UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA INGENIERÍA

CARRERA DE TELEMÁTICA

Trabajo de Integración Curricular previa la obtención del Grado Académico de Ingeniero en Telemática.

PROYECTO DE INVESTIGACIÓN:

ANÁLISIS DEL DESEMPEÑO DE REDES DE ÁREA AMPLIA DEFINIDA POR SOFTWARE FRENTE A REDES DE CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO

AUTOR:

MARCO ISAIAS CHIMBO FOGACHO

DIRECTOR DE PROYECTO DE INVESTIGACIÓN:

ING. EMILIO RODRIGO ZHUMA MERA, MSC.

QUEVEDO – LOS RÍOS – ECUADOR

2024

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

Yo, **Marco Isaias Chimbo Fogacho,** declaro que la investigación aquí descrita es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Técnica Estatal de Quevedo, puede hacer uso de los derechos correspondientes a este documento, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Marco Chimbo

Marco Isaias Chimbo Fogacho

C.I: 0201999315

CERTIFICACIÓN DE CULMINACIÓN DEL PROYECTO DE INVESTIGACIÓN

El suscrito, **Ing. Emilio Rodrigo Zhuma Mera, MSc.** Docente de la Universidad Técnica Estatal de Quevedo, certifica que el estudiante **Marco Isaias Chimbo Fogacho**, realizó el Proyecto de Investigación de grado titulado **"ANÁLISIS DEL DESEMPEÑO DE REDES DE ÁREA AMPLIA DEFINIDA POR SOFTWARE FRENTE A REDES DE CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO"**, previo a la obtención del título de Ingeniería Telemática, bajo mi dirección, habiendo cumplido con las disposiciones reglamentarias establecidas para el efecto.

Ing. Emilio Rodrigo Zhuma Mera, MSc.
DIRECTOR DEL PROYECTO DE INVESTIGACIÓN

CERTIFICADO DEL REPORTE DE LA HERRAMIENTA DE PREVENCIÓN DE COINCIDENCIA Y/O PLAGIO ACADÉMICO

El suscrito, **Ing. Emilio Rodrigo Zhuma Mera, MSc.** mediante el presente cumplo en presentar a usted, el informe de proyecto de Investigación titulado **"ANÁLISIS DEL DESEMPEÑO DE REDES DE ÁREA AMPLIA DEFINIDA POR SOFTWARE FRENTE A REDES DE CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO"** Presentado por el estudiante, **Marco Isaias Chimbo Fogacho**, egresado de la Carrera de Ingeniería en Telemática, que fue revisado bajo mi dirección según resolución del Consejo Directivo de la Facultad de Ciencias de la Ingeniería, que se ha desarrollado de acuerdo al Reglamento de la Unidad de Integración Curricular de la Universidad Técnica Estatal de Quevedo y cumple con el requerimiento de análisis de URKUND el cual avala los niveles de originalidad en un 95% y similitud 5%, del trabajo investigativo. Valido este documento para que el estudiante siga con los trámites pertinentes, de acuerdo como lo estable el Reglamento.


CERTIFICADO DE ANÁLISIS
magister

CHIMBO_PROY_INVESTIGACION

5%
Textos sospechosos

5% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
0% Idiomas no reconocidos

Nombre del documento: CHIMBO_PROY_INVESTIGACION.pdf
ID del documento: dd4c9f3e69ee1ad4fe3305310e9281e62a1d5214
Tamaño del documento original: 854,64 kB
Autores: []

Depositante: EMILIO RODRIGO ZHUMA MERA
Fecha de depósito: 23/9/2024
Tipo de carga: interface
fecha de fin de análisis: 23/9/2024

Número de palabras: 8368
Número de caracteres: 55.608

Ing. Emilio Rodrigo Zhuma Mera, MSc.
DIRECTOR DEL PROYECTO DE INVESTIGACIÓN

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA INGENIERÍA

CARRERA DE TELEMÁTICA

PROYECTO DE INVESTIGACION

TÍTULO:

"ANÁLISIS DEL DESEMPEÑO DE REDES DE ÁREA AMPLIA DEFINIDA POR SOFTWARE FRENTE A REDES DE CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO"

Presentado al Consejo Directivo de Facultad como requisito previo a la obtención del título de Ingeniero en Telemática.

Aprobado por:

PRESIDENTE DEL TRIBUNAL

Ing. Eduardo Amable Samaniego Mena, MSc.

MIEMBRO DEL TRIBUNAL

Ing. Janeth Ines Mora Secaira, MSc.

MIEMBRO DEL TRIBUNAL

Ing. Jose Luis Tubay Vergara, MSc.

QUEVEDO – LOS RIOS – ECUADOR

2024

AGRADECIMIENTO

Quiero expresar mi gratitud y agradecimiento a Dios por todos los buenos y malos momentos en donde me he fortalecido como estudiante, persona, para superar todos los obstáculos que se han presentado.

A mi director de proyecto, Ing. Emilio Rodrigo Zhuma Mera por su paciencia, sabiduría, valioso tiempo, sugerencias, comentarios y compromiso han sido invaluables durante todo el proyecto.

Agradezco a mis padres, hermanos, por ser un pilar fundamental a lo largo de la vida en donde me han apoyado y motivado en mi formación profesional.

A la Secretaria de Educación Superior, Ciencia, Tecnología e Innovación del Ecuador(SENECYT) por el apoyo recibido para mi desarrollo académico y profesional.

Además, a la prestigiosa Universidad Técnica Estatal de Quevedo y docentes por el aporte de sus experiencias, desafíos, paciencia, sabidurías y conocimientos que durante el transcurso de mi formación me ha permitido comprender el mundo de la ingeniería Telemática.

Finalmente, quiero agradecer a todos los compañeros del aula con quienes se compartió muchas experiencias y momentos agradables.

DEDICATORIA

A Dios fuente de inspiración y fortaleza para durante todo el proceso de mi formación académica.

A mis padres y mis hermanos debido que esto es el fruto de todo el esfuerzo y apoyo que me han brindado durante el transcurso de mi formación profesional.

A los docentes y compañeros de aula que me han impartido sus experiencias y conocimientos.

RESUMEN EJECUTIVO Y PALABRAS CLAVES

El presente proyecto de investigación evalúa el desempeño de las redes de área amplia definidas por software (SD-WAN) frente a las redes de conmutación de etiquetas multiprotocolo (MPLS), en respuesta a la creciente demanda de conectividad en las infraestructuras de red. El objetivo principal es comparar ambas tecnologías en términos de capacidad de gestión de tráfico, empleando métricas de latencia, jitter, ancho de banda, y pérdida de paquetes, entre otras. La metodología utilizada fue revisión bibliográfica para fundamentar el análisis, y el desarrollo de escenarios emulados. Los datos recolectados se almacenaron en una base de datos permitiendo realizar un análisis en tiempo real. Los resultados evidencian que SD-WAN, gracias a su control centralizado y adaptabilidad al tráfico, mostró un mejor rendimiento en términos de latencia y jitter. Por otro lado, MPLS se destacó por su estabilidad en la gestión de tráfico, aunque con mayor complejidad. Este estudio ofrece un análisis comparativo que resulta útil para investigadores y profesionales interesados en optimizar redes empresariales.

Palabras claves: redes, análisis, MPLS, SD-WAN, métricas, GNS3.

ABSTRACT AND KEY WORDS

This research project evaluates the performance of software-defined wide area networks (SD-WAN) versus multiprotocol label switching (MPLS) networks, in response to the growing demand for connectivity in network infrastructures. The main objective is to compare both technologies in terms of traffic management capacity, using latency, jitter, bandwidth, and packet loss metrics, among others. The methodology used was a bibliographic review to base the analysis, and the development of emulated scenarios. The collected data was stored in a database allowing real-time analysis to be carried out. The results show that SD-WAN, thanks to its centralized control and adaptability to traffic, showed better performance in terms of latency and jitter. On the other hand, MPLS stood out for its stability in traffic management, although with greater complexity. This study provides a comparative analysis that is useful for researchers and practitioners interested in optimizing enterprise networks.

Keywords: networks, analysis, MPLS, SD-WAN, metrics, GNS3.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CÓDIGO DUBLIN

Título:	Análisis del desempeño de redes de área amplia definida por software frente a redes de conmutación de etiquetas multiprotocolo
Autor:	Chimbo Fogacho Marco Isaias
Palabras claves:	SD-WAN,MPLS,Métricas
Fecha de publicación:	Noviembre del 2024
Director del proyecto:	Ing. Zhuma Mera Emilio Rodrigo
Editorial:	Quevedo – UTEQ "La María", 2024
Resumen:	El presente proyecto de investigación evalúa el desempeño de las redes de área amplia definidas por software (SD-WAN) frente a las redes de conmutación de etiquetas multiprotocolo (MPLS), en respuesta a la creciente demanda de conectividad en las infraestructuras de red. El objetivo principal es comparar ambas tecnologías en términos de capacidad de gestión de tráfico, empleando métricas de latencia, jitter, ancho de banda, y pérdida de paquetes, entre otras. La metodología utilizada fue revisión bibliográfica para fundamentar el análisis, y el desarrollo de escenarios emulados. Los datos recolectados se almacenaron en una base de datos permitiendo realizar un análisis en tiempo real. Este estudio ofrece un análisis comparativo que resulta útil para investigadores y profesionales interesados en optimizar redes empresariales.
Abstract:	This research project evaluates the performance of software-defined wide area networks (SD-WAN) versus multiprotocol label switching (MPLS) networks, in response to the growing demand for connectivity in network infrastructures. The main objective is to compare both technologies in terms of traffic management capacity, using latency, jitter, bandwidth, and packet loss metrics, among others. The methodology used was a bibliographic review to base the analysis, and the development of emulated scenarios. The collected data was stored in a database allowing real-time analysis to be carried out. This study provides a comparative analysis that is useful for researchers and professionals interested in optimizing business networks.
Descripción:	87 hojas: dimensiones, 29 x 21 cm + CD-ROM 6162
URI:	

INTRODUCCIÓN

Las tecnologías de la información evolucionan constantemente debido a las crecientes demandas de los usuarios, organizaciones, esta rápida evolución ha generado la aparición de nuevos estándares y arquitecturas dentro las redes LAN, MAN, WAN, todo ello con la finalidad de estar siempre conectados y acceder a nuevos servicios. Este avance está estrechamente relacionado con la revolución industrial 4.0 impulsado por la conectividad a IoT (Internet of Things) y el despliegue de redes móviles e inalámbricas de nueva generación (Wifi 6E, 5G, 6G) [5].

La tecnología MPLS(Multiprotocol Label Switching) se ha destacado por proporcionar mayor calidad de servicio, pero su costo es elevado debido a los equipos especializados. Asimismo, su capacidad para responder rápidamente al aumento repentino de la demanda del ancho de banda también requiere considerable tiempo y esfuerzo [2].

Así, como MPLS reemplazo a tecnologías como Frame Relay y ATM, simplificando la traducción IP, el ancho de banda y la calidad de servicio(QoS), en el año 2012 surge SD-WAN surge SD-WAN para revolucionar las redes convencionales y llevar a proveedores y empresas a un entorno tecnología moderno [3].

SD-WAN se adapta dinámicamente a los cambios sin intervención, proporcionando control centralizado del tráfico, rendimiento óptimo para aplicaciones críticas y evitando interrupciones en el tráfico. además, ofrece ventajas sobre las redes convencionales, como una capa de seguridad de con túneles cifrado de extremo a extremo y redundancia de transporte [4] [5].

En la actualidad dentro del Ecuador, las empresas están incorporando SD-WAN dentro de su organización, para un mayor aprovechamiento de la red digital y de los nuevos servicios en surgimiento [4].

El presente proyecto contiene capítulos estructurados que analiza el desempeño de redes SD-WAN frente a redes MPLS a través de escenarios emulados utilizando diferentes métricas de evaluación.

CAPÍTULO I

CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

1.1. Problema de investigación

1.1.1. Planteamiento del problema

Durante muchos años, el enfoque principal para construir la infraestructura de red utilizada por las empresas fueron las redes de área amplia(WAN) construidas utilizando cableado dedicado y conmutación de etiquetas multiprotocolo(MPLS). Si bien este enfoque sigue siendo popular [5]. A medida que la demanda de aplicaciones basadas en la nube, IOT y los requisitos de ancho de banda siguen creciendo, algunas empresas y proveedores de servicios comienzan a desplegar servicios de red de área amplia definida por software. La pandemia del COVID-19, intensifico muchas dificultades a nivel mundial al forzar aplicaciones del área de la educación, salud y sectores estratégicos a través de aplicaciones basadas en cloud computing [5].

En la actualidad las organizaciones deben adaptarse al cambio y encontrar formas de mantenerse a la vanguardia de la tecnología para brindar un servicio de alta calidad en entornos empresariales [4]. La elección entre SD-WAN y MPLS para la gestión de redes plantea desafíos significativos en términos de desempeño [3].

La necesidad de optimizar el ancho de banda, reducir la latencia, garantizar la resiliencia frente a fallos, gestionar QoS (calidad de servicio). Además, la carencia de una comprensión integral y de soluciones efectivas en estas áreas puede afectar la eficiencia operativa y la experiencia del usuario.

Esta problemática destaca la importancia de una investigación detallada para abordar específicamente las áreas clave de rendimiento en las tecnologías SD-WAN y MPLS, ofreciendo así una guía emulada para la implementación de redes empresariales.

A través de la investigación detallada de características, análisis de casos previos, comprobación del rendimiento, análisis de eficiencia y la verificación de la viabilidad de un enfoque híbrido, a través de entornos emulados.

Diagnostico

Durante la última década, MPLS ha sido la tecnología predominante debido a la capacidad de proporcionar mayor calidad de servicio (QoS). Sin embargo, enfrenta desafíos como los altos costos de implementación, respuesta lenta al aumento en la demanda del ancho de banda y la complejidad en la gestión. La pandemia del COVID-19, acentuó estas

limitaciones al incrementar la dependencia de aplicaciones basadas en la nube para mantener sistemas críticos.

El desarrollo de SD-WAN tuvo un impedimento que lo afecto a corto plazo, a pesar de ello, SD-WAN creció positivamente debido a la implementación de redes 5G en donde requiere infraestructura de tipo SD-WAN para lograr una adecuada infraestructura moderna capaz de soportar un gran flujo masivos de datos en tiempo real [5]. Ante todos estos problemas se están desarrollando soluciones innovadoras para las redes.

Pronostico

En un artículo denominado "SD-WAN, Una oportunidad para la transformación digital" menciona que entre el 30% y 50% del tráfico de datos de las grandes empresas se ha migrado a la nube [6].

Para el año 2030, el 80% del despliegue de aplicaciones o servicios serán en la nube. En el cual el 89% de las empresas considera los datos abiertos como un reto de futuro, y en donde el ancho de banda crece a una media del 20% anualmente, las infraestructuras de nube están reemplazando al centro de datos tradicional [6].

La idea de implementar redes centralizadas, de fácil gestión y manejo del tráfico a través de política se ha convertido indispensable durante los últimos años debido a la automatización que es un elemento clave en el futuro de las redes digital, incluso NetDevOps (desarrollo y operaciones de red) posee en su núcleo la automatización a través de APIs [5].

En el análisis del desempeño de red de área amplia definida por software y la red de conmutación de etiquetas multiprotocolo se pronostica tener una respuesta favorable en la evaluación de diferentes métricas como ancho de banda, la latencia, garantizar la resiliencia frente a fallos, gestionar QoS(calidad de servicio) en las dos redes; pero se prevé un mejor desempeño para el caso de las redes SD-WAN.

1.1.2. Formulación del problema

¿De qué manera los escenarios emulados permitirán determinar el impacto desempeño de las redes de área amplia definidas por software (SD-WAN) en comparación con las redes de conmutación de etiquetas multiprotocolo (MPLS)?

1.1.3. Sistematización del problema

¿Qué herramientas son apropiadas para efectuar la comparación entre redes de área amplia definida por software y redes de conmutación de etiquetas multiprotocolo?

¿Cómo se puede verificar el desempeño de las redes SD-WAN y MPLS utilizando métricas de evaluación?

¿Cuáles son los beneficios percibidos de la emulación para las redes SD-WAN y MPLS?

1.2. Objetivos

1.2.1. Objetivo General

Analizar las redes de área amplia definida por software (SD-WAN) frente a las redes de conmutación de etiquetas multiprotocolo (MPLS) a través de escenarios emulados para una visión integral de desempeño.

1.2.2. Objetivos Específicos

- Identificar herramientas, controladores, protocolos para redes de área amplia definida por software y redes de conmutación de etiquetas multiprotocolo.
- Diseñar escenarios para la evaluación del rendimiento en la gestión del tráfico de las redes de área amplia definida por software y redes de conmutación de etiquetas multiprotocolo.
- Evaluar los resultados obtenidos de los escenarios de las redes para la verificación de capacidad en la gestión del tráfico.

1.3. Justificación

El presente proyecto se justifica debido a la necesidad de examinar y comparar el desempeño de las dos tecnologías SD-WAN y MPLS. Para proporcionar una comparacion en términos de implementación, costos, seguridad, facilidad de implementación y gestión, ofreciendo una guía práctica para una elección adecuada a la necesidad de implementación.

Cabe mencionar que con el aumento de las demandas de conectividad y la necesidad de eficiencia operativa es crucial comprender las ventajas y desventajas, asi como las limitaciones de cada tecnología. SD-WAN ha emergido como una solución de ofrecer flexibilidad, reducción de costos a diferencia de MPLS es conocido por la estabilidad y eficiencia en la conmutación de tráfico.

En el año 2016 el 1% de las organizaciones emplearon soluciones de SD-WAN, Garther (empresa de consultoría e investigación de TIC) evaluaron un crecimiento del 30% para el año 2019, además, según el informe de IDC (International Data Corporation) las ventas de SD-WAN se aproximó a los 1,4 mil millones de dólares en el año 2017 [7].

En el Ecuador diversas empresas se encuentran implementando redes SD-WAN para maximizar el potencial de la red y los nuevos servicios emergentes. Se puede mencionar como el caso de Claro, CNT, Telconet, Telefónica, Etapa, Punto Net entre otras empresas de telecomunicaciones locales e internacionales, en donde ha empezado migrar su tecnología a la nueva era en telecomunicaciones conocidas como SD-WAN [4].

Este proyecto investigación tiene como finalidad generar un impacto académico mediante el proceso investigativo. Además presentar una solución a los desafíos asociados con las redes MPLS a través del análisis de desempeño de SD-WAN en escenarios emulados utilizando software de emulación.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN

2.1. Marco conceptual

2.1.1. Redes

Las redes en el ámbito de telecomunicaciones se definen como la interconexión entre varios dispositivos a distancia remotas, mediante señales electromagnéticas, cables de cobre, luz óptica o cualquier otro medio de transmisión, por ende permite la comunicación y transmisión de información como video, voz, datos, etc.[9].

2.1.1.1. Clasificación de redes

Red de Área Personal (PAN): Se utiliza para la comunicación entre dispositivos cerca de los usuarios y su cubertura es de pocos metros [10].

Red de Área Local (LAN): Son utilizadas en edificios, empresas, colegios, etc., y posibilitan la interconexión entre varios dispositivos con la finalidad de intercambiar información [9].

Red de Área de Campus (CAN): Se utilizan en un campus universitario o base militar, se conectan a la red LAN a través de un área geográfica limitada [9].

Red de Área Metropolitana (MAN): Es una red de banda ancha que conecta varias redes LAN en una zona geográfica cercana y transmite servicios como voz, video, datos a través de cobre o fibra óptica [10].

Red de Área Amplia (WAN): Son redes que están conformada por varias redes LAN interconecta. Posee un rango de cubertura geográfica extensa ya sea un continente o país [9].

Red de Área de Almacenamiento (SAN): Es una red que permite interconexión de los sistemas de almacenamientos y servidores. Posee una infraestructura de información segura, dedicada y con administración centralizada [9].

2.1.2. Arquitectura de red

En una red de ordenadores la arquitectura se define como la infraestructura, servicios y protocolos que se ejecutan en un mismo entorno y con el objetivo de enviar datos a todos los dispositivos y se fundamenta en el protocolo TCP/IP. Las características que debe poseer una arquitectura de red en la actualidad son [1]:

- Tolerancia a fallos.
- Escalabilidad.
- Calidad del Servicio (QoS).
- Seguridad

2.1.3. Protocolo de red

El protocolo se define como el conjunto de políticas o normas que regulan el intercambio de datos dentro de una arquitectura entre múltiples componentes conocido como emisor y receptor [19]. Tambien se dispone mecanismo de recuperación de información cuando existe pérdidas de datos [1].

2.1.4. Simulación

Es una técnica que recrea la funcionalidad de un programa dentro de otro sistema que no es compatible debido a una tecnología diferente [1].

2.1.5. Emulación

Un emulador es un software que permite crear un escenario donde se recrea el funcionamiento de un dispositivo de manera similar en un entorno físico real y utiliza los recursos disponibles del anfitrión [1].

2.1.6. Software de análisis de red

Es un software que permite identificar, analizar, monitorear, gestionar el rendimiento y la seguridad de la red en tiempo real, localizando la ubicación del problema con el objetivo de garantizar que el rendimiento y el estado de la red no se afecte [20]. Por lo cual deberá cumplir con los requisitos de redes bajo demanda para volúmenes de tráfico en constante crecimiento [18].

2.1.7. Base de datos

Es un sistema digital que almacena, organiza y gestiona información de forma estructurada e interrelacionados permitiendo el acceso, modificación y recuperación de manera eficiente y rápida para la toma de decisiones y automatizar procesos [19].

