPN3
- Payload Preservado: El paquete IP original (192.168.1.254 → 192.168.2.254) está intacto
- Tamaño aumentado: De 98 bytes a 128 bytes (30 bytes de cabecera MPLS)

5.1.4 Captura de Paquetes entre P3 (eth2) y P4 (eth2)

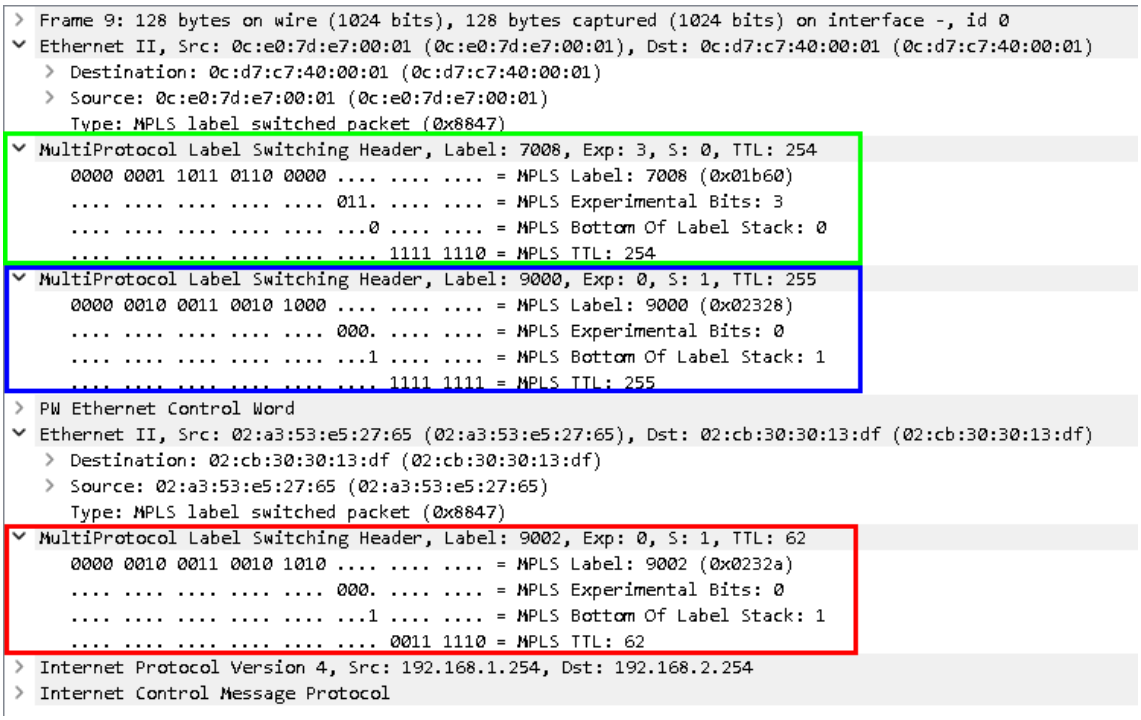


Figura 5.1.7 Captura de paquetes entre P3 y P4 del Dominio IP/MPLS

Análisis del Frame 9: Del tráfico entre los enrutadores P3 y P4

Se produce la operación de intercambio (SWAP) de la etiqueta exterior en este caso la etiqueta de ingeniería de tráfico.

Primera Etiqueta MPLS (Exterior) – etiqueta del túnel de ingeniería de trafico

- Label: 7008 (0x1b60) - Cambio de 6009 a 7008
- Exp: 3 (QoS marcado)
- S: 0 (Indica que la etiqueta no es el último de la Pila)
- TTL: 254 (decrementado de 255)

Segunda Etiqueta MPLS - VPLS

- Label: 9000 (0x2328) - Sin cambios
- Exp: 0 (sin QoS)
- S: 1 (Es una etiqueta interior de la pila de etiquetas)
- TTL: 255 (sin cambios)

Tercera Etiqueta MPLS - VPN3

- Label: 9002 (0x232a) - Sin cambios
- Exp: 0 (sin QoS)
- S: 1 (La última etiqueta de la pila de etiquetas)
- TTL: 62 (sin cambios)

Operaciones MPLS Observadas:

Label Swapping (MPLS-TE)

- P3 realizó una operación de SWAP: 6009 → 7008
- Este es el túnel de trasporte de los paquetes, esto lo hace a través de la conmutación de etiquetas.
- TTL decrementado: 255 → 254

[Ethernet] [MPLS-TE: 7008, Exp:3] [VPLS: 9000] [VPN3: 9002][IP Original]

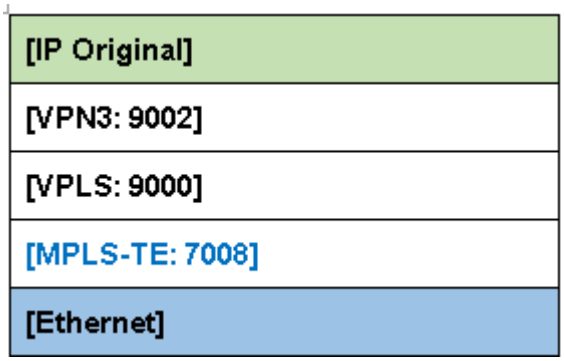


Figura 5.1.8 Pila de Etiquetas entre P3 y P4

- LSR: P3 actúa como LSR intermedio, solo modifica la etiqueta exterior
- Ingeniería de Trafico: El cambio de etiqueta indica un LSP preestablecido
- QoS: La red está aplicando políticas de QoS en el core

5.1.5 Captura de Paquetes entre P4 (eth1) y PE5 (eth1)

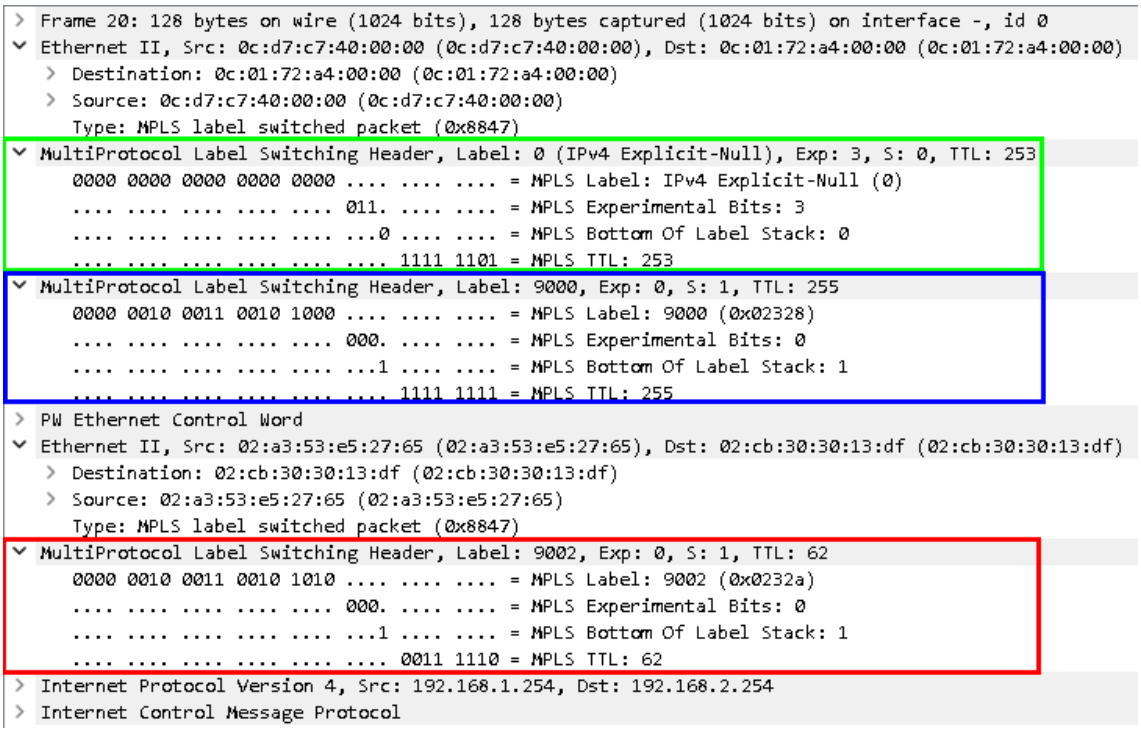


Figura 5.1.9 Captura de paquetes entre P4 y PE5 del Dominio IP/MPLS

Análisis del Frame 20: P4 → PE5

Operación MPLS Crítica: Retirar la etiqueta (POP)

Primera Etiqueta MPLS - MPLS-TE

- Label: 0 (IPv4 Explicit-Null) - Operación POP, esto permite menor procesamiento para el router PE5.
- Exp: 3 (QoS preservado)
- S: 0 (No es la última etiqueta de la pila)
- TTL: 253 (decrementado de 254)

Segunda Etiqueta MPLS - VPLS

- Label: 9000 (0x2328) – La etiqueta de mantiene, no existe cambios.
- Exp: 0 (sin QoS)
- S: 1 (Etiqueta interior de la pila)

- TTL: 255 (sin cambios)

Tercera Etiqueta MPLS – Etiqueta de servicio VPN3

- Label: 9002 (0x232a) – La etiqueta se mantiene no existe ningún cambio con otra etiqueta.
- Exp: 0 (sin QoS)
- S: 1 (Etiqueta de servicio de la Pila)
- TTL: 62 (sin cambios)

Análisis de la Operación

1. Penultimate Hop Popping (PHP)
    - P4 realizó POP del túnel MPLS-TE (7008 → 0): La etiqueta con valor 0 es reservada, ya que este le dice al enrutador de penúltimo salto que el realice la operación de retirar la etiqueta de transporte.
    - Explicit-Null: Etiqueta 0 indica que PE5 es el router de salida del túnel TE
    - P4 sabe que PE5 es el último LSR del túnel MPLS-TE, porque el router PE5 es el que le anuncia esta etiqueta al router P4.
2. Preservación de QoS
    - Exp bits: 3 mantenidos en la etiqueta 0
    - Transferencia de QoS: PE5 puede interpretar la QoS del túnel removido
3. Servicios Intactos
    - VPLS y VPN3: Etiquetas preservadas para procesamiento en PE5
    - Paquete IP: Completamente intacto

Jerarquía Actualizada

[Ethernet] → [IPv4-Explicit-Null: 0, Exp:3] → [VPLS: 9000] → [VPN3: 9002] → [IP Original]

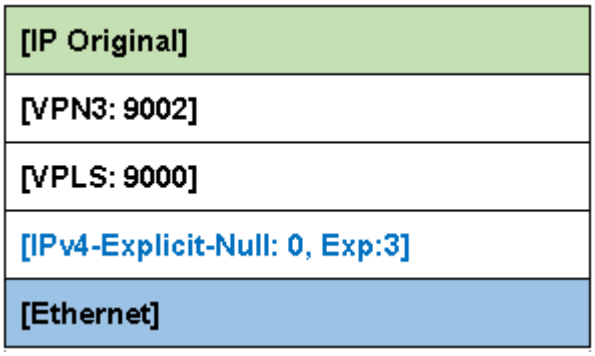


Figura 5.1.10 Pila de Etiquetas entre P4 y PE5

Entonces se puede decir que:

- El túnel de ingeniería de tráfico termina en PE5
- PE5 debe procesar las etiquetas de servicio restantes
- PHP evita que PE5 haga doble lookup (procesamiento).

5.1.6 Captura de Paquetes entre PE5 (eth2) y CE1-B (eth2)

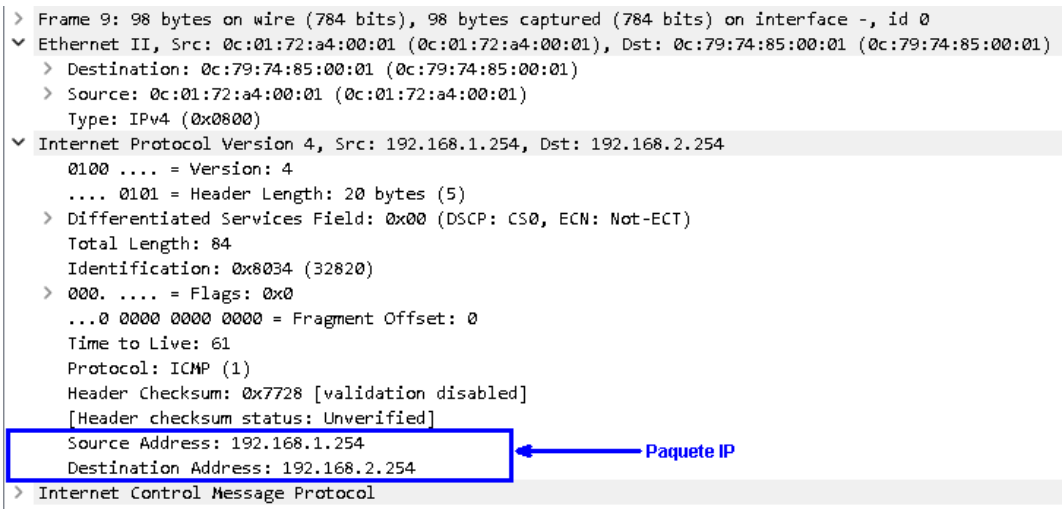


Figura 5.1.11 Captura de paquetes entre los enrutadores PE5 y CE1-B del Dominio IP

La desencapsulación completa en PE5 hacia CE1-B. Indica el análisis del ciclo completo de la formación del LSP (Label Switching Path):

Análisis del Frame 9: PE5 → CE1-B

Desencapsulación Completa

- Sin etiquetas MPLS, El tráfico vuelve a ser puro IPv4
- Tamaño: 98 bytes (igual al original en CE1-A)
- Tipo Ethernet: IPv4 (0x0800)

Capa IP Restaurada

- Src IP: 192.168.1.254 (CE1-A original)
- Dst IP: 192.168.2.254 (CE1-B destino)
- TTL: 61 (decrementado de 63 → 62 → 61)
- Protocolo: ICMP (ping original)

Capa Ethernet

- Src MAC: 0c:01:72:a4:00:01 (PE5)
- Dst MAC: 0c:79:74:85:00:01 (CE1-B)

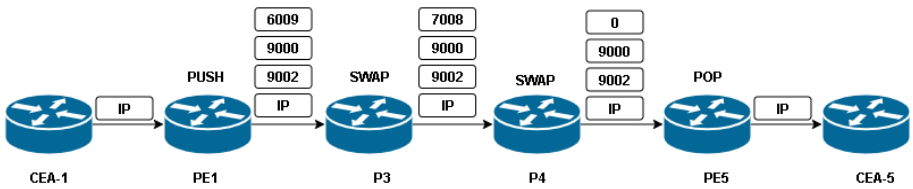


Figura 5.1.12 Trayectoria Completa del Paquete

El análisis con Wireshark nos permite detallar como RouterOS hace el tratamiento de la transmisión de paquetes IP sobre una infraestructura IP/MPLS con ingeniería de tráfico. Haciendo en análisis del recorrido del tráfico sobre la infraestructura implementada se puede llegar a verificar que el dato que ingresa desde el lado del usuario (CE1-A) son paquetes IP, los cuales al ingresar al dominio IP/MPLS son empaquetados por una pila de etiquetas. La etiqueta de transporte forma el túnel de ingeniería de tráfico que es el encargado de trasportar el tráfico del cliente, esta etiqueta es conmutada por cada router del core IP/MPLS en la ruta del túnel de ingeniería de tráfico. El análisis nos permite verificar que tenemos dos etiquetas de servicio una etiqueta de transporte, la etiqueta de servicio VPLS en RouterOS permite relacionar de manera automática hacia un túnel de ingeniería de tráfico, esto nos permite utilizar la ingeniería de tráfico para el transporte del servicio de L3VPN. Lo que nos genera un apilamiento de etiquetas formada por una etiqueta de transporte, y dos etiquetas de servicio(etiqueta VPLS, L3VPN), el

análisis nos permite verificar que la conmutación de las etiquetas de trasporte se da a través del protocolo RSVP-TE para su distribución en el core IP/MPLS , y la asignación de las etiquetas de servicio se da a través del protocolo MP-BGP que gracias a su versatilidad nos permite distribuir etiquetas de servicios para las VPNs implementadas en la topología de red. En la Figura 5.1.12 podemos verificar de mejor manera el comportamiento de la asignación de etiquetas y el transporte del tráfico del cliente.

Evolución de la pila de etiquetas:

1. CE1-A hacia PE1: El tráfico son paquetes IP.
2. PE1 hacia P3: Se verifica el apilamiento de etiquetas con la siguiente estructura [MPLS-TE:6009][VPLS:9000][VPN3:9002][IP] (128 bytes)
3. P3 hacia P4: Aquí se genera la conmutación de la etiqueta de transporte (túnel de ingeniería de tráfico), verificándose la siguiente estructura de la pila de etiquetas [MPLS-TE:7008, Exp:3][VPLS:9000][VPN3:9002][IP] (128 bytes)
4. P4 hacia PE5: Verificamos que aquí se aplica la operación de Penultime Hop Popping realizado por el router P4. La estructura del paquete seria tiene la siguiente estructura de pila de etiquetas PE5: [IPv4-Null:0, Exp:3][VPLS:9000][VPN3:9002][IP] (128 bytes)
5. PE5 hacia CE1-B: En este tramo del recorrido del tráfico el paquete IP del cliente se regenera con la siguiente estructura IPv4 puro (98 bytes).

El análisis del tráfico sobre el core IP/MPLS nos permite verificar las operaciones que se realizan en cada enrutador del recorrido del tráfico.

1. Router PE1, es el router de ingreso al dominio IP/MPLS la operación que realiza sobre las etiquetas es denominada PUSH, por el cual este enrutador utiliza el protocolo MP-BGP para asignar las etiquetas de servicio (Etiquetas 9000, 9002), y el protocolo RSVP-TE para la asignación de la etiqueta de transporte (Etiqueta 6009). Es el encargado de encapsular el paquete IP del cliente hacia el dominio IP/MPLS.
2. Router de tránsito P3: Se verifica que la operación sobre la etiqueta de transporte que realiza se denomina SWAP, cambiando la etiqueta 6009 por la etiqueta 7008, las etiquetas de servicio (9000, 9002) se mantienen sin ninguna modificación.
3. Router Penultime Hop Popping (P4): Se puede verificar que la operación sobre la etiqueta de transporte (7008) se denomina POP, lo que permite que el router del siguiente salto PE5 ya no realice la operación sobre esta etiqueta de transporte.
4. Router de egreso del dominio IP/MPLS (PE5): Verificamos que la operación que realiza este enrutador de borde se denomina POP, retirando todas las etiquetas tanto de servicio des encapsulando el paquete IP del cliente.

5.1.7 Generacion de Trafico para el Analisis de Rendimeinto

El Generador de Tráfico de MikroTik es una herramienta integrada en RouterOS, el sistema operativo de los dispositivos MikroTik. Su función principal es la de simular y generar flujos de tráfico de red con características específicas, en el presente trabajo nos permitira probar el comportamiento de la topologia de red implementada bajo un escenario con trafico Generico, Multicast y Telefonia IP. A diferencia de una simple prueba de ancho de banda el Generador de Tráfico ofrece un control mucho más granular sobre los parámetros del tráfico generado.

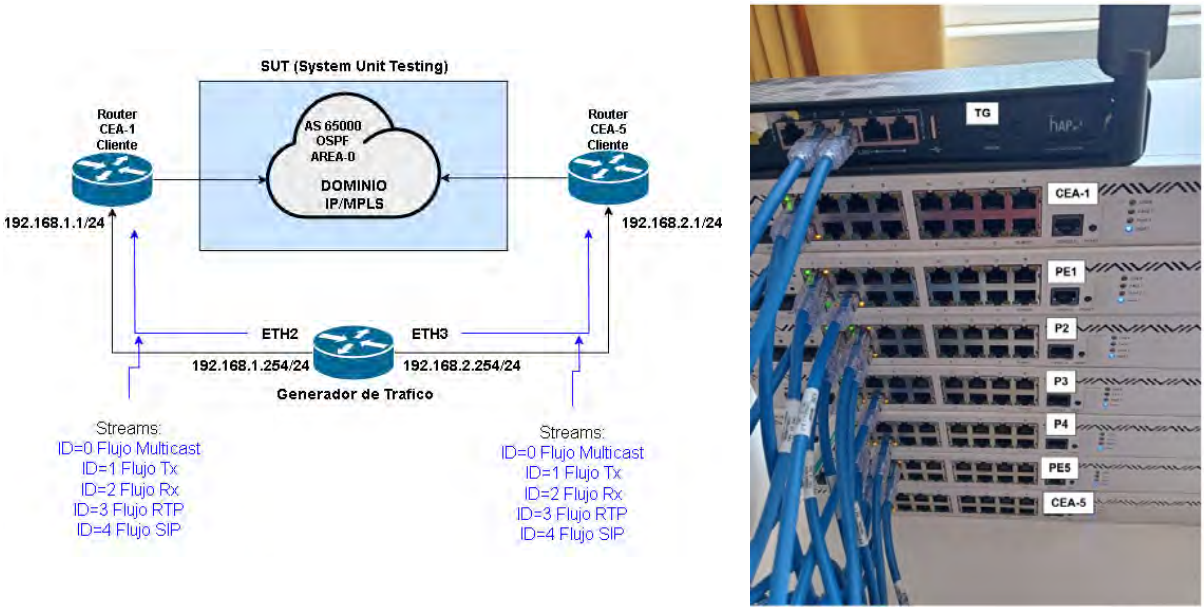
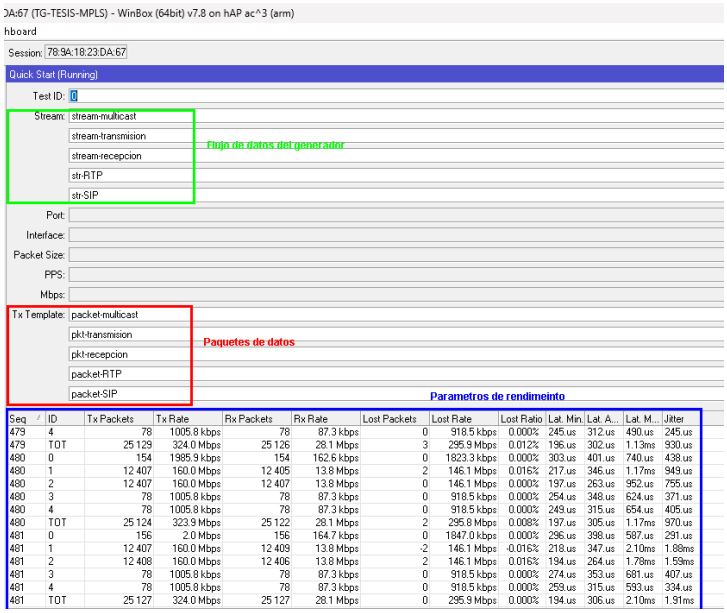


Figura 5.1.13 Generacion de flujos de tráfico para VPN3



```
[admin@TG-TESIS-MPLS] > tool/traffic-generator/packet-template/print
 0 name="packet-multicast" header-stack=mac,ip,udp assumed-port=dynamic0 assumed-interface=ether2 assumed-mac-src=78:9A:18:23:DA:65 assumed-mac-dst=78:9A:18:A9:DC:B8
   assumed-mac-protocol=ip assumed-ip-dscp=0 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-src=192.168.1.254 ip-dst=239.1.1.10 ip-protocol=pim
   ip-gateway=192.168.1.1 udp-src-port=5004 udp-dst-port=5004 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks="" random-ranges=""
   special-footer=yes compute-checksum-from-offset=no-checksum

 1 name="pkt-transmision" header-stack=mac,ip,udp assumed-port=dynamic0 assumed-interface=ether2 assumed-mac-src=78:9A:18:23:DA:65 assumed-mac-dst=78:9A:18:A9:DC:B8
   assumed-mac-protocol=ip assumed-ip-dscp=0 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-src=192.168.1.254 ip-dst=192.168.2.254 ip-gateway=192.168.1.1
   assumed-ip-protocol=udp assumed-udp-src-port=100 assumed-udp-dst-port=200 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks=""
   random-ranges="" special-footer=yes compute-checksum-from-offset=no-checksum

 2 name="packet-RTP" header-stack=mac,ip,udp assumed-port=dynamic0 assumed-interface=ether2 assumed-mac-src=78:9A:18:23:DA:65 assumed-mac-dst=78:9A:18:A9:DC:B8
   assumed-mac-protocol=ip ip-dscp=184 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-dst=192.168.2.254 ip-protocol=udp ip-gateway=192.168.1.1
   assumed-ip-src=192.168.1.254 udp-dst-port=16384-32767 assumed-udp-src-port=100 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks=""
   random-ranges="" special-footer=yes compute-checksum-from-offset=no-checksum

 3 name="packet-SIP" header-stack=mac,ip,udp assumed-port=dynamic0 assumed-interface=ether2 assumed-mac-src=78:9A:18:23:DA:65 assumed-mac-dst=78:9A:18:A9:DC:B8
   assumed-mac-protocol=ip ip-dscp=104 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-dst=192.168.2.254 ip-protocol=udp ip-gateway=192.168.1.1
   assumed-ip-src=192.168.1.254 udp-dst-port=5060,5061 assumed-udp-src-port=100 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks=""
   random-ranges="" special-footer=yes compute-checksum-from-offset=no-checksum

 4 name="pkt-recepcion" header-stack=mac,ip,udp assumed-port=dynamic1 assumed-interface=ether3 assumed-mac-src=78:9A:18:23:DA:66 assumed-mac-dst=D4:01:C3:2B:1C:06
   assumed-mac-protocol=ip assumed-ip-dscp=0 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-src=192.168.2.254 ip-dst=192.168.1.254 ip-gateway=192.168.2.1
   assumed-ip-protocol=udp assumed-udp-src-port=100 assumed-udp-dst-port=200 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks=""
   random-ranges="" special-footer=yes compute-checksum-from-offset=no-checksum
[admin@TG-TESIS-MPLS] >
```

Figura 5.1.14 Paquetes y Streams del Generador de Trafico

```
[admin@TG-TESIS-MPLS] > tool/traffic-generator/export
# jan/02/1970 00:32:26 by RouterOS 7.8
# software id = 9KDZ-DQSR
#
# model = RBD53iG-5HacD2HnD
# serial number = HET09BDA4HN
/tool traffic-generator packet-template
add ip-dst=239.1.1.10 ip-gateway=192.168.1.1 ip-protocol=pim ip-src=192.168.1.254 name=packet-multicast udp-dst-port=5004 udp-src-port=5004
add ip-dst=192.168.2.254 ip-gateway=192.168.1.1 ip-src=192.168.1.254 name=pkt-transmision
add ip-dscp=184 ip-dst=192.168.2.254 ip-gateway=192.168.1.1 ip-protocol=udp name=packet-RTP udp-dst-port=16384-32767
add ip-dscp=104 ip-dst=192.168.2.254 ip-gateway=192.168.1.1 ip-protocol=udp name=packet-SIP udp-dst-port=5060,5061
add ip-dst=192.168.1.254 ip-gateway=192.168.2.1 ip-src=192.168.2.254 name=pkt-recepcion
/tool traffic-generator stream
add mbps=2 name=stream-multicast packet-size=1612 tx-template=packet-multicast
add id=1 mbps=160 name=stream-transmision packet-size=1612 tx-template=pkt-transmision
add id=2 mbps=160 name=stream-recepcion packet-size=1612 tx-template=pkt-recepcion
add id=3 mbps=1 name=str-RTP packet-size=1612 tx-template=packet-RTP
add id=4 mbps=1 name=str-SIP packet-size=1612 tx-template=packet-SIP
[admin@TG-TESIS-MPLS] >
```

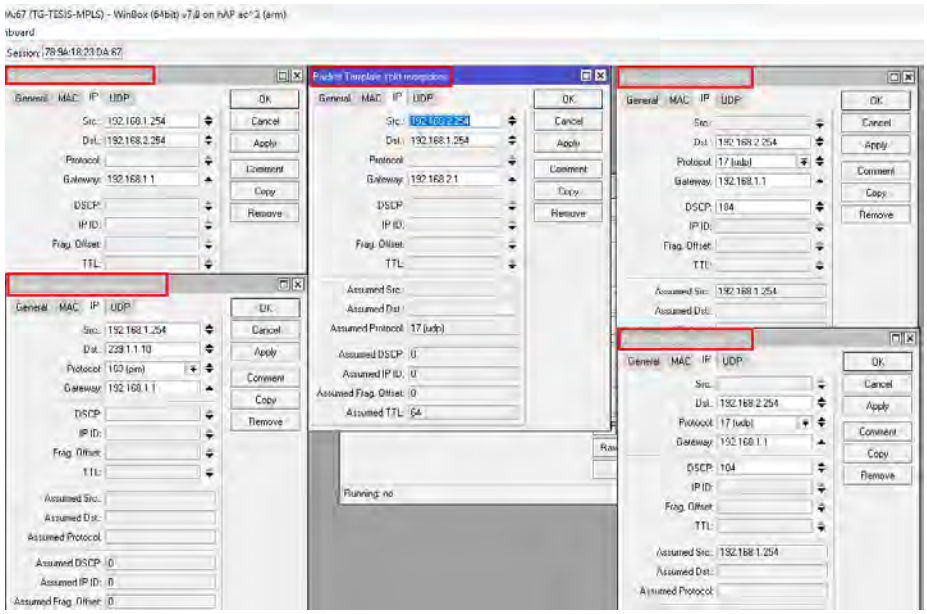


Figura 5.1.15 Características de los paquetes

```
[admin@TG-TESIS-MPLS] > tool/traffic-generator/stream/export
# jan/02/1970 00:38:40 by RouterOS 7.8
# software id = 9KDZ-DQSR
#
# model = RBD53iG-5HacD2HnD
# serial number = HET09BDA4HN
/tool traffic-generator stream
add mbps=2 name=stream-multicast packet-size=1612 tx-template=packet-multicast
add id=1 mbps=160 name=stream-transmision packet-size=1612 tx-template=pkt-transmision
add id=2 mbps=160 name=stream-recepcion packet-size=1612 tx-template=pkt-recepcion
add id=3 mbps=1 name=str-RTP packet-size=1612 tx-template=packet-RTP
add id=4 mbps=1 name=str-SIP packet-size=1612 tx-template=packet-SIP
[admin@TG-TESIS-MPLS] >
```

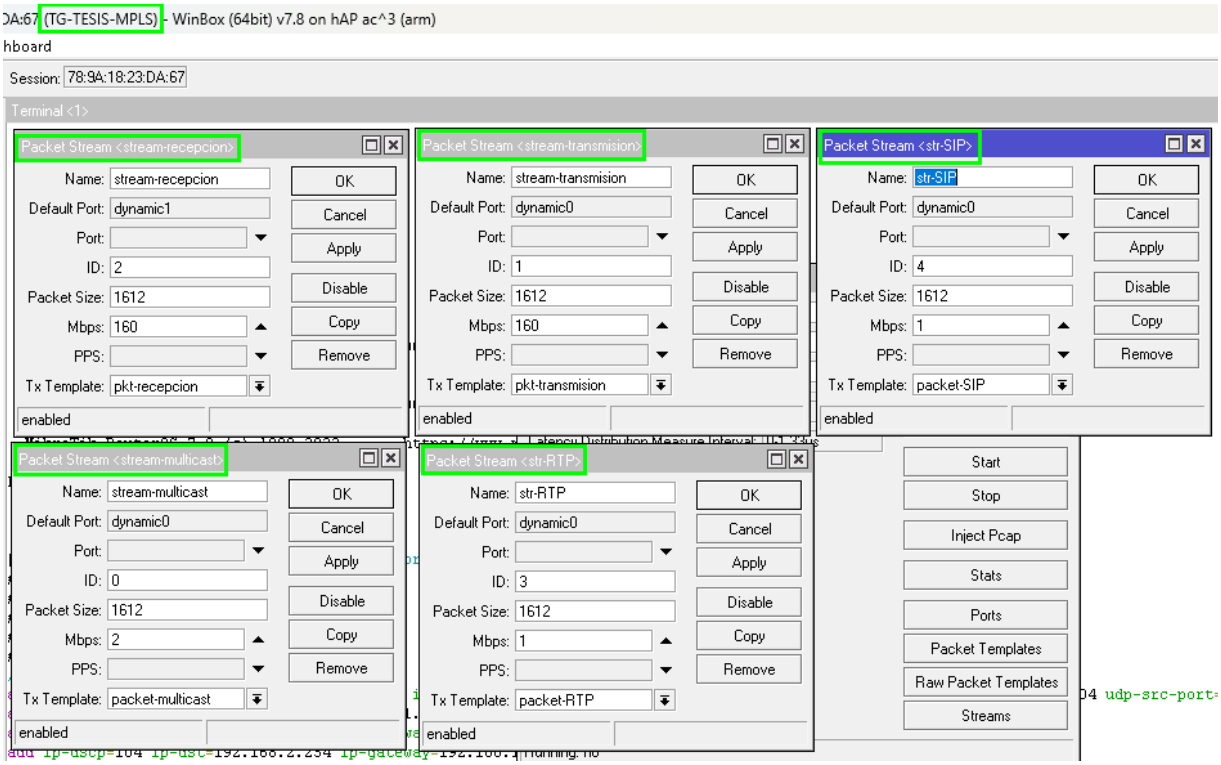


Figura 5.1.16 Características de los Streams

5.1.8 Recorrido del Paquetes a Traves del Tunel TE.

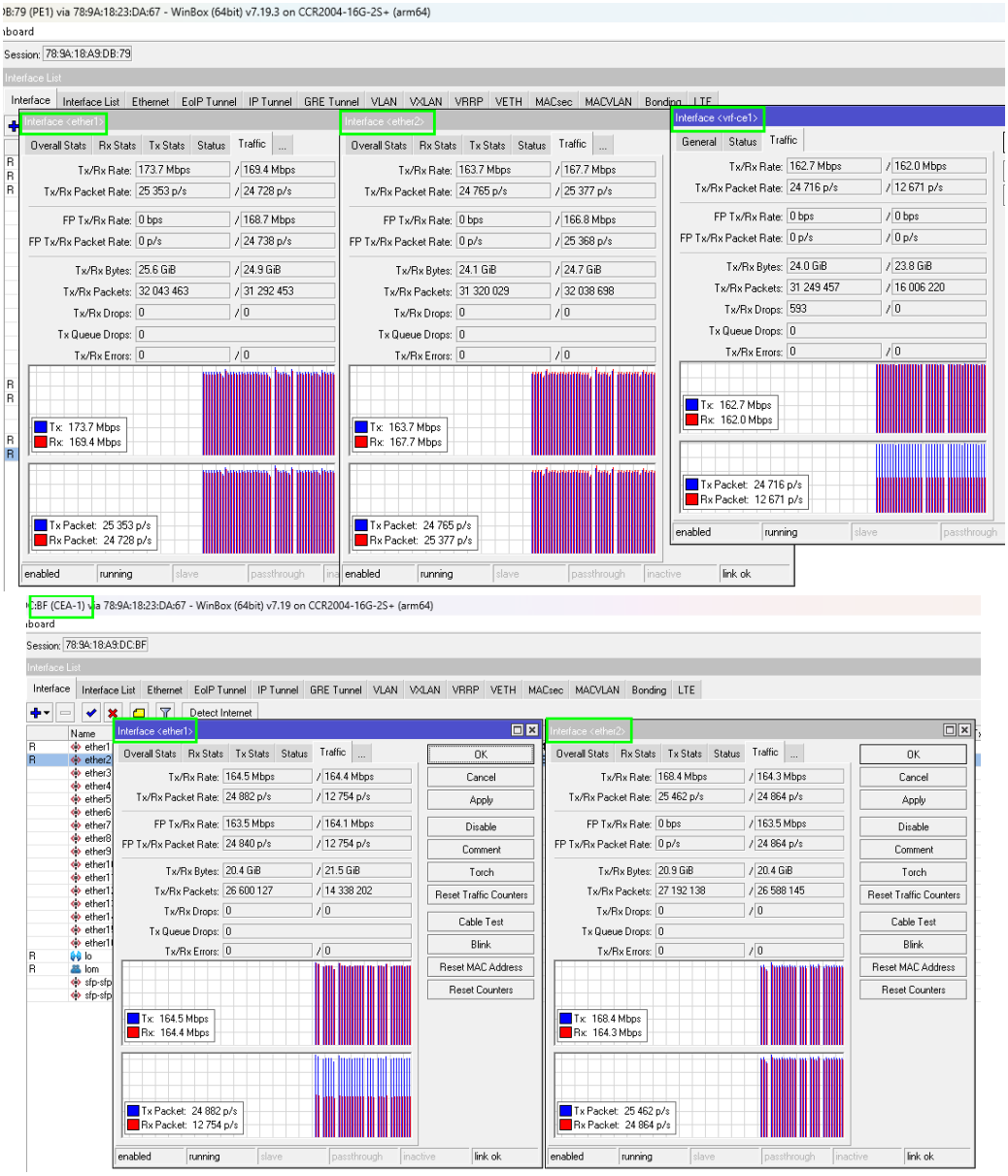


Figura 5.1.17 Ancho de banda en las interfaces de CEA-1 y PE-1

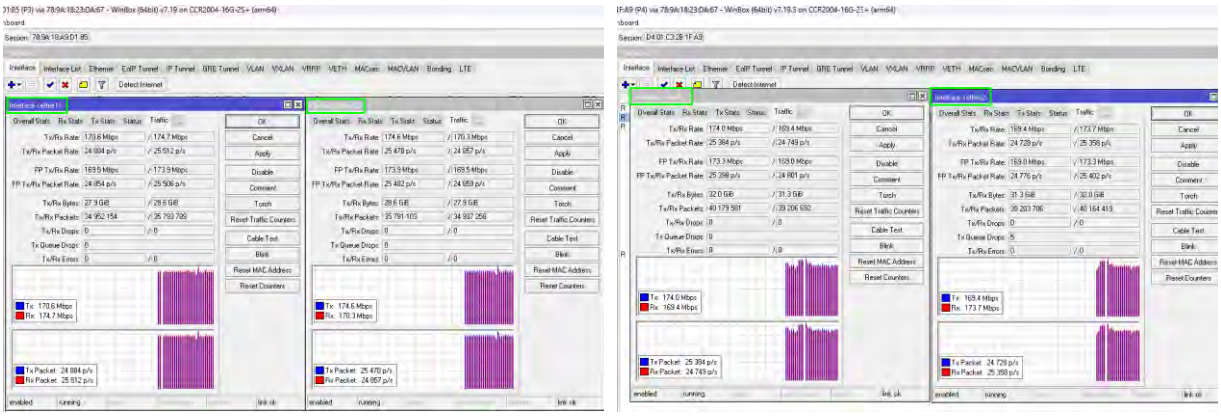
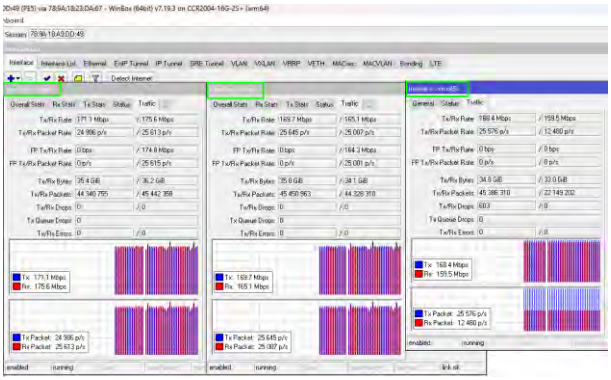
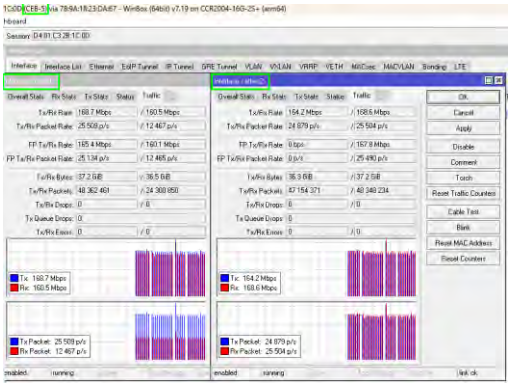


Figura 5.1.18 Ancho de banda en las interfaces de P3 y P4

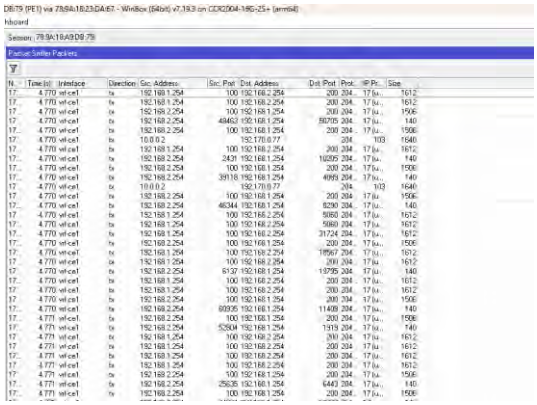


Trafico a traves de ether1, ether2 de PE-5

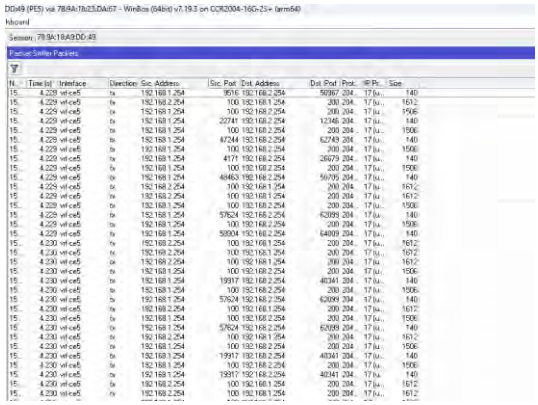


Trafico a traves de ether2, ether1 de CEA5

Figura 5.1.19 Ancho de banda en las interfaces de PE-5 y CEB-5



a) Captura de paquetes en las interfaz vrf-ce1 en PE-1



b) Captura de paquetes en las interfaz vrf-ce5 en PE-5

Figura 5.1.20 Captura de paquetes sobre PE-1 y PE-5

5.2 Análisis de Rendimiento VPN L3

El objetivo es evaluar el desempeño de la red en términos de delay (latencia promedio), packet loss (pérdida de paquetes), jitter, MOS (Mean Opinion Score) e ICPIF (Impairment Calculated Planning Impairment Factor) para cada tipo de tráfico (Multicast, RTP, SIP, Rx, Tx). La generación de los diferentes tipos de tráfico es mediante la herramienta Generador de tráfico de RouterOS de Mikrotik implementando los siguientes flujos de datos.

- **ID=0**: Tráfico multicast
- **ID=1**: Tráfico de transmisión (Tx)
- **ID=2**: Tráfico de recepción (Rx)
- **ID=3**: Tráfico RTP
- **ID=4**: Tráfico SIP

La figura 5.2.1 muestra topología implementada conectado al generador de tráfico.

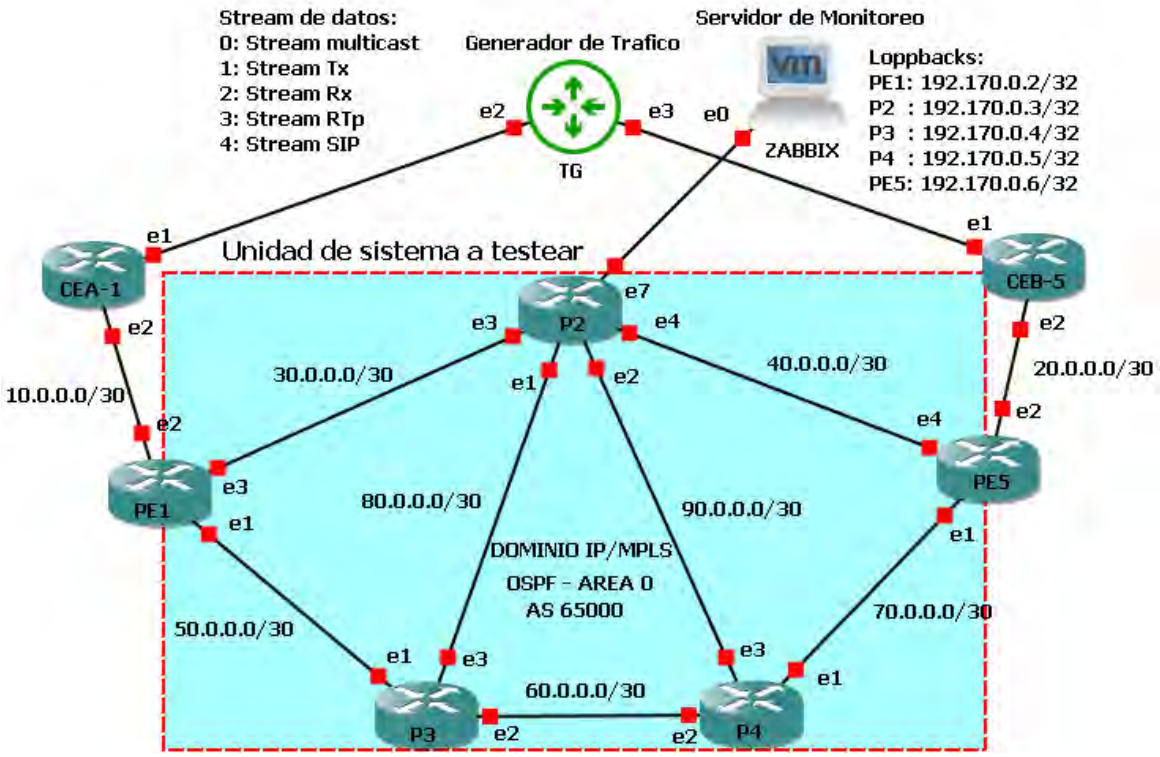


Figura 5.2.1 Topología de red con generador de trafico

El flujo de datos multicast implementado en la red hace uso del protocolo PIM-SM que viene implementado en el sistema operativo de RouterOS. Esto debido a que en una topologia de VPN L3 la comunicación entre usuario y el dominio IP/MPLS se da a nivel de capa 3 (enrutamiento), y PIM-SM es el protocolo de enrutamiento a nivel de capa 3 para trafico multicast.

Un generador de trafico es una herramienta que permite evaluar el rendimiento de un DUT(Device Under Test) o SUT (System Under Test). Nuestro sistema a probar sera el servicio VPN L3 sobre una red IP/MPLS, para lo cual se ha conectado el generador de trafico a traves de su puerto ether2 hacia el puerto ether1 del router CEA-1 y el puerto ether3 del generador de trafico hacia el puerto ether1 del router CEA-5. Mayor referencia en la figura 5.2.1

El generador de trafico de Mikrotik version 7, en puertos especificos permite generar flujos de datos de diferentes caracteristicas (pim, udp, tcp, etc.). Permite tambien exportar valores de red como la latencia y jitter, tasas de transmision y recepcion, perdida de paquetes, que luego seran procesados para su análisis e interpretación.

5.2.1 Consideraciones para Análisis de Rendimiento del SUT

- El ancho de banda del SUT sera de 200 Mbps.
- Generacion de traficos de 160 Mbps, 200 Mbps y 250 Mbps.
- Implementacion de SUT con calidad de servicio (QoS).
- Implementacion de SUT sin calidad de servicio (QoS).

Para identificar diferentes problemas en cada tipo de tráfico compararemos con métricas con umbrales, donde:

- Latencia promedio > 150 ms
- Jitter promedio > 30 ms
- Pérdida de paquetes > 1%
- MOS < 3.5
- ICPIF > 20

MOS (mean opinión score), Es una métrica utilizada para evaluar la calidad de servicios de voz y video, como las llamadas de VoIP, se califica en una escala de 1 a 5, donde 5 es la mejor calidad. Para el cálculo se utiliza la version simplificada del modelo E (ITU-T G.107) basado en latencia, jitter y perdida de paquetes.

ICPIF (Calculated Planning Impairment Factor) Es una métrica utilizada para medir y cuantificar los efectos de diversas deficiencias en la calidad de la voz, especialmente en redes de Voz sobre protocolo de internet (VoIP). El valor ICPIF representa el impacto general de problemas de red como el retardo y la perdida de paquetes en la experiencia del usuario. El cálculo está basado en el estándar ITU-T G.113, que considera la latencia, jitter y perdida de paquetes. Valores < 10 indican buena calidad, > 20 indican problemas.

5.2.2 Análisis de Rendimiento para Tráfico de 160 Mbps

Tabla 5.2.1 Reporte de parámetros de rendimiento para tráfico de 160 Mbps con QoS

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	Bytes Perdidos	MOS	ICPIF
Multicast	0.31	0.21	0	0	0	0
Rx	0.23	0.88	5.79	1.01	0	0
Tx	0.21	0.78	4.31	0.74	0	0
RTP	0.23	0.21	0	0	4.41	10.01
SIP	0.21	0.21	0	0	4.41	10.01

Tabla 5.2.2 Reporte de parámetros de rendimiento para tráfico de 160 Mbps sin QoS

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	Bytes Perdidos	MOS	ICPIF
Multicast	0.32	0.17	0.31	0.76	0	0
Rx	0.23	0.83	6.72	1.19	0	0
Tx	0.21	0.64	6.85	1.21	0	0
RTP	0.23	0.16	0.07	0.09	4.14	20.01
SIP	0.22	0.12	0.02	0.03	4.14	20.01

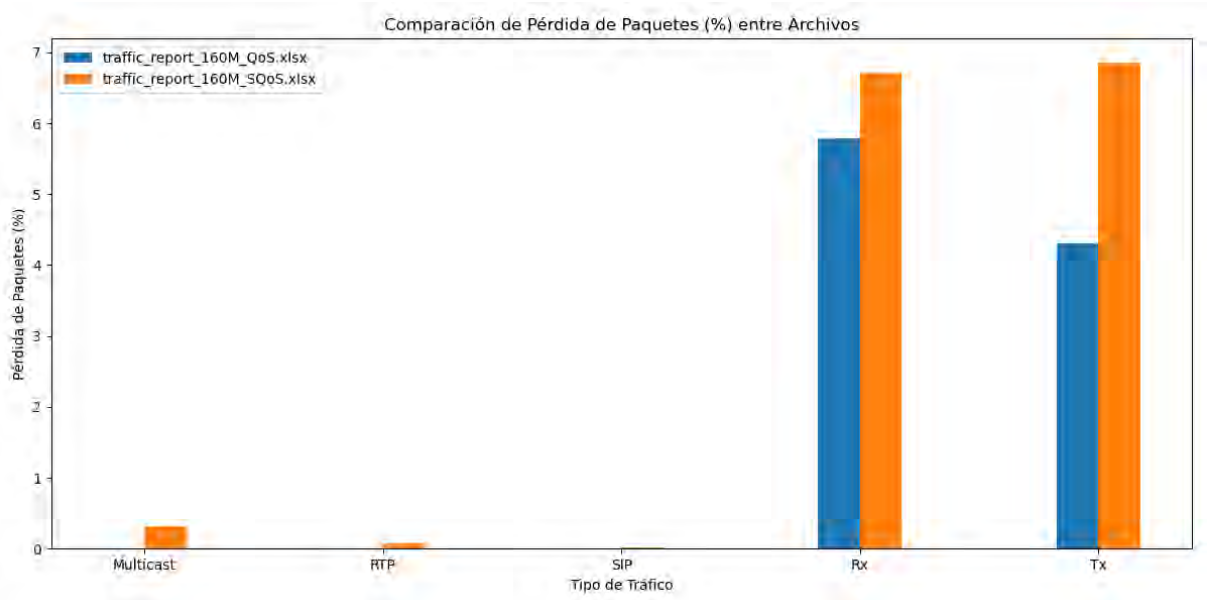
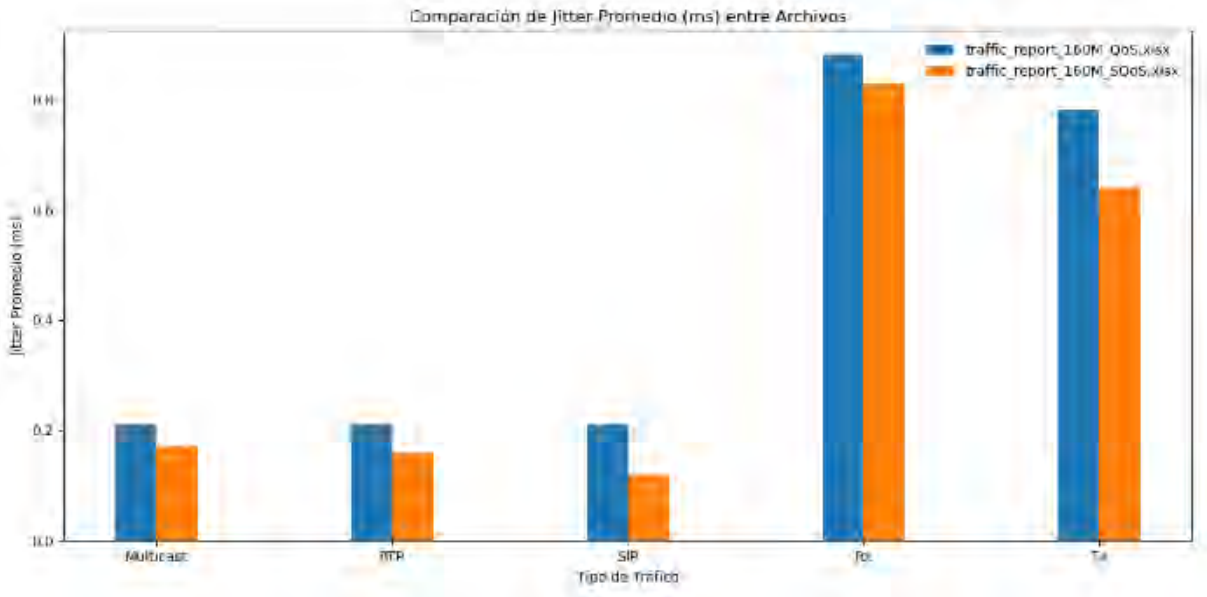


Figura 5.2.2 Parámetro de perdida de paquetes para 160 Mbps



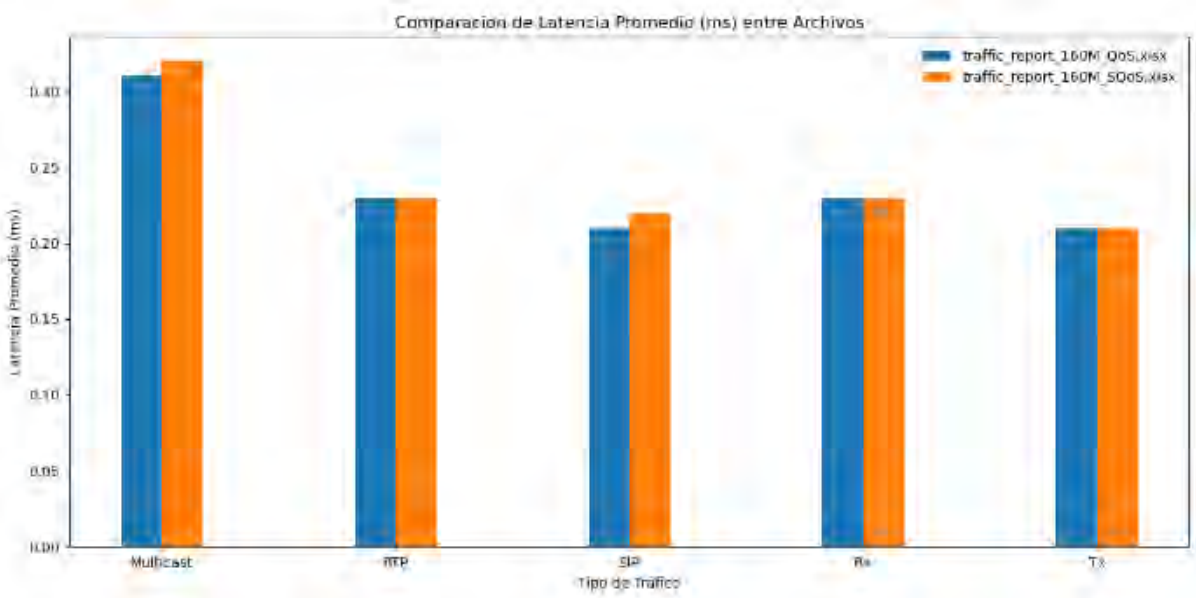
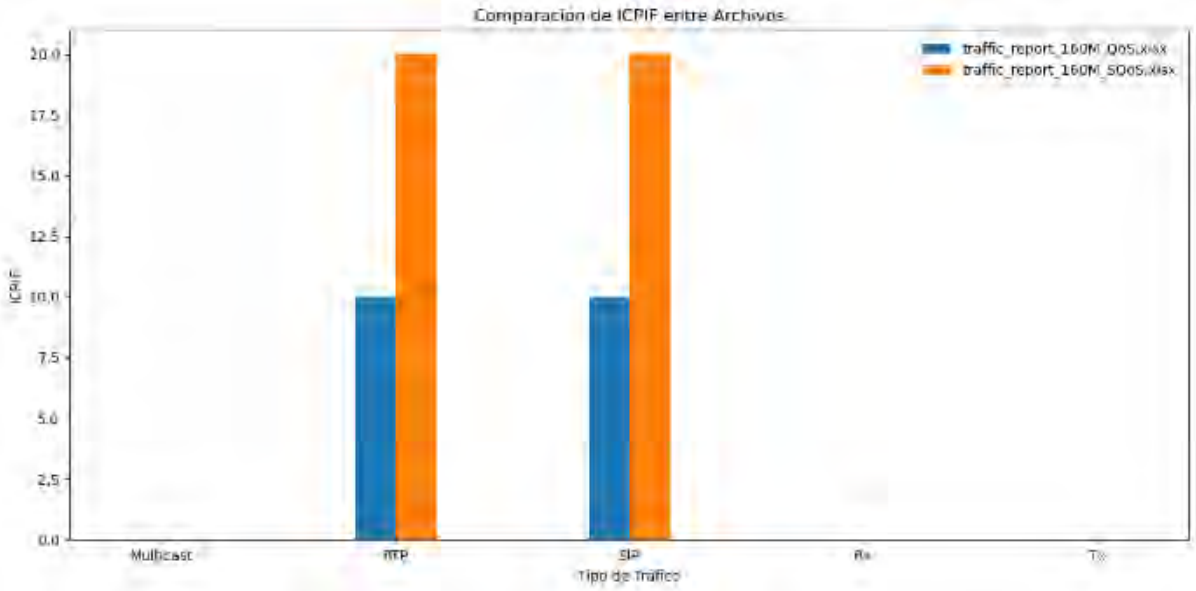


