PROYECTO DE TITULACIÓN

Carrera de Ingeniería en Tecnologías de la Información

TEMA: Análisis comparativo del impacto de las redes tradicionales y VXLAN en el rendimiento de redes empresariales.

AUTOR: Espinosa Vinueza, Jordan Enrique

TUTOR: Ing. Núñez Agurto, Alberto Daniel, Mgtr.

Santo Domingo, 28 de Febrero del 2024

Reporte de verificación de contenido

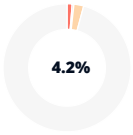
Plagiarism and AI Content Detection Report

EspinosaJordan_TesisCorreción.pdf

Scan details

Scan time:	Total Pages:	Total Words:
March 4th, 2024 at 12:13 UTC	52	12886

Plagiarism Detection



Types of plagiarism		Words
Identical	1.2%	160
Minor Changes	0.4%	52
Paraphrased	2.4%	305
Omitted Words	4.6%	591

AI Content Detection

Text coverage		Words
AI text	0%	0
Human text	100%	12295

Learn more

Alerts: (1)

Cross Language: Same Document Language

Submitted language and cross-language text are the same language. No credits were used.

2/5 Severity

Plagiarism Results: (16)

Your File — 3.1%

en el ́ ambito de las tecnolog ́ ıas de la informacı ́ on.

Description: Hybrid Networking SDN y SD-WAN: Interoperabilidad de arq... — 0.9%

https://repositoriosdigitales.mincyt.gob.ar/vufind/record/sedici_8b86c4723646d9f6be20626ae548c3d9

Skip to content Argentina.gob.ar Presidencia de la Nación ...

Hybrid Networking SDN y SD-WAN: Interoperabilidad de Arquitecturas d... — 0.9%

https://libros.unlp.edu.ar/index.php/unlp/catalog/book/2207

Crear una cuenta Iniciar sesión ...

Departamento de Ciencias de la Computación

Carrera de Ingeniería en Tecnologías de la Información

Certificación

Certifico que el trabajo de integración curricular: "**Análisis comparativo del impacto de las redes tradicionales y VXLAN en el rendimiento de redes empresariales**" fue realizado por el señor **Espinosa Vinueza, Jodan Enrique,** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Santo Domingo, 01 de marzo del 2024

Firma:

Firmado electrónicamente por:
ALBERTO DANIEL
NUNEZ AGURTO

.....

Núñez Agurto, Alberto Daniel

C. C: 1716572548

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Ciencias de la Computación

Carrera de Ingeniería en Tecnologías de la Información

Responsabilidad de Autoría

Yo, **Espinosa Vinueza, Jordan Enrique**, con cédula de ciudadanía n° 2350637217, declaro/declaramos que el contenido, ideas y criterios del trabajo de integración curricular: **Análisis comparativo del impacto de las redes tradicionales y VXLAN en el rendimiento de redes empresariales** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Santo Domingo, 01 de marzo del 2024

Firma:

.....

Espinosa Vinueza, Jordan Enrique

C.C.: 2350637217

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Ciencias de la Computación

Carrera de Ingeniería en Tecnologías de la Información

Autorización de Publicación

Yo **Espinosa Vinueza, Jordan Enrique**, con cédula de ciudadanía n° 2350637217, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **Análisis comparativo del impacto de las redes tradicionales y VXLAN en el rendimiento de redes empresariales** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Santo Domingo, 01 de marzo del 2024

Firma:

.....

Espinosa Vinueza, Jordan Enrique
C.C.: 2350637217

DEDICATORIA

Dedico este título académico en primer lugar a Dios, pues es Él quien me ha sostenido hasta el día de hoy.

A mis padres, Luis Enrique Espinosa Males y Dolores Isabel Vinueza Jingo, quienes, con su amor, paciencia y compañía han sido la inspiración de este sueño. Como su hijo, anhelo expresar mi más profundo cariño por sus enseñanzas y valores que han inculcado a lo largo de mi vida. A mi hermana, Dorcas Damaris Espinosa Vinueza, quien ha contribuido en la formación de este sueño y espero, como su hermano, sembrar en ella aprendizajes útiles para toda su vida.

Finalmente, dedico este trabajo a mí mismo, reconociendo que el esfuerzo y la valentía que empleé al iniciar esta carrera fueron fundamentales para culminar este anhelo. Quiero dejar constancia de que los sueños se materializan con el apoyo y el amor de aquellos que nos rodean.

Espinosa Vinueza, Jordan Enrique

AGRADECIMIENTO

Agradezco profundamente a mis padres Luis Enrique Espinosa Males y Dolores Isabel Vinueza Jingo por ser ese apoyo emocional y económico constante que me permitió alcanzar este sueño que me propuse cuatro años atrás, graduarme de la universidad. De ellos, he aprendido sobre la constancia, el respeto y el amor; cada una de sus enseñanzas esta arraigada en mi corazón.

Expreso mi gratitud hacia mi tutor, el Ing. Alberto Daniel Nuñez Agurto, quien siempre mostró predisposición para enseñar, ayudar y resolver cualquier duda. Compartió su conocimiento con humildad, lo cual me permitió culminar este trabajo con éxito.

Asimismo, agradezco a la Universidad de las Fuerzas Armadas ESPE por ser la institución que me acogió para cumplir este sueño; estoy orgulloso de formar parte de esta maravillosa institución.

Además, quiero expresar mi agradecimiento a mis más sinceros amigos Hector Cedeño, Luis Paredez, Julissa Rentería, Liseth Poma, David Sangucho y Melannie Cisneros. Su compañía durante este recorrido académico estuvo lleno de camaradería y honestidad. Sus consejos y ayuda me permiten estar hoy aquí, agradeciéndoles sinceramente.

Finalmente, quiero agradecer a mi mejor amiga Hanashi Haidy Gualapuro Burga por siempre estar a mi lado, su apoyo y compañía fue de gran ayuda para nunca rendirme y poder culminar esta etapa de mi vida.

Espinosa Vinueza, Jordan Enrique

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En la actualidad, los entornos empresariales dependen cada vez más de la tecnología y la comunicación, por lo que la evaluación del rendimiento de las redes se vuelve crucial. Este estudio se centra en comparar las redes tradicionales con la tecnología VXLAN para determinar su impacto en el rendimiento de las redes empresariales. Utilizando la metodología PPDIOO, se estructuró y guió el proceso de análisis y mejora de la red. Esta metodología se utiliza para asegurar una implementación efectiva y óptima en cada etapa del ciclo de vida de la red empresarial. Además, se llevó a cabo la configuración de los dispositivos de red utilizando routers MikroTik, que desempeñaron un papel central en las topologías utilizadas en el estudio, con el sistema operativo RouterOS. Durante el estudio, se realizaron pruebas detalladas de ancho de banda, latencia y tasa de transferencia en entornos simulados, utilizando herramientas como hping, iperf y Wireshark. Estas herramientas permiten medir el tráfico, el ancho de banda y la latencia de manera precisa, proporcionando información valiosa para entender el comportamiento de la red en diferentes escenarios. Los resultados muestran que VXLAN ofrece un rendimiento superior en términos de latencia, aunque las redes tradicionales superan ligeramente en ancho de banda. Este hallazgo resalta la importancia de considerar diversos factores al elegir entre estas tecnologías, asegurando así una implementación que se alinee con las necesidades específicas de la red empresarial.

Palabras clave: Ancho de banda, Latencia, Tasa de transferencia, VXLAN, RouterOS

ABSTRACT

Today's business environments are increasingly dependent on technology and communication, making the evaluation of network performance crucial. This study focuses on comparing traditional networks with VXLAN technology to determine its impact on enterprise network performance. Using the PPDIOO methodology, the network analysis and improvement process was structured and guided. This methodology is used to ensure effective and optimal implementation at each stage of the enterprise network lifecycle. In addition, configuration of the network devices was carried out using MikroTik routers, which played a central role in the topologies used in the study, running the RouterOS operating system. During the study, detailed bandwidth, latency and transfer rate tests were performed in simulated environments, using tools such as hping, iperf and Wireshark. These tools allow traffic, bandwidth and latency to be measured accurately, providing valuable information for understanding network behavior in different scenarios. The results show that VXLAN offers superior performance in terms of latency, although traditional networks slightly outperform in bandwidth. This finding highlights the importance of considering various factors when choosing between these technologies, thus ensuring a deployment that aligns with the specific needs of the enterprise network.

Keywords: Bandwidth, Latency, Transfer Rate, VXLAN, RouterOS

I. Introducción y estado del arte

A. Introducción

La conectividad eficiente y el rendimiento de la red son aspectos fundamentales en el actual entorno empresarial, marcado por una creciente dependencia de la tecnología y la comunicación [1]. En este contexto, surge la necesidad de evaluar exhaustivamente el impacto que tienen las redes tradicionales en comparación con la nueva tecnología VXLAN (Virtual Extensible Local Area Network). La creación de escenarios de red empresarial que proporcionen flexibilidad, mejores características de segmentación y escalabilidad se vuelve crucial para adaptarse a la inminente demanda de servicios y aplicaciones en constante evolución.

La mejora en el rendimiento de las redes empresariales conlleva una minuciosa reflexión sobre las tecnologías disponibles y aplicables. VXLAN aparece como una respuesta que supera las múltiples limitaciones de las redes tradicionales al posibilitar la superposición de redes de capa 2 sobre las de capa 3, permitiendo así una amplia variedad de posibilidades en cuanto a la segmentación, sin dejar de lado el aislamiento de tráfico. Por otro lado, aunque posea enormes beneficios, aún se puede identificar una brecha en la comprensión sobre cómo VXLAN influye en el rendimiento de las redes empresariales en comparación con las redes tradicionales.

El análisis comparativo entre las redes tradicionales y VXLAN es crucial para abordar esta pregunta fundamental y mantener los altos estándares de rendimiento en las infraestructuras de red empresarial. Este estudio se centra en explorar cómo las redes tradicionales y VXLAN impactan el rendimiento de las redes empresariales, enfocándose en aspectos clave como la eficacia en la distribución y gestión del tráfico, la escalabilidad y la capacidad de adaptación a entornos empresariales dinámicos.

La evaluación minuciosa de estos aspectos proporciona una comprensión más integral de las implicaciones prácticas de la adopción de VXLAN en comparación con las redes tradicionales, facilitando así la toma de decisiones informadas en la creación y distribución de escenarios de red empresariales.

Para abordar este tema, se llevará a cabo un proceso estructurado en diversas etapas utilizando la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar). La emulación de una única topología en GNS3, una herramienta de emulación ampliamente

utilizada, será el eje central de este análisis comparativo. Esta topología será utilizada para simular tanto redes tradicionales basadas en EoIP (Ethernet over IP) como la implementación de VXLAN. Este enfoque práctico permitirá una evaluación específica y detallada de cómo VXLAN influye en aspectos específicos del rendimiento de las redes empresariales en comparación con las soluciones tradicionales. Al comprender las ventajas y desventajas asociadas con VXLAN, este estudio proporcionará a las empresas una base sólida para la toma de decisiones informadas en la implementación de infraestructuras de red, adaptadas a sus necesidades operativas y de expansión en un entorno empresarial dinámico.

B. Estado del Arte

Desde hace diez años, las infraestructuras de redes empresariales han experimentado cambios innovadores debido a la adopción de nuevos modelos y protocolos de red. Las redes tradicionales, en el ámbito empresarial, han sido la base de las infraestructuras para las telecomunicaciones. Estas redes, que se basan en protocolos como Ethernet y VLAN, son muy populares, principalmente porque proporcionan alta flexibilidad y eficacia, ofreciendo conectividad confiable y segmentación de tráfico mediante modelos de red convencionales.

En el trabajo de [2], se materializa la implementación de redes híbridas SDN y SD-WAN, focalizándose en la interoperabilidad entre arquitecturas de redes tradicionales y definidas por software en la era digital. [2] destaca la rápida evolución de las redes de datos empresariales en la última década, impulsada por la adopción de modelos basados en la nube, contenedores y microservicios. Estos avances representan una respuesta a las crecientes necesidades de flexibilidad, eficiencia y reducción de costos en el ámbito de las Tecnologías de la Información.

Además, se subraya la importancia crítica de las redes de datos en la transmisión de información en cualquier momento y lugar, especialmente en un contexto marcado por la pandemia de COVID-19. Durante esta crisis, se ha evidenciado la importancia de la virtualización, la transformación digital y la seguridad en la transferencia de datos. En este sentido, los datos emergen como el activo intangible más significativo del siglo XXI, reafirmando la necesidad de una infraestructura de red que sea ágil, adaptable y segura en todo momento.

Por otro lado, con el aumento del tamaño y complejidad de las empresas, junto con la introducción de nuevas aplicaciones y servicios, se añade una carga adicional de envío y

procesamiento a la red. Esto genera dificultades en la administración, monitoreo y configuración. También surgen problemas significativos, como la limitada escalabilidad y congestión en el tráfico. En la investigación de [3] se destaca la importancia de implementar VXLAN en entornos empresariales para mejorar la eficiencia y disponibilidad de la red. El investigador propone un nuevo diseño y simulación de red basado en la implementación de redes definidas por software VXLAN, con el objetivo de crear una red altamente disponible para el Departamento Nacional de Planeación de Colombia.

Además, [3] destaca que la adopción de VXLAN abre nuevas posibilidades para la mejora del rendimiento y la escalabilidad de la infraestructura de red empresarial. La implementación de VXLAN ofrece una arquitectura flexible y adaptable que puede satisfacer las demandas cambiantes del entorno empresarial moderno. Este enfoque proporciona una base sólida para la creación de redes ágiles y altamente eficientes, fundamentales para el éxito de las organizaciones en el panorama actual de negocios.

VXLAN es considerado como la respuesta clave para avanzar en el rendimiento y la eficiencia en las infraestructuras de red. En el trabajo de [4], se llevó a cabo un análisis conceptual del protocolo VXLAN en el contexto de la virtualización de centros de datos. Se destacó la implementación de VXLAN en entornos de emulación para visualizar su funcionamiento y eficiencia, incluyendo la comparación con el protocolo 802.1q. Además, se exploraron las ventajas de VXLAN en la segmentación de redes virtuales, la movilidad de máquinas virtuales y la escalabilidad en redes empresariales. Este análisis permitió identificar los parámetros clave para optimizar la implementación de VXLAN y mejorar el procesamiento en los centros de datos, demostrando su funcionalidad como una extensión de VLAN en una topología spine and leaf.

C. Objetivos

1. Objetivo General

Realizar un análisis comparativo del impacto de las tecnologías de redes tradicionales y VXLAN en el rendimiento de redes empresariales para identificar ventajas y desventajas específicas.

2. *Objetivos Específicos*

- Investigar y entender las tecnologías de redes tradicionles y VXLAN, explorando sus características de segmentación y escalabilidad, así como su influencia en el tráfico de red.
- Diseñar y configurar escenarios de red utilizando redes tradicionales y VXLAN en un entorno de emulación controlado, midiendo parámetros clave de rendimiento bajo distintas condiciones.
- Analizar y comparar los resultados obtenidos en términos de latencia, ancho de banda, tasa de transferencia y eficiencia del tráfico.

II. Marco teórico/Marco conceptual

A. *MikroTik*

MikroTik, líder en soluciones de red, despliega su versátil sistema operativo, RouterOS, como una opción robusta para las redes empresariales. Con funciones avanzadas de enrutamiento, firewall, VPN y servicios esenciales como DHCP y DNS, MikroTik brinda la flexibilidad necesaria para construir infraestructuras de red seguras y eficientes. Destaca por su capacidad de implementar enrutamiento multicapa, protocolos avanzados y servicios adicionales, convirtiéndolo en una opción integral. Su énfasis en la seguridad, con firewall y monitoreo efectivos, se combina con una interfaz amigable. Desde túneles VPN hasta servicios como DHCP y DNS, MikroTik simplifica la administración de redes. Su versatilidad y costo-efectividad lo posicionan como un actor clave, desde pequeñas empresas hasta implementaciones en sucursales y centros de datos, adaptándose a las diversas necesidades de conectividad empresarial [5]. Además, MikroTik RouterOS ofrece soporte para protocolos de enrutamiento avanzados como BGP, permitiendo la conectividad a nivel de sistemas autónomos y desempeñando un papel crucial en la gestión de grandes redes empresariales. Posteriormente, RouterOS también integra tecnologías como EoIP [6] y VXLAN, proporcionando una conectividad eficiente y una gestión avanzada de redes en entornos empresariales [7].

B. *Protocolo BGP*

El protocolo Border Gateway Protocol (BGP) desempeña un papel fundamental en el contexto empresarial al facilitar la conectividad entre redes autónomas. BGP, como protocolo de enrutamiento de puerta de enlace, se centra en intercambiar información de enrutamiento entre sistemas autónomos (AS), permitiendo a las empresas gestionar eficientemente la conectividad con redes externas. BGP utiliza una serie de reglas y políticas para tomar decisiones de enrutamiento, lo que le confiere una gran flexibilidad y capacidad para adaptarse a la estructura jerárquica de la infraestructura de red empresarial. Este protocolo es especialmente valioso para empresas que gestionan conexiones a Internet y tienen múltiples rutas para optimizar la eficiencia del tráfico y garantizar una conectividad confiable [8].

La configuración y gestión efectivas de BGP en routers MikroTik son esenciales para aprovechar al máximo las capacidades de este protocolo en entornos empresariales. MikroTik

RouterOS proporciona herramientas avanzadas para la configuración de BGP, permitiendo a los administradores definir políticas de enrutamiento, filtrar rutas y ajustar parámetros para optimizar el flujo de tráfico. La interfaz amigable de MikroTik simplifica el proceso de configuración, desde establecer sesiones BGP hasta gestionar la propagación de rutas. La implementación exitosa de BGP en routers MikroTik garantiza una conectividad estable y eficiente, contribuyendo así al rendimiento óptimo de las redes empresariales. La importancia de esta configuración radica en su capacidad para influir directamente en la forma en que la empresa se conecta con el resto de Internet y otras redes autónomas, proporcionando una base robusta para la comunicación y la colaboración empresarial [9].

C. Redes Tradicionales

Las redes tradicionales, como infraestructura en el entorno empresarial, han sido durante muchos años los cimientos imprescindibles para la comunicación y el traspaso de información. Tienen como característica el uso de protocolos bien establecidos, como lo es EoIP. Esta tecnología representa para muchas empresas un estándar confiable y arraigado en la historia de las infraestructuras de redes. Su fama se debe a las buenas valoraciones en cuanto a la estabilidad y la simplicidad, convirtiéndose en una opción de conectividad muy popular en diversas organizaciones [10]. Al mencionar redes tradicionales, se encuentran elementos importantes, como routers y switches, los cuales tienen como objetivo encargarse del tráfico y establecer la conectividad. Comúnmente se emplean las topologías jerárquicas, las cuales buscan mejorar la eficiencia y el rendimiento. Esta estructura ha sido fundamental en la configuración de entornos empresariales, proporcionando una base sólida para la comunicación interna y externa [11].

D. Protocolo EoIP

EoIP, como protocolo de comunicación, despliega un papel fundamental en la interconexión de dispositivos en entornos empresariales, brindando una solución robusta para la comunicación en tiempo real. A diferencia de la percepción común que lo visualiza simplemente como un cable o línea T1, EoIP aprovecha la infraestructura Ethernet tradicional de una empresa, permitiendo la conectividad de múltiples dispositivos en toda la empresa [12].

La Figura 1 muestra los componentes de EoIP distribuidos en el modelo OSI, un marco que describe las siete capas utilizadas por los sistemas informáticos para comunicarse a través de una red. En la primera capa, se encuentran Ethernet Físico y Ethernet MAC designados para las capas Física y de Enlace de Datos, respectivamente. La capa de Red alberga el protocolo IP, mientras que en la capa de Transporte se identifican UDP y TCP. La gestión de conexiones se ubica en la capa de Sesión, y en la capa de Presentación se distinguen los aspectos de Mensaje Explícito/Implícito. Finalmente, la capa de Aplicación incorpora el Perfil de Dispositivo.

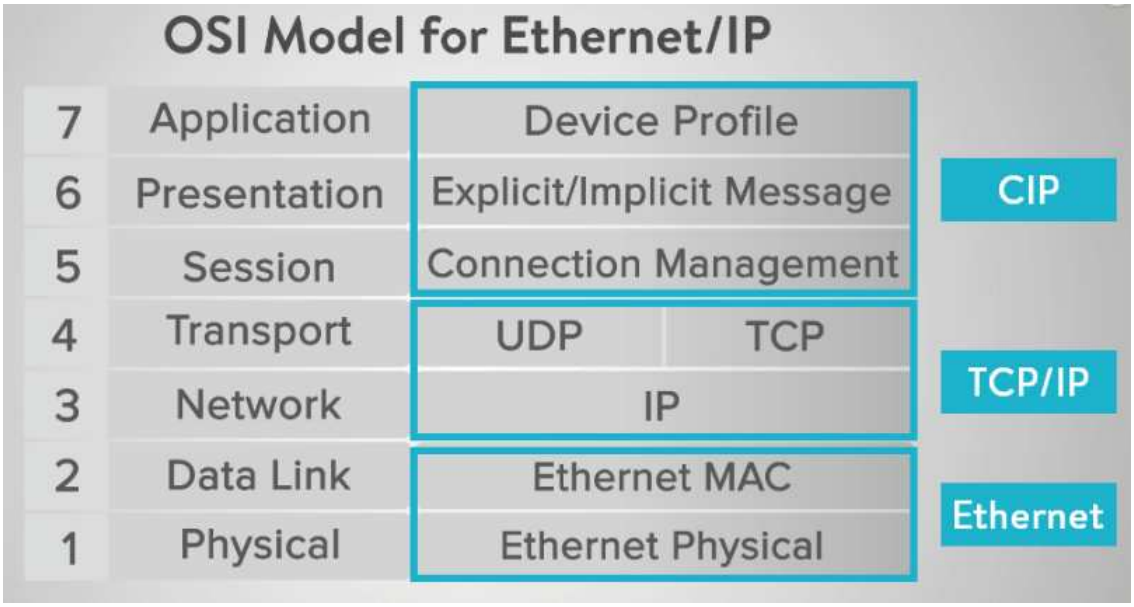


Fig. 1. Modelo OSI para EoIP [13].