2.1.8. Lenguaje de programación

Conjunto de instrucciones que permite a los seres humanos comunicarse con las computadoras, tablets, celulares. Existe distintos lenguajes de programación de bajo y alto nivel [19].

2.1.9. Controladores

Un controlador de red es un componente de software o hardware que centraliza la gestión, configuración, monitorización y control de una red [1].

La principal función es coordinar y supervisar las actividades de los dispositivos de red, como los enrutadores, conmutadores y puntos de acceso, para asegurar un rendimiento optimo, una gestión eficiente y la implementación de políticas de red [1].

2.1.10. Modelo de referencia OSI

Este modelo se base en una propuesta formulada por la Organización Internacional de Normalización (ISO) con el objetivo de estandarizar a nivel mundial debido a la aceptación de la propuesta de modelos de capas [1].

El modelo se compone de sietes capas, cada una de ellas contiene protocolos que funcionan en conjunto para transportar paquetes de datos. A continuación se detalla las capas:

Física: Hardware que se ocupa de la transferencia de bits a través de un canal de comunicación, el cual puede ser alámbrico e inalámbrico.

Enlace de Datos: Transferencia de datos entre nodos adyacentes, detección y corrección de errores.

Red: Se encarga de las funciones de la subredes y direccionamiento a través de enrutadores.

Transporte: Segmentación de las tramas de datos para la transferencia de extremo a extremo, control de errores y flujo.

Sesión: Gestión de sesiones y control de conexiones entre aplicaciones.

Presentación: Traducción de datos transferidos de las capas inferiores a formatos de red y aplicaciones para la comprensión y encriptación.

Aplicación: Interfaz directa que proporciona servicios de red directamente a las aplicaciones de usuario.

2.1.11. Red de área amplia definida por software (SD-WAN)

La red SD-WAN (red de área amplia definida por software) es el resultado de aplicar el concepto de SDN en redes WAN (red de área amplia) [12].

El objetivo principal es reducir los costos en los servicios de conectividad, empleando una infraestructura existente y en varios servicios de la nube que ofrecen soluciones empresariales [12]. Debido a los términos de SaaS, Cloud, Transformación Digital y SDN que cuentan con protagonismo en los entornos TI durante los últimos años, transformando el estándar de utilizar centros de datos tradicionales para administrar, gestionar, monitorear servicios y aplicaciones, en donde se requieren satisfacer las necesidades de conexión con redes hibridas [11].

2.1.11.1. Descripción funcional de SD-WAN

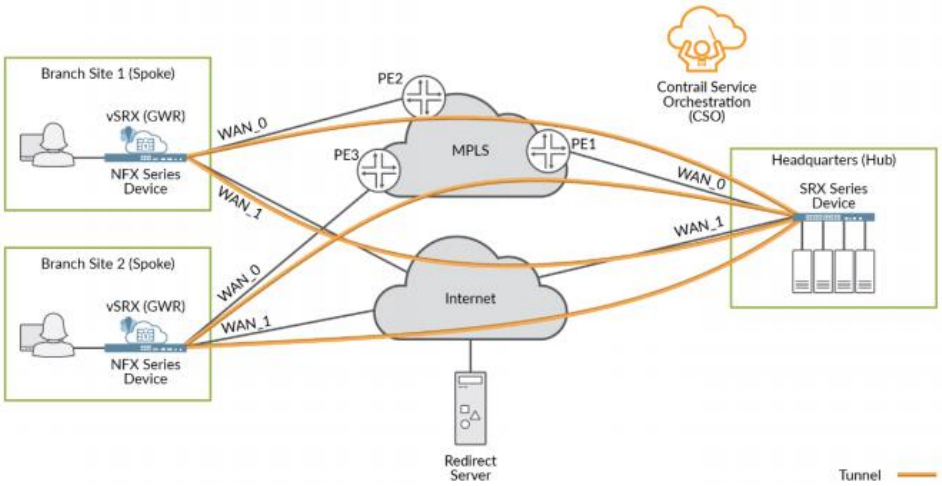
La red SD-WAN, debido a su integración con la tecnología SDN, opera separando el plano de control del plano de datos, lo que garantiza que no habrá pérdida de servicio en caso de pérdida de conexión [11].

El plano de datos transporta los datos entre la aplicación y el usuario, concentrándose en la virtualización, conectividad, seguridad, disponibilidad y calidad del servicio [11]. En el momento de ejecutar una instancia del plano de control presentar varias instancias del plano de datos (enrutadores y conmutadores) [1].

El plano de control es el encargado de señalar el tráfico de la red para y tomar decisiones de enrutamiento de paquetes; incluyendo la administración y configuraciones sistema [1].

En la figura 1 se presenta la red overlay que es la responsable de transportar el tráfico de los usuarios entre equipos. La red underlay es la que se encarga de la conectividad con los dispositivos SD-WAN [11].

Figura 1 Funcionamiento SD-WAN red underlay y overlay

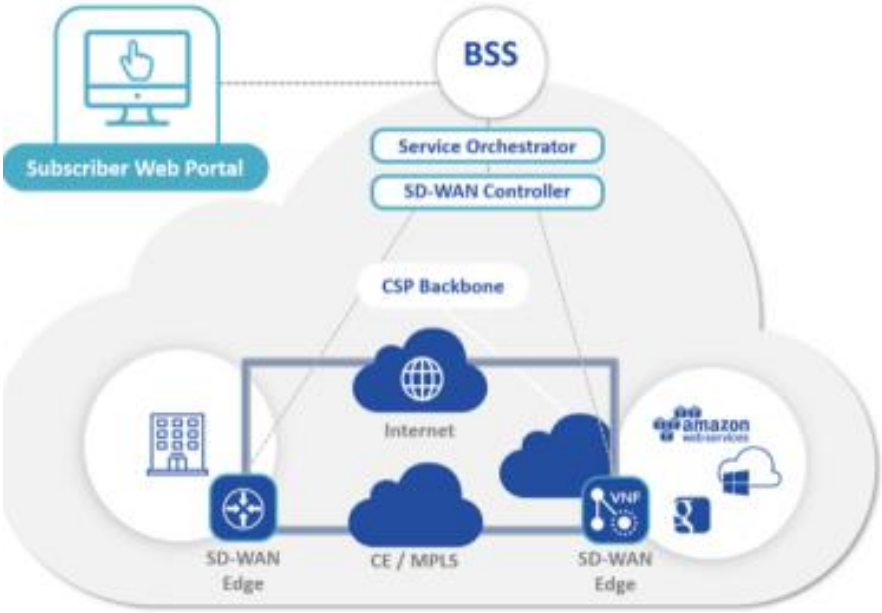


FUENTE: JIMÉNEZ DE LA CUEVA, N. J. (2020) [11]

2.1.11.2. Componentes

Los componentes y arquitecturas dependen de cada fabricante de SD-WAN, debido que no existe un estándar, sin embargo, se ha utilizo como referencia a MEF (Metro Ethernet Forum) debido que es información recopilada de varios fabricantes. Una SD-WAN está conformada por los siguientes componentes que se detallan en la figura 2 [11].

Figura 2 Componentes de la red SD-WAN



FUENTE: JIMÉNEZ DE LA CUEVA, N. J. (2020) [11]

SD-WAN Edge: Son dispositivos físicos o virtuales que brindan conectividad segura a aplicaciones privadas, públicas o híbridas y puede alojar servicios VNF (Virnual Network Eunction).

SD-WAN Controller: Administración y gestión centralizada de los SD-WAN Edges y gateways, es donde por lo general se encuentra el plano de control.

Service Orchestrator: Ejecuta los procesos operativos y funcionales del ciclo de vida de servicios que incluyen la creación y prestación del servicio de extremo a extremo.

Subscriber Web Portal: Desde donde se realiza el pedido y modificación de servicios del suscriptor.

2.1.12. Red de conmutación de etiquetas multiprotocolo (MPLS)

La tecnología MPLS es una red orientada a la conexión, establecida por el IEF (Internet Engineering Task Force) y documentada en RFC 3031 en el año 1998 y varios RFCs, dentro del modelo de referencia OSI se la puede clasificar en la capa 2.5 debido que trabaja entre la capa de enlace de datos y la capa de red [11].

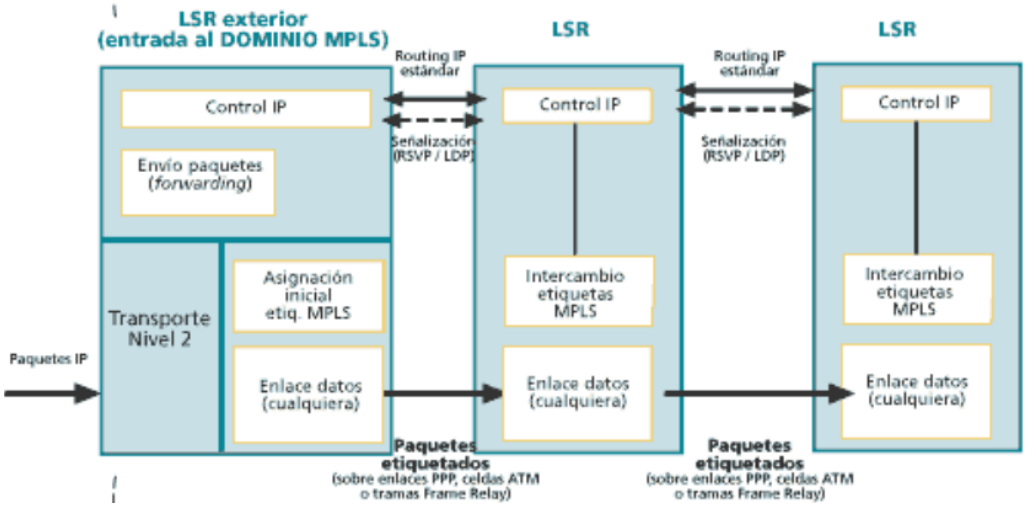
Esta tecnología posibilita seguridad, escalabilidad, fiabilidad y versatilidad en el momento de transmitir cualquier tipo de tráfico: L2VPN, L3VPN, NG-MVPN, VPLS y servicios, debido que funciona con protocolos de enrutamiento en capa 3 [11].

2.1.12.1. Descripción funcional de MPLS

La funcionalidad de la red MPLS se basa en la funcionalidad de envio y control que actúa entre sí. El funcionamiento de MPLS se compone de los siguientes pasos [21]:

1. Creación y distribución de etiquetas
2. Creación de tablas de reenvío en cada enrutador
3. Establecimiento de LSPs (Ruta de conmutación de etiquetas)
4. Asignación de etiquetas a los paquetes según la información de la tabla de reenvío
5. Envio del paquete

Figura 3 Funcionalidad de la red MPLS



FUENTE: GUAS OJEDA, D. S. (2004) [21]

2.1.12.2. Componentes

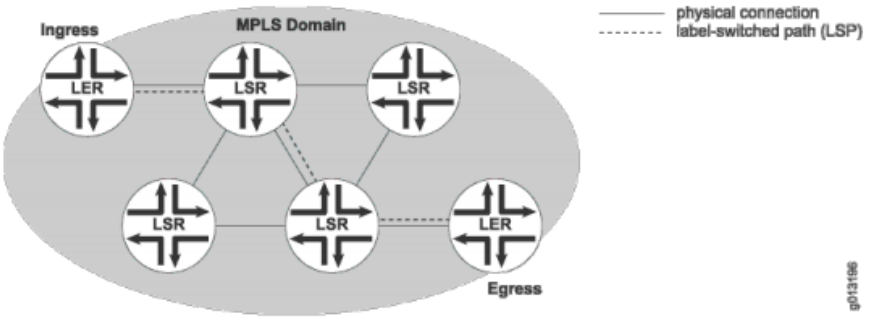
LER (Ruta del borde de la etiqueta): Es un enrutador que se encuentra en el borde del dominio MPLS y se conecta a todos los nodos externos de la red. Pero maneja protocolos de enrutamiento y señalización MPLS [11].

LSR (Ruta conmutada por etiqueta): Es el enrutador interno y central o núcleo de la red MPLS, que permite la conmutación de etiquetas, además es quien maneja los protocolos de enrutamiento y de señalización de MPLS [11].

LSP (Ruta conmutada de etiqueta): Es una ruta lógica en un dominio MPLS, creado por la asociación de etiquetas perteneciente a una misma FEC [11].

LIB (Base de Información de Etiquetas): Todas las tablas de etiquetas e interfaces construye cada LSR y LER [11].

Figura 4 Elementos MPLS



FUENTE: JIMÉNEZ DE LA CUEVA, N. J. (2020) [11]

En la figura 4 se explica el proceso de un paquete cuando ingresa al dominio MPLS, a través del nodo LER, se activa el protocolo LDP o RSVP, en el momento que se establece las vecindades y adyacencias en los nodos LSR a través de mensajes HELLO entre los interfaces que hablan MPLS informando de esta forma a los vecinos las etiquetas con las que trabajarán para conmutar hasta el destino [11].

Cuando llegan los paquetes al nodo LER de final de LSP este se encarga de eliminar la etiqueta MPLS y reenviar el paquete fuera del dominio MPLS mediante routing [11].

2.2. Métricas de evaluación

Las métricas de redes se definen como acknowledge (ACK acuse de recibo) y es un valor que recibe una ruta IP en una interfaz de red. Estas métricas se utilizan para evaluar los dispositivos de enrutamiento con la finalidad de determinar cuál de ellos opera de manera más eficiente, considerando la tasa de entrega en el nodo receptor [14]. A continuación métricas comunes utilizadas [14]:

Ancho de banda (Bandwidth)

Es la capacidad de transmisión de datos en el interior de una red por un periodo de tiempo y su medida se expresa en Mbps [1].

Jitter

Esta apoyado en la conmutación de paquetes, en donde es el resultado de redes de datos no orientados a conexión, además, se lo identifica como la variación del tiempo de llegada entre paquetes y puede ser producido por perdida de congestión de la red o sincronización [1].

Latencia

Es el parámetro que habilita medir el tiempo de espera de un paquete a su destino [1].

Paquetes

Es un bit de datos que se encapsula para la transmisión a través de una red como LAN o Internet. Cada paquete incluye un origen y un destino y a veces se define por el protocolo que utiliza como TCP, UDP, ARP, IP [1].

Tiempo de procesamiento

Es el periodo de tiempo que requiere un sistema o dispositivo para realizar una tarea o procesar datos.

Tasa de transferencia

Tambien se le conoce como tasa de bits consiste en la velocidad de transmisión de los datos[40].

Bit error rate (BER)

Es la cantidad de bits transmitidos que se reciben incorrectamente debido a interferencias, ruido u otros problemas en el canal de comunicación. Se expresa como la relación entre bits erróneos y total de bits transmitidos. Un BER menor indica una comunicación fiable y eficiente [39].

2.3. Marco referencial

El desarrollo del presente proyecto se fundamenta en una revisión bibliográfica de fuentes primarias secundarias de origen nacional e internacional.

2.3.1. Fuentes primarias

Hybrid Networking SDN y SD-WAN: Interoperabilidad de arquitecturas de redes tradicionales y redes definidas por software en la era de la digitalización

La investigación doctoral finalizada en la Universidad Nacional de La Plata por el autor realizo un análisis de la evolución de las redes SDN a SD-WAN con la finalidad de demostrar la facilidad de la implementación [5].

Tambien subraya la importancia de adoptar una cultura de NetDevOps en donde se combina las practica de desarrollo de software con la gestión de redes con la finalizar para garantizar automatización, agilidad y colaboración entre equipos de desarrollo y operaciones [5].

Implementación de una solución SD-WAN para el uso eficiente de los recursos de red en su aplicación en la Empresa Asertia en el año 2021

La implementación realizada en la empresa Asertia por parte del autor abordo la implementación de una solución SD-WAN para mejorar la eficiencia de red y el control de accesos en Asertia hacia aplicaciones corporativas [12].

Además, identifico problemas críticos en la red MPLS como alta latencia y pérdida de paquetes que afectaba la comunicación entre sucursales y la oficina matriz generando costos adicionales. Implementó SD-WAN como solución para optimizar la gestión del tráfico y reducir los problemas anteriores [12]. Posteriormente realizo pruebas para comparar el rendimiento de SD-WAN y MPLS, utilizando la prueba U de Mann-Whitnet para evaluar estadísticamente la latencia y la perdida de paquetes [12].

2.3.2. Fuentes secundarias

Análisis del desempeño de redes definida por software(SDN) frente a redes de arquitectura (TCP/IP)

Este proyecto de investigación realizado en la universidad Técnica Estatal de Quevedo en el año 2019 se centró en el análisis del desempeño de arquitecturas basadas en redes definidas por software (SDN) en comparacion con la arquitectura TCP/IP. El estudio inicio con la identificación y selección de protocolos, controladores y herramientas de emulación para SDN [1].

Posterior el diseño de escenarios para evaluar métricas como latencia, Jitter, paquetes para realizar un análisis estadístico utilizando RStudio con el lenguaje R, obteniendo y resaltando los beneficios obtenidos [1].

Diseño y simulación de una red MPLS utilizando equipos Mikrotik y el emulador GNS3 en entornos PYMES

Este trabajo de titulación realizado en la Universidad de las América en la ciudad de Quito en el año 2019 se concentró en el diseño y simulación de una red MPLS utilizando equipos Mikrotik y el emulador GNS3 con el objetivo de demostrar que Mikrotik ofrece un rendimiento comparable a las marcas principales de telecomunicación [15].

El autor configuro routers Mikrotik en el núcleo (P Core) para el reenvió de paquetes y routers de acceso (PE) para el empaquetado de MPLS, utilizo el ruteo de capa 3 mediante VPN L3 y VRF en conjunto rutas BGP [15].

Además, instalo routers CPE en los clientes con uno router configurado como matriz y las como sucursales conectadas a través de rutas estáticas para asegurar la comunicación [15].

Implementación de un prototipo de una red SD-WAN (Software - Defined Wide Área Network) utilizando tecnología de Juniper Networks

El presente proyecto de titulación fue realizado en la Escuela Politécnica Nacional (EPN) ubicada en la ciudad de Quito del año 2021 implemento un prototipo de red SD-WAN utilizando tecnología Juniper Network [11].

Identifico los conceptos claves de las tecnologías WAN asi como MPLS, Ethernet, LTE para detallar aspectos técnicos de SD-WAN. Además agrego políticas de seguridad aprovechando la capacidad de los enrutadores-firewall mediante la plataforma Sky Enterprise. Finalmente realizo pruebas de funcionamiento y realizo un análisis económico basado en el costo total de propiedad (TCO) de las tecnologías implementadas [11].

2.4. Marco legal

En la constitución del 2008 de la Republica del Ecuador establece [27]:

Articulo 261.10.- *El espectro radioeléctrico y el régimen general de comunicaciones y telecomunicaciones; puertos y aeropuertos.*

Articulo 313.- *Se considera sectores estratégicos la energía en todas sus formas, las telecomunicaciones, los recursos naturales no renovables.*

Articulo 314.- *El Estado será responsable de la provisión de los servicios públicos de agua potable y de riego, saneamiento, energía eléctrica, telecomunicaciones, vitalidad, infraestructuras portuarias y aeroportuarias, y lo demas que determine la ley.*

Dentro de la Ley de Orgánica de Telecomunicaciones (LOTC) especifica lo siguiente [28]:

Artículo 3.3: *Incentivar el desarrollo de la industria de productos y servicios de telecomunicaciones.*

Artículo 3.4: *Promover y fomentar la convergencia de redes, servicios y equipos.*

A pesar de estos marcos legales, en el Ecuador no existe ley alguna que regularice la implementación de redes SD-WAN y MPLS que estén vigentes por parte de los proveedores de servicios de telecomunicaciones generando una brecha normativa. Si bien, el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) impulsa la transformación digital del Ecuador, siendo un instrumento de política pública que vincula prioridades de varios sectores.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Localización

El proyecto de investigación se realizó en el laboratorio de redes del campus "Manuel Haz Álvarez" de la Universidad Técnica Estatal de Quevedo, ubicado en el cantón Quevedo – Los Ríos, Ecuador con coordenadas -1.0127304854926973, -79.46953610493159.

Figura 5 Ubicación del campus central de la universidad UTEQ

FUENTE: GOOGLE MAPS

3.2. Tipo de investigación

3.2.1. Investigación bibliográfica

La recopilación de información sobre SD-WAN y MPLS para conocer el funcionamiento y los controladores fue a través de la investigación bibliográfica. Además, se recurrió a tesis de grado, postgrado y artículos científicos relacionados con el tema, para identificar parámetros relevantes que permitan evaluar el rendimiento de SD-WAN frente a MPLS.

3.3. Métodos de investigación

3.3.1. Método inductivo

Se utilizó para construir una comprensión sólida y progresiva del tema, partiendo desde conceptos de SD-WAN y MPLS asi como la estructura y componentes. Este enfoque permitió a partir de observaciones desarrollar una visión integral de su desempeño.

3.3.2. Método analítico

El método analítico permitió descomponer y examinar las métricas de rendimiento (latencia, jitter, ancho de banda, pérdida de paquetes, etc.) en cada tecnología. Este enfoque facilito

una comparación detallada de SD-WAN y MPLS al analizar cada parámetro influyente en el desempeño general de la red en distintas condiciones.

3.3.3. Método cuasiexperimental

Permitió establecer configuraciones para SD-WAN y MPLS en condiciones controladas sin intervenir en redes reales de producción permitiendo analizar y comparar los resultados recopilados.