Figura 5.2.3 Parámetros, Jitter, Latencia



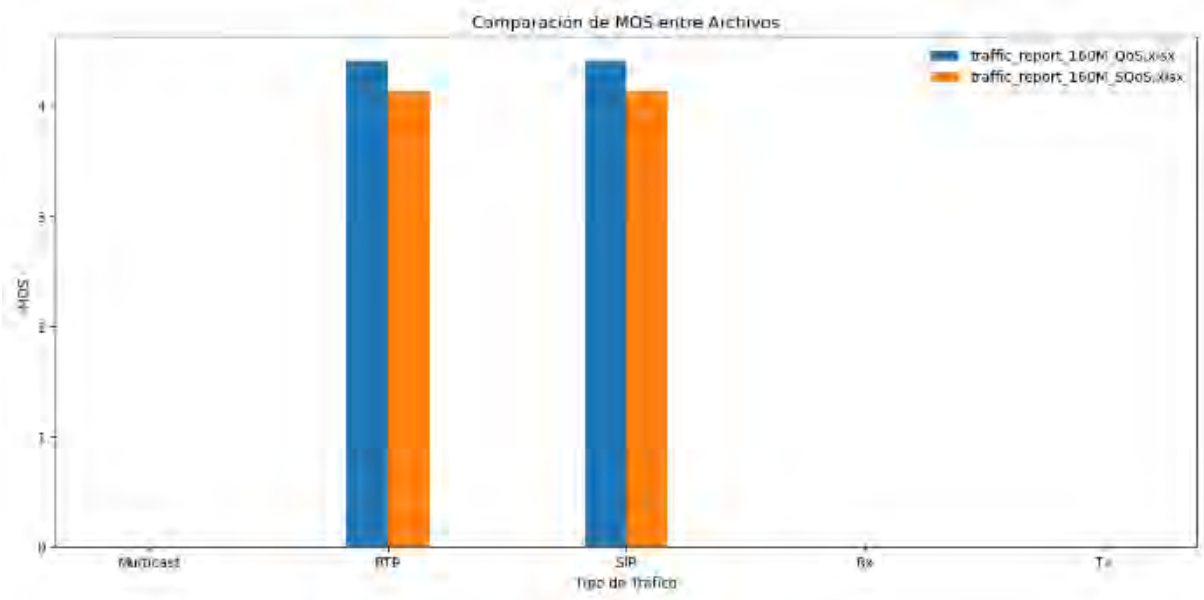


Figura 5.2.4 Parámetros ICPIF, MOS

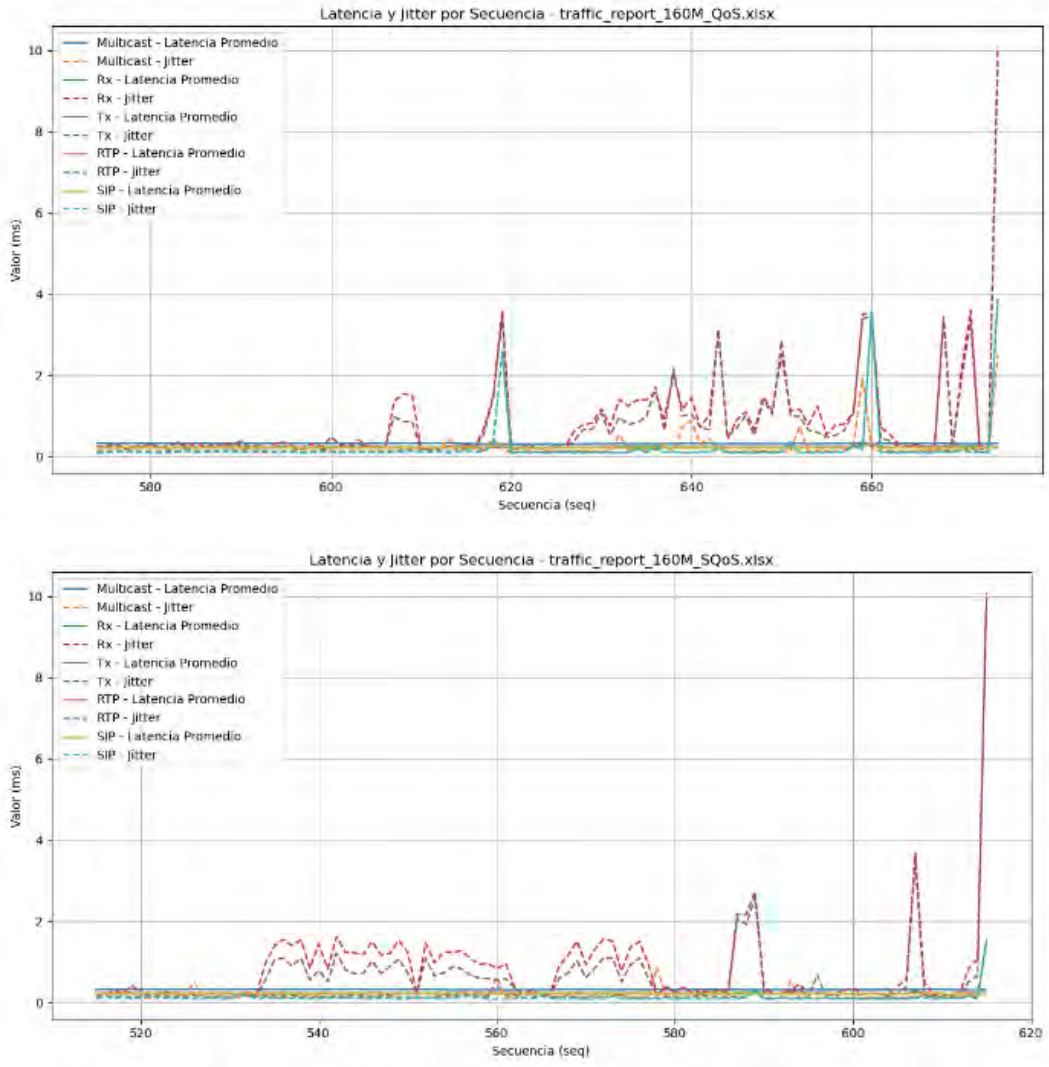


Figura 5.2.5 Grafica lineal de parámetros de rendimiento

- Se puede verificar del análisis de tráfico la generación de tablas y graficas comparativas para tráfico de 160 Mbps con y sin calidad de servicio, donde los parámetros a evaluar son métricas de tasa de Tx/Rx, perdida de paquetes, latencia, jitter, MOS e ICPIF, que nos permite evaluar el rendimiento de la red implementada, el cual transporta tráficos generadas por un generador de tráfico de red.
- Las tablas muestran métricas de rendimiento de red para tráficos con y sin calidad de servicio. La tabla 5.2.1 (tráfico de 160 Mbps con calidad de servicio) nos muestra que los parámetros de rendimiento están por debajo de los umbrales críticos de funcionamiento descrito en la sección 5.2.1 con lo que podemos concluir que el tráfico será optimo y estable. La métrica de MOS tiene el valor de 4.41 tanto para tráfico RTP y SIP, pero tenemos valores de 0 para tráfico Multicast y tráfico genérico. El valor de la métrica ICPIF está por debajo del valor umbral de 20 lo que indica que son valores adecuados para los diferentes tipos de tráfico que viajan por la red.
- Las tablas muestran métricas de rendimiento de red para tráficos con y sin calidad de servicio. La tabla 5.2.2 (tráfico de 160 Mbps sin calidad de servicio) nos muestra que los parámetros de rendimiento están por debajo de los umbrales críticos de funcionamiento descrito en la sección 5.2.1 con lo que podemos concluir que el tráfico será optimo y estable. La métrica de MOS tiene el valor de 4.14 tanto para tráfico RTP y SIP, pero tenemos valores de 0 para tráfico Multicast y trafico genérico. El valor de la métrica ICPIF está por debajo del valor umbral de 20 lo que indica que son valores adecuados para los diferentes tipos de tráfico que viajan por la red.
- En las tablas y graficas se verifica que el rendimiento de la red está directamente relación a la calidad de servicio que se aplica a cada tipo de tráfico (VoIP, Multicast y Genérica). El tráfico con calidad de servicio muestra un mejor rendimiento para los diferentes tipos de tráfico.

5.2.3 Análisis de Rendimiento para Tráfico de 200 Mbps

Tabla 5.2.3 Parámetros de rendimiento con QoS para 200Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	Bytes Perdidos	MOS	ICPIF
Multicast	0.31	0.22	0	0	0	0
Rx	0.23	0.88	5.56	1.21	0	0
Tx	0.21	0.87	4.65	1.01	0	0
RTP	0.22	0.2	0	0	4.41	10.01
SIP	0.21	0.2	0	0	4.41	10.01

Tabla 5.2.4 Parámetros de rendimiento sin QoS para 200Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	Bytes Perdidos	MOS	ICPIF
Multicast	0.73	0.55	1.42	3.33	0	0
Rx	0.64	1.39	982.47	234.86	0	0
Tx	0.22	0.91	4.73	1.01	0	0
RTP	0.69	0.5	10.81	13.22	3.51	35
SIP	0.69	0.47	13.34	16.38	3.51	35

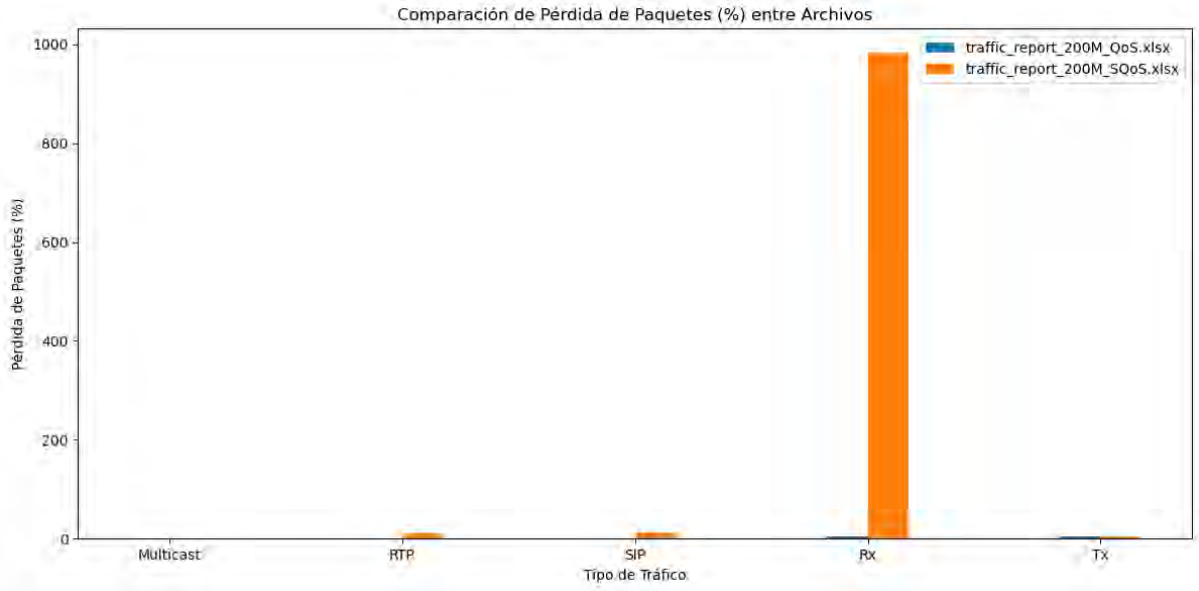
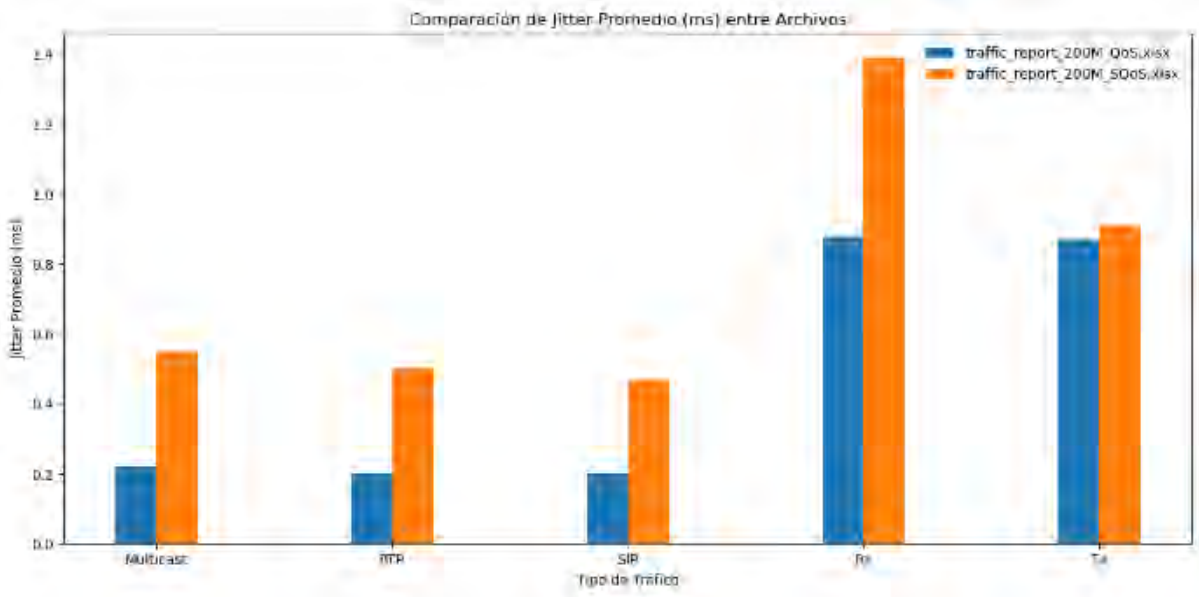


Figura 5.2.6 Parámetro de perdida de paquetes para 200 Mbps



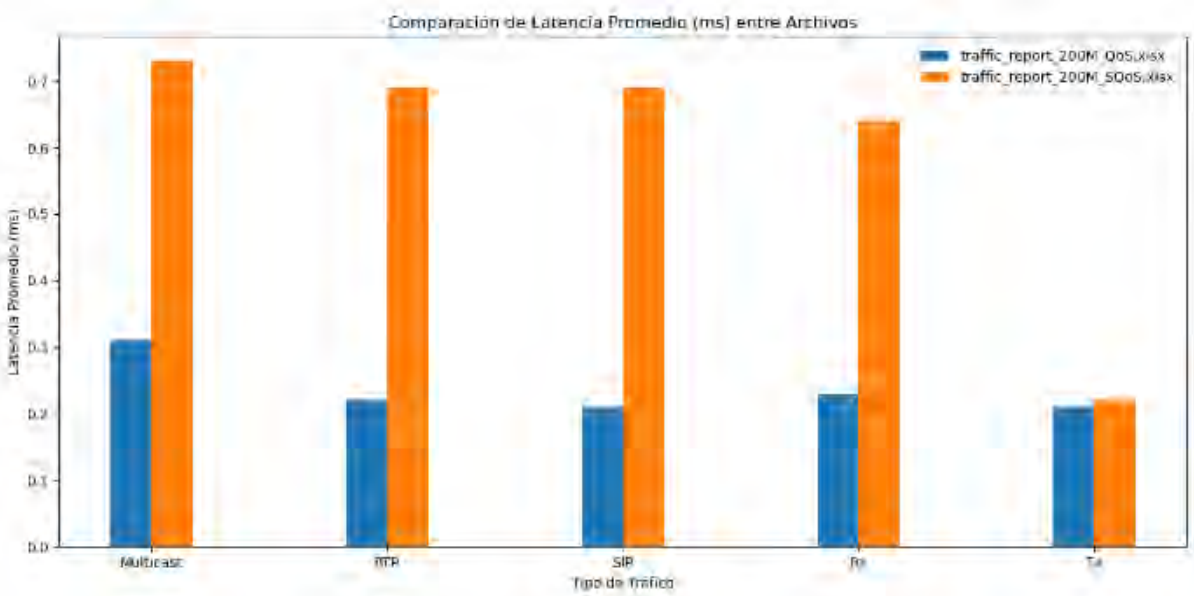


Figura 5.2.7 Parámetros, Jitter, Latencia

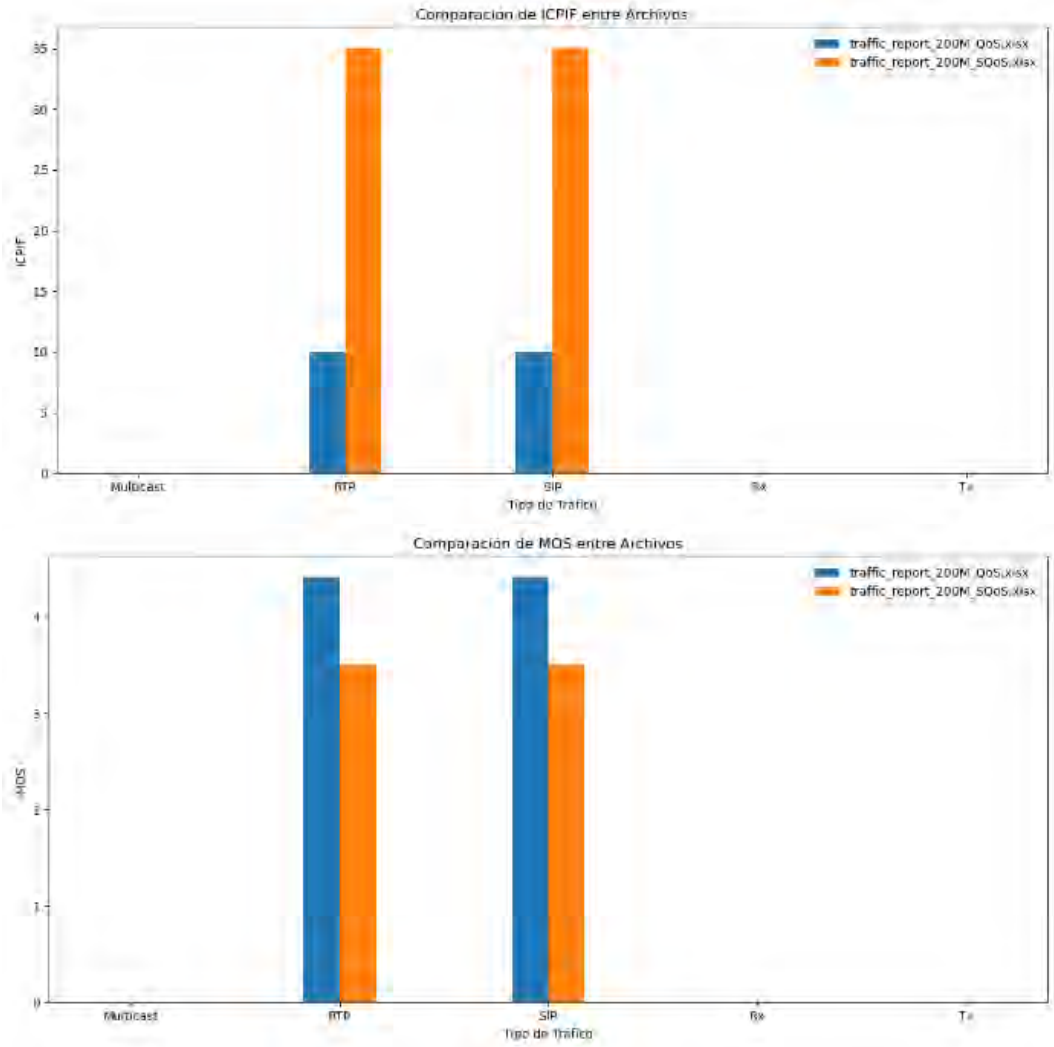


Figura 5.2.8 Parámetros ICPIF, MOS

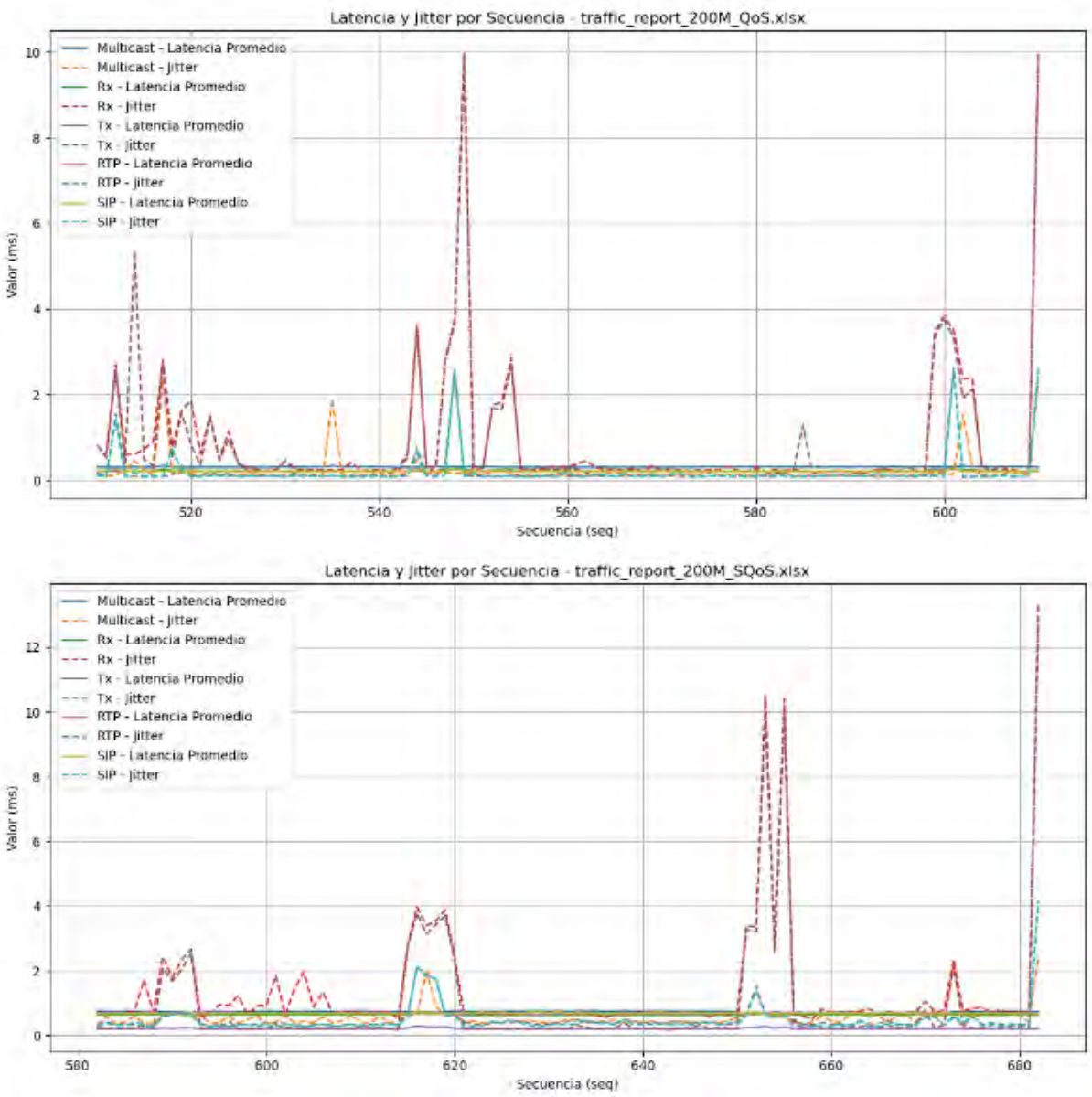


Figura 5.2.9 Grafica lineal de parámetros de rendimiento

- Se puede verificar del análisis de tráfico la generación de tablas y graficas comparativas para tráfico de 200 Mbps con y sin calidad de servicio, donde los parámetros a evaluar son métricas de tasa de Tx/Rx, perdida de paquetes, latencia, jitter, MOS e ICPIF, que nos permite evaluar el rendimiento de la red implementada, el cual transporta tráficos generadas por un generador de tráfico de red.
- Las tablas muestran métricas de rendimiento de red para tráficos con y sin calidad de servicio. La tabla 5.2.3 (tráfico de 200 Mbps con calidad de servicio) nos muestra que los parámetros de rendimiento están por debajo de los umbrales críticos de funcionamiento descrito en la sección 5.2.1 con lo que podemos concluir que el tráfico será optimo y estable. La métrica de MOS tiene el valor de 4.41 tanto para tráfico RTP

y SIP, pero tenemos valores de 0 para tráfico Multicast y trafico genérico. El valor de la métrica ICPIF está por debajo del valor umbral de 20 lo que indica que son valores adecuados para los diferentes tipos de tráfico que viajan por la red.

- Las tablas muestran métricas de rendimiento de red para tráficos con y sin calidad de servicio. La tabla 5.2.4 (tráfico de 200 Mbps sin calidad de servicio) nos muestra que los parámetros de rendimiento están por debajo de los umbrales críticos de funcionamiento descrito en la sección 5.2.1 con lo que podemos concluir que el tráfico será optimo y estable. La métrica de MOS tiene el valor de 3.51 tanto para tráfico RTP y SIP, pero tenemos valores de 0 para tráfico Multicast y trafico genérico. El valor de la métrica ICPIF está por debajo del valor umbral de 20 lo que indica que son valores adecuados para los diferentes tipos de tráfico que viajan por la red.
- En las tablas y graficas se verifica que el rendimiento de la red está directamente relación a la calidad de servicio que se aplica a cada tipo de tráfico (VoIP, Multicast y Genérica). El tráfico con calidad de servicio muestra un mejor rendimiento para los diferentes tipos de tráfico.

5.2.4 Análisis de Rendimiento para Tráfico de 250 Mbps

Tabla 5.2.5 Parámetros de rendimiento con QoS para 250Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	Bytes Perdidos	MOS	ICPIF
Multicast	0.33	0.22	0.01	0.03	0	0
Rx	0.73	1.64	19.81	5.94	0	0
Tx	0.22	1.06	8.05	2.24	0	0
RTP	0.25	0.28	0	0	4.41	10.01
SIP	0.24	0.27	0	0	4.41	10.01

Tabla 5.2.6 Parámetros de rendimiento sin QoS para 250Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	Bytes Perdidos	MOS	ICPIF
Multicast	0.81	0.42	30.23	74.98	0	0
Rx	0.73	1.28	20.07	6	0	0
Tx	0.21	0.79	15.11	3.13	0	0
RTP	0.75	0.32	31.71	39.24	3.51	35.02
SIP	0.75	0.32	33.32	41.24	3.51	35.02

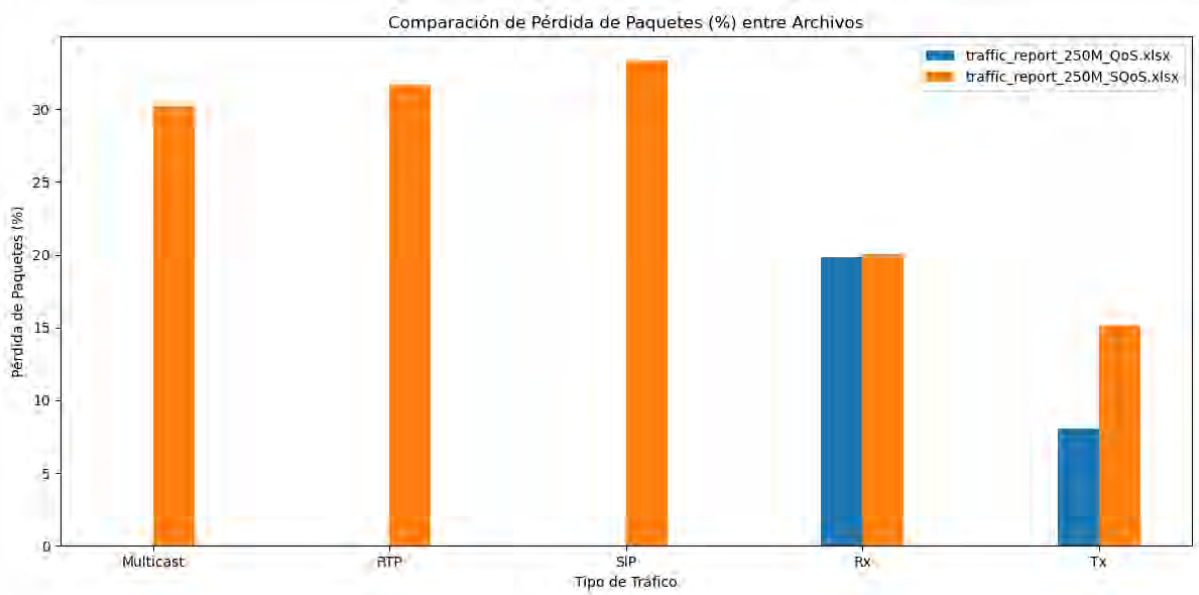
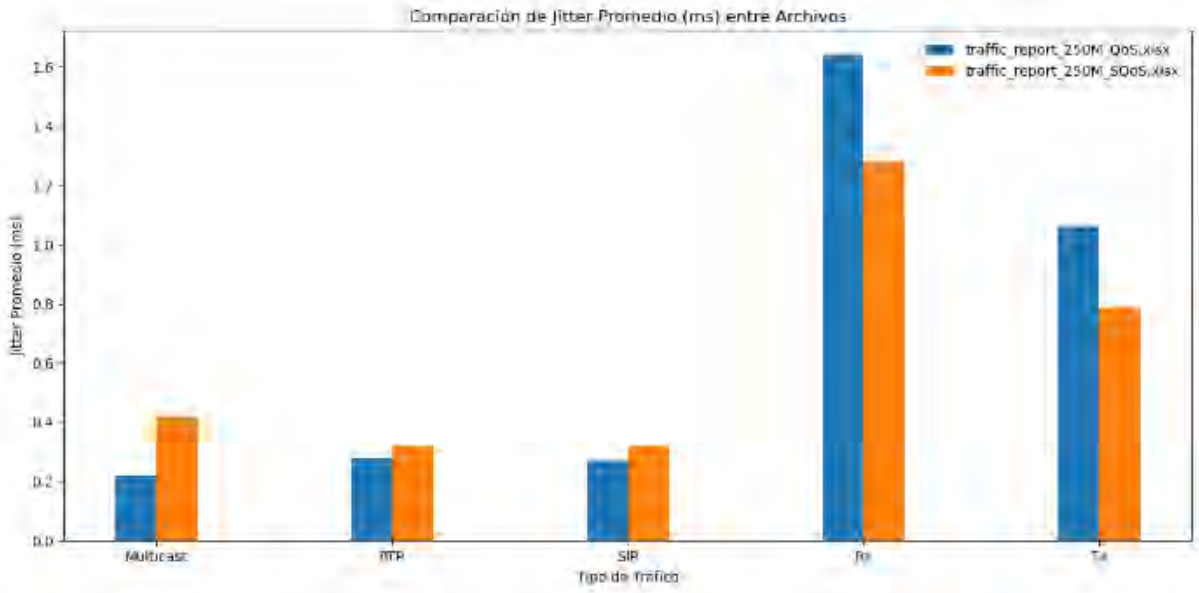


Figura 5.2.10 Parámetro de perdida de paquetes para 250 Mbps



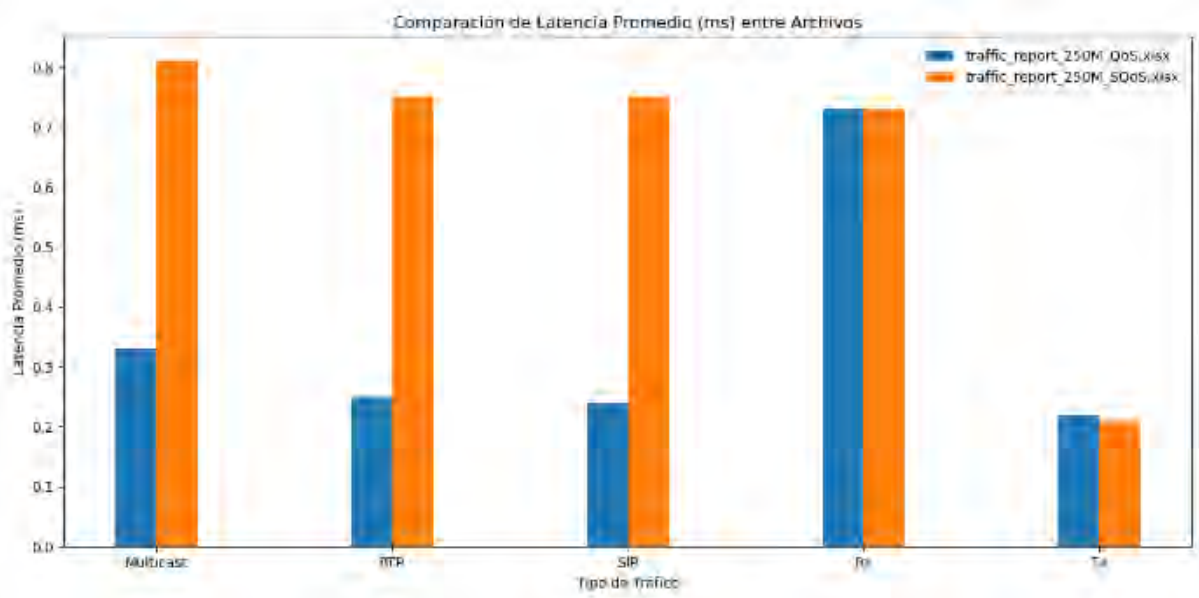
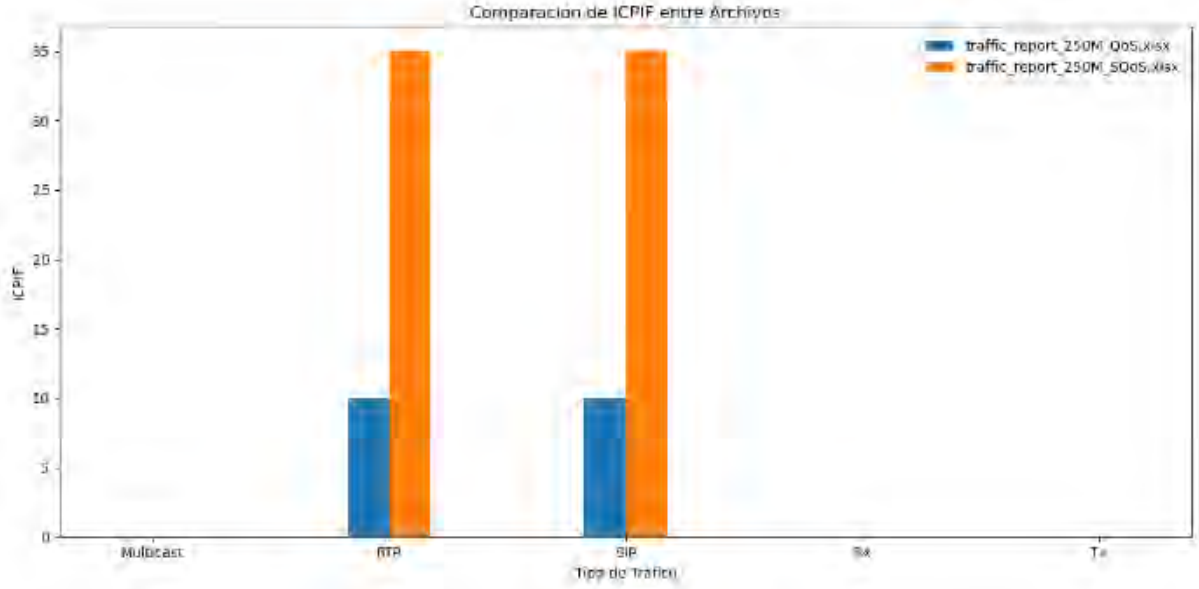


Figura 5.2.11 Parámetros, Jitter, Latencia



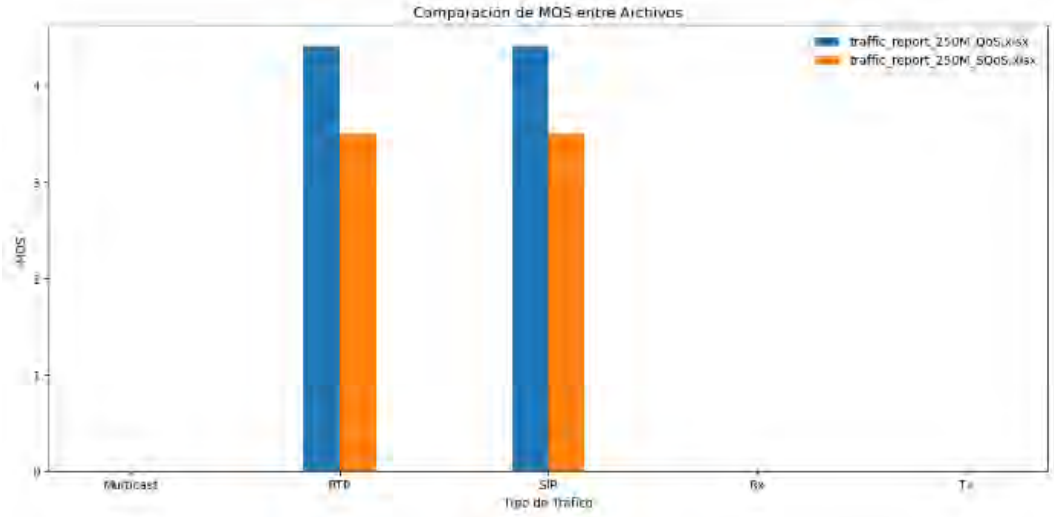


Figura 5.2.12 Parámetros ICPIF, MOS

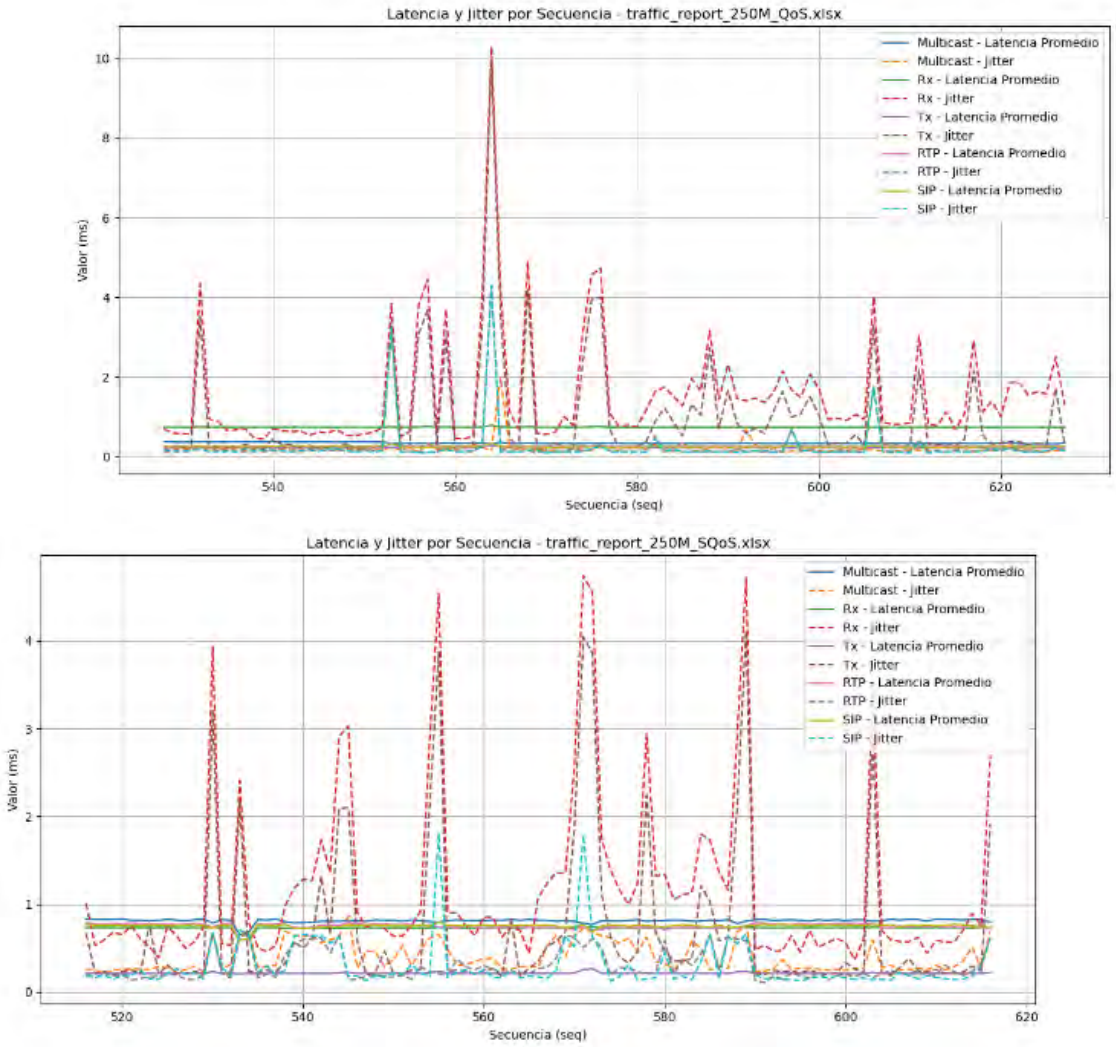


Figura 5.2.13 Grafica lineal de parámetros de rendimiento

- Se puede verificar del análisis de tráfico la generación de tablas y graficas comparativas para tráfico de 250 Mbps con y sin calidad de servicio, donde los parámetros a evaluar son métricas de tasa de Tx/Rx, perdida de paquetes, latencia, jitter, MOS e ICPIF, que nos permite evaluar el rendimiento de la red implementada, el cual transporta tráficos generadas por un generador de tráfico de red.
- Las tablas muestran métricas de rendimiento de red para tráficos con y sin calidad de servicio. La tabla 5.2.5 (tráfico de 250 Mbps con calidad de servicio) nos muestra que los parámetros de rendimiento están por debajo de los umbrales críticos de funcionamiento descrito en la sección 5.2.1 con lo que podemos concluir que el tráfico será optimo y estable. La métrica de MOS tiene el valor de 4.41 tanto para tráfico RTP y SIP, pero tenemos valores de 0 para tráfico Multicast y trafico genérico. El valor de la métrica ICPIF está por debajo del valor umbral de 20 lo que indica que son valores adecuados para los diferentes tipos de tráfico que viajan por la red.
- Las tablas muestran métricas de rendimiento de red para tráficos con y sin calidad de servicio. La tabla 5.2.7 (tráfico de 250 Mbps sin calidad de servicio) nos muestra que los parámetros de rendimiento están por debajo de los umbrales críticos de funcionamiento descrito en la sección 5.2.1 con lo que podemos concluir que el tráfico será optimo y estable. La métrica de MOS tiene el valor de 3.51 tanto para tráfico RTP y SIP, pero tenemos valores de 0 para tráfico Multicast y trafico genérico. El valor de la métrica ICPIF está por debajo del valor umbral de 35.02 lo que indica que son valores no son los adecuados para los diferentes tipos de tráfico que viajan por la red.
- En las tablas y graficas se verifica que el rendimiento de la red está directamente relación a la calidad de servicio que se aplica a cada tipo de tráfico (VoIP, Multicast y Genérica). El tráfico con calidad de servicio muestra un mejor rendimiento para los diferentes tipos de tráfico.

Se verifica el rendimiento de la red para los tres tipos de tráfico (160, 200 y 250 Mbps) generados por el generador de tráfico, sobre el ancho de banda de 200 Mbps de la red evaluada. Para tráfico de 160 Mbps la red se comporta de una manera estable en ambos casos; con y sin calidad de servicio evidenciándose en la tabla 5.2.1 un mejor rendimiento para tráfico con calidad de servicio. Para tráfico de 200 Mbps la red se comporta de una manera estable para el caso de tráfico con calidad de servicio como se muestra en la tabla 5.2.3, el rendimiento para una red sin calidad de servicio ve afectado su rendimiento como se muestra en la tabla 5.2.4. Para tráfico de 250 Mbps la red se comporta de una manera estable para el caso de tráfico con calidad de servicio como se muestra en la tabla 5.2.5, el rendimiento para una red sin calidad de servicio ve afectado su rendimiento como se muestra en la tabla 5.2.6, generándose caída de servicios (perdida de paquetes muy altas).

5.3 Análisis de Tráfico con Wireshark - VPLS

La captura de paquetes se realizará en la ruta marcada de color Azul que es el túnel entre los routers PE1 y PE3, Figura 5.3.2. Wireshark es una herramienta de software que permite analizar los protocolos de las diferentes capas del modelo TCP/IP. En este caso analizaremos como se da la conmutación de etiquetas a través del dominio IP/MPLS de la topología implementada.

Protocolo	Porcentaje de paquetes	Paquetes	Porcentaje de bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	257	100.0	36463	61 k	0	0	0	257
Ethernet	100.0	257	15.5	5656	9499	0	0	0	404
MultiProtocol Label Switching Header	57.2	147	3.2	1176	1975	0	0	0	294
PW Ethernet Control Word	57.2	147	1.6	588	987	0	0	0	147
Logical-Link Control	1.9	5	0.5	195	327	0	0	0	5
Spanning Tree Protocol	1.9	5	0.5	180	302	5	180	302	5
Internet Protocol Version 4	1.6	4	0.2	80	134	0	0	0	4
User Datagram Protocol	0.8	2	0.0	16	26	0	0	0	2
Label Distribution Protocol	0.8	2	0.2	68	114	2	68	114	2
Open Shortest Path First	0.8	2	0.3	96	161	2	96	161	2
Data	92.6	238	75.3	27444	46 k	238	27444	46 k	238
802.1Q Virtual LAN	29.6	76	0.8	304	510	0	0	0	76
Internet Protocol Version 4	3.9	10	0.5	200	335	0	0	0	10
Internet Control Message Protocol	3.9	10	1.8	640	1074	10	640	1074	10

Figura 5.3.1 Jerarquía de protocolos para IPMPLS – VPLS

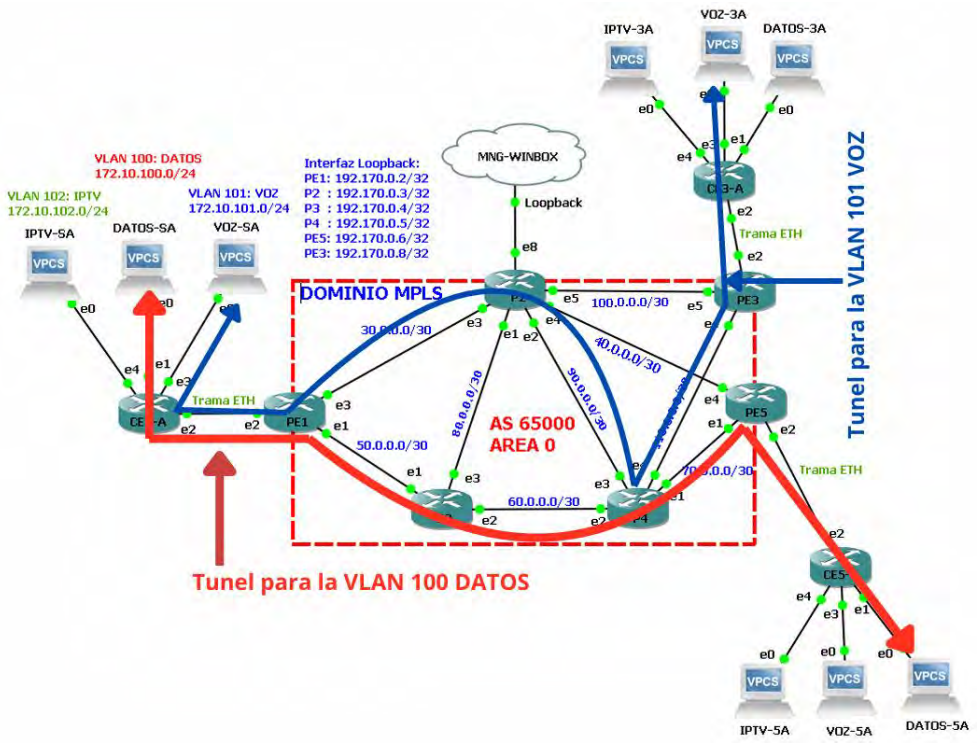


Figura 5.3.2 Topología de red Con túnel de TE para el transporte de VPLS

Componentes del dominio MPLS de la topología:

- Dominio MPLS (AS 65000 - Área 0) con múltiples PE (Provider Edge) y P (Provider)
- Túnel MPLS-TE (marcado en azul) para la VLAN 102: IPTV
- Servicios VPLS para diferentes VLANs:
  - VLAN 100: DATOS (172.10.100.0/24)
  - VLAN 101: VOZ (172.10.101.0/24)
  - VLAN 102: IPTV (172.10.102.0/24)
- Interfaces Loopback configuradas en cada router del core IP/MPLS con direccionamiento 192.170.0.x/32

Para realizar el análisis de tráfico de Wireshark en esta red MPLS con VPLS, se realiza:

1. Capturar tráfico en puntos estratégicos (interfaces PE, enlaces core MPLS)
2. Analizar las etiquetas MPLS en los paquetes
3. Verificar el funcionamiento del VPLS entre sitios
4. Monitorear el túnel MPLS-TE para la VLAN 102 - IPTV

Configuración de la ruta del túnel TE sobre el enrutador PE1 se marca con un rectángulo azul, donde se puede ver los saltos (routers) de la ruta del túnel la cual es prestablecida manualmente, y es diferente a la ruta que OSPF tomaría según su propio algoritmo.

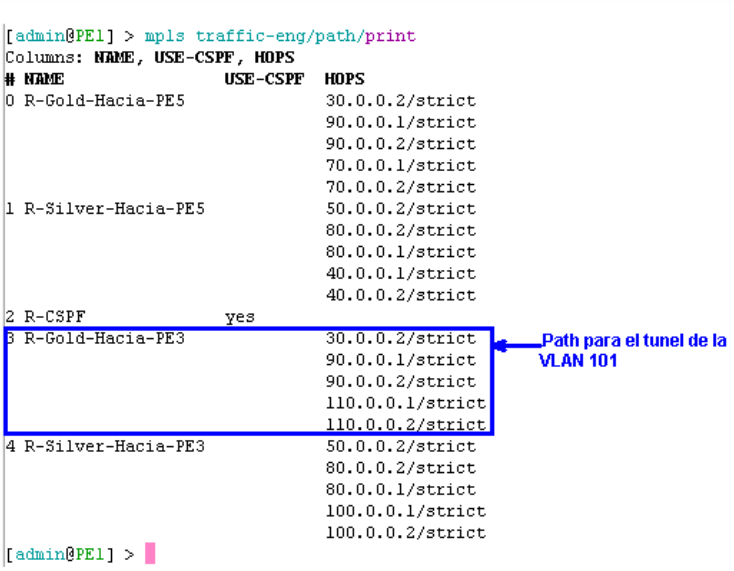


Figura 5.3.3 Saltos del túnel de ingeniería de trafico

En la figura 5.3.3 se ve la configuración del túnel MPLS-TE desde la perspectiva del router PE1. El comando **mpls traffic-eng/path/print** muestra las rutas de ingeniería de tráfico configuradas.

Análisis de la ruta del túnel (marcada en azul): Ruta, R-Gold-Hacia-PE3

- Destino: Router de borde PE3 (según la topología)
- Hops configurados (routers de la ruta del túnel):
  - 30.0.0.2/strict
  - 90.0.0.1/strict
  - 90.0.0.2/strict
  - 110.0.0.1/strict
  - 110.0.0.2/strict

Este túnel está configurado con strict hops**,** lo que significa que el tráfico debe seguir exactamente esta ruta específica, sin permitir desviaciones automáticas por parte del protocolo de ruteo.

Según el diagrama, este túnel sigue el camino azul que conecta los PE1 y PE3 para transportar el tráfico de VLAN 102 (IPTV) como se indica.

Para el análisis con Wireshark, se realizará:

1. Capturar tráfico en las interfaces que corresponden al túnel de ingeniería de tráfico (TE).
2. Filtrar por las etiquetas MPLS específicas de este túnel
3. Verificar que el tráfico sigue efectivamente esta ruta estricta

5.3.1.1 Captura de Paquetes entre CE1-A(eth2) y PE1(eth2)

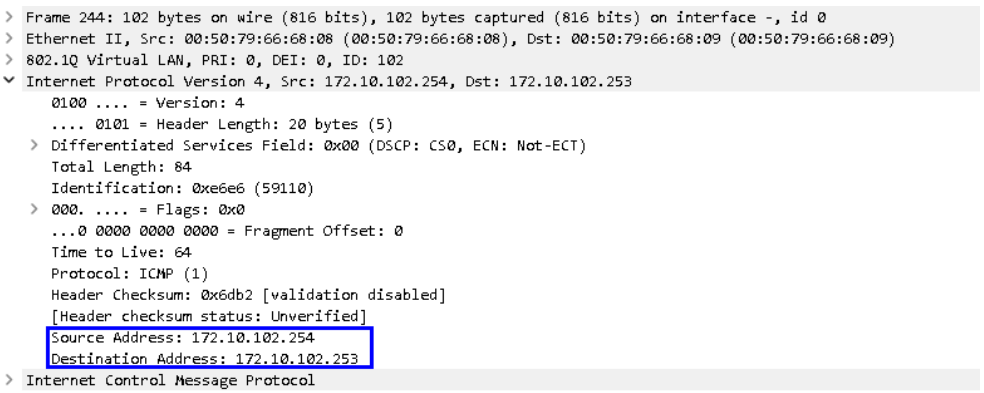


Figura 5.3.4 Captura de paquetes entre los nodos CE1 y PE1

Esta es una captura que muestra el tráfico antes de ingresar al dominio MPLS.

Análisis del Frame 244:

Información de enlace:

- La captura de paquetes se da entre las interfaces de CE1-A(ether2) y PE1(ether2)
- Tamaño de la captura: 102 bytes (816 bits)
- VLAN: 802.1Q Virtual LAN, ID: 102

Análisis del tráfico IP:

- Protocolo: IPv4 con ICMP
- Origen: 172.10.102.254
- Destino: 172.10.102.253
- Red: VLAN 102 (IPTV según la topología)

Por lo que podemos decir: Tráfico de VLAN 102**;** Este es exactamente el tráfico de IPTV que utilizara el túnel de ingeniería de tráfico. La captura de tráfico se realiza antes de que se encapsule con etiquetas MPLS. El Tráfico de prueba/conectividad (ping) entre dispositivos en la misma red VLAN 102 (Origen: 172.10.102.254 - Destino: 172.10.102.253). Lo que confirma la expansión de la red LAN del cliente.

5.3.1.2 Captura con Wireshark entre PE1(Eth3) y P2(Eth3)

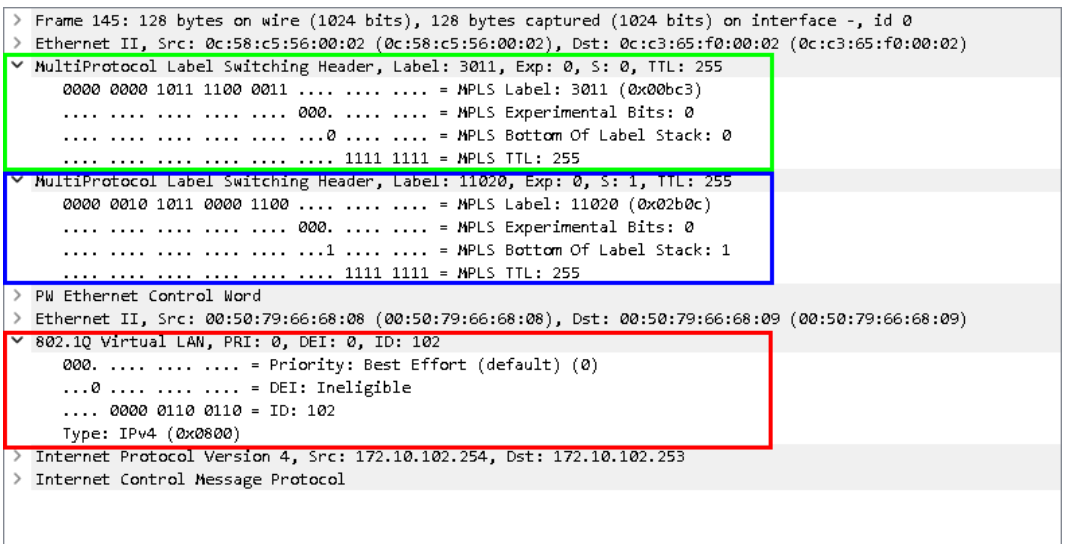


Figura 5.3.5 Captura de paquetes entre PE1 y P2.