E. VXLAN

VXLAN redefine la infraestructura de redes empresariales al proporcionar una tunelización que superpone redes de capa 2 sobre capa 3, abordando así limitaciones clave de los protocolos tradicionales como EoIP. Esta tecnología, al ofrecer una capacidad excepcional de segmentación y aislamiento del tráfico, permite la creación de redes virtuales más flexibles y escalables. La comparativa con los protocolos tradicionales destaca la capacidad de VXLAN para admitir hasta 16 millones de redes virtuales, superando las restricciones de VLANs. Además, se explorarán casos de uso y escenarios de implementación, revelando cómo VXLAN optimiza la conectividad en centros de datos virtualizados, gestiona redes en entornos con requisitos de seguridad más rigurosos y se adapta a diversas necesidades empresariales, consolidando su

posición como una solución versátil para las demandas cambiantes de las redes empresariales modernas. [14].

1. Parámetros en la Implementación de VXLAN

La correcta implementación de VXLAN en entornos empresariales requiere una atención meticulosa a varios parámetros y consideraciones para garantizar su eficiencia y rendimiento óptimo. Un aspecto crucial es la definición adecuada de los identificadores de red virtual (VNI), evitando conflictos y permitiendo la coexistencia de múltiples redes sobre una infraestructura compartida. Además, la elección de métodos de encapsulamiento y la configuración precisa de dispositivos de red, como los VTEP (VXLAN Tunnel Endpoint), son determinantes para impactar directamente en la conectividad y la escalabilidad de la red [15].

La seguridad también desempeña un papel fundamental en la implementación de VXLAN. La aplicación de medidas como la segmentación de red y la autenticación en los túneles VXLAN son esenciales para proteger la integridad de la información transmitida. La gestión eficaz del tráfico multicast, utilizado por VXLAN para la difusión de información de aprendizaje, también debe ser considerada para evitar congestiones y garantizar una distribución eficiente de los paquetes. Este análisis detallado de los parámetros y consideraciones clave proporcionará una guía integral para los profesionales de redes, permitiéndoles aprovechar al máximo los beneficios de VXLAN mientras abordan los desafíos específicos asociados a su despliegue en entornos empresariales [15].

Existen parámetros críticos en la implementación de VXLAN en entornos empresariales. Se destaca la importancia de definir correctamente los identificadores de red virtual (VNI) y la configuración precisa de dispositivos de red como los VTEP (VXLAN Tunnel Endpoint) para garantizar la conectividad y la escalabilidad de la red [16]. Asimismo, resaltan la relevancia de las medidas de seguridad, como la segmentación de red y la autenticación en los túneles VXLAN, para proteger la integridad de la información transmitida y gestionar eficazmente el tráfico multicast [17].

La Figura 2 representa una infraestructura de red con un túnel VXLAN. Se muestra cómo los Virtual Tunnel End Points se conectan a las máquinas virtuales y al túnel VXLAN dentro de la red. Hay dos VTEP (Virtual Tunnel End Points) en lados opuestos, cada uno conectado a tres VM (máquinas virtuales). Los Virtual Tunnel End Points están conectados a un “túnel

VXLAN" que está dentro de la nube que representa la "red". La nube de la red está en el centro del diagrama, indicando que los Virtual Tunnel End Points y las máquinas virtuales están conectados a través de esta red.

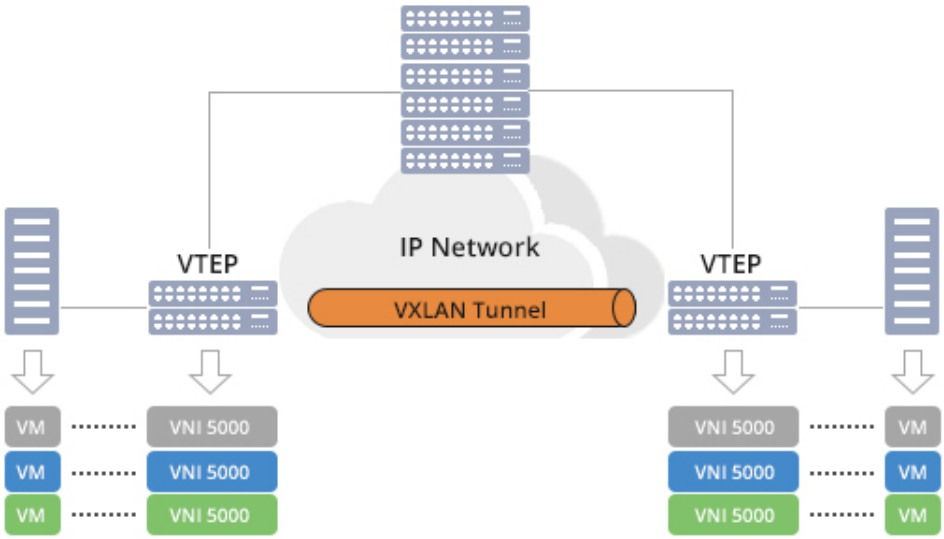


Fig. 2. Infraestructura de red con un túnel VXLAN [18].

F. Metodología PPDIOO

La metodología PPDIOO encuentra su fundamento en las directrices delineadas en el ciclo de vida PPDIOO, una estructura ampliamente empleada por Cisco para la gestión de redes. La adherencia a este ciclo de vida predefinido emerge como una estrategia efectiva para alcanzar metas predeterminadas, tales como la reducción del costo total de administración de la red, el incremento de la disponibilidad de la infraestructura y una mejora sustancial en la agilidad para implementar cambios estructurales. Este ciclo de vida se revela beneficioso tanto para la implementación de nuevas redes como para la modernización de redes ya existentes. Los componentes que integran el ciclo de vida forman un ciclo continuo e interconectado, donde, por ejemplo, el paso de optimización desencadena actividades como la identificación de cambios y la validación en la infraestructura existente, impulsando así un retorno al paso inicial de preparación [19].

1. Beneficios de PPDIOO

La Metodología PPDIOO se distingue por su capacidad para reducir el costo total de propiedad mediante validaciones detalladas, desde requerimientos tecnológicos hasta la planificación de cambios en la infraestructura. Este enfoque incluye la determinación precisa de recursos y la alineación de estrategias con objetivos técnicos y de negocio, generando mejoras significativas en la eficiencia de la red y reduciendo los costos operativos [19].

Además, la Metodología PPDIOO garantiza una mayor disponibilidad de la red mediante un diseño robusto que incorpora consideraciones exhaustivas de seguridad y la ejecución de pruebas piloto antes de la implementación en producción. En términos de agilidad empresarial, destaca por establecer requisitos de negocio, integrarlos con objetivos técnicos y traducirlos en un diseño detallado. La experiencia avanzada en configuración, instalación e integración de componentes, junto con un enfoque continuo de mejora, respalda la agilidad de la empresa y contribuye a la velocidad de acceso a aplicaciones y servicios [19].

La Figura 3 muestras las fases fundamentales de la Metodología PPDIOO, proporcionando una guía visual que refuerza la comprensión de su implementación en la gestión eficiente y estratégica de las redes empresariales.

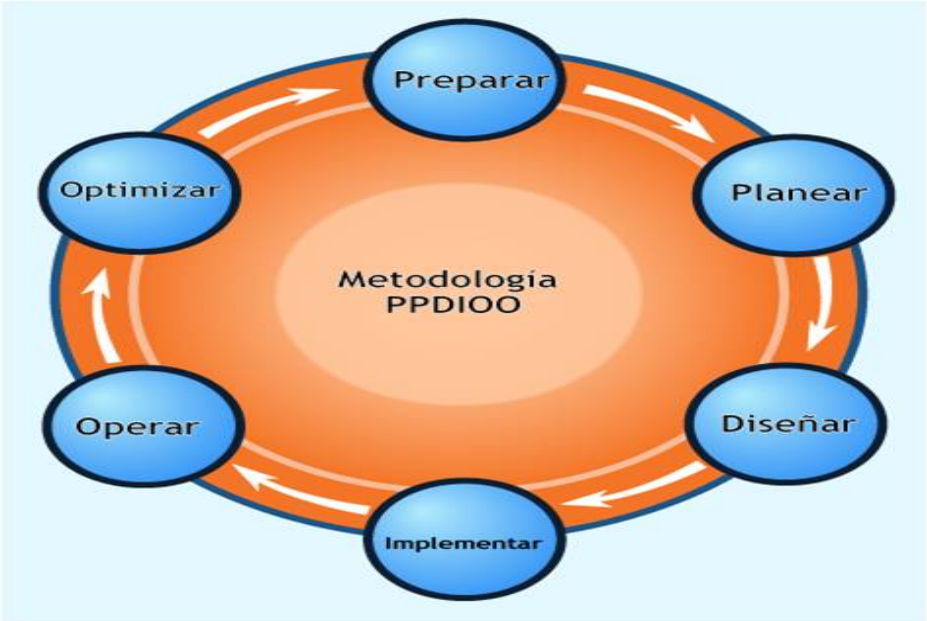


Fig. 3. Fases de Metodología PPDIOO [19].

III. METODOLOGÍA/TÉCNICAS/DISEÑO

A. *Metodología de Desarrollo*

Se detallara el proyecto con la implementación efectiva de la Metodología PPDIOO. Esta elección estratégica surge de su estructura organizada y coherente, alineada con el propósito de entender el impacto de la adopción de VXLAN en el rendimiento de las redes empresariales frente a las redes tradicionales. Originada en el ciclo de vida propuesto por Cisco para la administración de redes, la Metodología PPDIOO se despliega en fases secuenciales de preparación, planificación, diseño, implementación, operación y optimización. En las siguientes secciones, se detallará el desarrollo del proyecto bajo esta metodología, resaltando su aplicabilidad y relevancia para alcanzar los objetivos propuestos.

1. Preparación

Se inicia con la etapa de preparación, la cual implica reconocer las tecnologías necesarias para el diseño del escenario de la red, así como llevar a cabo un estudio preciso de los aspectos más relevantes. Por esta razón, se detallan todos los dispositivos y tecnologías aplicadas dentro de este trabajo:

GNS3: Es una herramienta de código abierto que permite diseñar, emular y simular redes de manera eficiente. Con esta plataforma, se pueden crear topologías complejas que incluyan una variedad de dispositivos de red, como routers, switches y firewalls, replicando así entornos de red reales.

MikroTik CHR: Son imagenes diseñadas para funcionar como máquinas virtuales en entornos de virtualización, estan basadas en el sistema operativo RouterOS, son optimizadas para arquitecturas x86 de 64 bits y son compatibles con una amplia gama de hipervisores, incluyendo VMWare, Hyper-V, VirtualBox, KVM, entre otros. Estas imágenes ofrecen todas las funcionalidades completas de RouterOS, que incluyen soporte para enrutamiento MPLS, protocolos de enrutamiento dinámico como BGP y OSPF, gestión de ancho de banda, seguridad y más, adaptadas para su implementación en entornos virtualizados.

La compatibilidad con tecnologías como EoIP [20] y VXLAN [20] es fundamental en las imágenes CHR de MikroTik, permitiendo la creación de túneles y la virtualización avanzada. Esto ofrece una solución completa para redes empresariales, con capacidad de enrutamiento avanzado,

seguridad, gestión de ancho de banda y más, todo adaptado para su implementación en entornos virtualizados.

Contenedor Ubuntu: La instancia de un contenedor Ubuntu representa una instancia del sistema operativo Linux, construida sobre la base de Debian en su versión 20. Esta imagen está disponible para su descarga a través de la tienda de GNS3, proporcionando una plataforma versátil y confiable para implementar servicios y aplicaciones dentro de entornos virtuales [21].

Switch: Conmutador que viene integrada por defecto en la plataforma GNS3.

2. Planifiación

Con base en las tecnologías detalladas en la fase de preparación, se inicia con el diseño de una red empresarial para llevar a cabo el estudio comparativo. Dado que se trata de una emulación de red, las pruebas se realizaron de manera local en un entorno controlado, si bien el diseño puede aplicarse en cualquier infraestructura empresarial. En la Tabla I se puede visualizar el plan con la tareas que se van a realizar.

Durante el primer mes, se dedicó a la preparación y planificación del proyecto; en el segundo mes, se procedió con las fases de diseño e implementación de la red; el tercer mes estuvo enfocado en la etapa operativa, y finalmente, en el cuarto mes, se completó la operación de la red con las modificaciones necesarias.

TABLA I
PLAN DE TRABAJO PARA EL DISEÑO DE UNA RED TRADICIONAL (ETHERNET/IP) Y UNA RED CON VXLAN PARA MEDIR EL IMPACTO EN EL RENDIMIENTO DE REDES EMPRESARIALES.

Fase	**Mes 1**	**Mes 2**	**Mes 3**	**Mes 4**
Preparación	X			
Planificación	X			
Diseño de red		X		
Implementación		X		
Operación			X	
Optimización				X

3. Diseño

Topologia de red tradicional EoIP

La red tradicional Ethernet over IP se basa en un diseño BGP (Border Gateway Protocol) que incluye cuatro routers MikroTik, cada uno ejecutando el sistema operativo RouterOS, con asignaciones de sistemas autónomos (AS) diferentes para cada router. Estos routers BGP forman parte de una topología que conecta dos sucursales, denominadas A y B. Cada sucursal tiene un border router, también ejecutando BGP, para gestionar la conexión con otras redes externas.

En cada sucursal, además del router border, se ubica un router adicional de MikroTik, un switch y una PC con sistema Ubuntu. La configuración Ethernet over IP se establece entre los routers de ambas sucursales, lo que permite la comunicación y el intercambio de datos entre ellas a través de la infraestructura BGP, tal como se observa en la Figura 4.

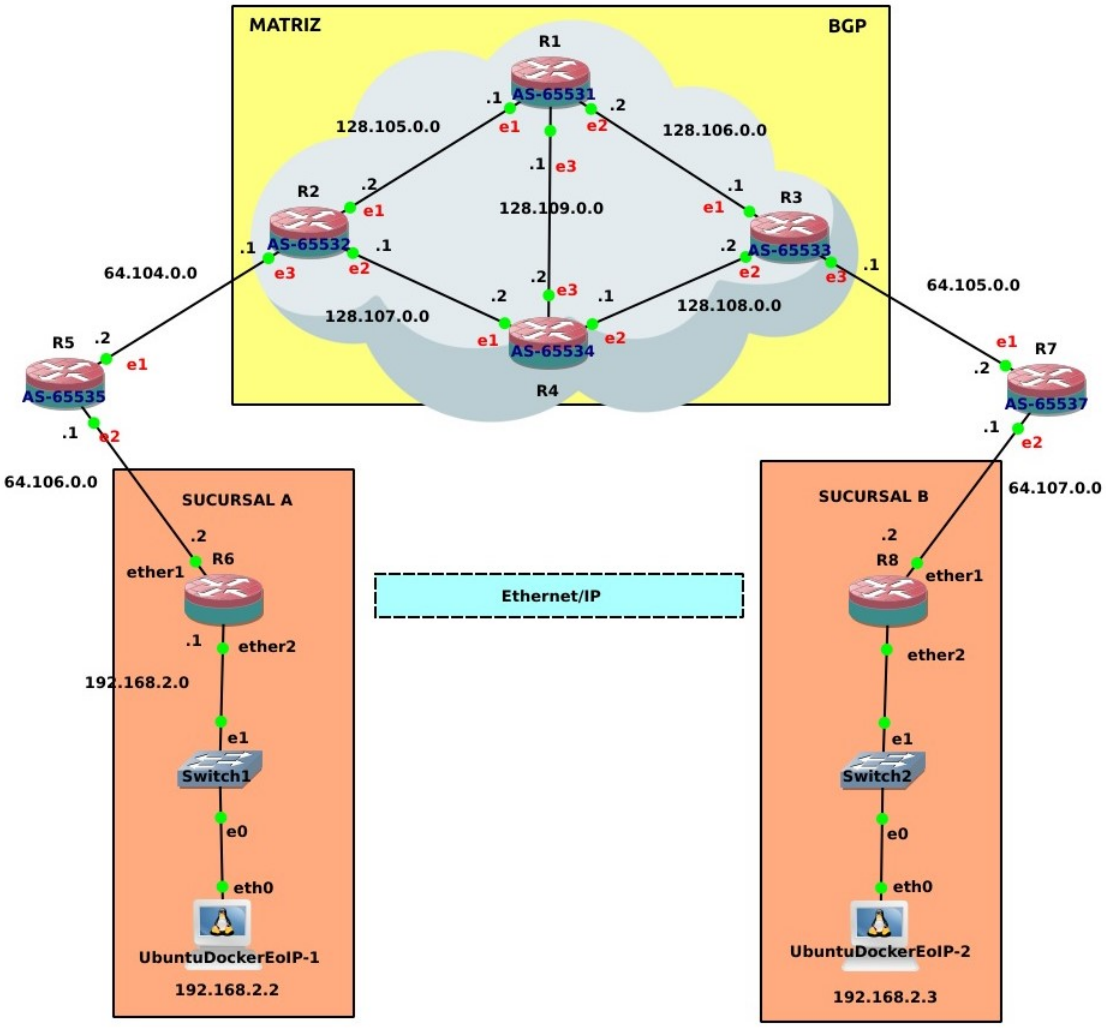


Fig. 4. Topologia de red tradicional EoIP.

Topologia de red tradicional VXLAN

Para la topología basada en VXLAN, se mantiene la misma infraestructura de red que en la configuración EoIP. Sin embargo, la diferencia principal radica en la implementación de VXLAN en los routers MikroTik de cada sucursal, los cuales ejecutan el sistema operativo RouterOS.

Es importante destacar que los routers de cada sucursal utilizan exclusivamente la versión 7 de RouterOS para habilitar VXLAN, mientras que los otros routers continúan ejecutando la versión 6. Esto se debe a que en la versión 6 de RouterOS no se cuenta con la función necesaria para configurar VXLAN. Todos estos elementos de la topología VXLAN se pueden visualizar

en la Figura 5.

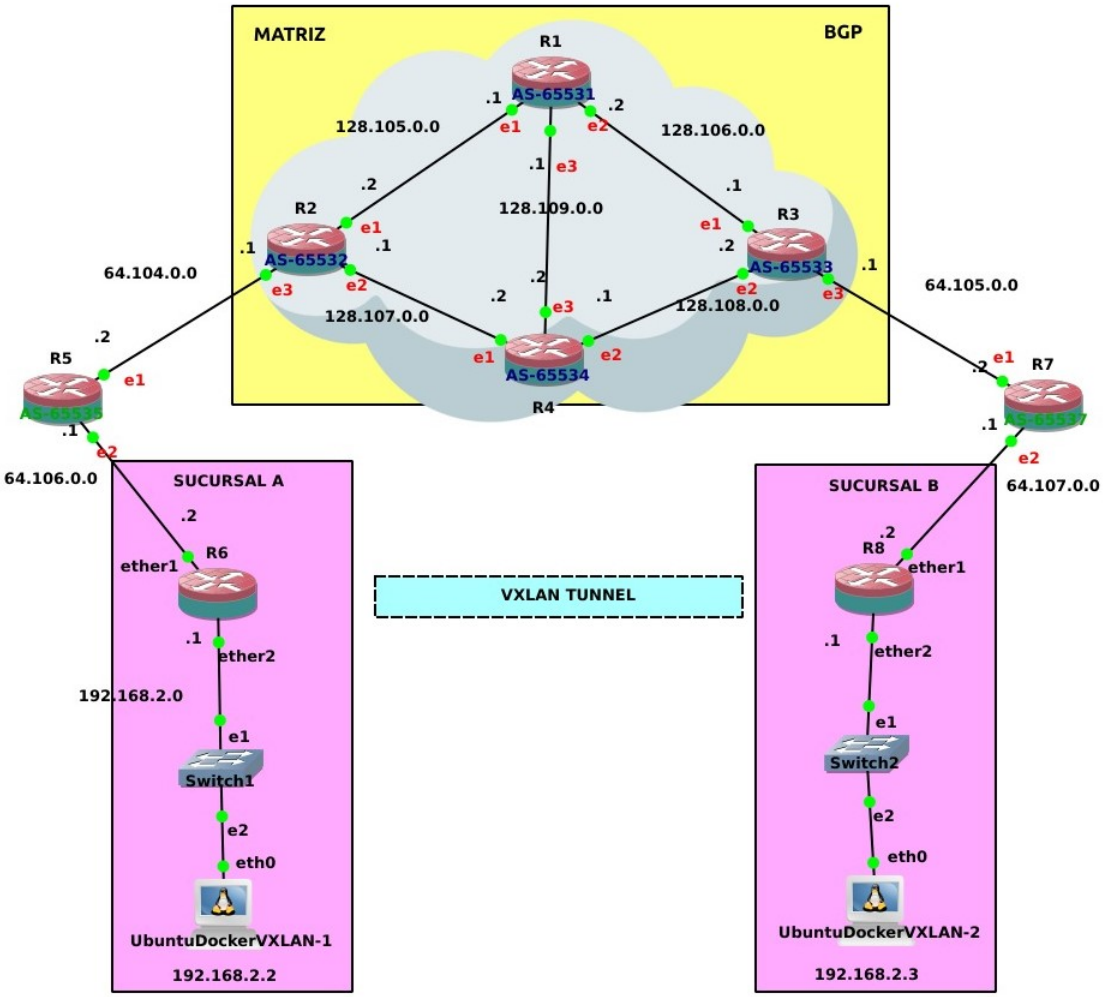


Fig. 5. Topologia de red VXLAN.