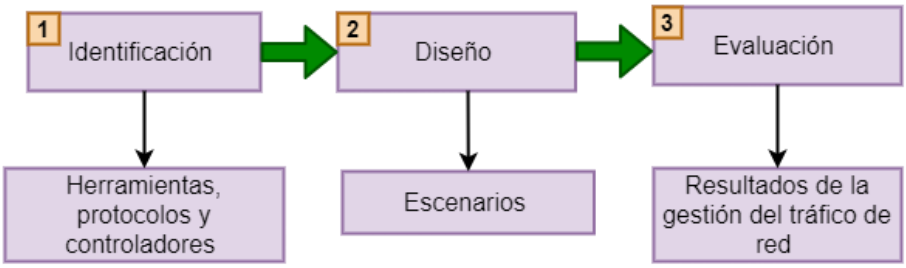
3.4. Fuentes de recopilación de información

La recopilación de información primordial para el proyecto de investigación mediante diferentes fuentes: revistas científicas, libros, tesis relacionadas al tema planteado.

3.5. Diseño de la investigación

En la figura 6 se observa las fases del proyecto de investigación que conlleva al cumplimiento de los objetivos propuestos.

Figura 6 Fases del proyecto de investigación



ELABORADOR POR: CHIMBO FOGACHO MARCO ISAIAS

3.5.1. Identificación de herramientas, protocolos y controladores

Identificación de los controladores, protocolos y herramientas de emulación y simulación que se utilizarían en la investigación, además se seleccionaran aquellas que mejor se ajustaban a los objetivos del estudio.

3.5.2. Diseño de escenarios

Diseño de emulados, empleando las herramientas identificadas. Se diseñaron topologías de red incluyendo configuraciones tanto para SD-WAN como para MPLS. Cada escenario fue configurado con parámetros específicos para replicar condiciones reales de tráfico y evaluar el comportamiento de las redes bajo niveles de carga.

3.5.3. Evaluación de resultados de la gestión del tráfico de red

Finalmente, se llevó a cabo el análisis de los resultados obtenidos de las simulaciones. En esta fase se analizaron métricas clave como latencia, jitter, pérdida de paquetes, ancho de banda y tasa de bits, entre otras.

Los datos recopilados fueron procesados y almacenados en una base de datos de series temporales, permitiendo una evaluación detallada y en tiempo real. Este análisis permitió extraer conclusiones sólidas sobre el desempeño de las redes estudiadas y formular recomendaciones basadas en evidencia para su optimización.

3.6. Recursos y presupuesto

3.6.1. Talento humano

El autor del trabajo investigativo:

- Chimbo Fogacho Marco Isaias

3.6.2. Recursos de hardware

- Computadora Portátil HP 14’ 2.30 GHz - Core i3 7ma Gen – 20Gb RAM

3.6.3. Recursos de software

Tabla 1 Requerimientos de software

Software	Descripción	Costo
Ubuntu 22.04.4 LTS	Sistema operativo GNU/Linux	$0
Debian 10	Sistema operativo GNU/Linux	$0
VMware Workstation Pro 15.5.2	Virtualización	$0
GNS3 2.2.40.1	Simulación e emulación de redes	$0
Grafana 11.1.0	Análisis de datos y visualización	$0
Winbox 6.49.15	Administración de Mikrotik	$0
Solar-Putty 4.2.0.0	Administración remota	$0
InfluxDB 2.7	Base de datos de serie temporal	$0
Python 3.11	Lenguaje de programación	$0
Sublime Text 2	Editor de código	$0
	Total	$0

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. Identificación de herramientas, protocolos y controladores

4.1.1. Identificación de las herramientas de emulación

En el ámbito del diseño de redes, las herramientas de emulación desempeñan un papel importante permitiendo replicar el comportamiento de dispositivos y redes en entornos emulados, la elección de la herramienta adecuada depende a las características del proyecto de investigación. La tabla 2 presenta una comparativa de diversos emuladores.

Tabla 2 Comparacion de software para emulacion y simulacion de redes

Características	Cisco Packet Tracert	GNS3	EVE-NG	Mininet
Simulador	Si	Si	Si	Si
Emulador	No	Si	Si	No
Open Source	No	Si	Si	Si
Interfaz de usuario(GUI)	Si	Si	Si	No
Multiplataforma	No	Si	Si	Si
Programabilidad	No	Si	Si	Si
Controladores admitidos	No	Si	Si	Si
Herramientas de trafico	No	Si	Si	Si
Escalabilidad	No	Si	Si	Si
Compatibilidad con Dynamips	No	Si	Si	No
Complejidad	Bajo	Media	Alto	Alto
Programabilidad	No	Si	Si	Si
Documentación	Si	Si	Si	Si
Requiere Máquina Virtual	No	Si	Si	No
Memoria RAM	4 Gb	4 Gb	4 Gb	2 Gb

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

A partir de la tabla comparativa se determinó que GNS3 es el emulador más adecuado para el presente proyecto, GNS3 permite diseñar redes ip incluyendo una WAN(Wide Area Network) [13][22]. Además se destaca por su facilidad de utilización, escalabilidad, compatibilidad, admisión de protocolos y dispositivos como router, switch, máquina virtual de diferentes fabricantes.

4.1.2. Identificación de los protocolos de la red

En el área de existe diferentes protocolos por lo cual se realizó una tabla comparativa de los protocolos de MPLS y SD-WAN desarrollado por el IEFT (Grupo de Trabajo de Ingeniería de Internet).

Tabla 3 Protocolos de red

Protocolo	Creador	Función
Label Distribuition Protocolo(LDP)	IEFT	Proporciona mecanismo para que los routers de conmutación de etiquetas puedan localizar a sus pares y establecer comunicación entre ellos.
Resource Reservation Protocol(RSVP)	IEFT	Reserva recursos de red a través de una ruta especifica, garantizando la calidad de servicio para el flujo de datos.
Segment Routing(SR)	IEFT	Simplifica y optimiza la gestión de rutas en la red permitiendo a los paquetes seguir rutas predefinidas utilizando una lista de segmentos cada uno identificado por un segment identifier(SID)
Protocol BGP Label Unicast(BGP-LU)	IEFT	Distribuye etiquetas MPLS entre routers, permitiendo la construcción de rutas eficientes y escalables
Netconfig	IEFT	Utiliza XML sobre SSH para proporcionar un medio seguro y estandarizado para la gestión y configuración de dispositivos de red.
Simple Network Management Protocol(SNMP)	IEFT	Monitorizar y gestionar dispositivos de red como routers, switches y servidores a través de la recolección de información de estado y rendimiento.
Protocolo de control de transmisión(TCP)	Vinton Cerf y Robert E. Khan	Establecer y mantener una conexión fiable entre dos dispositivos para garantizar la entrega segura y ordenada de datos.
Protocolo de datagrama del usuario (UDP)	Vinton Cerf y Robert E. Khan	Establece una comunicación entre dos dispositivos de manera similar a TCP pero no garantiza la fiabilidad de los datos transmitidos.
Protocolo de mensaje de internet(ICMP)	RFC 792	Envia mensajes sobre el estado de conexión y detectar problemas.

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

A través de la tabla comparativa se eligió el protocolo ICMP para el análisis de las redes MPLS y SD-WAN. El protocolo IMCP destaca en facilitar la gestión de redes debido a la transferencia de datos de diagnóstico en tiempo real [29] [25].

Permitiendo evaluar métricas como latencia, jitter y pérdida de paquetes. Además, ICMP es ampliamente utilizado para identificar y solucionar problemas de conectividad de manera eficiente y práctica, optimizando el desempeño de las redes analizadas.

4.1.3. Identificación de los controladores para MPLS y SD-WAN

4.1.3.1. Controladores de SD-WAN

Los controladores de SD-WAN permite la administración centralizada, automatización de servicios y la optimización del tráfico a través de políticas definidas. En la tabla 4 se clasifica los controladores más destacados.

Tabla 4 Controladores SD-WAN

Características	Cisco vManage	Cisco Meraki	VMware Velocloud SD-WAN	Juniper Contrail SD-WAN	Fortimanager
Proveedor	Cisco	Cisco	VMware	Juniper Networks	Fortinet
Interfaz de usuario	Web	Web	Web	Web, CLI	Web, CLI
Api	Restful	Restful	Restful	Restful	Restful
Lenguaje	Js, Python	Js	Js, Python	Java, Python	C++, Python
Multiplataforma	Si	Si	Si	Si	Si
Seguridad	Si	Si	Si	Si	Si
Análisis y reporte	Si	Si	Si	Si	Si
Memoria RAM	8GB	4GB	8GB	8GB	8GB
Consumo de recursos	Alto	Bajo	Medio	Alto	Medio
Componentes Adicional	Cisco Vbond, Vedge, Vsmart	No	Orchestrator, Gateway	Gateway, Orchestrator	Fortigate, Fortianalizer
Dificultad de configuración	Alto	Bajo	Medio	Medio	Medio
Virtualización	Si	No	Si	Si	Si

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

Fortimanager usa el sistema operativo FortiOs el mismo que emplean los dispositivos Fortigate y fue una elección ideal debido que existe una documentación completa, pero una red SD-WAN usando Fortigate puede operar sin la necesidad del controlador Fortimanager a diferencia de Cisco en donde se requiere controladores adicionales para su funcionamiento [16] [30].

Además Fortigate es un dispositivo de NGFW (Next-Generation Firewall) que se basa en autenticación de usuario y posee la capacidad de filtrar paquetes según las aplicaciones o políticas. Estas características lo convierten en una solución robusta y versátil para redes empresariales que buscan alta seguridad y facilidad de gestión

4.1.3.2. Controladores de MPLS

Cabe mencionar que NO existe controladores para las redes MPLS debido a su arquitectura que opera de manera distribuida en diversos dispositivos de red sin la necesidad de un controlador a diferencia de SD-WAN [41].

A continuación se presenta una tabla comparativa de diversos dispositivos para MPLS.

Tabla 5 Dispositivos de red para MPLS

Características	Cisco IOS XR	Juniper Junos	Mikrotik RouterOs	Huawei (VRP)
Proveedor	Cisco	Juniper	Mikrotik	Huawei
GUI	Si	Si	Si	Si
Multiplataforma	Si	Si	Si	Si
Escalabilidad	Alta	Alta	Alta	Alta
Soporte de scripts	Python	Python	Python, Winbox scripts	Python, Shell
Documentación	Extensa, profesional	Detallada y estructurada	Amplia y fácil de entender	Amplia y detallada
Facilidad de uso	Alta y requiere conocimiento especializado	Alta y familiaridad con Junos	Alta e intuitiva con Winbox	Alta y requiere conocimiento Huawei
Memoria	16GB	512MB	352MB	2Gb
Componentes adicionales	Si	No	No	No
Virtualización	Si	Si	Si	Si

ELABORADOR POR: CHIMBO FOGACHO MARCO ISAIAS

Mediante la tabla comparativa se elegio Mikrotik RouterOS porque ofrece una configuración accesible y flexible facilitando su utilización incluso para aquellos con menos experiencia en redes [26] [31].

Además, Mikrotik permite la integración del software Winbox con GNS3 permitiendo la administración más intuitiva y eficiente de topologías complejas. Estas características, junto con su documentación clara y facilidad de uso, posicionan a MikroTik como una solución práctica y eficiente para la implementación de redes MPLS en entornos educativos y empresariales.

4.1.3.3. Herramientas de monitorización de redes

En la búsqueda de una solución integral para el monitoreo y la gestión de las redes MPLS y SD-WAN se identificó herramientas de monitoreo centralizados que me facilito para la administración y de los datos a analizar. A continuación en la tabla 6 se presenta herramientas de monitoreo:

Tabla 6 Software de monitorización de redes

Características	Zabbix	Grafana	Nagios
Función principal	Monitoreo y recolección de datos de redes, servidores y aplicaciones	Visualización y análisis de datos de monitoreo	Monitoreo y recolección de datos de sistemas, redes y aplicaciones
Tipo de software	Server y agente	Servidor	Servidor
Interfaz de usuario	Web y CLI	Web	Web
Escalabilidad	Si	Si	Si
Protocolo de comunicación	SNMP, IPMI, JMX, SMTP	HTTP y API	SNMP, HTTP, SMTP, FTP
Integración con otras herramientas	Si	Si	Si
Multiplataforma	Si	Si	Si
Documentación	Si	Si	Si
Memoria RAM	8Gb	4 Gb	1 Gb

ELABORADOR POR: CHIMBO FOGACHO MARCO ISAIAS

Tras un análisis exhaustivo de las opciones disponibles, se determinó a Grafana como la herramienta propicia de análisis centralizado de datos. Grafana destaca por su capacidad de integración con diversas herramientas y su interfaz facilita la visualización y el análisis detallado de las métricas de red [32].

Además, Grafana puede complementarse con otros sistemas para ampliar sus funcionalidades, como la integración con bases de datos y protocolos de comunicación como HTTP y API.

4.1.3.4. Base de datos

Las bases de datos constituyen el núcleo de los sistemas informático y la selección fue crucial para la presente investigación. A continuación se realizó una tabla comparativa de las diferentes bases de datos:

Tabla 7 Base de datos

Características	Relacional	No relacional	Serie Temporal
Modelos de datos	Ordenados por filas, columnas y tablas	Clave-valor, documentos	Datos ordenados por tiempo
Esquema	Estructura rígida y predefinida	Flexible y dinámico	Optimizado para datos temporales
Lenguaje de consulta	SQL(Structured Query Languaje)	Diferentes lenguajes de consulta	SQL para serie temporal o lenguajes específicos de consulta(InfluxDB)
Escalabilidad	Escalabilidad vertical	Escalabilidad vertical	Escalabilidad horizontal y optimizada
Transacciones	Soporte completo(ACID)	Varia en el uso de transacciones	Optimizado para inserciones rápidas
Usos Típicos	Aplicaciones empresariales, sistemas de gestión de datos	Aplicaciones web, grandes volúmenes de datos no estructurados o semiestructurados	Análisis de series temporales, IOT, finanzas, ciencia de datos
Ejemplos de SGBD	MySQL, Oracle, PostgreSQL	MongoDB, Casandra, Redis	InfluxDB, Prometheus, TimeScaleDB

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

Finalizado la tabla comparativa se seleccionó una base de serie temporal como InfluxDB d debido a su capacidad de almacenar y gestionar datos de alta frecuencia de manera eficiente lo cual es ideal para capturar y almacenas métricas de rendimiento de una red o sistema en tiempo real [23] [24].

Estas características resultan especialmente valiosas para analizar las métricas obtenidas en entornos de redes MPLS y SD-WAN, garantizando resultados confiables y oportunos.

4.2. Diseño de escenarios

El diseño de la red es importante por diversas razones en especial para la funcionalidad y la eficiencia entre los nodos. La topología de red adecuada puede mejorar la identificación, rendimiento y resolución de problemas, asi como la una prudente distribución de los recursos para garantizar un funcionamiento optimo [34].

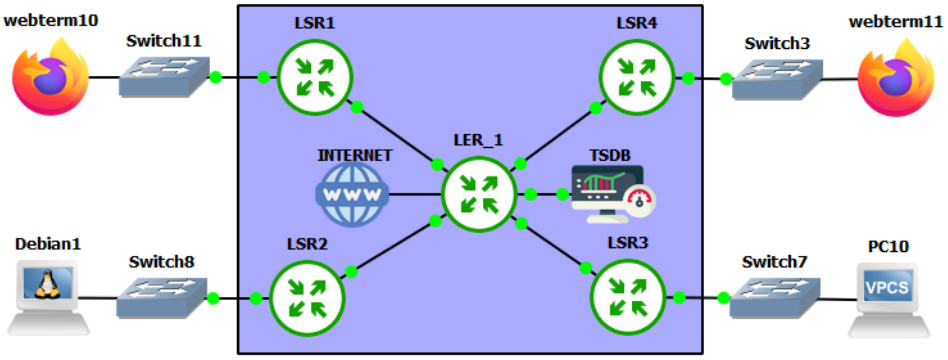
El diseño de los escenarios se fundamenta en el trabajo de Jalil, M. A. bin. (2023) [34] considerando la convergencia, redireccionamiento y el ámbito practico de redes basadas en MPLS y SD-WAN. Para ello, se diseñaron dos topologías (estrella y malla) y sus configuraciones para MPLS, SD-WAN y una red hibrida o mixta entre MPLS y SD-WAN.

4.2.1. Diseño del escenario para la red MPLS

Topología estrella

En la figura 7 se visualiza la topología y consta de 5 enrutadores, 4 switch, 2 navegadores, 1 vpcs y una máquina virtual con el sistema operativo linux para establecer las rutas y asegurar el flujo de datos entre los routers, switches y dispositivos finales.

Figura 7 Diseño de la topología estrella para la red mpls



ELABORADOR POR: CHIMBO FOGACHO MARCO ISAIAS

La Tabla 8 detalla las direcciones ip asignadas a cada interfaz de los equipos de red, esta información es clave para la implementación y monitoreo del escenario, ya que permite identificar y gestionar el flujo de tráfico en la red.

Tabla 8 Direccionamiento ip de la topología estrella para la red mpls

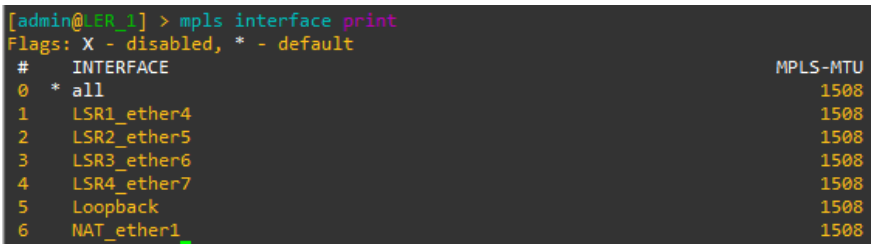
Dispositivo	Interfaz	Direccionamiento	DHCP
LER	ether1	192.168.83.153/24	
	ether2	192.168.10.10/24	
	ether4	192.168.10.1/24	
	ether5	170.168.10.1/24	
	ether6	170.168.20.1/24	
	ether7	170.168.30.1/24	
	Loopback	20.1.1.1/24	
LSR1	ether2	192.168.10.11/24	
	ether4	170.168.10.2/24	
	ether9	190.168.10.1/24	190.168.10.10-190.168.10.254
	Loopback	20.2.2.2/24	
LSR2	ether2	192.168.10.12/24	
	ether5	170.168.20.2/24	
	ether9	190.168.20.1/24	190.168.20.10-190.168.20.254
	Loopback	20.3.3.3/24	
LSR3	ether2	192.168.10.13/24	
	ether6	170.168.30.2/24	
	ether9	190.168.30.1/24	190.168.30.10-190.168.30.254

	Loopback	20.4.4.4/24	
LSR4	ether2	192.168.10.14/24	
	ether6	170.168.40.2/24	
	ether9	190.168.40.1/24	190.168.40.10-190.168.40.254
	Loopback	20.5.5.5/24	

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

La configuración presentada en las siguientes ilustraciones proporciona una visión técnica detallada de cómo se integraron las interfaces al protocolo MPLS y al protocolo de distribución de etiquetas (LDP).

Figura 8 Interfaces agregadas al protocolo mpls

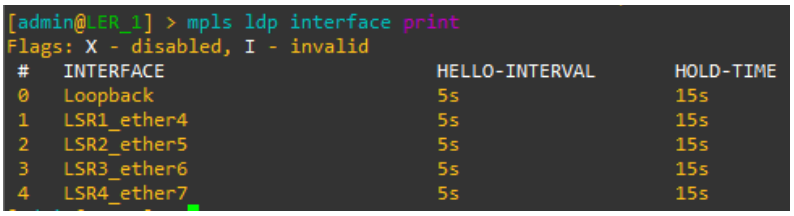


FUENTE: CHIMBO FOGACHO MARCO ISAIAS

En la figura 8 se visualiza las interfaces agregadas al protocolo MPLS en el nodo LER_1.

La asignación uniforme del valor de MTU (1508) en todas las interfaces es esencial para evitar fragmentación de paquetes, asegurando un transporte eficiente de datos. Este valor ligeramente superior al estándar de Ethernet (1500 bytes) se ajusta para incluir la sobrecarga de las etiquetas MPLS.

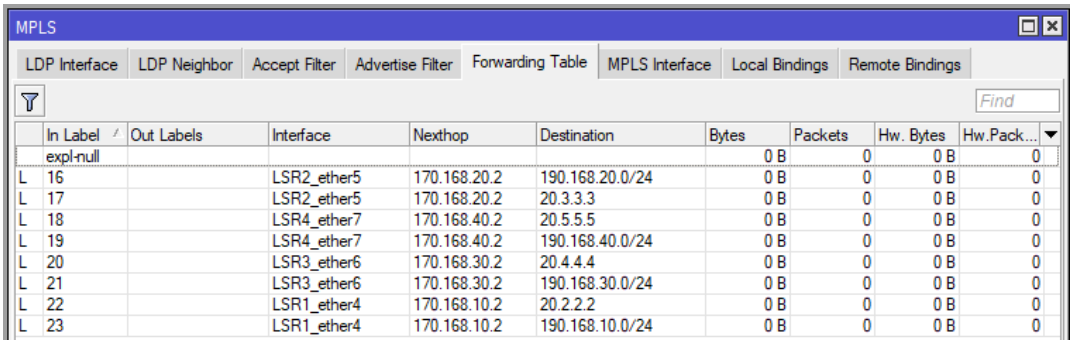
Figura 9 Interfaces configuradas para el protocolo ldp



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

La figura 9, detalla la configuración de las interfaces para el protocolo LDP, que es responsable de la asignación y distribución de etiquetas entre los nodos de la red MPLS. Los parámetros de *hello-interval* y *hold-time* configurados en 5 y 15 segundos, respectivamente, son clave para establecer sesiones de señalización estables, garantizando que los nodos puedan detectar fallos rápidamente y minimizar interrupciones en la red.