Ahora vemos el mismo tráfico, pero dentro del dominio MPLS. Esta captura permite verificar el funcionamiento de MPLS-VPLS.

Análisis del Frame 145 (PE1 - P2):

Encapsulación MPLS completa:

- Tamaño: 128 bytes (vs 102 bytes en CE-PE) - 26 bytes adicionales por las etiquetas MPLS

Pila de etiquetas MPLS (de exterior a interior):

Etiqueta Externa (Transporte)**:**

- Label**:** 3011 (0x0bc3)
- S-bit**:** 0 (no es la última etiqueta)
- TTL**:** 255

Etiqueta Interna (Servicio/VPLS)**:**

- Label**:** 11020 (0x2b0c)
- S-bit**:** 1 (última etiqueta de la pila)
- TTL**:** 255

Paquete original preservado:

- VLAN ID**:** 102 (mantenida)
- IPs: 172.10.102.254 hacia 172.10.102.253
- Protocolo: ICMP (prueba de conectividad)

Interpretación de las etiquetas:

Etiqueta 3011**:** Etiqueta de transporte MPLS-TE (corresponde al túnel configurado R-Gold-Hacia-PE3).

Etiqueta 11020**:** Etiqueta de servicio VPLS para la VLAN 102 (IPTV)

Doble encapsulación**:** Confirma implementación MPLS-VPLS con ingeniería de tráfico

El tráfico de VLAN 102 está siendo transportado exitosamente a través del túnel MPLS-TE específico, con la etiqueta de servicio VPLS correspondiente.

5.3.1.3 Captura de Paquetes entre P2(Eth2) y P4(Eth3)

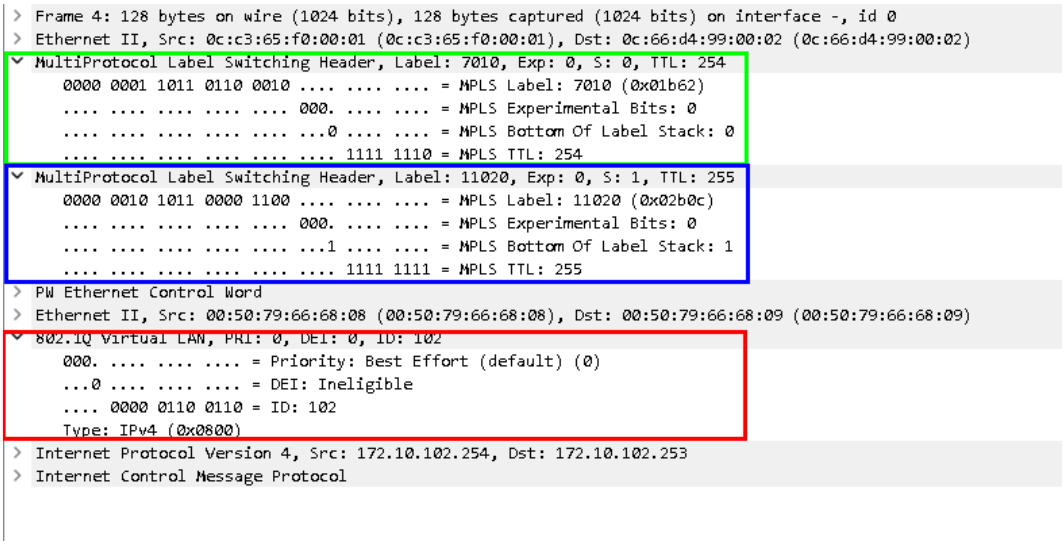


Figura 5.3.6 Captura de paquetes entre los router P2 y P4

Esta captura muestra la conmutación de etiquetas MPLS en el dominio IP/MPLS de la red.

Análisis del Frame 4 (P2 → P4):

Tabla 5.3.1 Conmutación de etiquetas MPLS

Posición	PE1→P2	P2→P4	Operación
Etiqueta Externa	3011	7010	Swap
Etiqueta Interna	11020	11020	Se mantiene

En esta tabla podemos ver como se da la computación de etiquetas de transporte

Label Swapping: La etiqueta de transporte cambió de 3011 a 7010

- Esto es el comportamiento normal de MPLS Label Switching en el core
- Cada salto (hop) asigna una nueva etiqueta de reenvió.

Etiqueta de servicio se mantiene: 11020 se mantiene intacta

- Confirma que es la etiqueta VPLS para VLAN 102
- Solo se procesa en los PE de borde (edges), no en el core (LSR).

El tráfico original (VLAN 102, IPs 172.10.102.x) permanece inalterado

TTL decrementado: 255 → 254 (comportamiento normal en MPLS forwarding)

El funcionamiento del túnel MPLS-TE, indica que el:

- El tráfico está siguiendo correctamente la ruta (path) configurado según la figura 5.3.2
- La conmutación de etiquetas funciona apropiadamente
- El servicio VPLS se mantiene a través del dominio MPLS.

5.3.1.4 Captura de Paquetes entre P4(Eth4) y PE3(Eth4)

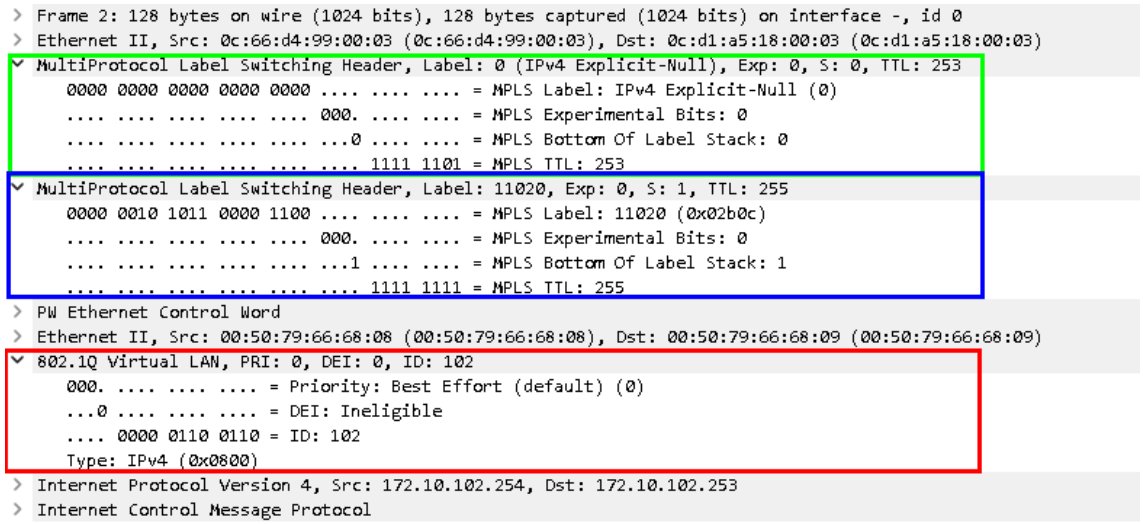


Figura 5.3.7 Captura de paquetes entre P4 y PE3

Esta captura muestra el penúltimo salto antes de llegar al PE3 de destino, y aquí vemos una característica muy importante de MPLS, PHP (Penultimate hop Popping).

Análisis del Frame 2 (P4→PE3):

Tabla 5.3.2 Evolución de las etiquetas MPLS

Salto	Etiqueta Externa	Etiqueta Interna	Observación
PE1→P2	3011	11020	Doble etiqueta
P2→P4	7010	11020	Label swap
P4→PE3	IPv4 Explicit-Null (0)	11020	PHP aplicado

Penultimate Hop Popping (PHP):

- La etiqueta externa fue removida("popped") por P4
- En su lugar: IPv4 Explicit-Null (Label 0)
- Esto es una optimización MPLS.

Etiqueta de servicio preservada:

- 11020 se mantiene intacta
- PE3 la procesará para determinar el servicio VPLS
- TTL se mantiene en 255 (característica del servicio)

Beneficios del PHP:

- PE3 solo debe procesar una etiqueta (la de servicio)
- Mejora el rendimiento en el PE3 de destino
- Reduce la carga de procesamiento

El tráfico completó exitosamente la ruta(path) configurada, la ingeniería de tráfico funcionó correctamente, ahora PE3 puede procesar directamente la etiqueta VPLS 11020

5.3.1.5 Captura de Paquetes entre PE3(Eth2) y CE3A(Eth2)

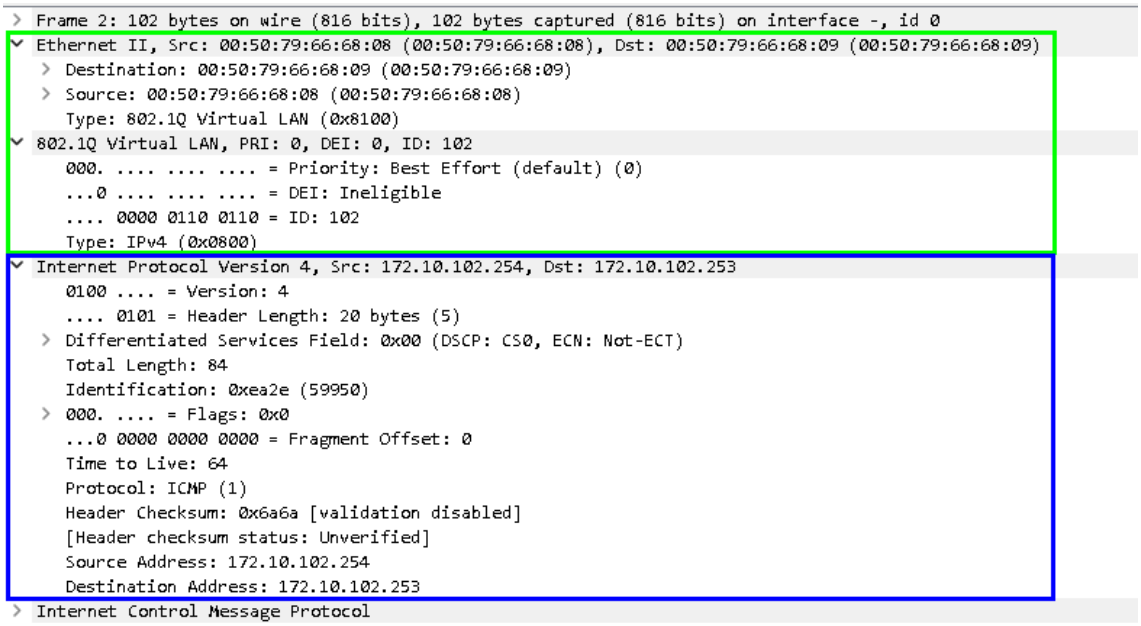


Figura 5.3.8 Captura de paquetes entre PE3 y CE3-A

Esta es la captura final que completa todo el recorrido del servicio MPLS-VPLS. Aquí vemos la desencapsulación completa en el PE3.

Análisis del Frame 2 (PE3→CE3-A):

Tabla 5.3.3 Transformación completa del paquete

Parámetro	Origen (CE1→PE1)	Destino (PE3→CE3)	Estado
Tamaño	102 bytes	102 bytes	Restaurado
Etiquetas MPLS	Ninguna	Ninguna	Decapsulado
VLAN ID	102	102	Intacto
IP Origen	172.10.102.254	172.10.102.254	Intacto
IP Destino	172.10.102.253	172.10.102.253	Intacto
Protocolo	ICMP	ICMP	Intacto

Funcionamiento VPLS confirmamos que:

- PE3 procesó correctamente la etiqueta de servicio 11020
- Identificó VLAN 102 y restauró el frame original
- Entrega exitosa del tráfico IPTV

Túnel MPLS-TE funcionando correctamente:

- Path estricto R-Gold-Hacia-PE3 ejecutado
- Etiquetas de transporte conmutadas: 3011 → 7010 → IPv4-Explicit-Null
- PHP aplicado en el penúltimo salto

Servicio VPLS operativo:

- Etiqueta de servicio 11020 para VLAN 102 transportada a través del túnel TE.
- VLAN ID preservado a través de todo el dominio MPLS
- Conectividad L2 transparente entre CE1-A y CE3-A

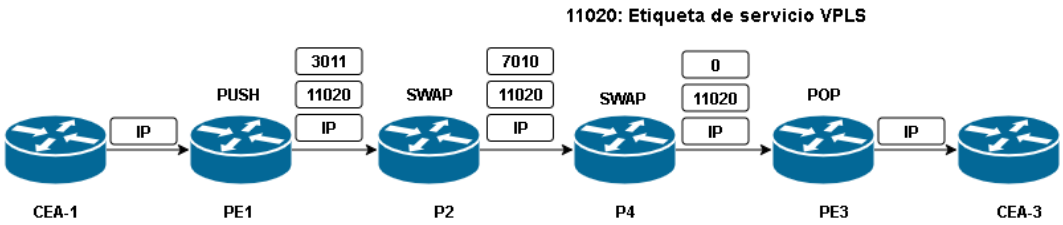


Figura 5.3.9 Conmutación de etiquetas a través de la red

El análisis con Wireshark nos permite verificar como RouterOS hace el tratamiento de la transmisión de tramas ethernet (VPLS) sobre una infraestructura IP/MPLS con ingeniería de tráfico. Haciendo en análisis del recorrido del tráfico sobre la infraestructura implementada se puede llegar a verificar que el tráfico que ingresa desde el lado del usuario son tramas ethernet, los cuales al ingresar al dominio IP/MPLS son empaquetados por una pila de etiquetas. La etiqueta de transporte forma el túnel de ingeniería de tráfico que es el encargado de trasportar el tráfico del cliente, esta etiqueta es conmutada por cada router del core IP/MPLS en la ruta del túnel de ingeniería de tráfico. El análisis nos permite verificar que tenemos una etiqueta de servicio una etiqueta de transporte, la etiqueta de servicio VPLS en RouterOS permite identificar la trama ethernet del cliente y la etiqueta de transporte permite generar el túnel de ingeniería de tráfico. Generando un apilamiento de etiquetas formada por una etiqueta de transporte, y una etiqueta de servicio (etiqueta VPLS), se puede verificar que la conmutación y distribución de las etiquetas de trasporte se da a través del protocolo RSVP-TE en el core IP/MPLS, y la asignación de la etiqueta de servicio se da a través del protocolo MP-BGP que gracias a su versatilidad nos permite distribuir etiquetas de servicios para VPLS (L2VPN) implementada en la topología de red. En la Figura 5.3.9 podemos verificar de mejor manera el comportamiento de la asignación de etiquetas y el transporte del tráfico del cliente.

Evolución de la pila de etiquetas:

1. CE1-1 hacia PE1: El tráfico son tramas ethernet.
2. PE1 hacia P2: Se verifica el apilamiento de etiquetas con la siguiente estructura [MPLS-TE:3011][VPLS:11020][ETHERNET].
3. P2 hacia P4: Aquí se genera la conmutación de la etiqueta de transporte (túnel de ingeniería de tráfico), verificándose la siguiente estructura de la pila de etiquetas [MPLS-TE:7010][VPLS:11020][ETHERNET].
4. P4 hacia PE3: Verificamos que aquí se aplica la operación de Penultime Hop Popping realizado por el router P4. La estructura del paquete tiene la siguiente estructura de pila de etiquetas PE5: [IPv4-Null:0, Exp:3][VPLS:11020][ETHERNET].
5. PE3 hacia CE3-A: En este tramo del recorrido del tráfico son tramas ETHERNET.

El análisis del tráfico sobre el core IP/MPLS nos permite verificar las operaciones que se realizan en cada enrutador.

1. Router PE1, es el router de ingreso al dominio IP/MPLS la operación que realiza sobre las etiquetas es denominada PUSH, por el cual este enrutador utiliza el protocolo MP-BGP para asignar la etiqueta de servicio (Etiquetas 11020), y el protocolo RSVP-TE para la asignación de la etiqueta de transporte (Etiqueta 3011). Es el encargado de encapsular la trama ethernet del cliente hacia el dominio IP/MPLS.
2. Router de tránsito P2: Se verifica que la operación sobre la etiqueta de transporte que realiza se denomina SWAP, cambiando la etiqueta 3011 por la etiqueta 7010, la etiqueta de servicio (11020) se mantienen sin ninguna modificación.
3. Router Penultime Hop Popping (P4): Se puede verificar que la operación sobre la etiqueta de transporte (7010) se denomina POP, lo que permite que el router del siguiente salto PE3 ya no realice la operación sobre esta etiqueta de transporte.
4. Router de egreso del dominio IP/MPLS (PE3): Verificamos que la operación que realiza este enrutador de borde se denomina POP, retirando todas las etiquetas de servicio desencapsulando la trama ethernet del cliente.

5.3.2 Análisis del Rendimiento con Paquetes Generados

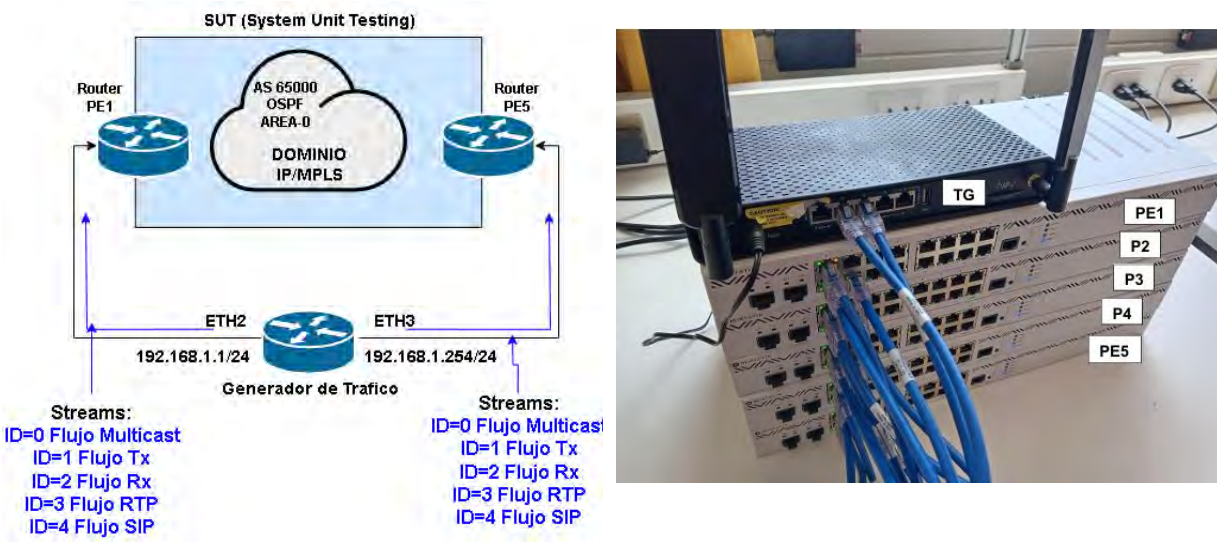
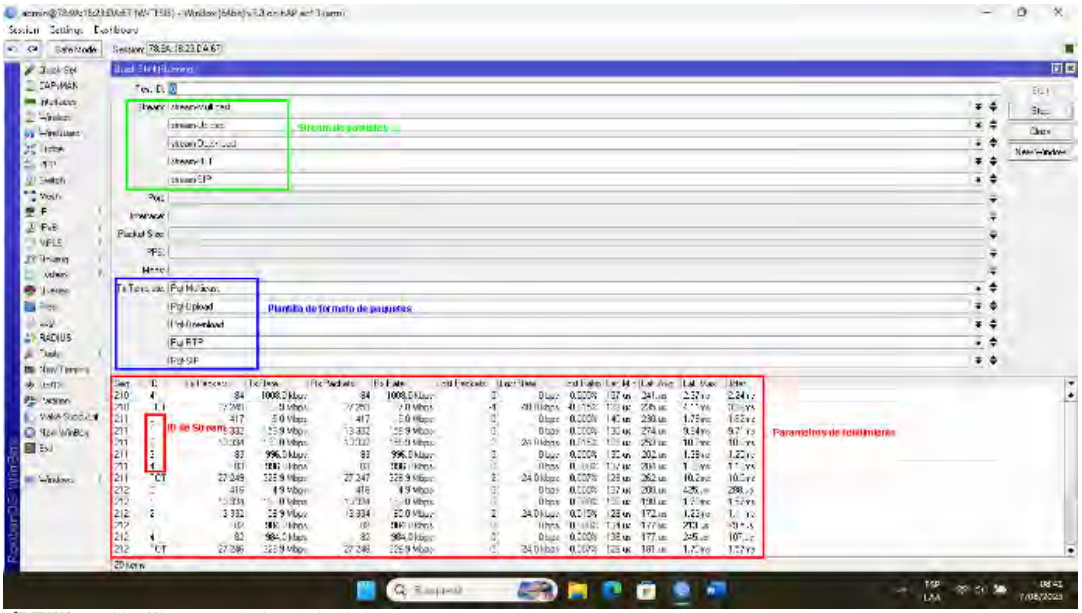


Figura 5.3.10 Generador de tráfico sobre VPLS

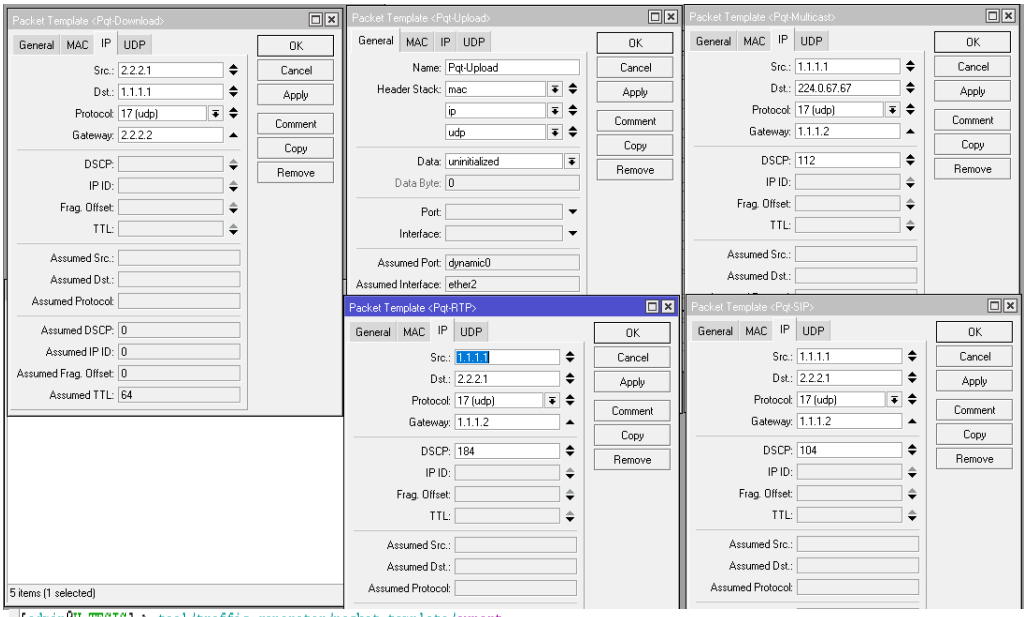
5.3.3 Generacion de Trafico para el Analisis de Rendimiento

El Generador de Tráfico de MikroTik es una herramienta integrada en RouterOS, el sistema operativo de los dispositivos MikroTik. Su función principal es la de simular y generar flujos de tráfico de red con características específicas, en el presente trabajo nos permitira probar el comportamiento de la topologia de red implementada bajo un escenario con trafico Generico, Multicast y Telefonia IP. A diferencia de una simple prueba de ancho de banda el Generador de Tráfico ofrece un control mucho más granular sobre los parámetros del tráfico generado.



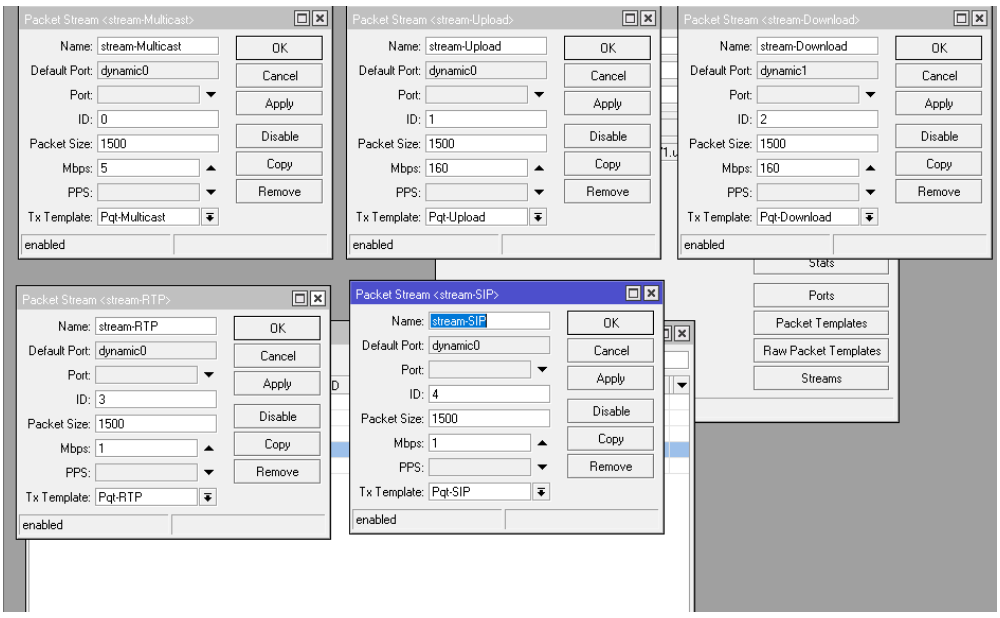

```
[admin@W-TESIS] > tool/traffic-generator/packet-template/print
 0 name="Pqt-Multicast" header-stack=mac,ip,udp assumed-port=dynamic0 assumed-interface=ether2 assumed-mac-src=78:9A:18:23:DA:65 assumed-mac-dst=78:9A:18:A9:DB:73
   assumed-mac-protocol=ip ip-dscp=112 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-src=1.1.1.1 ip-dst=224.0.67.67 ip-protocol=udp ip-gateway=1.1.1.2
   udp-src-port=5001 udp-dst-port=5001 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks="" random-ranges="" special-footer=yes
   compute-checksum-from-offset=no-checksum

 1 name="Pqt-Download" header-stack=mac,ip,udp assumed-port=dynamic1 assumed-interface=ether3 assumed-mac-src=78:9A:18:23:DA:66 assumed-mac-dst=78:9A:18:A9:DD:43
   assumed-mac-protocol=ip assumed-ip-dscp=0 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-src=2.2.2.1 ip-dst=1.1.1.1 ip-protocol=udp ip-gateway=2.2.2.2
   assumed-udp-src-port=100 assumed-udp-dst-port=200 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks="" random-ranges=""
   special-footer=yes compute-checksum-from-offset=no-checksum

 2 name="Pqt-Upload" header-stack=mac,ip,udp assumed-port=dynamic0 assumed-interface=ether2 assumed-mac-src=78:9A:18:23:DA:65 assumed-mac-dst=78:9A:18:A9:DB:73
   assumed-mac-protocol=ip assumed-ip-dscp=0 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-src=1.1.1.1 ip-dst=2.2.2.1 ip-protocol=udp ip-gateway=1.1.1.2
   assumed-udp-src-port=100 assumed-udp-dst-port=200 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks="" random-ranges=""
   special-footer=yes compute-checksum-from-offset=no-checksum

 3 name="Pqt-RTP" header-stack=mac,ip,udp assumed-port=dynamic0 assumed-interface=ether2 assumed-mac-src=78:9A:18:23:DA:65 assumed-mac-dst=78:9A:18:A9:DB:73
   assumed-mac-protocol=ip ip-dscp=184 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-src=1.1.1.1 ip-dst=2.2.2.1 ip-protocol=udp ip-gateway=1.1.1.2
   udp-dst-port=16384-16484 assumed-udp-src-port=100 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks="" random-ranges=""
   special-footer=yes compute-checksum-from-offset=no-checksum

 4 name="Pqt-SIP" header-stack=mac,ip,udp assumed-port=dynamic0 assumed-interface=ether2 assumed-mac-src=78:9A:18:23:DA:65 assumed-mac-dst=78:9A:18:A9:DB:73
   assumed-mac-protocol=ip ip-dscp=104 assumed-ip-id=0 assumed-ip-frag-off=0 assumed-ip-ttl=64 ip-src=1.1.1.1 ip-dst=2.2.2.1 ip-protocol=udp ip-gateway=1.1.1.2
   udp-dst-port=5060,5061 assumed-udp-src-port=100 assumed-udp-checksum=0 data=uninitialized data-byte=0 random-byte-offsets-and-masks="" random-ranges=""
   special-footer=yes compute-checksum-from-offset=no-checksum
[admin@W-TESIS] >
```

Figura 5.3.11 Generador de paquetes, caracteristicas de los paquetes




```
[admin@W-TESIS] > tool/traffic-generator/packet-template/export
# jan/06/1970 12:47:35 by RouterOS 7.8
# software id = 9KDZ-DQSR
#
# model = RBD53iG-5HacD2HnD
# serial number = HET09BDA4HN
/tool traffic-generator packet-template
add ip-dscp=112 ip-dst=224.0.67.67 ip-gateway=1.1.1.2 ip-protocol=udp ip-src=1.1.1.1 name=Pqt-Multicast udp-dst-port=5001 udp-src-port=5001
add ip-dst=1.1.1.1 ip-gateway=2.2.2.2 ip-protocol=udp ip-src=2.2.2.1 name=Pqt-Download
add ip-dst=2.2.2.1 ip-gateway=1.1.1.2 ip-protocol=udp ip-src=1.1.1.1 name=Pqt-Upload
add ip-dscp=184 ip-dst=2.2.2.1 ip-gateway=1.1.1.2 ip-protocol=udp ip-src=1.1.1.1 name=Pqt-RTP udp-dst-port=16384-16484
add ip-dscp=104 ip-dst=2.2.2.1 ip-gateway=1.1.1.2 ip-protocol=udp ip-src=1.1.1.1 name=Pqt-SIP udp-dst-port=5060,5061
[admin@W-TESIS] >
```

Figura 5.3.12 Plantillas de formato de paquetes



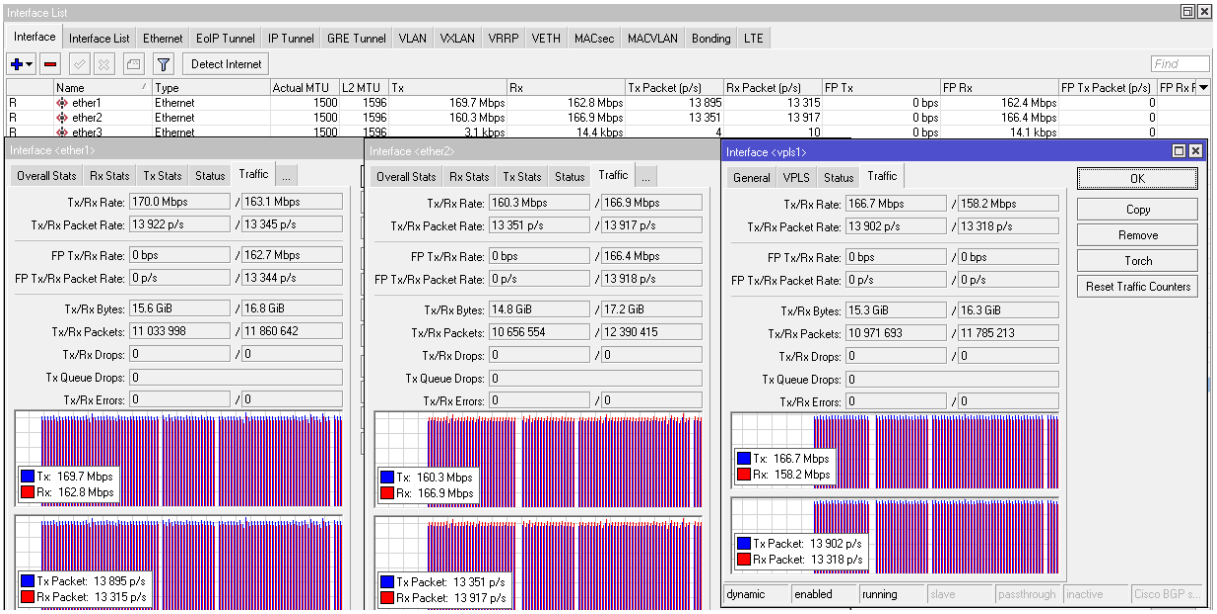
```
[admin@W-TESIS] > tool/traffic-generator/stream/print
Columns: NAME, DEFAULT-PORT, ID, PACKET-SIZE, MBPS, PPS, TX-TEMPLATE, PACKET-COUNT, CPU-CORE
# NAME             DEFAULT-PORT  ID  PACKET-SIZE  MBPS  PPS  TX-TEMPLATE    PACKET-COUNT  CPU-CORE
0 stream-Multicast  dynamic0       0         1500     5    0  Pqt-Multicast  unlimited     0-3
1 stream-Download   dynamic1       2         1500   160    0  Pqt-Download   unlimited     0-3
2 stream-Upload     dynamic0       1         1500   160    0  Pqt-Upload     unlimited     0-3
3 stream-RTP        dynamic0       3         1500     1    0  Pqt-RTP        unlimited     0-3
4 stream-SIP        dynamic0       4         1500     1    0  Pqt-SIP        unlimited     0-3
[admin@W-TESIS] >
```

Figura 5.3.13 Flujos de datos transmitidos

```
[admin@W-TESIS] > tool/traffic-generator/stream/export
# jan/06/1970 12:46:02 by RouterOS 7.8
# software id = 9KDZ-DQSR
#
# model = RBD53iG-5HacD2HnD
# serial number = HET09BDA4HN
/tool traffic-generator stream
add mbps=5 name=stream-Multicast packet-size=1500 tx-template=Pqt-Multicast
add id=2 mbps=160 name=stream-Download packet-size=1500 tx-template=Pqt-Download
add id=1 mbps=160 name=stream-Upload packet-size=1500 tx-template=Pqt-Upload
add id=3 mbps=1 name=stream-RTP packet-size=1500 tx-template=Pqt-RTP
add id=4 mbps=1 name=stream-SIP packet-size=1500 tx-template=Pqt-SIP
[admin@W-TESIS] >
```

Figura 5.3.14 Configuración de flujo de datos

5.3.4 Recorrido del Trafico a traves del Tunnel TE.



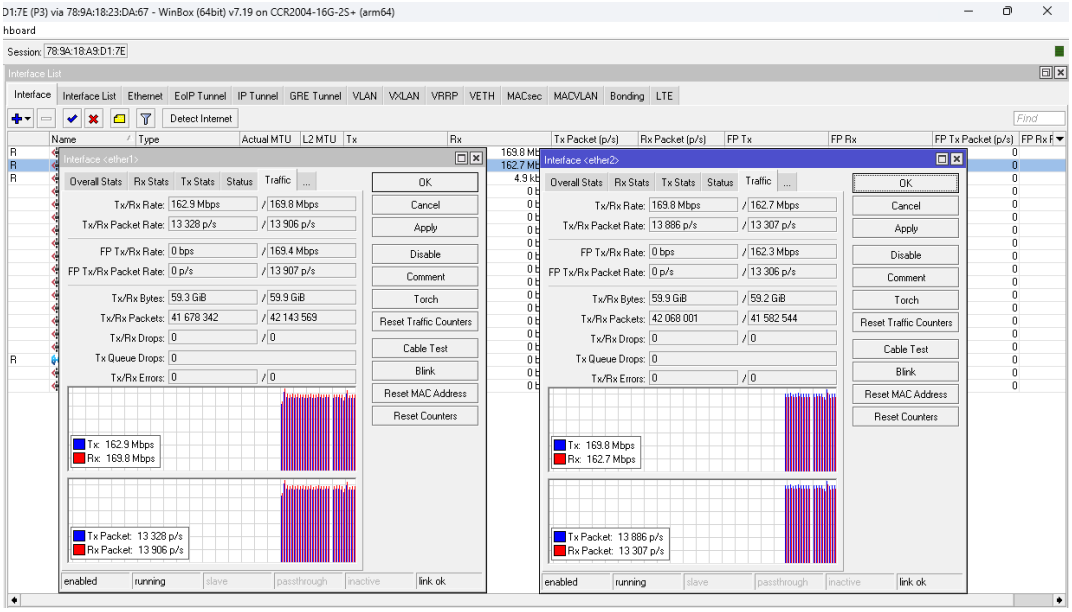
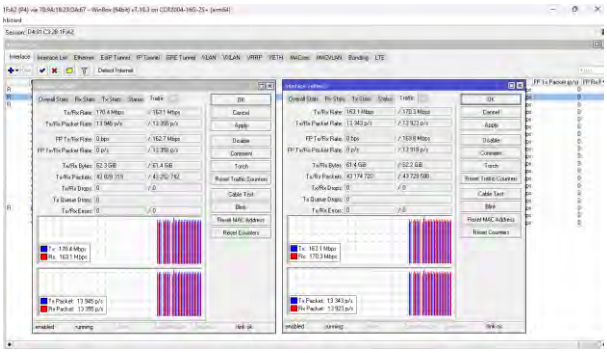
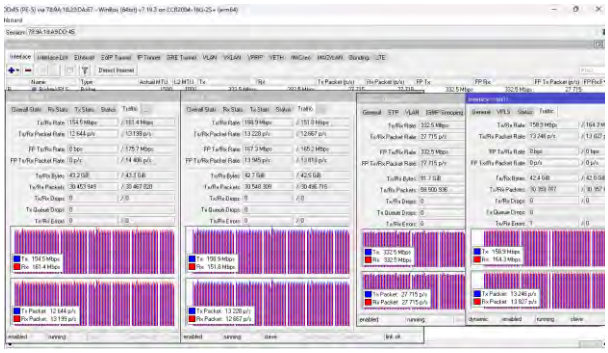


Figura 5.3.15 Throughput de las interfaces PE1 y P3

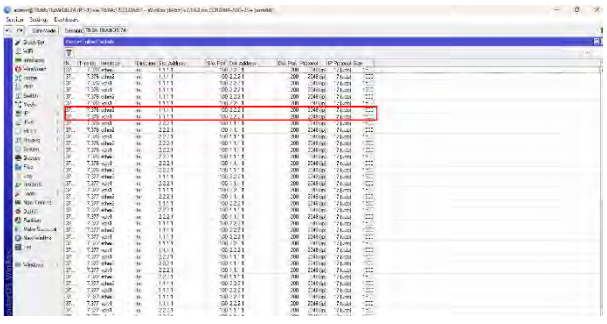


a) Trafico a traves de ether2, ether1 del enrutador P4

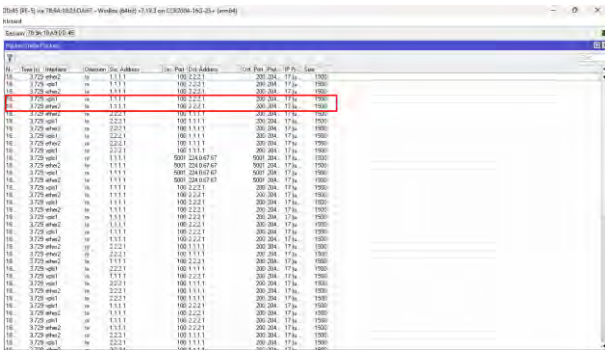


b) Trafico a traves de ether1, vpls1 (Bridge-VPLS), y ether2, del enrutador PE-5

Figura 5.3.16 Throughput de las interfaces P4 y PE-5



a) Captura de paquetes en ether2 y vpls1 en PE-1



b) Captura de paquetes en vpls1 y ether2 en PE-5

Figura 5.3.17 Captura de paquetes en las interfaces de PE-1 y PE-5

5.4 Análisis de Rendimiento en VPLS

El objetivo es evaluar el desempeño de la red en términos de delay (latencia promedio), packet loss (pérdida de paquetes), jitter, MOS (Mean Opinion Score) e ICPIF (Impairment Calculated Planning Impairment Factor) para cada tipo de tráfico (Multicast, RTP, SIP, Rx, Tx). La generación de los diferentes tipos de tráfico es mediante la herramienta Generador de tráfico de RouterOS de Mikrotik implementando los siguientes flujos de datos.

- **ID=0**: Tráfico multicast
- **ID=1**: Tráfico de transmisión (Tx)
- **ID=2**: Tráfico de recepción (Rx)
- **ID=3**: Tráfico RTP
- **ID=4**: Tráfico SIP

La figura 5.4.1 muestra la conexión del generador de tráfico a la topología de red implementada.

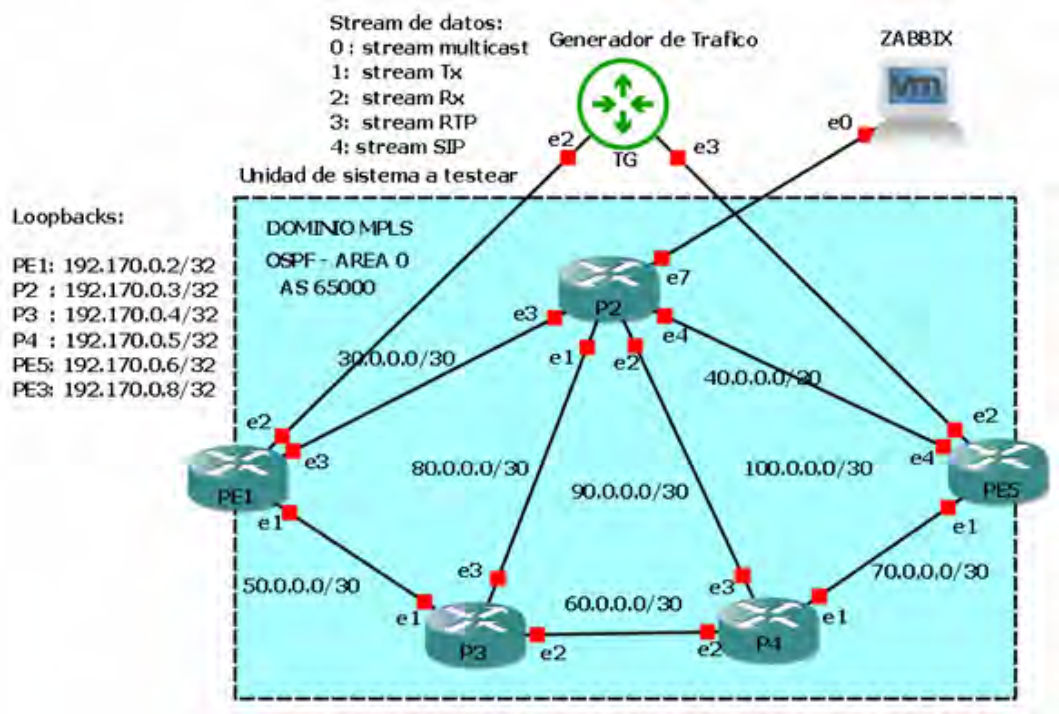


Figura 5.4.1 Topología de red con generador de trafico

El flujo de datos multicast implememtado en la red hace uso del protocolo IGMP proxy y IGMP Snooping que viene implementado en el sistema operativo de RouterOS. Esto debido a que en una topologia de VPLS la comunicación entre usuario y el dominio IP/MPLS se da a nivel de capa 2 (conmutacion), y IGMP proxy y IGMP Snooping es el protocolo a nivel de capa 2 para trafico multicast, que soporta RouterOS.

Un generador de trafico es una herramienta que permite evaluar el rendimiento de un DUT(Device Under Test) o SUT (System Under Test). Nuestro sistema a probar sera el servicio VPLS sobre una red IP/MPLS, para lo cual se ha conectado el generador de trafico a traves de su puerto ether2 hacia el puerto ether2 del router PE-1 y el puerto ether3 del generador de trafico hacia el puerto ether2 del router PE-5.

El generador de trafico de Mikrotik version 7 en puertos especificos permite generar flujos de datos de diferentes caracteristicas (igmp, udp, tcp, etc.). Permite tambien exportar valores de red como la latencia y jitter, tasas de transmision y recepcion, perdida de paquetes; los cuales seran procesados para generar tablas con valores de los parametros de rendimiento.

Consideraciones para analisis de rendimiento del SUT:

- El ancho de banda del SUT sera de 200 Mbps.
- Generacion de traficos de 160 Mbps, 200 Mbps y 250 Mbps.
- Implementacion de SUT con calidad de servicio (QoS).
- Implementacion de SUT sin calidad de servicio (QoS).

5.4.1 Valores Umbrales de los Diferentes Parámetros

Identifica problemas en cada tipo de tráfico comparando métricas con umbrales:

- Latencia promedio > 150 ms
- Jitter promedio > 30 ms
- Pérdida de paquetes > 1%
- MOS < 3.5
- ICPIF > 20

MOS (mean opinión score), Es una métrica utilizada para evaluar la calidad de servicios de voz y video, como las llamadas de VoIP, se califica en una escala de 1 a 5, donde 5 es la mejor calidad. Para el cálculo se utiliza la version simplificada del modelo E (ITU-T G.107) basado en latencia, jitter y perdida de paquetes.

ICPIF (Calculated Planning Impairment Factor) Es una métrica utilizada para medir y cuantificar los efectos de diversas deficiencias en la calidad de la voz, especialmente en redes de Voz sobre protocolo de internet (VoIP). El valor ICPIF representa el impacto general de

problemas de red como el retardo y la perdida de paquetes en la experiencia del usuario. El cálculo está basado en el estándar ITU-T G.113, que considera la latencia, jitter y perdida de paquetes. Valores < 10 indican buena calidad, > 20 indican problemas.

5.4.2 Análisis de Rendimiento para Tráfico 160 Mbps

Tabla 5.4.1 Parámetros de rendimiento VPLS con QoS para 160 Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	MOS	ICPIF
Multicast	0.21	0.55	0	4.14	20
Rx	0.18	1.03	5.81	3.51	35
Tx	0.19	1.13	5.04	3.51	35
RTP	0.19	0.25	0.19	4.14	20
SIP	0.18	0.23	0	4.41	10

Tabla 5.4.2 Parámetros de rendimiento VPLS sin QoS para 160 Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	MOS	ICPIF
Multicast	1.13	14.27	72.18	3.51	35.03
Rx	0.66	0.87	41.8	3.51	35.02
Tx	0.68	0.92	47.64	3.51	35.02
RTP	0.67	0.35	51.96	3.51	35.02
SIP	0.67	0.38	44.45	3.51	35.02

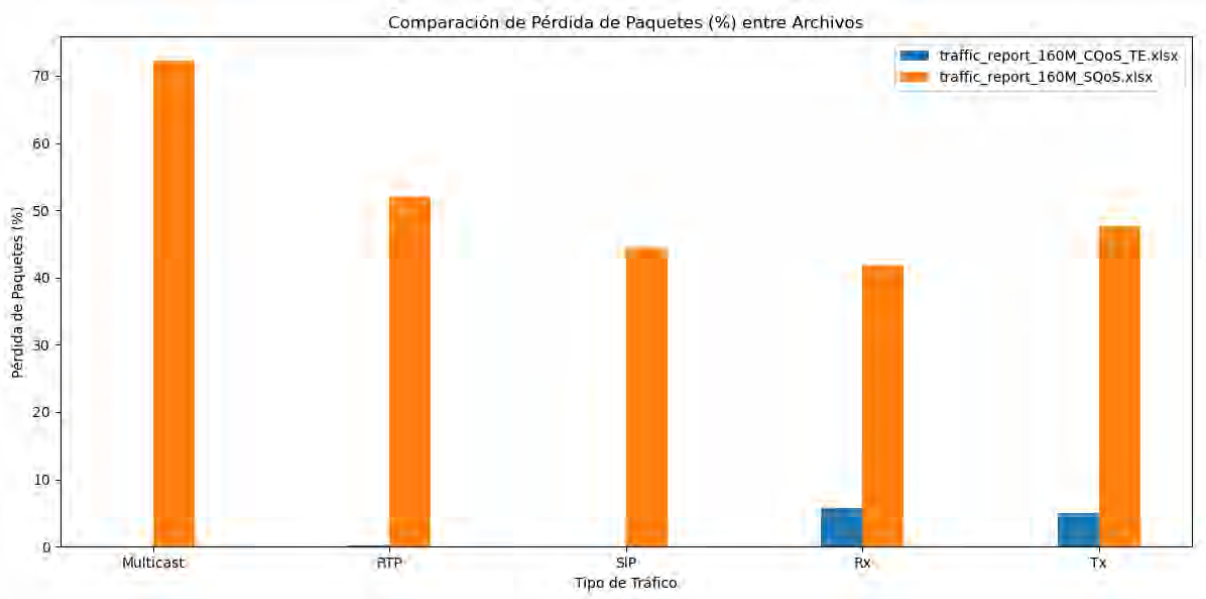


Figura 5.4.2 Perdida de paquetes para tráfico de 160 Mbps

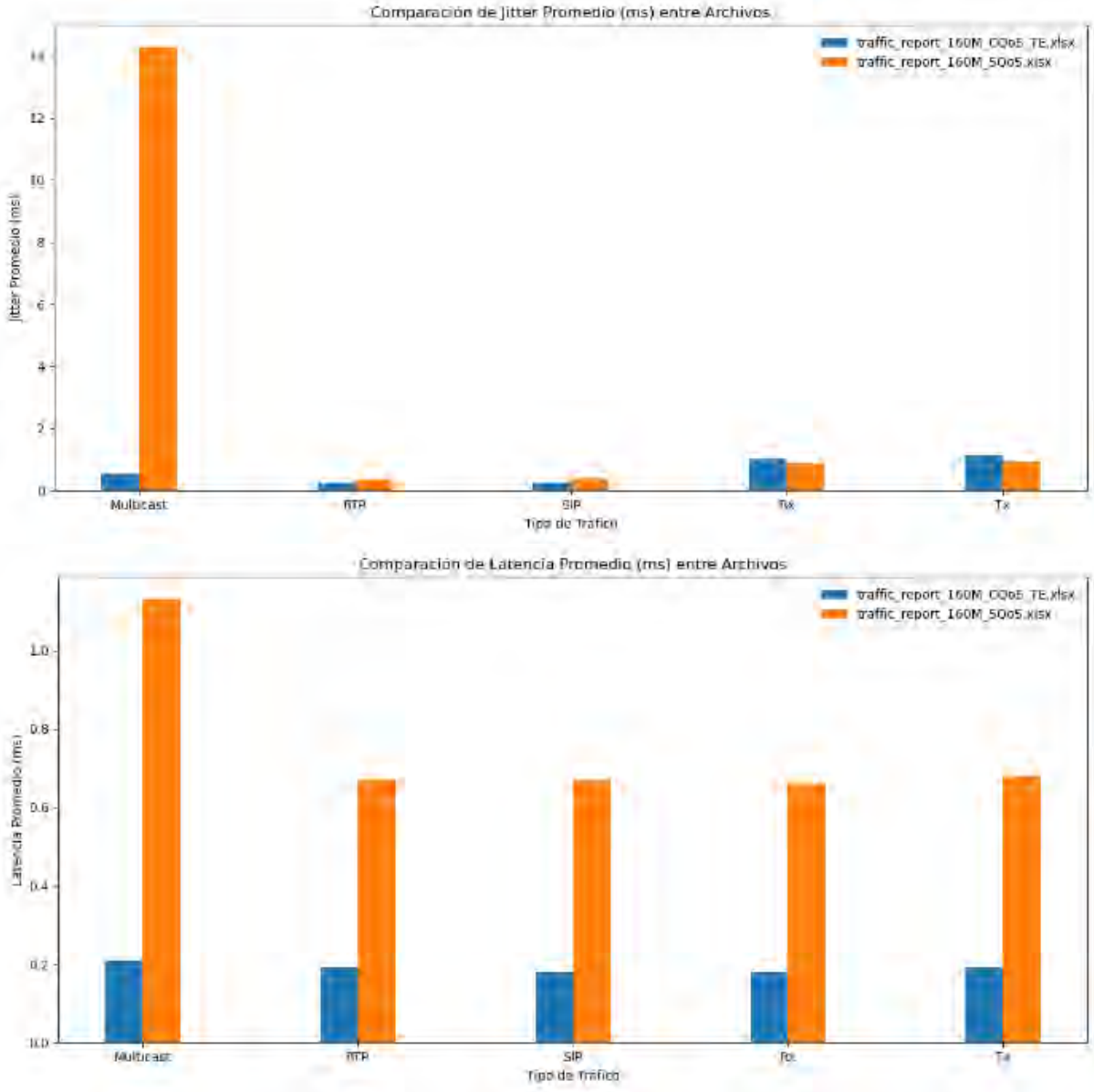


Fig. 5.61: Jitter y Latencia para trafico de 160 Mbps

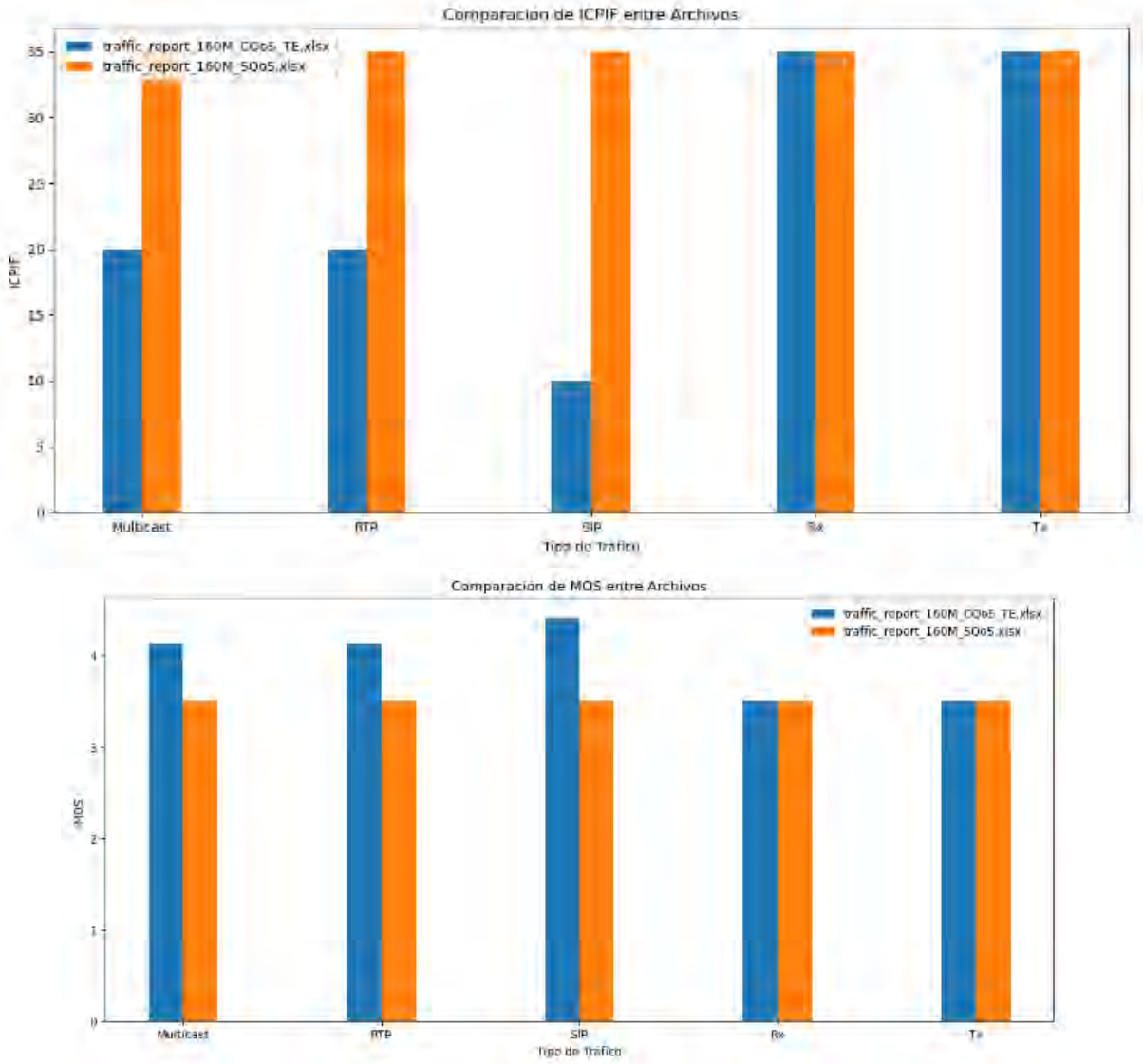
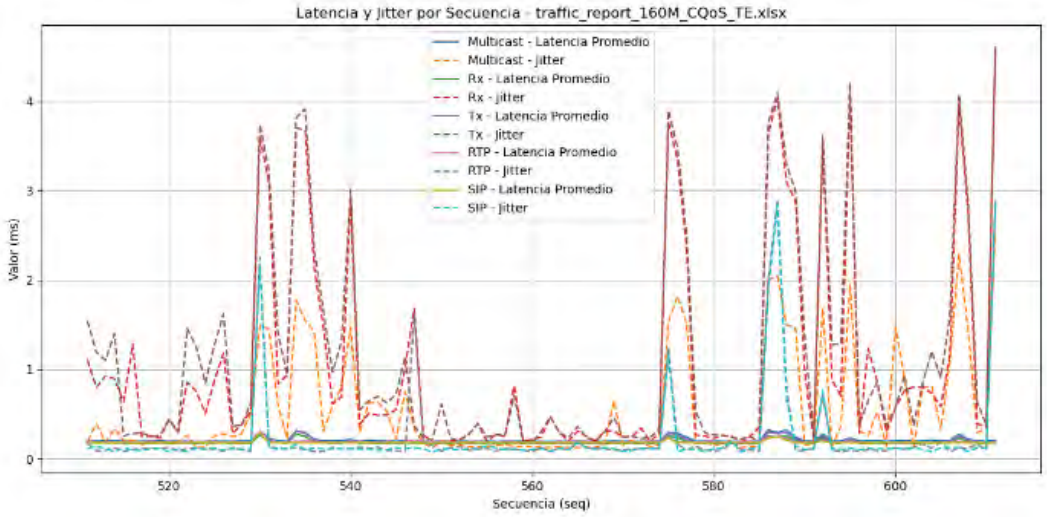


Figura 5.4.3 ICPF y MOS para trafico de160 Mbps



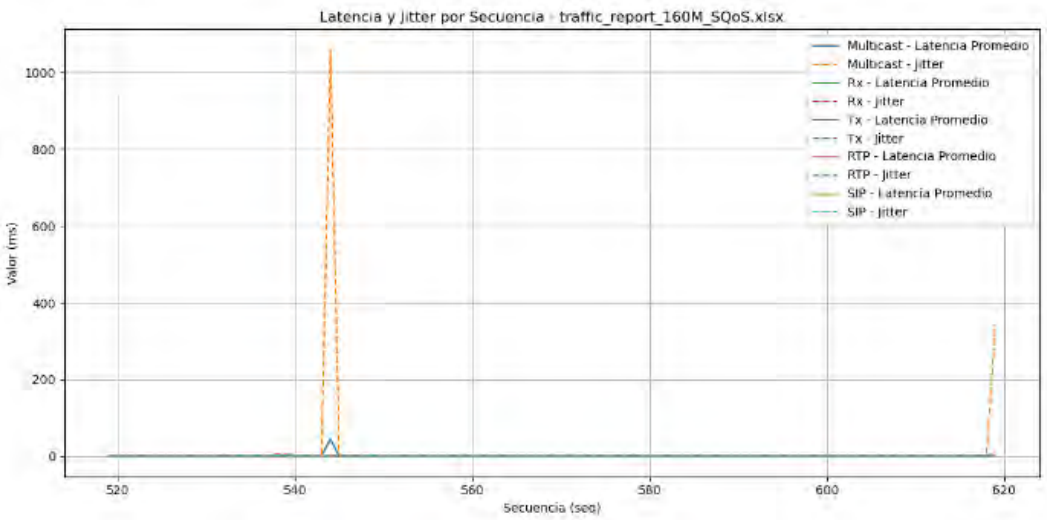


Figura 5.4.4 Grafica línea para tráfico de 160 Mbps

- Se puede verificar del análisis de tráfico la generación de tablas y graficas comparativas para tráfico de 160 Mbps con y sin calidad de servicio, donde los parámetros a evaluar son métricas de tasa de Tx/Rx, perdida de paquetes, latencia, jitter, MOS e ICPIF, que nos permite evaluar el rendimiento de la red implementada, el cual transporta tráficos generadas por un generador de tráfico de red.
- Las tablas muestran métricas de rendimiento de red para tráficos con y sin calidad de servicio. La tabla 5.4.1 (tráfico de 160 Mbps con calidad de servicio) nos muestra que los parámetros de rendimiento están por muy debajo de los umbrales críticos de funcionamiento descrito en la sección 5.4.1 con lo que podemos concluir que el tráfico será optimo y estable. La métrica de MOS se encuentra entre los valores 3.51 y 4.41 lo cual nos indica que son valores óptimos para tráficos críticos como VoIP. La métrica ICPIF se encuentra entre los valores de 10 y 20 que también indican comportamiento óptimo para el transporte de tráfico como VoIP y multicast.
- De la tabla 5.4.2 (tráfico de 160 Mbps sin calidad de servicio) podemos verificar que los parámetros de rendimiento para los diferentes tipos de tráfico sobrepasan los valores umbrales listados en la sección 5.4.1 como es el caso de la perdida de paquetes que supera los 41.8 % que afecta el rendimiento de la red generando retrasmisiones por perdida de paquetes. Las métricas de MOS están por encima del valor umbral de 3.5 el

cual afectara a tráficos en tiempo real como es el caso de VoIP y multicast. La métrica de ICPIF sobrepasa el límite umbral de 20, afectando de manera directa el rendimiento de la red para tráficos de VoIP y multicast.