A partir de esta configuración de red, se asigna un direccionamiento IP específico a cada uno de los dispositivos, siguiendo el esquema detallado en el contenido de la Tabla II. Es importante destacar que este direccionamiento IP se mantiene igual en ambas topologías, tanto en la configuración basada en EoIP como en la basada en VXLAN.

TABLA II
ASIGNACIÓN DE DIRECCIONES IP EN LA RED

Dispositivo	**Interfaz**	**Dirección IP**	**Máscara de subred**	**Gateway**
R1	Eth1	128.105.0.1	255.255.255.255	
	Eth2	128.106.0.2	255.255.255.255	
	Eth3	128.109.0.1	255.255.255.255	
R2	Eth1	128.105.0.2	255.255.255.255	
	Eth2	128.107.0.1	255.255.255.255	
	Eth3	64.104.0.1	255.255.255.255	
R3	Eth1	128.106.0.1	255.255.255.255	
	Eth2	128.108.0.2	255.255.255.255	
	Eth3	64.105.0.1	255.255.255.255	
R4	Eth1	128.107.0.2	255.255.255.255	
	Eth2	128.108.0.1	255.255.255.255	
	Eth3	128.109.0.2	255.255.255.255	
R5	Eth1	64.104.0.2	255.255.255.255	
	Eth2	64.106.0.1	255.255.255.255	
R6	Eth1	64.106.0.2	255.255.255.255	
	Eth2	192.168.2.1	255.255.255.0	
R7	Eth1	64.105.0.2	255.255.255.255	
	Eth2	64.107.0.1	255.255.255.255	
R8	Eth1	64.107.0.2	255.255.255.255	
PC1	Eth0	192.168.2.2	255.255.255.0	192.168.2.1
PC2	Eth0	192.168.2.3	255.255.255.0	192.168.2.1

4. Implementación

Configuración de Direccionamiento para EoIP

Como primer paso en la configuración de la red BGP en el router R1, se procedió a asignar nombres a las interfaces Ethernet (ether1, ether2, ether3) con el objetivo de simplificar su identificación y gestión. Esto se logró mediante el siguiente comando: /interface ethernet set [find default-name=ether1] name=ether1. A continuación, se asignó un nombre a la interfaz de bucle (loopback1) mediante el comando: /interface ethernet set [find default-name=loopback1] name=loopback1. Posteriormente, se configuraron las direcciones IP con el comando: /ip address add address=128.105.0.1/30 interface=ether1, en cada interfaz conforme a la tabla de direccionamiento IP establecida para la red BGP (consulte la Tabla II). Estos pasos se repitieron para todas las interfaces Ethernet, garantizando la asignación de un nombre a cada una y la configuración de una dirección IP única. Esta práctica se llevó a cabo con el fin de evitar conflictos y facilitar una comunicación efectiva dentro de la red BGP. Para mostrar los resultados de las configuraciones de las direcciones IP, se utilizó el comando: '/ip address print', tal como se muestra en la Figura 6.

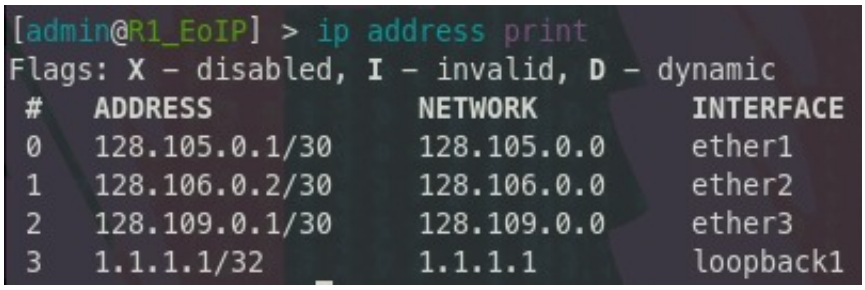


Fig. 6. Asignación de Direcciones IP en el Router R1 para EoIP.

Configuración de Direccionamiento para VXLAN

En la implementación de la red VXLAN, se siguieron procedimientos similares a los de la configuración de la red Ethernet/IP. Inicialmente, se asignaron nombres a las interfaces Ethernet en el router R1 para facilitar su gestión y identificación mediante comandos específicos.

Posteriormente, se configuraron las direcciones IP en cada interfaz del router R1 utilizando los comandos correspondientes, ajustándolas conforme a la tabla de direccionamiento IP definida previamente para la red VXLAN (consulte la Tabla II). Este proceso se replicó para todas las interfaces Ethernet en el router R1, asegurando una correcta asignación de nombres y direcciones

IP en toda la infraestructura de la red VXLAN, tal como se muestra en la Figura 7.

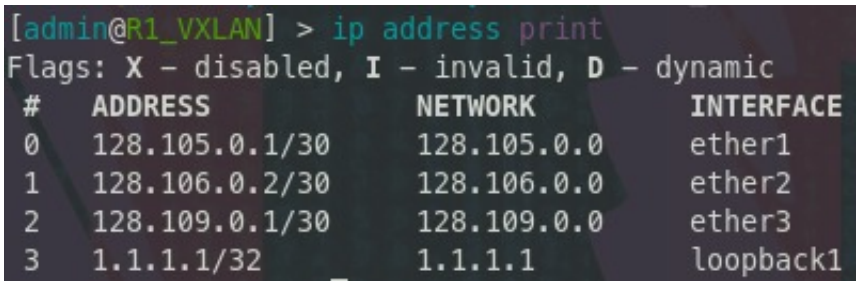


Fig. 7. Asignación de Direcciones IP en el Router R1 para VXLAN.

Configuración de Protocolo BGP para EoIP

Después de finalizar la configuración de las interfaces y direcciones IP en el router R1, se procedió a configurar el protocolo BGP ((Border Gateway Protocol). Se estableció el número del sistema autónomo (AS) predeterminado para la instancia BGP utilizando el comando: '/routing bgp instance set default as=65531'. Esta configuración define el número del sistema autónomo que identifica de forma única al router en la red BGP. Se configuró el identificador del router BGP (Router ID) para la instancia BGP con el comando: /routing bgp instance set default router-id=1.1.1.1. El identificador del router BGP es una dirección IP que identifica de manera única al router dentro del protocolo BGP.

Además de estos comandos, se agregaron pares BGP necesarios utilizando comandos como: '/routing bgp peer add remote-address=128.105.0.2 remote-as=65532', y también se definieron las redes que se anunciarán a través del protocolo BGP mediante el comando: '/routing bgp network add network=128.105.0.0/30'. Estos pasos se repitieron para todos los pares BGP y para todas las redes que se debían anunciar en la configuración del router R1. Vea la Figura 8 para la configuración completa.

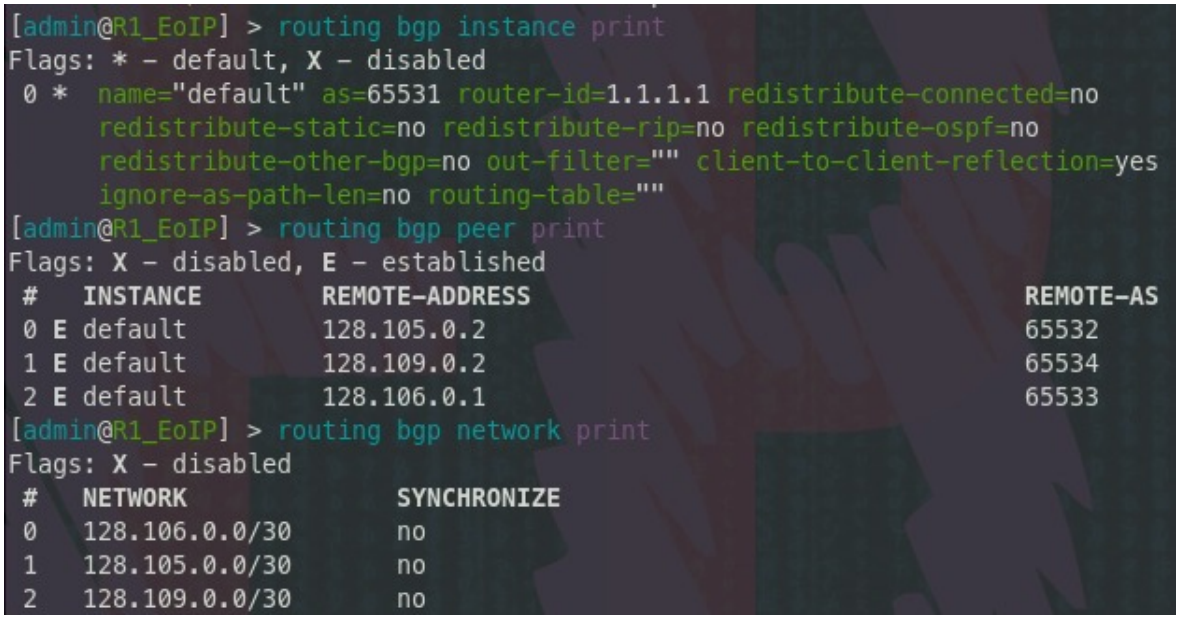


Fig. 8. Configuración de protocolo BGP en el router R1 EoIP.

Configuración de Protocolo BGP para VXLAN.

Para la topología VXLAN, la configuración del protocolo BGP en el router R1 siguió el mismo procedimiento que en Ethernet over IP. Después de configurar las interfaces y direcciones IP, se estableció el número de sistema autónomo (AS) y el identificador del router BGP. Se añadieron pares BGP y se definieron las redes a anunciar, replicando así la configuración de Ethernet over IP. Esto se muestra en la Figura 9.

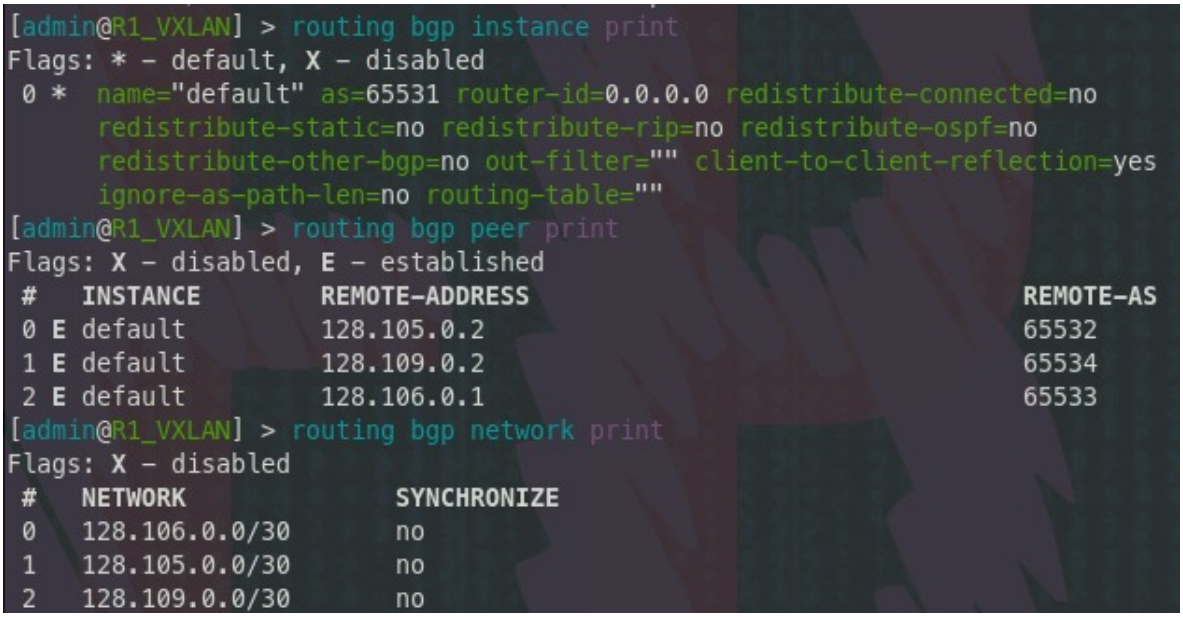


Fig. 9. Configuración de protocolo BGP en el router R1 VXLAN.

Configuración de Direccionamiento IP y Protocolo BGP para los demas routers en EoIP

Después de completar la configuración inicial en el router R1, que incluyó la asignación de nombres a las interfaces Ethernet y la configuración de direcciones IP, se procedió a configurar el protocolo BGP para establecer la conectividad y el intercambio de información de enrutamiento en la red BGP. Para garantizar la coherencia en toda la red BGP, las mismas configuraciones realizadas en el router R1 deben aplicarse en los routers R2, R3 y R4. Esto incluye la asignación de nombres a las interfaces, la configuración de direcciones IP y la configuración del protocolo BGP con los números de sistema autónomo (AS) y los identificadores de router (Router ID) correspondientes.

Después de aplicar estas configuraciones en cada uno de los routers R2, R3 y R4, es importante verificar que las configuraciones se hayan realizado correctamente. Se adjuntan imágenes de verificación que muestran las configuraciones realizadas en cada uno de los routers para asegurar la consistencia y la adecuada implementación del protocolo BGP en toda la red. Estas imágenes de verificación pueden encontrarse en la Figura 10, Figura 11, y Figura 12.

```
[admin@R2_EoIP] > ip addres print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   128.105.0.2/30     128.105.0.0     ether1
 1   128.107.0.1/30     128.107.0.0     ether2
 2   64.104.0.1/30      64.104.0.0      ether3
 3   2.2.2.2/32         2.2.2.2         loopback2
[admin@R2_EoIP] > routing bgp instance print
Flags: * - default, X - disabled
 0 *  name="default" as=65532 router-id=2.2.2.2 redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-ospf=no
      redistribute-other-bgp=no out-filter="" client-to-client-reflection=yes
      ignore-as-path-len=no routing-table=""
[admin@R2_EoIP] > routing bgp peer print
Flags: X - disabled, E - established
 #   INSTANCE        REMOTE-ADDRESS                                  REMOTE-AS
 0 E default         128.105.0.1                                     65531
 1 E default         128.107.0.2                                     65534
 2 E default         64.104.0.2                                      65535
[admin@R2_EoIP] > routing bgp network print
Flags: X - disabled
 #   NETWORK              SYNCHRONIZE
 0   128.105.0.0/30       no
 1   128.107.0.0/30       no
 2   64.104.0.0/30        no
```

Fig. 10. Direcciones IP y Protocolo BGP en el router R2 EoIP.

```
[admin@R3_EoIP] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   128.106.0.1/30     128.106.0.0     ether1
 1   128.108.0.2/30     128.108.0.0     ether2
 2   64.105.0.1/30      64.105.0.0      ether3
 3   3.3.3.3/32         3.3.3.3         loopback3
[admin@R3_EoIP] > routing bgp instance print
Flags: * - default, X - disabled
 0 *  name="default" as=65533 router-id=3.3.3.3 redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-ospf=no
      redistribute-other-bgp=no out-filter="" client-to-client-reflection=yes
      ignore-as-path-len=no routing-table=""
[admin@R3_EoIP] > routing bgp peer print
Flags: X - disabled, E - established
 #   INSTANCE        REMOTE-ADDRESS                                  REMOTE-AS
 0 E default         128.106.0.2                                     65531
 1 E default         128.108.0.1                                     65534
 2 E default         64.105.0.2                                      65537
[admin@R3_EoIP] > routing bgp network print
Flags: X - disabled
 #   NETWORK              SYNCHRONIZE
 0   128.106.0.0/30       no
 1   128.108.0.0/30       no
 2   64.105.0.0/30        no
```

Fig. 11. Direcciones IP y Protocolo BGP en el router R3 EoIP.

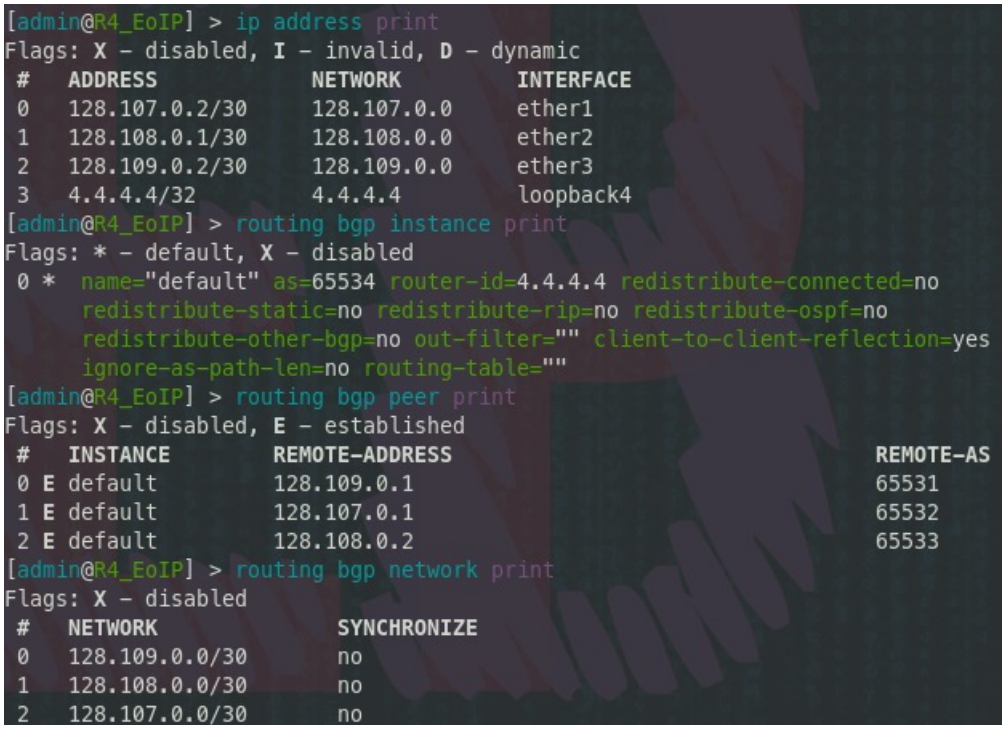


Fig. 12. Direcciones IP y Protocolo BGP en el router R4 EoIP.