Figura 10 Estado de tabla de reenvió del protocolo mpls



	In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets	Hw. Bytes	Hw.Pack...
	expl-null					0 B	0	0 B	0
L	16		LSR2_ether5	170.168.20.2	190.168.20.0/24	0 B	0	0 B	0
L	17		LSR2_ether5	170.168.20.2	20.3.3.3	0 B	0	0 B	0
L	18		LSR4_ether7	170.168.40.2	20.5.5.5	0 B	0	0 B	0
L	19		LSR4_ether7	170.168.40.2	190.168.40.0/24	0 B	0	0 B	0
L	20		LSR3_ether6	170.168.30.2	20.4.4.4	0 B	0	0 B	0
L	21		LSR3_ether6	170.168.30.2	190.168.30.0/24	0 B	0	0 B	0
L	22		LSR1_ether4	170.168.10.2	20.2.2.2	0 B	0	0 B	0
L	23		LSR1_ether4	170.168.10.2	190.168.10.0/24	0 B	0	0 B	0

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

La figura 10 presenta la tabla de reenvío (Forwarding Table) del nodo LER_1. Este mecanismo es central para MPLS, debido que permite a los paquetes ser reenviados basándose únicamente en etiquetas, reduciendo la latencia en comparación con el enrutamiento tradicional.

Figura 11 Interfaces agregadas al protocolo mpls y ldp del nodo LSR2

```
[admin@LSR2] > ip ad print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.10.12/24   192.168.10.0    Admin_ether2
 1   20.3.3.3/32        20.3.3.3        Loopback2
 2   170.168.20.2/24    170.168.20.0    LER_ether5
 3   190.168.20.1/24    190.168.20.0    LAN_ether9
[admin@LSR2] >
[admin@LSR2] > mpls interface print
Flags: X - disabled, * - default
 #    INTERFACE                                                  MPLS-MTU
 0  * all                                                            1508
 1    ether1                                                         1508
 2    LER_ether5                                                     1508
 3    Loopback2                                                      1508
[admin@LSR2] > mpls ldp print
                      enabled: yes
                       lsr-id: 20.3.3.3
            transport-address: 20.3.3.3
            path-vector-limit: 255
                    hop-limit: 255
                 loop-detect: yes
            use-explicit-null: no
  distribute-for-default-route: no
[admin@LSR2] > mpls ldp neighbor print
Flags: X - disabled, D - dynamic, O - operational, T - sending-targeted-hello,
V - vpls
 #      TRANSPORT       LOCAL-TRANSPORT PEER                    SEN
 0 DO   20.1.1.1        20.3.3.3        20.1.1.1:0              no
```

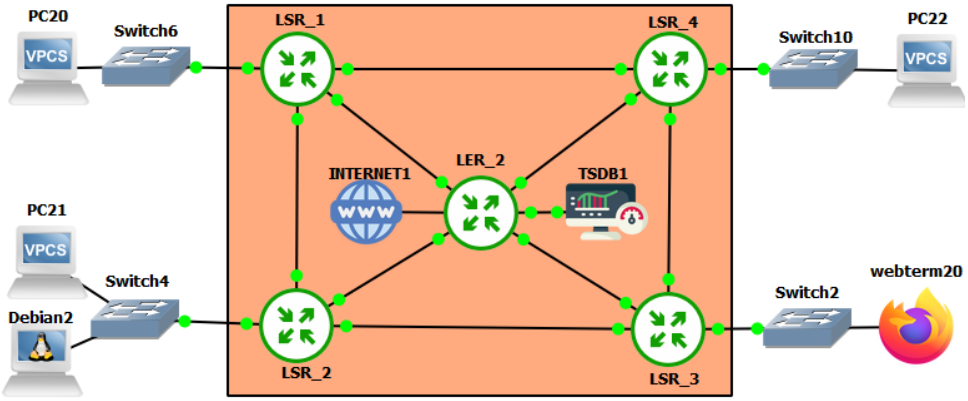
FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Finalmente, en la figura 11 se visualiza la integración de las interfaces del nodo LSR2 tanto al protocolo MPLS como al LDP. Este nodo, como parte de la red de conmutación de etiquetas, tiene un rol crucial en la creación y propagación de etiquetas. La asignación de direcciones y la asociación de las interfaces permiten un tráfico fluido y eficiente, asegurando que los paquetes alcancen su destino con la menor cantidad de saltos posible.

Topología malla

En este escenario se utilizó cinco enrutadores están completamente interconectados, garantizando alta redundancia y disponibilidad. Los cuatro switches conectan dispositivos finales como dos VPCS, un navegador y una máquina virtual linux, que actúa como punto de monitoreo.

Figura 12 Diseño de la topología malla para la red mpls



ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

La siguiente tabla de direccionamiento detalla las direcciones ip asignadas a las interfaces para asegurar la comunicación eficiente entre los nodos y dispositivos finales. Esta configuración complementa la robustez de la topología malla, asegurando un tráfico de datos fluido y confiable.

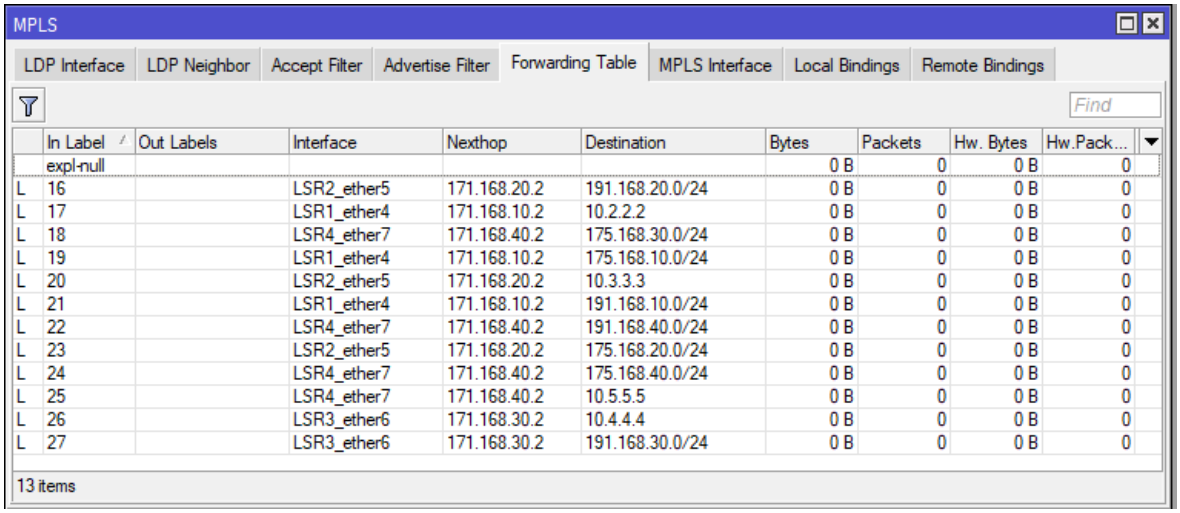
Tabla 9 Direccionamiento ip de la topología malla para la red mpls

Dispositivo	Interfaz	Direccionamiento	DHCP
LER_2	ether1	192.168.83.154/24	
	ether2	192.168.10.20/24	
	ether4	170.168.10.1/24	
	ether5	170.168.20.1/24	
	ether6	170.168.30.1/24	
	ether7	171.168.40.1/24	
	Loopback	10.1.1.1/24	
LSR1	ether2	192.168.10.21/24	
	ether4	171.168.10.2/24	
	ether3	175.168.10.1/24	
	ether6	175.168.40.10/24	
	Loopback	10.2.2.2/24	
	ether9	191.168.10.1/24	191.168.10.10-191.168.10.254
LSR2	ether2	192.168.10.22/24	
	ether5	171.168.20.2/24	
	ether3	175.168.10.10/24	

	ether4	175.168.20.1/24	
	Loopback	10.3.3.3/24	
	ether9	191.168.20.1/24	191.168.20.10-191.168.20.254
LSR3	ether2	192.168.10.23/24	
	ether6	171.168.30.2/24	
	ether4	175.168.20.10/24	
	ether5	175.168.30.1/24	
	Loopback	10.4.4.4/24	
	ether9	191.168.30.1/24	191.168.30.10-191.168.30.254
LSR4	ether2	192.168.10.23/24	
	ether7	171.168.40.2/24	
	ether6	175.168.40.1/24	
	ether5	175.168.30.10/24	
	Loopback	10.5.5.5/24	
	ether9	191.168.40.1/24	191.168.40.10-191.168.40.254

ELABORADO POR: Chimbo Fogacho Marco Isaias

Figura 13 Estado de tabla de reenvió del protocolo mpls en la topología malla



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

La figura 13 representa la tabla de reenvío (forwarding table) en el nodo LER_2 y se visualiza las etiquetas asignadas a cada destino, las interfaces asociadas, y los nexthops.

Figura 14 Estado de conexión en la topología malla de la red MPLS

```
PC22> ip dhcp
DORA IP 191.168.40.254/24 GW 191.168.40.1

PC22> ping 8.8.8.8 -l 1400
1428 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=171.552 ms
1428 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=153.276 ms
1428 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=163.878 ms
1428 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=152.435 ms
1428 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=136.037 ms

PC22> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=155.956 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=149.961 ms
8.8.8.8 icmp_seq=3 timeout
8.8.8.8 icmp_seq=4 timeout
84 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=179.093 ms

PC22> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   191.168.40.1   1.719 ms  1.345 ms  1.439 ms
 2   175.168.30.1   4.463 ms  2.096 ms  1.898 ms
 3   171.168.40.1   3.143 ms  3.442 ms  2.800 ms
 4   192.168.83.2   6.091 ms  4.834 ms  4.333 ms
 5     *  *  *
```

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

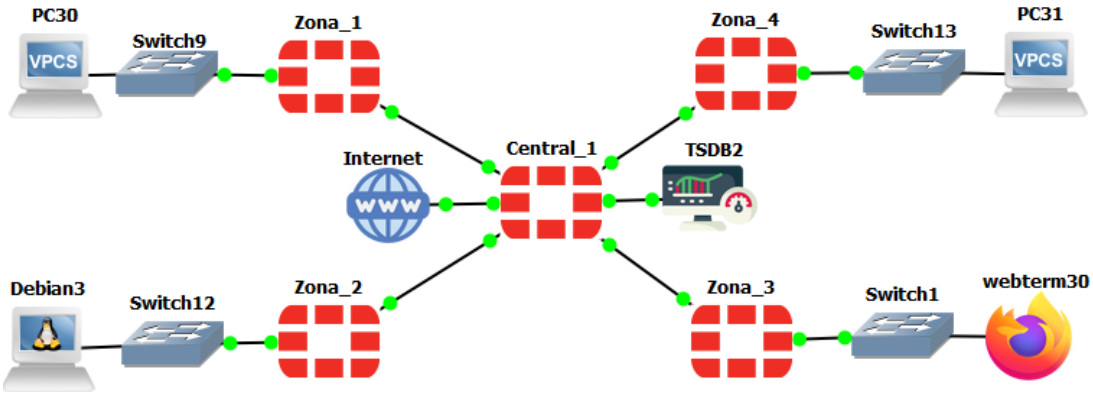
En la figura 14 presenta el estado de conexión desde el host final confirmando la operación correcta de la topología malla en la red MPLS.

4.2.2. Diseño del escenario de la red SD-WAN

Topología estrella

La topología estrella centraliza la comunicación a través de 5 enrutadores, 4 switch, 1 navegador web, 2 vpcs y una máquina virtual con sistema operativo linux.

Figura 15 Diseño de la topología estrella para la red SD-WAN



ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

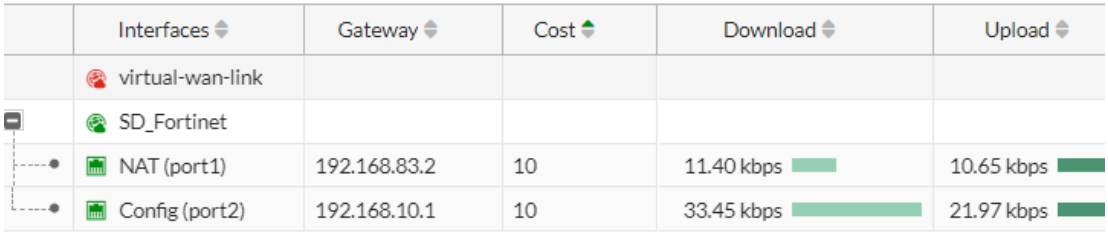
La Tabla 10 presenta el direccionamiento ip de la topología estrella, con detalles de las interfaces asignadas a cada dispositivo. Esta configuración es esencial para establecer las rutas de tráfico y garantizar la conectividad entre las zonas y el nodo central.

Tabla 10 Direccionamiento ip de la topología estrella para la red SD-WAN

Dispositivo	Interfaz	Direccionamiento	DHCP
Central 1	Port1	192.168.83.2	
	Port2	192.168.10.30/24	
	Port4	182.168.10.1/24	
	Port5	182.168.20.1/24	
	Port6	182.168.30.1/24	
	Port7	182.168.40.1/24	
Zona 1	Port2	192.168.10.31/24	
	Port4	182.168.10.2/24	
	Port9	189.168.10.1/24	189.168.10.10-189.168.10.254
Zona 2	Port2	192.168.10.32/24	
	Port5	182.168.20.2/24	
	Port9	189.168.20.1/24	189.168.20.10-189.168.20.254
Zona 3	Port2	192.168.10.33/24	
	Port6	182.168.30.2/24	
	Port9	189.168.30.1/24	189.168.30.10-189.168.30.254
Zona 4	Port2	192.168.10.34/24	
	Port7	182.168.40.2/24	
	Port9	189.168.40.1/24	189.168.40.10-189.168.40.254

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

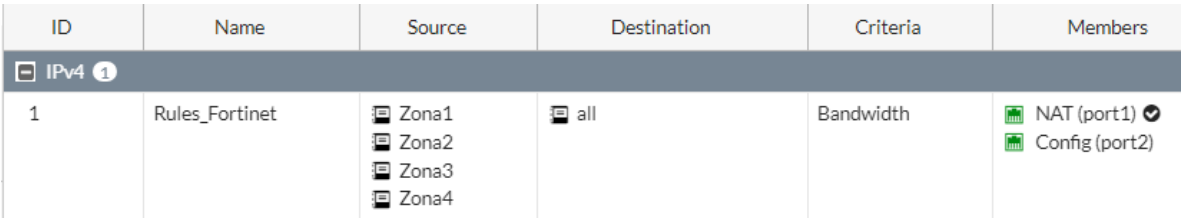
Figura 16 Configuración de zones en SD-WAN estrella



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

La figura 16 presenta la configuración de zonas en una red SD-WAN estrella, con interfaces físicas NAT (port1) y Config (port2) conectadas a un gateway. Ambas interfaces tienen un costo configurado de 10, lo que permite rutas balanceadas y esta configuración garantiza una gestión eficiente del tráfico interno y externo, asegurando conectividad y rendimiento óptimos.

Figura 17 Configuración de rules en la topología estrella de la red SD-WAN

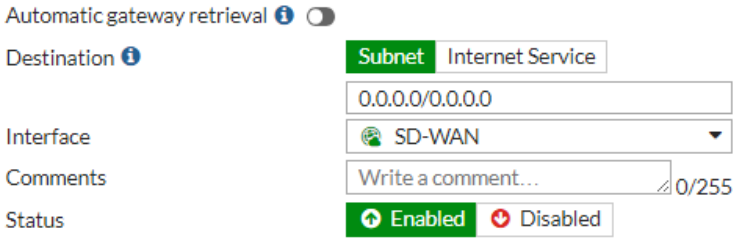


ID	Name	Source	Destination	Criteria	Members
IPv4 1					
1	Rules_Fortinet	Zona1 Zona2 Zona3 Zona4	all	Bandwidth	NAT (port1) Config (port2)

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Se observa en la figura 17 las reglas de tráfico (*Rules*) que define el manejo del tráfico entre las zonas y hacia el nodo central (*Central_1*). En la configuración presentada, las reglas permiten el tráfico entre todas las zonas, garantizando la comunicación entre los dispositivos finales y el nodo central con criterios como el ancho de banda.

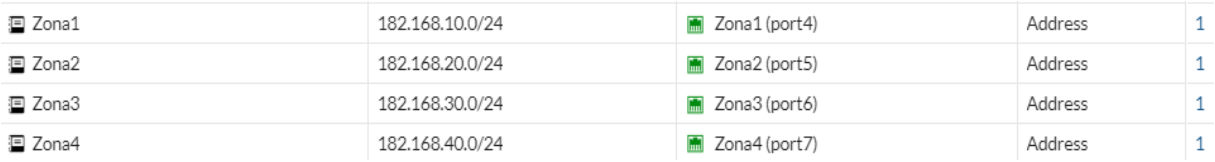
Figura 18 Configuración de ruta estática en la red SD-WAN estrella



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

En la figura 18 se establece la ruta estática en donde se especifica los caminos que debe seguir el tráfico para alcanzar destinos fuera de la red local. Estas configuraciones son fundamental para garantizar la conectividad de las zonas hacia internet y entre ellas a través del nodo central.

Figura 19 Configuración de address en policy & objects de SD-WAN estrella



Zona1	182.168.10.0/24	Zona1 (port4)	Address	1
Zona2	182.168.20.0/24	Zona2 (port5)	Address	1
Zona3	182.168.30.0/24	Zona3 (port6)	Address	1
Zona4	182.168.40.0/24	Zona4 (port7)	Address	1

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

En la figura 19 se visualiza las direcciones configuradas que permite identificar los segmentos de red asociados a cada zona y esto simplifica la implementación de políticas de seguridad y la asignación de reglas específicas para cada segmento de red.

Figura 20 Configuración de firewall policy en SD-WAN estrella

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Zona1 (port4) → SD_Fortinet 1									
Salida_Zona1	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	81.62 kB
Zona2 (port5) → SD_Fortinet 1									
Salida_Zona2	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	362.43 kB
Zona3 (port6) → SD_Fortinet 1									
Salida_Zona3	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	55.67 kB
Zona4 (port7) → SD_Fortinet 1									
Salida_zona4	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

La figura 20 presenta las políticas de firewall que aseguran el control del tráfico, estableciendo reglas para permitir o denegar conexiones. Esta configuración garantiza la seguridad en el acceso a los recursos de la red y el manejo eficiente de paquetes.

En las figuras 21,22 y 23 se presenta las configuraciones correspondientes del nodo zona 2, las cuales son similares a la figura 16, 17, 18, 19 y 20.

Figura 21 Configuración de ip del nodo central de zona 2 SD-WAN estrella.

Physical Interface 10				
Central (port5)	Physical Interface		182.168.20.2/255.255.255.0	PING HTTPS
Config (port2)	Physical Interface		192.168.10.32/255.255.255.0	PING HTTPS HTTP
Lan2 (port9)	Physical Interface		189.168.20.1/255.255.255.0	PING HTTPS

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 22 Configuración de zones del nodo zona 2 en SD-WAN estrella

	Interfaces	Gateway	Cost	Download	Upload
	virtual-wan-link				
	SD_Fortinet2				
	Central (port5)	182.168.20.1	10	2.03 kbps	2.15 kbps

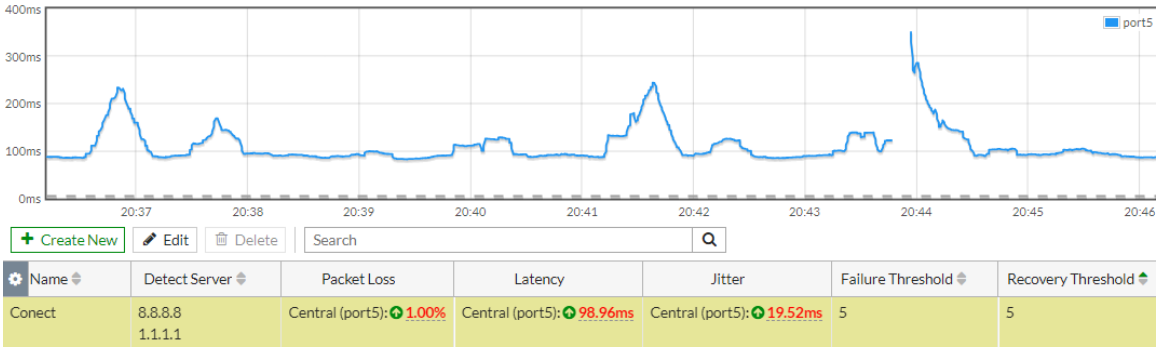
FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 23 Configuración de rules del nodo zona 2 en SD-WAN estrella

ID	Name	Source	Destination	Criteria	Members
IPv4 1					
1	Rules_Fortinet2	Lan2	all	Latency	Central (port5)

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 24 Configuración sla del nodo zona 2 en SD-WAN estrella.

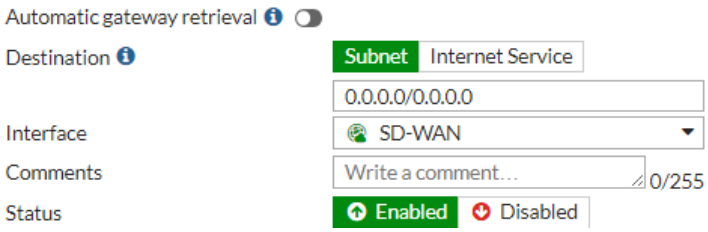


FUENTE: CHIMBO FOGACHO MARCO ISAIAS

La figura 24 se observa los acuerdos de nivel de servicio (SLA) que permite monitorear métricas críticas como latencia, pérdida de paquetes y jitter, asegurando la calidad del servicio en la red. Esto es clave para priorizar rutas y mantener un rendimiento óptimo.