- En las tablas y graficas se verifica que el rendimiento de la red está directamente relación a la calidad de servicio que se aplica a cada tipo de tráfico (VoIP, Multicast y Genérica). El tráfico con calidad de servicio muestra un mejor rendimiento para los diferentes tipos de tráfico.

5.4.3 Análisis de Rendimiento para Tráfico 200 Mbps

Tabla 5.4.3 Parámetros de rendimiento de tráfico con QoS 200 Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	MOS	ICPIF
Multicast	0.21	0.52	0	4.41	10
Rx	0.18	1.24	4.78	3.51	35
Tx	0.19	1.35	5.65	3.51	35
RTP	0.19	0.17	0	4.41	10
SIP	0.18	0.17	0	4.41	10

Tabla 5.4.4 Parámetros de rendimiento de tráfico sin QoS 200 Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	MOS	ICPIF
Multicast	10.09	103.09	82.11	3.5	35.24
Rx	0.68	1.03	54.76	3.51	35.02
Tx	0.7	1	61.63	3.51	35.02
RTP	0.68	0.4	53.24	3.51	35.02
SIP	0.68	0.4	58.09	3.51	35.02

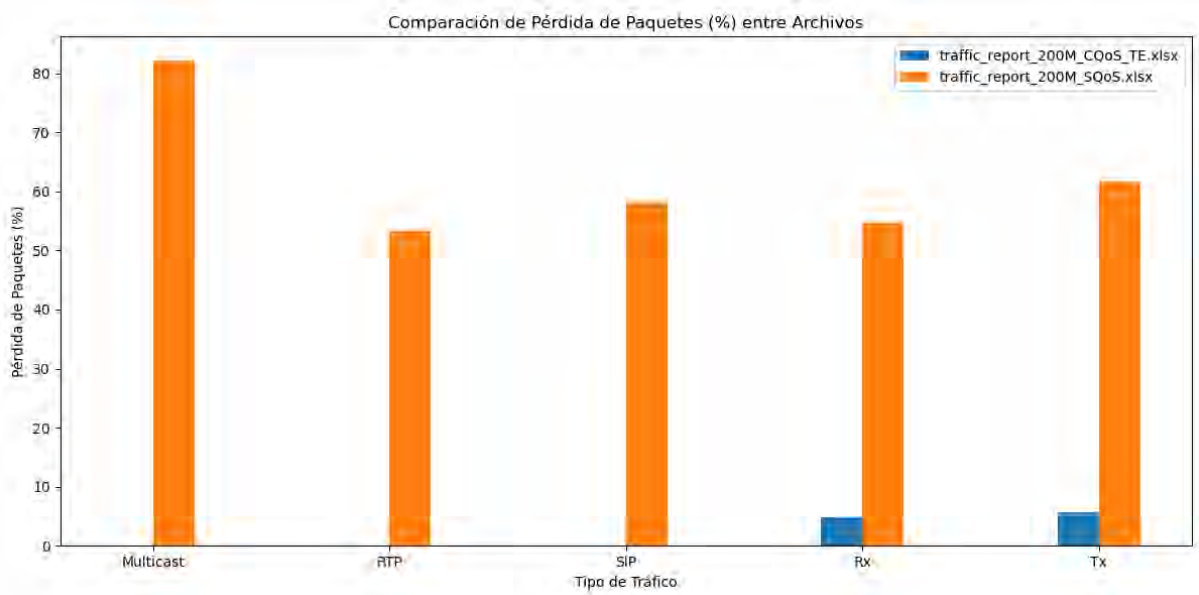
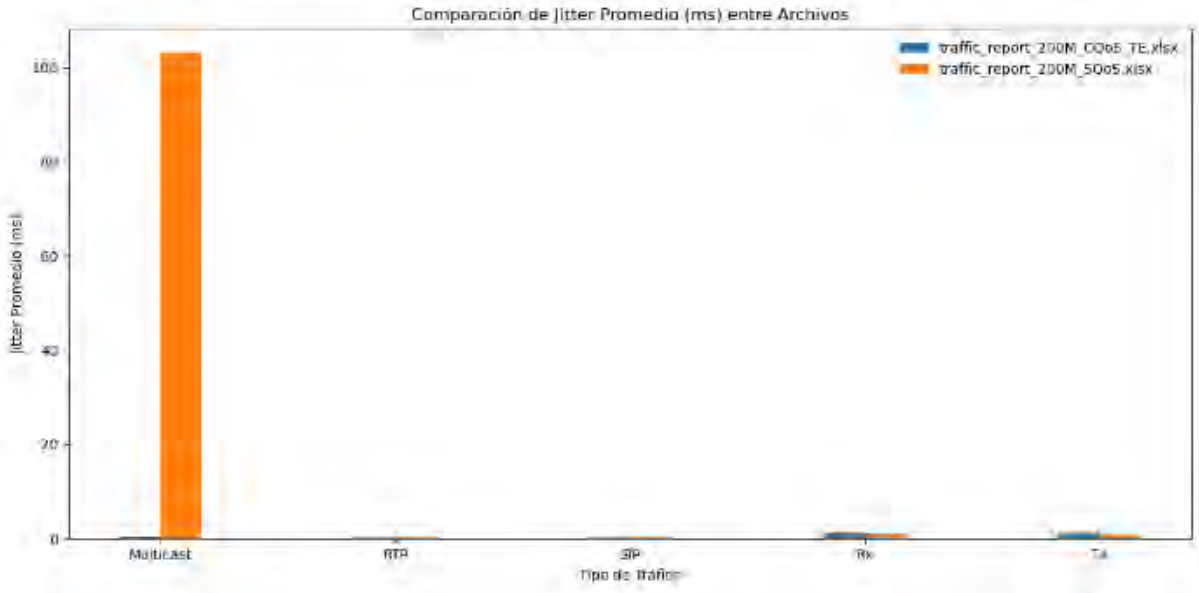


Figura 5.4.5 Perdida de paquetes para tráfico de 200 Mbps



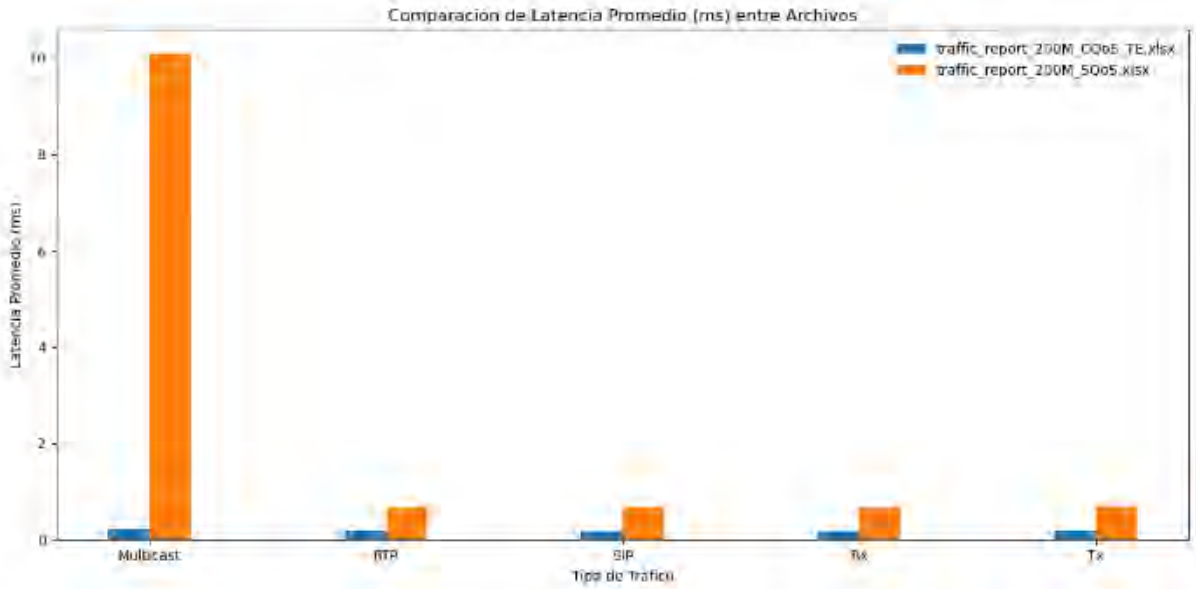
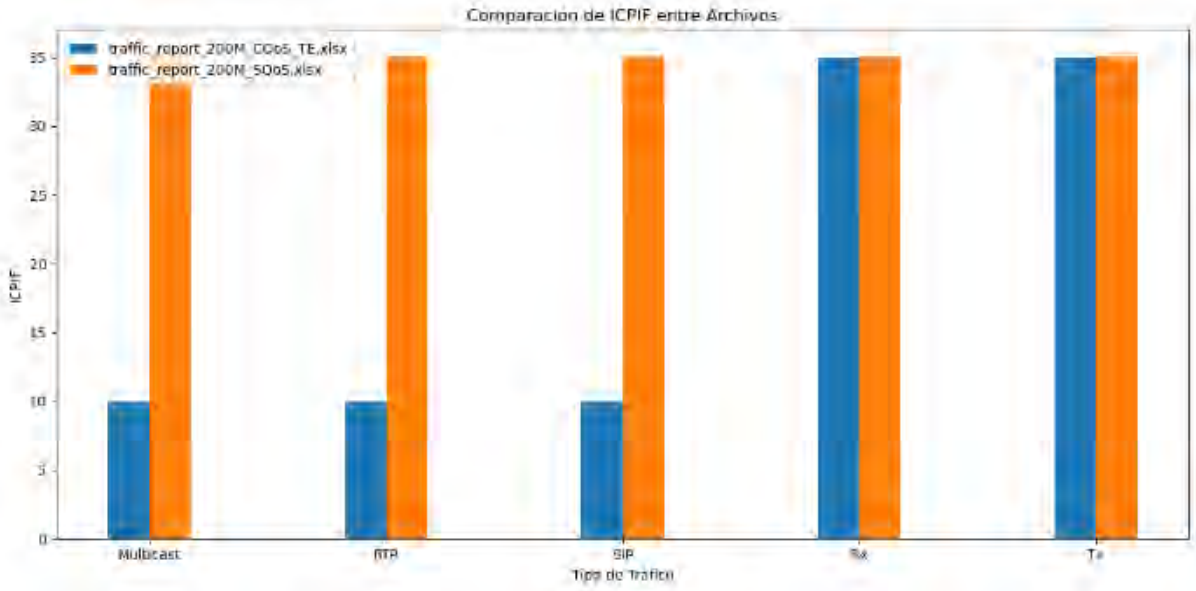


Figura 5.4.6 Jitter y Latencia para trafico de 200 Mbps



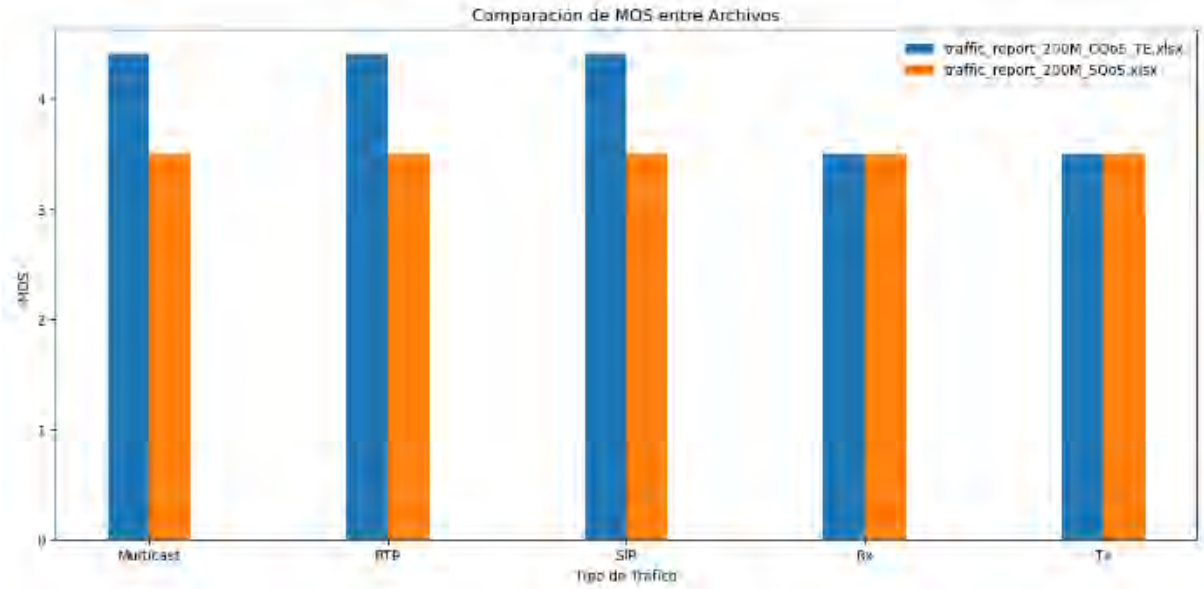


Figura 5.4.7 ICPF y MOS para trafico de 200 Mbps

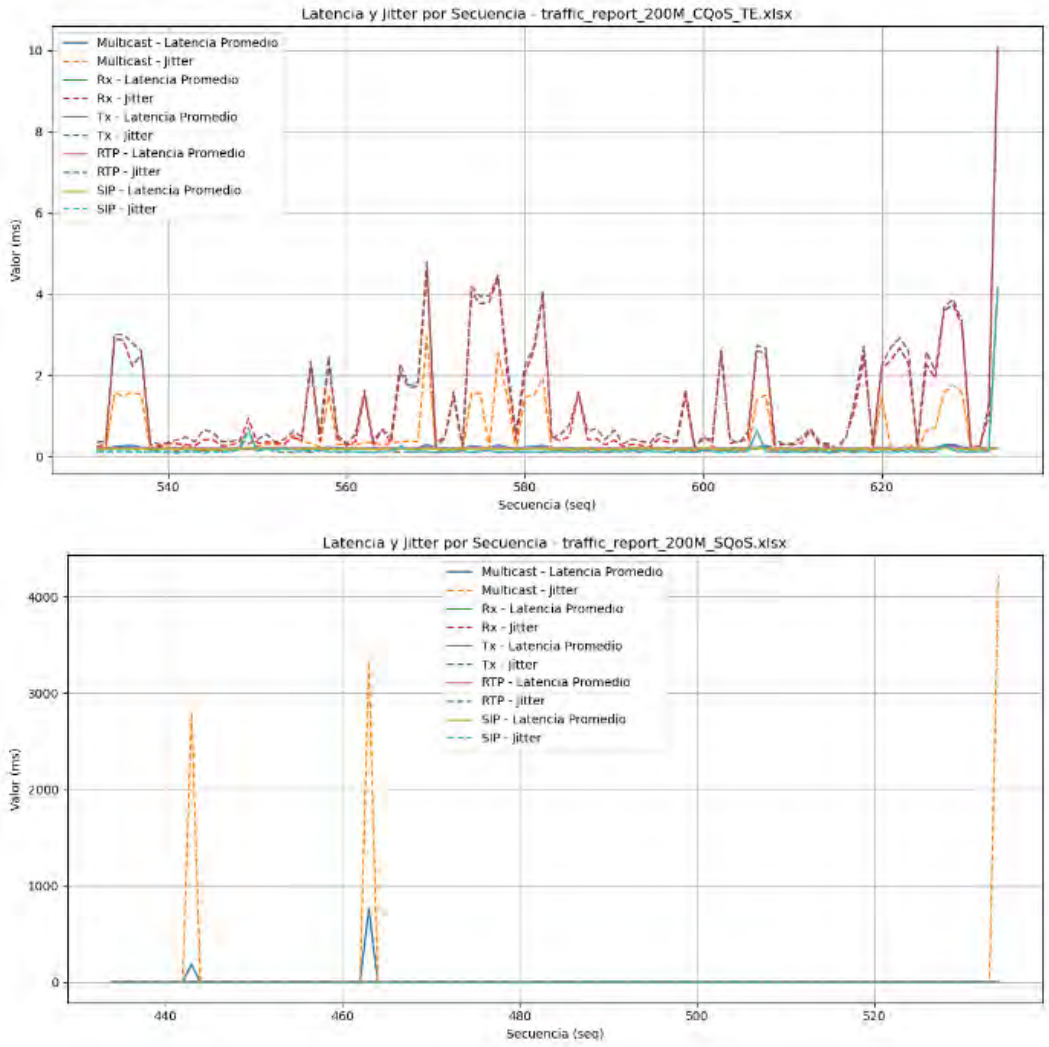


Figura 5.4.8 Grafica línea para tráfico de 200 Mbps

- Se puede verificar del análisis de tráfico la generación de tablas y graficas comparativas para tráfico de 200 Mbps con y sin calidad de servicio, donde los parámetros a evaluar son métricas de tasa de Tx/Rx, perdida de paquetes, latencia, jitter, MOS e ICPIF, que nos permite evaluar el rendimiento de la red implementada, el cual transporta tráficos generadas por un generador de tráfico de red.
- Las tablas muestran métricas de rendimiento de red para tráficos con y sin calidad de servicio. La tabla 5.4.3 (tráfico de 200 Mbps con calidad de servicio) nos muestra que los parámetros de rendimiento están por debajo de los umbrales críticos de funcionamiento descrito en la sección 5.4.1 con lo que podemos concluir que el tráfico será optimo y estable. La métrica de MOS se encuentra entre los valores 3.51 y 4.41 lo cual nos indica que son valores óptimos para tráficos críticos como VoIP. La métrica ICPIF se encuentra entre los valores de 10 que también indican comportamiento óptimo para el transporte de tráfico como VoIP y multicast.
- De la tabla 5.4.4 (tráfico de 200 Mbps sin calidad de servicio) podemos verificar que los parámetros de rendimiento para los diferentes tipos de tráfico sobrepasan los valores umbrales listados en la sección 5.4.1 como es el caso de la perdida de paquetes que supera los 54.76% que afecta el rendimiento de la red generando retrasmisiones por perdida de paquetes. Las métricas de MOS están por encima del valor umbral de 3.51 el cual afectara a tráficos en tiempo real como es el caso de VoIP y multicast. La métrica de ICPIF sobrepasa el límite umbral de 20 (35.24), afectando de manera directa el rendimiento de la red para tráficos de VoIP y multicast.
- En las tablas y graficas se verifica que el rendimiento de la red está directamente relación a la calidad de servicio que se aplica a cada tipo de tráfico (VoIP, Multicast y Genérica). El tráfico con calidad de servicio muestra un mejor rendimiento para los diferentes tipos de tráfico.

5.4.4 Análisis de Rendimiento para Tráfico de 250 Mbps

Tabla 5.4.5 Parámetros de rendimiento de tráfico con QoS 250 Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	MOS	ICPIF
Multicast	0.22	0.75	0	4.41	10.01
Rx	0.69	2.26	19.89	3.51	35.02
Tx	0.19	1.81	26.02	3.51	35
RTP	0.2	0.58	0	4.41	10
SIP	0.19	0.38	0	4.41	10

Tabla 5.4.6 Parámetros de rendimiento de tráfico sin QoS 250 Mbps

Tipo de Tráfico	Latencia Promedio (ms)	Jitter Promedio (ms)	Pérdida de Paquetes (%)	MOS	ICPIF
Multicast	5.42	60.77	90.02	3.51	35.13
Rx	0.46	0.51	69.74	3.51	35.01
Tx	0.5	0.56	76.26	3.51	35.01
RTP	0.47	0.13	72.77	3.51	35.01
SIP	0.47	0.13	71.57	3.51	35.01

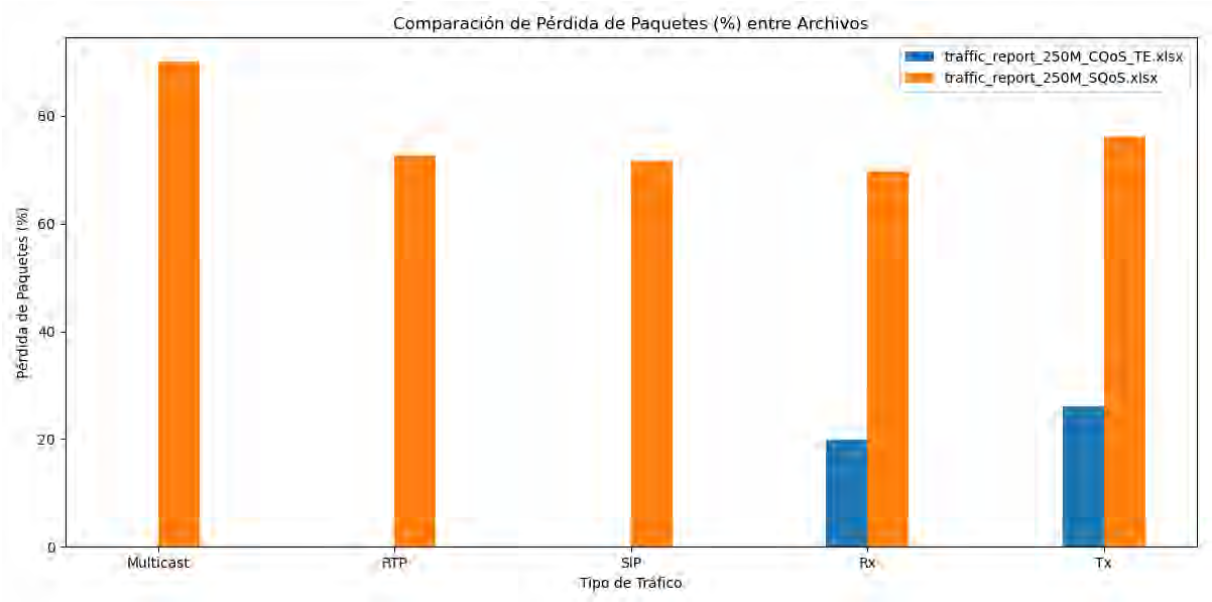


Figura 5.4.9 Perdida de paquetes para tráfico de 250 Mbps

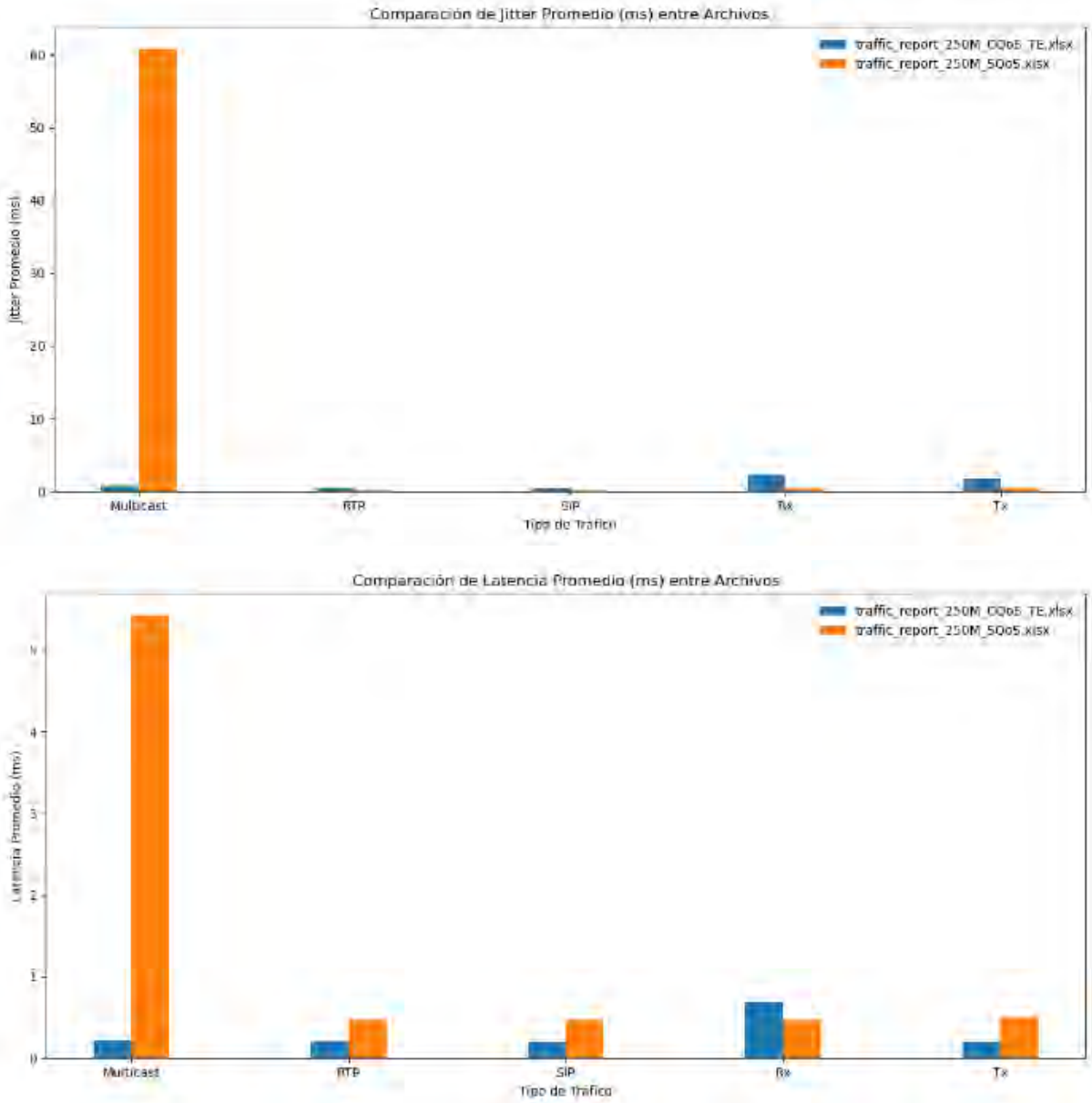


Figura 5.4.10 Jitter y Latencia para trafico 250 Mbps

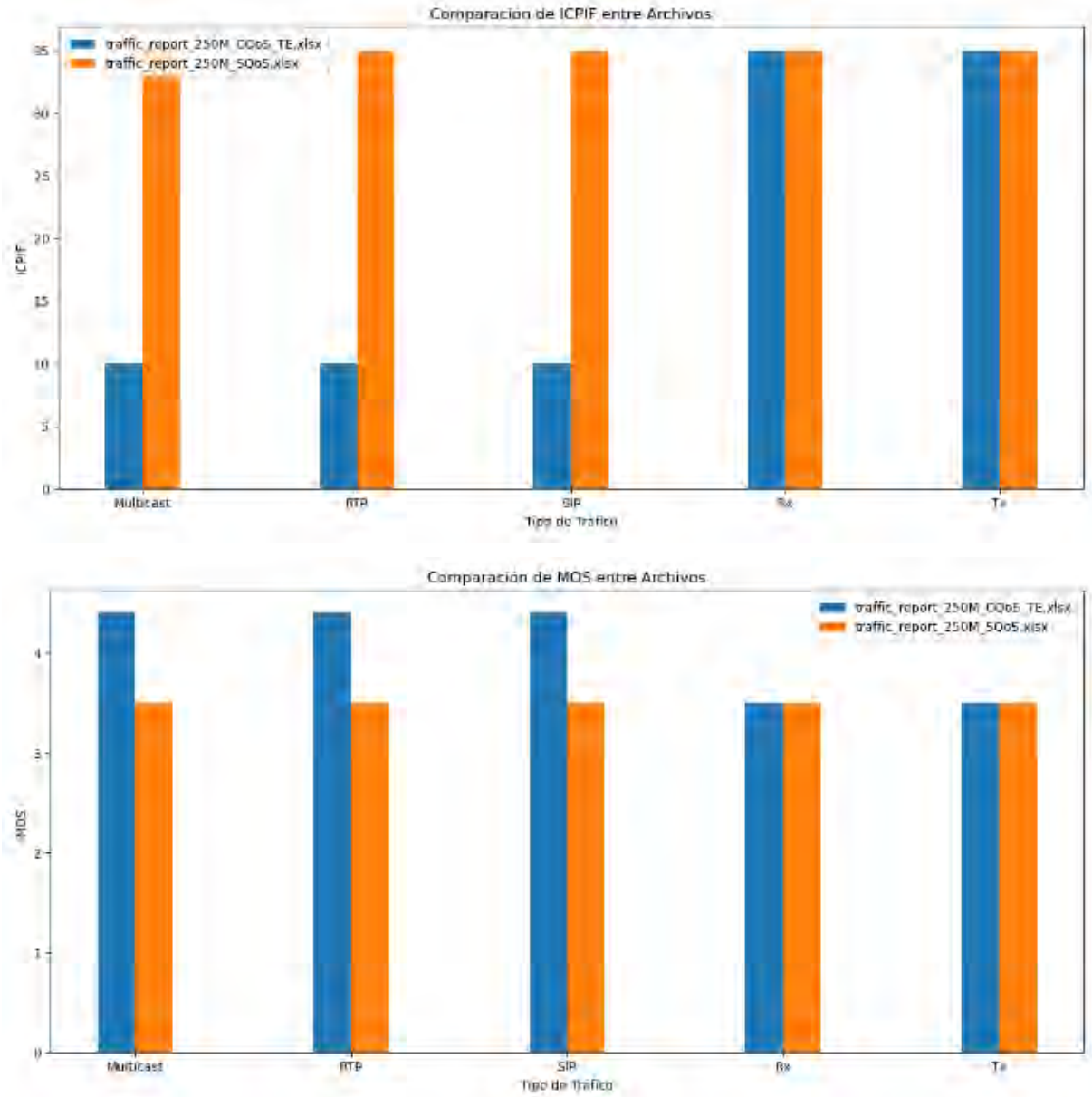


Figura 5.4.11 ICPF y MOS para trafico 250 Mbps

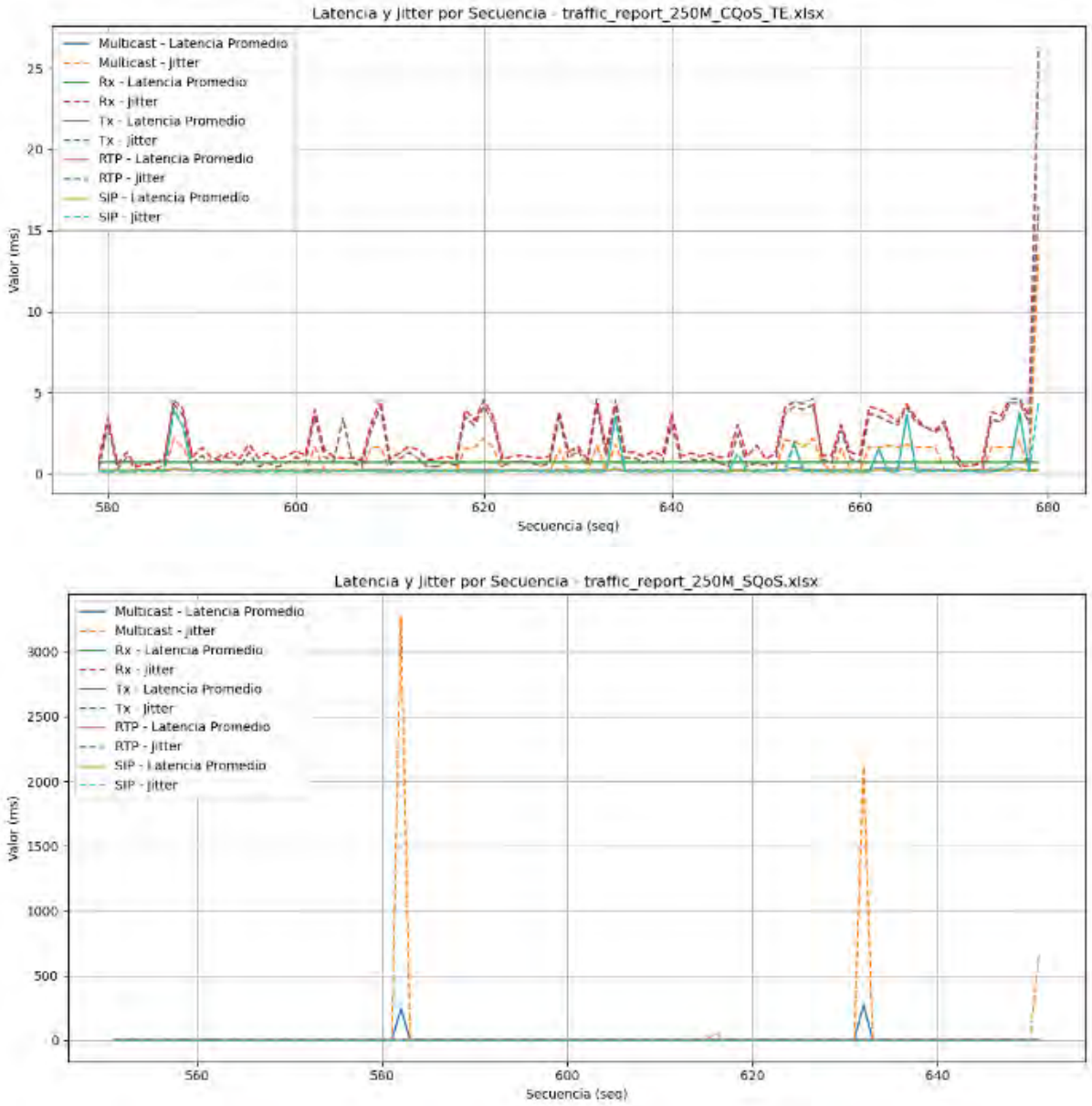


Figura 5.4.12 Grafica lineal para tráfico de 250 Mbps

- Se puede verificar del análisis de tráfico la generación de tablas y graficas comparativas para tráfico de 250 Mbps con y sin calidad de servicio, donde los parámetros a evaluar son métricas de tasa de Tx/Rx, perdida de paquetes, latencia, jitter, MOS e ICPIF, que nos permite evaluar el rendimiento de la red implementada, el cual transporta tráficos generadas por un generador de tráfico de red.
- Las tablas muestran métricas de rendimiento de red para tráficos con y sin calidad de servicio. La tabla 5.4.5 (tráfico de 250 Mbps con calidad de servicio) nos muestra que los parámetros de rendimiento están por debajo de los umbrales críticos de funcionamiento descrito en la sección 5.4.1 con lo que podemos concluir que el tráfico será optimo y estable. La métrica de MOS se encuentra entre los valores 3.51 y 4.41 lo

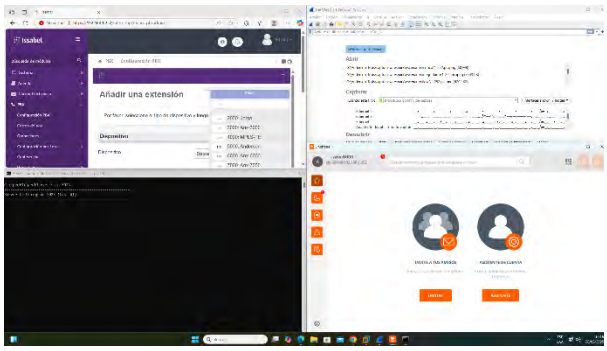
cual nos indica que son valores óptimos para tráficos críticos como VoIP. La métrica ICPIF se encuentra entre los valores de 10.1 que también indican comportamiento óptimo para el transporte de tráfico como VoIP y multicast.

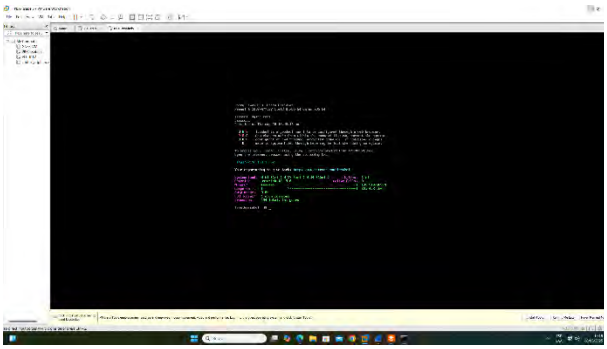
- De la tabla 5.4.6 (tráfico de 250 Mbps sin calidad de servicio) podemos verificar que los parámetros de rendimiento para los diferentes tipos de tráfico sobrepasan los valores umbrales listados en la sección 5.4.1 como es el caso de la perdida de paquetes que supera los 71.57% que afecta el rendimiento de la red generando retrasmisiones por perdida de paquetes. Las métricas de MOS están por encima del valor umbral de 3.5 el cual afectara a tráficos en tiempo real como es el caso de VoIP y multicast. La métrica de ICPIF sobrepasa el límite umbral de 20 (35.01), afectando de manera directa el rendimiento de la red para tráficos de VoIP y multicast.
- En las tablas y graficas se verifica que el rendimiento de la red está directamente relación a la calidad de servicio que se aplica a cada tipo de tráfico (VoIP, Multicast y Genérica). El tráfico con calidad de servicio muestra un mejor rendimiento para los diferentes tipos de tráfico.

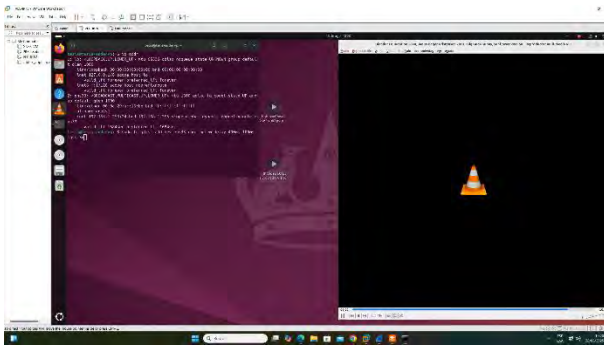
Se verifica el rendimiento de la red para los tres tipos de tráfico (160, 200 y 250 Mbps) generados por el generador de tráfico, sobre el ancho de banda de 200 Mbps de la red evaluada. Para tráfico de 160 Mbps la red se comporta de una manera estable en ambos casos tanto con y sin calidad de servicio evidenciándose en la tabla 5.4.1 un mejor rendimiento para tráfico con calidad de servicio. Para tráfico de 200 Mbps la red se comporta de una manera estable para el caso de tráfico con calidad de servicio como se muestra en la tabla 5.4.3, el rendimiento para una red sin calidad de servicio ve afectado su rendimiento como se muestra en la tabla 5.4.4. Para tráfico de 250 Mbps la red se comporta de una manera estable para el caso de tráfico con calidad de servicio como se muestra en la tabla 5.4.5, el rendimiento para una red sin calidad de servicio ve afectado su rendimiento como se muestra en la tabla 5.4.6, generándose caída de servicios (perdida de paquetes muy altas).

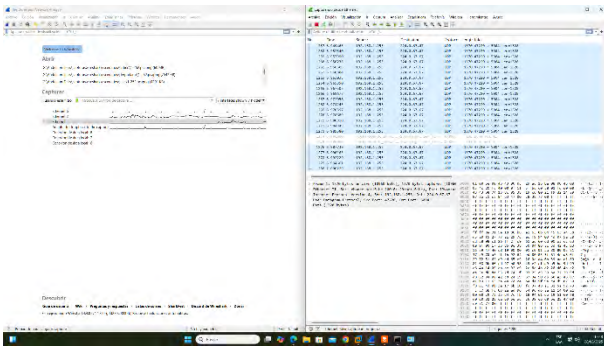
5.5 Analisis de una Red con Trafico Real

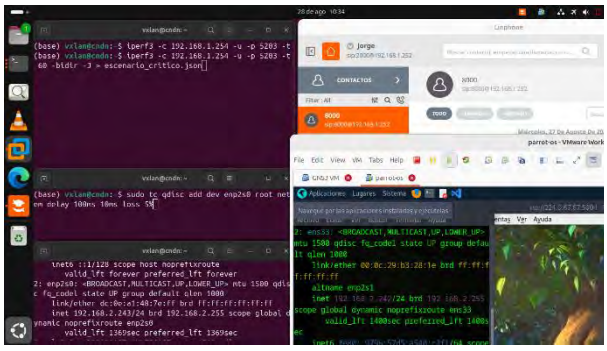
En este apartado del trabajo de tesis, relaizaremos un analisis de los paquetes de trafico con Wireshark, sobre trafico real generado entre servidores (Servidors Multicast, Telefonia IP y Iperf3) y clientes que consumen estos servicios (Cliente IPTV, Softphone, Iperf3 Cliente) y tambien se crearan condicones de red controladas (ingresar retardo, jitter, etc) en la red para ver el comportamiento de los diferentes traficos sobre que viajan a traves de la red. Esto se realizara con una aplicación de software NETEM.

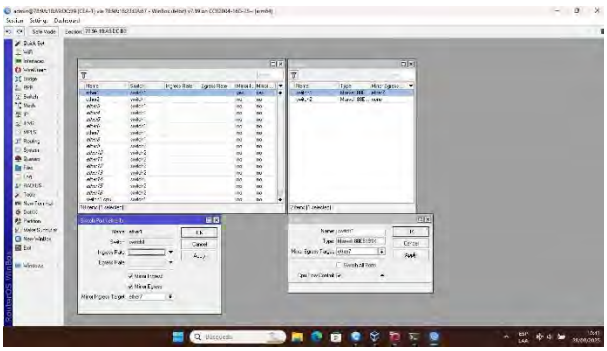












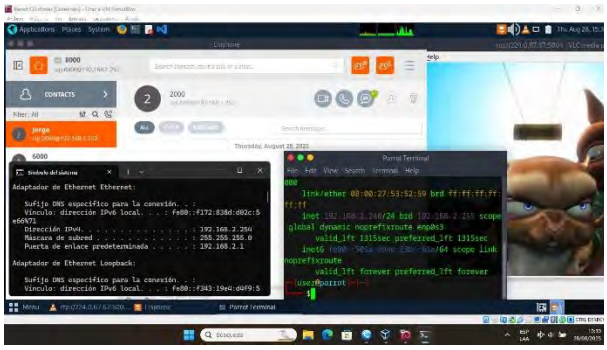


Figura 5.5.1 Configuraciones de la implementación

Tabla 5.5.1 Muestra la arquitectura implementada

[Servidores] – [CEA-1] – [PE1] - [MPLS Core] – [PE5] – [CEA-5] - [Usuarios Finales]		
PBX Issabel Servidor VLC Servidor IPERF3	P2, P3, P4 (Core MPLS) TE-LSPs activos	Softphone Clientes VLC Clientes IPERF3

5.5.1 Captura de Paquetes de Trafico de Red con Wireshark

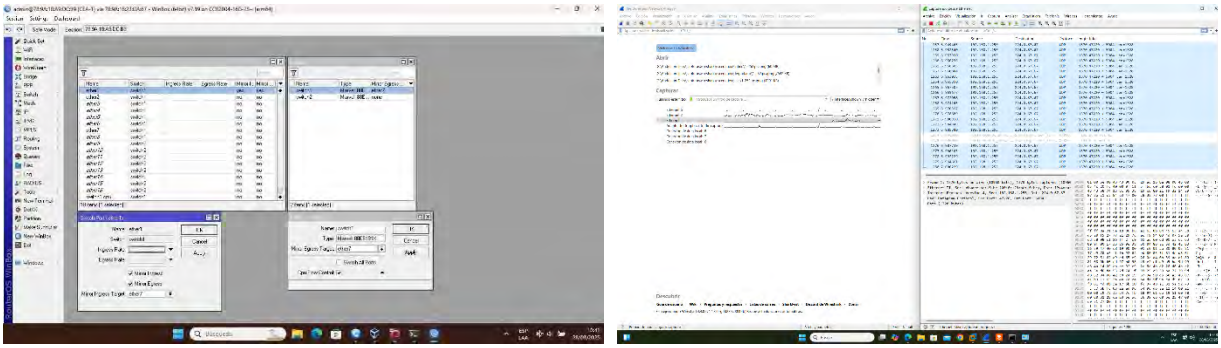


Figura 5.5.2 Port Mirror y PC en modo promiscuo

Flujo de Tráfico Esperado:

Dirección Servidores hacia Usuarios Finales (PE1 hacia PE5):

- VoIP: PBX Issabel (PE1) con Softphones (PE5)
- Multicast: Servidor VLC Player (PE1) con Clientes VLC Player (PE5)
- IPERF3: Servidor (PE1) con Cliente (PE5)

Dirección de Usuarios Finales hacia Servidores (PE5 hacia PE1):

- Señalizacion SIP: Softphones hacia PBX Issabel
- IPERF3: Cliente hacia Servidor
- IGMP/PIM-SM: Solicitudes multicast

Lo que se espera ver en este analisis de la implementacion, sera:

En capturas sobre el router PE1 (Ingress):

- Paquetes IP nativos entrando desde servidores
- Encapsulación: IP → Etiqueta de Servicio (VPN3) → Etiqueta VPLS → Etiqueta TE

En capturas en el Core (P2/P3/P4):

- Stack MPLS visible: Etiqueta de tunnel de TE (Ingenieria de trafico)
- Switching: Solo conmutación de etiqueta de ingenieria de trafico (etiqueta de transporte).

En capturas en el router PE5 (Egress):

- Desencapsulación: TE-Label sobre VPLS-Label sobre Etiqueta de Servicio (VPN3) sobre IP
- Entrega de paquetes IP nativos a usuarios finales

5.5.2 Análisis de Paquetes sobre Router CEA1(Eth1)

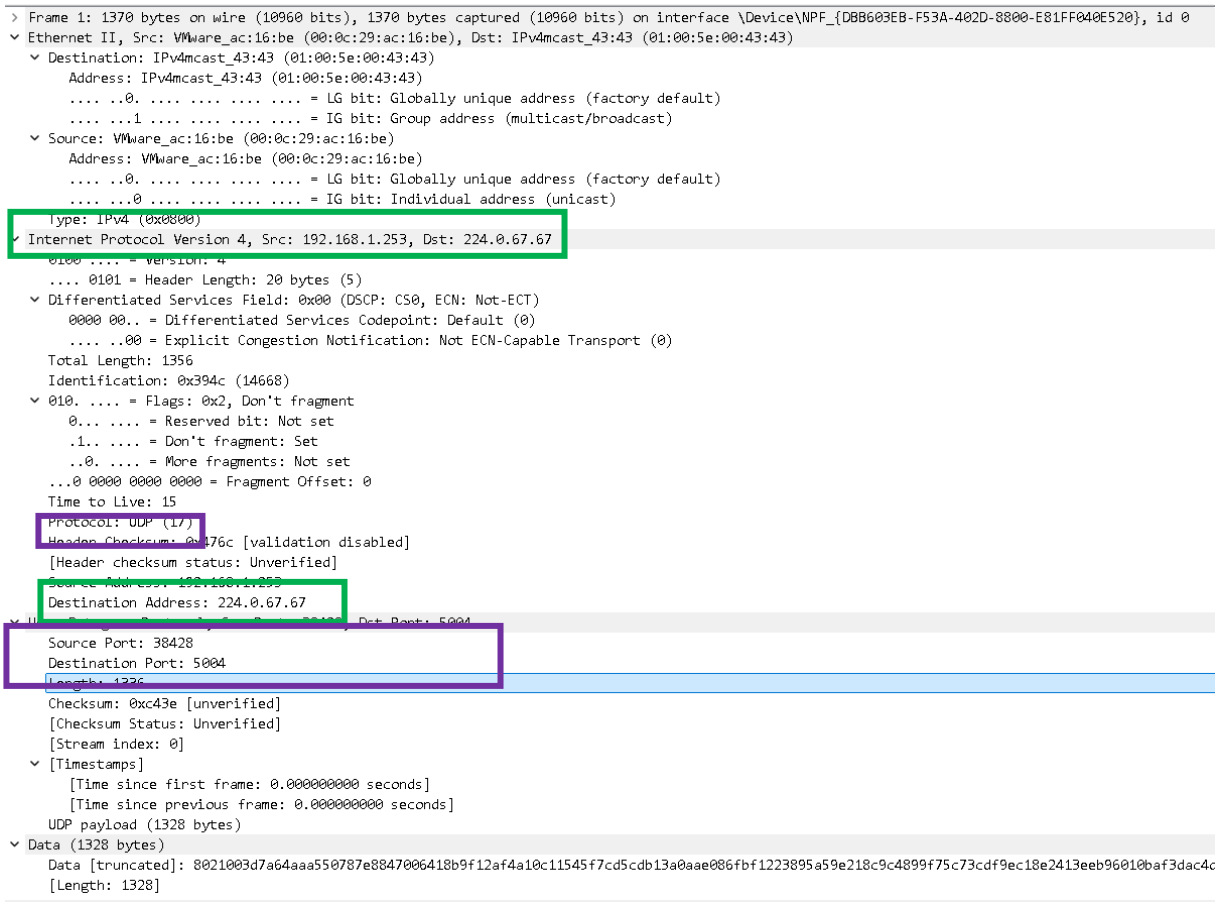


Figura 5.5.3 Captura de paquetes en CEA1

5.5.2.1 Análisis Detallado del Paquete (Frame 1)

Basado en la imagen de la captura de Wireshark en el router CEA1, antes de entrar al dominio MPLS (es decir, en el borde del cliente, la interfaz conectada a los servidores). Por lo tanto, aquí vemos el paquete original del cliente (tráfico multicast de streaming con VLC Player), sin encapsulación MPLS. No hay pila de etiquetas MPLS visible (el Ethertype es 0x0800 para IPv4, no 0x8847 para MPLS unicast), lo que confirma que no existe encapsulacion por etiquetas.

El paquete es un datagrama UDP multicast, que se alinea con uno de los servicios implementados: el streaming multicast vía VLC Player. En el dominio MPLS, este paquete se viajara a traves de la L3VPN que luego se encapsulara en un túnel VPLS (para transparencia

L2) y luego en un túnel de Ingeniería de Tráfico (TE) para seguir la ruta: CEA1 – PE1 – P3 – P4 – PE5 – CEA5.

5.5.2.2 Metadatos del Frame

Número de Frame: 1

Longitud del Frame: 1378 bytes en el cable (10960 bits capturados)

Longitud Capturada: 1378 bytes

Tipo de Encapsulación: Ethernet

Protocolos en el Frame: ethernet:ip, udp, data (sin MPLS ni disección de capas superiores más allá de UDP)

5.5.2.3 Capa 2: Cabecera Ethernet (14 bytes)

Tabla 5.5.2 Campos de la cabecera ethernet en CEA-1

Campo	Valor	Descripción
MAC de Destino	01:00:5e:00:43:43	Dirección MAC multicast, derivada de la IP multicast de destino (224.0.67.67). Sigue el mapeo estándar IETF: bits altos fijos como 01:00:5E:00:00:00, y los 23 bits bajos de la IP. Indica que es para miembros del grupo multicast en el segmento local.
MAC de Origen	00:0c:29:ac:16:be	MAC virtual asignada por Vmware (OUI 00:0C:29 pertenece a Vmware). El origen es una máquina virtual o interfaz virtual, servidor VLC conectado a CEA1.
Ethertype	0x0800	Ipv4. Confirma ausencia de MPLS (que usaría 0x8847 para unicast o 0x8848 para multicast).

5.5.2.4 Capa 3: Cabecera Ipv4 (20 bytes)

Tabla 5.5.3 Campos de la cabecera Ipv4 en CEA-1

Campo	Valor	Descripción
Versión	4	Estándar Ipv4.
Longitud de Cabecera (IHL)	5 (20 bytes)	Sin opciones IP adicionales.
Longitud Total	1356 bytes	Incluye cabecera IP + cabecera UDP + payload.
Identificación	0x339c (13468 decimal)	Para reensamblaje de fragmentos (no aplica aquí).
Flags	0x2 (binario 010)	Bit reservado: 0; Don't Fragment (DF): 1 (evita fragmentación); More Fragments (MF): 0.
Fragment Offset	0	No fragmentado.

Time to Live (TTL)	15	TTL inicial bajo, posiblemente configurado por la aplicación para limitar el alcance multicast. Se decrementará en la ruta.
Protocolo	17 (UDP)	Protocolo que transportara
IP de Origen	192.168.1.253	Dirección privada, del servidor VLC en la LAN del cliente detrás de CEA1.
IP de Destino	224.0.67.67	Grupo multicast (Clase D). En el bloque de control local, pero extendido; grupo personalizado para el streaming. Los clientes se suscriben vía IGMP.

5.5.2.5 Capa 4: Cabecera UDP (8 bytes)

Tabla 5.5.4 Campos de cabecera UDP, CEA-1

Campo	Valor	Descripción
Puerto de Origen	38428	Puerto efímero (rango dinámico >1023), asignado por el SO/aplicación (VLC). Puede variar por sesión.
Puerto de Destino	5004	Puerto conocido para RTP (Real-time Transport Protocol), para streaming video/audio.
Longitud	1336 bytes	Cabecera UDP + payload.