Configuración de Direccionamiento IP y Protocolo BGP para los demas routers en VXLAN

Para la red VXLAN, el proceso de configuración del protocolo BGP sigue el mismo procedimiento. Después de aplicar estas configuraciones en cada uno de los routers VXLAN, es esencial verificar que se hayan realizado correctamente. Las imágenes de verificación pueden encontrarse en la Figura 13, Figura 14 y Figura 15.

```
[admin@R2_VXLAN] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   128.105.0.2/30     128.105.0.0     ether1
 1   128.107.0.1/30     128.107.0.0     ether2
 2   64.104.0.1/30      64.104.0.0      ether3
 3   2.2.2.2/32         2.2.2.2         loopback2
[admin@R2_VXLAN] > routing bgp instance print
Flags: * - default, X - disabled
 0 *  name="default" as=65532 router-id=2.2.2.2 redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-ospf=no
      redistribute-other-bgp=no out-filter="" client-to-client-reflection=yes
      ignore-as-path-len=no routing-table=""
[admin@R2_VXLAN] > routing bgp peer print
Flags: X - disabled, E - established
 #   INSTANCE        REMOTE-ADDRESS                                  REMOTE-AS
 0 E default         128.105.0.1                                     65531
 1 E default         128.107.0.2                                     65534
 2 E default         64.104.0.2                                      65535
[admin@R2_VXLAN] > routing bgp network print
Flags: X - disabled
 #   NETWORK             SYNCHRONIZE
 0   128.105.0.0/30      no
 1   128.107.0.0/30      no
 2   64.104.0.0/30       no
```

Fig. 13. Direcciones IP y Protocolo BGP en el router R2 VXLAN.

```
[admin@R3_VXLAN] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   128.106.0.1/30     128.106.0.0     ether1
 1   128.108.0.2/30     128.108.0.0     ether2
 2   64.105.0.1/30      64.105.0.0      ether3
 3   3.3.3.3/32         3.3.3.3         loopback3
[admin@R3_VXLAN] > routing bgp instance print
Flags: * - default, X - disabled
 0 *  name="default" as=65533 router-id=3.3.3.3 redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-ospf=no
      redistribute-other-bgp=no out-filter="" client-to-client-reflection=yes
      ignore-as-path-len=no routing-table=""
[admin@R3_VXLAN] > routing bgp peer print
Flags: X - disabled, E - established
 #   INSTANCE        REMOTE-ADDRESS                                  REMOTE-AS
 0 E default         128.106.0.2                                     65531
 1 E default         128.108.0.1                                     65534
 2 E default         64.105.0.2                                      65537
[admin@R3_VXLAN] > routing bgp network print
Flags: X - disabled
 #   NETWORK             SYNCHRONIZE
 0   128.106.0.0/30      no
 1   128.108.0.0/30      no
 2   64.105.0.0/30       no
```

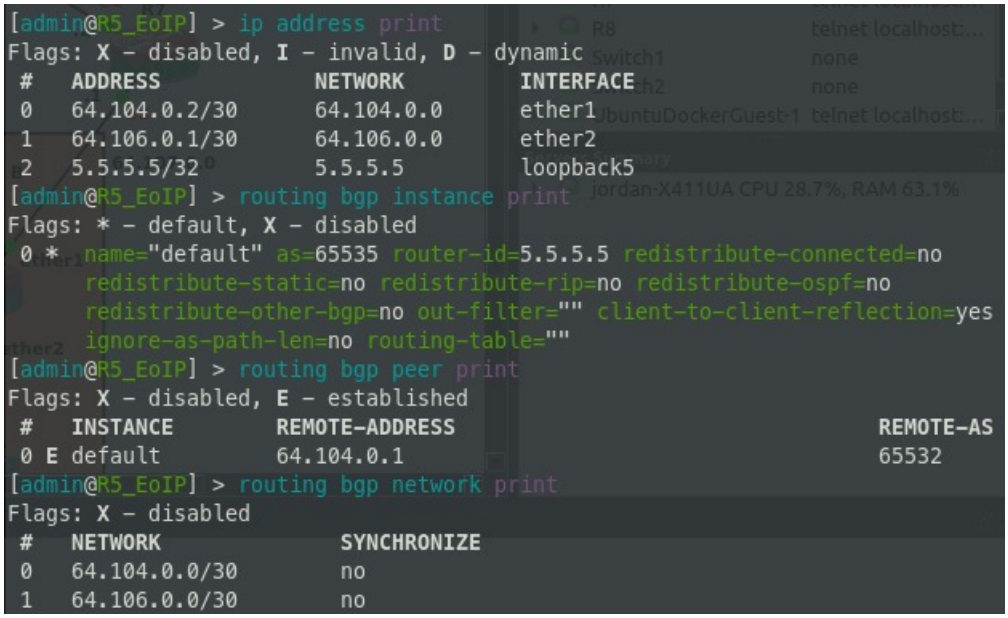
Fig. 14. Direcciones IP y Protocolo BGP en el router R3 VXLAN.

```
[admin@R4_VXLAN] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   128.107.0.2/30     128.107.0.0     ether1
 1   128.108.0.1/30     128.108.0.0     ether2
 2   128.109.0.2/30     128.109.0.0     ether3
 3   4.4.4.4/32         4.4.4.4         loopback4
[admin@R4_VXLAN] > routing bgp instance print
Flags: * - default, X - disabled
 0 *  name="default" as=65534 router-id=4.4.4.4 redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-ospf=no
      redistribute-other-bgp=no out-filter="" client-to-client-reflection=yes
      ignore-as-path-len=no routing-table=""
[admin@R4_VXLAN] > routing bgp peer print
Flags: X - disabled, E - established
 #   INSTANCE        REMOTE-ADDRESS                                  REMOTE-AS
 0 E default         128.109.0.1                                     65531
 1 E default         128.107.0.1                                     65532
 2 E default         128.108.0.2                                     65533
[admin@R4_VXLAN] > routing bgp network print
Flags: X - disabled
 #   NETWORK             SYNCHRONIZE
 0   128.109.0.0/30      no
 1   128.108.0.0/30      no
 2   128.107.0.0/30      no
```

Fig. 15. Direcciones IP y Protocolo BGP en el router R4 VXLAN.

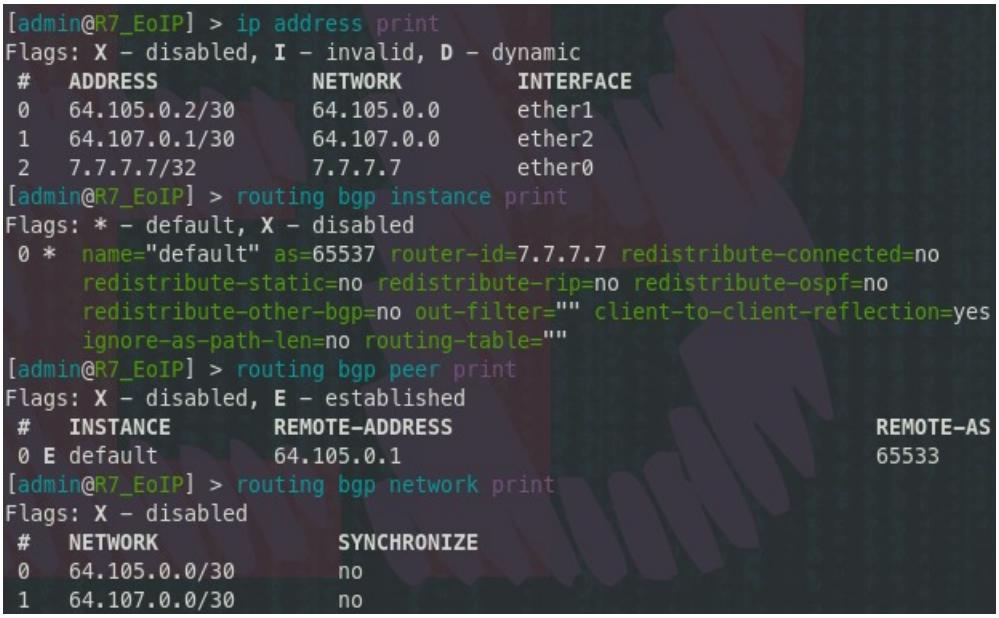
Configuración Border Router para EoIP

Los routers R5 y R7, designados como routers de borde en la red BGP, se configuraron siguiendo el mismo proceso empleado en los demás routers. Esto incluyó la asignación de nombres a las interfaces, la configuración de direcciones IP y la implementación del protocolo BGP con los números de sistema autónomo (AS) y Router ID correspondientes. La Figura 16 y Figura 17 ilustran la verificación de la configuración en los routers R5 y R7, respectivamente.



```
[admin@R5_EoIP] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   64.104.0.2/30      64.104.0.0      ether1
 1   64.106.0.1/30      64.106.0.0      ether2
 2   5.5.5.5/32         5.5.5.5         loopback5
[admin@R5_EoIP] > routing bgp instance print
Flags: * - default, X - disabled
 0 *  name="default" as=65535 router-id=5.5.5.5 redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-ospf=no
      redistribute-other-bgp=no out-filter="" client-to-client-reflection=yes
      ignore-as-path-len=no routing-table=""
[admin@R5_EoIP] > routing bgp peer print
Flags: X - disabled, E - established
 #   INSTANCE        REMOTE-ADDRESS                                  REMOTE-AS
 0 E default         64.104.0.1                                      65532
[admin@R5_EoIP] > routing bgp network print
Flags: X - disabled
 #   NETWORK             SYNCHRONIZE
 0   64.104.0.0/30       no
 1   64.106.0.0/30       no
```

Fig. 16. Verificación de la configuración de direcciones IP y Protocolo BGP en el border router R5 EoIP.



```
[admin@R7_EoIP] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   64.105.0.2/30      64.105.0.0      ether1
 1   64.107.0.1/30      64.107.0.0      ether2
 2   7.7.7.7/32         7.7.7.7         ether0
[admin@R7_EoIP] > routing bgp instance print
Flags: * - default, X - disabled
 0 *  name="default" as=65537 router-id=7.7.7.7 redistribute-connected=no
      redistribute-static=no redistribute-rip=no redistribute-ospf=no
      redistribute-other-bgp=no out-filter="" client-to-client-reflection=yes
      ignore-as-path-len=no routing-table=""
[admin@R7_EoIP] > routing bgp peer print
Flags: X - disabled, E - established
 #   INSTANCE        REMOTE-ADDRESS                                  REMOTE-AS
 0 E default         64.105.0.1                                      65533
[admin@R7_EoIP] > routing bgp network print
Flags: X - disabled
 #   NETWORK             SYNCHRONIZE
 0   64.105.0.0/30       no
 1   64.107.0.0/30       no
```

Fig. 17. Verificación de la configuración de direcciones IP y Protocolo BGP en el border router R7 EoIP.

Configuración Border Router para VXLAN

Para la topología de VXLAN, se aplicaron procedimientos idénticos a los utilizados en la configuración de la red BGP de la topologia Ethernet over IP. La Figura 18 y Figura 19 proporcionan una visión detallada de la verificación de la configuración en los routers R5 y R7, respectivamente. Estas imágenes muestran el estado de las interfaces, la correcta asignación de direcciones IP y la configuración del protocolo BGP, lo que garantiza la coherencia y la adecuada implementación en toda la infraestructura de red.

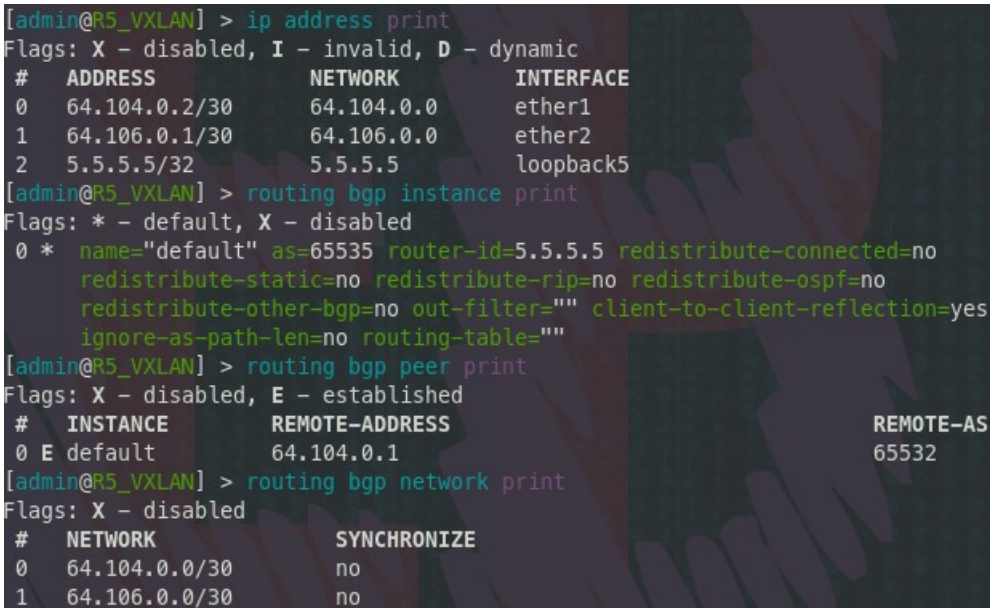


Fig. 18. Configuración de direcciones IP y Protocolo BGP en el border router R5 VXLAN.

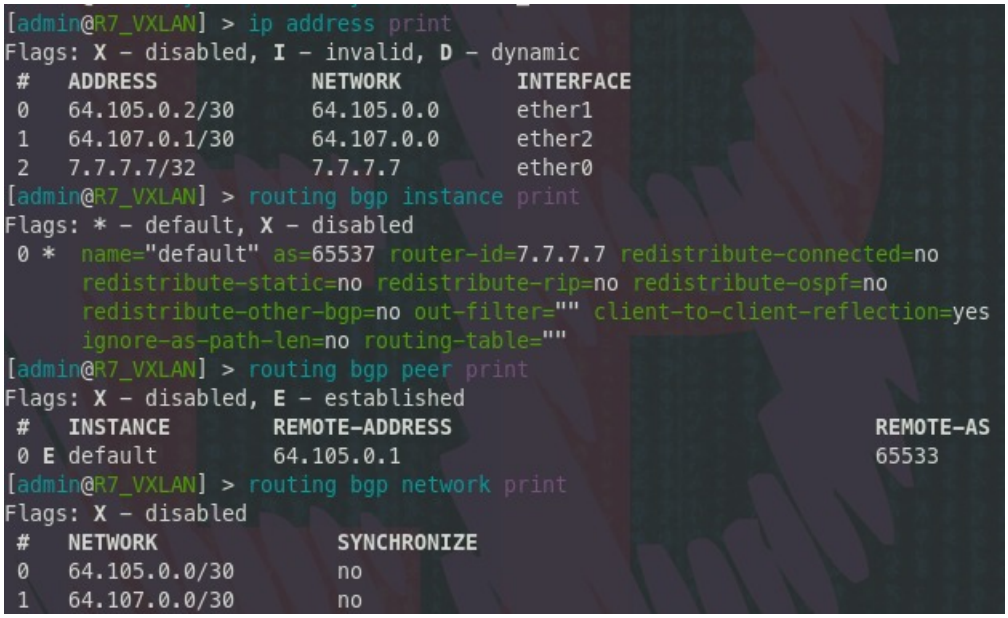


Fig. 19. Configuración de direcciones IP y Protocolo BGP en el border router R7 VXLAN.

Configuración de rutas estáticas para EoIP

Además, se añadieron manualmente rutas estáticas en cada uno de estos routers para mejorar el enrutamiento en la red. Estas rutas fueron diseñadas para dirigir el tráfico de manera específica, de acuerdo con los requisitos de la red, asegurando una conectividad confiable y eficiente en toda la infraestructura. La línea número 3 muestra una ruta estática para la red con una puerta de enlace designada como ”Db”. Estas configuraciones se presentan detalladamente en la Figura 20 y Figura 21.

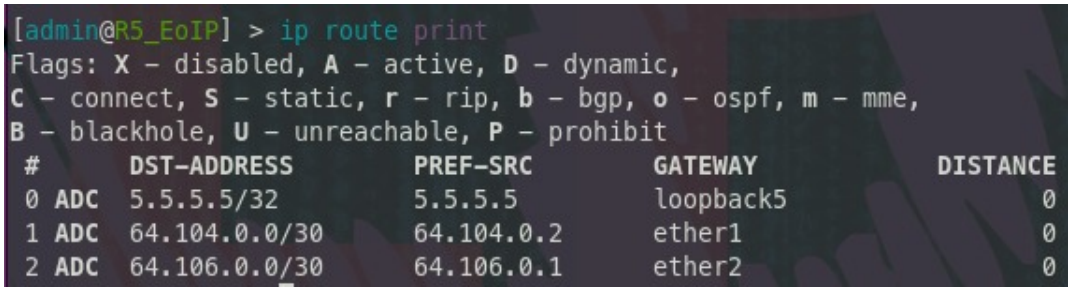


Fig. 20. Verificación de rutas estaticas en el border router R5 EoIP.

```
[admin@R7_EoIP] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  7.7.7.7/32         7.7.7.7         ether0                    0
 1 ADC  64.105.0.0/30      64.105.0.2      ether1                    0
 2 ADC  64.107.0.0/30      64.107.0.1      ether2                    0
```

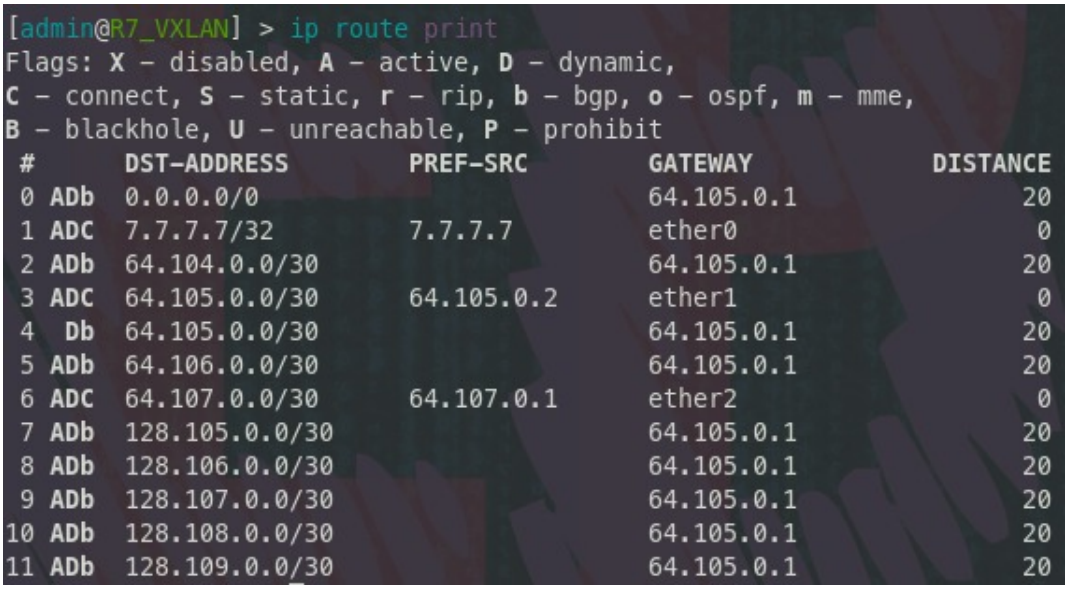
Fig. 21. Verificación de rutas estaticas en el border router R7 EoIP.

Configuración de rutas estáticas para VXLAN

Para VXLAN, se implementaron las mismas configuraciones en cada uno de los routers, incluyendo la adición manual de rutas estáticas para optimizar el enrutamiento. Estas rutas se diseñaron para gestionar el tráfico de manera específica, proporcionando una conectividad sólida y eficiente en toda la infraestructura de red. Los detalles de estas configuraciones se muestran en las mismas Figuras 22 y Figura 23.

```
[admin@R5_VXLAN] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADb  0.0.0.0/0                          64.104.0.1               20
 1 ADC  5.5.5.5/32         5.5.5.5         loopback5                 0
 2 ADC  64.104.0.0/30      64.104.0.2      ether1                    0
 3  Db  64.104.0.0/30                      64.104.0.1               20
 4 ADb  64.105.0.0/30                      64.104.0.1               20
 5 ADC  64.106.0.0/30      64.106.0.1      ether2                    0
 6 ADb  64.107.0.0/30                      64.104.0.1               20
 7 ADb  128.105.0.0/30                     64.104.0.1               20
 8 ADb  128.106.0.0/30                     64.104.0.1               20
 9 ADb  128.107.0.0/30                     64.104.0.1               20
10 ADb  128.108.0.0/30                     64.104.0.1               20
11 ADb  128.109.0.0/30                     64.104.0.1               20
```

Fig. 22. Verificación de rutas estaticas en el border router R5 VXLAN.



```
[admin@R7_VXLAN] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADb  0.0.0.0/0                          64.105.0.1               20
 1 ADC  7.7.7.7/32         7.7.7.7         ether0                    0
 2 ADb  64.104.0.0/30                      64.105.0.1               20
 3 ADC  64.105.0.0/30      64.105.0.2      ether1                    0
 4  Db  64.105.0.0/30                      64.105.0.1               20
 5 ADb  64.106.0.0/30                      64.105.0.1               20
 6 ADC  64.107.0.0/30      64.107.0.1      ether2                    0
 7 ADb  128.105.0.0/30                     64.105.0.1               20
 8 ADb  128.106.0.0/30                     64.105.0.1               20
 9 ADb  128.107.0.0/30                     64.105.0.1               20
10 ADb  128.108.0.0/30                     64.105.0.1               20
11 ADb  128.109.0.0/30                     64.105.0.1               20
```

Fig. 23. Verificación de rutas estaticas en el border router R7 VXLAN.

Configuración de tuneles EoIP

La configuración Ethernet over IP en los routers R6 y R8 se llevó a cabo mediante la creación de un túnel EoIP. En el router R6, se estableció el túnel EoIP utilizando el comando /interface eoip add name=.eoip-tunel1, seguido de su habilitación remota con /interface eoip enable eoip-tunel1". En el router remoto (R8), se configuró un túnel EoIP adicional con el comando /interface eoip add name=.eoip-tunel2, habilitándolo como túnel principal con /interface eoip enable eoip-tunel2". Luego, se creó un puente entre la interfaz local y el túnel EoIP en ambos routers: en R6 se utilizó /interface bridge add name=bridge1-eoip"seguido de /interface bridge port add bridge=bridge1-eoip interface=eoip-tunel1ᴢ /interface bridge port add bridge=bridge1-eoip interface=ether2", mientras que en R8 se emplearon los mismos comandos con la diferencia de la interfaz del túnel (/interface bridge port add bridge=bridge1-eoip interface=eoip-tunel2"). Esta configuración permite la comunicación eficiente entre los routers R6 y R8 mediante el túnel EoIP establecido, facilitando así el intercambio de datos en la red. Los resultados de estas configuraciones se pueden observar en la Figura 24 y Figura 25.