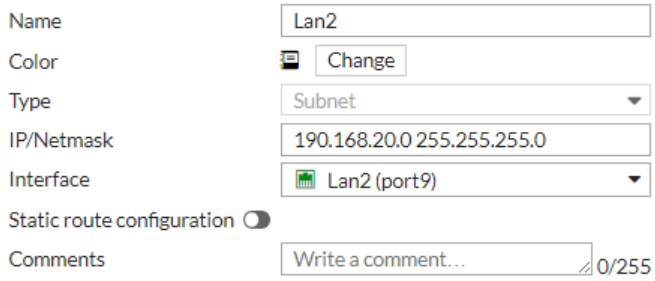
En las figuras 25,26 y 27 se establece configuraciones similares a las figuras 18, 19 y 20 pero con su respectivo direccionamiento.

Figura 25 Configuración de rutas estáticas del nodo zona 2 en SD-WAN estrella.



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 26 Configuración de address del nodo zona 2 en SD-WAN estrella.



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 27 Configuración de firewall policy del nodo zona 2 en SD-WAN estrella.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Lan2 (port9) → SD_Fortinet2 1							
Lan_Central	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

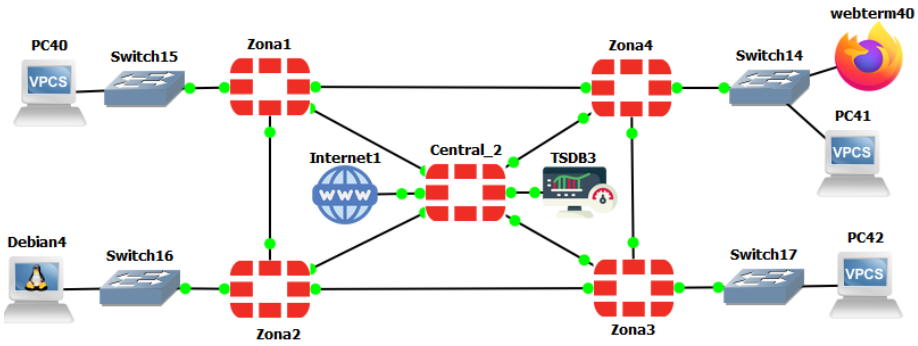
Para las zonas 1, 3 y 4, se aplicó el mismo procedimiento de la zona 2 pero con sus respectivas direcciones ip, asegurando consistencia de implementación y operación de la red.

Topología malla

El diseño de esta topología conecta cinco enrutadores, permitiendo que cada nodo se comunique con los demás y un nodo central. Los cuatro switches facilitan la conexión de los dispositivos finales, como cuatro VPCS, dos navegadores web y una máquina virtual con sistema operativo Linux.

Este diseño asegura redundancia y flexibilidad, optimizando las rutas de tráfico mediante políticas definidas.

Figura 28 Diseño la topología malla para la red SD-WAN



ELABORADO POR: Chimbo Fogacho Marco Isaias

La tabla 11 de direccionamiento presenta las asignaciones ip para cada zona y sus respectivas interfaces, asegurando la comunicación eficiente entre los nodos y dispositivos finales.

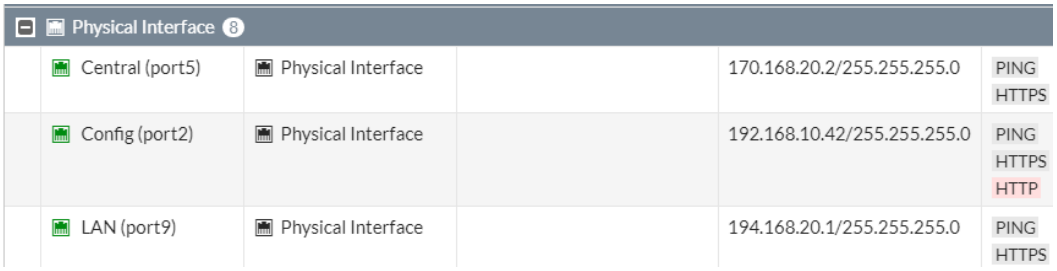
Tabla 11 Direccionamiento ip de la topología malla para la red SD-WAN

Dispositivo	Interfaz	Direccionamiento	DHCP
Central 2	Port1	192.168.83.2/24	
	Port2	192.168.10.40/24	
	Port4	170.168.10.1/24	
	Port5	170.168.20.1/24	
	Port6	170.168.30.1/24	
	Port7	170.168.40.1/24	
Zona 1	Port2	192.168.10.41/24	
	Port3	181.168.10.1 /24	
	Port4	170.168.10.2/24	
	Port6	181.168.40.2 /24	
	Port9	194.168.10.1/24	194.168.10.10-194.168.10.254
Zona 2	Port2	192.168.10.42/24	
	Port3	181.168.10.2/24	
	Port4	181.168.20.1 /24	
	Port5	170.168.20.2/24	
	Port9	194.168.20.1/24	194.168.20.10-194.168.20.254
Zona 3	Port2	192.168.10.43/24	
	Port4	181.168.20.2/24	
	Port6	170.168.30.2/24	
	Port9	194.168.30.1/24	194.168.30.10-194.168.30.254
Zona 4	Port2	192.168.10.43/24	
	Port5	181.168.30.2/24	
	Port6	181.168.40.1 /24	
	Port7	170.168.40.2/24	
	Port9	194.168.40.1/24	194.168.40.10-194.168.40.254

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

En la topología malla para la red SD-WAN se requiere configuraciones que permitan establecer rutas redundantes y garantizar la conectividad directa entre los nodos. Mejorando la tolerancia a fallos y asegura una alta disponibilidad de los servicios de red. A continuación, se detalla el proceso técnico reflejado en las ilustraciones:

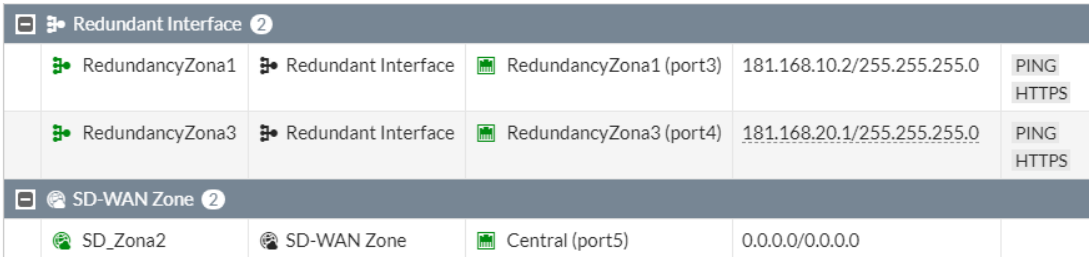
Figura 29 Configuración de ip en la zona 2 de SD-WAN malla



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

En la figura 29 se estable configuraciones de direcciones ip en la zona 2 que garantiza la conectividad con el nodo central y las demás zonas de la topología malla.

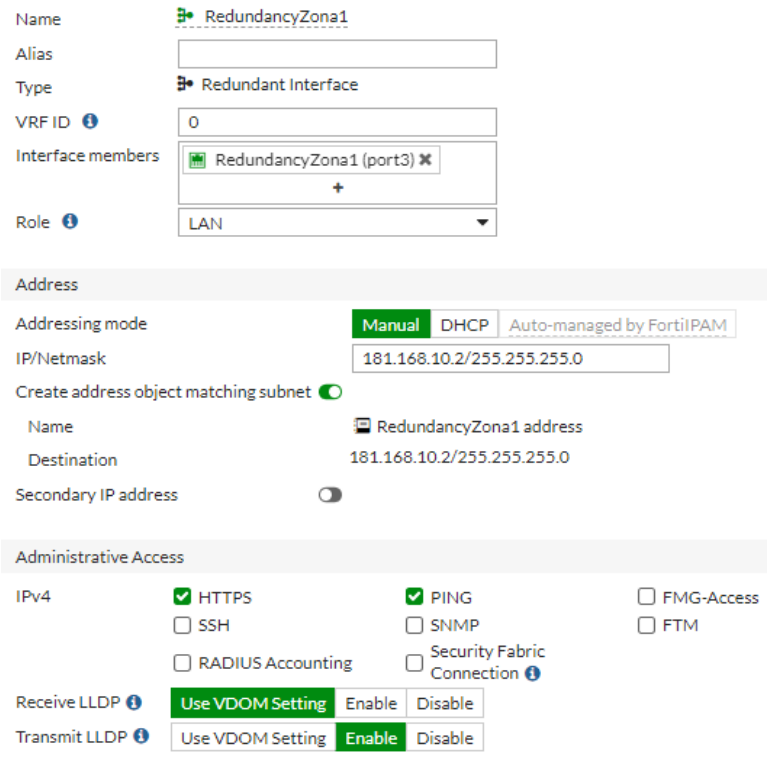
Figura 30 Configuración interfaces redundantes en SD-WAN malla



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

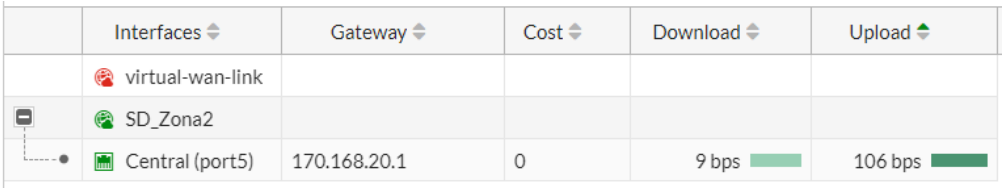
En la figura 30, 31 se define las interfaces redundantes que permite que cada nodo pueda conectarse directamente a los demás. Estas interfaces aseguran múltiples rutas de comunicación, distribuyendo el tráfico de manera eficiente y evitando puntos únicos de fallo.

Figura 31 Configuración interfaces redundantes hacia la zona 1



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 32 Configuración de zones para la zona 2 de SD-WAN malla

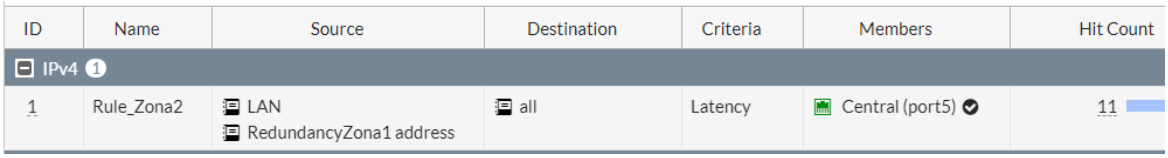


	Interfaces	Gateway	Cost	Download	Upload
	virtual-wan-link				
	SD_Zona2				
	Central (port5)	170.168.20.1	0	9 bps	106 bps

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

En esta figura se define la configuración de zonas como la zona 2 hacia el nodo central, y de esa manera para zona 3, zona 4 y zona 1 estableciendo un control del tráfico y facilita la implementación de reglas de seguridad.

Figura 33 Configuración de rules para la zona 2 en la red SD-WAN malla

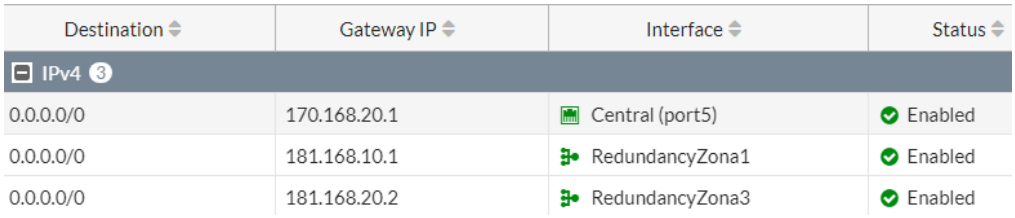


ID	Name	Source	Destination	Criteria	Members	Hit Count
IPv4 1						
1	Rule_Zona2	LAN RedundancyZona1 address	all	Latency	Central (port5)	11

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Las reglas de tráfico determinan la comunicación entre las zonas y hacia el nodo central. Estas reglas permiten priorizar rutas basadas en criterios como latencia, ancho de banda y jitter, optimizando el desempeño de la red.

Figura 34 Configuración de rutas estáticas para la zona 2 en la red SD-WAN malla

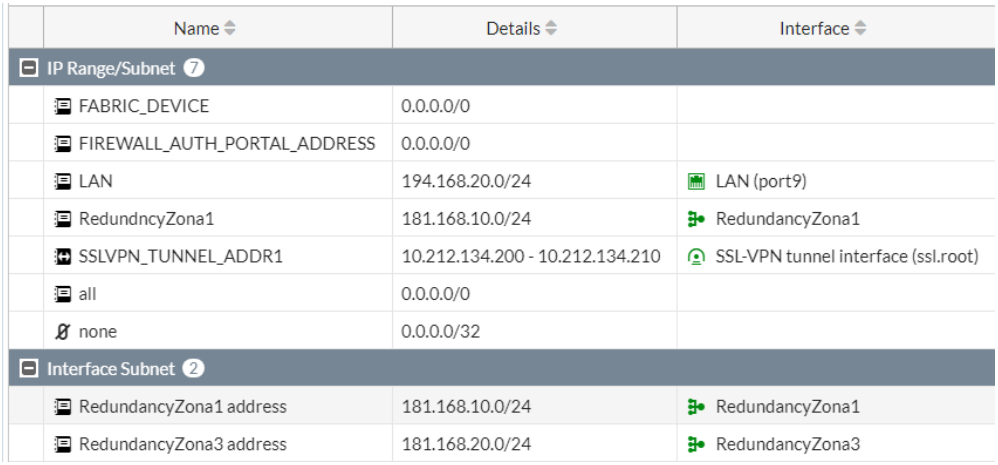


Destination	Gateway IP	Interface	Status
IPv4 3			
0.0.0.0/0	170.168.20.1	Central (port5)	Enabled
0.0.0.0/0	181.168.10.1	RedundancyZona1	Enabled
0.0.0.0/0	181.168.20.2	RedundancyZona3	Enabled

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

En la figura 34 se establece los caminos que el tráfico debe seguir hacia su destino. Esto garantiza que el tráfico entre zonas fluya eficientemente y se mantenga la conectividad con el nodo central y otros recursos externos.

Figura 35 Configuración de address en la zona 2 para la red SD-WAN malla

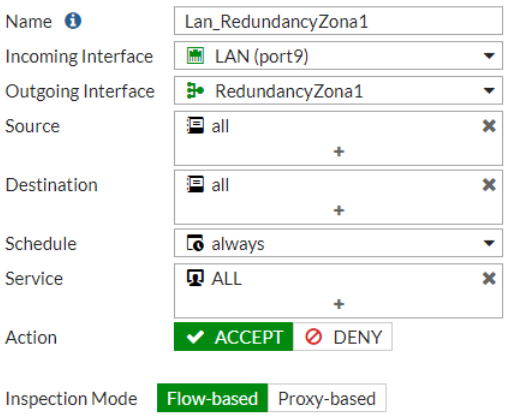


Name	Details	Interface
IP Range/Subnet 7		
FABRIC_DEVICE	0.0.0.0/0	
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0	
LAN	194.168.20.0/24	LAN (port9)
RedundncyZona1	181.168.10.0/24	RedundancyZona1
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)
all	0.0.0.0/0	
none	0.0.0.0/32	
Interface Subnet 2		
RedundancyZona1 address	181.168.10.0/24	RedundancyZona1
RedundancyZona3 address	181.168.20.0/24	RedundancyZona3

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

En la figura 36 y 37 se asigna las políticas de firewall permitiendo el control del tráfico, aplicando reglas que garantizan la seguridad y el manejo eficiente de paquetes entre las zonas y hacia el exterior de la red.

Figura 36 Configuración de firewall policy en la zona 2 para la red SD-WAN malla



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 37 Configuración de firewall policy en la zona 2 para la red SD-WAN malla

Name	Source	Destination	Schedule	Service	Action	NAT
LAN (port9) → RedundancyZona1 1						
Lan_RedundancyZona1	all	all	always	ALL	ACCEPT	Enabled
LAN (port9) → RedundancyZona3 1						
Lan_RedundancyZona3	all	all	always	ALL	ACCEPT	Enabled
LAN (port9) → SD_Zona2 1						
Lan_Central	all	all	always	ALL	ACCEPT	Enabled
RedundancyZona1 → SD_Zona2 1						
Redundancy1_Central	all	all	always	ALL	ACCEPT	Enabled
RedundancyZona3 → SD_Zona2 1						
RedundancyZona3_Central	all	all	always	ALL	ACCEPT	Enabled

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 38 Estado de conexión desde el host final en la red SD-WAN malla

```
PC40> ip dhcp
DDORA IP 194.168.10.10/24 GW 194.168.10.1

PC40> ping 8.8.8.8 -l 1024
1052 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=109.863 ms
1052 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=112.387 ms
1052 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=115.706 ms
1052 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=108.665 ms
1052 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=110.028 ms

PC40> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   194.168.10.1   1.792 ms  2.880 ms  2.685 ms
 2   170.168.10.1   4.623 ms  4.134 ms  5.217 ms
 3   192.168.83.2   6.887 ms  6.995 ms  8.440 ms
 4     *  *  *
```

FUENTE: CHIMBO FOGACHO MARCO ISAIAS

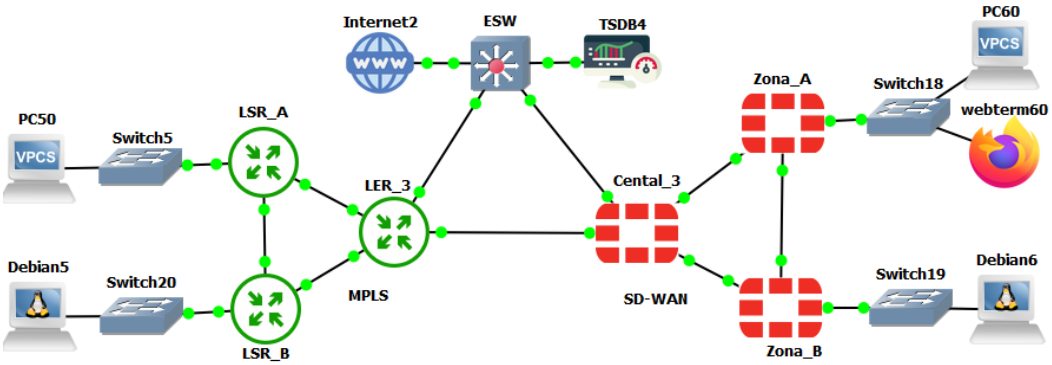
La figura 38 presenta el estado de conexión desde el host final confirmando la operación correcta de la red malla. Este monitoreo en tiempo real permite verificar métricas como latencia, pérdida de paquetes y jitter, garantizando que los parámetros del SLA sean cumplidos.

4.2.3. Diseño del escenario de la red SD-WAN y MPLS

El diseño de una topología mixta que combina las tecnologías SD-WAN y MPLS, proporcionando un enfoque híbrido que aprovecha las fortalezas de ambas redes.

Este diseño incluye seis enrutadores, cuatro switches, dos máquinas virtuales linux, dos VPCS, un navegador web y un switch Ethernet de capa 3 que interconecta los segmentos de la red.

Figura 39 Diseño de la red mixta SD-WAN y MPLS



ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

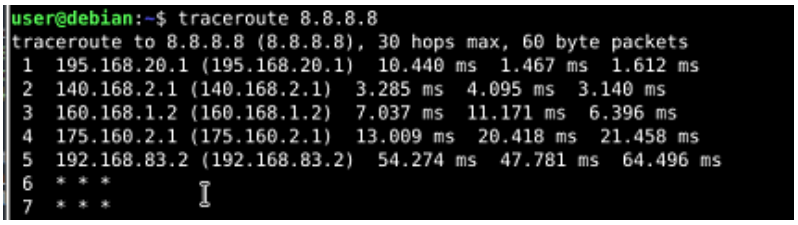
La tabla 12 presenta el esquema de direccionamiento ip utilizado para cada nodo y segmento de la red.

Tabla 12 Direccionamiento ip de la red mixta MPLS y SD-WAN

Dispositivo	Interfaz	Direccionamiento	DHCP
ESW	Fa1/0	192.168.83.80/24	
	Fa1/1	192.168.10.80/24	
	Fa1/7	175.160.1.1/24	
	Fa1/8	175.160.2.1/24	
LER 3	ether4	160.168.1.1/24	
	ether5	140.168.1.1/24	
	ether6	140.168.2.1/24	
	ether7	175.160.1.2/24	
	Loopback	40.1.1.1/24	
LSR A	ether5	140.168.1.1/24	
	ether7	140.168.3.1/24	
	Loopback	40.2.2.2/24	
	ether9	195.168.10.1/24	195.168.10.10-195.168.10.254
LSR B	ether6	140.168.2.2/24	
	ether7	140.168.3.2/24	
	Loopback	40.3.3.3/24	
	ether9	195.168.20.1/24	195.168.20.10-195.168.20.254
Central 3	Port4	160.168.1.2/24	
	Port5	173.168.10.1/24	
	Port6	173.168.20.1/24	
	Port8	175.160.2.2/24	
Zona A	Port5	173.168.10.2/24	
	Port7	183.168.10.1/24	
	Port9	193.168.10.1/24	193.168.10.10-193.168.10.254
Zona B	Port6	173.168.20.2/24	
	Port7	183.168.10.2/24	
	Port9	193.168.20.1/24	193.168.20.10-193.168.20.254

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

Figura 40 Estado de conexión desde host final en la red SD-WAN y MPLS



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

La figura 40 presenta el tráfico entre nodos de diferentes segmentos y destaca las métricas clave capturadas, como latencia y pérdida de paquetes.