5.5.2.6 Payload (1328 bytes)

- Datos: Mostrado truncado en la imagen, comenzando con hex: 8021903d7a64aaa5509787e8847900641b09f12af4a41b0c11545f7cd5cdb13a0aaea086fbf1223895a5e218c9cd889f75f73cdf9ec18a2413eeb96691baf3d4ac…

- Análisis de Estructura del Payload:
    - Se disecciona como un paquete RTP.
        - Cabecera RTP (primeros 12 bytes):
            - Byte 0: 0x80 (128 decimal) – Versión 2 (bits 7-6: 10), Padding=0, Extension=0, CSRC Count=0.
            - Byte 1: 0x21 (33 decimal) → Marker=0 (bit 7: 0), Payload Type (PT)=33 (MPEG-2 Transport Stream, común para video en VLC).
            - Bytes 2-3: Número de Secuencia = 0x20c9 (8393 decimal) – Rastrea orden de paquetes para detectar pérdidas.
            - Bytes 4-7: Timestamp = 0x146be0af (342614191 decimal) – Temporización de medios para sincronización.
            - Bytes 8-11: SSRC Identifier = 0x3ea71ad3 (1051138771 decimal) – ID único de fuente de sincronización para el stream.

        - Después de la cabecera RTP: Datos de medios reales, paquetes MPEG-2 TS (Transport Stream) de 188 bytes cada uno, con video/audio codificado del servidor VLC.
    - Identificación del Servicio: Coincide con el servicio multicast de streaming (VLC Player).

- Longitud: 1328 bytes – Payload grande, típico para video para minimizar overhead, pero bajo MTU Ethernet (1500 bytes) para evitar fragmentación.

- Servicio: Multicast (streaming con VLC). La IP multicast y encapsulación UDP/RTP lo confirman. Los otros servicios (telefonía Issabel PBX o tráfico general iPerf3) muestran puertos/protocolos diferentes.

5.5.3 Captura de Paquetes en PE1-ETH2

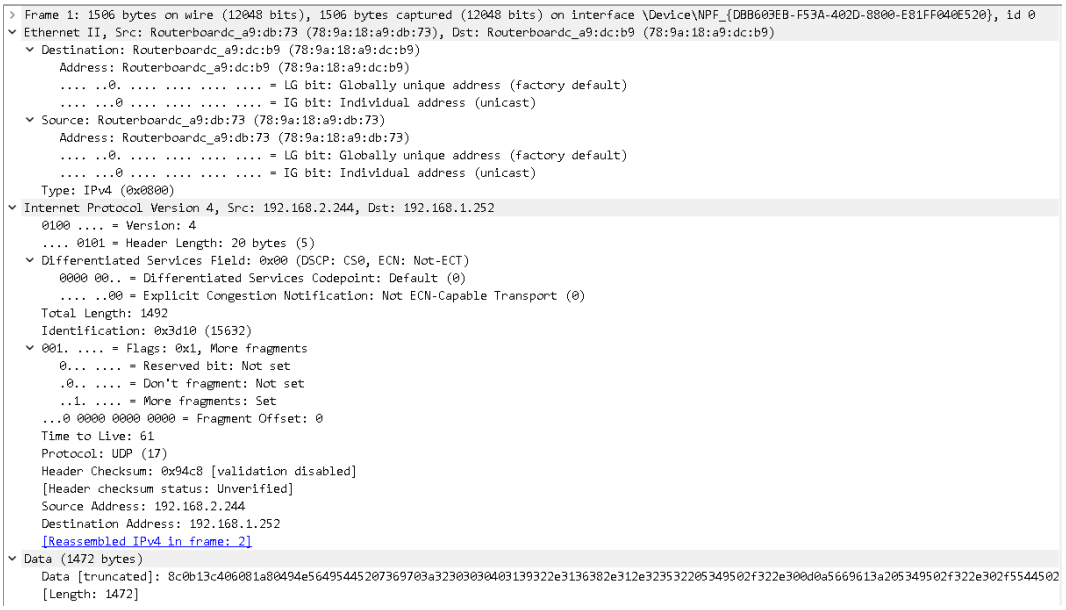


Figura 5.5.4 Captura de paquetes con Wireshark en interfaz eth2 de PE1

5.5.3.1 Análisis Detallado de Paquete (PE1-eth2)

Basado en la nueva imagen de Wireshark, la estructura del paquete capturado en la interfaz eth2 del router PE1, que está conectada a CEA1. Este tráfico aún está en formato IP y no incluye etiquetas MPLS, lo que confirma que la captura se realizó antes de que el paquete entre en el dominio MPLS (es decir, en la interfaz de entrada de PE1 hacia CEA1, antes de la encapsulación en el túnel VPLS y el túnel de Ingeniería de Tráfico).

Dado que la ruta es CEA1 – PE1 – P3 – P4 – PE5 – CEA5, esta captura representa el tráfico recibido por PE1 desde CEA1, aún en su forma original (pre-encapsulación MPLS).

5.5.3.2 Metadatos del Frame

- Número de Frame: 1
- Longitud del Frame: 1506 bytes en el cable (12048 bits capturados)
- Longitud Capturada: 1506 bytes
- Tipo de Encapsulación: Ethernet
- Protocolos en el Frame: ethernet, ip, udp, data (sin MPLS, aún en formato IP nativo)

5.5.3.3 Capa 2: Cabecera Ethernet (14 bytes)

Tabla 5.5.5 Campos de la cabeceara ethernet – PE1-ether2

Campo	Valor	Descripción
MAC de Destino	Routerboardc_a9:dc:b9 (78:9ª:18:a9:dc:b9)	Dirección MAC unicast, de la interfaz de PE1 (RouterBoard Mikrotik).
MAC de Origen	Routerboardc_a9:db:73 (78:9ª:18:a9:db:73)	Dirección MAC unicast, correspondiente a CEA1 (otro RouterBoard Mikrotik). Indica que el tráfico proviene de CEA1 hacia PE1.
Ethertype	0x0800	Ipv4. No hay MPLS aún (Ethertype 0x8847 estaría presente si el tráfico estuviera encapsulado).

5.5.3.4 Capa 3: Cabecera IPv4 (20 bytes)

Tabla 5.5.6 Campos de la cacera IPv4 en -PE1-ether2

Campo	Valor	Descripción
Versión	4	Estándar IPv4.
Longitud Total	1492 bytes	Incluye cabecera IP + datos
Identificación	0x3d10 (15632 decimal)	Identificador común para todos los fragmentos de este datagrama, usado para reensamblaje.
Protocolo	17 (UDP)	Protocolo a ser trasportado

IP de Origen	192.168.2.244	IP del cliente de telefonía
IP de Destino	192.168.1.252	IP del servidor PBX

5.5.3.5 Capa 4: Cabecera UDP (8 bytes)

- Puerto de Origen y Destino: Telefonía IP 5060.

5.5.3.6 Payload (1472 bytes)

- Datos: Truncado, comenzando con hex: 8c0b13c4068a1a8494….

  Análisis de Estructura del Payload:

  - Este fragmento contiene datos de un protocolo de señalización, SIP (Session Initiation Protocol), basado en el texto visible ("SIP/2.0" y "INVITE"). Esto sugiere que este paquete corresponde al servicio de telefonía IP con Issabel PBX, no al streaming multicast VLC (que usaba RTP en puerto 5004).
  - Cabecera SIP:
    - "INVITE": Método SIP para iniciar una sesión (llamada telefónica).
    - "SIP/2.0": Versión del protocolo.
    - Direcciones como "192.168.2.244" (de un softphone) y "192.168.1.252" (Issabel PBX en CEA1).
  - Longitud: 1472 bytes, ocupando casi todo el espacio disponible tras cabeceras, típico para mensajes SIP con cuerpos SDP (Session Description Protocol) que describen la sesión multimedia.

- Identificación del Servicio: Telefonía IP con Issabel PBX. Diferente del streaming VLC (RTP/UDP puerto 5004) y del tráfico general iPerf3 (puerto 5201).
- Servicio: Telefonía IP (Issabel PBX). La presencia de SIP sugiere que este paquete es parte de la señalización para establecer una llamada, transportada a través de la VPN3 y los túneles VPLS/TE.
- Pila de Etiquetas MPLS: Ausente aquí, como esperábamos en la interfaz eth2 de PE1.

5.5.4 Captura de Paquetes en PE1-Eth1

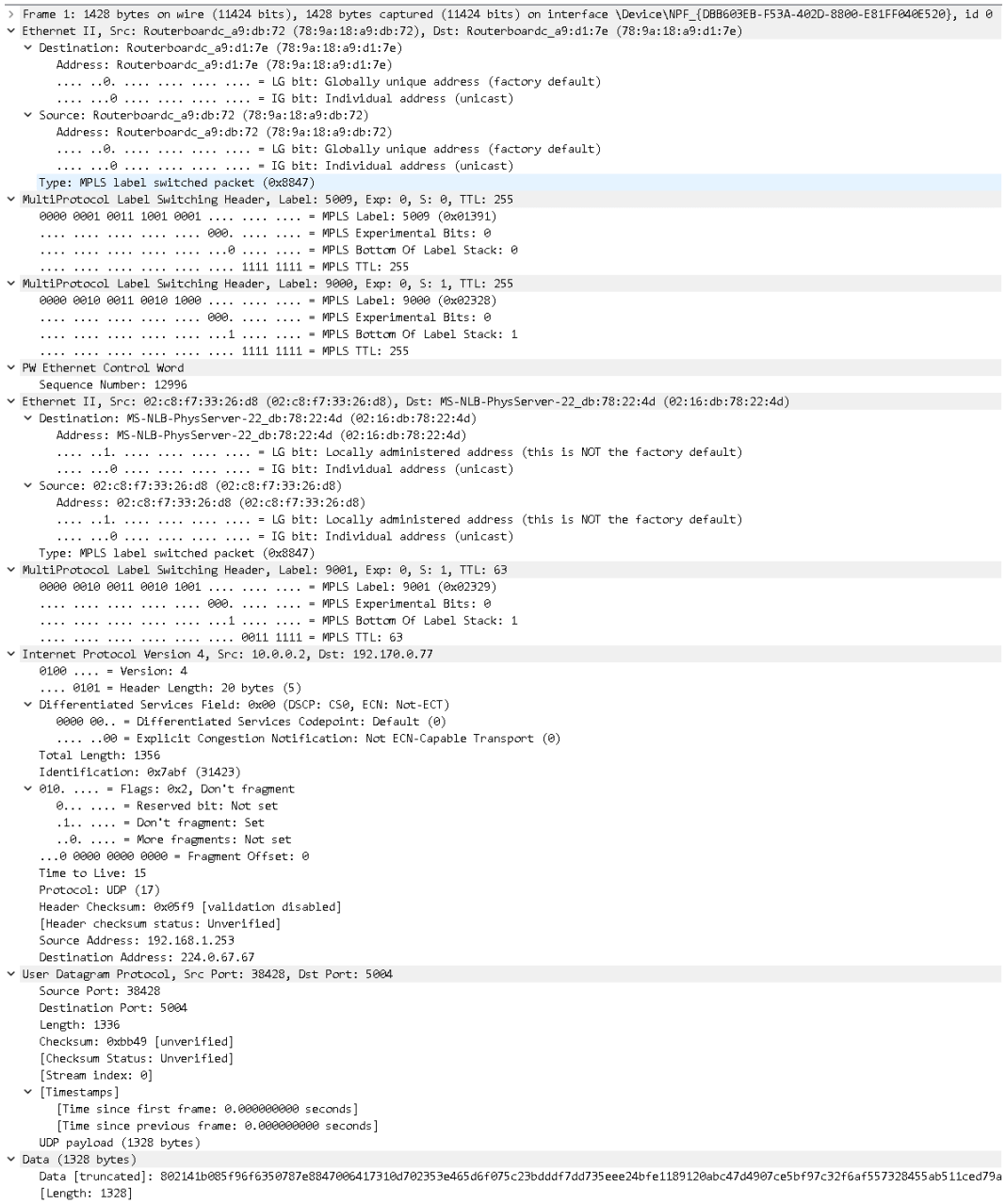


Figura 5.5.5 Captura de Paquete en el router PE1 interfaz Eth1

5.5.4.1 Análisis Detallado de Paquete (PE1- Eth1)

Basado en la imagen de la captura con Wireshark, se analizará la estructura del paquete capturado en la interfaz eth1 del router PE1, que está conectada al dominio IP/MPLS. Esta captura muestra el paquete después de la encapsulación MPLS en la salida de PE1 hacia el núcleo de la red. Aquí observaremos la pila de etiquetas MPLS junto con el paquete IP/UDP original, lo que refleja la transición del tráfico desde el dominio IP al dominio MPLS.

Este paquete corresponde al servicio de streaming multicast con VLC Player, como lo indican los puertos (origen 38428, destino 5004) y la estructura RTP, similar a la captura inicial en CEA1.

5.5.4.2 Metadatos del Frame

- Número de Frame: 1
- Longitud del Frame: 1428 bytes en el cable (11424 bits capturados)
- Longitud Capturada: 1428 bytes
- Tipo de Encapsulación: Ethernet
- Protocolos en el Frame: ethernet, mpls, IPv4, udp, data (incluye MPLS, confirmando la encapsulación)

Este frame transporta un datagrama UDP encapsulado en MPLS.

5.5.4.3 Capa 2: Cabecera Ethernet (14 bytes)

Tabla 5.5.7 Campos de la cabecera ethernet – PE1-ether1

Campo	Valor	Descripción
MAC de Destino	Routerboardc_a9:d1:7e (78:9a:18:a9:d1:7e)	Dirección MAC unicast, la interfaz del router (P3), otro RouterBoard Mikrotik.
MAC de Origen	Routerboardc_a9:db:72 (78:9a:18:a9:db:72)	Dirección MAC unicast de PE1, indicando que este es el punto de salida hacia el dominio MPLS.
Ethertype	0x8847	MPLS unicast. Confirma que el paquete ha sido encapsulado con etiquetas MPLS.

5.5.4.4 Capa 2.5: Cabecera MPLS (8 bytes por etiqueta)

Tabla 5.5.8 Cabecera MPLS en PE1-ether1

Campo	Valor	Descripción
Etiqueta del tunnel de Ingeniería de trafico	Label: 5009, Exp: 0, S: 0, TTL: 255	Etiqueta externa (transporte TE). Label 5009 identifica el LSP (Label Switched Path).
Etiqueta del túnel VPLS	Label: 9000, Exp: 0, S: 1, TTL: 255	Etiqueta interna (VPLS pseudowire). Label 9000 identifica el VC (Virtual Circuit) del túnel VPLS.

Tunnel de servicio (VPN3)	Label: 9001, Exp: 0, S: 1, TTL: 255	Etiqueta interna (VPN3) Label 9001 identifica el servicio VPN3 que la red trasporta.

Pila de Etiquetas MPLS:

- Etiqueta Externa (5009): Corresponde al túnel de Ingeniería de Tráfico (TE) que dirige el tráfico por la ruta PE1 - P3 - P4 - PE5.
- Etiqueta Interna (9000): Corresponde al túnel VPLS, que transporta el tráfico VPN3 de forma transparente entre CEA1 y CEA5.
- Etiqueta Interna (9001): Corresponde a la etiqueta de servicio VPN3.

5.5.4.5 Capa 3: Cabecera IPv4 (20 bytes)

Tabla 5.5.9 Campos de la cabecera IPv4 en PE1-ether1

Campo	Valor	Descripción
Versión	4	Estándar IPv4.
Longitud Total	1356 bytes	Incluye cabecera IP + cabecera UDP + payload.
Identificación	0x7a6f (31343 decimal)	Identificador del datagrama IP original.
Flags	0x0 (binario 000)	Bit reservado: 0; Don't Fragment (DF): 0; More Fragments (MF): 0 (no fragmentado).
Fragment Offset	0	Datagrama completo.
Protocolo	17 (UDP)	Protocolo a transportar
IP de Origen	192.168.1.253	Dirección privada, el servidor VLC en CEA1.
IP de Destino	224.0.67.67	Grupo multicast, destino del streaming VLC.

5.5.4.6 Capa 4: Cabecera UDP (8 bytes)

Tabla 5.5.10 Cabecera UDP en PE1-ether1

Campo	Valor	Descripción
Puerto de Origen	38428	Puerto efímero, asignado por el servidor VLC

Puerto de Destino	5004	Puerto RTP, confirma streaming multicast con VLC.
Longitud	1336 bytes	Cabecera UDP + payload.

5.5.4.7 Payload (1328 bytes)

- Datos: Truncado, comenzando con hex: 802141b05f6f37078e847906417310d70….
- Análisis de Estructura del Payload:
    - Se identifica como un paquete RTP.
        - Cabecera RTP (primeros 12 bytes):
            - Byte 0: 0x80 - Versión 2, Padding=0, Extension=0, CSRC Count=0.
            - Byte 1: 0x21 - Marker=0, Payload Type (PT)=33 (MPEG-2 TS).
            - Bytes 2-3: 0x41b0 (16816 en decimal) Número de Secuencia variable.
            - Bytes 4-7: 0x85f96f63 (2247716707 valor decimal) Timestamp variable.
            - Bytes 8-11: 0x50787e88 (1350073992valor decimal) SSRC variable.
        - Datos: MPEG-2 TS para video/audio del streaming VLC de 188 Bytes.
    - Servicio: Streaming multicast con VLC Player.
- Longitud: 1328 bytes, ocupando el payload completo tras cabeceras.

Contexto de la topología:

- Servicio: Streaming multicast (VLC Player). Los puertos y la estructura RTP lo confirman.
- Pila de Etiquetas MPLS: Presente con tres etiquetas:
    - Etiqueta 5009 (TE) para ruta de ingeniería de tráfico.
    - Etiqueta 9000 (VPLS) para el pseudowire.
    - Etiqueta 9001 (servicio VPN3).
    - Esto valida el diseño donde VPLS conecta con TE para transportar el tráfico VPN3.

5.5.5 Captura de Paquetes en P3-Eth2

Figura 5.5.6 Captura de paquetes con Wireshark en la interfaz ETH2 del router 3

5.5.5.1 Análisis de Paquete (P3-Eth2)

Basado en la captura de imagen de Wireshark, analizaremos la estructura del paquete capturado en la interfaz eth2 del router P3, que forma parte del núcleo de tu red IP/MPLS. Este router P3 actúa como un LSR (Label Switching Router) en el dominio MPLS, procesando el tráfico encapsulado con etiquetas MPLS. La captura muestra el paquete después de atravesar PE1, permitiendo analizar cómo se manejan las etiquetas MPLS en el núcleo.

Este paquete corresponde al servicio de streaming multicast con VLC Player, como lo indican los puertos UDP (origen 38428, destino 5004) y la estructura RTP, consistente con capturas previas en CEA1 y PE1.

5.5.5.2 Metadatos del Frame

- Número de Frame: 1
- Longitud del Frame: 1428 bytes en el cable (11424 bits capturados)
- Longitud Capturada: 1428 bytes
- Tipo de Encapsulación: Ethernet
- Protocolos en el Frame: ETHERNET, MPLS, IPV4, UDP, data (incluye MPLS, confirmando la encapsulación)

Este frame transporta un datagrama UDP encapsulado en MPLS.

5.5.5.3 Capa 2: Cabecera Ethernet (14 bytes)

Tabla 5.5.11 Cabecera ethernet en P3-ether2

Campo	Valor	Descripción
MAC de Destino	Routerboardc_2b:1f:a3 (44:01:c2:b1:f:a3)	Dirección MAC unicast, del router P4, otro RouterBoard Mikrotik.
MAC de Origen	Routerboardc_a9:d1:7f (78:9a:18:a9:d1:7f)	Dirección MAC unicast de P3.
Ethertype	0x8847	MPLS unicast. Confirma que el paquete sigue encapsulado con etiquetas MPLS.

5.5.5.4 Capa 2.5: Cabecera MPLS (8 bytes por etiqueta)

Tabla 5.5.12 Cabecera MPLS – P3-ether2

Campo	Valor	Descripción
Multiprotocol Label Switching Header	Label: 7009	Etiqueta externa (Etiqueta de transporte TE). Label 7009 identifica el LSP (Label Switched Path) del túnel de ingeniería de tráfico.
Multiprotocol Label Switching Header	Label: 9000	Etiqueta interna (VPLS pseudowire). Label 9000 se mantiene igual que en PE1, indicando que no cambia en el núcleo (especifica el VC del túnel VPLS).
Multiprotocol Label Switching Header	Label: 9001	Etiqueta 9001 interna de servicio VPN3.

Pila de Etiquetas MPLS:

- Etiqueta Externa (7009): Sustituye la etiqueta 5009 de PE1, típico del intercambio de etiquetas en MPLS. P3 ha actualizado la etiqueta de transporte TE según su tabla de forwarding para dirigir el tráfico hacia P4.
- Etiqueta Interna (9000): Se preserva, ya que identifica el tunnel VPLS, que no cambia en el núcleo.
- Etiqueta Interna (9001): Se preserva, ya que identifica el servicio VPN3.

5.5.5.5 Capa 3: Cabecera IPv4 (20 bytes)

Tabla 5.5.13 Cabecera IPv4 en P3-ether2

Campo	Valor	Descripción
Versión	4	Estándar IPv4.
Longitud Total	1356 bytes	Incluye cabecera IP + cabecera UDP + payload.
Identificación	0x1c5b (7099 decimal)	Identificador del datagrama IP original.
Flags	0x0 (binario 000)	Bit reservado: 0; Don't Fragment (DF): 0; More Fragments (MF): 0 (no fragmentado).

Fragment Offset	0	Datagrama completo.
Protocolo	17 (UDP)	Protocolo a transportar
IP de Origen	192.168.1.253	Dirección privada, el servidor VLC en CEA1.
IP de Destino	224.0.67.67	Grupo multicast, destino del streaming VLC.

5.5.5.6 Capa 4: Cabecera UDP (8 bytes)

Tabla 5.5.14 Cabecera UDP en P3-ether2

Campo	Valor	Descripción
Puerto de Origen	38428	Puerto efímero, asignado por el servidor VLC.
Puerto de Destino	5004	Puerto RTP, confirma streaming multicast con VLC.
Longitud	1336 bytes	Cabecera UDP + payload.

5.5.5.7 Payload (1328 bytes)

- Datos: Truncado, comenzando con hex: 8021dbcba5d152678784709617310d702….
- Análisis de Estructura del Payload:
    - Se identifica como un paquete RTP.
        - Cabecera RTP (primeros 12 bytes):
            - Byte 0: 0x80 → Versión 2, Padding=0, Extension=0, CSRC Count=0.
            - Byte 1: 0x21 → Marker=0, Payload Type (PT)=33 (MPEG-2 TS).
            - Bytes 2-3: Número de Secuencia variable.
            - Bytes 4-7: Timestamp variable.
            - Bytes 8-11: SSRC variable.
        - Datos: MPEG-2 TS para video/audio del streaming VLC – 188 Bytes.
    - Servicio: Streaming multicast con VLC Player.
- Longitud: 1328 bytes, ocupando el payload completo tras cabeceras.

Contexto en la topología:

- Servicio: Streaming multicast (VLC Player).
- Pila de Etiquetas MPLS: Actualizada en P3:
    - Etiqueta externa cambió de 5009 (PE1) a 7009 (P3), reflejando el intercambio de etiquetas en el núcleo.
    - Etiqueta interna (9000) se mantiene, como esperado en P3 (LSR) que no modifica el túnel VPLS.
    - Etiqueta interna (9001) se mantiene, el router P3(LSR) no modifica la etiqueta de servicio VPN3.
- Procesamiento en el Núcleo: P3 actuó como LSR, intercambiando la etiqueta de transporte (TE).

5.5.6 Captura de paquetes en P4-ETH1

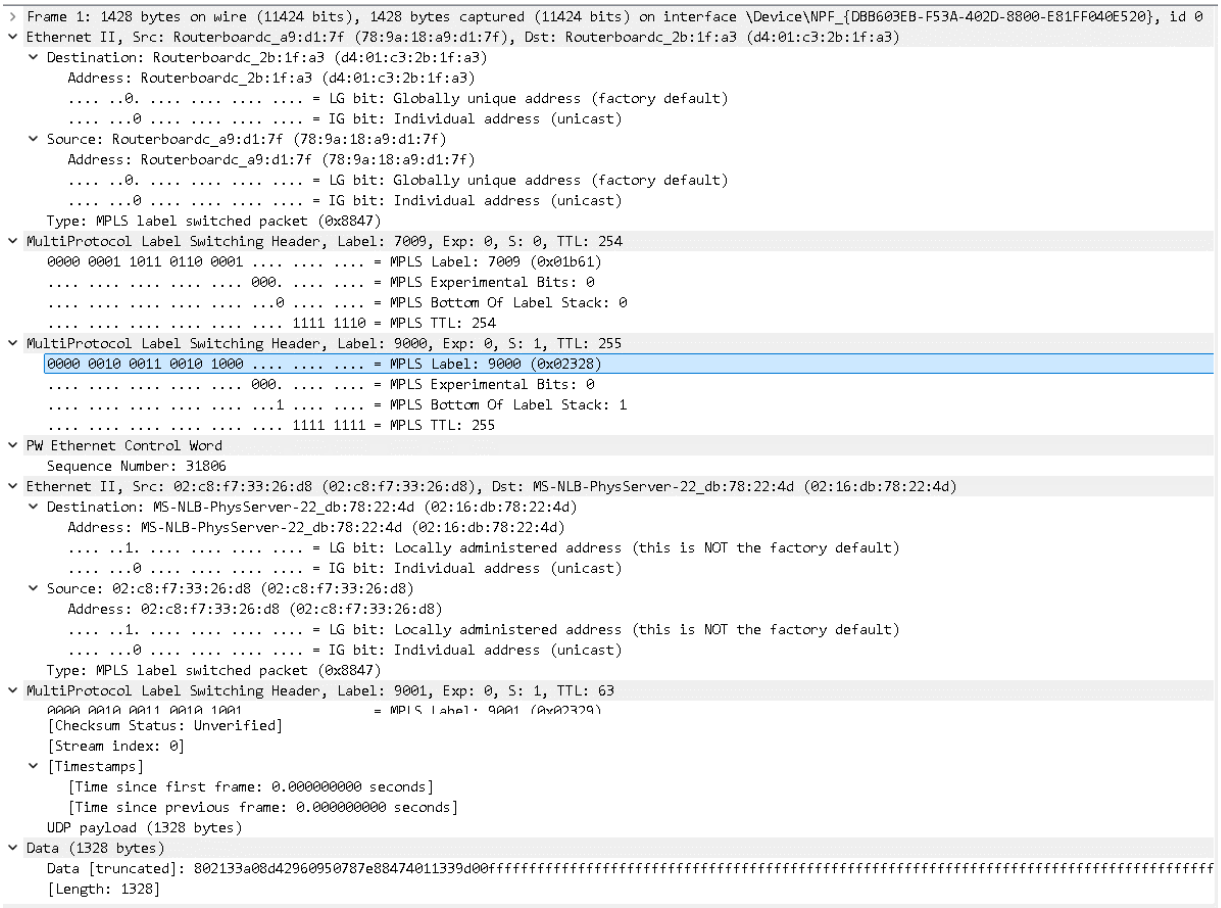


Figura 5.5.7 Captura de paquetes en la interfaz ETH1 del router P4

5.5.6.1 Análisis de Paquete (Eth1 de P4)

Basado en la imagen de Wireshark, analizaremos la estructura del paquete capturado en la interfaz eth1 del router P4, que forma parte del núcleo de tu red IP/MPLS (ruta CEA1 → PE1 → P3 → P4 → PE5 → CEA5). Como P4 es un LSR (Label Switching Router) en el dominio MPLS y está conectado al router de borde PE5, esta captura muestra el paquete después de atravesar P3 y al salir hacia PE5. Esto nos permite observar cómo se procesan las etiquetas MPLS en el núcleo y cómo se preparan para la desencapsulación en PE5.

Este paquete corresponde al servicio de streaming multicast con VLC Player, como lo indican los puertos UDP (origen 38428, destino 5004) y la estructura RTP, consistente con capturas previas en CEA1, PE1 y P3.

5.5.6.2 Metadatos del Frame

- Número de Frame: 1
- Longitud del Frame: 1428 bytes en el cable (11424 bits capturados)
- Longitud Capturada: 1428 bytes
- Tipo de Encapsulación: Ethernet
- Protocolos en el Frame: ethernet, mpls, ipv4, udp, data (incluye MPLS, confirmando la encapsulación)

Este frame transporta un datagrama UDP encapsulado en MPLS.

5.5.6.3 Capa 2: Cabecera Ethernet (14 bytes)

Tabla 5.5.15 Cabecera ethernet – P4-eth1

Campo	Valor	Descripción
MAC de Destino	Routerboardc_2b:1f:a3 (44:01:c2:b1:f:a3)	Dirección MAC unicast, de la interfaz de PE5, otro RouterBoard Mikrotik.
MAC de Origen	Routerboardc_a9:d1:7f (78:9a:18:a9:d1:7f)	Dirección MAC unicast de P4.
Ethertype	0x8847	MPLS unicast. Confirma que el paquete sigue encapsulado con etiquetas MPLS.

5.5.6.4 Capa 2.5: Cabecera MPLS (8 bytes por etiqueta)

Tabla 5.5.16 Cabecera MPLS – P4-eth1

Campo	Valor	Descripción
Multiprotocol Label Switching Header	Label: 7009	Etiqueta externa (transporte TE). Label 7009 identifica el LSP (Label Switched Path) de ingeniería de tráfico.
Multiprotocol Label Switching Header	Label: 9000	Etiqueta interna (VPLS pseudowire). Label 9000 se mantiene igual que en PE1 y P3, indicando que no cambia en el núcleo (especifica el VC del túnel VPLS).
Multiprotocol Label Switching Header	Label: 9001	Etiqueta interna de servicio VPN3. Label 9001 se mantiene igual que en PE1 y P3

Pila de Etiquetas MPLS:

- Etiqueta Externa (7009): Sustituye la etiqueta 7009 de P3, típico del intercambio de etiquetas en MPLS. P4 ha actualizado la etiqueta de transporte TE según su tabla de forwarding para dirigir el tráfico hacia PE5.
- Etiqueta Interna (9000): Se preserva, como es esperado en un LSR que no modifica la etiqueta del túnel VPLS.
- Etiqueta Interna (9001): Se preserva, como esperado en un LSR.

5.5.6.5 Capa 3: Cabecera IPv4 (20 bytes)

Tabla 5.5.17 Cabecera IPv4 – P4-eth1

Campo	Valor	Descripción
Versión	4	Estándar IPv4.
Longitud Total	1356 bytes	Incluye cabecera IP + cabecera UDP + payload.
Identificación	0x31806 (201350 decimal)	Identificador del datagrama IP original
Flags	0x0 (binario 000)	Bit reservado: 0; Don't Fragment (DF): 0; More Fragments (MF): 0 (no fragmentado).

Fragment Offset	0	Datagrama completo.
Protocolo	17 (UDP)	Protocolo a transportar
IP de Origen	192.168.1.253	Dirección privada, el servidor VLC en CEA1.
IP de Destino	224.0.67.67	Grupo multicast, destino del streaming VLC.

5.5.6.6 Capa 4: Cabecera UDP (8 bytes)

Tabla 5.5.18 Cabecera UDP – P4-eth1

Campo	Valor	Descripción
Puerto de Origen	38428	Puerto efímero, asignado por el servidor VLC.
Puerto de Destino	5004	Puerto RTP, confirma streaming multicast con VLC.
Longitud	1336 bytes	Cabecera UDP + payload.

5.5.6.7 Payload (1328 bytes)

- Datos: Truncado en la imagen, comenzando con hex: 8021dbcba5d152678784709617310d70….
- Análisis de Estructura del Payload:
    - Se identifica como un paquete RTP, similar a capturas previas.
        - Cabecera RTP (primeros 12 bytes):
            - Byte 0: 0x80 → Versión 2, Padding=0, Extension=0, CSRC Count=0.
            - Byte 1: 0x21 → Marker=0, Payload Type (PT)=33 (MPEG-2 TS).
            - Bytes 2-3: Número de Secuencia variable.
            - Bytes 4-7: Timestamp variable.
            - Bytes 8-11: SSRC variable.
        - Datos: 188 Bytes - MPEG-2 TS para video/audio del streaming VLC.
    - Servicio: Streaming multicast con VLC Player, consistente con capturas anteriores.

- Longitud: 1328 bytes, ocupando el payload completo tras cabeceras.

Contexto en la Topología:

- Servicio: Streaming multicast (VLC Player). Los puertos y la estructura RTP lo confirman, alineándose con capturas en CEA1, PE1 y P3.
- Procesamiento en el Núcleo: P4 actuó como LSR, intercambiando la etiqueta de transporte TE.

5.5.7 Captura de paquetes en PE5-eth1

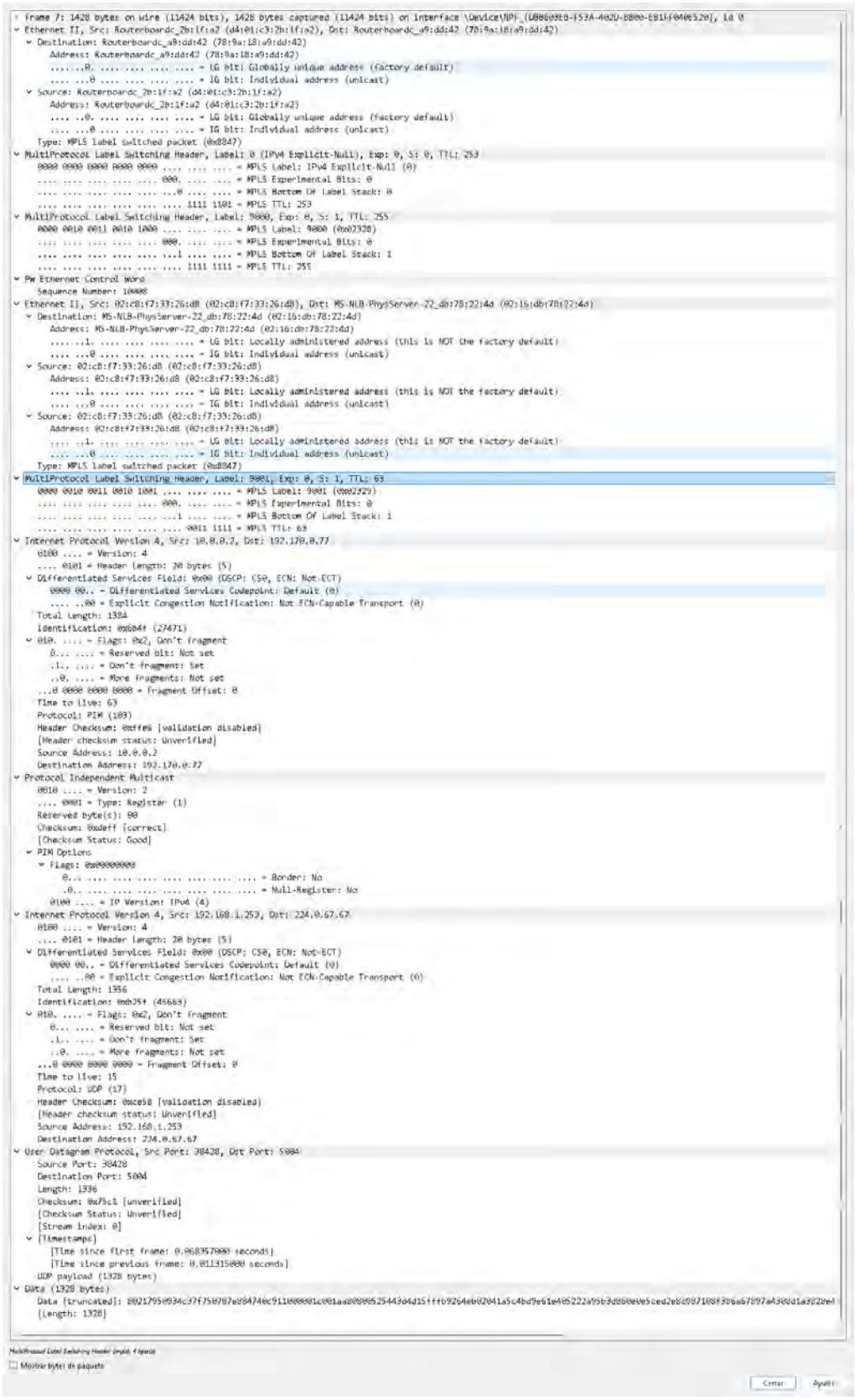


Figura 5.5.8 Captura de paquetes en la interfaz ETH1 del router PE5

5.5.7.1 Análisis de Paquete (PE5-Eth1)

Basado en la captura de imagen de Wireshark, analizaremos la estructura del paquete capturado en la interfaz eth1 del router PE5, que actúa como router de borde en la red IP/MPLS. Esta interfaz está conectada al router P4 del núcleo MPLS, por lo que la captura muestra el paquete al entrar en PE5, aún encapsulado con etiquetas MPLS, antes de la desencapsulación final hacia CEA5. Esto nos permite observar el estado del tráfico al final del dominio MPLS.

Este paquete corresponde al servicio de streaming multicast con VLC Player, como lo indican los puertos UDP (origen 38428, destino 5004) y la estructura RTP, consistente con capturas previas en CEA1, PE1, P3 y P4.

5.5.7.2 Metadatos del Frame

- Número de Frame: 1
- Longitud del Frame: 1428 bytes en el cable (11424 bits capturados)
- Longitud Capturada: 1428 bytes
- Tipo de Encapsulación: Ethernet
- Protocolos en el Frame: ethernet, mpls, ipv4, udp, data (incluye MPLS, confirmando la encapsulación)

Este frame transporta un datagrama UDP encapsulado en MPLS.

5.5.7.3 Capa 2: Cabecera Ethernet (14 bytes)

Tabla 5.5.19 Cabecera ethernet – PE5-eth1

Campo	Valor	Descripción
MAC de Destino	Routerboardc_a9:dd:42 (78:9a:18:a9:dd:42)	Dirección MAC unicast, de la interfaz de PE5, otro RouterBoard Mikrotik.
MAC de Origen	Routerboardc_2b:1f:a2 (44:01:c3:2b:1f:a2)	Dirección MAC unicast de P4.
Ethertype	0x8847	MPLS unicast. Confirma que el paquete sigue encapsulado con etiquetas MPLS al llegar a PE5.

5.5.7.4 Capa 2.5: Cabecera MPLS (8 bytes por etiqueta)

Tabla 5.5.20 Cabecera MPLS – PE5-eth1

Campo	Valor	Descripción
Multiprotocol Label Switching Header	Label: IPv4 Explicit-Null (0)	Etiqueta externa (transporte TE). Label 0 (IPv4 Explicit-Null) indica que PE5 está configurado para desencapsular el tráfico MPLS al salir del dominio.
Multiprotocol Label Switching Header	Label: 9000	Etiqueta interna (VPLS pseudowire). Label 9000 se mantiene igual que en PE1, P3 y P4, identificando el VC del túnel VPLS.
Multiprotocol Label Switching Header	Label: 9001	Etiqueta interna (VPLS pseudowire). Label 9001 se mantiene igual que en PE1, P3 y P4, identificando el servicio VPN3.

Pila de Etiquetas MPLS:

- Etiqueta Externa (IPv4 Explicit-Null, 0): Usada por PE5 como señal de que este es el último LSR antes de la desencapsulación. Indica que la etiqueta de transporte TE se eliminará aquí, y el paquete IP será procesado o reenviado.
- Etiqueta Interna (9000): Se preserva hasta PE5, donde se usará para mapear el pseudowire VPLS al tráfico VPN3 antes de enviarlo a CEA5.
- Etiqueta Interna (9001): Se preserva hasta PE5, donde se usará para mapear el servició VPN3.

5.5.7.5 Capa 3: Cabecera IPv4 (20 bytes)

Tabla 5.5.21 Cabecera IPv4 – PE5-eth1

Campo	Valor	Descripción
Versión	4	Estándar IPv4.
Longitud Total	1356 bytes	Incluye cabecera IP + cabecera UDP + payload.
Identificación	0x4e5b2	Identificador del datagrama IP original.
Flags	0x0 (binario 000)	Bit reservado: 0; Don't Fragment (DF): 0; More Fragments (MF): 0 (no fragmentado).
Fragment Offset	0	Datagrama completo.

Protocolo	17 (UDP)	Protocolo a transportar.
IP de Origen	192.168.1.253	Dirección privada, el servidor VLC en CEA1.
IP de Destino	224.0.67.67	Grupo multicast, destino del streaming VLC.

5.5.7.6 Capa 4: Cabecera UDP (8 bytes)

Tabla 5.5.22 Cabecera UDP – PE5-eth1

Campo	Valor	Descripción
Puerto de Origen	38428	Puerto efímero, asignado por el servidor VLC.
Puerto de Destino	5004	Puerto RTP, confirma streaming multicast con VLC.
Longitud	1336 bytes	Cabecera UDP + payload.

5.5.7.7 Payload (1328 bytes)

- Datos: Truncado, comenzando con hex: 8021f794a934c1ff55078e84790641731….
- Análisis de Estructura del Payload:
    - Se identifica como un paquete RTP, similar a capturas previas.
        - Cabecera RTP (primeros 12 bytes):
            - Byte 0: 0x80, Versión 2, Padding=0, Extension=0, CSRC Count=0.
            - Byte 1: 0x21, Marker=0, Payload Type (PT)=33 (MPEG-2 TS).
            - Bytes 2-3: Número de Secuencia variable.
            - Bytes 4-7: Timestamp variable.
            - Bytes 8-11: SSRC variable.
        - Datos: MPEG-2 TS para video/audio del streaming VLC.
    - Servicio: Streaming multicast con VLC Player.
- Longitud: 1328 bytes, ocupando el payload completo tras cabeceras.

Contexto en la Topología:

- Servicio: Streaming multicast (VLC Player). Los puertos y la estructura RTP lo confirman, alineándose con capturas en CEA1, PE1, P3 y P4.
- Pila de Etiquetas MPLS: Preparada para desencapsulación:
    - Etiqueta externa cambió a IPv4 Explicit-Null (0) en P4 o PE5, indicando que PE5 es el punto de salida del dominio MPLS.
    - Etiqueta interna (9000) permanece, para mapear el pseudowire VPLS al tráfico original.
    - Etiqueta interna (9001) permanece, para mapear al servicio VPN3.
- Procesamiento en el Borde: PE5, como router de borde, recibirá este paquete y desencapsulará las etiquetas. La etiqueta externa (0) sugiere que PE5 eliminará la capa de transporte TE, y la etiqueta 9001 permitirá mapear el tráfico VPLS al VRF o interfaz hacia CEA5.

5.5.8 Captura de paquetes en PE5-eth2

Figura 5.5.9 Captura de paquetes en la interfaz ETH2 de PE5

5.5.8.1 Análisis de Paquete (PE5-eth2)

Basado en la imagen de Wireshark, analizaremos la estructura del paquete capturado en la interfaz eth2 del router PE5, que actúa como router de borde en tu red IP/MPLS (ruta CEA1 → PE1 → P3 → P4 → PE5 → CEA5). Esta interfaz está conectada al router del cliente CEA5, aquí la comunicación es solo a nivel de IP, sin encapsulación MPLS. Esto significa que PE5 ha desencapsulado completamente las etiquetas MPLS, restaurando el paquete original antes de enviarlo a CEA5. La captura refleja el estado final del tráfico al salir del dominio MPLS.

Este paquete corresponde al servicio de streaming multicast con VLC Player, como lo indican los puertos UDP (origen 38428, destino 5004) y la estructura RTP, consistente con capturas previas en CEA1, PE1, P3, P4 y la entrada en PE5.

5.5.8.2 Metadatos del Frame

- Número de Frame: 1
- Longitud del Frame: 1428 bytes en el cable (11424 bits capturados)
- Longitud Capturada: 1428 bytes
- Tipo de Encapsulación: Ethernet
- Protocolos en el Frame: ethernet, IPV4, PIM, IPV4, UDP, data (incluye IGMP para multicast y el payload UDP)

Este frame transporta un datagrama UDP con una cabecera PIMv2 adicional, lo que es típico para el manejo de tráfico multicast al salir del dominio MPLS.

5.5.8.3 Capa 2: Cabecera Ethernet (14 bytes)

Tabla 5.5.23 Cabecera ethernet – PE5-eth2

Campo	Valor	Descripción
MAC de Destino	Routerboardc_2b:1c:07 (44:01:c3:2b:1c:07)	Dirección MAC unicast, la interfaz de CEA5, otro RouterBoard Mikrotik.
MAC de Origen	Routerboardc_a9:dd:43 (78:9a:18:a9:dd:43)	Dirección MAC unicast de PE5.
Ethertype	0x0800	IPv4. Confirma que no hay encapsulación MPLS, solo tráfico IP nativo.

5.5.8.4 Capa 3: Cabecera IPv4 (20 bytes) - Capa Externa

Tabla 5.5.24 Cabecera IPv4 – PE5-eth2

Campo	Valor	Descripción
Versión	4	Estándar IPv4.
Longitud Total	1384 bytes	Incluye cabecera IP + cabecera PIMv2 + segundo IPv4 + cabecera UDP + payload.
Identificación	0x3cd2 (15570 decimal)	Identificador del datagrama IP externo, usado para reensamblaje si es necesario.
Flags	0x2 (binario 010)	Bit reservado: 0; Don't Fragment (DF): 1 (evita fragmentación); More Fragments (MF): 0.
Fragment Offset	0	Datagrama completo.
Protocolo	PIMv2	Protocolo PIMv2, enrutamiento multicast
Checksum de Cabecera	0xf63f	Validación desactivada en Wireshark, pero parece correcto.
IP de Origen	10.0.0.2	Dirección IP de PE5
IP de Destino	192.176.0.77	Dirección IP de router RP.

5.5.8.5 Capa 3: Cabecera PIMv2

Tabla 5.5.25 Cabecera PIMv2 – PE5-eth2

Campo	Valor	Descripción
Type	2	Reporte de membresía PIMv2.
Grupo	224.0.67.67	Dirección del grupo multicast al que se reporta.

5.5.8.6 Capa 3: Cabecera IPv4 (20 bytes) - Capa Interna

Tabla 5.5.26 Cabecera IPv4 – PE5-eth2

Campo	Valor	Descripción
Versión	4	Estándar IPv4.

Longitud Total	1356 bytes	Incluye cabecera IP + cabecera UDP + payload.
Identificación	0x0820 (2080 decimal)	Identificador del datagrama IP interno
Flags	0x0 (binario 000)	Bit reservado: 0; Don't Fragment (DF): 0; More Fragments (MF): 0 (no fragmentado).
Fragment Offset	0	Datagrama completo.
Protocolo	17 (UDP)	Protocolo a transportar
IP de Origen	192.168.1.253	Dirección privada, el servidor VLC en CEA1.
IP de Destino	224.0.67.67	Grupo multicast, destino del streaming VLC.

5.5.8.7 Capa 4: Cabecera UDP (8 bytes)

Tabla 5.5.27 Cabeceara UDP – PE5-eth2

Campo	Valor	Descripción
Puerto de Origen	38428	Puerto efímero, asignado por el servidor VLC.
Puerto de Destino	5004	Puerto RTP, confirma streaming multicast con VLC.
Longitud	1336 bytes	Cabecera UDP + payload.

5.5.8.8 Payload (1328 bytes)

- Datos: Truncado, comenzando con hex: 8021f719557dbc5f78e847906417310d7….
- Estructura del Payload:
    - Se identifica como un paquete RTP.
        - Cabecera RTP (primeros 12 bytes):
            - Byte 0: 0x80 → Versión 2, Padding=0, Extension=0, CSRC Count=0.
            - Byte 1: 0x21 → Marker=0, Payload Type (PT)=33 (MPEG-2 TS).
            - Bytes 2-3: Número de Secuencia variable.
            - Bytes 4-7: Timestamp variable.
            - Bytes 8-11: SSRC variable.
        - Datos: MPEG-2 TS para video/audio del streaming VLC.

- Servicio: Streaming multicast con VLC Player, consistente con capturas anteriores.

- Longitud: 1328 bytes, ocupando el payload completo tras cabeceras.

Contexto de la Topología:

- Servicio: Streaming multicast (VLC Player). Los puertos y la estructura RTP lo confirman, alineándose con capturas en CEA1, PE1, P3, P4 y la entrada en PE5.

- Desencapsulación MPLS: La ausencia de etiquetas MPLS en esta captura indica que PE5 ha removido completamente la pila de etiquetas (IPv4 Explicit-Null, 9001 y 9000) al salir por eth2. El paquete IP/UDP original se ha restaurado.

5.5.9 Captura de paquetes en CEA5-eth1

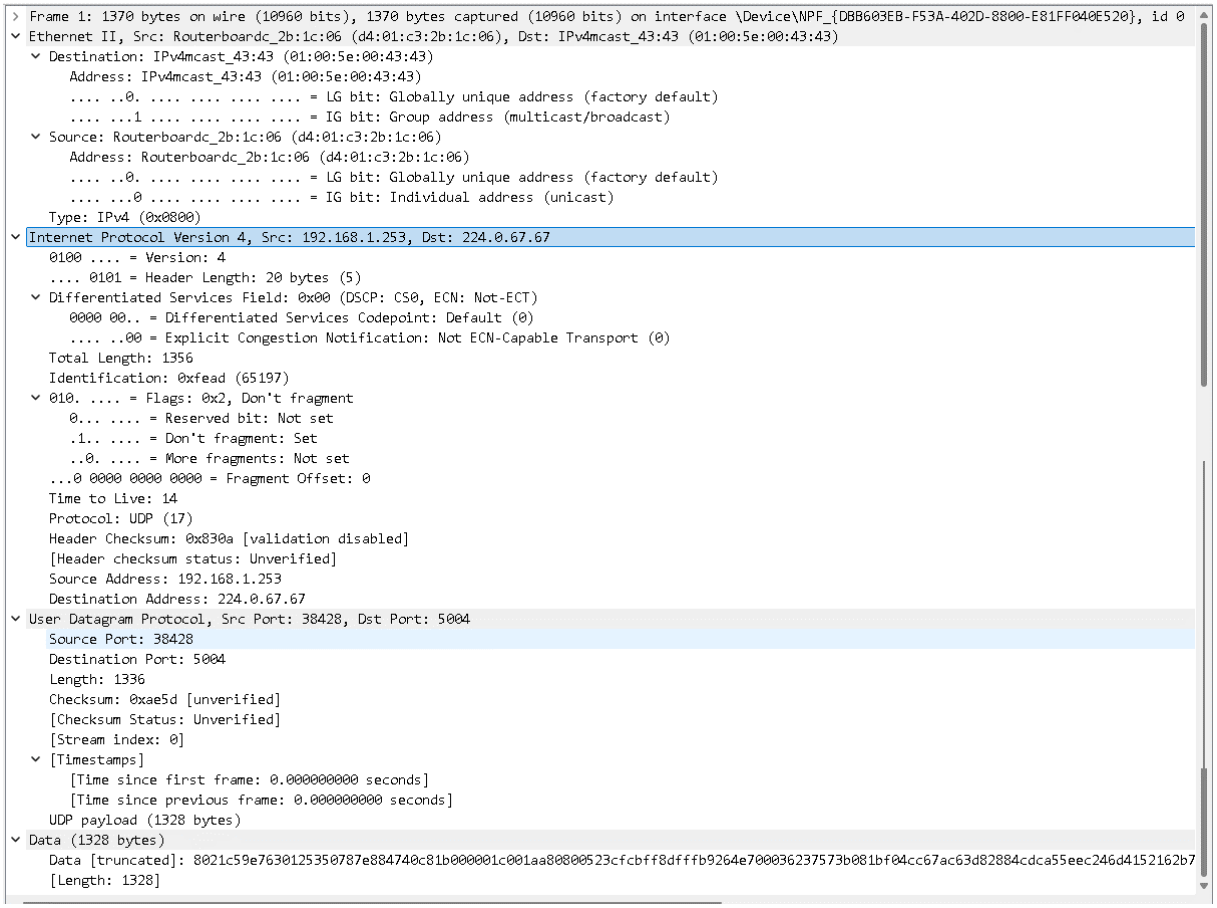


Figura 5.5.10 Captura de paquete en CEA-a eth1

5.5.9.1 Análisis de Paquete (CEA5-Eth1)

Basado en la imagen de Wireshark, la estructura del paquete capturado en la interfaz de salida del router CEA5, que se conecta a los usuarios finales. Esta captura muestra el tráfico después de la entrega desde PE5 a CEA5, ya en formato IP puro (sin MPLS), y encaminado hacia los clientes que consumen los recursos (streaming, telefonía o tráfico general). El paquete ha sido desencapsulado completamente en PE5, restaurado a su forma original, y ahora CEA5 lo reenvía.

Este paquete corresponde al servicio de streaming multicast con VLC Player, como lo indican los puertos UDP (origen 38428, destino 5004) y la estructura RTP, consistente con las capturas previas en CEA1, PE1, P3, P4, PE5 entrada y salida.

5.5.9.2 Metadatos del Frame

- Número de Frame: 1
- Longitud del Frame: 1378 bytes en el cable (10968 bits capturados)
- Tipo de Encapsulación: Ethernet
- Protocolos en el Frame: ethernet, ip, udp, data (sin MPLS solo IP/UDP puro)

Este frame transporta un datagrama UDP con payload, sin fragmentación, similar al original en CEA1.

5.5.9.3 Capa 2: Cabecera Ethernet (14 bytes)

Tabla 5.5.28 Cabecera ethernet – CEA-5 – eth1

Campo	Valor	Descripción
MAC de Destino	01:00:5e:00:43:43	Dirección MAC multicast, derivada de la IP multicast de destino (224.0.67.67). Igual que en la captura inicial de CEA1, indicando que el tráfico se replica a los usuarios finales suscritos al grupo.
MAC de Origen	Routerboardc_2b:1c:06 (44:01:c3:2b:1c:06)	Dirección MAC unicast de CEA5, confirmando que este router está reenviando el paquete hacia los clientes.
Ethertype	0x0800	IPv4. Confirma la ausencia de MPLS (desencapsulado en PE5).

5.5.9.4 Capa 3: Cabecera IPv4 (20 bytes)

Tabla 5.5.29 Cabecera IPv4 – CEA5-eth1

Campo	Valor	Descripción
Versión	4	Estándar IPv4.
Longitud Total	1356 bytes	Incluye cabecera IP + cabecera UDP + payload, igual que en CEA1.
Identificación	0x5ead (24221 decimal)	Identificador del datagrama IP original
Flags	0x2 (binario 010)	Bit reservado: 0; Don't Fragment (DF): 1 (evita fragmentación); More Fragments (MF): 0.
Fragment Offset	0	No fragmentado.
Protocolo	17 (UDP)	Protocolo a transportar
IP de Origen	192.168.1.253	Dirección privada, el servidor VLC en CEA1 (igual que en origen).
IP de Destino	224.0.67.67	Grupo multicast, destino del streaming (igual que en CEA1).

5.5.9.5 Capa 4: Cabecera UDP (8 bytes)

Tabla 5.5.30 Cabecera UDP – CEA5-eth1

Campo	Valor	Descripción
Puerto de Origen	38428	Puerto efímero, asignado por el servidor VLC (igual que en CEA1).
Puerto de Destino	5004	Puerto RTP, confirma el servicio de streaming multicast con VLC.
Longitud	1336 bytes	Cabecera UDP + payload.

5.5.9.6 Payload (1328 bytes)

- Datos: Truncado, comenzando con hex: 8021c5967630125350787e884740c81b000….
- Análisis de Estructura del Payload:
    - Se disecciona como un paquete RTP, idéntico en estructura al de CEA1.

- Cabecera RTP (primeros 12 bytes):
    - Byte 0: 0x80 → Versión 2, Padding=0, Extension=0, CSRC Count=0.
    - Byte 1: 0x21 → Marker=0, Payload Type (PT)=33 (MPEG-2 Transport Stream).
    - Bytes 2-3: Número de Secuencia variable.
    - Bytes 4-7: Timestamp variable.
    - Bytes 8-11: SSRC variable.
- Datos: Paquetes MPEG-2 TS para video/audio del streaming VLC.

- Identificación del Servicio: Streaming multicast con VLC Player. No es telefonía ni iPerf3.

- Longitud: 1328 bytes, igual que en origen.

Contexto de la Topología:

- Servicio: Multicast (streaming con VLC). La IP multicast, puertos y RTP confirman que el paquete ha atravesado la red intacta, entregado a los usuarios finales suscritos vía IGMP.
- Pila de Etiquetas MPLS: Ausente, como esperado en la salida de CEA5 (post-desencapsulación en PE5).
- Integridad: El paquete es idéntico al original en CEA1, confirmando que los túneles VPLS y TE funcionaron correctamente sin alteraciones.

Con esta captura, hemos cubierto toda la ruta CEA1-PE1-P3-P4-PE5-CEA5. El tráfico multicast se transportó exitosamente a través de VPN3 vía VPLS y TE, entregado de manera intacta.