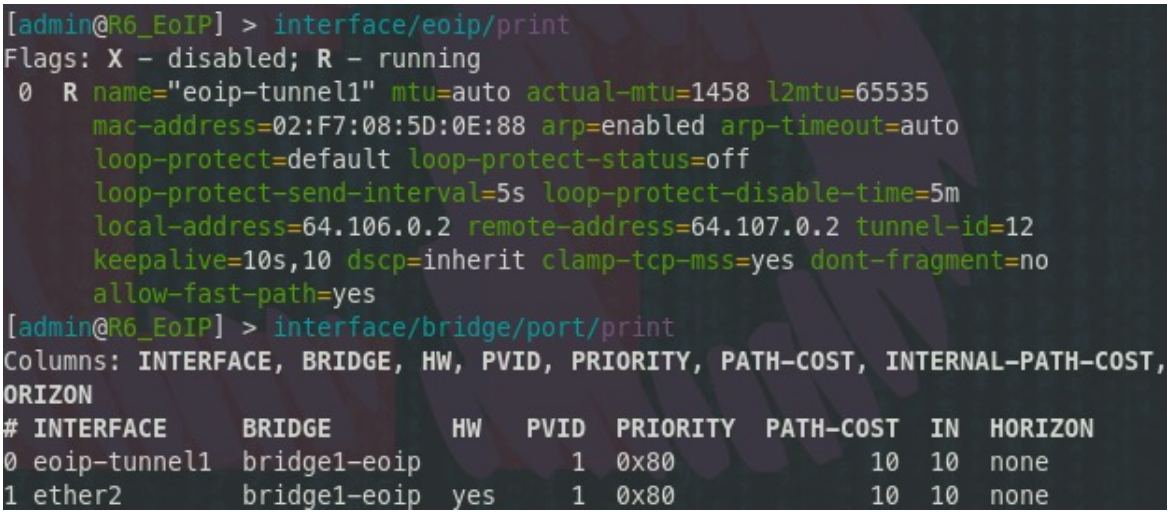


Fig. 24. Configuración de protocolo Ethernet/IP en el router R6 EoIP.

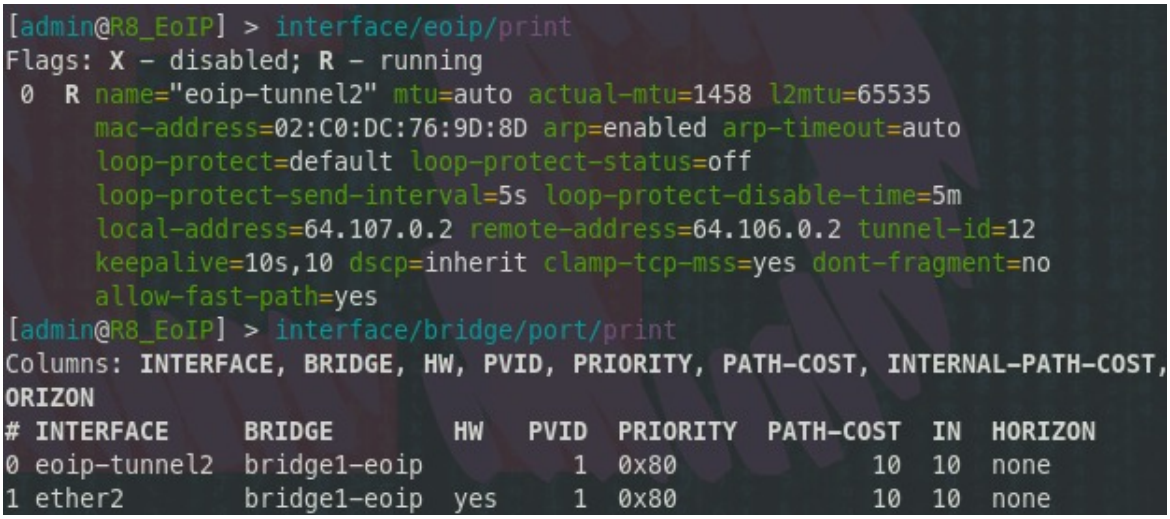


Fig. 25. Configuración de protocolo Ethernet/IP en el router R8 EoIP.

Configuración de tuneles VXLAN

Para la configuración VXLAN en los routers R6 y R8 se realizó la creación de un túnel VXLAN. En el router R6, se estableció el túnel VXLAN utilizando el comando /interface vxlan add name=vxlan1", seguido de su habilitación remota con /interface vxlan enable vxlan1". En el router remoto (R8), se configuró un túnel VXLAN adicional con el comando /interface vxlan add name=vxlan1", habilitándolo como túnel principal con /interface vxlan enable vxlan1". Luego, se creó un puente entre la interfaz local y el túnel VXLAN en ambos routers: en R6 se utilizó /interface bridge add name=bridgeVxlan"seguido de /interface bridge

port add bridge=bridgeVxlan interface=vxlan1ƨ /interface bridge port add bridge=bridgeVxlan interface=ether1”, mientras que en R8 se emplearon los mismos comandos con la diferencia de la interfaz del túnel (/interface bridge port add bridge=bridgeVxlan interface=vxlan1”). Esta configuración permite la comunicación eficiente entre los routers R6 y R8 mediante el túnel VXLAN establecido, facilitando así el intercambio de datos en la red. Los resultados de estas configuraciones se pueden observar en la Figura 26 y Figura 27.

```
[admin@R6_VXLAN] > interface/vxlan/print
Flags: R - RUNNING
Columns: NAME, MTU, ARP, VNI, PORT, VTEPS-IP-VERSION, VRF
#   NAME     MTU  ARP      VNI  PORT  VTEPS-IP-VERSION  VRF
0 R vxlan1  1500  enabled   10  8472  ipv4              main
[admin@R6_VXLAN] > interface/vxlan/fdb/print
 0 remote-ip=0.0.0.0 mac-address=C6:55:CF:FD:39:F7 interface=vxlan1

 1 remote-ip=0.0.0.0 mac-address=AE:CA:11:65:4A:BC interface=vxlan1

 2 remote-ip=64.107.0.2 mac-address=AE:CA:11:65:4A:BC interface=vxlan1

 3 remote-ip=64.107.0.2 mac-address=C6:55:CF:FD:39:F7 interface=vxlan1
[admin@R6_VXLAN] > interface/bridge/port/print
Columns: INTERFACE, BRIDGE, HW, PVID, PRIORITY, PATH-COST, INTERNAL-PATH-COST, H
ORIZON
# INTERFACE  BRIDGE       HW   PVID  PRIORITY  PATH-COST  IN  HORIZON
0 ether2     bridgeVxlan  yes     1  0x80             10  10  none
1 vxlan1     bridgeVxlan          1  0x80             10  10  none
```

Fig. 26. Configuración de protocolo VXLAN en el router R6 VXLAN.

```
[admin@R8_VXLAN] > interface/vxlan/print
Flags: R - RUNNING
Columns: NAME, MTU, ARP, VNI, PORT, VTEPS-IP-VERSION, VRF
#   NAME     MTU  ARP      VNI  PORT  VTEPS-IP-VERSION  VRF
0 R vxlan1  1500  enabled   10  8472  ipv4              main
[admin@R8_VXLAN] > interface/vxlan/fdb/print
 0 remote-ip=0.0.0.0 mac-address=2A:24:0B:E3:98:A3 interface=vxlan1

 1 remote-ip=64.106.0.2 mac-address=2A:24:0B:E3:98:A3 interface=vxlan1
[admin@R8_VXLAN] > interface/bridge/port/print
Columns: INTERFACE, BRIDGE, HW, PVID, PRIORITY, PATH-COST, INTERNAL-PATH-COST, H
ORIZON
# INTERFACE  BRIDGE       HW   PVID  PRIORITY  PATH-COST  IN  HORIZON
0 vxlan1     bridgeVxlan          1  0x80             10  10  none
1 ether2     bridgeVxlan  yes     1  0x80             10  10  none
```

Fig. 27. Configuración de protocolo VXLAN en el router R8 VXLAN.

Configuración de PCs para EoIP

Para finalizar la configuración, se añaden las direcciones IP a las PCs de ambas sucursales (UbuntuDockerEoIp1 y UbuntuDockerEoIp2). Dado que ambas sucursales comparten las mismas redes gracias al túnel EpIP configurado anteriormente, se asignan las direcciones IP 192.168.2.2 y 192.168.2.3 respectivamente. La configuración se realiza mediante el siguiente comando en cada PC: "ip addr add [dirección IP/máscara de red] dev eth0". Esta configuración asegura la conectividad adecuada entre las PCs y el resto de la red, permitiendo la comunicación eficiente entre las sucursales A y B. Los resultados de estas configuraciones se pueden observar en la Figura 28 y Figura 29.

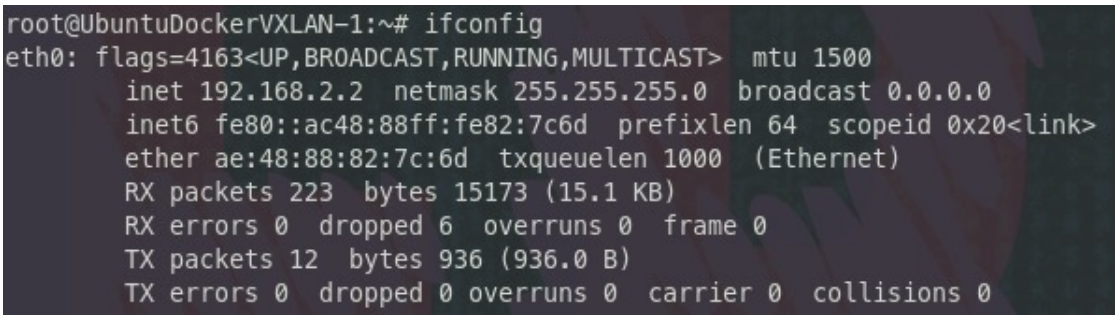


Fig. 28. Configuración de PC1.

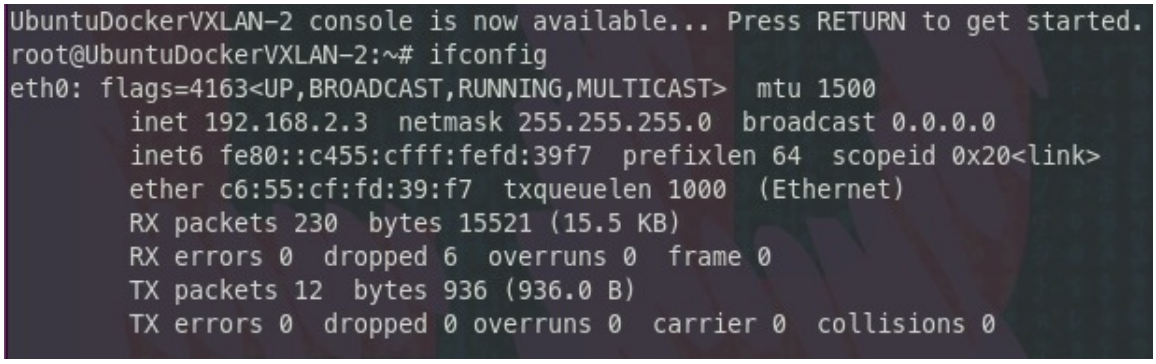


Fig. 29. Configuración de PC2.

Configuración de PCs para VXLAN

En las PCs de la topología VXLAN (UbuntuDockerVXLAN1 y UbuntuDockerVXLAN2) se realizan las mismas configuraciones para garantizar la conectividad adecuada y la comunicación eficiente entre las sucursales A y B. Los resultados de estas configuraciones se pueden observar en la Figura 30 y Figura 31.

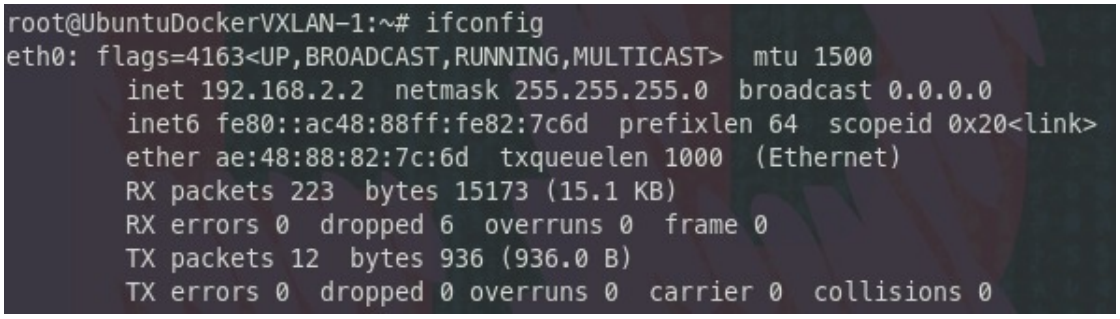


Fig. 30. Configuración de PC1.

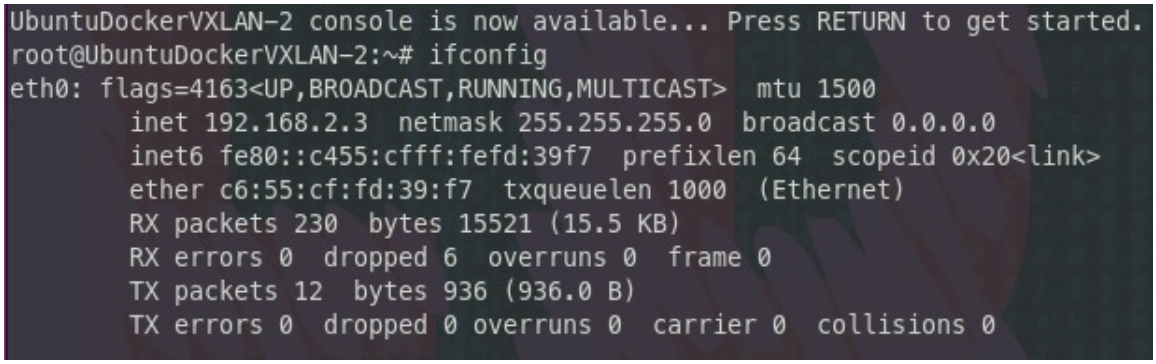


Fig. 31. Configuración de PC2.

5. Operación

Prueba de comunicación para EoIP

Durante esta fase, se monitoreó el estado de la red EoIP, realizando pruebas de ping de una PC a otra para confirmar la correcta implementación de las tecnologías mencionadas anteriormente. La Figura 32 muestra la verificación de la comunicación desde la PC1 hasta la PC2.

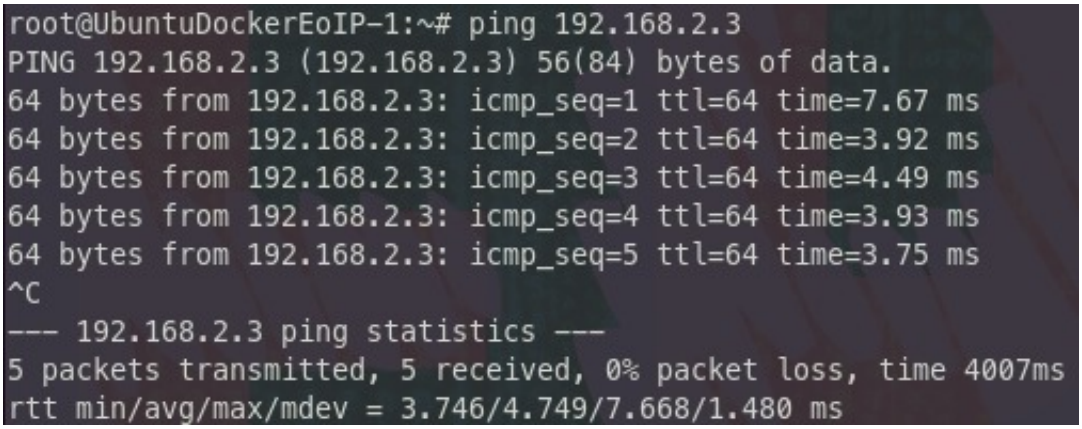


Fig. 32. Ping de Pc1 a Pc2.

Prueba de comunicación para VXLAN

Para la red VXLAN, en esta etapa se realizó un monitoreo del estado de la red, llevando a cabo pruebas de ping de una PC a otra para confirmar la implementación adecuada de las tecnologías específicas de VXLAN. La Figura 33 muestra la verificación de la comunicación desde la PC1 hasta la PC2 en la topología VXLAN.

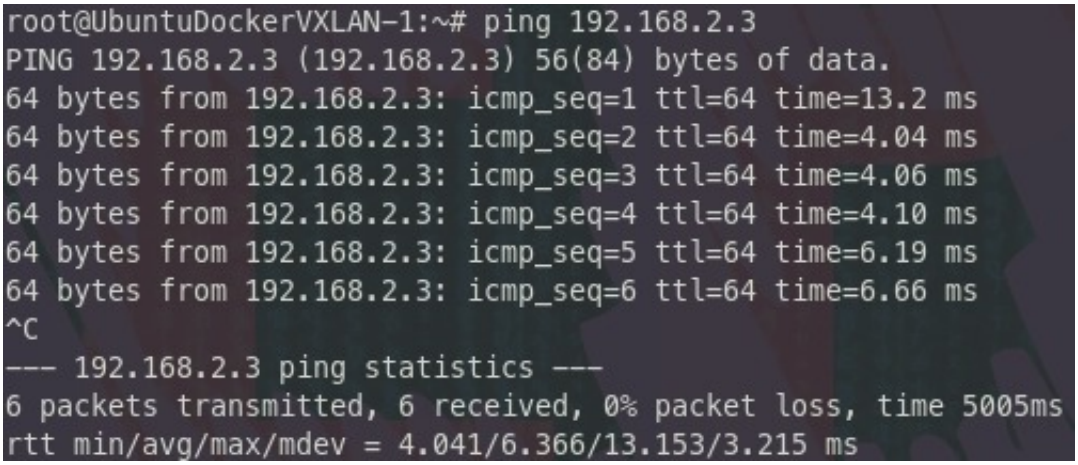


Fig. 33. Ping de Pc1 a Pc2.

6. Optimización

Se llevó a cabo una optimización en la red, que incluyó reforzar la seguridad de los routers mediante la configuración de una contraseña robusta para el modo privilegiado. Esto se logró utilizando el comando /user set admin password=NUEVA CONTRASEÑA". Cabe destacar que esta medida de seguridad se implementó tanto en la topología Ethernet sobre IP como en la

de VXLAN, tal como se muetsra en la Figura 34 y Figura 35.

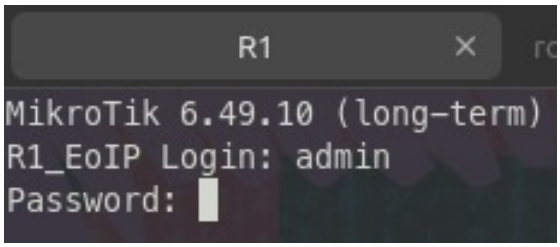


Fig. 34. Configuraciones de seguridad en topologia EoIP.

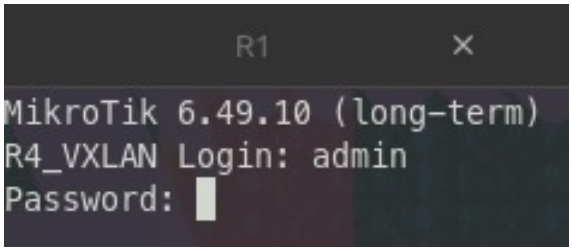


Fig. 35. Configuraciones de seguridad en topologia VXLAN.

IV. RESULTADOS

Se evalúa la topología implementada: una utilizando el protocolo EoIP y la otra con VXLAN. El objetivo es analizar y medir parámetros como la latencia, el ancho de banda, la tasa de transferencia y la eficiencia del tráfico. Estos resultados permitirán identificar las ventajas y desventajas específicas en el rendimiento de cada una de estas tecnologías.

Resultados de pruebas de ping para EoIP

En los resultados de la prueba de ping entre las sucursales utilizando los túneles EoIP, se observa una conectividad estable y confiable entre los dispositivos de ambas sucursales. Los tiempos de respuesta (latencia) son consistentes y relativamente bajos, con valores que oscilan entre 6.58 ms y 17.0 ms. Esto sugiere una buena calidad de conexión y una baja latencia en la comunicación entre las sucursales.

La respuesta del ping muestra que los paquetes ICMP (Internet Control Message Protocol) se entregan de manera eficiente y sin pérdida notable en el tráfico. Cada paquete ICMP enviado desde la sucursal origen (192.168.2.2) hacia la sucursal destino (192.168.2.3) recibe una respuesta exitosa (64 bytes recibidos) con un número secuencial de secuencia ICMP.

Además, el valor del campo TTL (Time To Live) en las respuestas ICMP muestra que los paquetes tienen un TTL de 64, lo que indica que están siendo reenviados correctamente a través de la red y alcanzando su destino sin problemas de tiempo de vida del paquete.

Los resultados de la prueba de ping indican una conectividad efectiva y eficiente entre las sucursales utilizando los túneles EoIP, con tiempos de respuesta bajos y consistentes, lo que sugiere un rendimiento satisfactorio de la infraestructura de red implementada, todo esto se puede observar en la Figura 36.