Este enfoque permite validar el rendimiento de la red mixta y garantizar la conectividad en todos los niveles.

4.3. Análisis de resultados de la gestión del tráfico de red

Para evaluar el rendimiento de las redes diseñadas se realizó mediante el comando ping de la librería ping3 de Python desde el host final, generando un total de 2200 paquetes de 1024 bytes hacia el servidor DNS de Google (8.8.8.8) y se estableció un timeout de 2 segundos. A continuación se presentan los resultados obtenidos.

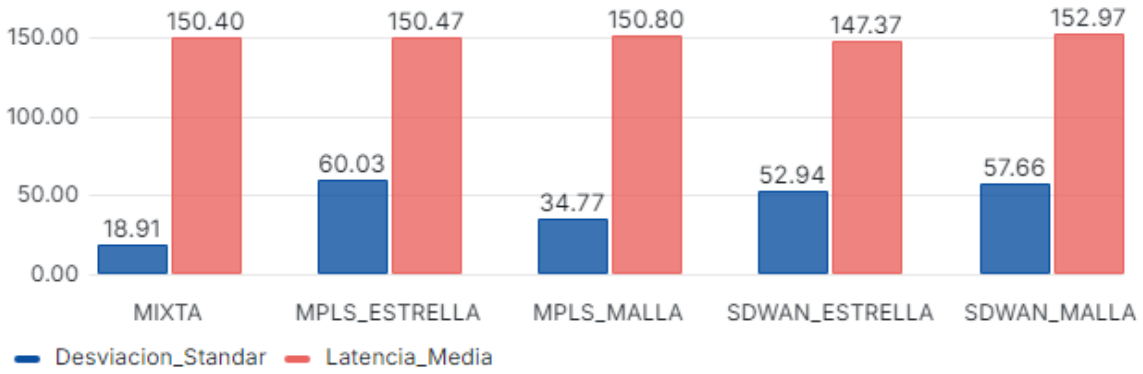
Tabla 13 Métricas obtenidas de las redes

Fecha	Network	IP Host	Latencia (ms)	Desv. Stand.	Jitter (ms)	Paquete Perdido	Tiempo (s)	Bandwidth (Mbps)	Tasa Bits (Mbps)	Bit Error Rate (BER)
04/10/ 2024 22:34	Mixta	195.168.20.254	329076	18.9	30093	12	355	0.101	0.0654	0.0007
04/10/ 2024 22:01	SDWAN Malla	194.168.20.11	334238	57.7	48146	15	366	0.0975	0.103	0.0008
04/10/ 2024 21:26	SDWAN Estrella	189.168.20.10	318321	52.9	43330	40	400	0.0882	0.111	0.0022
04/10/ 2024 21:02	MPLS Malla	191.168.20.254	324983	34.8	46215	45	416	0.0851	0.0885	0.0025
04/10/ 2024 20:35	MPLS Estrella	190.168.20.254	324402	60	44668	44	414	0.0874	0.0904	0.0024

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

4.3.1. Latencia

Figura 41 Latencia media y desviación estándar



ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

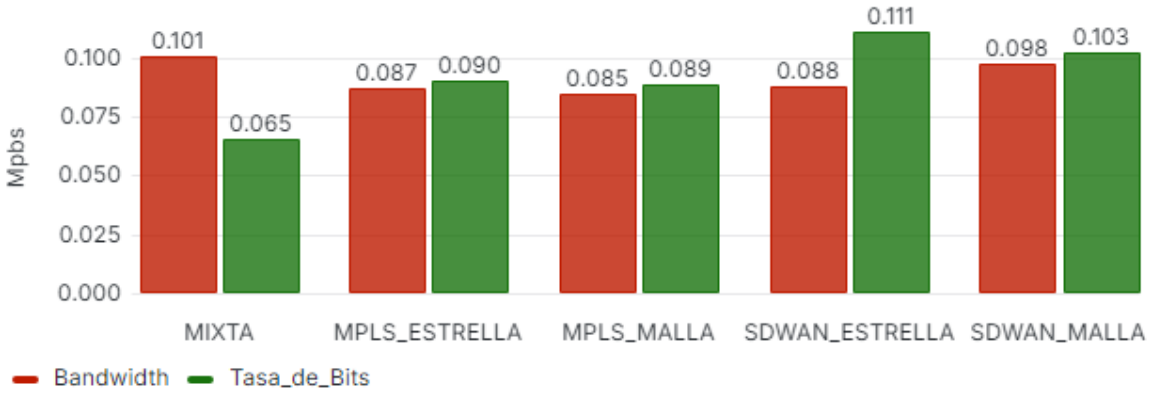
Los resultados obtenidos indican que la latencia promedio es similar entre las topologías, la estabilidad presenta variaciones significativas.

La topología malla de la red SD-WAN exhibió la mayor latencia media de 157.97 ms, seguido de la topología estrella 147.37 ms.

En términos de estabilidad, la topología estrella de la red MPLS demostró la mayor fluctuación en los tiempos de respuesta, con una desviación estandar de 60.03 ms, lo que sugiere una mayor sensibilidad a condiciones variables de la red. Por el contrario la red mixta presento menor variabilidad de18.91 ms, indicando un desempeño consistente.

4.3.2. Ancho de banda y tasa de bits

Figura 42 Consumo del ancho de banda y tasa de transferencia



ELABORADOR POR: CHIMBO FOGACHO MARCO ISAIAS

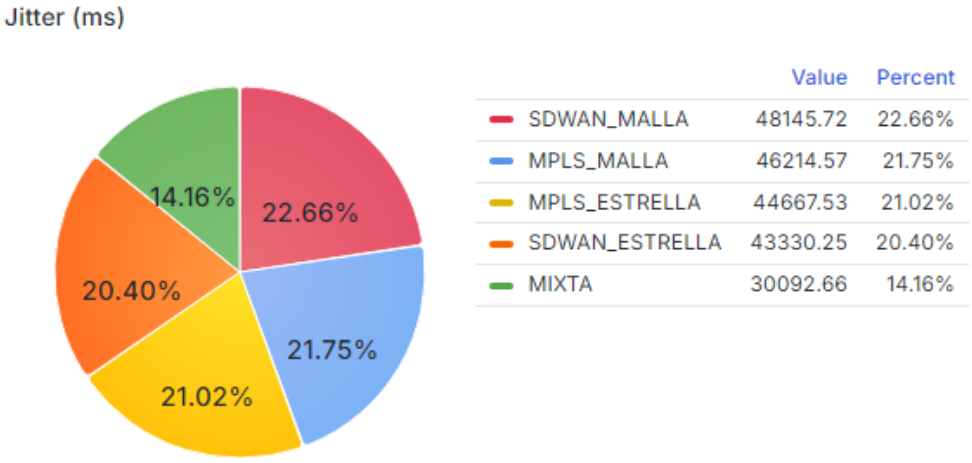
En cuanto al ancho de banda total consumido y la tasa de bits, los resultados muestran que la topología estrella de la red SD-WAN es la más eficiente, registrando un mayor consumo de ancho de banda (0.111 Mbps) y una tasa de transferencia de 0.888 Mbps.

La red mixta, por otro lado, aunque requirió un ancho de banda de 0.101 Mbps, tiene una tasa de bits más baja (0.065 Mbps), lo que indica menor eficiencia en la transferencia de datos.

Las topologías de la red MPLS y la topología malla de la red SD-WAN tiene un comportamiento similar en términos de consumo en donde los valores oscilan entre 0.085 y 0.103 Mbps, lo que refleja un rendimiento intermedio en comparacion a la topología estrella SD-WAN. En general, las topologías de la red SD-WAN presentan un mejor uso del ancho de banda y eficiencia en la transferencia de datos.

4.3.3. Jitter

Figura 43 Resultado de jitter en las diferentes topologías



ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

El análisis del jitter, presentado en la figura 43, revela una considerable variabilidad en los tiempos de latencia entre las topologías evaluadas.

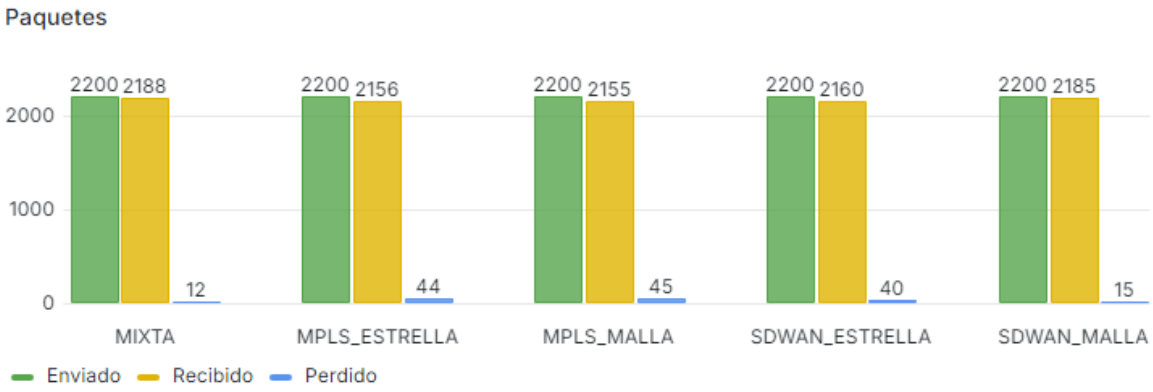
La topología malla de la red SD-WAN presento el mayor valor de jitter 48145.72 ms, representando el 22.6%, lo que indica una fluctuación significativa en los tiempos de respuesta. Las topologías de la red MPLS malla de 462145.57 ms y estrella 44667.53 ms mostrando un comportamiento similar en términos de variabilidad.

Por otro lado la topología estrella de la red SD-WAN registro un jitter 43330.25 ms y la red mixta, el menor valor (30092.66 ms) correspondiente al 14.16%.

Estos resultados sugieren que la topología SD-WAN malla es la más susceptible a variaciones de latencia, lo cual puede afectar a la QoS (calidad de servicio) en aplicaciones sensible al retardo. En contraste, la topología mixta exhibe una menor fluctuación en los tiempos de respuestas indicando un rendimiento más estable.

4.3.4. Paquetes

Figura 44 Transmisión de paquetes



ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

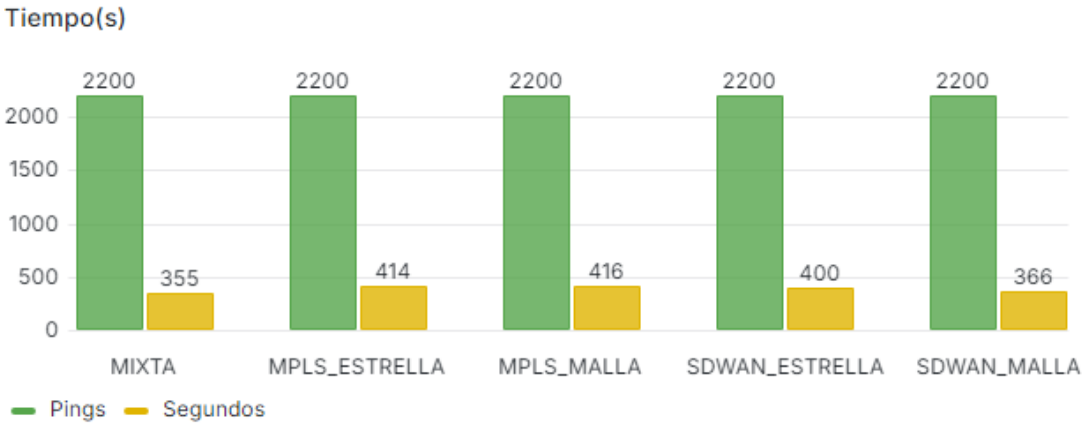
En respecto a la transmisión de paquetes se muestra que la red mixta y la topología malla de la red SD-WAN experimentaron una menor tasa de perdida indicando una mayor robustez en la transmisión de datos.

Por otro lado, las topologías de la red MPLS mostraron una perdida paquetes considerable, lo que genera problemas de calidad en aplicaciones que requiere fiabilidad.

La pérdida de paquetes en las topologías podría ser causada por diversos factores, como la congestión de la red, errores en los dispositivos de red o problemas en la configuración de las rutas.

4.3.5. Tiempo de procesamiento

Figura 45 Tiempo de procesamiento



ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

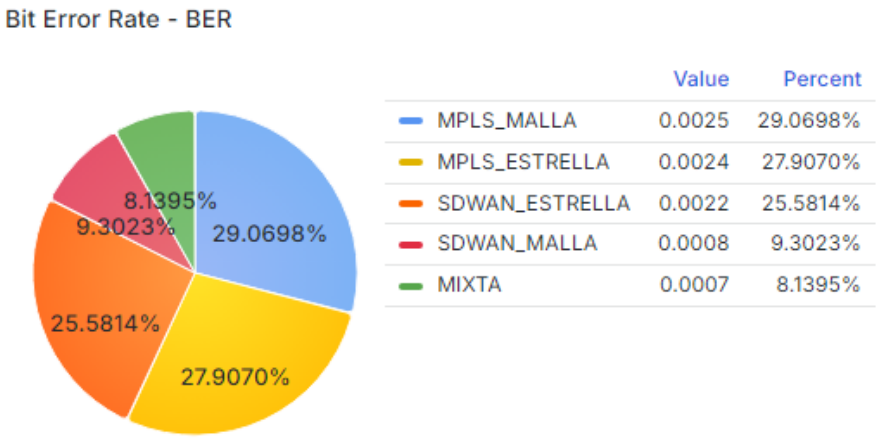
Los resultados del tiempo de procesamiento indica que la red mixta fue la más eficiente completando la prueba en 355 segundos (5.9 minutos). Le sigue la topología malla de la red SD-WAN con 366 segundos (6.1 minutos) y estrella con un tiempo de 400 segundos (6.7 minutos).

En cuanto a las topologías de la red MPLS, estrella y malla presentaron tiempos similares alrededor de 414 y 416 segundos (6.9 minutos).

Estos resultados demuestran que las topologías basadas en la tecnología SD-WAN especialmente la red mixta ofrece un rendimiento superior en términos de respuestas, lo que sugiere una mayor eficiencia en el procesamiento.

4.3.6. Bit error rate

Figura 46 Tasa de error de bits (BER)



ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

El resultado del BER revela que las topologías de la red MPLS presenta una tasa de error elevada.

La topología malla de la red MPLS registro 0.0025, seguido de la topología estrella (0.0024) y la topología estrella de la red SD-WAN (0.0022). Por el contrario, la topología malla de la red SD-WAN y la red mixta, presentaron el BER con valores de (0.0008 y 0.0007).

Estos resultados indica que las topologías de la red MPLS son más propensas a errores de bit lo que podría comprometer a la QoS (calidad de servicio).

4.3.7. Prueba de normalidad

Tabla 14 Resultados de la prueba de normalidad

Topología	Estadístico	gl	p-value
MIXTA	0.722	2188	0
MPLS_ESTRELLA	0.27	2156	0
MPLS_MALLA	0.517	2155	0
SDWAN_ESTRELLA	0.529	2160	0
SDWAN_MALLA	0.275	2185	0

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

Para determinar si los datos de latencia de las redes SD-WAN y MPLS seguían una distribución normal se aplicó la prueba de Shapiro-Wilk con una significancia del 5% a los resultados obtenidos en cada una de las topologías estrella y malla de la red MPLS, SD-WAN y la red Mixta.

Con base a los resultados obtenidos, en todos los casos el valor de **p-value** es **0**, lo cual es una evidencia contundente que los datos no se ajustan a una distribución normal y no es apropiado emplear pruebas estadísticas paramétricas como el ANOVA para comparar el rendimiento de ambas tecnologías, ya que estas pruebas asumen que los datos provienen de una distribución normal [42] [12].

4.4. Discusión

4.4.1. Identificación de herramientas, protocolos y controladores

La primera fase se centró en la identificación de las herramientas de redes necesarias para simular y emular redes SD-WAN y MPLS. Durante este contexto, la selección de GNS3 como software de emulación fue fundamental debido a su capacidad para replicar de manera realista el comportamiento de dispositivos de red en entornos simulados.

También se identificaron y compararon diferentes herramientas, protocolos y controladores, como Cisco vManage, Cisco IOS, en donde Fortigate que demostró ser adecuado para gestionar el tráfico en redes SD-WAN, mientras que RouterOS de Mikrotik resultó ser la elección idónea para MPLS, por su flexibilidad y accesibilidad en redes medianas y grandes.

La elección de herramientas no solo permitió crear un entorno controlado, sino también facilitó la replicación de condiciones reales de tráfico.

4.4.2. Diseño de escenarios

En la fase 2 se diseñaron 3 escenarios emulados para las redes MPLS, SD-WAN y una configuración mixta que combina ambas tecnologías. Estos escenarios se basaron en topologías estrella y malla, y se implementaron utilizando GNS3, RuterOs, FortiOs y máquinas virtuales con sistemas operativos Linux.

El diseño de las topologías fue un papel crucial en el rendimiento de la red, ya que afecta directamente la latencia, el ancho de banda, el jitter y la pérdida de paquetes. La elección de una topología estrella para la red MPLS y SD-WAN refleja las configuraciones tradicionales utilizadas en redes empresariales, mientras que las topologías malla proporcionaron un enfoque más robusto en cuanto a redundancia y estabilidad.

4.1. Análisis de resultados de la gestión del tráfico de red

Latencia

La latencia media total en la red SD-WAN fue de 300.34 ms y una media de 150.17 ms y en MPLS fue de 301.27 ms total y una media de 150.63 ms siendo similares. Sin embargo, estos resultados coinciden de los reportados por **Heredia Arias, J. O. (2022).** ***Implementación de una solución sd-wan para el uso eficiente de los recursos de red en su aplicación en la Empresa Asertia en el año 2021*** en donde evidencio una latencia media de 128 ms en el caso de MPLS y 81.94 ms para SD-WAN[12].

La similitud en la latencia obtenida podria estar relacionada con diversos factores como la congestión de red, tamaño de paquete, ancho de banda, configuración de los dispositivos y las características de las aplicaciones en ejecución, etc.

Perdida de paquetes

Los resultados totales de la pérdida de 55 paquetes de las topologías en la red SD-WAN en comparacion de MPLS con 99 paquetes, lo cual coincide con los hallazgos de **Heredia Arias, J. O. (2022).** ***Implementación de una solución sd-wan para el uso eficiente de los recursos de red en su aplicación en la Empresa Asertia en el año 2021*** [12], en donde obtuvo una perdida 33 paquetes en la red SD-WAN y 557 paquetes en MPLS.

Estos resultados sugieren que la red SD-WAN puede ser más eficiente en la gestión de tráfico, minimizando la pérdida de datos.

Prueba de normalidad

En los resultados de prueba de normalidad para las latencias de todas las topologías se obtuvo p-value de 0, indicando que los datos no siguen una distribución normal.

Esto es consistente con los hallazgos de **Heredia Arias, J. O. (2022).** ***Implementación de una solución sd-wan para el uso eficiente de los recursos de red en su aplicación en la Empresa Asertia en el año 2021***, quien tambien determino que los datos de latencia para los escenarios de la red MPLS y SD-WAN no se ajusta a una distribución normal [12].

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La red SD-WAN presento menores tiempos de latencia, perdida de paquetes en comparacion con MPLS, este comportamiento destaca que SD-WAN es una opción adecuada para aplicaciones que requiere tráfico en tiempo real.
- El protocolo ICMP ha demostrado ser una herramienta adecuada para analizar métricas de red y complementar este con otros protocolos o herramientas permitiría obtener información detallada sobre el estado y el tráfico de los dispositivos de red.
- El tiempo de procesamiento rapido en la red SD-WAN y Mixta en comparación con MPLS, reafirma su capacidad para manejar y optimizar el flujo de datos de manera eficiente.

5.2. Recomendaciones

- Implementar redes SD-WAN para aplicaciones sensibles a la latencia y pérdida de paquetes, como videoconferencias o tráfico en tiempo real, debido a su capacidad de gestión demostrada.
- Considerar el diseño de redes híbridas para aprovechar tanto la adaptabilidad de SD-WAN y la robustez de MPLS, optimizando así la capacidad de gestión de tráfico.
- Integrar herramientas de análisis predictivo, como modelos de IA(inteligencia artificial) para maximizar la eficiencia en la gestión del tráfico y anticiparse a demandas variables en el flujo de datos.