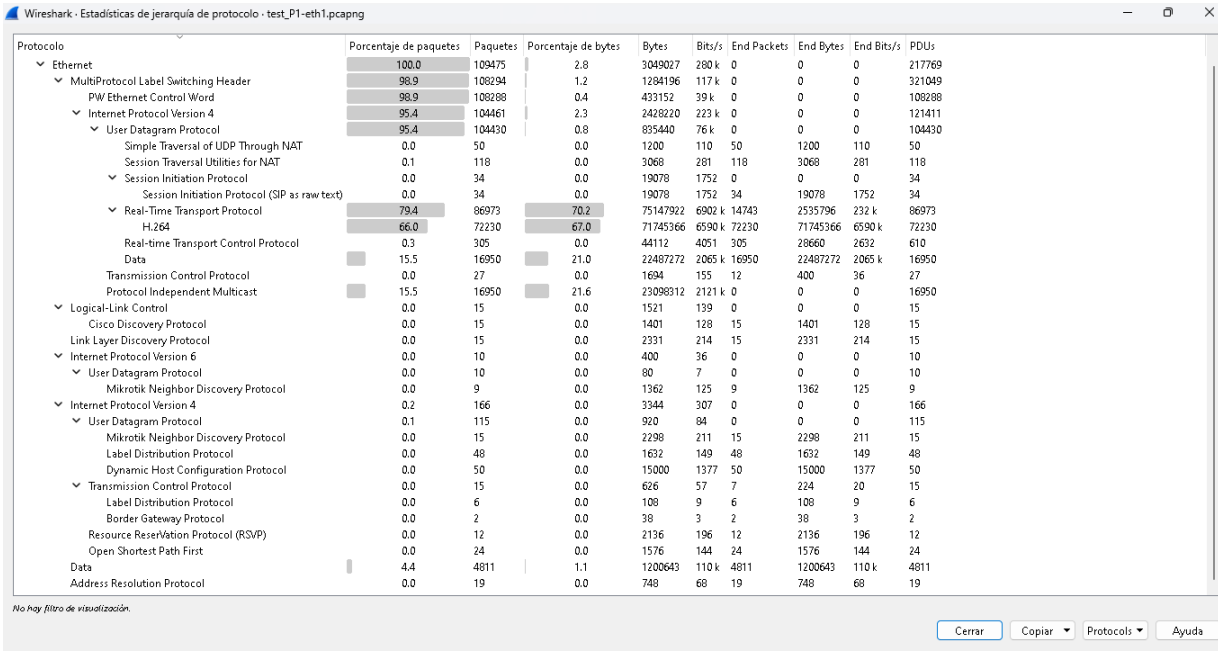


Figura 5.5.11 Jerarquía de protocolos de la implementación

La captura de paquetes con Wireshark nos permite verificar como están estructurados los paquetes en su recorrido a través del dominio IP/MPLS. El tráfico multicast es generada por un servidor que pertenece al cliente, el cual es consumido a través de usuarios que también pertenecen al cliente, la captura de paquete nos permite verificar que la interacción entre el cliente y el dominio IP/MPLS (proveedor) es a nivel de capa 3 (enrutamiento), siendo el enrutador PE de borde del dominio IP/MPLS el encargado de encapsular y desencapsular el tráfico generado por el cliente, esto para que el tráfico sea transportado a través del dominio IP/MPLS. Se verifica que los enrutadores PE de borde tienen tabla de enrutamiento a nivel IP y tablas de etiquetas a nivel de tráfico MPLS. En este análisis de tráfico multicast a través de la L3VPN se verifica el protocolo PIM-SM para el enrutamiento de tráfico multicast, y RSVP-TE para el túnel de ingeniería de tráfico, y túneles VPLS los cuales en caso de RouterOS es asociado de manera automática a un túnel de ingeniería de tráfico, el túnel VPLS es asociado al servicio L3VPN para que el tráfico de este servicio pueda utilizar el túnel de ingeniería de tráfico. Con el análisis se verifica que el tráfico del servicio L3VPN del cliente hace uso del túnel de ingeniería de tráfico implementado en el dominio IP/MPLS. Se puede verificar como se da la interacción de diferentes protocolos de red, como es el caso de MP-BGP para la distribución de la etiqueta para el túnel VPLS, y la distribución de las etiquetas de servicio L3VPN; EL protocolo RSVP-TE para la distribución de etiquetas en la formación del túnel de ingeniera de tráfico, y los diferentes protocolos para el tráfico multicast (PIM-SM, IGMP proxy, IGMP Snooping).

Evolución de la pila de etiquetas a través del túnel de ingeniería de tráfico: CEA1 – PE1 – P3 – P4 – PE5 – CEA5.

1. CEA1 hacia PE1: Tráfico multicast generado por servidor del cliente que recorrerá el proveedor del dominio IP/MPLS. El grupo multicast es la dirección IP 224.0.67.67 y dirección IP del servidor es 192.168.1.252.

2. PE1 hacia P3: Se verifica el apilamiento de etiquetas con la siguiente estructura [MPLS-TE:5009][VPLS:9000][VPN3:9001][multicast]. Esto valida que la VPLS conecta con el túnel de TE para transportar tráfico L3VPN.

3. P3 hacia P4: Aquí se genera la conmutación de la etiqueta de transporte (túnel de ingeniería de tráfico), verificándose la siguiente estructura de la pila de etiquetas [MPLS-TE:7009, Exp:3][VPLS:9000][VPN3:9001][multicast]. Este paquete corresponde al servicio de multicast con VPLC player, como se puede verificar a través de los puertos (origen 38428, destino 5004) y la estructura RTP.

4. P4 hacia PE5: Verificamos que aquí se aplica la operación de Penultime Hop Popping realizado por el router P4. La estructura del paquete seria tiene la siguiente estructura de pila de etiquetas PE5: [MPLS-TE:7009][VPLS:9000][VPN3:9001][multicast]

5. PE5 hacia CE1-B: En este tramo del recorrido del tráfico del cliente se regenera con estructura de tráfico multicast.

El análisis del tráfico sobre el core IP/MPLS nos permite verificar las operaciones que se realizan en cada enrutador del recorrido del tráfico.

1. Router PE1, es el router de ingreso al dominio IP/MPLS la operación que realiza sobre las etiquetas es denominada PUSH, por el cual este enrutador utiliza el protocolo MP-BGP para asignar las etiquetas de servicio (Etiquetas 9000, 9001), y el protocolo RSVP-TE para la asignación de la etiqueta de transporte (Etiqueta 5009). Es el encargado de encapsular el paquete IP del cliente hacia el dominio IP/MPLS.

2. Router de tránsito P3: Se verifica que la operación sobre la etiqueta de transporte que realiza se denomina SWAP, cambiando la etiqueta 5009 por la etiqueta 7009, las etiquetas de servicio (9000, 9001) se mantienen sin ninguna modificación.

3. Router (P4): Se puede verificar que la operación sobre la etiqueta de transporte (7009) se denomina SWAP, cambiando la etiqueta 7009 por la etiqueta 7009, las etiquetas de servicio (9000, 9001) se mantienen sin ninguna modificación.

4. Router de egreso del dominio IP/MPLS (PE5): Verificamos que la operación que realiza este enrutador de borde se denomina POP, retirando todas las etiquetas tanto de servicio des encapsulando el paquete IP del cliente.

5. El tráfico multicast es transportado exitosamente a través de L3VPN vía VPLS y TE, siendo esta entregada de manera intacta al usuario final del cliente.

5.6 Simulación de Escenarios de Red Controlado - NETEM

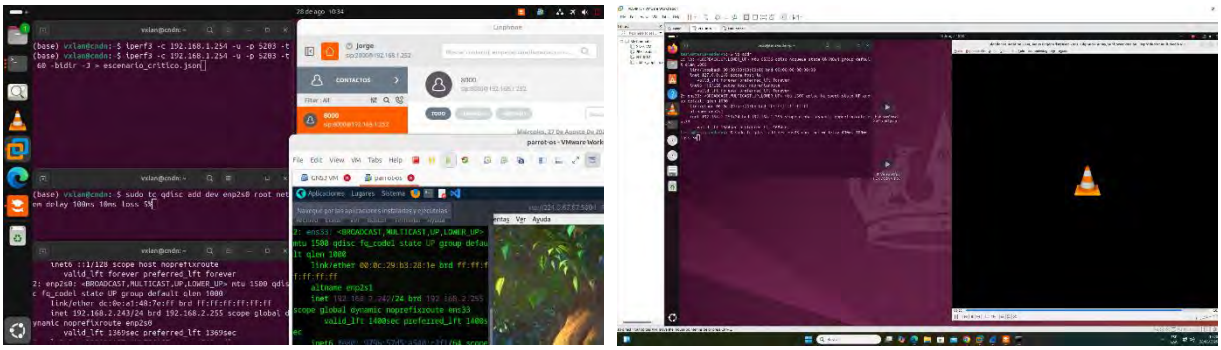


Figura 5.6.1 Configuración de parámetros - NETEM

En este apartado de la tesis trabajaremos con NETEM para crear condiciones donde emularemos escenarios, donde controlaremos parámetros que afecten el rendimiento de la red. Estos parámetros que se pueden configurar con NETEM incluyen Latencia, Jitter, Perdida de Paquetes, Reordenamiento, y paquetes corruptos. Valores de correlación entre los parámetros podría también ser establecidos para que los escenarios sean lo más reales posibles. El objetivo de este apartado es controlar los parámetros en las redes y cómo podemos medir el rendimiento de la red en estas condiciones.

El simulador NETEM juega un rol importante en el estudio de protocolos y aplicaciones de redes. Permitiendo realizar, probar escenarios reales de una manera controlada, NETEM es un emulador de redes que funciona en Linux, que nos permite emular una red WAN en un entorno de laboratorio.

Ya se tiene varios tipos de tráfico coexistiendo en la red (VoIP, multicast, datos generales), y lo que se quiere es poder monitorear el rendimiento de cada uno por separado. Para estos tráficos crearemos escenarios que serán creados con NETEM, el cual nos permitirá modificar los parámetros tales como retardo, jitter, perdida de paquetes, duplicación y reordenación de paquetes.

Para lograrlo, realizaremos lo siguiente.

- Generar condiciones controladas con Netem (latencia, pérdida, jitter, etc.).
- Inyectar tráfico de prueba con Iperf3 (para datos generales).

- Clasificar/monitorear tráfico real (VoIP SIP/RTP, multicast de video/audio, otros) con herramientas de análisis.

a) Clasificación de tráfico

Se tiene flujos implementados en laboratorio.

- Telefonía IP (Issabel PBX)
    - Señalización SIP: puertos UDP/TCP 5060.
    - Voz RTP: generalmente puertos UDP 10000–20000.
- Multicast (VLC Media Player)
    - Grupo Multicast 224.0.67.67.
    - UDP específico al grupo multicast.
- Datos Generales (generado con Iperf3)
    - Se hará uso de la herramienta de software Iperf3.

b) Crear condiciones de red con Netem

Simula condiciones de red, poder ingresar parámetros de red controlados.

c) Generar tráfico con Iperf3

Iperf3 nos permite generar tráfico en los diferentes escenarios implementados, permitiéndonos medir el rendimiento del enlace. Con Iperf3 se obtiene medidas de los parámetros de rendimiento de red los cuales serán procesados para su representación gráfica y posterior interpretación del mismo.

Tabla 5.6.1 Comandos de Iperf3 server y Cliente

Tipo de Trafico	**Cliente**	**Servidor**
Tráfico unicast	Iperf3 -c 10.0.0.2 -u -b -bidir -t 30 -p 5203	Iperf3 -s p-5203
Tráfico multicast (UDP):	Iperf3 -c 224.0.67.67 -u -p 5004 -b 5M -t 30	Iperf3 -s 224.0.67.67 -u -p 5004
Múltiples flujos	Iperf3 -c 10.0.0.2 -u -b 10M -t 30 -p 5201 & iperf3 -c 10.0.0.2 -u -b 5M -t 30 -p 5202 &	Iperf3 -s -p 5201 & Iperf3 -s -p 5202

Para añadir y cambiar el delay para emular los escenarios se procedería de la siguiente manera. Invocamos NETEM usando la línea de comandos *tc.* Cuando no se le pasa ningún parámetro de configuración, NETEM se comporta como FIFO con retardo, perdida, duplicación, o reordenación de paquetes propios de la red. La sintaxis básica de *tc* con NETEM es como sigue.

sudo tc qdisc [add|del|replace|change|show] dev dev_root netem opts
• sudo: Ejecuta el comando con privilegios de administrador. • tc: Comando para interactuar con NETEM. • qdisc: Es el encolamiento aplicado a los paquetes para decidir cuándo enviamos cada paquete. • [add | del | replace | change | show]: Es la operación que realizara qdisc. • dev id: Este parámetro indica el interfaz sujeto a la emulación de las condiciones. • opts: Este parámetro indica la cantidad de retardo, perdida de paquetes, duplicación, corrupción, y otros.

Los perfiles de NetEm: Esto son la configuración controlada de los parámetros de red para diferentes escenarios, que nos permitirá verificar el comportamiento de los diferentes tipos de tráficos que pasan por la red.

No hay un estándar único y estricto que defina exactamente "leve, degradado y crítico" para NETEM, pero basándome en recomendaciones de ITU-T (como Y.1541 para clases de QoS en redes IP, G.114 para retardos en VoIP y G.107 para modelado de calidad), y prácticas en laboratorio se emulo condiciones controladas de red (considerando que los servidores están sobre máquinas virtuales), se propone valores razonables. Estos incluyen delay (latencia), jitter (variación de latencia) y packet loss (pérdida de paquetes), que son los parámetros más relevantes para NETEM.

Los valores se expresan en:

Delay: milisegundos (ms).

Jitter: ms (variación, a menudo con distribución normal en NETEM).

Packet loss: porcentaje (%).

Estructura de los comandos NETEM como:

tc qdisc add dev <interfaz> root netem delay <delay>ms <jitter>ms distribution normal loss <loss>%

A continuación, se describe los valores de los parámetros de rendimiento en los diferentes escenarios controlados (laboratorios). Estos parámetros están configurados en las interfaces virtuales de los sistemas operativos instalados en VmWare y VirtualBox.

Tráfico VoIP (sensible a delay y jitter, basado en ITU-T G.114: <150ms bueno, >250ms degradación; Y.1541).

Tabla 5.6.2 Parámetros configurados - VoIP

Escenario	Delay (ms)	Jitter (ms)	Packet Loss (%)
Leve	30	5	0.5
Degradado	150	20	3
Crítico	300	50	5

Tráfico Multicast (streaming de video/audio, tolera más delay, pero sensible a perdidas; basado en Y.1541 para multimedia)

Tabla 5.6.3 Parámetros configurados - Multicast

Escenario	Delay (ms)	Jitter (ms)	Packet Loss (%)
Leve	50	10	0.1
Degradado	200	50	1
Crítico	400	100	5

Estos son valores aproximados para emulación; estos serán ajustados según las necesidades para cada escenario descrito. Para VoIP, jitter >30ms ya afecta la calidad.

Basado en los escenarios controlados que discutimos previamente (leve, degradado y crítico) para cada tipo de tráfico (VoIP, multicast y genérico), se detalla cómo implementar el laboratorio de prueba. El objetivo es emular condiciones de red con NETEM (en Linux) y medir parámetros de rendimiento como retardo (delay), jitter (variación de delay), pérdida de paquetes (packet loss), MOS (Mean Opinion Score, una métrica subjetiva de calidad de voz en una escala de 1 a 5) y ICPIF (Impairment/Calculated Planning Impairment Factor, un factor de degradación para planificación de redes VoIP según ITU-T G.113).

5.6.1 Configuración del Laboratorio

Hardware y Software requerido:

- Una maquina física con sistemas operativos virtualizados (VirtualBox o VMWARE) conectadas vía un switch virtual, en los se configuraran los servidores de Multicast, Telefonía IP y trafico genérico. En estos sistemas operativos virtualizados se configurarán NETEM. Al otro extremo del dominio IP-MPLS (cliente) se configurarán los clientes que tendrán acceso a estos servidores (softphone, reproductor multimedia).

- Configuración de interfaz de red en los servidores (sistema operativo virtualizado).
- Herramientas: tc (para NETEM), iperf (para tráfico genérico/UDP), Wireshark (para capturar y analizar paquetes), VLC (para multicast), Linphone (para VoIP simulado). Para MOS/ICPIF en VoIP, se usa scripts Python con fórmulas ITU-T.

Configurar NETEM en los servidores:

1. Instalamos NETEM: En Ubuntu o Debian, sudo apt install iproute2.
2. Configuramos NETEM en la interfaz del emulador: sudo tc qdisc add dev eth0 root netem delay <delay>ms <jitter>ms distribution normal loss <loss>%.
3. Generamos tráfico real (VoIP, Multicast y Genérico).
4. Uso de herramientas de software: iperf3 para métricas básicas, Wireshark para análisis detallado. Para MOS/ICPIF, el cálculo se realiza con scripts (ver fórmulas abajo).
5. Limpia NETEM: sudo tc qdisc del dev eth0 root.

Fórmulas para MOS e ICPIF (para VoIP):

- R-factor (base para MOS): R = 93.2 - Id - Ie, donde Id está relacionado al delay y jitter (aprox. 0.024 * delay + 0.11 * (delay - 177.3) si delay >177.3 ms), Ie por perdida (depende de codec, G.711: Ie = 30 * log (1 + 15 * perdida/%)).
- MOS: MOS = 1 + 0.035 * R + 7 * 10^ {-6} * R * (R - 60) * (100 - R). (Escala: >4 bueno, <3 pobre).
- ICPIF: ICPIF = Idd + Ie + Idq, donde Idd = relacionado al delay (0 si <100ms, aumenta lineal), Ie por perdida/codec, Idq por jitter. (Valor <10 bueno, >20 pobre).

5.6.2 Implementación para Tráfico VoIP

VoIP es sensible a delay (<150ms ideal) y jitter (<30ms). El codec de audio es G.711 para simulación. Se genera tráfico con Linphone para llamadas reales. Se mide con Wireshark (filtro RTP). Para mayor referencia dirigirse a la sección 5.6 “Simulación de Escenarios de Red Controlado - NETEM”, del trabajo de tesis.

Tabla 5.6.4 Implementación Trafico VoIP

Escenario	Configuración NETEM	Generación de Tráfico	Medición e Interpretación
Leve	tc qdisc add dev eth0 root netem delay 30ms 5ms distribution normal loss 0.5%	Se inicia llamada VoIP entre máquinas.	Delay alrededor de los 30ms (bueno), jitter alrededor de los 5ms

			(aceptable), loss baja: MOS entre 4.0-4.5, ICPIF <5. Tráfico fluido, voz clara.
Degradado	tc qdisc add dev eth0 root netem delay 150ms 20ms distribution normal loss 3%	Se inicia una llamada VoIP, durante 5-10 min para capturar variaciones.	Delay cercano a los 150ms (notable), jitter cercano a los 20ms (interrupciones), Perdida media: MOS entre los 3.0-3.5, ICPIF entre los10-15. Voz con ecos y demoras, degradación moderada.
Crítico	tc qdisc add dev eth0 root netem delay 300ms 50ms distribution normal loss 5%	Se inicia llamadas VoIP, se produce fallos en la conexión.	Delay >300ms (inusable), jitter alto, perdida alta: MOS <2.5, ICPIF >20. se produce fallo total en la comunicación.

5.6.3 Implementación para Tráfico Multicast

Multicast (streaming video y audio) tolera más delay, pero es sensible a la perdida de paquetes. Se hace uso de VRF y VLANs para aislar tráfico. Se genera con VLC (vlc video.mp4 --sout '#rtp{mux=ts,dst=224.0.67.67,port=5004}'). Se evalúa el tráfico con Wireshark, para mayor detalle se hace referencia a la sección 5.5.1 “Captura de Paquetes de Trafico de Red con Wireshark” de la presente tesis.

Tabla 5.6.5 Implementación Trafico Multicast

Escenario	**Configuración NETEM**	**Generación de Tráfico**	**Medición e Interpretación**
Leve	tc qdisc add dev eth0 root netem delay 50ms 10ms distribution normal loss 0.1%	Stream multicast desde fuente (VLC a grupo 224.0.67.67). El cliente se une en destino con VLC rtp://@224.0.67.67:5004.	Delay cercanos a los 50ms (aceptable para streaming), jitter moderado, perdida baja: Video fluido con mínimo buffering.
Degradado	tc qdisc add dev eth0 root netem delay 200ms 50ms distribution normal loss 1%	Stream multicast desde fuente (VLC a grupo 224.0.67.67). El cliente se une en destino con	Delay alto (buffering notable), jitter causa pixeles: Pérdida media

		VLC rtp://@224.0.67.67:5004	afecta calidad. Generándose degradación visible en video.
Crítico	tc qdisc add dev eth0 root netem delay 400ms 100ms distribution normal loss 5%	Se trasmite flujo multicast hacia el grupo 224.0.67.67. Produciendo deterioro del servicio.	Delay extremo (stream inestable), perdida alta: Video congelado o perdido. Produciendo fallo en la distribución de multicast.

5.6.4 Implementación para Tráfico Genérico

Tráfico best-effort (web/data). Menos sensible. Generada con iperf3 (iperf3 -c <IP> -u para UDP) o ping para pruebas simples. Se mide throughput general.

El trabajo de tesis se enfoca en explicar el impacto en los parámetros de rendimiento clave: retardo (delay, en ms), jitter (variación del delay, en ms), pérdida de paquetes (packet loss, en %). Para VoIP, se incluye MOS (Mean Opinion Score, escala de 1 a 5, donde >4 es excelente y <3 es pobre) e ICPIF (Impairment/Calculated Planning Impairment Factor, donde <10 es bueno y >20 indica problemas severos), basados en modelos ITU-T como G.107 (E-model) y G.113. Para multicast y genérico, no aplican directamente MOS/ICPIF (son métricas específicas de voz), pero se menciona impactos equivalentes en calidad percibida (buffering en streaming o throughput en datos).

Estos impactos se basan en estándares ITU-T (Y.1541 para QoS IP, G.114 para delay en voz) y prácticas comunes en emulaciones con NETEM. En general:

- Retardo: Afecta la interactividad; valores bajos son ideales para aplicaciones reales. Los puertos ethernet de los diferentes equipos son puertos virtuales.
- Jitter: Causa variabilidad; buffers compensan, pero altos valores generan interrupciones. Los buffers estos sujetos que los servidores y clientes están implementados sobre máquinas virtuales.
- Pérdida de paquetes: Provoca retransmisiones o corrupción; sensible en aplicaciones en tiempo real.

Se hará uso de tablas para claridad, con explicaciones por escenario.

Tráfico VoIP (Voz sobre IP, llamadas SIP/RTP)

VoIP requiere delay <150ms, jitter <30ms y loss <1% para calidad óptima. Códecs como G.711 asumen buffers para jitter, pero altos valores degradan la conversación.

Tabla 5.6.6 MOS y ICPIF para VoIP

Escenario	Retardo (ms)	Jitter (ms)	Pérdida de Paquetes (%)	MOS (aprox.)	ICPIF (aprox.)
Leve	30	5	0.5	4.0-4.5	<5
Degradado	150	20	1	3.0-3.5	10-15
Crítico	300	50	5	<2.5	>20

Según la tabla se realiza una descripción de la asignación de los valores a los parámetros de rendimiento según los diferentes escenarios implementados en el laboratorio.

Escenario Leve

- **Retardo**: Con un valor de 30ms en laboratorio se percibe el retardo, pero es tolerable en conversaciones; no causa ecos notables ni interrupciones en el flujo natural.
- **Jitter**: 5ms se maneja fácilmente con buffers adaptativos; la voz suena fluida sin variaciones audibles.
- **Pérdida**: 0.5% es mínima.
- **MOS/ICPIF**: Alta calidad percibida (como una llamada telefónica clara); ideal para entornos de oficina estables.

Escenario Degradado

- **Retardo**: 150ms introduce demoras notables (eco o "hablar sobre el otro"); al hacer las llamadas en laboratorio se notó falta de interactividad.
- **Jitter**: 20ms causa fluctuaciones que agotan buffers, resultando en voz entrecortada o pausas breves.
- **Pérdida**: 1% genera efectos audibles (ruido o silencios); codecs compensan, pero calidad baja.
- **MOS/ICPIF**: Calidad aceptable pero frustrante (como una llamada con interferencias); usable para comunicaciones no críticas, pero al hacer las llamadas se notan degradación.

Escenario Critico

- **Retardo:** 300ms hace la conversación inusable (demoras extremas); usuarios se interrumpen constantemente.
- **Jitter:** 50ms sobrecarga buffers, causando cortes masivos y voz distorsionada.
- **Pérdida:** 5% resulta en pérdida significativa de audio; imposible ocultar, llevando a fallos en la llamada.
- **MOS/ICPIF:** Calidad pobre (inusable para voz); simula redes congestionadas, donde la comunicación colapsa.

Para una mejor referencia podemos referirnos a la figura 5.6.11 del trabajo de tesis.

Tráfico Multicast (Streaming de video/audio en grupo; tolera más delay, pero sensible a la perdida de paquetes)

Multicast prioriza entrega eficiente; delay hasta 200ms es manejable con buffering, pero jitter/perdida causan deterioros visuales, audibles.

Tabla 5.6.7 Impacto en Calidad - Trafico Multicast

Escenario	Retardo (ms)	Jitter (ms)	Pérdida de Paquetes (%)	Impacto en Calidad Percibida
Leve	50	10	0.1	Bajo buffering; calidad alta (fluido)
Degradado	200	50	1	Buffering moderado; calidad media (deterioros visibles)
Crítico	400	100	5	Buffering extremo; calidad pobre (inusable)

Escenario Leve:

- **Retardo:** 50ms permite buffering inicial sin interrupciones; stream inicia rápidamente.
- **Jitter:** 10ms se absorbe con buffers grandes; no hay congelamientos notables en video.
- **Pérdida:** 0.1% causa pixeles menores o inestabilidad.
- **Calidad:** Streaming suave, como ver TV en red local; usuarios no perciben problemas.

Escenario Degradado:

- **Retardo:** 200ms aumenta tiempo de inicio y rebuffering; afecta experiencia en eventos en vivo.
- **Jitter:** 50ms genera variaciones que causan pausas frecuentes en el stream**.**
- **Pérdida:** 1% resulta en bloques pixelados o audio cortado; calidad degradada pero recuperable.
- **Calidad:** Usable para contenido no crítico, pero frustrante (como video con retardos en conferencias).

Escenario Critico:

- **Retardo:** 400ms hace el stream inestable; buffering constante interrumpe la visualización.
- **Jitter:** 100ms sobrecarga mecanismos de corrección, causando congelamientos prolongados.
- **Pérdida:** 5% destruye continuidad; video y audio se pierde por completo en secciones.
- **Calidad:** Fallo total, sobrecargada; imposible para distribución multicast efectiva.

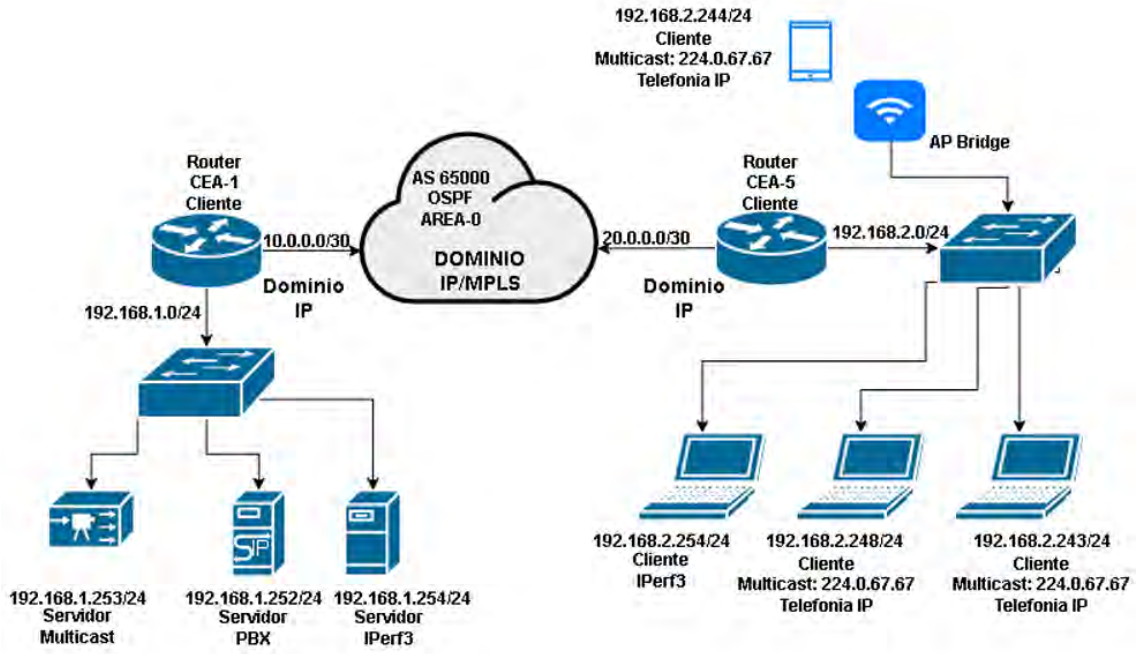


Figura: Topología de red con los equipos Router Mikrotik

Configuración de red:

Red interna 1: 192.168.1.0/24 (Entre Servidores y el Core IP-MPLS)

Red interna 2: 192.168.2.0/24 (Entre el Core IP-MPLS y los Clientes)

Sobre la topología de la Figura. Se realiza los siguientes pasos para la configuración de los diferentes escenarios.

1. Instalar herramientas en todas las máquinas (Ubuntu o Debian recomendado):

```
sudo apt update && sudo apt install iproute2 iperf iperf3 vlc wireshark sip-tester sipp ffmpeg
```

2. En el Emulador, aplica NETEM en la interfaz hacia el destino (eth1):

```
sudo tc qdisc del dev eth1 root    # Limpia configuraciones previas
sudo tc qdisc add dev eth1 root netem delay <delay>ms <jitter>ms distribution normal loss <loss>%
```

3. Generamos tráfico desde el Cliente.

4. Capturamos y medimos en el Servidor con Wireshark o iperf3.

5. Repetimos para cada escenario, limpiando NETEM entre pruebas.

Cálculo de MOS: Se hace uso de un script Python simple (basado en ITU-T G.107 E-model aproximado para G.711):

```
def calculate_mos(delay, jitter, loss):
```

```
    effective_delay = delay + (jitter * 2) + 10  # ms
    if effective_delay < 160:
        r = 93.2 - (effective_delay / 40)
    else:
        r = 93.2 - ((effective_delay - 120) / 10)
    r = r - (loss * 2.5)  # Aproximado para packet loss
    if r < 0:
        return 1.0
    mos = 1 + 0.035 * r + 0.000007 * r * (r - 60) * (100 - r)
    return min(mos, 4.5)  # Máximo realista

# Ejemplo para escenario leve: delay=100, jitter=20, loss=0.1
print(calculate_mos(100, 20, 0.1))  # ~4.3
```

El script se ejecuta con las métricas obtenidas en laboratorio. Mayor detalle de su interpretación de manera grafica en la sección 5.6.5 “Reporte Comparativo de Rendimiento de Ancho de Banda con IPERF3” de la tesis.

5.6.5 Mediciones e Interpretaciones en un Escenario Normal:

Tabla 5.6.8 Parámetros para un escenario normal

Escenario	Tipo de tráfico	Parámetros críticos	Comando NetEm
Normal	VoIP (RTP/SIP)	Propios de la red (por defecto)	Sin Configuración
	Multicast (video/audio)	Propios de la red (por defecto)	Sin Configuración

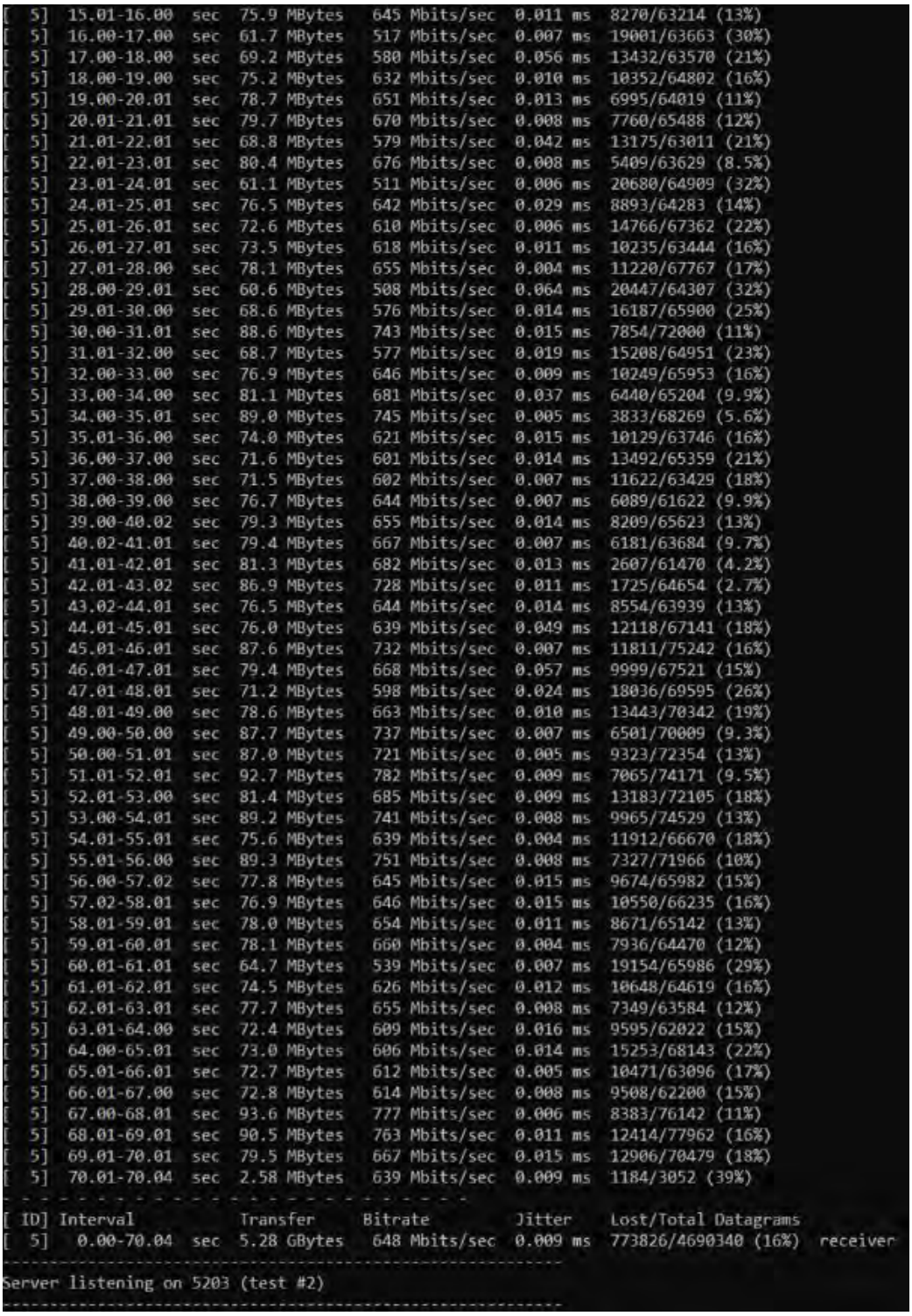


Figura 5.6.1: Trafico Generado por Iperf3

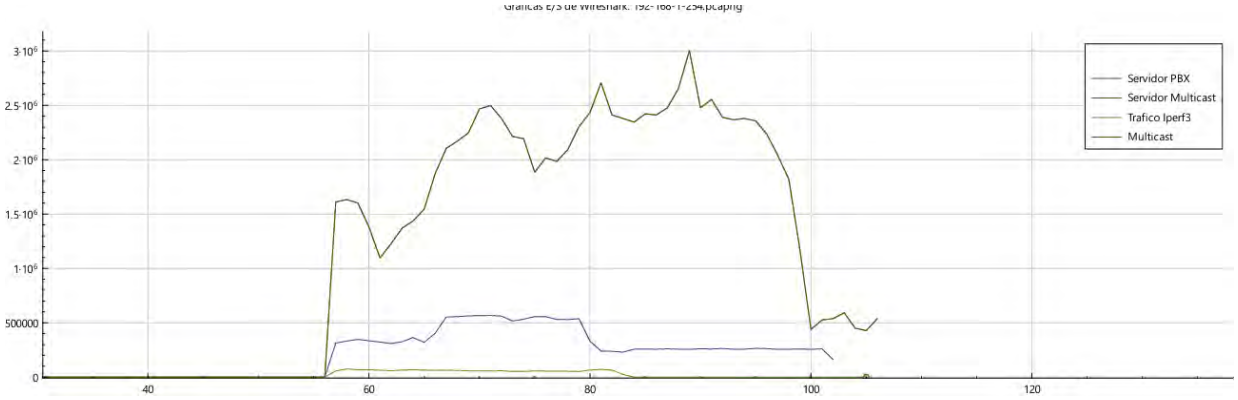


Figura 5.6.2 Trafico Multicast, Telefonía IP y Iperf3

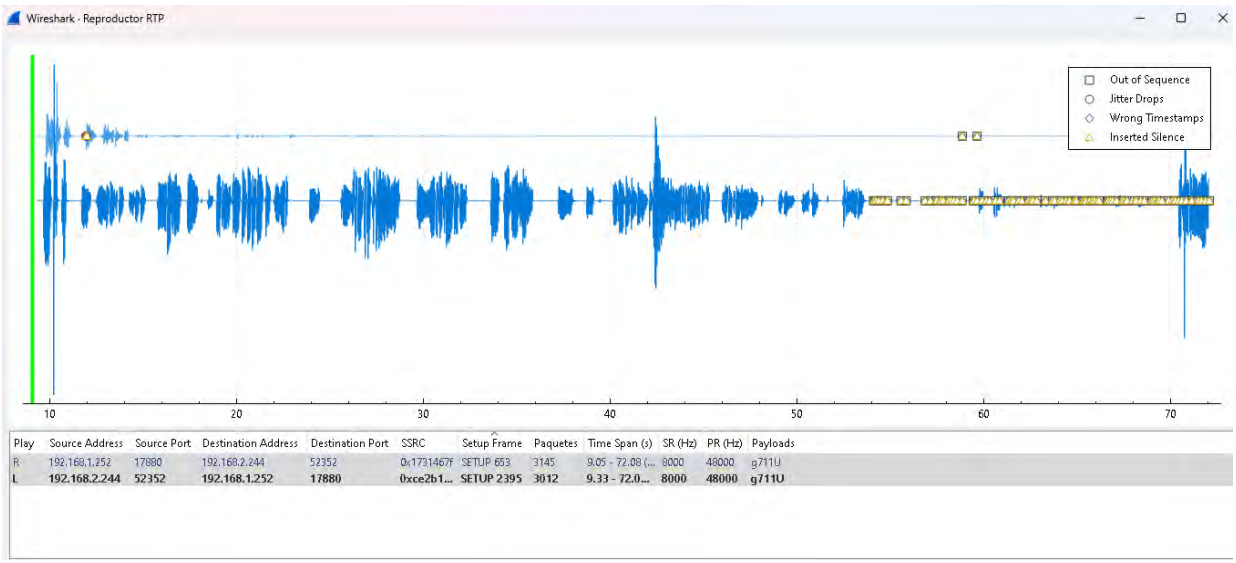
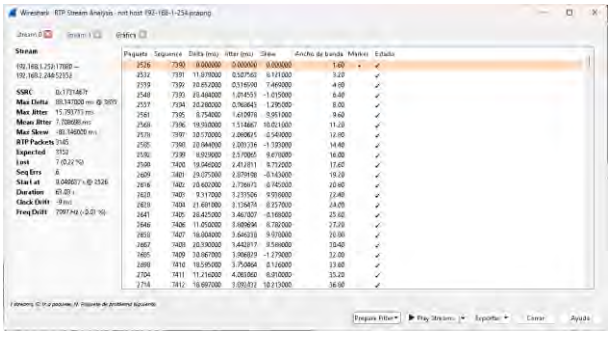
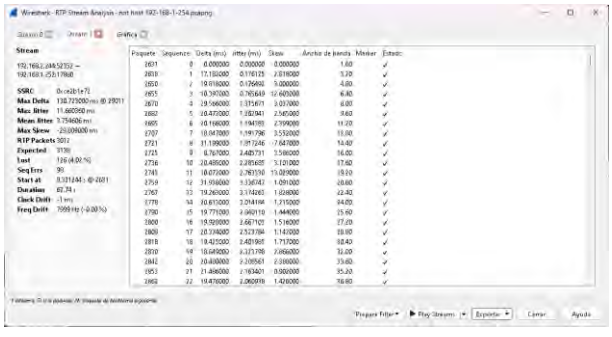


Figura 5.6.3 Reproducción del flujo de audio de Telefonía IP





Nota: Stream 0 y Stream 1 son los flujos de datos de una llamada (videollamada) bidireccional, donde podemos verificar retardo maximo significativo de 88.34 ms y un promedio de retardo de 29.74 ms que es cercano a los 30 ms para VoIP según Estandar, y el Jitter promedio es de 7.06 ms que es un valor bajo, indica estabilidad, la perdida de paquetes se considera optimo para comunicaciones de Telefonia IP optima. De lo mencionado podemos estimar el parametro MOS (Mean Opinion Score) esta entre 2.5-3.0 (acecptable), lo que sugiere una calidad de llamada agradable.

Figura 5.6.4 Representa un flujo de datos bidireccional de una llamada (videollamada)

Nota:

1. **Ejes y Estructura**

- Eje X (Arrival Time): Representa el tiempo de llegada de los paquetes, con un rango de aproximadamente 10 a 70 unidades de tiempo, con una duración visible de unos 60 segundos.
- Eje Y (Value in ms): Mide deltas y otras variaciones en milisegundos, con valores que van de 0 a 125 ms.
- Flujos: Incluye dos flujos:
    - Stream 0 (negro): Representa un flujo de datos.
    - Stream 1 (azul): Representa otro flujo, en la dirección opuesta.

2. **Métricas Clave**

- Delta (△): Indica el intervalo de tiempo entre la llegada de paquetes consecutivos.
    - La mayoría de los deltas están entre 20-40 ms, consistente con códecs VoIP estándar (e.g., G.711 con paquetes cada 20 ms).
    - Hay picos notables, especialmente en Stream 1, que alcanzan valores cercanos a 100-125 ms, con un pico excepcional que supera los 125 ms. Esto sugiere retrasos significativos en momentos puntuales.
- Jitter (●): Representa la variación en los tiempos de llegada. Las variaciones en los deltas indican jitter moderado a alto en los picos.

- Jitter estimado: entre los 10-20 ms en zonas estables, con picos que superan los 50 ms en los eventos de retraso.

3. **Análisis por FlujoStream 0 (negro):**

    - Muestra una densidad constante de paquetes a lo largo del tiempo, con deltas mayormente estables (entre 20-40 ms).
    - Picos ocasionales, pero menos pronunciados que en Stream 1, sugiriendo una transmisión más estable.

- **Stream 1 (azul):**

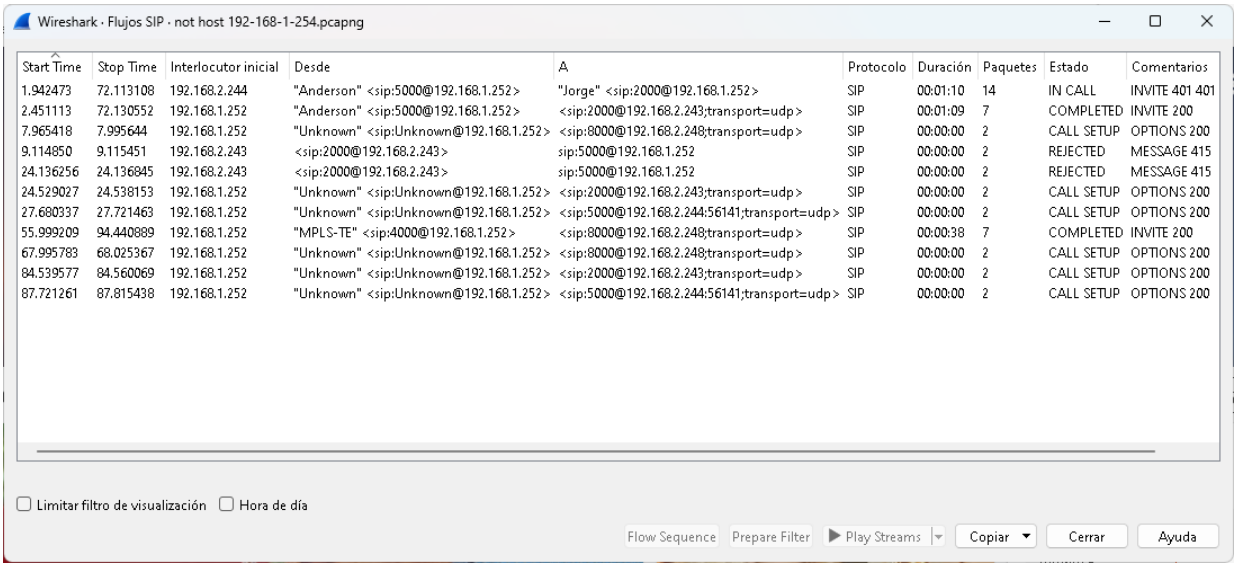
    - Dominante en el gráfico con picos más altos y frecuentes (entre los 100-125 ms, con un pico mayores a 125 ms).
    - Alta variabilidad en los deltas, especialmente entre 20-40 s y 50-60 s lo que indica problemas intermitentes de red (congestión o latencia).
    - Stream más afectado por condiciones de red adversas.

Des estos Stream se puedo observar que:

- Densidad: Alta concentración de paquetes al inicio (10-20 s) y una distribución más uniforme hacia el final (50-70 s), observandoce que la transmisión se estabiliza con el tiempo.
- Picos: Los picos en Stream 1 son más notorios, especialmente un pico extremo alrededor de 50-60 s que supera los 125 ms. Esto indica un evento de pérdida de paquetes.

El flujo empieza con alta actividad y muestra episodios de inestabilidad (picos), pero se mantiene una transmisión continua hasta el final.

Figura 5.6.5 Análisis de variación, jitter, perdida de paquetes en una llamada



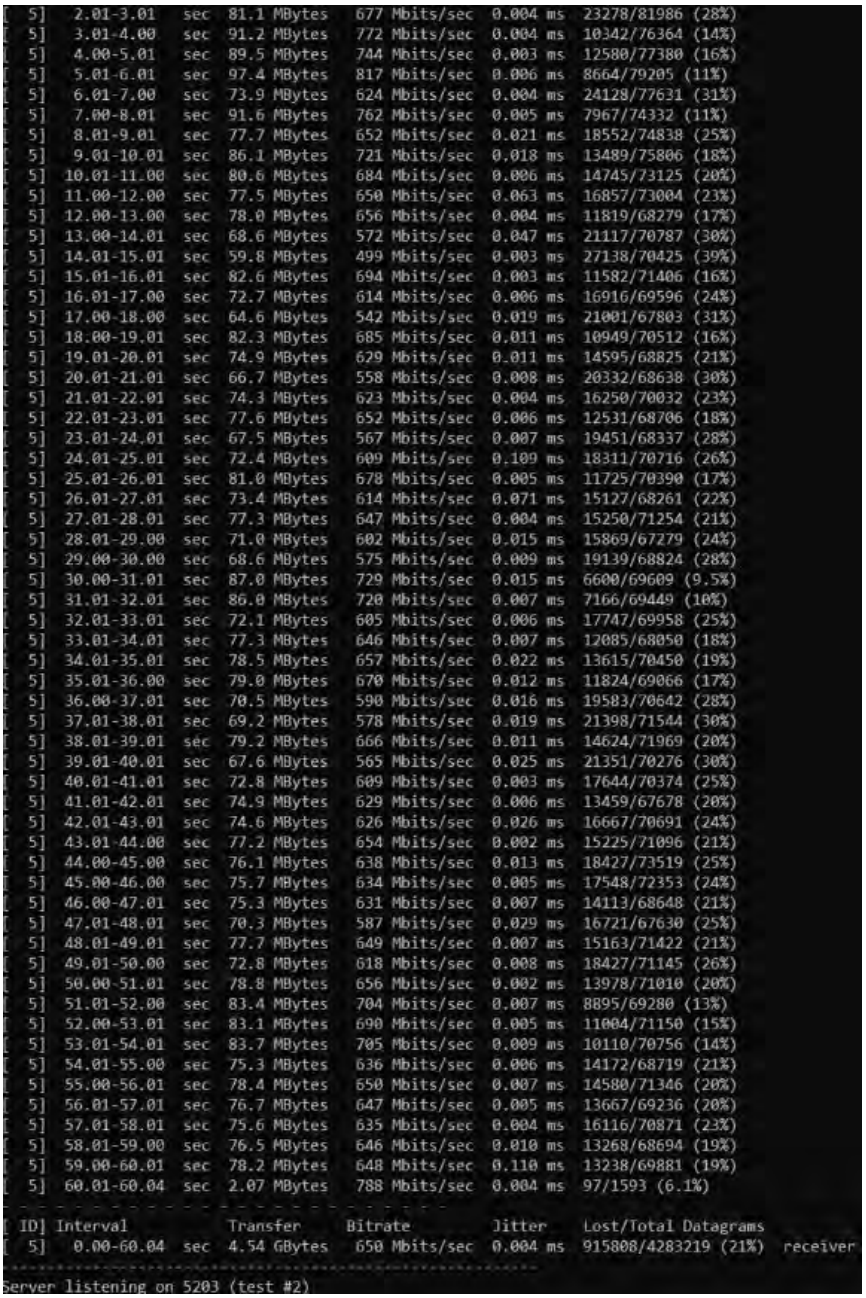
Nota: El origen del flujo SIP es 192.168.1.252 (servidor PBX) y el destino 192.168.2.243 (Softphone) ambos utilizan el protolcolo SIP sobre el puerto 5060 para poder establecer la llamada, se puede notar que todo los estan marcados como completados (llamada establecida).

Figura 5.6.6 Flujo de la señalización SIP

5.6.6 Medición e Interpretación en un Escenario Leve

Tabla 5.6.9 Configuración NETEM -escenario leve

Escenario	Tipo de tráfico	Parámetros críticos	Comando NetEm
Leve	VoIP (RTP/SIP)	Delay: 30 ms Jitter: 5 ms Loss: 0.5%	tc qdisc change dev eth0 root netem delay 30ms 5ms loss 0.5%
	Multicast (video/audio)	Delay: 50 ms Jitter: 10 ms Loss: 0.1%	tc qdisc change dev eth0 root netem delay 50ms 10ms loss 0.1%



Nota: Las métricas que se puede ver son la tasa promedio de bits cuyo valor es de 650 Mbps, el jitter promedio cuyo valor es de 0.004 ms y la perdida de datagramas con un valor de 21 %. Podemos concluir que la red es de gran capacidad donde tenemos pérdidas de 21 % lo que indica que los parámetros introducidos por Netem tiene relación directa a la perdida mencionada.

Figura 5.6.7: Trafico generado por Iperf3

Figura 5.6.8 Trafico Multicast, Telefonía IP y Iperf3

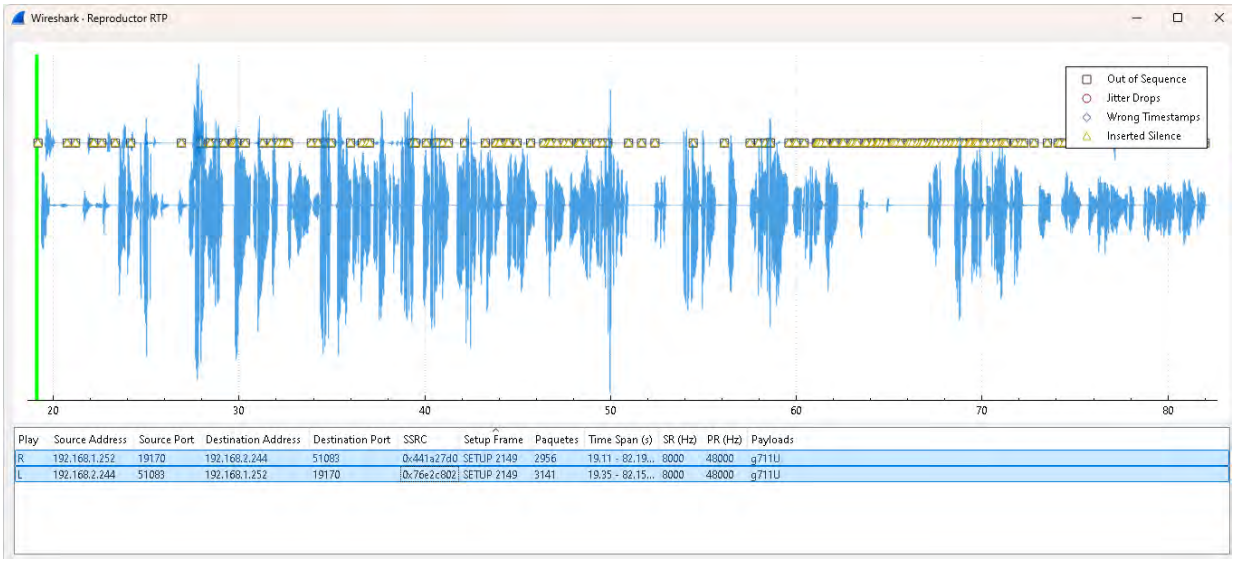
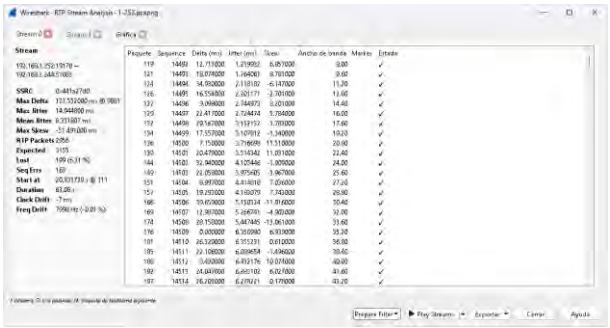
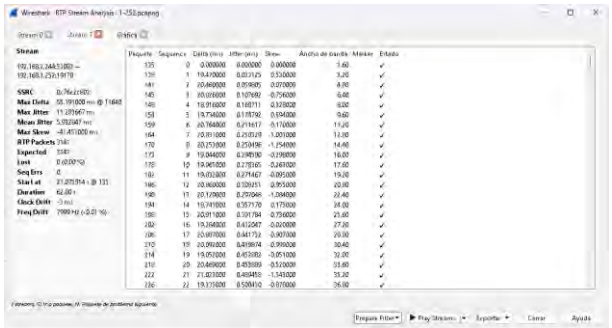


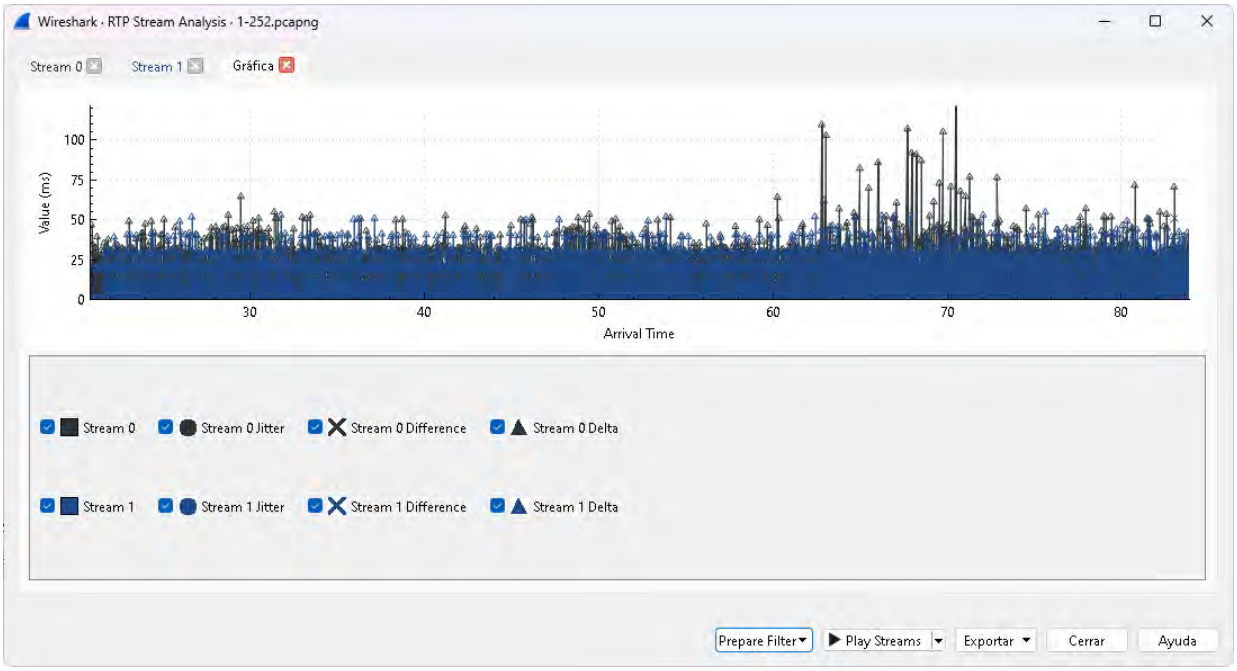
Figura 5.6.9 Reproducción de flujo de audio, telefonía IP





Nota: El retardo promedio es de 13.94 ms con maximos de 121.52 ms lo que indica retrasos inducidos por NETEM, el jitter promedio de 3.94 ms es menor a 20 ms (valor referencial según estandares) aunque tambien podemos notar jitter maximo de 14.94 ms.