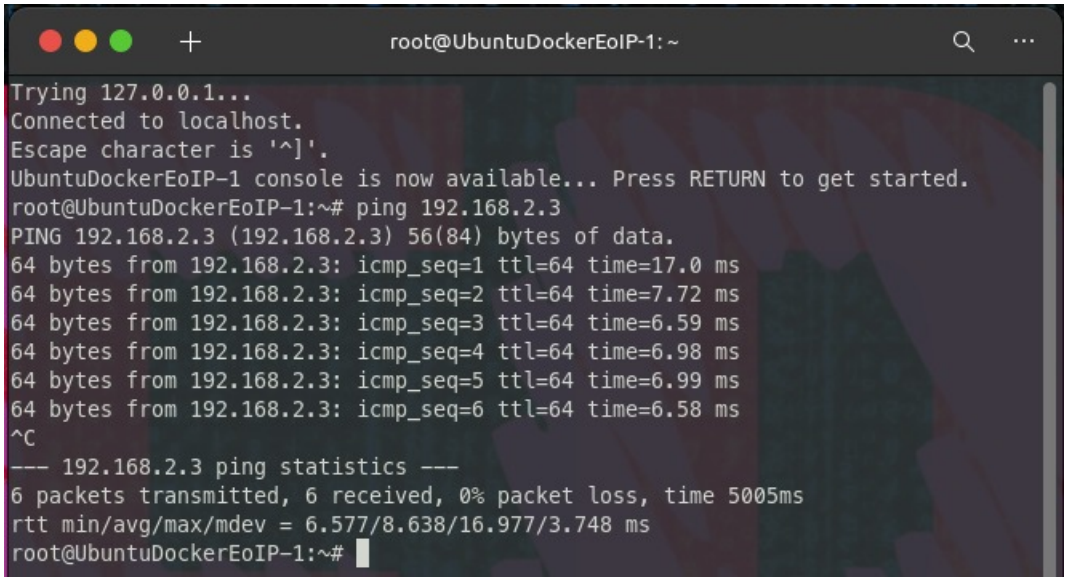


Fig. 36. Ping entre ambas sucursales en topologia EoIP.

Resultados de pruebas de ping para VXLAN

En los resultados de la prueba de ping utilizando la topología VXLAN, se observa una conectividad estable y efectiva entre el host local de la sucursal A y la dirección IP 192.168.2.3 correspondiente a la sucursal B.

Durante la prueba, se enviaron un total de 6 paquetes ICMP desde el host local hacia la dirección IP de la sucursal B. Todos los paquetes fueron recibidos con éxito, lo que indica una tasa de pérdida de paquetes del cero porciento.

Los tiempos de respuesta (latencia) registrados durante la prueba son consistentes y relativamente bajos, con un tiempo mínimo de 4.830 ms, un tiempo promedio de 6.547 ms y un tiempo máximo de 8.160 ms. Esto sugiere una buena calidad de conexión y una baja latencia en la comunicación entre las sucursales.

Los resultados de la prueba de ping indican una conectividad confiable y eficiente entre las sucursales A y B utilizando la topología VXLAN, con una tasa de pérdida de paquetes insignificante y tiempos de respuesta aceptables para la transferencia de datos entre los dispositivos de ambas sucursales, todo esto se puede observar en la Figura 37.

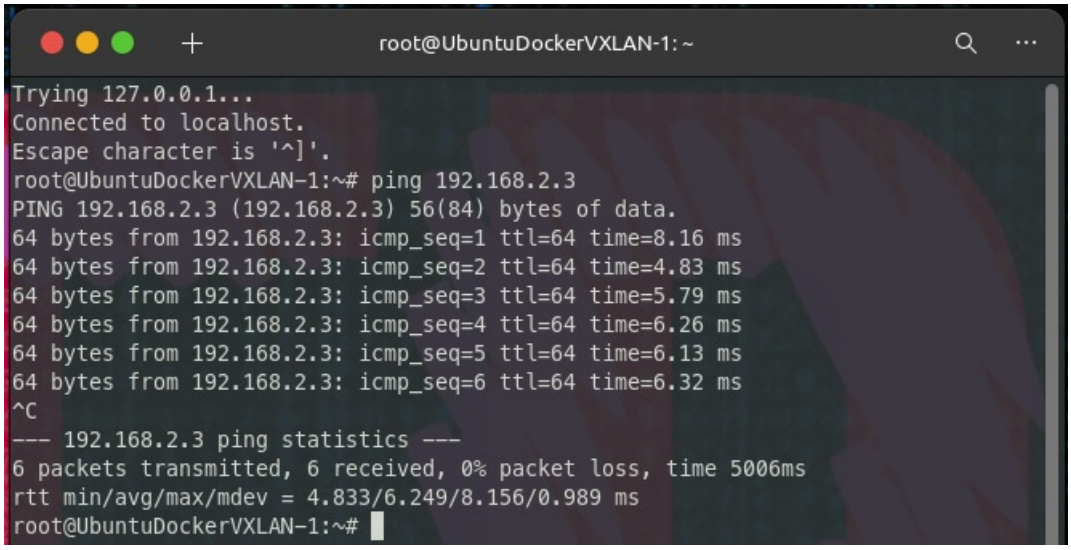


Fig. 37. Ping entre ammbas sucursales en topologia VXLAN.

Análisis comparativo entre EoIP y VXLAN

A continuación se presenta un análisis comparativo entre EoIP y VXLAN en términos de conectividad y rendimiento. Los resultados revelan que ambas topologías lograron transmitir y recibir todos los paquetes sin pérdida. Además, se observa que la topología VXLAN exhibió un ligero menor tiempo promedio de respuesta en comparación con la topología EoIP, lo que sugiere un rendimiento superior en términos de latencia. Estos hallazgos respaldan la eficacia de ambas tecnologías en la creación de redes virtuales escalables y de alto rendimiento. Consulte la Tabla III para más detalles.

TABLA III
ANÁLISIS ENTRE LAS TOPOLOGÍAS EoIP Y VXLAN EN TÉRMINOS DE CONECTIVIDAD Y RENDIMIENTO.

Topología	**Paquetes transmitidos**	**Paquetes recibidos**	**Pérdida de paquetes**	**Tiempo promedio de respuesta (ms)**	**Tiempo mínimo de respuesta (ms)**	**Tiempo máximo de respuesta (ms)**
EoIP	6	6	0	8.638	6.577	16.977
VXLAN	6	6	0	6.547	4.830	8.160

Resultados de pruebas de HPING3 para EoIP

Las siguientes pruebas se realizaron utilizando la herramienta HPING3, la cual permite enviar paquetes de datos personalizados con diferentes parámetros y analizar las respuestas recibidas. En este contexto, se empleó HPING3 para evaluar la conectividad y la latencia en la topología EoIP. Al enviar paquetes de datos con un tamaño de 1500 bytes a la dirección IP 192.168.2.3 desde el host de origen, se confirmó la recepción exitosa de todos los paquetes en el host de destino, sin pérdida de datos, lo que demuestra una comunicación efectiva entre los dispositivos.

El análisis de los tiempos de respuesta (RTT) revela una variación en los tiempos de viaje de los paquetes, con un RTT mínimo de 6.6 ms, un promedio de 18.5 ms y un máximo de 33.4 ms. Estos valores muestran una latencia razonablemente baja en la comunicación entre las sucursales, lo que sugiere un rendimiento aceptable de la red bajo estas condiciones.

La distribución de los tiempos de respuesta muestra que la mayoría de los paquetes tienen un RTT dentro del rango de 10 a 20 ms, con algunos picos que alcanzan valores más altos, pero en general se mantiene dentro de un margen aceptable para aplicaciones de comunicación en tiempo real, como voz sobre IP (VoIP) o videoconferencias, todo esto se puede observar en la Figura 38.

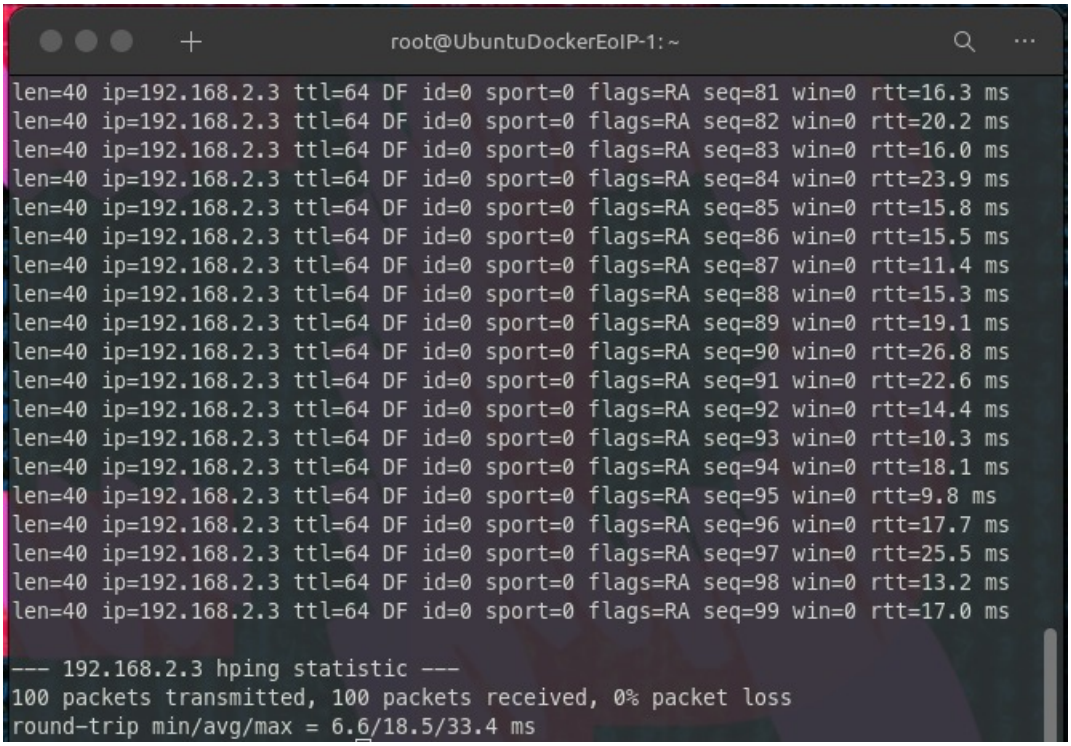


Fig. 38. Envio de paquetes para EoIP.

Resultados de pruebas de HPING3 para VXLAN

Las pruebas realizadas con la herramienta HPING3 en la topología VXLAN proporcionaron resultados destacables en cuanto a la conectividad y latencia. Al enviar paquetes de datos con un tamaño de 1500 bytes a la dirección IP 192.168.2.3 desde el host de origen, se confirmó la recepción exitosa de todos los paquetes en el host de destino, sin pérdida de datos, lo que indica una comunicación eficaz entre los dispositivos.

En cuanto a la latencia, se observó que el tiempo mínimo de ida y vuelta (RTT) fue de 7.8 ms, lo que sugiere que en algunos casos la comunicación fue muy rápida. El tiempo promedio de RTT fue de 14.5 ms, indicando el tiempo medio que tardaba un paquete en viajar desde el host de origen hasta el host de destino y volver. Por otro lado, el tiempo máximo registrado fue de 25.6 ms, lo que señala los casos en los que la comunicación experimentó una mayor demora.

Los resultados obtenidos para la red VXLAN muestran una distribución de los tiempos de respuesta en un margen bastante consistente. La mayoría de los paquetes tienen un RTT dentro del rango de 10 a 20 ms, lo que sugiere una latencia bastante estable y adecuada para aplicaciones sensibles al tiempo, como la transmisión de voz sobre IP (VoIP) o videoconferencias. Aunque

se observan algunos picos que alcanzan valores más altos, el hecho de que la mayoría de los paquetes se mantengan en este rango indica una buena calidad de servicio en términos de latencia para la red VXLAN, todo esto se puede observar en la Figura 39.

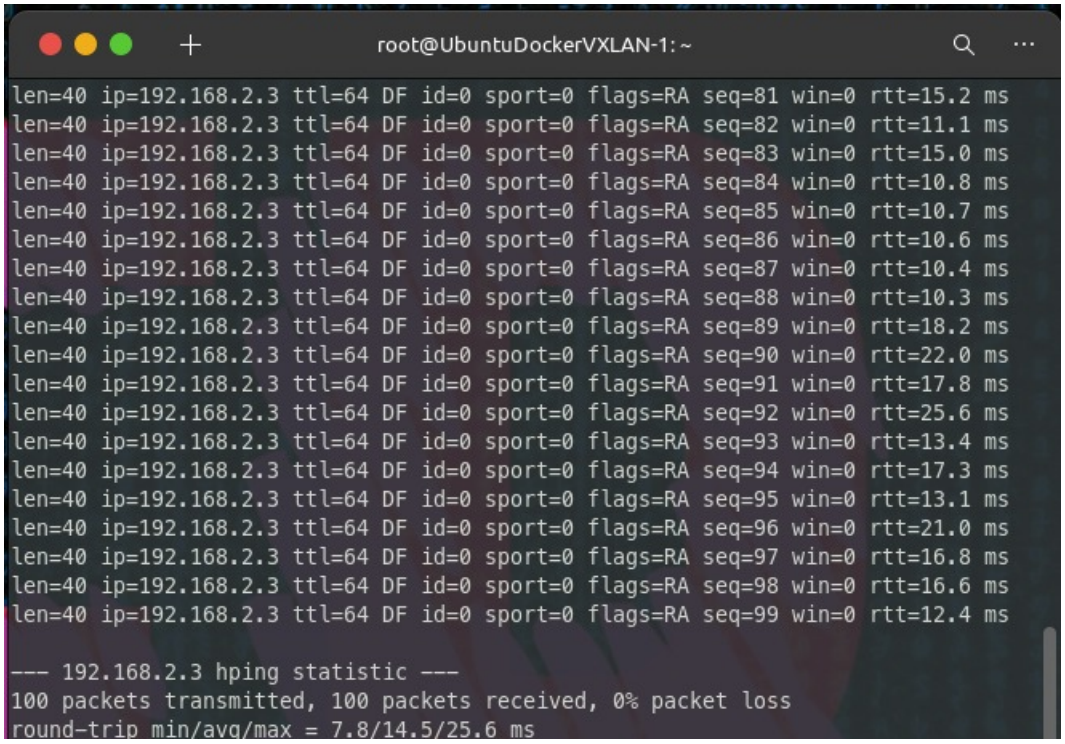


Fig. 39. Envio de paquetes para VXLAN.

Análisis comparativo entre EoIP y VXLAN

La tabla IV ofrece una comparación detallada entre las topologías EoIP y VXLAN en términos de tiempo de respuesta y pérdida de paquetes. Ambas tecnologías muestran tiempos de respuesta mínimos comparables, aunque con una ligera ventaja para VXLAN en cuanto al tiempo de respuesta promedio. Además, es importante destacar que ninguna de las topologías presentó pérdida de paquetes durante las pruebas realizadas, lo que demuestra la fiabilidad de ambas en términos de transmisión de datos.

TABLA IV
COMPARATIVA EN TIEMPO DE RESPUESA Y PÉRDIDA DE PAQUETES ENTRE LAS TOPOLOGÍAS EoIP Y VXLAN.

Topología	**Paquetes transmitidos**	**Paquetes recibidos**	**Pérdida de paquetes**	**Tiempo promedio de respuesta (ms)**	**Tiempo mínimo de respuesta (ms)**	**Tiempo máximo de respuesta (ms)**
EoIP	100	100	0	18.5	6.6	33.4
VXLAN	100	100	0	14.5	7.8	25.6

Resultados de pruebas con Wireshark para EoIP

En las siguientes pruebas se utilizó la herramienta Wireshark para monitorear los paquetes en la interfaz del host ubicado en la Sucursal A de la topología Ethernet over IP. Se inició el monitoreo de paquetes mientras se enviaban cien paquetes ICMP a la dirección IP remota de la Sucursal B. Estos paquetes fueron enviados con un intervalo de un segundo entre cada paquete, lo que permitirá analizar la latencia y otros aspectos del rendimiento de la red entre las sucursales, en la Figura 40 y en la Figura 41 se obsevra el envio de los paquetes y el monitoreo en la herramienta.

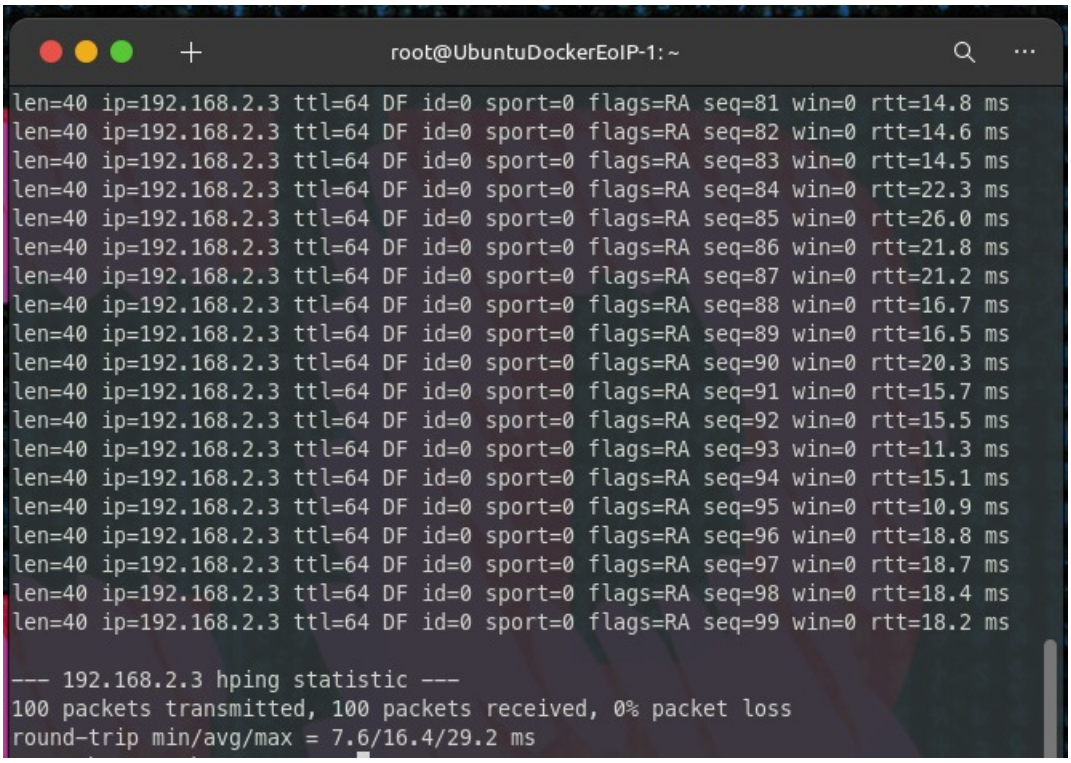


Fig. 40. Envio de paquetes para EoIP.

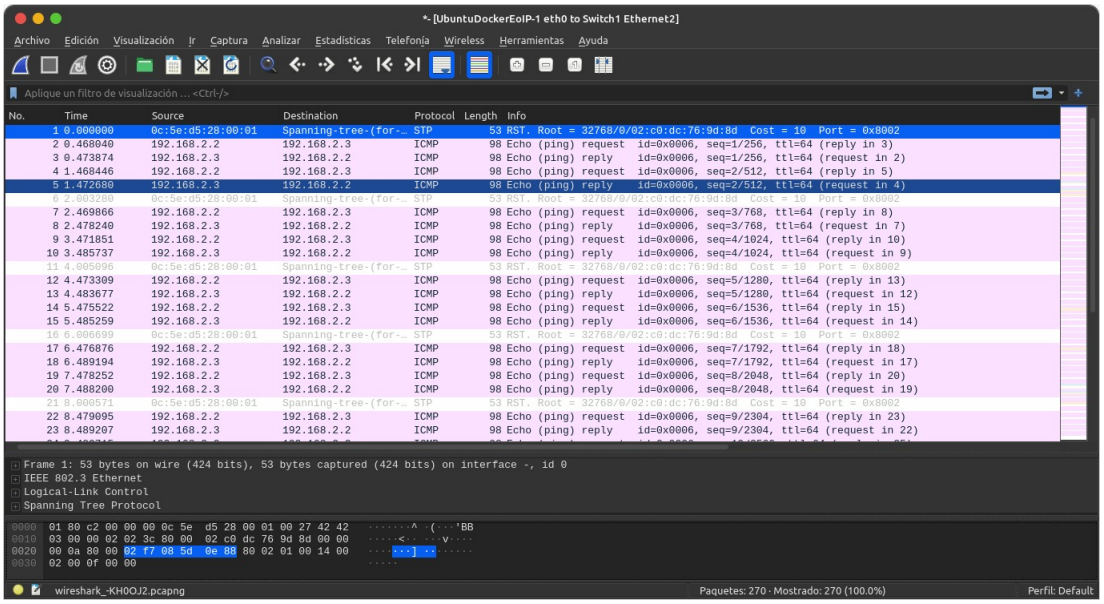


Fig. 41. Monitoreo de paquetes en EoIP.

Durante el monitoreo de la topología Ethernet over IP, se aplicó un filtro específico en Wireshark para analizar el tráfico generado por la Sucursal A hacia la Sucursal B. Este filtro, ip.src==192.168.2.2, se diseñó para capturar exclusivamente los paquetes de origen provenientes de la dirección IP de la Sucursal A (192.168.2.2), se observa una secuencia de paquetes ICMP de tipo ECHO request. Estos paquetes son enviados desde el host de la sucursal A hacia el host de la sucursal B con la intención de realizar un ping.