CAPÍTULO VI

BIBLIOGRAFÍA

REFERENCIAS

[1] Guzmán Vélez, D. M., & Cáceres Miranda, C. A. (2019). *Análisis del desempeño de redes definidas por software (SDN) frente a redes con arquitectura TCP/IP*. Quevedo - UTEQ. https://repositorio.uteq.edu.ec/handle/43000/3930

[2] Arlethv. (2023). *SD-WAN vs MPLS*. https://forum.huawei.com/enterprise/es/sd-wan-vs-mpls/thread/668658816134299648-667212882523336704

[3] Cusco Pérez, W. X., Cabrera Mejía, J. B., & Lugo García, J. (2022). *Análisis de las tecnologías SD-WAN usadas en Ecuador*. https://dialnet.unirioja.es/servlet/articulo?codigo=8637957#principal

[4] Romero Valdivieso, E. R., & Cuenca Tapia, J. P. (2020). *Implementación de SD-WAN Corporativo para el uso eficiente de las telecomunicaciones para el Holding Quito Motors*. https://dialnet.unirioja.es/servlet/articulo?codigo=7659364#principal

[5] Salazar Chacón, G. D. (2021). *Hybrid Networking SDN y SD-WAN: Interoperabilidad de arquitecturas de redes tradicionales y redes definidas por software en la era de la digitalización*. http://sedici.unlp.edu.ar/handle/10915/129910

[6] Carballo González, C. (2020). *SD-WAN, Una oportunidad para la transformación digital SD-WAN, An opportunity fot digital transformation*. https://www.researchgate.net/publication/343999151_sd-wan_una_oportunidad_para_la_transformacion_digital_sd-wan_an_opportunity_for_digital_transformation

[7] Sánchez Córtes, J. F., & Ochoa Velásquez, S. (2020). *Evaluación y análisis del rendimiento de una red de área extensa definida por software*. https://repository.udistrital.edu.co/handle/11349/25643

[8] s.f. (n.d.). *¿Qué es una SD-WAN? WAN definido por software - Intel*. https://www.intel.la/content/www/xl/es/communications/what-is-sd-wan.html

[9] Bowen Calero, G. K., & Patiño Maisanche, B. E. (2020). *Implementación de una red definida por software (Sdn) que permita brindar servicio de Voip Seguros*. https://repositorio.uteq.edu.ec/handle/43000/6102

[10] Sanchez, N. (2017). *Clasificación de las redes segun su cubertura WAN*. https://prezi.com/dgrbjplofzbl/clasificacion-de-las-redes-segun-su-cobertura/

[11] Jiménez de la Cueva, N. J. (2020). *Implementación de un prototipo de una red SDWAN (Software - Defined Wide Area Network) utilizando tecnología de Juniper Networks.* http://bibdigital.epn.edu.ec/handle/15000/21292

[12] Heredia Arias, J. O. (2022). *Implementación de una solución sd-wan para el uso eficiente de los recursos de red en su aplicación en la Empresa Asertia en el año 2021*. http://dspace.espoch.edu.ec/handle/123456789/18030

[13] GNS3. (2024). *Getting Started with GNS3 | GNS3 Documentation*. https://docs.gns3.com/docs/#introduction

[14] Vargas, J. C., Fajardo, S. S., & Gómez, E. J. (2019). Propuesta de métrica para evaluar los protocolos de enrutamiento y direccionamiento IP. *Avances Investigación En Ingeniería*, *16*(1 (Enero-Junio)), 111–116. https://doi.org/10.18041/1794-4953/AVANCES.1.5046

[15] Diego Marcelo, A. A. (2019). *Diseño y simulación de una red MPLS utilizando equipos Mikrotik y el emulador GNS3 en entornos PYMES*. http://dspace.udla.edu.ec/handle/33000/11528

[16] Fortinet. (2024). *Los FortiGate NGFW reforzados protegen la tecnología industrial y operativa (OT) | Fortinet*. https://www.fortinet.com/lat/products/rugged-firewall

[17] Systems Plus College Foundation. (2020). *Fortinet vs Palo alto ventajas desventajas.docx - FORTINET VS PALO ALTO Los firewalls de Fortinet y Palo Alto son altamente calificados por analistas | Course Hero*. https://www.coursehero.com/file/54515403/Fortinet-vs-Palo-alto-ventajas-desventajasdocx/

[18] Zhou, Y., Zhang, D., Gao, K., Sun, C., Cao, J., Wang, Y., Xu, M., & Wu, J. (2020). Newton. *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*, 295–308. https://doi.org/10.1145/3386367.3431298

[19] Huacón Salazar, L. Thalía., & Rosales Zambrano, J. M. (2018). *Sistema electronico para la deteccion de niveles de monoxido de carbono (CO) en la avenida 7 de octubre de la ciudad de Quevedo, que facilite la toma de decisiones del Departamento de Medio ambiente del GAD Municipal*. Quevedo: UTEQ. https://repositorio.uteq.edu.ec/handle/43000/2847

[20] ManageEngine. (2024). *Herramientas para analizar la red - ManageEngine NetFlow Analyzer*. https://www.manageengine.com/latam/netflow/herramienta-de-analisis-de-redes.html

[21] Guas Ojeda, D. S. (2004). *SABER UCV: Estudio de los protocolos de enrutamiento de Internet y su utilización en la arquitectura de red MPLS*. http://hdl.handle.net/10872/617

[22] Nedyalkov, I. (2023). Application of GNS3 to Study the Security of Data Exchange between Power Electronic Devices and Control Center. *Computers*, *12*(5), 101. https://doi.org/10.3390/computers12050101

[23] Rudakov, V., Timur, M., & Yedilkhan, A. (2023). Comparison of Time Series Databases. *2023 17th International Conference on Electronics Computer and Computation (ICECCO)*, 1–4. https://doi.org/10.1109/ICECCO58239.2023.10147153

[24] Praschl, C., Pritz, S., Krauss, O., & Harrer, M. (2022). A Comparison Of Relational, NoSQL and NewSQL Database Management Systems For The Persistence Of Time Series Data. *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 1–6. https://doi.org/10.1109/ICECCME55909.2022.9988333

[25] Alhilali, A. H. (2023). Design and implement a real-time network traffic management system using SNMP protocol. *Eastern-European Journal of Enterprise Technologies*, *5*(9 (125)), 35–44. https://doi.org/10.15587/1729-4061.2023.286528

[26] Rahman, T., Sumarna, S., & Nurdin, H. (2020). Analisis Performa RouterOS MikroTik pada Jaringan Internet. *INOVTEK Polbeng - Seri Informatika*, *5*(1), 178. https://doi.org/10.35314/isi.v5i1.1308

[27] Asamblea Nacional del Ecuador. (2008). Constitución de la República del Ecuador. *Registro Oficial*, *449*(20), 25–2021. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

[28] Asamblea Nacional de la Republica del Ecuador. (2015). *Tercer Suplemento-Registro Oficial Nº 439*. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Orgánica-de-Telecomunicaciones.pdf

[29] R, G., P, S., & Nagaraja, G. S. (2022). Analysis of SNMP Based Protocols in IoT and Real- World Scenarios. *International Journal for Research in Applied Science and Engineering Technology*, *10*(11), 1867–1871. https://doi.org/10.22214/ijraset.2022.47293

[30] Ngoc Hoan, N., Hoang Hiep, L., & Dinh Luc, D. (2022). Study to analyse, compare and evaluate the performance of next general firewalls: Case of Palo Alto and Fortigate Firewall. *Vinh University Journal of Science*, *51*(2A). https://doi.org/10.56824/vujs.2022nt08

[31] Miftah, Z. (2019). PENERAPAN SISTEM MONITORING JARINGAN DENGAN PROTOKOL SNMP PADA ROUTER MIKROTIK DAN APLIKASI DUDE STUDI KASUS STIKOM CKI. *Faktor Exacta*, *12*(1), 58. https://doi.org/10.30998/faktorexacta.v12i1.3481

[32] Velasco, A. R. H., Malla, E. E. G., Herrera, R. D. C. C., & Arévalo, F. D. M. (2023). Real-time monitoring and alerting system using Zabbix and Grafana software for wireless Internet access service management. *2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. https://doi.org/10.23919/CISTI58278.2023.10211432

[33] Melad, M., Musbah, M., & Almiqasbi, K. (2023). Evaluating Segment Routing Technology for MPLS-based Network. *E3S Web of Conferences*, *469*, 00075. https://doi.org/10.1051/e3sconf/202346900075

[34] Jalil, M. A. bin. (2023). The Study on the Importance of Various Network Topologies For Multinetwork Systems. *International Journal for Research in Applied Science and Engineering Technology*, *11*(12), 1380–1385. https://doi.org/10.22214/ijraset.2023.57613

[35] Gezer, A., & Warner, G. (2019). Exploitation of ICMP time exceeded packets for a large-scale router delay analysis. *˜The Œinternational Arab Journal of Information Technology*. https://www.semanticscholar.org/paper/Exploitation-of-ICMP-time-exceeded-packets-for-a-Gezer-Warner/350b0d2e2b453adeecedf2f53a0cc1a870bd2a1d

[36] Jose Lopez Vicario. (2019). *Presente y futuro de las redes WAN: SD-WAN y NFV*. https://openaccess.uoc.edu/bitstream/10609/87265/7/jdelolmobTFM0119memoria.pdf

[37] Mikrotik. (2024). *Software Specifications - RouterOS - MikroTik Documentation*. https://help.mikrotik.com/docs/display/ROS/Software+Specifications#SoftwareSpecifications-HardwareSupport

[38] Juniper Networks. (n.d.). *Medios de almacenamiento y motores de enrutamiento (Junos OS) | Junos OS | Juniper Networks*. https://www.juniper.net/documentation/mx/es/software/junos/junos-install-upgrade/topics/topic-map/storage-media-and-routing-engines.html

[39] Thuneibat, S. A., Al_Issa, H., & Ijjeh, A. (2015). A Simplified Model of Bit Error Rate Calculation. *Computer and Information Science*, *9*(1), 41. https://doi.org/10.5539/cis.v9n1p41

[40] Esteban C. Diego. (n.d.). *Ancho de banda y velocidad de transferencia (bps, Kbps, Mbps y Gbps) | by Diego Esteban C | Medium*. https://medium.com/@diego.coder/entendiendo-el-ancho-de-banda-y-la-velocidad-de-transferencia-bps-kbps-mbps-y-gbps-7a18f3abc406

[41] Andrew S. Tanaenbaum, & David J. Wetherall. (2012). *Redes de Computadoras 5th Edicion*. https://gc.scalahed.com/recursos/files/r161r/w25733w/redes_de_computadoras-freelibros-org.pdf

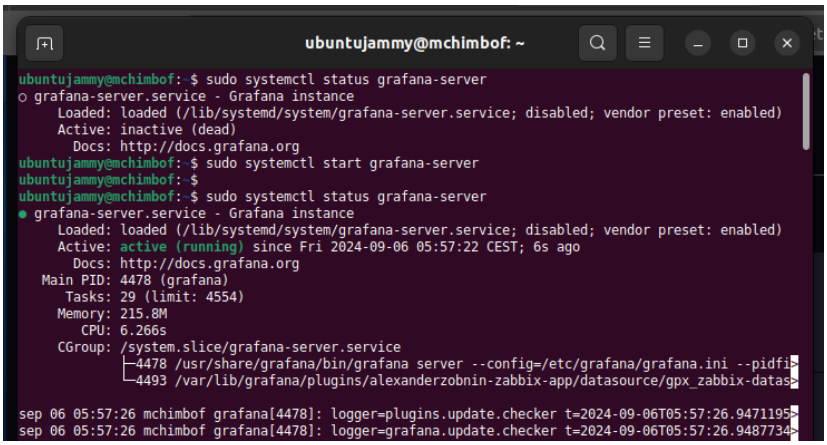
[42] Lynch, R. O. (1999). Introduction to Design and Analysis of Experiments. *Technometrics*, *41*(2), 170–170. https://doi.org/10.1080/00401706.1999.10485642

CAPÍTULO VII

ANEXOS

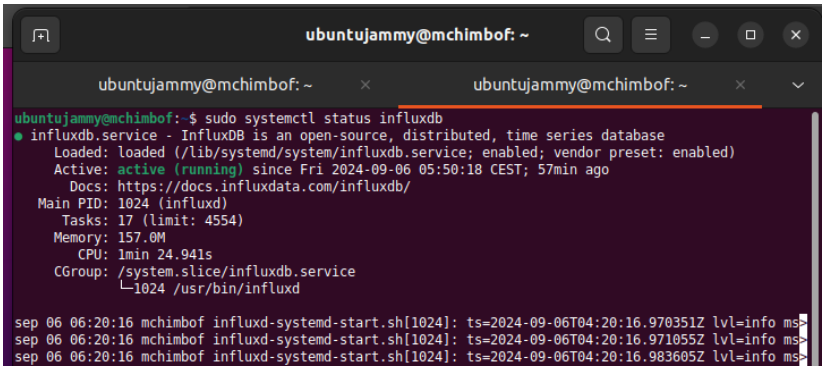
7.1. Estado de servicio de Grafana y InfluxDB

Figura 47 Estado de servicio de grafana



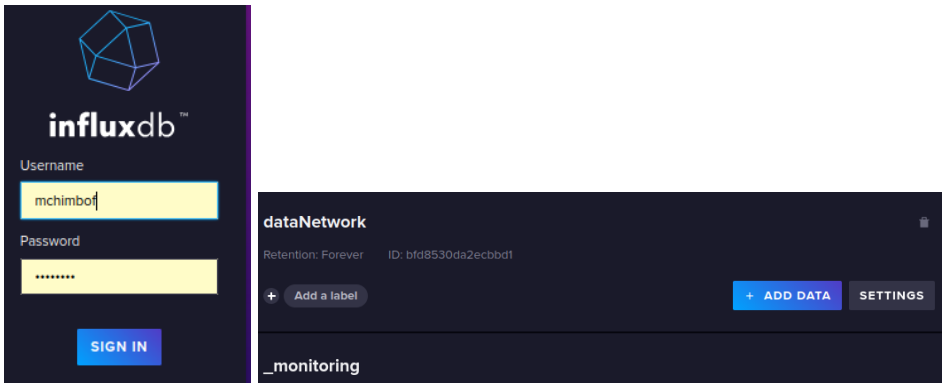
FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 48 Estado de servicio de InfluxDB



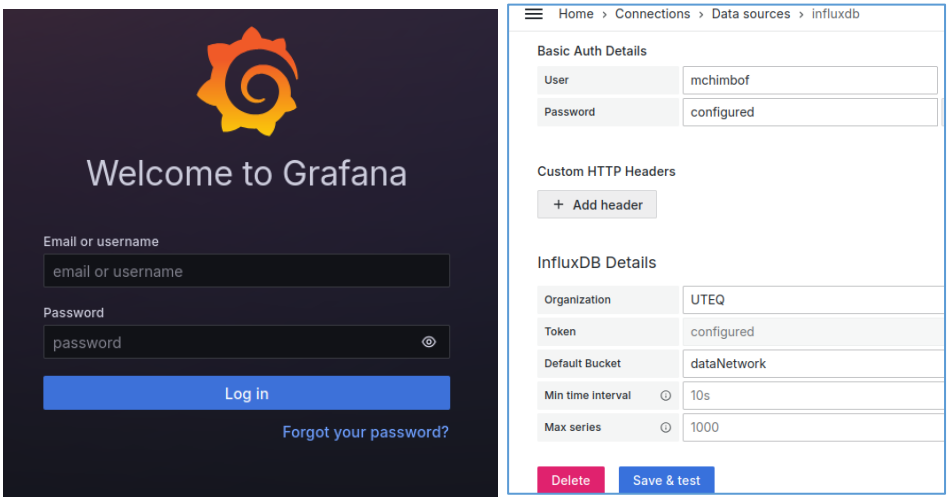
FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 49 Login de InfluxDB y visualización de la base de datos



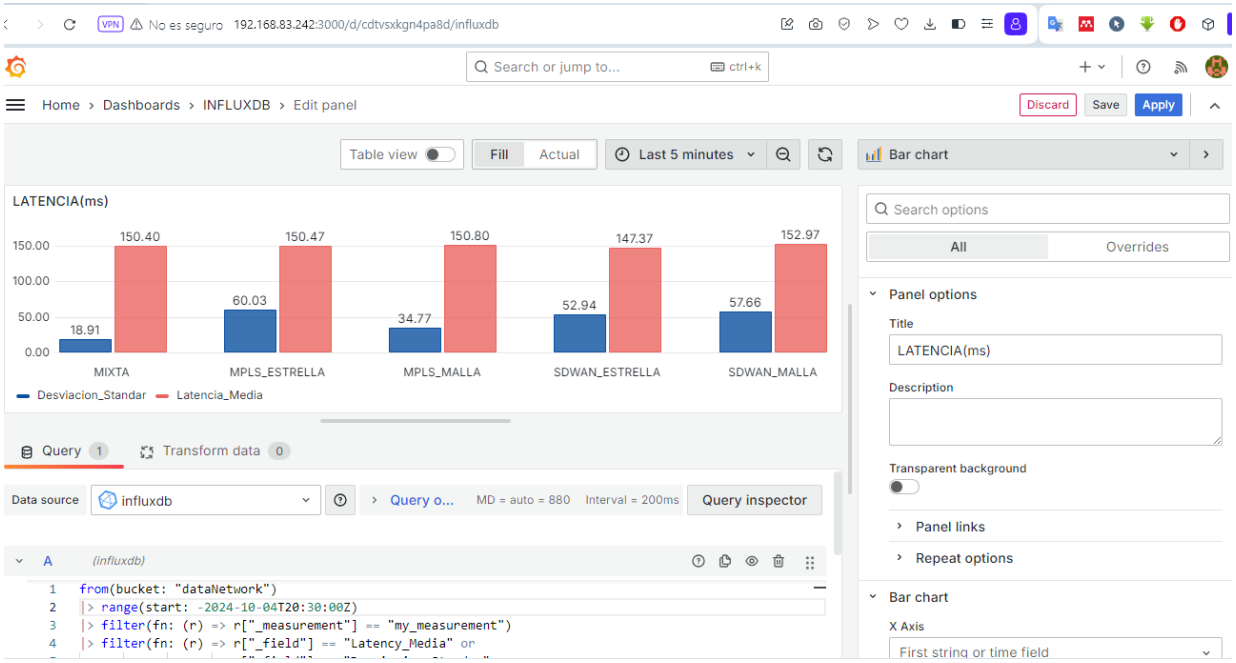
FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 50 Login de grafana y vinculación de la base de datos influxDB



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

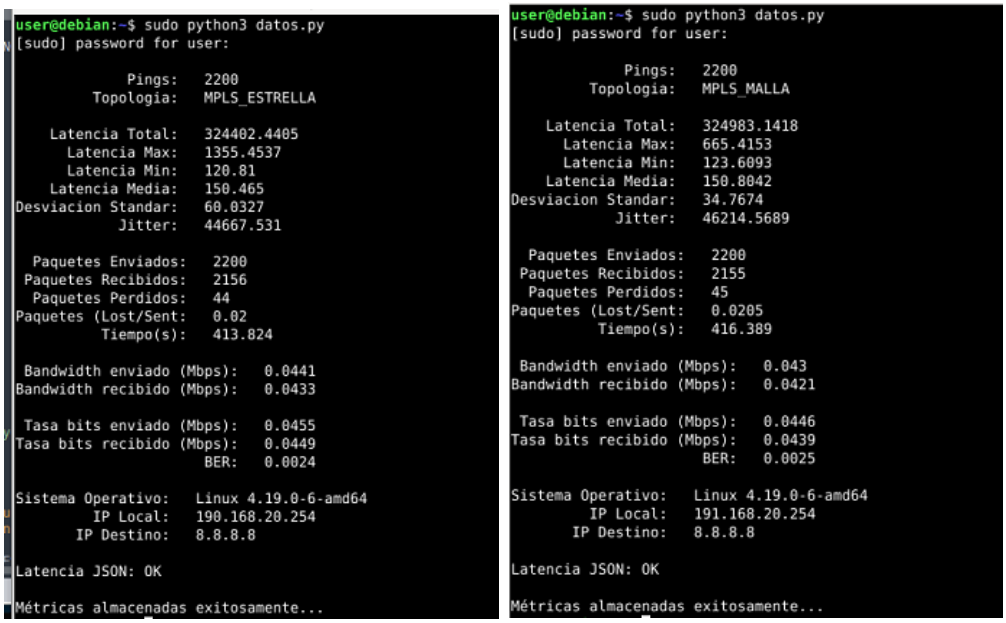
Figura 51 Consulta de datos influxDB desde grafana



ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

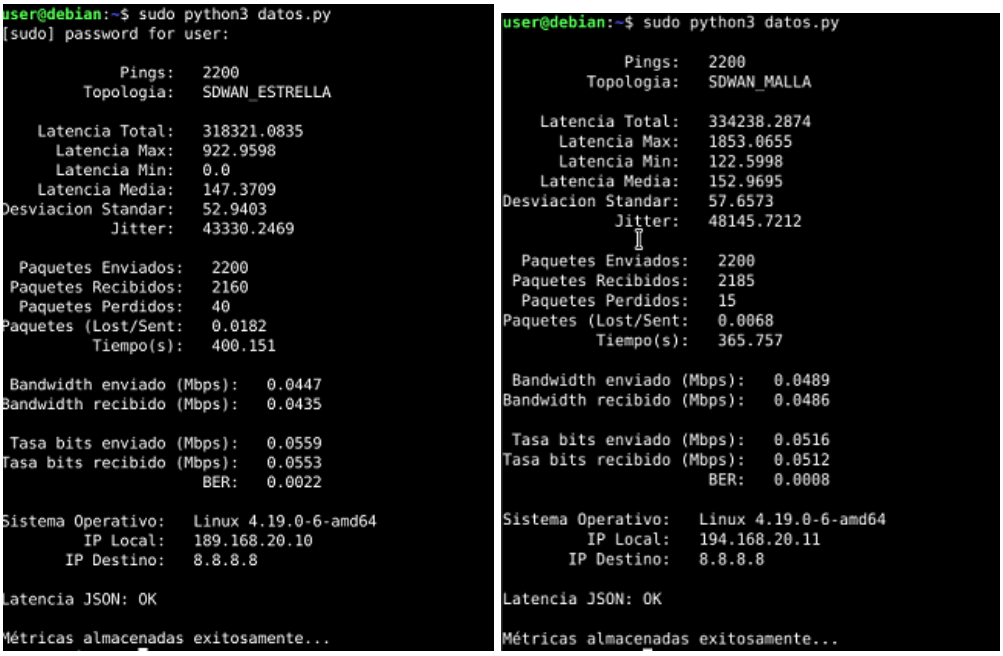
7.2. Recopilación y almacenamiento de métricas