Figura 5.6.10 RTP stream de una llamada (videollamada)



Nota:

- Eje X (Arrival Time): Representa el tiempo de llegada de los paquetes, con un rango de aproximadamente 30 a 80 unidades de tiempo. sugiriendo una duración de 50 segundos.
- Eje Y (Value in ms): Mide deltas y otras variaciones en milisegundos, con valores que van de 0 a 100 ms aproximadamente, aunque hay picos que alcanzan valores cercanos a 150 ms.
- Delta (△): Indica el intervalo de tiempo entre la llegada de paquetes consecutivos.
    - La mayoría de los deltas están entre 20-40 ms, lo cual es típico para códecs VoIP.
    - Hay picos ocasionales que llegan a los 150 ms, especialmente en Stream 1, indicando retrasos intermitentes significativos.
- Jitter (●): Representa la variación en los tiempos de llegada. Los puntos de jitter no son muy prominentes, pero las variaciones en los deltas indican jitter moderado en los picos.

- Jitter estimado: Esta entre los 10-20 ms en zonas estables, con picos que entre los 50 ms.

- Difference (X): Muestra la desviación entre el tiempo de llegada esperado y el real. Las marcas de diferencia se alinean con los delatas, indicando desfases acumulados.

- Densidad: Hay una alta concentración de paquetes al inicio (30-40 s), que disminuye hacia el final (70-80 s), esto es debido a que la comunicación se llega a estabilizar y se da el mismo comportamiento al terminar la llamada.

- Picos: Los picos en Stream 1 son más pronunciados y frecuentes, loq ue nos indica inestabilidad (posiblemente pérdida de paquetes o retrasos). Stream 0 muestra menos variabilidad.

Tendencia general: El flujo empieza con alta actividad y luego se reduce, lo que corresponde al inicio de una llamada (con establecimiento inicial) seguido de una fase más estable.

Figura 5.6.11 Análisis de variación, jitter, perdida de paquetes en una llamada

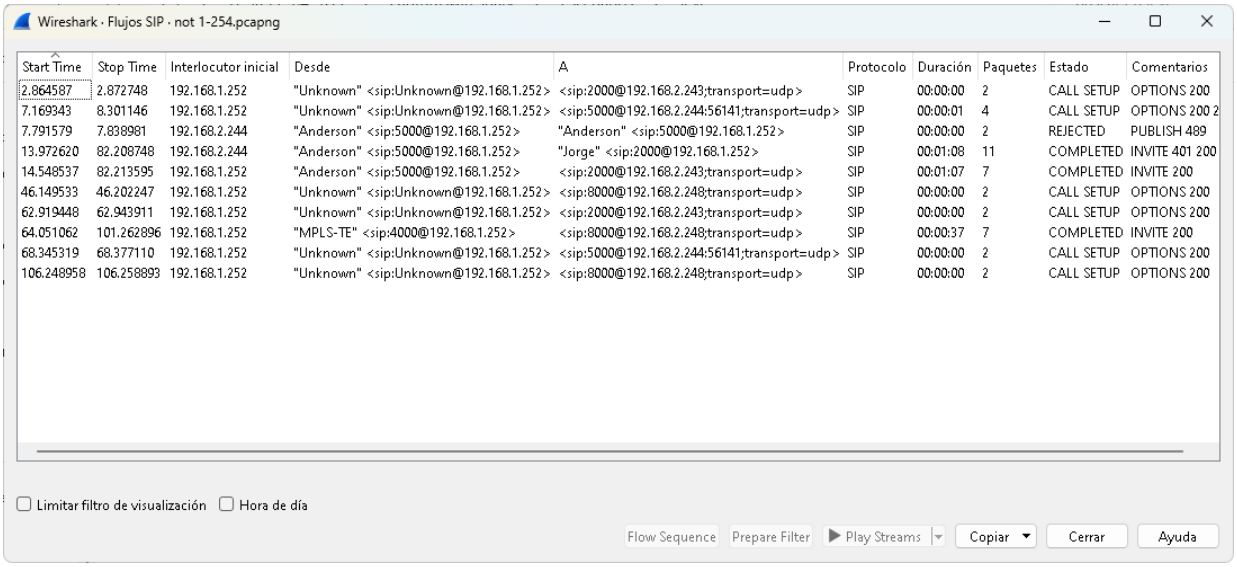
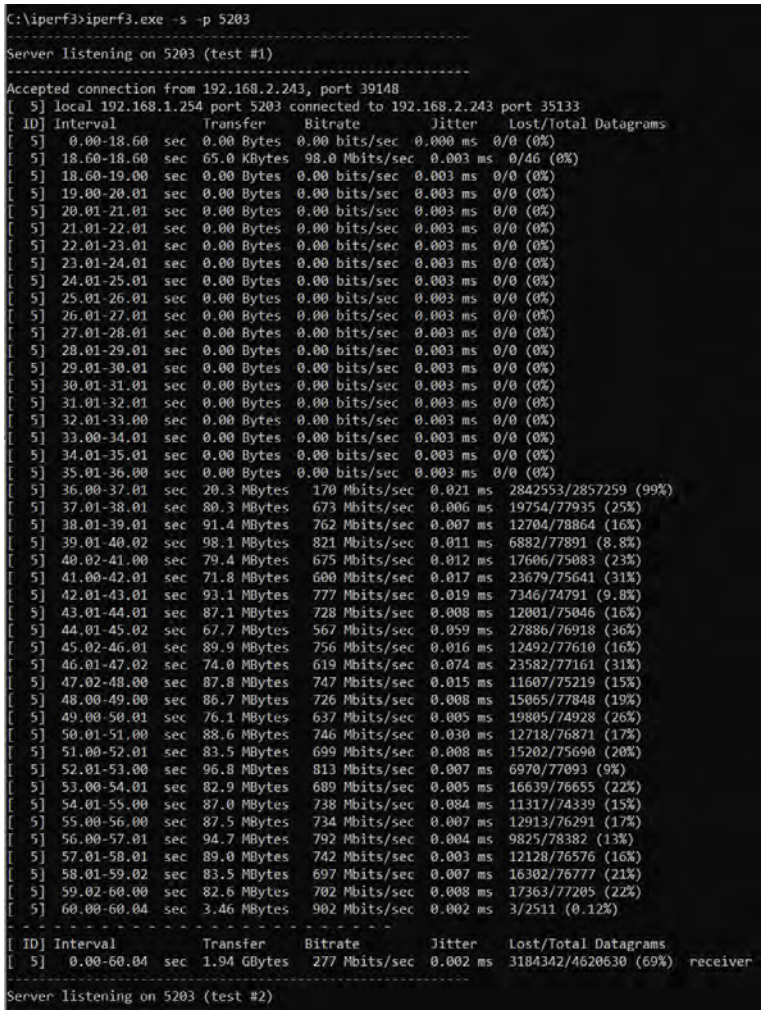


Figura 5.6.12 Flujo SIP entre central PBX y Usuarios Finales

5.6.7 Medición e Interpretación en un Escenario Degradado

Tabla 5.6.10 Configuración NETEM -escenario degradado

Escenario	Tipo de tráfico	Parámetros críticos	Comando NetEm
Degradado	VoIP (RTP/SIP)	Delay: 150 ms Jitter: 20 ms Loss: 3%	tc qdisc change dev eth0 root netem delay 150ms 20ms loss 3%
	Multicast (video/audio)	Delay: 200 ms Jitter: 50 ms Loss: 1%	tc qdisc change dev eth0 root Netem delay 200ms 50ms loss 1%



Nota: Podemos ver que existe una pérdida de paquetes 69 % lo que está relacionado a las condiciones de red configuradas por NETEM.

Fig. 5.96: Trafico Generado por Iperf3

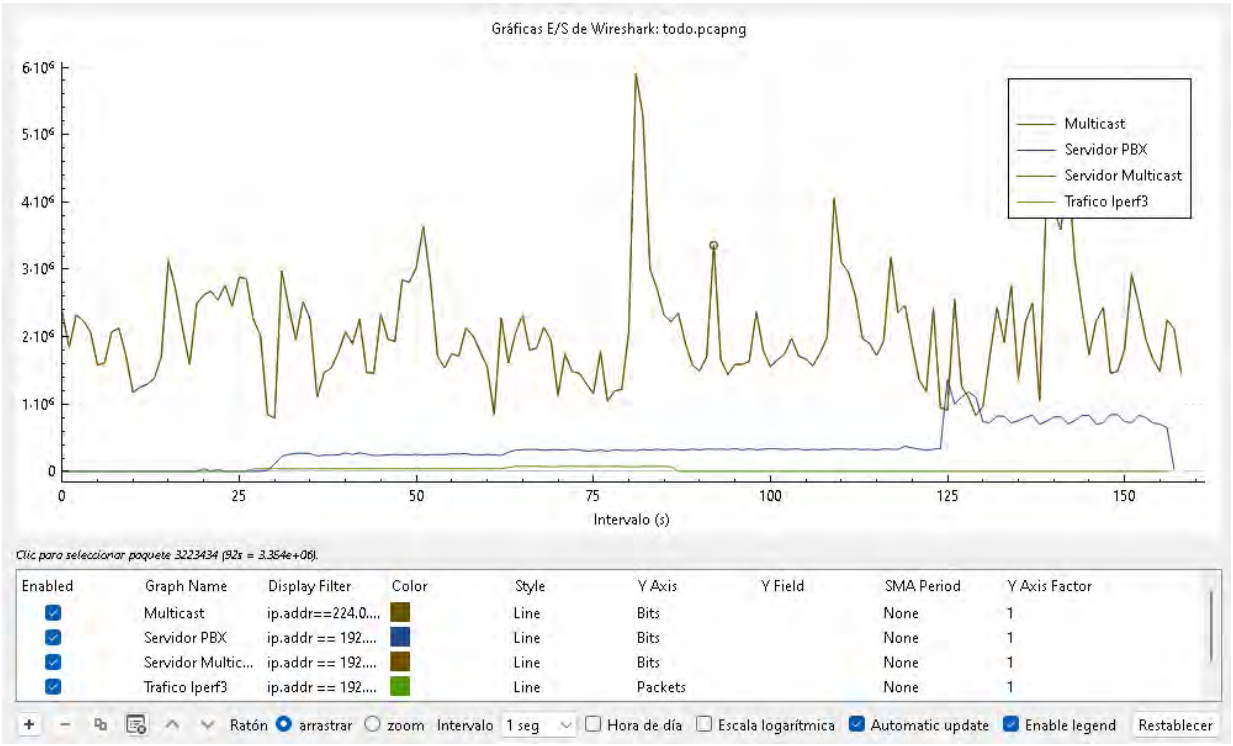


Figura 5.6.13 Trafico multicast, telefonía IP y Iperf3

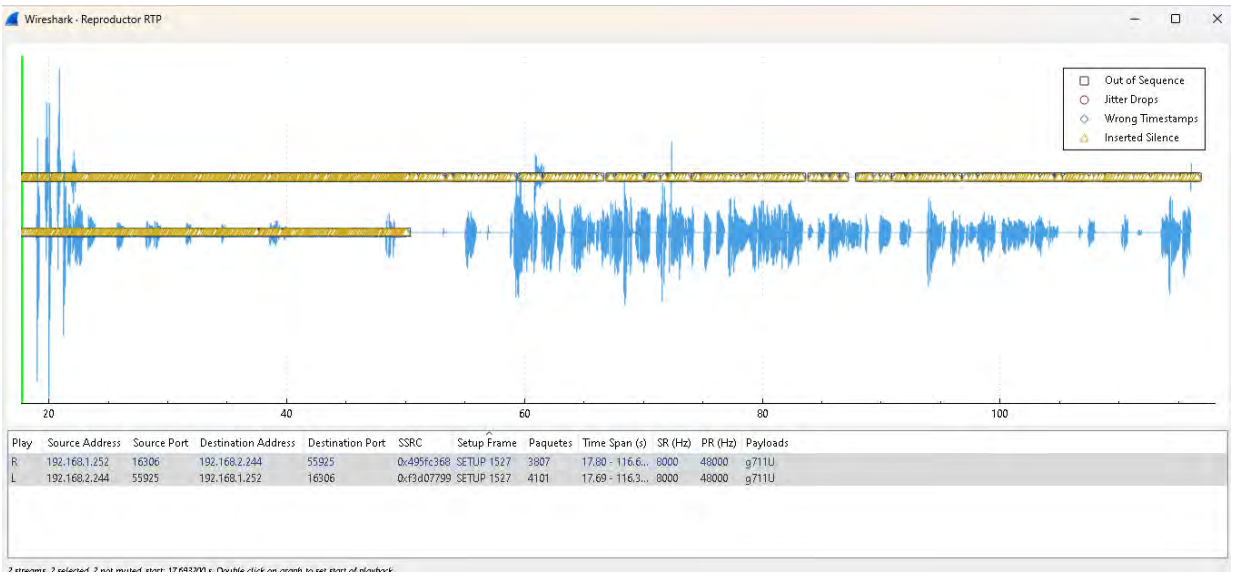
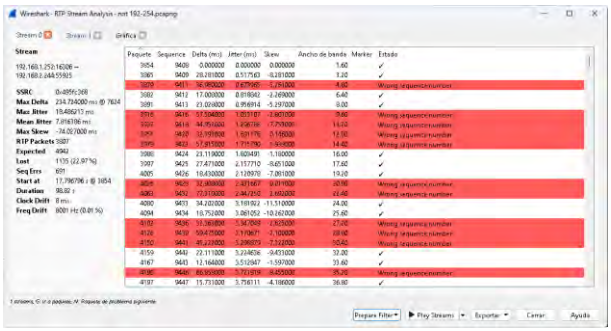
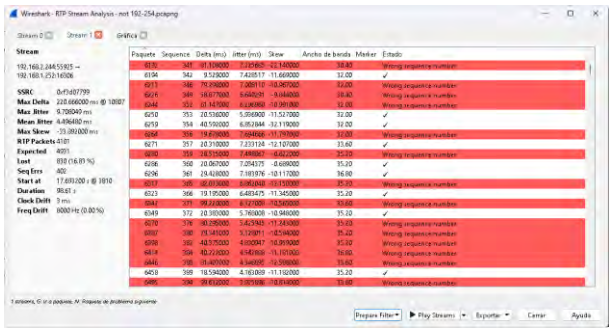


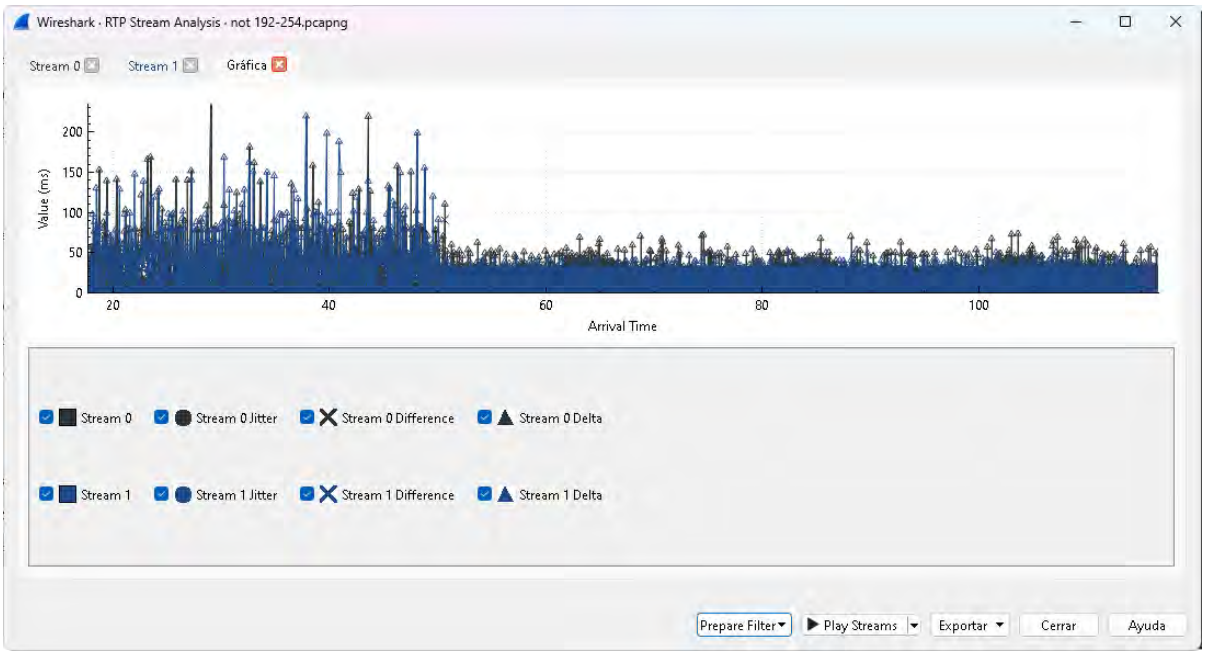
Figura 5.6.14 Reproducción del flujo de Audio





Nota: Stream RTP de una llamada, donde podemos verificar que tenemos una perdida de paquetes del 11.5 % lo que afecta la calidad del flujo de audio y video. El jitter promedio es de 7.81 ms con valores maximos de 18.48 ms lo que indica interrupciones en la transmision. Lo que podemos concluir problemas de perdida de paquetes, jitter y secuencias incorrectas lo que hace una red inestable y con congestion.

Figura 5.6.15 Flujo de datos RTP bidireccional



Nota:

El gráfico que se muestra es un gráfico de tiempo de llegada (Arrival Time) vs. Valor (ms). Más específicamente:

- En el eje X: el Arrival Time (tiempo en que van llegando los paquetes RTP).
- En el eje Y: valores en milisegundos (ms) correspondientes a delay, jitter o delta.

En la captura se ven activadas varias métricas por cada flujo RTP (“Stream 0” y “Stream 1”).

Interpretación del gráfico

- En los primeros 40 segundos, hay mucha dispersión y picos de jitter/delta, llegando incluso a valores por encima de 200 ms, lo cual indica inestabilidad en la red y congestión.
- Después del segundo 60, los valores se estabilizan mucho más, señal de que la calidad de transmisión mejora.
- Esto indica que:
    - Al inicio de la llamada hubo problemas de congestión o buffering.
    - Luego la red se estabilizó y el flujo RTP fue más regular.
- La llamada muestra inestabilidad inicial y luego estabilidad aceptable.

Figura 5.6.16 Gráfico de tiempo de llegada (Arrival Time) vs. Valor (ms)

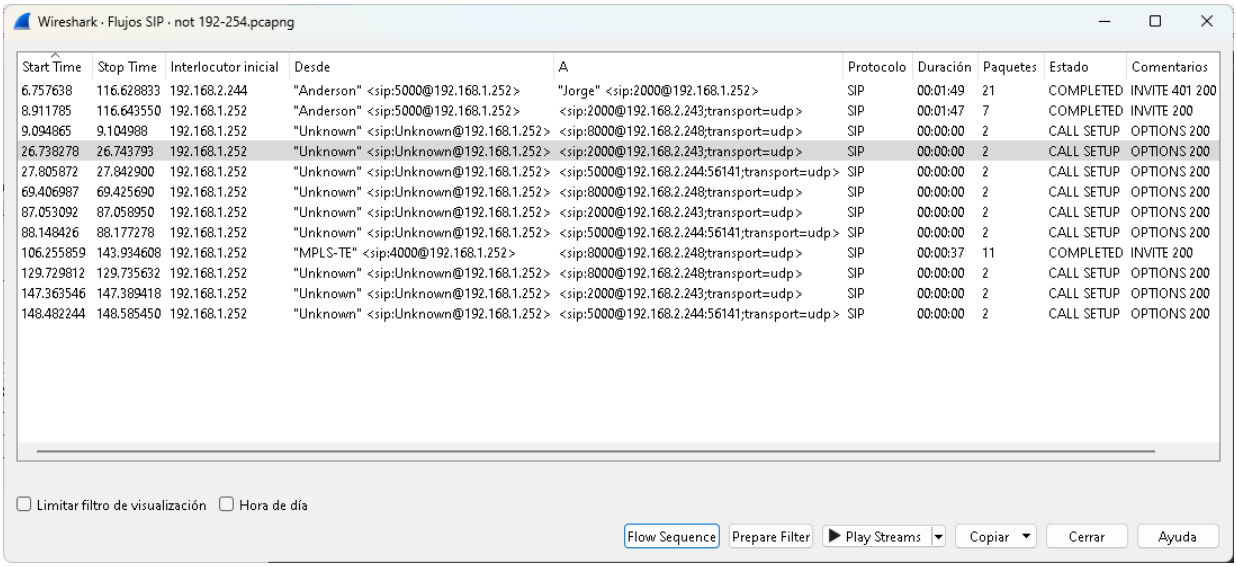


Figura 5.6.17 Flujo de SIP para establecimiento de la llamada (videollamada)

5.6.8 Medición e Interpretación en un Escenario Critico

Tabla 5.6.11 Configuración NETEM -escenario critico

Escenario	Tipo de tráfico	Parámetros críticos	Comando NetEm
Crítico	VoIP (RTP/SIP)	Delay: 300 ms Jitter: 50 ms Loss: 5%	tc qdisc change dev eth0 root Netem delay 300ms 50ms loss 5%
	Multicast (video/audio)	Delay: 400 ms Jitter: 100 ms Loss: 5%	tc qdisc change dev eth0 root Netem delay 400ms 100ms loss 5%

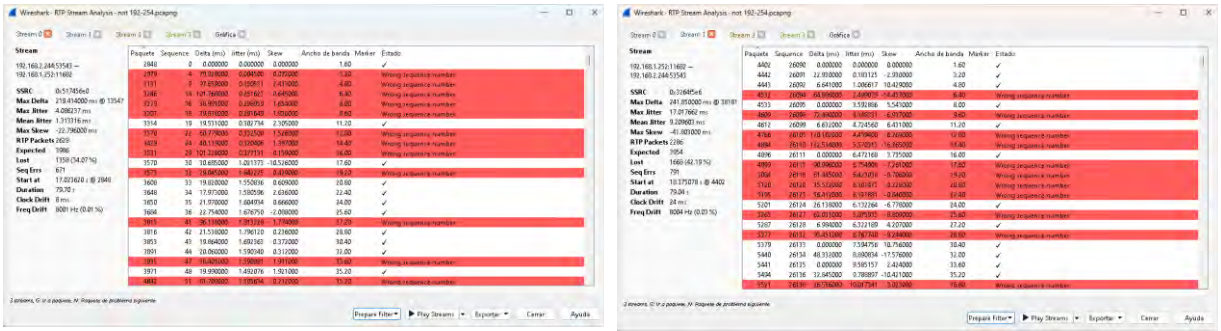
```
C:\iperf3>iperf3.exe -s -p 5203
-----------------------------------------------------------
Server listening on 5203 (test #1)
-----------------------------------------------------------
Accepted connection from 192.168.2.243, port 54550
[  5] local 192.168.1.254 port 5203 connected to 192.168.2.243 port 58850
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-60.04  sec  1.86 GBytes   266 Mbits/sec  0.025 ms  3136355/4514033 (69%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-60.04  sec  1.86 GBytes   266 Mbits/sec  0.025 ms  3136355/4514033 (69%)  receiver
-----------------------------------------------------------
Server listening on 5203 (test #2)
```

Nota: La pérdida de paquetes es muy alta (69 %) lo que presentara problemas sobre la red, generando congestión, al percibir en laboratorio el comportamiento de la red podemos notar que los servicio de multicast y videollamadas no lograron establecerse.

Figura 5.6.18 Trafico Multicast, Telefonía IP, Iperf3

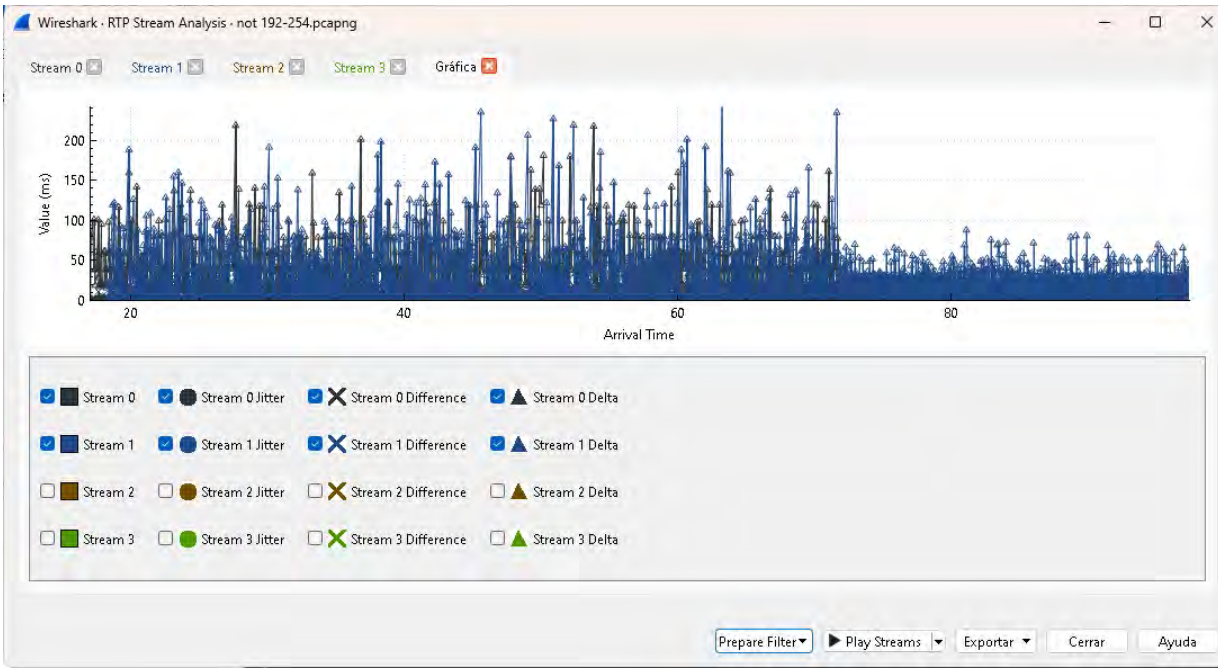
Figura 5.6.19 Trafico Multicast, Telefonía IP, Iperf3

Figura 5.6.20 Reproducción del stream de audio



Nota: La captura nos muestra que tenemos flujos RTP con errores por las condiciones de red configuradas por NETEM, induciendo un comportamiento de la red muy inestable con delay de hasta los 300 ms; en laboratorio se verifico la caida de todo los servicios.

Figura 5.6.21 Stream de RTP para la Telefonía IP

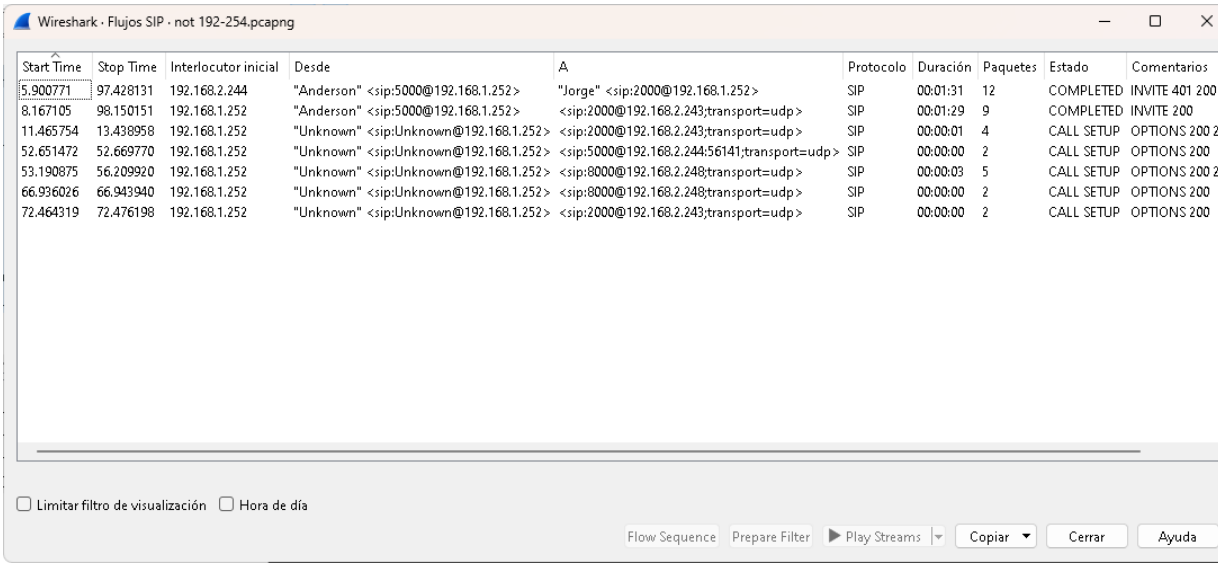


Nota:

- Hay picos notables en el Delta (hasta los 150 ms), especialmente en los flujos 0 y 1 (negro y azul), lo que indica retrasos o pérdida de paquetes en ciertos momentos.
- Patrones: Al inicio, variabilidad alta (esto es debido a establecimiento de la conexión SIP/RTP). Hacia un medio, más estable. Al final, deltas espaciados sugieren fin de la transmisión.
- Interpretación: Los valores de jitter indican inestabilidad de red. En el gráfico, los picos en delta sugieren jitter elevado en momentos puntuales, mayores a los 50 ms en algunos streams.
- Visualmente, las X estan alineadas con deltas, mostrando desviaciones. Valores altos indican desfase acumulativo, latencia variable.

Diferencias notables en los picos, afectando la sincronización de audio.

Figura 5.6.22 Análisis temporal de flujos RTP (Arrival Time vs. Jitter/Delta/Difference)



5.6.9 Reporte Comparativo de Rendimiento de Ancho de Banda con IPERF3

Esta tabla nos permite el comportamiento de los diferentes escenarios frente al tráfico generado por Iperf3, del mismo podemos concluir que el ratio de pérdidas son de 16, 21, 69, 70 por ciento que está directamente relacionado a la configuración de los parámetros de rendimiento realizado con NETEM, conforme los parámetros configurados son más críticos la perdida de paquetes es mayor afectando directamente el rendimiento de la red.

Tabla 5.6.12 Métricas de rendimiento Iperf3

Archivo	Throughput promedio (Mbps)	Throughput máx (Mbps)	Throughput mín (Mbps)	Jitter promedio (ms)	Paquetes enviados	Paquetes perdidos	Ratio de pérdida (%)	Duración (s)	Tamaño d bloque (bytes)
escenario_normal.json	776.168964	902.265541	698.391701	0.009057	4690340	773826	16.498292	70.001380	1448
escenario_leve.json	826.928443	948.597589	780.573572	0.004002	4283220	915808	21.381297	60.001347	1448
escenario_degradado.json	892.079938	918.667861	854.255052	0.002288	4620630	3184342	68.915754	60.000652	1448
escenario_critico.json	871.556982	932.049584	830.904999	0.024781	4514360	3136355	69.475075	60.001064	1448

5.6.10 Gráficos Throughput vs Tiempo (Comparativo)

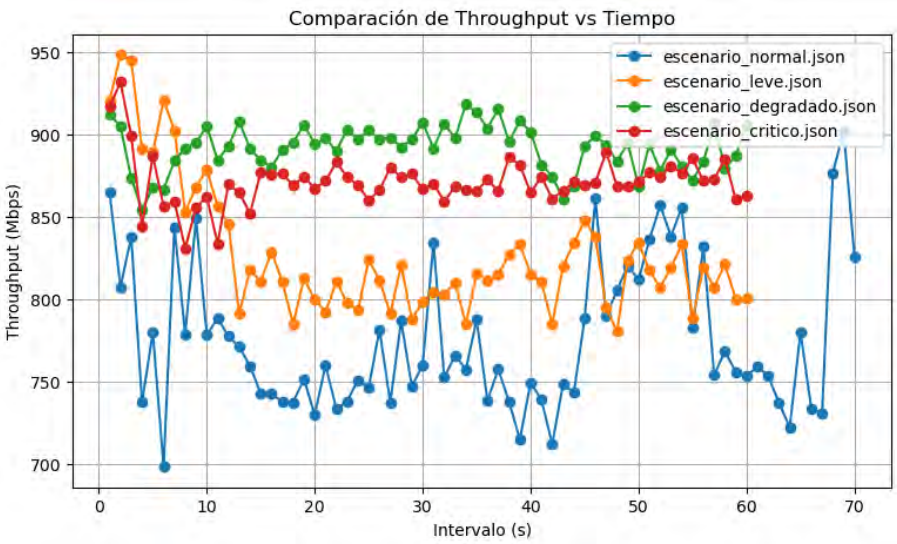


Figura 5.6.30: Comportamiento de throughput en los diferentes escenarios

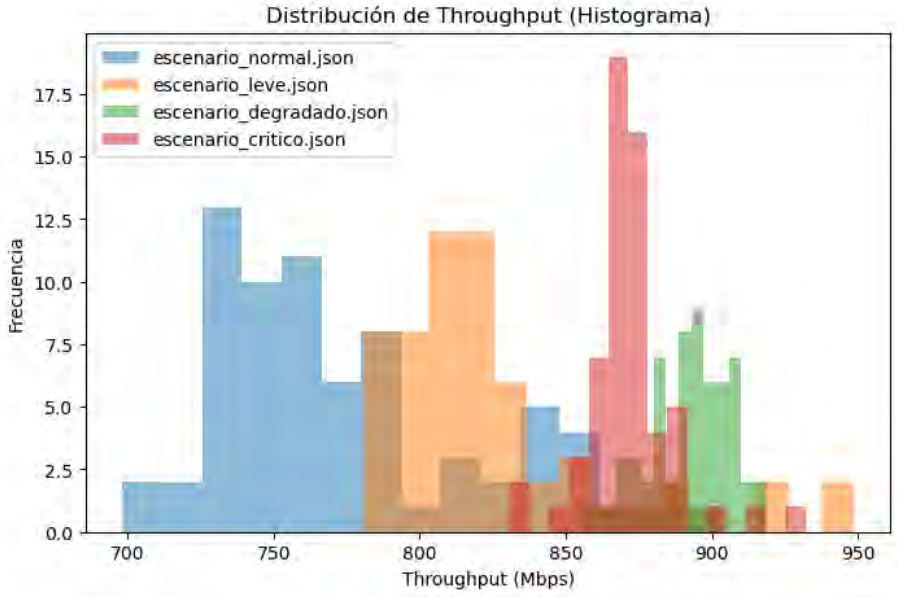


Figura 5.6.31: Histograma de Throughput

De las figuras 5.6.30 y 5.6.31 podemos interpretar que el rendimiento de la red está directamente relacionada a la variación de los parámetros de red como retardo, jitter, perdida de paquetes, donde podemos observar que mientras más altas sean los valores de estos parámetros el tráfico de la red se ve afectada hasta la caída de servicios como lo demuestra las curvas e histogramas de las figuras mencionadas.

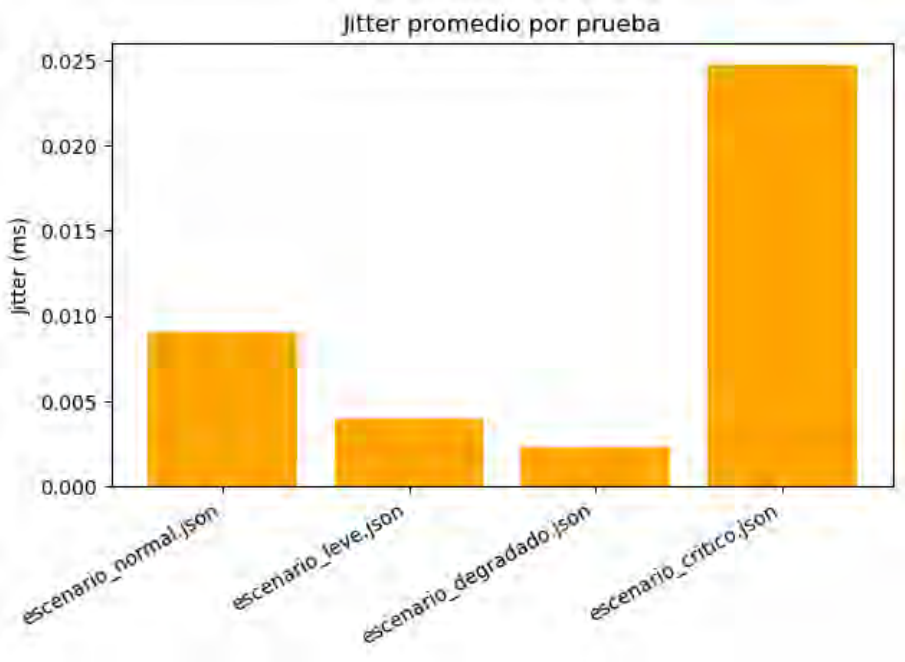


Figura 5.6.32: Jitter promedio por prueba

Las figuras 5.6.32, 5.6.33 nos permite verificar como, valores altos del (jitter) y de la perdida de paquetes está directamente relacionado a valores altos configurados de los parámetros de rendimiento de red, como se puede ver en la barra del histograma del caso “escenario_critico.json y escenario_degradado.json”.

Figura 5.6.33: Pérdida de paquetes por prueba

Conclusiones

- Se logró implementar un servicio L3VPN sobre MPLS que es transportado a través de un túnel de ingeniería de tráfico. Wireshark que es un analizador de paquetes permitió analizar el apilamiento de etiquetas, la estructura del paquete de datos en el core de la red IP/MPLS. Los diferentes tipos de tráficos (Telefonía IP, Multicast, Trafico Genérico) generados por el generador de tráfico del sistema operativo de RouterOS permito analizar el rendimiento y comportamiento de la L3VPN y VPLS, donde se observa que los equipos MikroTik tienen un mejor comportamiento con una implementación VPLS frente a una L3VPN. Esto debido a que una VPLS con ingeniería de tráfico necesita una pila de dos etiquetas, mientras que la L3VPN con ingeniería necesita una pila de tres etiquetas. Con los diferentes entornos (condiciones) de red simulados se observa como el funcionamiento de la red varia desde una red estable hasta la caída total de la red, lo que se puede verificar en las tablas y graficas del capítulo 5 (ej. tabla 5.6.6).
- Se logro analizar la interacción de los diferentes protocolos de red que hacen posible la implementación de los diferentes escenarios de laboratorio. Se puede verificar que MPLS se comporta como una red Overlay sobre una infraestructura de red Underlay IP (OSPF en nuestro caso) esto debido a que el protocolo LDP hace uso de la interconectividad lograda por OSPF para poder distribuir las etiquetas, como el protocolo BGP a través de su extensión MP-BGP nos permite distribuir las etiquetas de servicio (L3VPN y VPLS), como RSVP permite distribuir las etiquetas para formar los túneles de ingeniería de tráfico.
- Se logró implementar la red IP/MPLS, el cual permite observar cómo los paquetes IP son encapsulados por cabeceras MPLS. Esta encapsulación permite el transporte de los datos a través de la conmutación de etiquetas.
- Con la red IP/MPLS implementada, sobre esta red se logró implementar un servicio L3VPN el cual nos permite la interconectividad de un cliente a nivel de IP (protocolos de enrutamiento), se logró la conectividad del dominio IP/MPLS con la red del cliente a través de protocolos de enrutamiento, se puede ver como los enrutadores de borde (PE1, PE5) del dominio IP/MPLS usan el VRF (Virtual Routing and Forwarding) para aislar las tablas de enrutamiento de los diferentes clientes. Así diferentes clientes pueden hacer uso de la infraestructura de IP/MPLS de manera privada y segura.
- Se logró implementar el servicio VPLS sobre una infraestructura IP/MPLS el cual nos permitió transportar el tráfico de los clientes a nivel de la capa de enlace (Ethernet) no se necesitó ninguna configuración de protocolo de enrutamiento entre la red del cliente

y el dominio IP/MPLS. Para aislar el tráfico de los diferentes clientes, la VPLS hace de uso de los túneles VPLS formados por la señalización de MP-BGP y para la clasificación de los diferentes tipos de tráfico de cada cliente se hace por medio de las VLANs.

- En la implementación de los servicios de red (L3VPN y VPLS) se analizó su trasporte sobre túneles de Ingeniería de tráfico, permitiéndonos configurar rutas de trafico de manera manual, como una alternativa a las rutas que los protocolos de enrutamiento forman. Lo que nos permite una mejor gestión de los enlaces existentes de la topología implementada, y así poder evitar enlaces sobre utilizadas y subutilizadas. En el caso del servicio L3VPN se pudo verificar que el apilamiento de etiquetas en el core IP/MPLS se da a través de tres etiquetas, la sección 5.1" Análisis de Paquetes con Wireshark – L3VPN" describe este comportamiento. Mientras tanto que para el servicio VPLS es a través del apilamiento de dos etiquetas, la sección 5.3 "Análisis de Tráfico con Wireshark - VPLS" describe este comportamiento.
- La estructura de paquetes generado por el generador de paquetes de RouterOS, nos permitió estructurar diferentes tipos de paquetes que viajan a través de la red (IP/MPLS), con ello pudimos analizar y evaluar los parámetros de rendimiento de red como la latencia, jitter, perdida de paquetes. El análisis de la red con tráfico real, con servidores (servidor PBX, Multicast y Trafico Genérico) y equipos finales (Softphone, Cliente multimedia) del cliente permite observar y evaluar el funcionamiento de la red. El análisis con Wireshark sobre la red con tráfico real nos permitió verificar de mejor manera la estructura de paquetes que viaja por la red y la interacción de los diferentes protocolos que participan en el funcionamiento de la red, la sección 5.5 "Análisis de una Red con Trafico Real" detalla este comportamiento.

Recomendaciones

- Se recomienda la implementación de la tecnología MPLS con Mikrotik para clientes residenciales, empresas pequeñas y medianas, gracias a su sistema operativo de red RouterOS brinda suficiente rendimiento para implementar servicios L3VPN y VPLS con características de ingeniería de tráfico.
- Se recomienda el uso de la version 7 del sistema operativo de RouterOS que tiene una actualización muy importante en su sistema operativo que está basado en Linux 5.6 lo que le permite soportar nuevas funciones de red, hardware mejorando sus características como la del protocolo BGP que permite implementar EVPN (Ethernet VPN). Que vendría a ser un buen complemento para la implementación a MPLS.
- Se recomienda el despliegue de redes con routers Mikrotik, que, gracias a su sistema operativo, te da la flexibilidad de poder implementar muchos servicios de red a un costo relativamente bajo con respecto a otros routers, switches de capa 3 del mercado. Ofreciendo una relación costo-beneficio con respecto a otros equipos de redes.
- SI bien la tendencia es migrar hacia soluciones de tipo SDN, sin embargo, estas soluciones son ofrecidas utilizando internet como infraestructura. Esto no sería óptimo para soluciones de servicios sensibles a la latencia, perdía de paquetes. También por otro lado el proveedor que ofrece estos servicios a través de SDN no tiene control sobre las métricas de rendimiento.

Referencias

[1] T. S. N. D. A. Y. D. A. Sunat, Plan De Transición Al Protocolo Ipv6 De La Superintendencia Nacional De Aduanas Y De Administración Tributaria, Lima: Superintendencia Nacional De Aduanas Y De Administración Tributaria, 2019.

[2] G. d. T. S. R. MTC-PERU, «Informe del grupo de trabajo sectorial de naturaleza temporal del Ministerio de Transportes y Comunicaciones,» Ministerio de Transportes y Comunicaciones, Lima, 2022.

[3] O. S. d. I. P. e. T. OSIPTEL, Diciembre 2024. [En línea]. Available: https://www.osiptel.gob.pe/portal-del-usuario/noticias/peru-registro-mas-de-4-millones-de-conexiones-de-internet-fijo-al-cierre-de-2024/.

[4] CEPLAN, «Incremento de la conectividad digital,» CEPLAN, AMERICA LATINA, 2025.

[5] D. M. Alvaro Andragon, Diseño y Simulacion de una Red MPLS Utilizando Equipos Mikrotik y el Emulador GNS3 en entornos PYMES, Santiago de Chile: Universidad de las Americas, 2019.

[6] C. D. Moreno Ibañez y J. C. Quiñonez Pazmiño, Diseño de Una Red Con DMVPN Sobre la Red MPLS de PUNTONET, Quito: Universidad Politécnica Salesiana sede Quito, 2020.

[7] D. Carpio Ortiz, Desarrollo y Configuración de un Entorno MPLS en Equipos Mikrotik y Simulado en GNS3, Valencia - España: Universidad Politécnica de Valéncia, 2024.

[8] J. L. S. Escobar Poma, Implementacion de una infraestructura de red basada en tecnologias MPLS con mejoras de Ingenieria de Trafico para el Sector Industrial - Lima 2022, Lima: Universidad Tecnologica del Perú, 2023.

[9] J. E. Flores Baldés, Análisis del Desempeño de MPLS VPN L2 y L3, Santiago de Chile: Universidad de Chile, 2018.

[10] J. Wei y N. I. Roman, Deploy MPLS L3 VPN, Ho Chi Minh City, Viet nam: APNIC, 2017.

[11] J. Wei, Deploy VPLS, Ho Chi Minh City, Viet nam: APNIC, 2016.

[12] N. Islam Roman y J. Wei, Deploy MPLS Traffic Engineering, Ho Chi Minh City, Vietnam: APNIC, 2017.

[13] Mikrotik, «Mikrotik, Products,» 15 07 2022. [En línea]. Available: https://mikrotik.com/product/ccr2004_16g_2splus. [Último acceso: 09 09 2025].

[14] J. Crichigno, E. Kfoury y J. Gomez, NETWORK TOOLS AND PROTOCOLS LAB SERIES, Carolina del Sur: University of South Carolina, 2021.

[15] J. M. Roman, MIKROTIK TRAFFIC GENERATOR STUDY CASE, Spain: MUM EUROPE, MIKROTIK, 2017.

[16] Mikrotik, «Una empresa de fabricacion de equipos de redes y comunicaciones,» Mikrotik, [En línea]. Available: https://help.mikrotik.com/docs/. [Último acceso: 15 Enero 2025].

[17] A. S. Tanenbaum y D. J. Wetherall, Redes de Computadoras, México: PEARSON EDUCACION, 2012.

Anexos

Anexo A: Script de Configuración de los Equipos para L3VPN

PE1	PE2
# model = CCR2004-16G-2S+ /interface bridge add name=loop add disabled=yes name=tunnel-vpls /interface vpls add arp=enabled bridge=tunnel-vpls bridge-horizon=1 disabled=no mac-address=\ 02:A3:53:E5:27:65 mtu=1500 name=vpls15 peer=192.170.0.6 vpls-id=2:5 /ip vrf add interfaces=ether2 name=VRF-CE1 add interfaces=ether4,loop name=VRF-CE2 /mpls traffic-eng path add disabled=no hops="50.0.0.2/strict,60.0.0.1/strict,60.0.0.2/strict,70.0.0.1\ /strict,70.0.0.2/strict" name=R-Principal record-route=yes add disabled=no hops="30.0.0.2/strict,90.0.0.1/strict,90.0.0.2/strict,70.0.0.1\ /strict,70.0.0.2/strict" name=Respaldo record-route=yes use-cspf=no add disabled=no name=D-CFS record-route=yes use-cspf=yes /port set 0 name=serial0 /routing ospf instance add disabled=no mpls-te-address=192.170.0.2 mpls-te-area=0.0.0.0 name=\ ospf-instance-1 add disabled=no name=ospf-instance-2 redistribute=bgp-mpls-vpn router-id=\ 192.170.0.11 routing-table=VRF-CE2 vrf=VRF-CE2 /routing ospf area add disabled=no instance=ospf-instance-1 name=ospf-area-1 add disabled=no instance=ospf-instance-2 name=ospf-area-2 /routing pimsm instance add disabled=no name=pimsm-instance1 vrf=VRF-CE2 /snmp community set [find default=yes] disabled=yes add addresses=192.168.99.251/32 name=zabbix_test /ip address add address=192.170.0.2 interface=lo network=192.170.0.2 add address=30.0.0.1/30 interface=ether3 network=30.0.0.0 add address=50.0.0.1/30 interface=ether1 network=50.0.0.0 add address=10.0.0.1/30 interface=ether2 network=10.0.0.0 add address=192.168.10.1/24 interface=vpls15 network=192.168.10.0 add address=10.0.2.1/30 interface=ether4 network=10.0.2.0 add address=192.170.0.11 interface=loop network=192.170.0.11 /ip dhcp-client	# model = CCR2004-16G-2S+ /interface bridge add name=loop add disabled=yes name=tunnel-vpls /interface vpls add arp=enabled bridge=tunnel-vpls bridge-horizon=1 disabled=no mac-address=\ 02:CB:30:30:13:DF mtu=1500 name=vpls51 peer=192.170.0.2 vpls-id=2:5 /ip vrf add interfaces=ether2 name=VRF-CE2 add interfaces=ether3,loop name=VRF-CE3 /mpls traffic-eng path add disabled=no hops="70.0.0.1/strict,60.0.0.2/strict,60.0.0.1/strict,50.0.0.2\ /strict,50.0.0.1/strict" name=R-Principal record-route=yes add disabled=no hops="40.0.0.1/strict,80.0.0.1/strict,80.0.0.2/strict,50.0.0.2\ /strict,50.0.0.1/strict" name=Respaldo record-route=yes use-cspf=no add disabled=no name=D-CFS record-route=yes use-cspf=yes /port set 0 name=serial0 /routing ospf instance add disabled=no mpls-te-address=192.170.0.6 mpls-te-area=0.0.0.0 name=\ ospf-instance-1 add disabled=no name=ospf-instance-2 redistribute=bgp-mpls-vpn router-id=\ 192.170.0.21 routing-table=VRF-CE3 vrf=VRF-CE3 /routing ospf area add disabled=no instance=ospf-instance-1 name=ospf-area-1 add disabled=no instance=ospf-instance-2 name=ospf-area-2 /routing pimsm instance add disabled=no name=pimsm-instance1 vrf=VRF-CE3 /ip address add address=192.170.0.6 interface=lo network=192.170.0.6 add address=40.0.0.2/30 interface=ether4 network=40.0.0.0 add address=70.0.0.2/30 interface=ether1 network=70.0.0.0 add address=20.0.0.1/30 interface=ether2 network=20.0.0.0 add address=192.168.10.2/24 interface=vpls51 network=192.168.10.0 add address=20.0.2.1/30 interface=ether3 network=20.0.2.0 add address=192.170.0.21 interface=loop network=192.170.0.21 /ip dhcp-client add interface=ether1 /ip route add dst-address=192.170.0.2 gateway=192.168.10.1

```
add interface=ether1
/ip route
add dst-address=192.170.0.6 gateway=192.168.10.2
/mpls interface
add input=yes interface=ether1 mpls-mtu=1580
add input=yes interface=ether3 mpls-mtu=1580
/mpls ldp
add afi=ip disabled=no lsr-id=192.170.0.2 transport-
addresses=192.170.0.2 \
   use-explicit-null=no
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether3
/mpls settings
set dynamic-label-range=1000-2999
/mpls traffic-eng interface
add bandwidth=100Mbps disabled=no
interface=ether1
add bandwidth=100Mbps disabled=no
interface=ether3
/mpls traffic-eng tunnel
add bandwidth=15Mbps disabled=no from-
address=192.170.0.2 name=tunnel15 \
   primary-path=R-Principal secondary-
paths=Respaldo,D-CFS to-address=\
   192.170.0.6
/routing bgp connection
add as=65000 connect=yes disabled=no listen=yes
local.address=10.0.0.1 .role=\
   ebgp name=sesion-EBGP-CE1 nexthop-
choice=force-self output.redistribute=\
   bgp,bgp-mpls-vpn .remove-private-as=yes
remote.address=10.0.0.2/32 .as=\
   65500 router-id=192.170.0.2 routing-table=VRF-
CE1 vrf=VRF-CE1
add afi=ip,vpnv4 as=65000 connect=yes disabled=no
listen=yes local.address=\
   192.170.0.2 .role=ibgp multihop=no name=sesion-
IBGP-PE5 \
   output.redistribute=bgp
remote.address=192.170.0.6/32 .as=65000 \
   router-id=192.170.0.2 routing-table=main
/routing bgp vpn
add disabled=no export.redistribute=bgp .route-
targets=10:1 \
   import.route-targets=10:1 .router-id=VRF-CE1 label-
allocation-policy=\
   per-vrf name=bgp-mpls-vpn-1 route-
distinguisher=10:1 vrf=VRF-CE1
add disabled=no export.redistribute=ospf .route-
targets=20:1 \
   import.route-targets=20:1 .router-id=VRF-CE2 label-
allocation-policy=\
   per-vrf name=bgp-mpls-vpn-2 route-
distinguisher=20:1 vrf=VRF-CE2
/routing filter rule
add chain=te-policy disabled=yes rule=\
   "if (dst in 192.170.0.6/32) {set gw 50.0.0.2; accept}"
/routing ospf interface-template
add area=ospf-area-1 disabled=no interfaces=lo
passive
add area=ospf-area-1 disabled=no interfaces=ether1
type=ptp
add area=ospf-area-1 disabled=no interfaces=ether3
type=ptp
add area=ospf-area-2 disabled=no interfaces=ether4
type=ptp
```

```
/mpls interface
add input=yes interface=ether1 mpls-mtu=1580
add input=yes interface=ether4 mpls-mtu=1580
/mpls ldp
add afi=ip disabled=no lsr-id=192.170.0.6 transport-
addresses=192.170.0.6 \
   use-explicit-null=no
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether4
/mpls settings
set dynamic-label-range=9000-10999
/mpls traffic-eng interface
add bandwidth=100Mbps disabled=no
interface=ether1
add bandwidth=100Mbps disabled=no
interface=ether4
/mpls traffic-eng tunnel
add bandwidth=15Mbps disabled=no from-
address=192.170.0.6 name=tunnel51 \
   primary-path=R-Principal secondary-
paths=Respaldo to-address=192.170.0.2
/routing bgp connection
add as=65000 connect=yes disabled=no listen=yes
local.address=20.0.0.1 .role=\
   ebgp name=sesion-EBGP-CE2 nexthop-
choice=force-self output.redistribute=\
   bgp,bgp-mpls-vpn .remove-private-as=yes
remote.address=20.0.0.2/32 .as=\
   65500 router-id=192.170.0.6 routing-table=VRF-
CE2 vrf=VRF-CE2
add afi=ip,vpnv4 as=65000 connect=yes disabled=no
listen=yes local.address=\
   192.170.0.6 .role=ibgp multihop=no name=sesion-
IBGP-PE1 \
   output.redistribute=bgp
remote.address=192.170.0.2/32 .as=65000 \
   router-id=192.170.0.6 routing-table=main
/routing bgp vpn
add disabled=no export.redistribute=bgp .route-
targets=10:1 \
   import.route-targets=10:1 .router-id=VRF-CE2 label-
allocation-policy=\
   per-vrf name=bgp-mpls-vpn-1 route-
distinguisher=10:2 vrf=VRF-CE2
add disabled=no export.redistribute=ospf .route-
targets=20:1 \
   import.route-targets=20:1 .router-id=VRF-CE3 label-
allocation-policy=\
   per-vrf name=bgp-mpls-vpn-2 route-
distinguisher=20:2 vrf=VRF-CE3
/routing filter rule
add chain=te-policy disabled=yes rule=\
   "if (dst in 192.170.0.2/32) {set gw 70.0.0.1; accept}"
/routing ospf interface-template
add area=ospf-area-1 disabled=no interfaces=lo
passive
add area=ospf-area-1 disabled=no interfaces=ether1
type=ptp
add area=ospf-area-1 disabled=no interfaces=ether4
type=ptp
add area=ospf-area-2 disabled=no interfaces=ether3
type=ptp
add area=ospf-area-2 disabled=no interfaces=loop
passive
/routing pimsm interface-template
add disabled=no instance=pimsm-instance1
interfaces=ether3,loop
```

```
add area=ospf-area-2 disabled=no interfaces=loop
passive
/routing pimsm interface-template
add disabled=no instance=pimsm-instance1
interfaces=ether4,loop
/routing pimsm static-rp
add address=192.170.0.20 instance=pimsm-instance1
/system identity
set name=PE1
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
```

```
/routing pimsm static-rp
add address=192.170.0.20 instance=pimsm-instance1
/system identity
set name=PE5
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
/tool sniffer
set filter-interface=ether3,ether4
```

P2

```
# model = CCR2004-16G-2S+
/ip pool
add name=dhcp_pool0 ranges=192.168.99.2-
192.168.99.254
/port
set 0 name=serial0
/routing ospf instance
add disabled=no mpls-te-address=192.170.0.3 mpls-
te-area=0.0.0.0 name=\
    ospf-instance-1
/routing ospf area
add disabled=no instance=ospf-instance-1
name=ospf-area-1
/snmp community
set [ find default=yes ] disabled=yes
add addresses=192.168.99.254/32 name=zabbix_test
/ip address
add address=192.168.137.8/24 interface=ether8
network=192.168.137.0
add address=192.170.0.3 interface=lo
network=192.170.0.3
add address=30.0.0.2/30 interface=ether3
network=30.0.0.0
add address=80.0.0.1/30 interface=ether1
network=80.0.0.0
add address=90.0.0.1/30 interface=ether2
network=90.0.0.0
add address=40.0.0.1/30 interface=ether4
network=40.0.0.0
add address=192.168.99.1/24 interface=ether7
network=192.168.99.0
/ip dhcp-client
add interface=ether1
/ip dhcp-server
add address-pool=dhcp_pool0 interface=ether7
name=dhcp1
/ip dhcp-server network
add address=192.168.99.0/24 gateway=192.168.99.1
/mpls interface
add input=yes interface=ether1 mpls-mtu=1580
add input=yes interface=ether2 mpls-mtu=1580
add input=yes interface=ether3 mpls-mtu=1580
add input=yes interface=ether4 mpls-mtu=1580
/mpls ldp
add afi=ip disabled=no lsr-id=192.170.0.3 transport-
addresses=192.170.0.3
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether2
add disabled=no interface=ether3
add disabled=no interface=ether4
/mpls settings
set dynamic-label-range=3000-4999
/mpls traffic-eng interface
```