Cada paquete ICMP de solicitud tiene una longitud de 98 bytes y contiene un identificador (id=0x0006) y un número de secuencia único. El número de secuencia indica el orden de los paquetes y permite identificar si algún paquete se pierde en la red. Por ejemplo, el primer paquete tiene un número de secuencia de 1/256, lo que significa que es el primer paquete de una serie de 256.

La columna TIME indica el momento en el que se capturó cada paquete. Se puede observar un intervalo de tiempo aproximadamente constante entre el envío de cada paquete de solicitud, lo que sugiere un ritmo constante de envío de los paquetes ICMP, todo esto se evidencia en la Figura 42

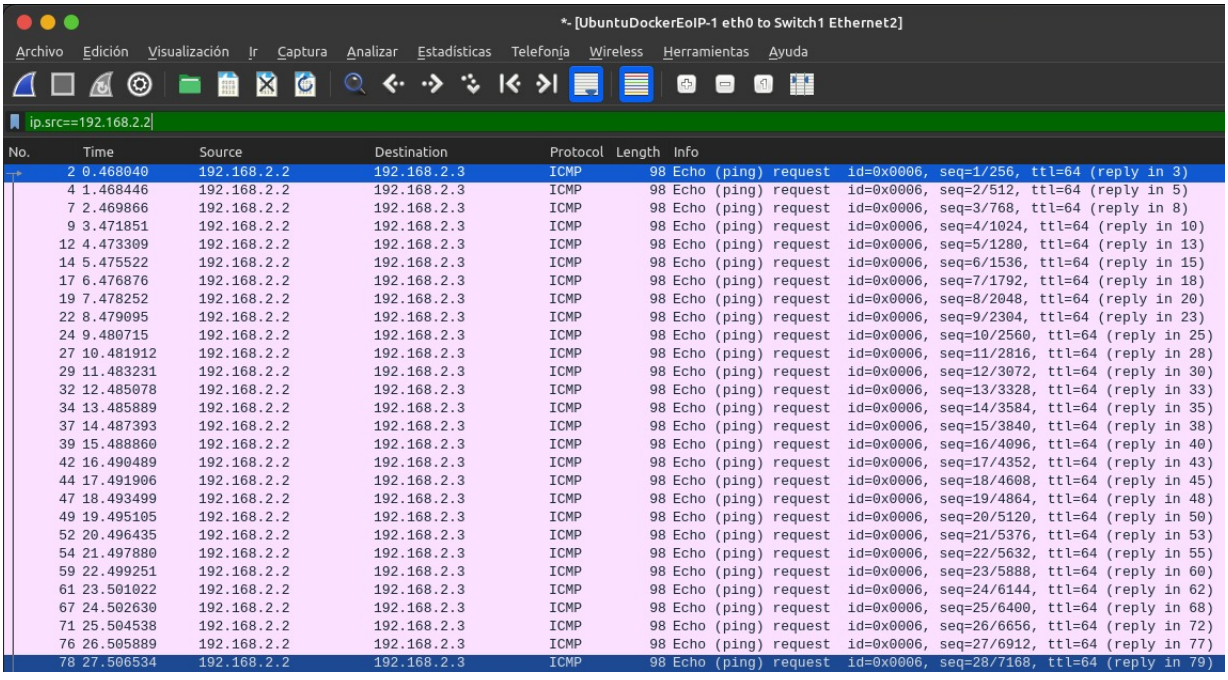


Fig. 42. Filtro de paquetes en Wireshark para EoIP.

Al aplicar el filtro ip.src==192.168.2.3 en la captura de la topología Ethernet over IP,

se observa una secuencia de paquetes ICMP de tipo ECHO reply. Estos paquetes son enviados desde el host de la sucursal B hacia el host de la sucursal A como respuesta a los paquetes de solicitud ICMP enviados desde la sucursal A.

Cada paquete ICMP de respuesta tiene una longitud de 98 bytes y contiene el mismo identificador que los paquetes de solicitud para establecer la correspondencia entre las solicitudes y las respuestas. El número de secuencia indica el número de secuencia de los paquetes de solicitud a los que se está respondiendo.

La columna TIME indica el momento en el que se capturó cada paquete. Al igual que con los paquetes de solicitud, se puede observar un intervalo de tiempo aproximadamente constante entre el envío de cada paquete de respuesta ICMP, todo esto se evidencia en la Figura 43.

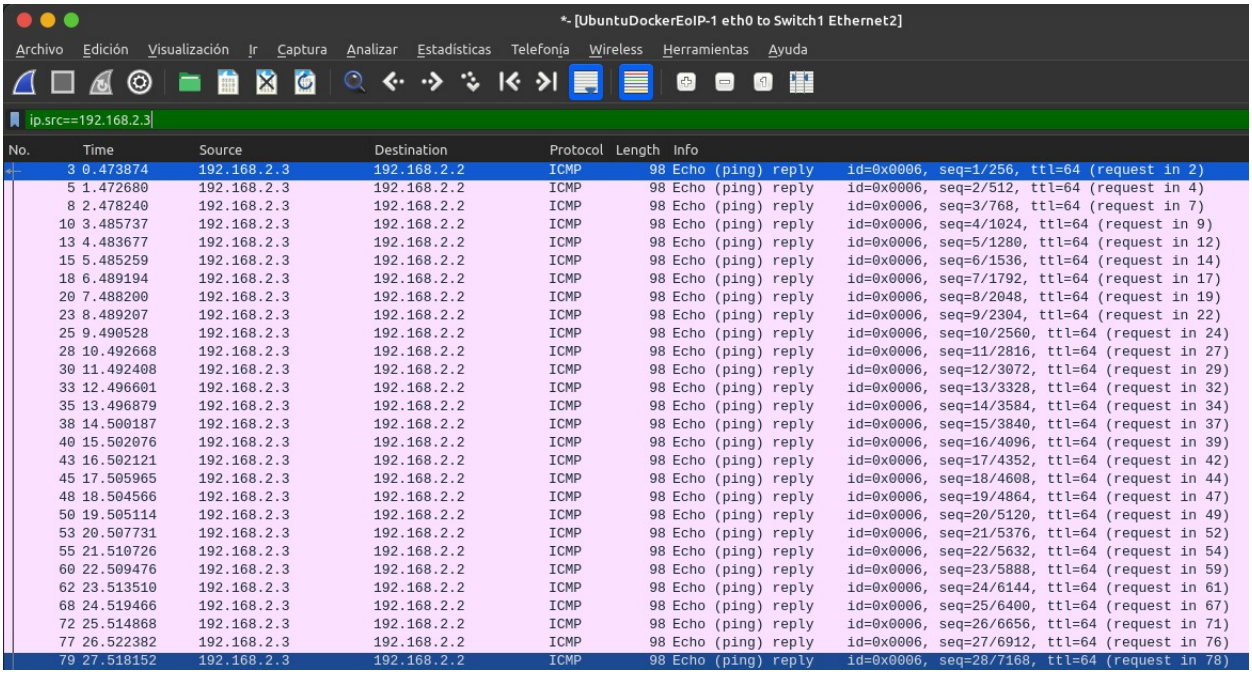


Fig. 43. Filtro de paquetes en Wireshark para la topologia EoIP.

La gráfica de E/S generada a partir de las estadísticas de Wireshark proporciona una representación visual del tráfico de paquetes a lo largo del tiempo en la captura realizada. Al analizar la gráfica, se observa una línea continua que representa el flujo de paquetes desde la sucursal A (192.168.2.2) y otra línea continua que representa el flujo de paquetes desde la sucursal B (192.168.2.3).

Durante el transcurso del tiempo, se pueden identificar varios picos en la linea que

muestra todos los paquetes, lo que indica momentos de mayor actividad de tráfico entre las sucrusales. Estos picos pueden ser indicativos de períodos de alta demanda de recursos de red o de transmisión de datos intensiva entre las dos ubicacionestodo, esto se evidencia en la Figura 44.

Fig. 44. Grafica de paquetes en Wireshark para EoIP

Resultados de pruebas con Wireshark para VXLAN

En las siguientes pruebas, se utilizará la herramienta Wireshark para monitorear los paquetes en la interfaz del host ubicado en la Sucursal A de la topología con VXLAN. Se iniciará el monitoreo de paquetes mientras se envían cien paquetes ICMP a la dirección IP remota de la Sucursal B. Estos paquetes serán enviados con un intervalo de un segundo entre cada paquete, lo que permitirá analizar la latencia y otros aspectos del rendimiento de la red entre las sucursales. En la Figura 45 y en la Figura 46 se observa el envío de los paquetes y el monitoreo en la herramienta.

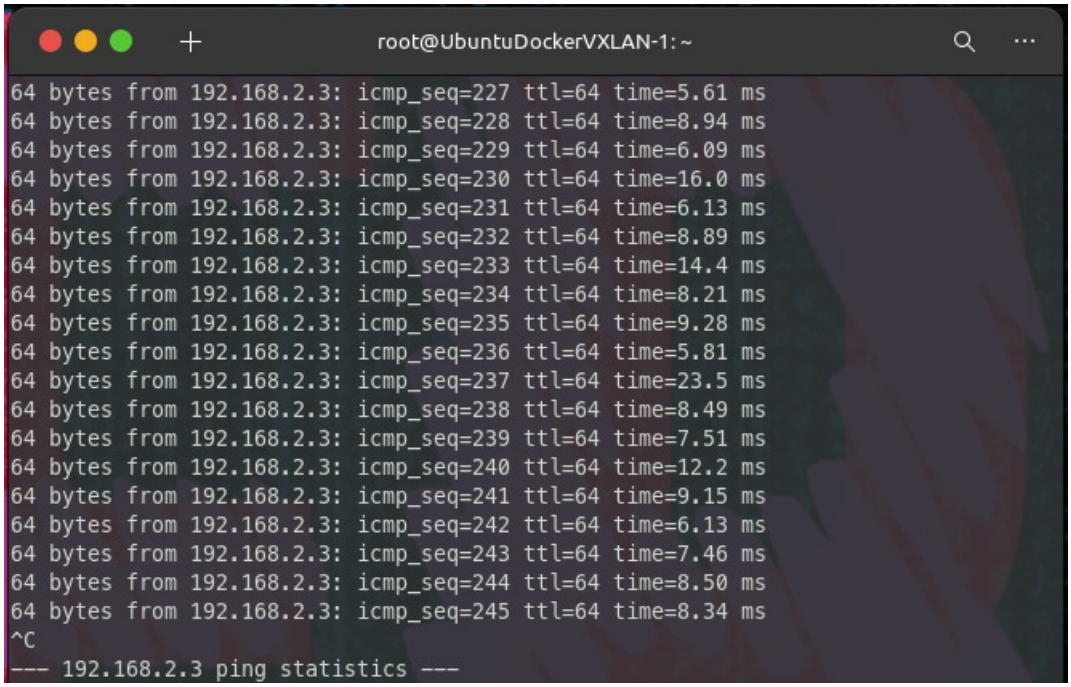


Fig. 45. Envio de paquetes para VXLAN.

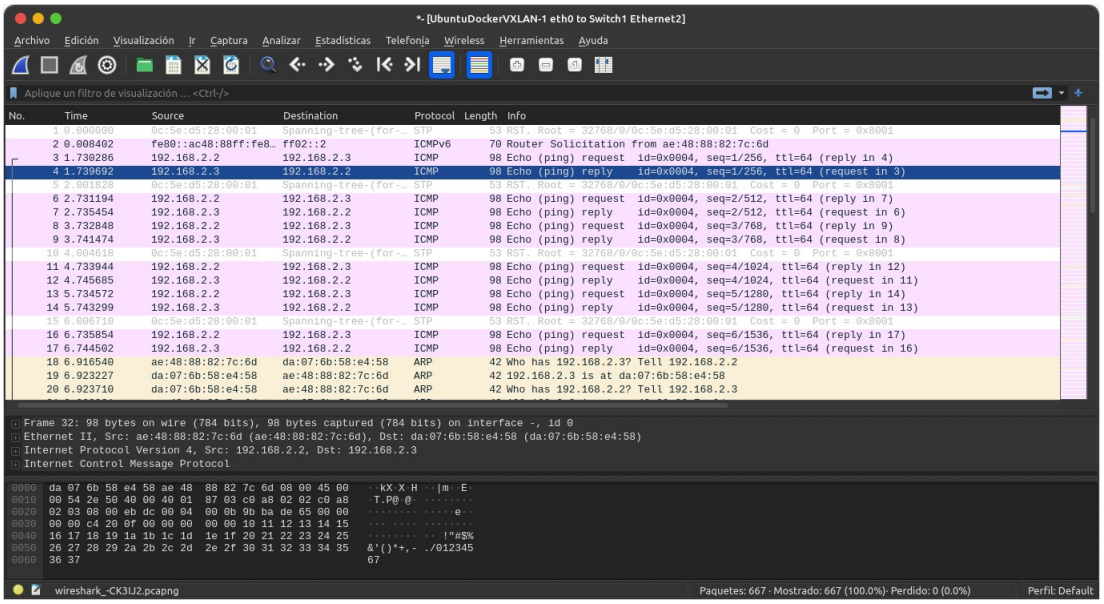


Fig. 46. Monitoreo de paquetes para VXLAN.

Después de filtrar los paquetes enviados desde la sucursal A con la dirección IP de origen 192.168.2.2, se observa una secuencia de paquetes ICMP de tipo ECHO request. Estos paquetes están destinados a la dirección IP de la sucursal B (192.168.2.3) y tienen una longitud de 98 bytes. Cada paquete ICMP tiene un identificador único (id=0x0004) y un número de secuencia que aumenta con cada paquete enviado.

La columna ”TIME”muestra el tiempo en el que se registró cada paquete. Los paquetes se envían con un intervalo de aproximadamente un segundo, como se evidencia en los tiempos registrados entre cada uno. Por ejemplo, el primer paquete se envió a las 1.730286 segundos, el segundo a las 2.731194 segundos, y así sucesivamente.

El protocolo utilizado para estos paquetes es ICMP (Protocolo de Mensaje de Control de Internet), que se utiliza comúnmente para enviar mensajes de control y errores en la red. En este caso, los paquetes son del tipo ECHO request, que se utiliza en las pruebas de conectividad para solicitar una respuesta de eco del host de destino, todo esto se evidencia en la Figura 47

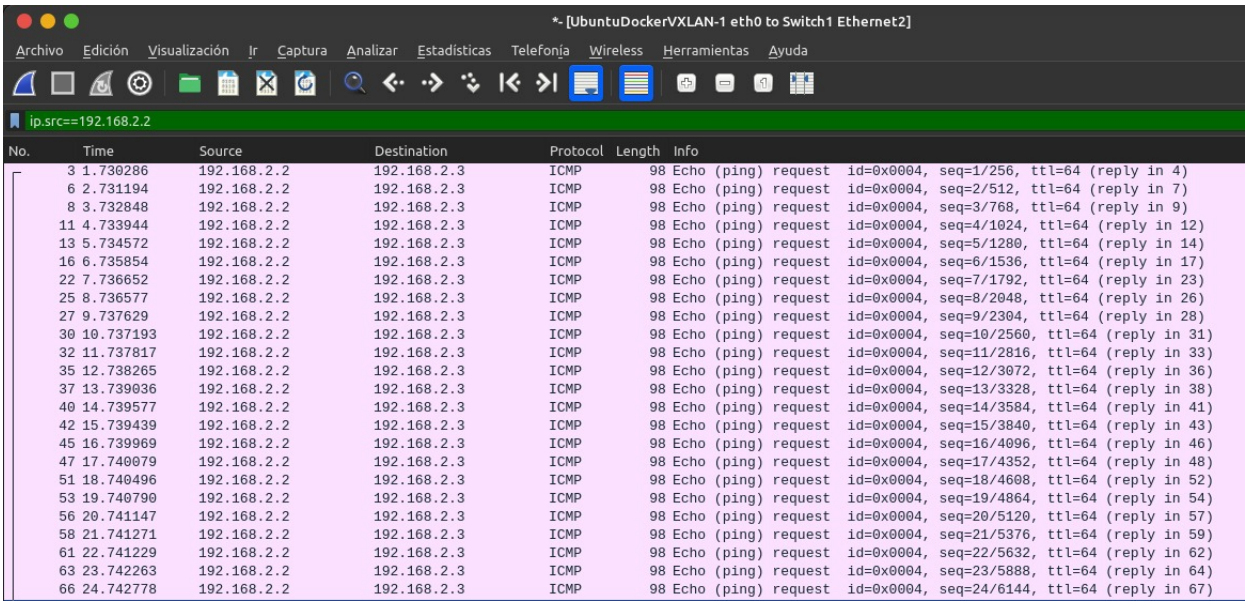


Fig. 47. Filtro de paquetes en Wireshark para topologia VXLAN

Al aplicar el filtro ip.src==192.168.2.3 en la misma captura de la topología VXLAN, se observa una secuencia de paquetes ICMP de tipo ECHO reply. Estos paquetes son respuestas a los paquetes ICMP ECHO request enviados previamente desde la sucursal A hacia la sucursal B. La dirección de origen de estos paquetes es 192.168.2.2, que corresponde al host de la sucursal

A, mientras que la dirección de destino es 192.168.2.3, que es el host de la sucursal B.

Los paquetes ICMP ECHO reply tienen la misma longitud que los paquetes ECHO request, que es de 98 bytes. Cada paquete ICMP de respuesta contiene un identificador (id=0x0004) y un número de secuencia que coincide con los paquetes de solicitud correspondientes. Por ejemplo, el primer paquete de respuesta tiene un número de secuencia de 1/256, lo que indica que está respondiendo al primer paquete de solicitud con el mismo número de secuencia.

La columna TIME muestra el tiempo en el que se registró cada paquete. Al igual que con los paquetes de solicitud, se observa un intervalo de aproximadamente un segundo entre cada paquete de respuesta, todo esto se evidencia en la Figura 48

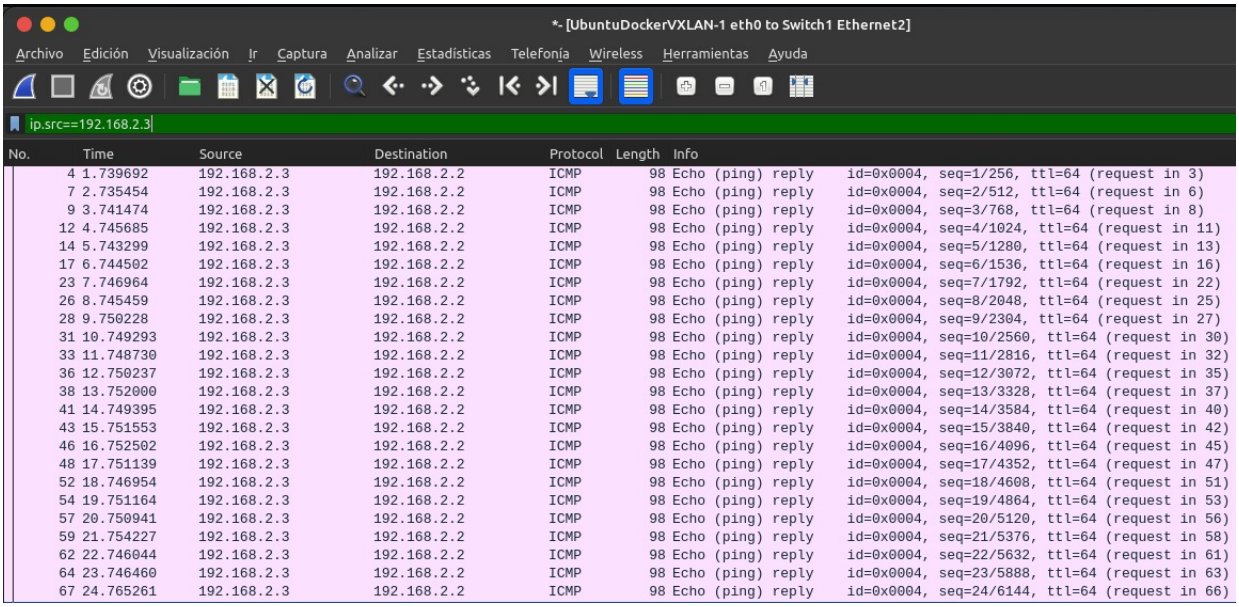


Fig. 48. Filtro de paquetes en Wireshark para topologia VXLAN

Después de analizar los datos obtenidos mediante la sección de Estadísticas y Gráficas de Wireshark, se generó un gráfico que ofrece una representación visual del tráfico de paquetes en la red. En este gráfico, se observa la evolución temporal de los paquetes capturados durante el período de monitoreo.

Una característica destacada es la presencia de picos en ciertos intervalos de tiempo, indicativos de momentos de mayor actividad en la red. Estos picos pueden deberse a ráfagas de tráfico o a eventos específicos en la comunicación entre las sucursales.

Además, se aplicaron filtros para distinguir el tráfico proveniente de la Sucursal A (ip.src==192.168.2.2)

y de la Sucursal B (ip.src==192.168.2.3). La línea correspondiente al filtro de la Sucursal A y la línea correspondiente al filtro de la Sucursal B son continuas en el gráfico, lo que facilita la comparación y el análisis del tráfico entre ambas sucursales.