Figura 52 Recopilación y envió de métricas de la red MPLS



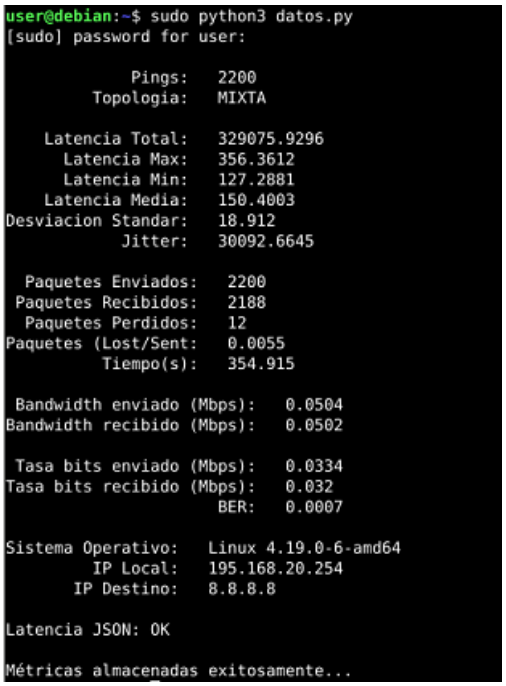
FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 53 Recopilación y envío de métricas de la red SD-WAN



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

Figura 54 Envió y recopilación de datos desde la red SD-WAN y MPLS



FUENTE: CHIMBO FOGACHO MARCO ISAIAS

7.3. Código fuente de Python

```
import influxdb_client
from influxdb_client.client.write_api import SYNCHRONOUS
from influxdb_client import Point
from ping3 import ping
import statistics, time, platform, socket, psutil, os, re, requests, json

#######################################  DATOS
objetivo = '8.8.8.8'
pings = 2200
timeout = 2  # segundos
topologia = 'SDWAN_MPLS'
size = 1400
decimal = 4
# URL de INFLUXDB, token, bucket y organización
url = "http://192.168.83.242:8086"
token                                                                    =
"P4HO0goq0hLqpIXSIoyLy3VPEEf05SfuVz_R_ryCiZn8X2a8tssNSioqBuZ3FVIvhGr_UyC9p9pSKsPGWw0y0g=="
bucket = "dataNetwork"
org = "UTEQ"
# Instancia de cliente INFLUXDB
influx_client = influxdb_client.InfluxDBClient(url=url, token=token, org=org)
write_api = influx_client.write_api(write_options=SYNCHRONOUS)
```

```
#####################################  FUNCIONES
def obtener_ip_local():
    resultado = os.popen("ip addr show ens5").read()
    ip_local = re.search(r'inet (\d+\.\d+\.\d+\.\d+)',resultado)
    if ip_local:
        return ip_local.group(1)
    else:
        return "Error"
def medir_trafico_inicial():
    net = psutil.net_io_counters()
    bytes_enviados = net.bytes_sent
    bytes_recibidos = net.bytes_recv
    return bytes_enviados, bytes_recibidos
def medir_trafico_final(bytes_enviados_inicial, bytes_recibidos_inicial):
    net = psutil.net_io_counters()
    bytes_enviados_final = net.bytes_sent
    bytes_recibidos_final = net.bytes_recv
    bytes_enviados = bytes_enviados_final - bytes_enviados_inicial
    bytes_recibidos = bytes_recibidos_final - bytes_recibidos_inicial
    return bytes_enviados, bytes_recibidos
def convertir_megabytes(bytes_segundo):
    return bytes_segundo / (1024 * 1024)
def convertir_megabits(bytes_segundo):
    return (bytes_segundo * 8) / (1024 * 1024)
def test_latencia(host, count, timeout,size):
    latencys = []
    enviado = 0
    recibido = 0
    start_time = time.time()
    for i in range(count):
        latencia = ping(host, timeout=timeout,size=size)
        enviado += 1
        if latencia is not None:
            latencys.append(round(latencia * 1000,decimal))  # Conversion a milisegundos
            recibido += 1
    end_time = time.time()
    tiempo = round((end_time - start_time),decimal-1)  # segundos
    # paquetes
    perdido = enviado - recibido
    porcentaje = (perdido / enviado)
    porcentaje = round(porcentaje,decimal)
    if latencys:
        lat_total = round(sum(latencys),decimal)
        lat_max = max(latencys)
        lat_min = float(min(latencys))
        lat_media = round(statistics.mean(latencys),decimal)
        desv_stand = round(statistics.stdev(latencys),decimal)
        return (lat_total, lat_max, lat_min, lat_media, desv_stand, enviado, recibido, perdido, porcentaje,
tiempo, latencys)
    else:
        return None
def tasa_de_bits(host, pings, timeout,size):
  bytes_enviados_inicial, bytes_recibidos_inicial = medir_trafico_inicial()
  (lat_total,lat_max,lat_min,lat_media,desv_stand,enviado,recibido,perdido,porcentaje,tiempo,latencys)
  = test_latencia(objetivo,pings,timeout,size)
  tiempo_transcurrido = tiempo
```

```
    bytes_enviados, bytes_recibidos = medir_trafico_final(bytes_enviados_inicial,
bytes_recibidos_inicial)
    # tasa de bits en Mbps
    tasa_bits_enviados = round(convertir_megabits(bytes_enviados / tiempo_transcurrido),decimal)
    tasa_bits_recibidos = round(convertir_megabits(bytes_recibidos / tiempo_transcurrido),decimal)
    return (tasa_bits_enviados,tasa_bits_recibidos)
def test_ber(bytes_enviados_final, bytes_recibidos_final, perdido, size):
    bytes_enviados = bytes_enviados_final*8
    bytes_recibidos = bytes_recibidos_final*8
    error =  perdido * size
    if bytes_enviados ==0:
        return 0.0
    ber = error/bytes_enviados
    return round(ber,decimal)
def latencys_json(lista):
     lista_json = json.dumps(lista)
     lista_origin = json.loads(lista_json)
     return (lista_json)
def test_jitter(latencys):
    jitter_total = 0
    for i in range(1, len(latencys)):
        jitter = abs(latencys[i] - latencys[i-1])
        jitter_total += jitter
    return round(jitter_total, decimal)
################################     EJECUCION DE FUNCIONES
# Tráfico inicial
bytes_enviados_inicial, bytes_recibidos_inicial = medir_trafico_inicial()
(lat_total,lat_max,lat_min,lat_media,desv_stand,enviado,recibido,perdido,porcentaje,tiempo,latencys)=t
est_latencia(objetivo,pings,timeout,size)
# Tráfico final
bytes_enviados_final, bytes_recibidos_final = medir_trafico_final(bytes_enviados_inicial,
bytes_recibidos_inicial)
# Bandwidth consumido en bytes por segundo (Bps)
bandwidth_enviado_bps = bytes_enviados_final / tiempo  # Bytes por segundo enviados
bandwidth_recibido_bps = bytes_recibidos_final / tiempo  # Bytes por segundo recibidos
# Bandwidth Megabits por segundo (Mbps)
bandwidth_enviado_Mbps =  round(convertir_megabits(bandwidth_enviado_bps),decimal)
bandwidth_recibido_Mbps = round(convertir_megabits(bandwidth_recibido_bps),decimal)
(ttx_bits, trx_bits) = tasa_de_bits(objetivo, pings, timeout,size)
ber = test_ber(bytes_enviados_final, bytes_recibidos_final, perdido,size)
latencias_json = latencys_json(latencys)
jitter = test_jitter(latencys)
################################## PRESENTACION
print('            Pings:  ', pings)
print('        Topologia:  ', topologia)
print('')
print('    Latencia Total:  ', lat_total)
print('      Latencia Max:  ', lat_max)
print('      Latencia Min:  ', lat_min)
print('    Latencia Media:  ', lat_media)
print('Desviacion Standar:  ', desv_stand)
print('           Jitter:  ', jitter)
print('')
print('  Paquetes Enviados:  ', enviado)
print(' Paquetes Recibidos:  ', recibido)
print('  Paquetes Perdidos:  ', perdido)
```

```
print('Paquetes (Lost/Sent:  ', porcentaje)
print('          Tiempo(s):  ', tiempo)
print()
print(' Bandwidth enviado (Mbps):  ', bandwidth_enviado_Mbps)
print('Bandwidth recibido (Mbps):  ', bandwidth_recibido_Mbps)
print()
print(" Tasa bits enviado (Mbps):  ",ttx_bits)
print("Tasa bits recibido (Mbps):  ",trx_bits)
print("                    BER:  ",ber)
print()
sistema_operativo = platform.system() + " " + platform.release()
ip_local = obtener_ip_local()
print("Sistema Operativo:  ", sistema_operativo)
print("         IP Local:  ", ip_local)
print("       IP Destino:  ", objetivo)
if latencias_json:
   print("Latencia JSON: OK")
######################################## ALMACENAR METRICAS EN INFLUXDB
if latencys:
   point = Point("my_measurement") \
      .tag('location', topologia) \
      .field('IP', objetivo) \
      .field('Topologia', topologia) \
      .field('IP_Local', ip_local) \
      .field('Pings', pings) \
      .field('Tiempo_Espera', timeout) \
      .field('System', sistema_operativo) \
      .field('Latency_Total', lat_total) \
      .field('Latency_Max', lat_max) \
      .field('Latency_Min', lat_min) \
      .field('Latency_Media', lat_media) \
      .field('Desviacion_Standar', desv_stand) \
      .field('Jitter', jitter) \
      .field('Paquetes_Enviados', enviado) \
      .field('Paquetes_Recibidos', recibido) \
      .field('Paquetes_Perdidos', perdido) \
      .field('Perdida_Porcentaje', porcentaje) \
      .field('Tiempo_Requerido', tiempo) \
      .field('Bandwidth_Enviado_Mbps', bandwidth_enviado_Mbps) \
      .field('Bandwidth_Recibido_Mbps', bandwidth_recibido_Mbps)\
      .field('Tasa_Bits_TX', ttx_bits) \
      .field('Tasa_Bits_RX', trx_bits) \
      .field('ICMP_Size', size) \
      .field('Bit_Error_Rate', ber) \
      .field('Lista_Latencia', latencias_json)
   try:
      write_api.write(bucket=bucket, org=org, record=point)
      print("\nMétricas almacenadas exitosamente...")
   except Exception as e:
      print(f"Error al almacenar métricas: {e}")
   finally:
      influx_client.close()
else:
   print("Error de metricas")
```

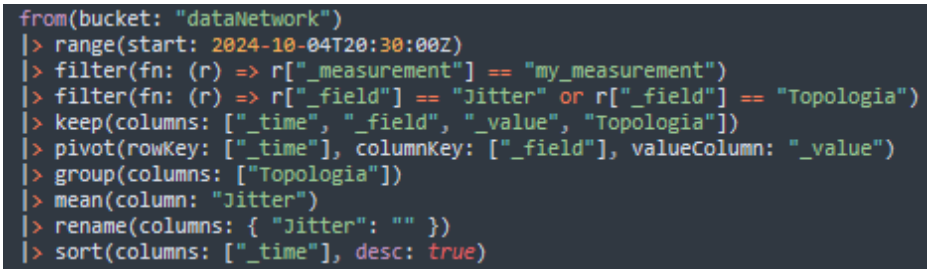
7.4. Código InfluxQL

Figura 55 Consulta influxQL de latencia media y desviación estándar

```
from(bucket: "dataNetwork")
|> range(start: 2024-10-04T20:30:00Z)
|> filter(fn: (r) => r["_measurement"] == "my_measurement")
|> filter(fn: (r) => r["_field"] == "Latency_Media" or
                     r["_field"] == "Desviacion_Standar" or
                     r["_field"] == "Topologia")
|> group(columns: ["Topologia", "_field"])
|> pivot(rowKey: ["_time"], columnKey: ["_field"], valueColumn: "_value")
|> map(fn: (r) => ({
      r with
      Latencia_Media: r.Latency_Media,
      Desviacion_Standar: r.Desviacion_Standar,
      Etiqueta: r.Topologia
}))
|> keep(columns: ["Etiqueta", "Latencia_Media", "Desviacion_Standar"])
|> sort(columns: ["Etiqueta"], desc: false)
```

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

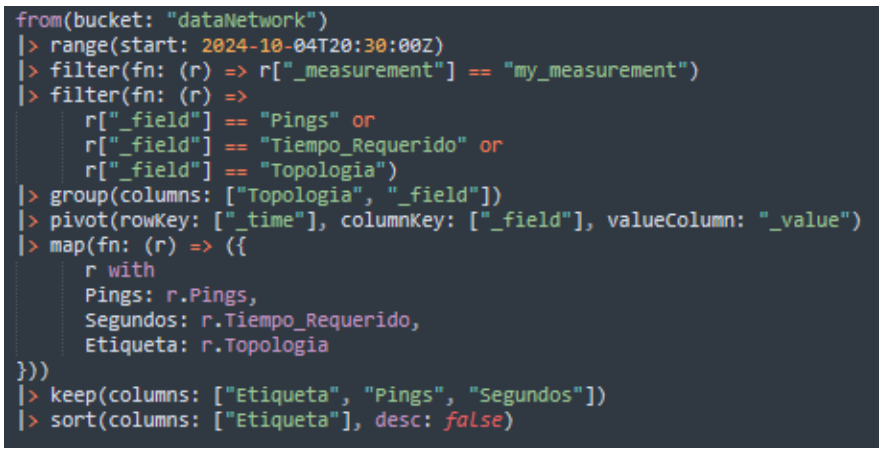
Figura 56 Consulta InfluxQL de jitter



```
from(bucket: "dataNetwork")
|> range(start: 2024-10-04T20:30:00Z)
|> filter(fn: (r) => r["_measurement"] == "my_measurement")
|> filter(fn: (r) => r["_field"] == "Jitter" or r["_field"] == "Topologia")
|> keep(columns: ["_time", "_field", "_value", "Topologia"])
|> pivot(rowKey: ["_time"], columnKey: ["_field"], valueColumn: "_value")
|> group(columns: ["Topologia"])
|> mean(column: "Jitter")
|> rename(columns: { "Jitter": "" })
|> sort(columns: ["_time"], desc: true)
```

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

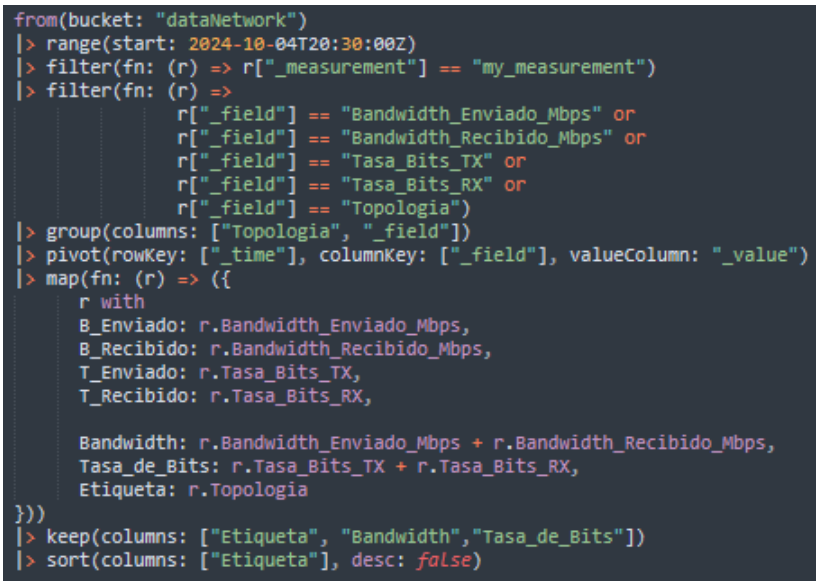
Figura 57 Consulta influxQL del tiempo de procesamiento



```
from(bucket: "dataNetwork")
|> range(start: 2024-10-04T20:30:00Z)
|> filter(fn: (r) => r["_measurement"] == "my_measurement")
|> filter(fn: (r) =>
      r["_field"] == "Pings" or
      r["_field"] == "Tiempo_Requerido" or
      r["_field"] == "Topologia")
|> group(columns: ["Topologia", "_field"])
|> pivot(rowKey: ["_time"], columnKey: ["_field"], valueColumn: "_value")
|> map(fn: (r) => ({
      r with
      Pings: r.Pings,
      Segundos: r.Tiempo_Requerido,
      Etiqueta: r.Topologia
}))
|> keep(columns: ["Etiqueta", "Pings", "Segundos"])
|> sort(columns: ["Etiqueta"], desc: false)
```

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

Figura 58 Consulta influxQL del ancho de banda y tasa de transferencia

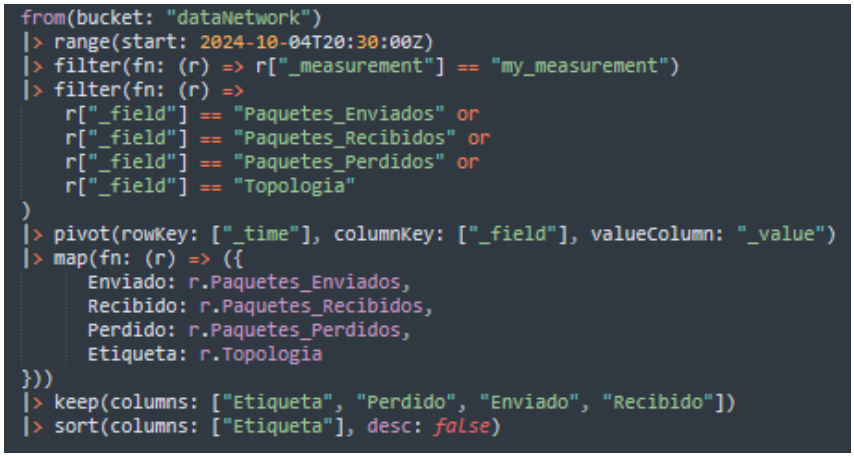


```
from(bucket: "dataNetwork")
|> range(start: 2024-10-04T20:30:00Z)
|> filter(fn: (r) => r["_measurement"] == "my_measurement")
|> filter(fn: (r) =>
                r["_field"] == "Bandwidth_Enviado_Mbps" or
                r["_field"] == "Bandwidth_Recibido_Mbps" or
                r["_field"] == "Tasa_Bits_TX" or
                r["_field"] == "Tasa_Bits_RX" or
                r["_field"] == "Topologia")
|> group(columns: ["Topologia", "_field"])
|> pivot(rowKey: ["_time"], columnKey: ["_field"], valueColumn: "_value")
|> map(fn: (r) => ({
      r with
      B_Enviado: r.Bandwidth_Enviado_Mbps,
      B_Recibido: r.Bandwidth_Recibido_Mbps,
      T_Enviado: r.Tasa_Bits_TX,
      T_Recibido: r.Tasa_Bits_RX,

      Bandwidth: r.Bandwidth_Enviado_Mbps + r.Bandwidth_Recibido_Mbps,
      Tasa_de_Bits: r.Tasa_Bits_TX + r.Tasa_Bits_RX,
      Etiqueta: r.Topologia
}))
|> keep(columns: ["Etiqueta", "Bandwidth","Tasa_de_Bits"])
|> sort(columns: ["Etiqueta"], desc: false)
```

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

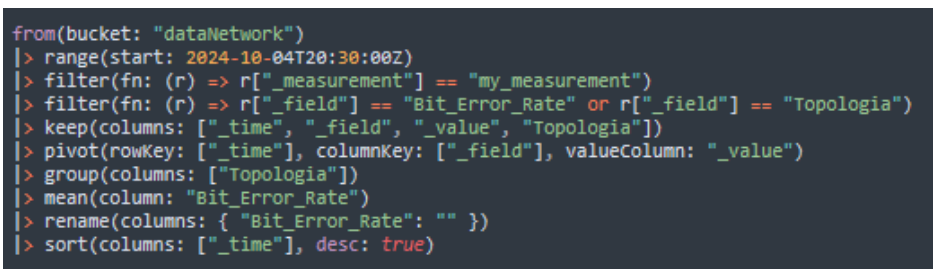
Figura 59 Consulta influxQL de la transmisión de paquetes



```
from(bucket: "dataNetwork")
|> range(start: 2024-10-04T20:30:00Z)
|> filter(fn: (r) => r["_measurement"] == "my_measurement")
|> filter(fn: (r) =>
    r["_field"] == "Paquetes_Enviados" or
    r["_field"] == "Paquetes_Recibidos" or
    r["_field"] == "Paquetes_Perdidos" or
    r["_field"] == "Topologia"
)
|> pivot(rowKey: ["_time"], columnKey: ["_field"], valueColumn: "_value")
|> map(fn: (r) => ({
      Enviado: r.Paquetes_Enviados,
      Recibido: r.Paquetes_Recibidos,
      Perdido: r.Paquetes_Perdidos,
      Etiqueta: r.Topologia
}))
|> keep(columns: ["Etiqueta", "Perdido", "Enviado", "Recibido"])
|> sort(columns: ["Etiqueta"], desc: false)
```

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS

Figura 60 Consulta influxQL del bit error rate



```
from(bucket: "dataNetwork")
|> range(start: 2024-10-04T20:30:00Z)
|> filter(fn: (r) => r["_measurement"] == "my_measurement")
|> filter(fn: (r) => r["_field"] == "Bit_Error_Rate" or r["_field"] == "Topologia")
|> keep(columns: ["_time", "_field", "_value", "Topologia"])
|> pivot(rowKey: ["_time"], columnKey: ["_field"], valueColumn: "_value")
|> group(columns: ["Topologia"])
|> mean(column: "Bit_Error_Rate")
|> rename(columns: { "Bit_Error_Rate": "" })
|> sort(columns: ["_time"], desc: true)
```

ELABORADO POR: CHIMBO FOGACHO MARCO ISAIAS