P3

```
# model = CCR2004-16G-2S+
/port
set 0 name=serial0
/routing ospf instance
add disabled=no mpls-te-address=192.170.0.4 mpls-
te-area=0.0.0.0 name=\
    ospf-instance-1
/routing ospf area
add disabled=no instance=ospf-instance-1
name=ospf-area-1
/ip address
add address=192.170.0.4 interface=lo
network=192.170.0.4
add address=50.0.0.2/30 interface=ether1
network=50.0.0.0
add address=80.0.0.2/30 interface=ether3
network=80.0.0.0
add address=60.0.0.1/30 interface=ether2
network=60.0.0.0
/ip dhcp-client
add interface=ether1
/mpls interface
add input=yes interface=ether1 mpls-mtu=1580
add input=yes interface=ether2 mpls-mtu=1580
add input=yes interface=ether3 mpls-mtu=1580
/mpls ldp
add afi=ip disabled=no lsr-id=192.170.0.4 transport-
addresses=192.170.0.4
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether2
add disabled=no interface=ether3
/mpls mangle
add chain=forward exp=0 set-exp=3 set-mark=m0
/mpls settings
set dynamic-label-range=6000-7999
/mpls traffic-eng interface
add bandwidth=100Mbps disabled=no
interface=ether1
add bandwidth=100Mbps disabled=no
interface=ether2
add bandwidth=100Mbps disabled=no
interface=ether3
/routing ospf interface-template
add area=ospf-area-1 disabled=no interfaces=lo
passive
add area=ospf-area-1 disabled=no interfaces=ether1
type=ptp
add area=ospf-area-1 disabled=no interfaces=ether2
type=ptp
add area=ospf-area-1 disabled=no interfaces=ether3
type=ptp
/system identity
set name=P3
```

```
add bandwidth=100Mbps disabled=no
interface=ether1
add bandwidth=100Mbps disabled=no
interface=ether2
add bandwidth=100Mbps disabled=no
interface=ether3
add bandwidth=100Mbps disabled=no
interface=ether4
/routing ospf interface-template
add area=ospf-area-1 disabled=no interfaces=lo
passive
add area=ospf-area-1 disabled=no interfaces=ether1
type=ptp
add area=ospf-area-1 disabled=no interfaces=ether2
type=ptp
add area=ospf-area-1 disabled=no interfaces=ether3
type=ptp
add area=ospf-area-1 disabled=no interfaces=ether4
type=ptp
add area=ospf-area-1 disabled=no interfaces=ether7
/snmp
set contact=andervalpe@gmail.com enabled=yes
location="Unsaac, Cusco" \
    src-address=192.168.99.1 trap-
community=zabbix_test
/system identity
set name=P2
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
```

```
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
```

P4

```
# model = CCR2004-16G-2S+
/port
set 0 name=serial0
/routing ospf instance
add disabled=no mpls-te-address=192.170.0.5 mpls-
te-area=0.0.0.0 name=\
    ospf-instance-1
/routing ospf area
add disabled=no instance=ospf-instance-1
name=ospf-area-1
/ip address
add address=192.170.0.5 interface=lo
network=192.170.0.5
add address=70.0.0.1/30 interface=ether1
network=70.0.0.0
add address=60.0.0.2/30 interface=ether2
network=60.0.0.0
add address=90.0.0.2/30 interface=ether3
network=90.0.0.0
/ip dhcp-client
add interface=ether1
/mpls interface
add input=yes interface=ether1 mpls-mtu=1580
add input=yes interface=ether2 mpls-mtu=1580
add input=yes interface=ether3 mpls-mtu=1580
/mpls ldp
add afi=ip disabled=no lsr-id=192.170.0.5 transport-
addresses=192.170.0.5
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether2
add disabled=no interface=ether3
/mpls mangle
add chain=forward exp=0 set-exp=3 set-mark=m0
/mpls settings
set dynamic-label-range=7000-8999
```

CE1

```
# model = CCR2004-16G-2S+
/interface bridge
add name=LAN
/ip pool
add name=dhcp_pool0 ranges=192.168.1.2-
192.168.1.254
/ip dhcp-server
add address-pool=dhcp_pool0 interface=ether1
name=dhcp1
/port
set 0 name=serial0
/ip address
add address=192.170.0.1 interface=lo
network=192.170.0.1
add address=10.0.0.2/30 interface=ether2
network=10.0.0.0
add address=192.168.1.1/24 interface=ether1
network=192.168.1.0
/ip dhcp-client
add interface=ether1
/ip dhcp-server network
add address=192.168.1.0/24 gateway=192.168.1.1
/ip firewall address-list
add address=192.168.1.0/24 list=BGP-OUT
/routing bgp connection
add as=65500 connect=yes disabled=no listen=yes
local.address=10.0.0.2 .role=\
    ebgp name=sesion-EBGP-PE1
output.network=BGP-OUT remote.address=\
    10.0.0.1/32 .as=65000 router-id=192.170.0.1
/system identity
set name=CE1-A
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
```

/mpls traffic-eng interface add bandwidth=100Mbps disabled=no interface=ether1 add bandwidth=100Mbps disabled=no interface=ether2 add bandwidth=100Mbps disabled=no interface=ether3 /routing ospf interface-template add area=ospf-area-1 disabled=no interfaces=lo passive add area=ospf-area-1 disabled=no interfaces=ether1 type=ptp add area=ospf-area-1 disabled=no interfaces=ether2 type=ptp add area=ospf-area-1 disabled=no interfaces=ether3 type=ptp /system identity set name=P4 /system routerboard settings set enter-setup-on=delete-key /tool romon set enabled=yes	

Anexo B: Script de Configuración de los Equipos para VPLS

PE1	**PE5**
# model = CCR2004-16G-2S+ /mpls traffic-eng path add comment="Ruta_Principal hacia PE5" hops="50.0.0.2/strict,60.0.0.1/strict,6\ 0.0.0.2/strict,70.0.0.1/strict,70.0.0.2/strict" name=Ruta_hacia_PE5 /port set 0 name=serial0 /queue tree add limit-at=200M max-limit=200M name=TRAFICO- MPLS parent=global add limit-at=200M max-limit=200M name=RESTO packet-mark=otros-paquetes \ parent=TRAFICO-MPLS add limit-at=5M max-limit=5M name=VOIP packet- mark=paquet-voip parent=\ TRAFICO-MPLS priority=1 add limit-at=20M max-limit=20M name=MULTICAST packet-mark=paquete-multicast \ parent=TRAFICO-MPLS priority=3 add disabled=yes limit-at=200M max-limit=200M name=TRAFICO_SINQOS \ packet-mark=sinqos-paquetes parent=global /routing bgp template set default afi=ip,l2vpn as=65000 disabled=no router- id=192.170.0.2 \ routing-table=main /routing ospf instance add disabled=no name=ospf-vpls-te router- id=192.170.0.2 /routing ospf area add disabled=no instance=ospf-vpls-te name=ospf- area-vpls-te /ip address add address=192.170.0.2 interface=lo network=192.170.0.2	# model = CCR2004-16G-2S+ /interface bridge add igmp-snooping=yes name=Bridge- VPLS /mpls traffic-eng path add comment="Ruta principal hacia PE1" hops="70.0.0.1/strict,60.0.0.2/strict,6\ 0.0.0.1/strict,50.0.0.2/strict,50.0.0.1/strict" name=Ruta_hacia_PE1 /port set 0 name=serial0 /routing bgp template set default afi=ip,l2vpn as=65000 disabled=no router-id=192.170.0.6 \ routing-table=main /routing ospf instance add disabled=no name=ospf-vpls-te router-id=192.170.0.6 /routing ospf area add disabled=no instance=ospf-vpls-te name=ospf-area-vpls-te /interface bridge port add bridge=Bridge-VPLS interface=ether2 /ip address add address=192.170.0.6 interface=lo network=192.170.0.6 add address=40.0.0.2/30 interface=ether4 network=40.0.0.0 add address=70.0.0.2/30 interface=ether1 network=70.0.0.0 add address=2.2.2.2/24 interface=ether2 network=2.2.2.0 add address=192.168.33.2/30 interface=vpls1 network=192.168.33.0 /ip route

```
add address=30.0.0.1/30 interface=ether3
network=30.0.0.0
add address=50.0.0.1/30 interface=ether1
network=50.0.0.0
add address=1.1.1.2/24 interface=ether2
network=1.1.1.0
add address=192.168.33.1/30 interface=vpls1
network=192.168.33.0
/ip firewall address-list
add address=192.170.0.77 disabled=yes list=Multicast
add address=239.1.1.10 list=Multicast
/ip firewall mangle
add action=mark-packet chain=prerouting
comment="REGLAS VOIP" dscp=46 \
   dst-address=2.2.2.1 new-packet-mark=paquet-voip
passthrough=no
add action=mark-packet chain=prerouting dscp=26 dst-
address=2.2.2.1 \
   new-packet-mark=paquet-voip passthrough=no
add action=mark-connection chain=prerouting
comment=REGLAS-MULTICAST dscp=28 \
   dst-address=224.0.67.67 new-connection-
mark=multicast-conn protocol=udp \
   src-address=1.1.1.1
add action=mark-packet chain=prerouting connection-
mark=multicast-conn \
   new-packet-mark=paquete-multicast passthrough=no
add action=mark-packet chain=prerouting
comment=OTRAS-REGLAS dst-address=\
   2.2.2.1 new-packet-mark=otros-paquetes
passthrough=no protocol=udp
add action=mark-packet chain=prerouting
comment="SIN QoS" disabled=yes \
   new-packet-mark=sinqos-paquetes passthrough=no
/ip route
add dst-address=2.2.2.0/24 gateway=192.168.33.2
/mpls ldp
add disabled=no lsr-id=192.170.0.2 transport-
addresses=192.170.0.2
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether3
/mpls settings
set allow-fast-path=no dynamic-label-range=1000-2999
/mpls traffic-eng interface
add bandwidth=1Gbps disabled=no interface=ether1
add bandwidth=1Gbps disabled=no interface=ether3
/mpls traffic-eng tunnel
add bandwidth=1Gbps disabled=no from-
address=192.170.0.2 name=\
   tunnel-hacia-pe5 primary-path=Ruta_hacia_PE5 to-
address=192.170.0.6
/routing bgp connection
add afi=l2vpn as=65000 connect=yes disabled=no
listen=yes local.address=\
   192.170.0.2 .role=ibgp name=conexion-ibgp-PE5
output.redistribute="" \
   remote.address=192.170.0.6/32 .as=65000 router-
id=192.170.0.2 \
   routing-table=main templates=default
/routing bgp vpls
add dst-address=1.1.1.0/24
gateway=192.168.33.1
/mpls ldp
add disabled=no lsr-id=192.170.0.6
transport-addresses=192.170.0.6
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether4
/mpls settings
set allow-fast-path=no dynamic-label-
range=9000-10999
/mpls traffic-eng interface
add bandwidth=1Gbps disabled=no
interface=ether1
add bandwidth=1Gbps disabled=no
interface=ether4
/mpls traffic-eng tunnel
add bandwidth=1Gbps disabled=no from-
address=192.170.0.6 name=\
   tunnel-hacia-pe1 primary-
path=Ruta_hacia_PE1 to-
address=192.170.0.2
/routing bgp connection
add afi=l2vpn as=65000 connect=yes
disabled=no listen=yes local.address=\
   192.170.0.6 .role=ibgp name=conexion-
ibgp-PE1 output.redistribute="" \
   remote.address=192.170.0.2/32
.as=65000 router-id=192.170.0.6 \
   routing-table=main templates=default
/routing bgp vpls
add bridge=Bridge-VPLS bridge-
horizon=1 disabled=no export-route-
targets=\
   65000:5 import-route-targets=65000:1
name=vpls-bgp rd=65000:5 site-id=5
/routing ospf interface-template
add area=ospf-area-vpls-te disabled=no
interfaces=lo networks=192.170.0.6/32 \
   passive
add area=ospf-area-vpls-te disabled=no
interfaces=ether1,ether2,ether4 \

networks=70.0.0.0/30,20.0.0.0/30,40.0.0.0
/30 type=ptp
/system identity
set name=PE-5
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
/tool sniffer
set file-name=cap-vpls-PE5-vpls1-2 filter-
interface=vpls1,ether2
```

```
add bridge-horizon=1 disabled=no export-route-
targets=65000:1 \
    import-route-targets=65000:5 name=vpls-bgp
rd=65000:1 site-id=1
/routing igmp-proxy interface
add interface=ether2 upstream=yes
add interface=vpls1
/routing ospf interface-template
add area=ospf-area-vpls-te disabled=no interfaces=lo
networks=192.170.0.2/32 \
    passive
add area=ospf-area-vpls-te disabled=no
interfaces=ether1,ether3 networks=\
    30.0.0.0/30,50.0.0.0/30 type=ptp
/system identity
set name=PE-1
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
/tool sniffer
set file-name=Cap-VPLS-PE1 filter-
interface=ether2,vpls1
```

P2

```
# model = CCR2004-16G-2S+
/port
set 0 name=serial0
/routing ospf instance
add disabled=no mpls-te-address=192.170.0.3 mpls-te-
area=0.0.0.0 name=\
    ospf-vpls-te router-id=192.170.0.3
/routing ospf area
add disabled=no instance=ospf-vpls-te name=ospf-
area-vpls-te
/ip address
add address=192.170.0.3 interface=lo
network=192.170.0.3
add address=30.0.0.2/30 interface=ether3
network=30.0.0.0
add address=40.0.0.1/30 interface=ether4
network=40.0.0.0
add address=90.0.0.1/30 interface=ether2
network=90.0.0.0
add address=80.0.0.1/30 interface=ether1
network=80.0.0.0
add address=100.0.0.1/30 interface=ether5
network=100.0.0.0
/mpls ldp
add disabled=no lsr-id=192.170.0.3 transport-
addresses=192.170.0.3
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether2
add disabled=no interface=ether3
add disabled=no interface=ether4
add disabled=no interface=ether5
/mpls settings
set allow-fast-path=no dynamic-label-range=3000-4999
/mpls traffic-eng interface
add bandwidth=1Gbps disabled=no interface=ether1
add bandwidth=1Gbps disabled=no interface=ether2
```

P3

```
# model = CCR2004-16G-2S+
/port
set 0 name=serial0
/routing ospf instance
add disabled=no name=ospf-vpls-te
router-id=192.170.0.4
/routing ospf area
add disabled=no instance=ospf-vpls-te
name=ospf-area-vpls-te
/ip address
add address=192.170.0.4 interface=lo
network=192.170.0.4
add address=60.0.0.1/30 interface=ether2
network=60.0.0.0
add address=50.0.0.2/30 interface=ether1
network=50.0.0.0
add address=80.0.0.2/30 interface=ether3
network=80.0.0.0
/mpls ldp
add disabled=no lsr-id=192.170.0.4
transport-addresses=192.170.0.4
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether2
add disabled=no interface=ether3
/mpls settings
set allow-fast-path=no dynamic-label-
range=5000-6999
/mpls traffic-eng interface
add bandwidth=1Gbps disabled=no
interface=ether1
add bandwidth=1Gbps disabled=no
interface=ether2
add bandwidth=1Gbps disabled=no
interface=ether3
/routing ospf interface-template
```

```
add bandwidth=1Gbps disabled=no interface=ether3
add bandwidth=1Gbps disabled=no interface=ether4
/routing ospf interface-template
add area=ospf-area-vpls-te disabled=no interfaces=lo
networks=192.170.0.3/32 \
    passive
add area=ospf-area-vpls-te disabled=no interfaces=\
    ether1,ether2,ether3,ether4,ether5 networks=\

80.0.0.0/30,90.0.0.0/30,30.0.0.0/30,40.0.0.0/30,100.0.0.
0/30 type=ptp
/system identity
set name=P2
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
/tool sniffer
set filter-interface=ether3,ether4
```

```
add area=ospf-area-vpls-te disabled=no
interfaces=lo networks=192.170.0.4/32 \
    passive
add area=ospf-area-vpls-te disabled=no
interfaces=ether1,ether2,ether3 \

networks=60.0.0.0/30,50.0.0.0/30,80.0.0.0
/30 type=ptp
/system identity
set name=P3
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
/tool sniffer
set file-name=cap-vpls-P3 filter-
interface=ether1,ether2
```

P4

```
# model = CCR2004-16G-2S+
/port
set 0 name=serial0
/routing ospf instance
add disabled=no name=ospf-vpls-te router-
id=192.170.0.5
/routing ospf area
add disabled=no instance=ospf-vpls-te name=ospf-
area-vpls-te
/ip address
add address=192.170.0.5 interface=lo
network=192.170.0.5
add address=70.0.0.1/30 interface=ether1
network=70.0.0.0
add address=90.0.0.2/30 interface=ether3
network=90.0.0.0
add address=60.0.0.2/30 interface=ether2
network=60.0.0.0
add address=110.0.0.1/30 interface=ether4
network=110.0.0.0
/mpls ldp
add disabled=no lsr-id=192.170.0.5 transport-
addresses=192.170.0.5
/mpls ldp interface
add disabled=no interface=ether1
add disabled=no interface=ether2
add disabled=no interface=ether3
add disabled=no interface=ether4
/mpls settings
set allow-fast-path=no dynamic-label-range=7000-8999
/mpls traffic-eng interface
add bandwidth=1Gbps disabled=no interface=ether1
add bandwidth=1Gbps disabled=no interface=ether2
add bandwidth=1Gbps disabled=no interface=ether3
/routing ospf interface-template
add area=ospf-area-vpls-te disabled=no interfaces=lo
networks=192.170.0.5/32 \
    passive
add area=ospf-area-vpls-te disabled=no
interfaces=ether1,ether2,ether3,ether4 \
```

```
networks=70.0.0.0/30,60.0.0.0/30,90.0.0.0/30,110.0.0.0/
30 type=ptp
/system identity
set name=P4
/system routerboard settings
set enter-setup-on=delete-key
/tool romon
set enabled=yes
/tool sniffer
set file-name=Cap-vpls-P4 filter-interface=ether1,ether2
```

Anexo C: Script de Pyhton para Leer y Procesar Archivos JSON y poder Generar Graficas

```
import json
import pandas as pd
import matplotlib.pyplot as plt
import base64
from io import BytesIO

# ==== CONFIGURACIÓN ====
INPUT_FILES = [
    "test_P1_eth2.json",
    # Agrega más archivos aquí, por ejemplo:
    # "test_160Mbps.json",
    # "test_200Mbps.json",
]
OUTPUT_HTML = "reporte_iperf3_comparativo.html"

# ==== FUNCIONES AUXILIARES ====
def fig_to_base64(fig):
    """Convierte una figura matplotlib a base64 para insertar en HTML."""
    buf = BytesIO()
    fig.savefig(buf, format="png", bbox_inches="tight")
    buf.seek(0)
    return base64.b64encode(buf.read()).decode("utf-8")

def procesar_json(file_path):
    """Procesa un archivo JSON de iPerf3 y devuelve DataFrame + métricas globales."""
    with open(file_path, "r") as f:
        data = json.load(f)

    # Intervalos
    rows = []
    for i, interval in enumerate(data["intervals"], start=1):
        s = interval["sum"]
        rows.append({
            "interval": i,
            "seconds": s["seconds"],
            "throughput_bps": s["bits_per_second"],
            "packets": s.get("packets", 0),
            "bytes": s["bytes"],
        })
    df = pd.DataFrame(rows)
```

```
    # Métricas globales
    end_sum = data["end"]["sum"]
    end_stream = data["end"]["streams"][0]["udp"]

    stats = {
        "Archivo": file_path,
        "Throughput promedio (Mbps)": end_sum["bits_per_second"] / 1e6,
        "Throughput máx (Mbps)": df["throughput_bps"].max() / 1e6,
        "Throughput mín (Mbps)": df["throughput_bps"].min() / 1e6,
        "Jitter promedio (ms)": end_sum.get("jitter_ms", None),
        "Paquetes enviados": end_stream["packets"],
        "Paquetes perdidos": end_stream["lost_packets"],
        "Ratio de pérdida (%)": end_stream["lost_percent"],
        "Duración (s)": end_stream["seconds"],
        "Tamaño de bloque (bytes)": data["start"]["test_start"]["blksize"],
    }

    return df, stats

# ==== PROCESAMIENTO DE TODOS LOS ARCHIVOS ====
dfs = {}
stats_list = []

for file in INPUT_FILES:
    df, stats = procesar_json(file)
    dfs[file] = df
    stats_list.append(stats)

stats_df = pd.DataFrame(stats_list)

# ==== GRÁFICOS ====
figs_base64 = {}

# Curva comparativa de throughput
fig1, ax1 = plt.subplots(figsize=(9,5))
for file, df in dfs.items():
    ax1.plot(df["interval"], df["throughput_bps"]/1e6, marker="o", linestyle="-", label=file)
ax1.set_title("Comparación de Throughput vs Tiempo")
ax1.set_xlabel("Intervalo (s)")
ax1.set_ylabel("Throughput (Mbps)")
ax1.grid(True)
ax1.legend()
figs_base64["throughput"] = fig_to_base64(fig1)
plt.close(fig1)

# Histograma comparativo de throughput
fig2, ax2 = plt.subplots(figsize=(8,5))
for file, df in dfs.items():
    ax2.hist(df["throughput_bps"]/1e6, bins=15, alpha=0.5, label=file)
ax2.set_title("Distribución de Throughput (Histograma)")
ax2.set_xlabel("Throughput (Mbps)")
ax2.set_ylabel("Frecuencia")
ax2.legend()
figs_base64["histogram"] = fig_to_base64(fig2)
plt.close(fig2)
```

```
# Gráfico de Jitter (solo valores globales disponibles)
fig3, ax3 = plt.subplots(figsize=(7,4))
ax3.bar(stats_df["Archivo"], stats_df["Jitter promedio (ms)"], color="orange")
ax3.set_title("Jitter promedio por prueba")
ax3.set_ylabel("Jitter (ms)")
ax3.set_xticklabels(stats_df["Archivo"], rotation=30, ha="right")
figs_base64["jitter"] = fig_to_base64(fig3)
plt.close(fig3)

# Gráfico de pérdida de paquetes (% global)
fig4, ax4 = plt.subplots(figsize=(7,4))
ax4.bar(stats_df["Archivo"], stats_df["Ratio de pérdida (%)"], color="red")
ax4.set_title("Pérdida de paquetes por prueba")
ax4.set_ylabel("Pérdida (%)")
ax4.set_xticklabels(stats_df["Archivo"], rotation=30, ha="right")
figs_base64["loss"] = fig_to_base64(fig4)
plt.close(fig4)

# ==== GENERAR REPORTE HTML ====
html_content = f"""
<html>
<head>
   <meta charset="UTF-8">
   <title>Reporte iPerf3 Comparativo</title>
   <style>
      body {{ font-family: Arial, sans-serif; margin: 20px; }}
      table {{ border-collapse: collapse; width: 95%; margin-bottom: 30px; }}
      th, td {{ border: 1px solid #ccc; padding: 8px; text-align: center; }}
      th {{ background-color: #f2f2f2; }}
      h2 {{ color: #2c3e50; }}
      img {{ max-width: 900px; display: block; margin-bottom: 25px; }}
   </style>
</head>
<body>
   <h1>Reporte Comparativo de Rendimiento - iPerf3</h1>

   <h2>Métricas Globales</h2>
   {stats_df.to_html(index=False, border=0)}

   <h2>Gráficos</h2>
   <h3>Throughput vs Tiempo (Comparativo)</h3>
   <img src="{figs_base64["throughput"]}">
   <h3>Histograma de Throughput</h3>
   <img src="{figs_base64["histogram"]}">
   <h3>Jitter promedio por prueba</h3>
   <img src="{figs_base64["jitter"]}">
   <h3>Pérdida de paquetes por prueba</h3>
   <img src="{figs_base64["loss"]}">
</body>
</html>
"""
with open(OUTPUT_HTML, "w", encoding="utf-8") as f:
   f.write(html_content)
```

```
print(f" Reporte comparativo generado: {OUTPUT_HTML}")
```

Anexo D: Especificaciones técnicas del router Mikrotik ccr2004-16g-2s+

Specifications

Product code	CCR2004-16G-2S+
CPU	AL32400 1.7 GHz
CPU architecture	ARM 64bit
CPU core count	4
Size of RAM	4 GB
RAM type	DDR4
Storage	128 MB, NAND
Number of 1G Ethernet ports	16
Number of 10G SFP+ ports	2
Operating system	RouterOS v7 only
Switch chip model	88E6191X, 88E619X
Dimensions	443 x 210 x 44 mm
Operating temperature	-20°C to +60°C

Powering

Number of AC inputs	2
AC input range	100-240 V
Max power consumption (without attachments)	35 W
Max power consumption	48 W

Certification & Approvals

Certification	CE, FCC, IC

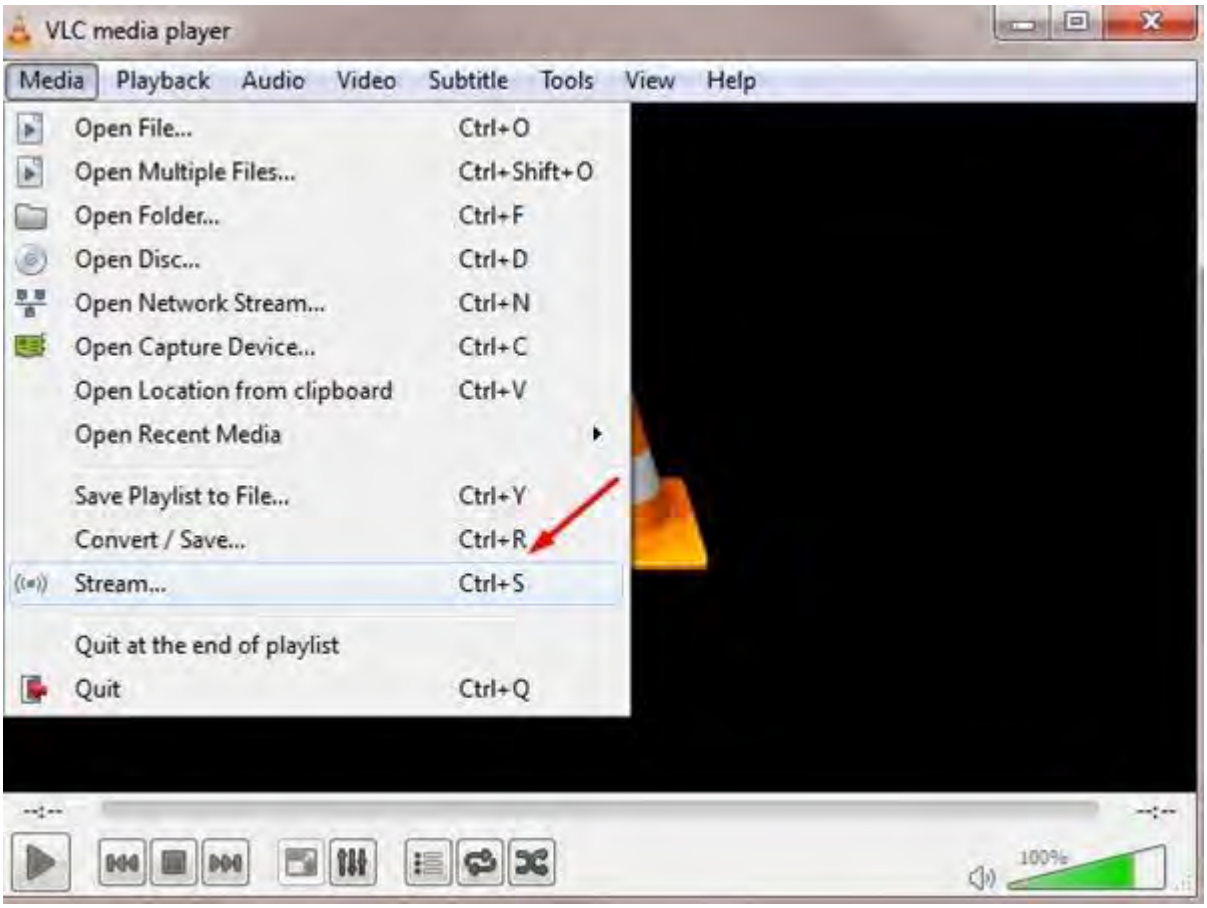
Included parts

2 Power cords

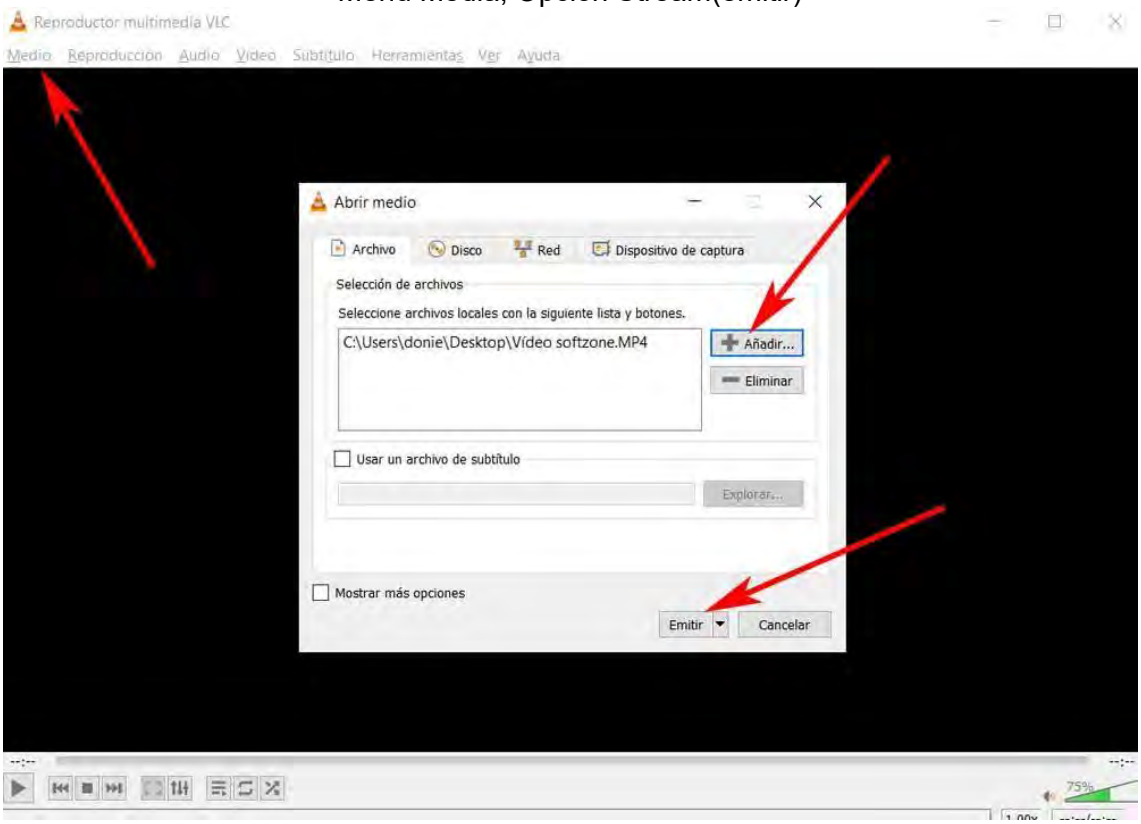
Rackmount bracket white

Fastening set

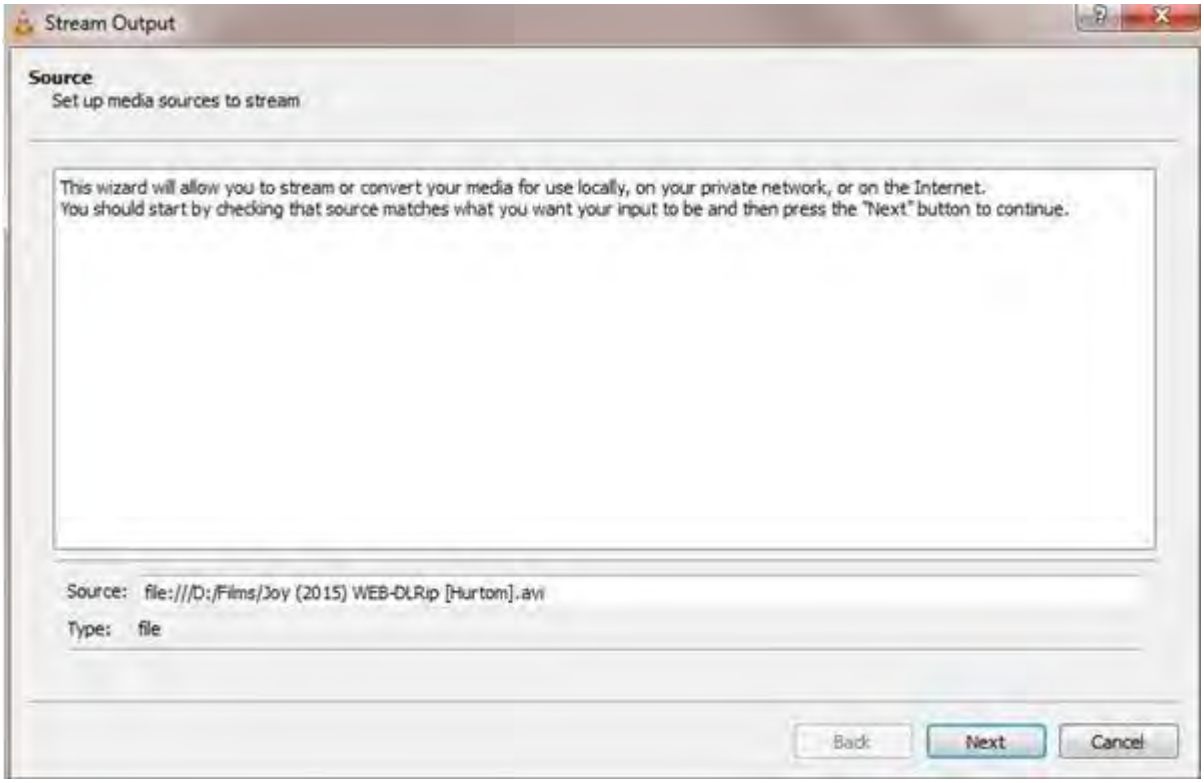
Anexo E: Configuración de VLC Media Player



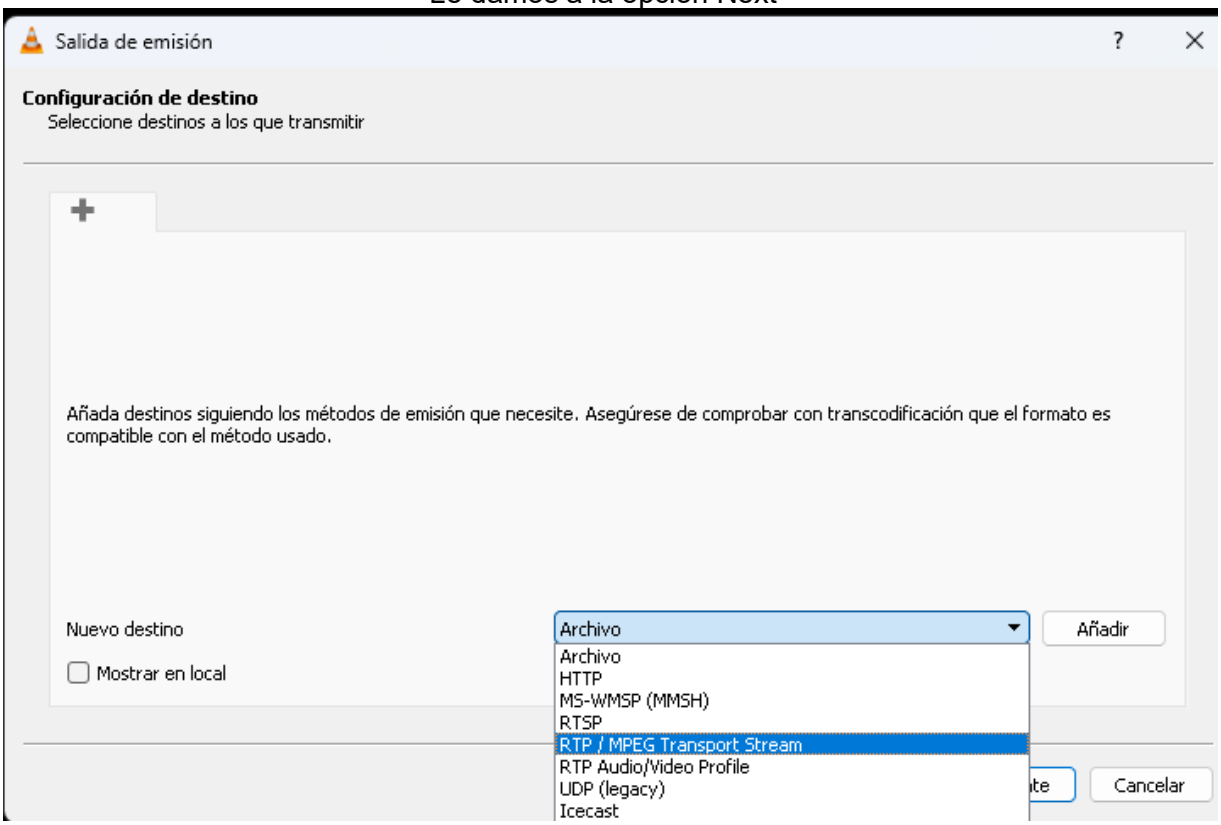
Menu Media, Opcion Stream(emitir)



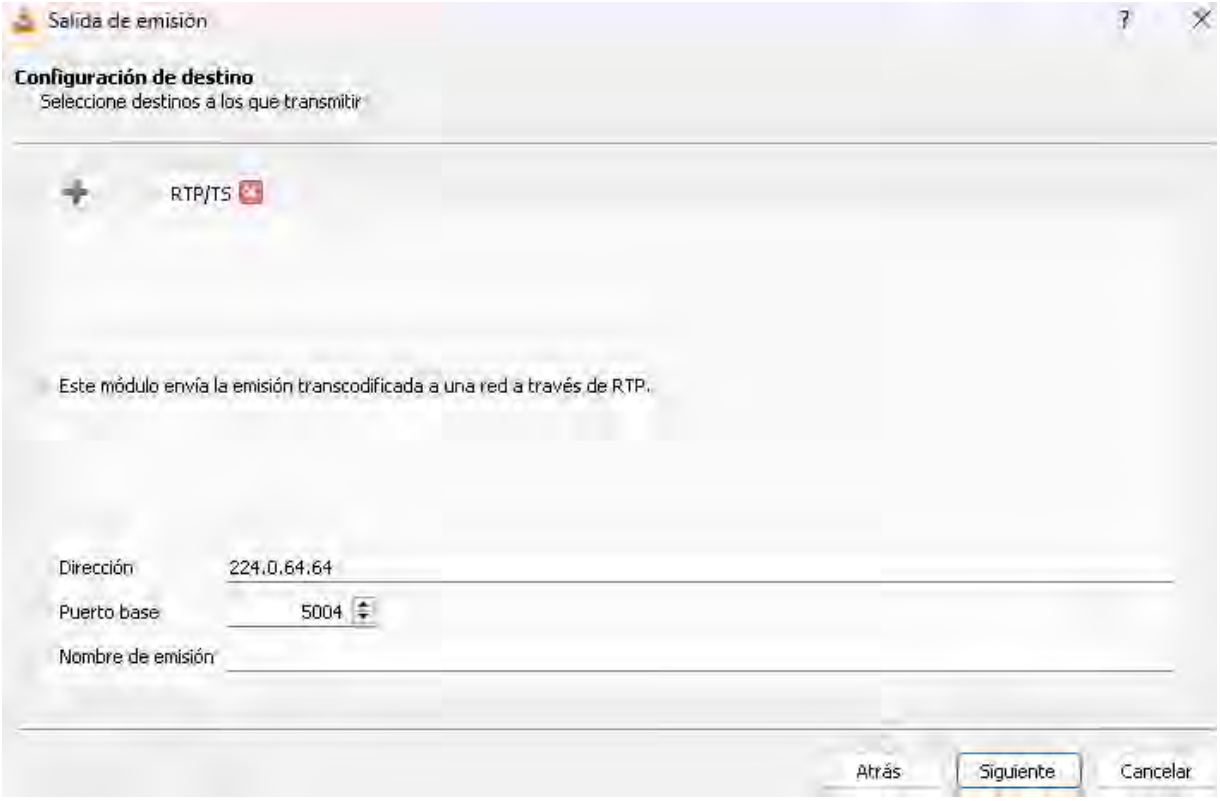
Seleccionamos el archivo-luego emitir



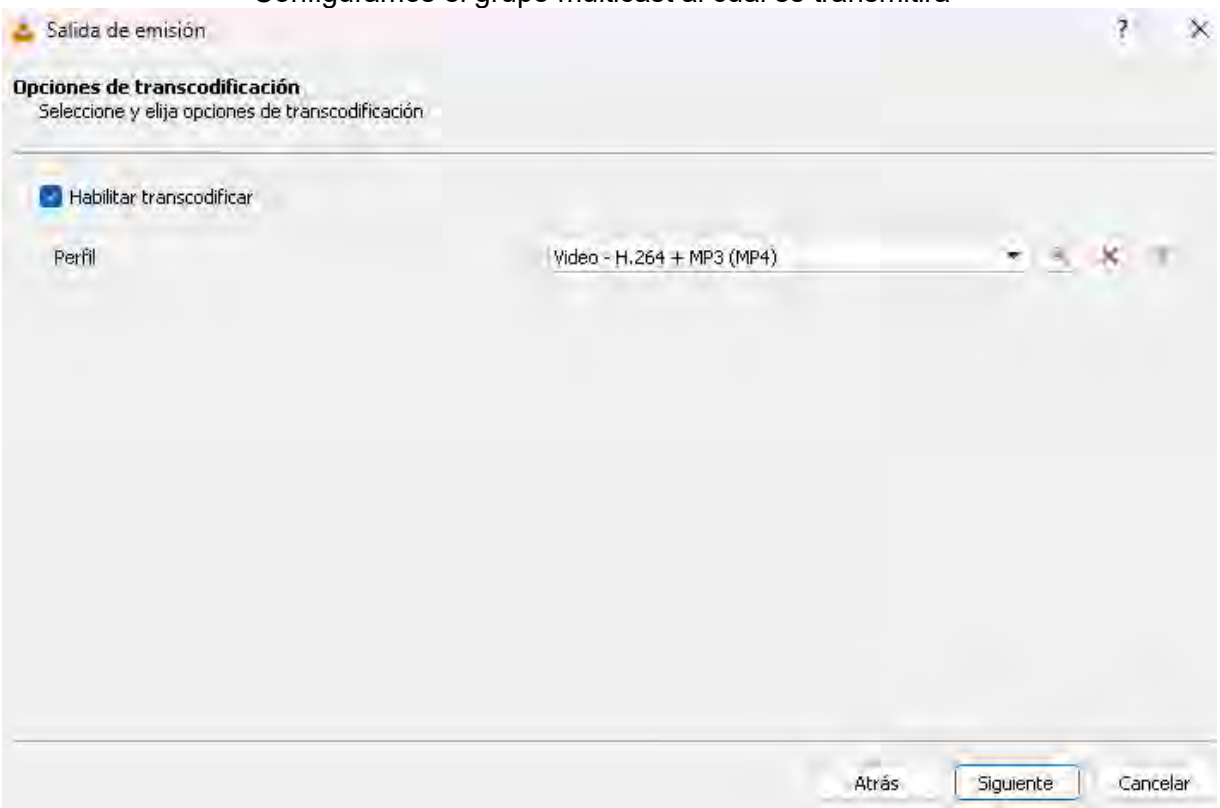
Le damos a la opcion Next



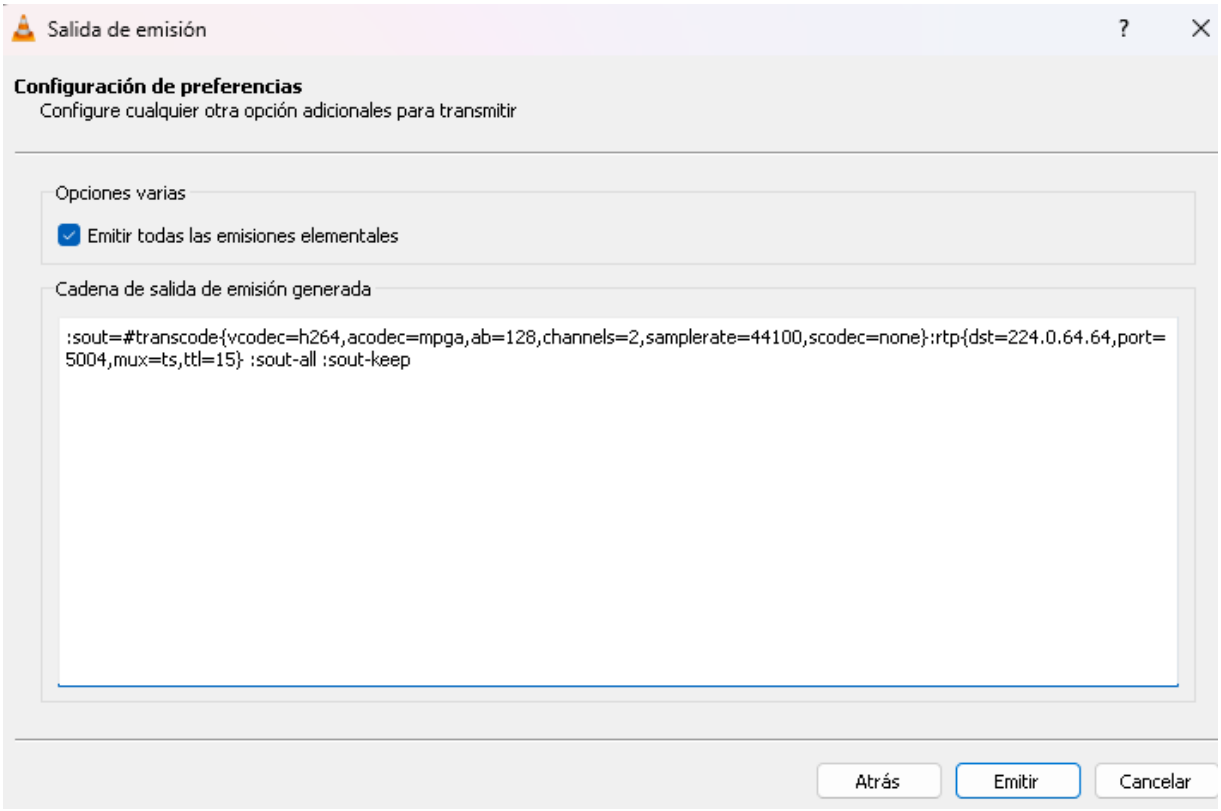
Selección el metodo de transcodificacion, luego seleccionamos Añadir



Configuramos el grupo multicast al cual se transmitira

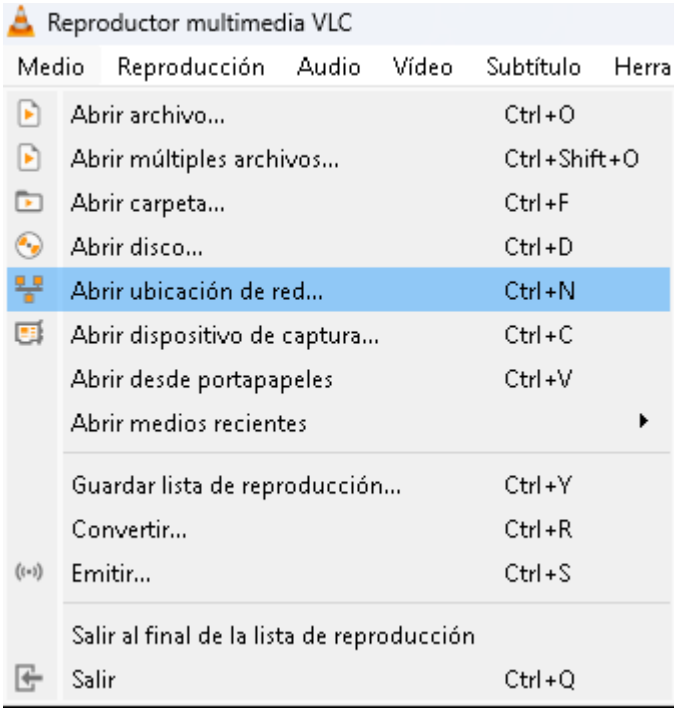


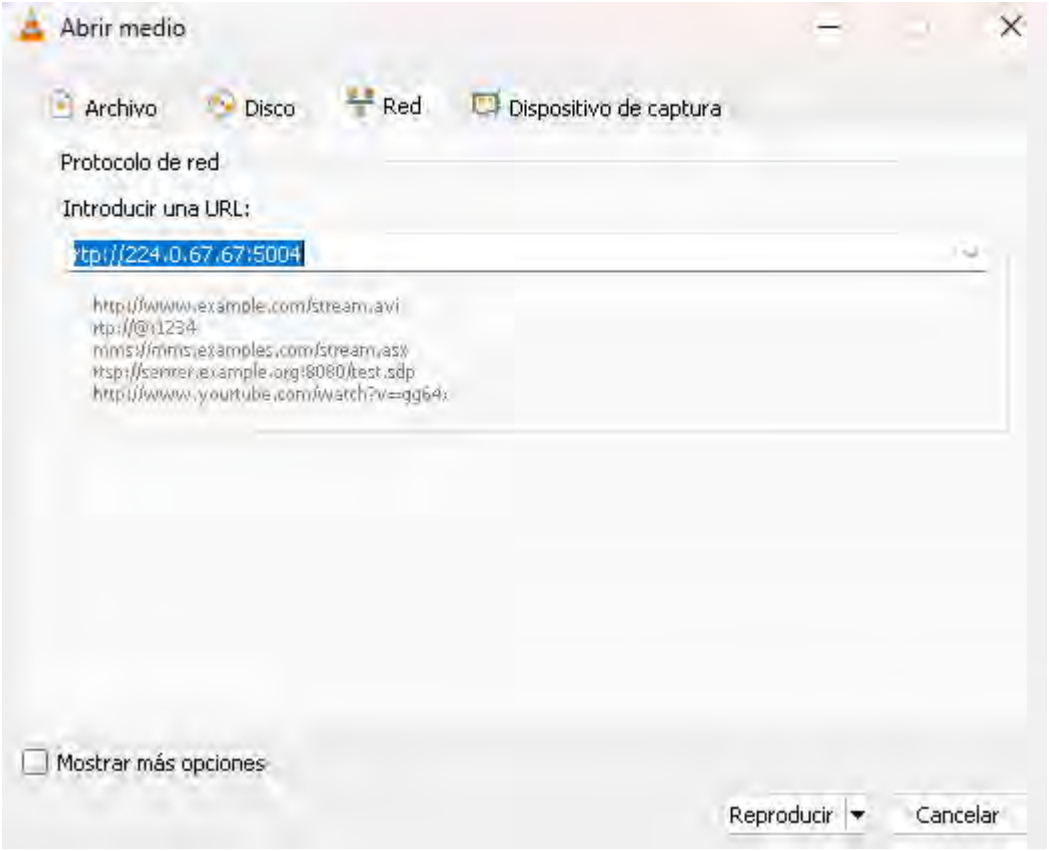
Seleccionamos la opcion de transcodificacion



Resumen de los parametros configuramos, añdimos el campo ttl=15

Del lado del cliente



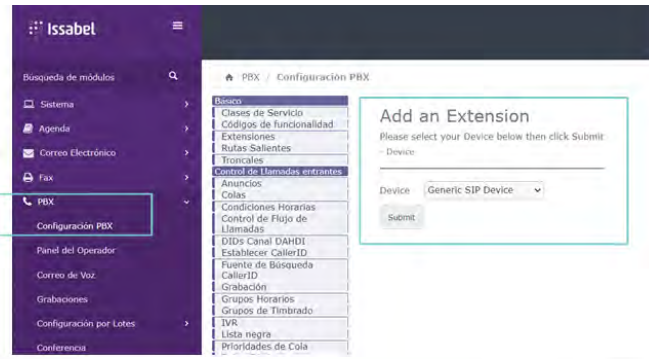


Configuramos el grupo multicast al cual pertenecera el cliente

Anexo F: Configura de Telefonía IP

Configuración de Extensiones en el servidor PBX-Issabel

- Para configurar una extensión debemos ingresar a PBX ->Configuración PBX -> Extensiones -> add an Extension -> Seleccionar Generic SIP Device y Submit.

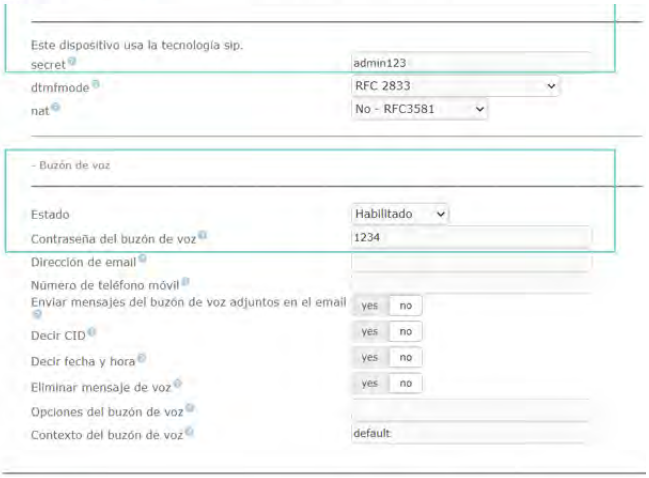


- Los siguientes parámetros deben ser configurados:
  - **Extensión del usuario:** 2001.
  - **Nombre para mostrar:** Gerencia.
  - **Alias SIP:** 2001.

- **Contraseña secreta que usarán los teléfonos IP:** admin123.

  Buzón de Voz: habilitado.

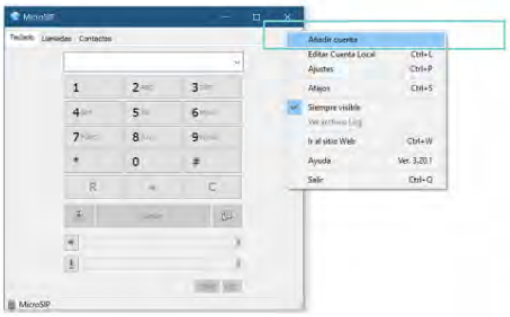
  Contraseña del Buzón de Voz: 1234.

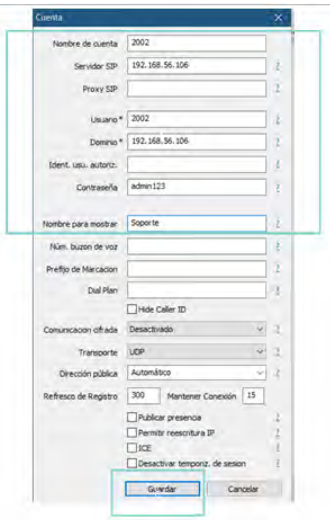


- Ahora debemos seleccionar Enviar y después Aplicar los Cambios. Y nuestra primera extensión está Creada.
- El mismo proceso se debe realizar con las demás extensiones.

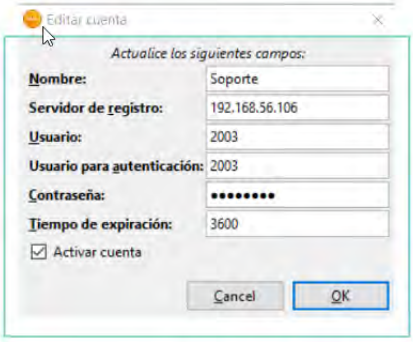
Configuración de los clientes Softphone

- **Paso 1:** Abrir aplicación de Softphone, seleccionar el botón a la derecha, luego añadir cuenta, configurar los parámetros y Guardar.

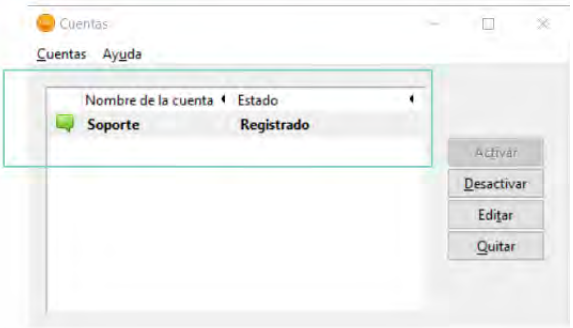




- **Paso 2:** Configurar los parámetros de la cuenta SIP, luego elegir Ok.



- **Paso 3:** Aparece la extensión Registrado.



- **Paso 4:** Para llamar debe hacer como aparece en la imagen.