Es importante destacar que la tercera línea en el gráfico muestra todos los paquetes capturados. Esta línea proporciona una visión general del tráfico total en la red, permitiendo contextualizar el tráfico específico de cada sucursal dentro del panorama general.

En comparación con el gráfico generado para la topología EoIP, se observa que en este gráfico de la topología con VXLAN, los picos pueden ser más pronunciados o presentarse en intervalos diferentes, lo que puede deberse a las características específicas de la comunicación en la red VXLAN, todo esto se evidencia en la Figura 49

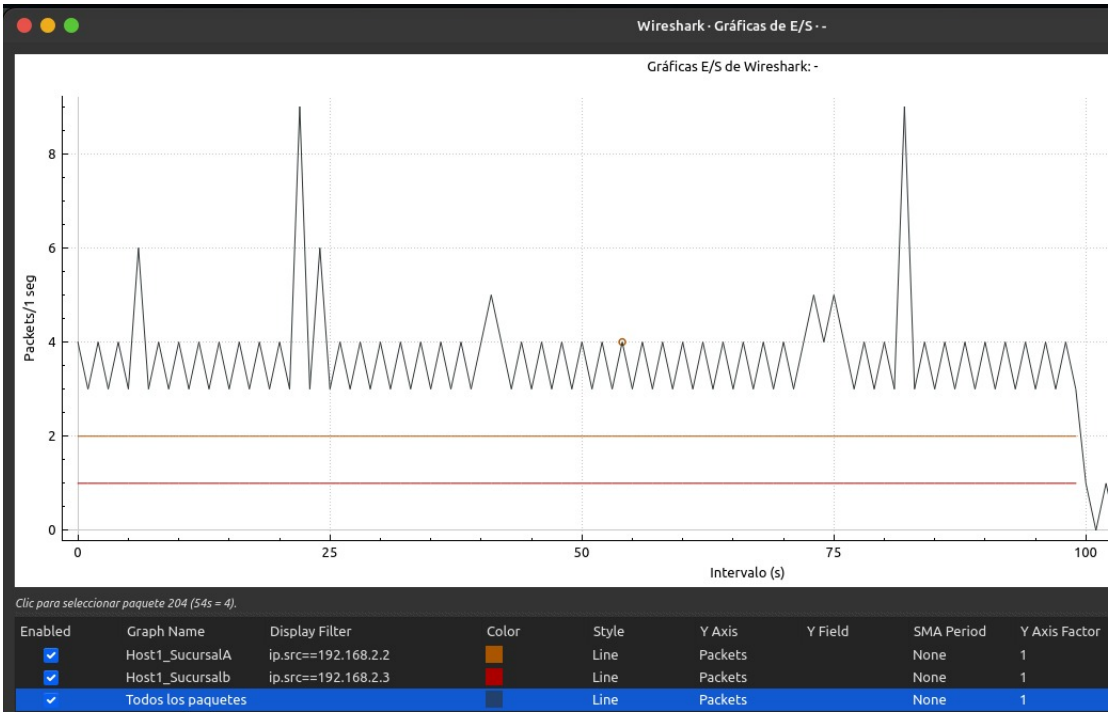


Fig. 49. Grafica de paquetes en Wireshark para la topologia VXLAN

Resultados de pruebas de IPERF para EoIP

El siguiente análisis comparativo que se realizó fue del ancho de banda para EoIP. Al analizar los resultados de las pruebas de ancho de banda para EoIP, se observa lo siguiente: En el host de la Sucursal A, configurado como el servidor iperf, se registró una transferencia de 7.25 MBytes durante un intervalo de 64.6 segundos, lo que resulta en una tasa de transferencia

de 941 Kbits por segundo. Por otro lado, en el host de la Sucursal B, que actuó como cliente iperf, se observó una transferencia de datos similar de 7.25 MBytes durante un intervalo de prueba de 60 segundos, generando una tasa de transferencia de 1.01 Mbits por segundo. Estos resultados indican una consistencia en la tasa de transferencia entre ambas sucursales en la topología Ethernet over IP, con velocidades de aproximadamente 1 Mbits por segundo en ambas direcciones, se comprueba la información en la Figura 50 y Figura 51.

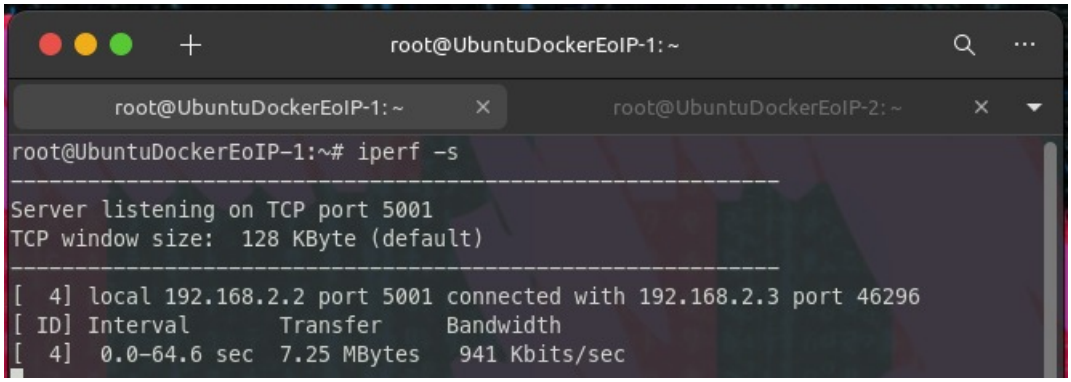


Fig. 50. Servidor en escucha en el puerto TCP para EoIP.

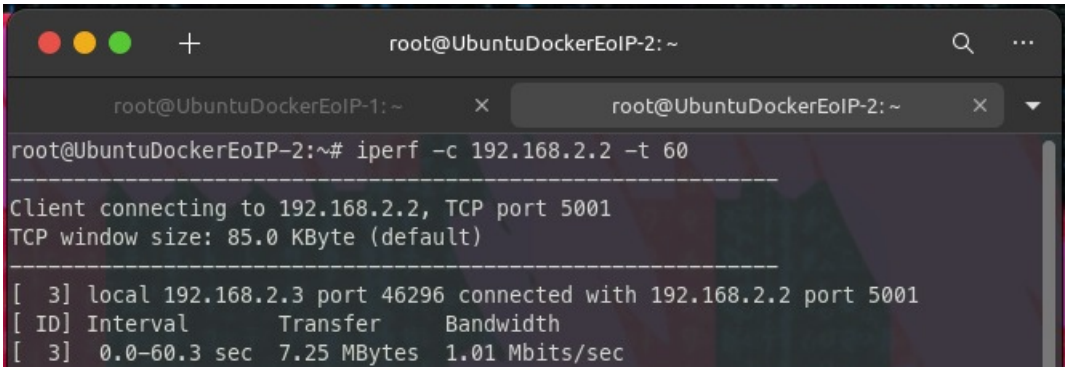


Fig. 51. Cliente conectado al servidor para EoIP.

Resultados de pruebas de IPERF para VXLAN

Siguiendo con la topología VXLAN, se realizó el análisis comparativo del ancho de banda utilizando la herramienta iperf. Al examinar los resultados de las pruebas de ancho de banda en esta topología, se observa lo siguiente: En el host de la Sucursal A, configurado como el servidor iperf, se registró una transferencia de 7.00 MBytes durante un intervalo de 65.1 segundos, lo que resulta en una tasa de transferencia de 902 Kbits por segundo. Por otro lado, en el host de la Sucursal B, actuando como cliente iperf, se observó una transferencia de datos similar de 7.00

MBytes durante un intervalo de prueba de 60.4 segundos, generando una tasa de transferencia de 973 Kbits por segundo. Estos resultados indican una consistencia en la tasa de transferencia entre ambas sucursales en la topología VXLAN, con velocidades de aproximadamente 900 Kbits por segundo en ambas direcciones, se comprueba la información en la Figura 52 y Figura 53.

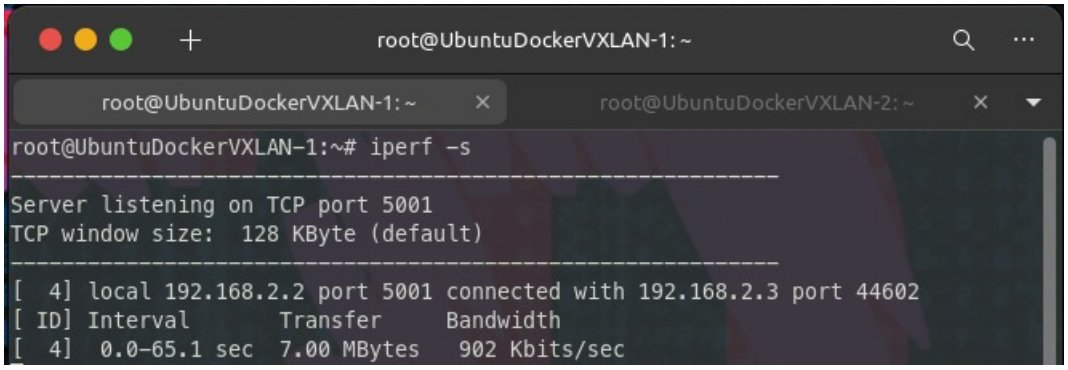


Fig. 52. Servidor en escucha en el puerto TCP para VXLAN.

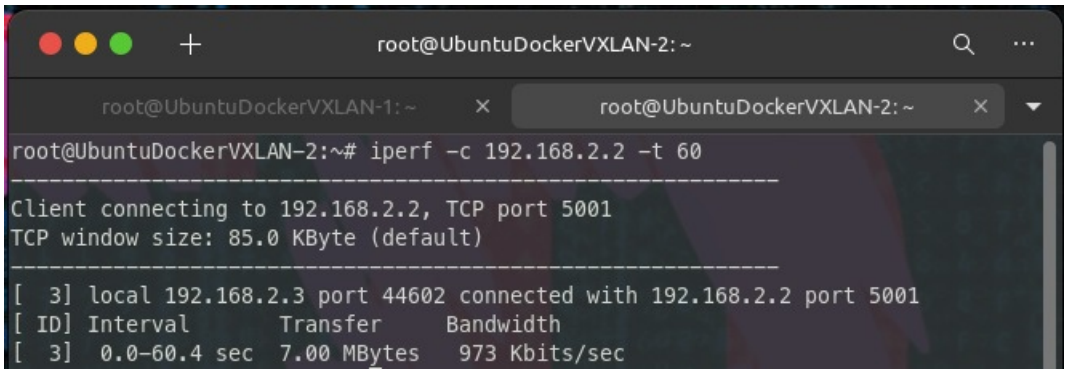


Fig. 53. Cliente conectado al servidor para VXLAN.

Análisis comparativo entre EoIP y VXLAN

La tabla V proporciona una comparación detallada de los resultados obtenidos en las pruebas de ancho de banda y tasa de transferencia para las topologías EoIP y VXLAN en las sucursales A y B.

En primer lugar, al analizar los resultados de la topología EoIP, se observa que en la sucursal A se registró un ancho de banda de 941 Kbits/sec y una tasa de transferencia de 7.25 MBytes. Por otro lado, en la sucursal B, el ancho de banda fue ligeramente superior, alcanzando los 1,010 Kbits/sec, con una tasa de transferencia consistente de 7.25 MBytes. Estos resultados sugieren una capacidad de transferencia satisfactoria en ambas sucursales para esta topología.

Por otro lado, al considerar los resultados de la topología VXLAN, se nota una ligera disminución en el rendimiento en ambas sucursales en comparación con EoIP. En la sucursal A, el ancho de banda fue de 902 Kbits/sec, mientras que en la sucursal B fue de 973 Kbits/sec. Esto indica una reducción significativa en la capacidad de transferencia de datos en comparación con la topología Ethernet over IP.

TABLA V
COMPARATIVA EN EL ANCHO DE BANDA Y LA TASA DE TRANSFERENCIA ENTRE EoIP Y VXLAN.

Topología	**Ancho de Banda (Mbits/sec)**	**Tasa de Transferencia (Mbytes)**
EoIP (Sucursal A)	941	7.25
EoIP (Sucursal B)	1,010	7.25
VXLAN (Sucursal A)	902	7.0
VXLAN (Sucursal B)	973	7.0

V. Conclusiones y recomendaciones

A. Conclusiones

Se cumplió con cada uno de los objetivos planteados en el trabajo. El análisis comparativo de las tecnologías de redes tradicionales y VXLAN se llevó a cabo siguiendo la metodología PPDIOO, lo que permitió una evaluación precisa y sistemática de ambas tecnologías. Mediante pruebas detalladas de ancho de banda, latencia y tasa de transferencia en entornos simulados, se identificaron las fortalezas y debilidades de cada enfoque. Estos hallazgos proporcionan una guía valiosa para las empresas que buscan implementar tecnología VXLAN, destacando su potencial para mejorar la segmentación y escalabilidad de las redes empresariales, lo que a su vez puede conducir a una mejor adaptación para las demandas cambiantes del entorno empresarial actual.

En las pruebas realizadas para cada tecnología, se encontró que VXLAN logró un tiempo promedio de respuesta significativamente inferior al de EoIP, con valores de 14.5 ms y 18.5 ms respectivamente. Además, VXLAN mostró un tiempo mínimo de respuesta más rápido y un tiempo máximo de respuesta más bajo en comparación con EoIP. Estos resultados llevan a concluir que VXLAN ofrece un mejor rendimiento en términos de latencia en la comunicación de red entre las sucursales. Por lo tanto, es una opción viable y prometedora al momento de diseñar redes empresariales o realizar actualizaciones, gracias a su rendimiento superior en términos de latencia.

La comparativa en el ancho de banda y la tasa de transferencia entre las topologías EoIP y VXLAN muestra que ambas tecnologías obtuvieron rendimientos similares en términos de tasa de transferencia, con valores cercanos a 7.25 Mbytes en EoIP y 7.0 Mbytes en VXLAN para ambas sucursales. Sin embargo, se evidencia una ligera ventaja en el ancho de banda para la topología EoIP, con 1.010 Mbits/sec en la Sucursal B, en comparación con los 973 Mbits/sec obtenidos por VXLAN en la misma sucursal. Estos hallazgos indican que, si bien VXLAN presenta un rendimiento competitivo en términos de tasa de transferencia, EoIP supera ligeramente en ancho de banda. Lo que deja en consideración que la elección entre estas tecnologías dependerá de las necesidades específicas de la red empresarial, considerando tanto el rendimiento como otros factores como la escalabilidad y la complejidad de implementación.

B. Recomendaciones

Tener en cuenta la versión del router MikroTik al implementar VXLAN en entornos de red es fundamental. Es importante asegurarse de que el router esté actualizado a la versión 7 o posterior, ya que las versiones anteriores, como la 6, no ofrecen soporte para la implementación de VXLAN.

Es importante mantenerse al tanto de las actualizaciones y avances tecnológicos en el campo de las redes, especialmente en lo que respecta a las tecnologías comparadas en este estudio (EoIP y VXLAN), para aprovechar nuevas funcionalidades y mejoras que puedan surgir en el futuro y que puedan beneficiar la infraestructura de red de las empresas.

Se recomienda considerar el uso de un sistema operativo Linux para futuros proyectos e implementaciones de emulaciones de redes. La eficacia y estabilidad que ofrece Linux, especialmente en entornos de virtualización como GNS3, pueden contribuir significativamente a la productividad y éxito del proyecto. Al evitar la necesidad de virtualizar GNS3 en Linux, se optimizan los recursos de la máquina, lo que puede resultar en un rendimiento mejorado y una experiencia de usuario más fluida.

VI. Referencias

[1] X. A. Arcas Landa, «Evaluación de los límites de un microcontrolador de 8 bits en las comunicaciones bajo protocolos TCP/IP y UDP a través de Ethernet,» 2016.

[2] G. D. Salazar Chacón, «Hybrid Networking SDN y SD-WAN: Interoperabilidad de arquitecturas de redes tradicionales y redes definidas por software en la era de la digitalización,» Tesis doct., Universidad Nacional de La Plata, 2021.

[3] J. C. Navarro Bastidas, «Diseño de una red altamente disponible VxLAN para la transición de protocolo Ipv4 a Ipv6 en el datacenter del Departamento Nacional de Planeación,» Tesis doct., Universidad Nacional de Colombia.

[4] A. P. Razo Achig, «Automatización de redes utilizadas para EOT: análisis conceptual del protocolo VXLAN para la virtualización de centro de datos para EOT.,» B.S. thesis, Quito: EPN, 2022., 2022.

[5] A. Hidayat, «Building a expert system application for help problem solving network on Mikrotik Router,» *MIKROTIK: Jurnal Manajemen Informatika*, vol. 6, nº 1, 2017.

[6] R. Albar y R. O. Putra, «ANALISIS KEAMANAN JARINGAN MENGGUNAKAN METODE SNIFFING DAN IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS V6. 48.3 MENGGUNAKAN METODE PORT KNOCKING,» *JOURNAL OF INFORMATICS AND COMPUTER SCIENCE*, vol. 8, nº 1, págs. 1-11, 2022.

[7] T. Rahman, S. Sumarna y H. Nurdin, «Analisis performa routerOS mikrotik pada jaringan internet,» *INOVTEK Polbeng-Seri Informatika*, vol. 5, nº 1, págs. 178-192, 2020.

[8] F. A. Cruz Quimbiulco y R. G. Montaluisa Toalisa, «Análisis y diseño de una red MPLS que soporte Ipv6 con protocolos de enrutamiento OSFP, Is-Is y BGP emulando un escenario típico de empresas multinacionales,» B.S. thesis, 2017.

[9] A. A. Putra et al., «Implementation of Multihoming Border Gateway Protocol for Internet Connection of Two Internet Service Providers,» *Procedia of Engineering and Life Science*, vol. 1, nº 1, 2021.

[10] I. Nurhaida y Ngadiyono, «Quality of service for traffic monitoring system based on static routing using EoIP tunnel over IPSec,» en *Proceedings of the 2019 Asia Pacific Information Technology Conference*, 2019, págs. 91-99.

[11] J. G. Brida, D. Matesanz Gómez y W. A. Risso, «Estructura jerárquica y dinámica en los mercados cambiarios latinoamericanos,» *Investigación económica*, vol. 68, nº 267, págs. 115-146, 2009.

[12] H. A. DAMANIK y M. ANGGRAENI, «IMPROVING COMPETENCE OF AN-NURMANIYAH VOCATIONAL HIGH SCHOOL STUDENTS THROUGH TRAINING AND IMPLEMENTING OF VPN ETHERNET OVER IP (EOIP) AND PPTP TUNNELING ON MULTI-SITE NETWORK AREA SCALE,» en *ICCD*, vol. 4, 2022, págs. 410-416.

[13] Realpars. «OSI Model Ethernet/IP.» (2023), dirección: https://assets-global.website-files.com/64ed06228d24e5d52132b49f/64f0e78da6d52d22dabf22bb_Ethernet-IP-Over-OSI-Model.png.

[14] V. Shukla, *Introduction to Software Defined Networking: Openflow & VxLAN*. CreateSpace Independent Publishing Platform, 2013, vol. 1.

[15] D. A. S. GEORGE y A. H. George, «A Brief Overview of VXLAN EVPN,» *Ijireeicein-ternational Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, vol. 9, nº 7, págs. 1-12, 2021.

[16] D. Nunez-Agurto, W. Fuertes, L. Marrone y M. Macas, «Machine Learning-Based Traffic Classification in Software-Defined Networking: A Systematic Literature Review, Challenges, and Future Research Directions.,» *IAENG International Journal of Computer Science*, vol. 49, nº 4, 2022.

[17] D. Nuñez-Agurto, W. Fuertes, L. Marrone, E. Benavides-Astudillo y M. Vásquez-Bermúdez, «Traffic Classification in Software-Defined Networking by Employing Deep Learning Techniques: A Systematic Literature Review,» en *Technologies and Innovation*, R. Valencia-García, M. Bucaram-Leverone, J. Del Cioppo-Morstadt, N. Vera-Lucio y P. H. Centanaro-Quiroz, eds., Cham: Springer Nature Switzerland, 2023, págs. 67-80, ISBN: 978-3-031-45682-4.

[18] J. Networks. «infraestructura de red con un túnel VXLAN.» (2023), dirección: https://media.fs.com/images/community/upload/kindEditor/202205/13/20220513-093324-1652405775-z6WaLRMBOm.jpg.

[19] C. P. Lagla Gallardo, «Propuesta de rediseño de red de datos de la empresa Cobrafacil Fabrasilisa SA bajo metodología PPDIOO y diseño TOP-DOWN.,» B.S. thesis, 2019.

[20] J. Duponchelle, *MikroTik CHR*, https://gns3.com/marketplace/appliances, Fecha de acceso: 4 Enero 2024, Enero de 2016.

[21] F. B. Menegidio, D. L. Jabes, R. Costa de Oliveira y L. R. Nunes, «Dugong: a Docker image, based on Ubuntu Linux, focused on reproducibility and replicability for bioinformatics analyses,» *Bioinformatics*, vol. 34, nº 3, págs. 514-515, 2018.