UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

Previo a la obtención del título de:

INGENIERO EN TELECOMUNICACIONES

Implementación De Redes Orientadas al ambiente controlado basado en la Optimización De La Unidad Máxima De Transmisión.

AUTOR

Baquerizo Suárez Melanie Aurora

DOCENTE TUTOR

Ing. Luis miguel Amaya, Mgtr

SANTA ELENA, ECUADOR

2025-2

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. Ronald Rovira Jurado, PhD.
DIRECTOR DE LA CARRERA

Ing. Luis Amaya Fariño, Mgt.
DOCENTE TUTOR

Ing. Daniel Jaramillo Chamba
DOCENTE ESPECIALISTA

Ing, Corina Gonzabay De La A, Mgt.
SECRETARIA

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Baquerizo Suárez Melanie Aurora**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 16 días del mes de diciembre del año 2025

EL AUTOR

Ing. Luis Miguel Amaya Mgt.

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Baquerizo Suárez Melanie Aurora, como requerimiento para la obtención del título de Ingeniero en Telecomunicaciones.

La Libertad, a los 06 días del mes de enero del año 2026

TUTOR

Ing. Luis Miguel Amaya, Mgtr

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Baquerizo Suárez Melanie Aurora**

DECLARO QUE:

El trabajo de Titulación, Implementación de redes orientada al ambiente controlado basado en la unidad máxima de transmisión previo a la obtención del título en Ingeniero en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 16 días del mes de diciembre del año 2025

Baquerizo Suárez Melanie Aurora

AGRADECIMIENTO

Al comenzar este viaje académico, no solo enfrente un reto personal, sino también un proceso en el que muchas personas han sido fundamentales en cada paso. No quiero dejar de agradecer a cada una de ellas ya que sin su apoyo este proyecto no había sido posible.

En primer lugar, agradezco a Dios por guiar mi camino, darme la paciencia y fortaleza necesaria para enfrentar cada desafío que se presentó a lo largo de esta etapa. Su presencia constante en mi vida me ha dado la fuerza para seguir adelante, incluso cuando las dificultades parecían insuperables. Agradezco por la salud, por cada oportunidad y por darme el valor de luchar por mis sueños.

A mis padres Noemí Suárez y Tito Baquerizo, no tengo palabras suficientes para agradecerles por su amor, sacrificio y apoyo incondicional. Han sido el pilar fundamental de mi formación personal y académica acompañándome en cada etapa de mi vida. Su ejemplo, dedicación y confianza en mí han sido determinantes para alcanzar este logro. Este trabajo no solo representa un cumplimiento académico, sino también el reflejo de todo el esfuerzo y sacrificio que han realizado para que pueda dar por culminada esta etapa. Los amo profundamente.

A mis hermanos, Alex, Stalin y Matías, por su apoyo y por estar siempre a mi lado, cada uno de ustedes tiene un lugar especial en mi corazón. Gracias por ser mi fuerza, por entenderme incluso en los momentos más complicados, y por compartir conmigo esta etapa de mi vida.

A mi tutor, el Ing. Luis Miguel Amaya, por su invaluable apoyo y dedicación durante todo este proyecto. Gracias por su orientación, por compartir sus conocimientos y por estar siempre dispuesto a brindarme su ayuda. Su compromiso y paciencia han

sido esenciales para la realización de este trabajo y me han permitido crecer académicamente.

A mis amigos, Jorge y Efrain por su solidaridad y su apoyo en esos momentos difíciles. Gracias por estar siempre presentes, por brindarme su amistad y compañía, y por darme el aliento necesario para seguir adelante.

Los amigos son esas personas que te hacen reír a carcajadas cuando quieres llorar. En especial a Anthony Lascano, porque estar en las buenas es fácil, pero estar en las malas con una sonrisa y una mano extendida es lo que te hace ser tú. Estoy profundamente agradecida por su presencia en mi vida y por todo lo que me han aportado durante este proceso.

Melanie Aurora Baquerizo Suárez

DEDICATORIA

El presente trabajo de titulación se lo dedico con todo mi corazón a mi mamá, Noemi Suárez. Gracias por todo el amor, sacrificio y apoyo que han sido base para cada logro en mi vida. Por tus palabras de aliento, tus enseñanzas y tus esfuerzos que se convierte en mi fuente de inspiración para seguir adelante, todo lo que soy y todo que he logrado es gracias a ti.

A mi papa, Tito baquerizo, gracias papá por ti esfuerzo que hiciste y sigues haciendo por querer vernos superarnos cada día. Por tu apoyo incondicional, por estar siempre a mi lado, en los momentos buenos y en los difíciles. Tu ejemplo de perseverancia, sacrificio y amor me ha enseñado a nunca rendirme. Cada uno de tus esfuerzos, tus sacrificios y tu firme creencia en mí, han sido el impulso para seguir adelante cuando las fuerzas flaqueaban. Sé que, con tu apoyo, siempre puedo lograr lo que me proponga. Eres un pilar fundamental en mi vida, y estoy eternamente agradecida por tu amor y por todo lo que haces por mí y por nuestra familia.

Siempre estaré agradecida con ustedes, por enseñarme que con esfuerzo y dedicación se puede superar cualquier obstáculo. Este logro no solo es mío, sino también de ustedes, porque sin su amor, dedicación y cariño, no habría sido posible cumplir este sueño.

A mis hermanos, Ale, Stalin y Matías, por su apoyo constante y por estar a mi lado en todo momento. Gracias por ser parte de este camino y por compartir conmigo este logro. Cada uno de ustedes tiene un lugar especial en mi corazón.

A mis tías, Patricia y Zoila quienes han sido una constante fuente de apoyo, amor y aliento. Gracias por su presencia

incondicional, por brindarme su cariño y por estar siempre ahí cuando más las necesitaba. Su apoyo me ha dado la fortaleza necesaria para seguir adelante y este logro también es gracias a ellas.

Melanie Aurora Baquerizo Suárez

RESUMEN

El presente proyecto tiene como finalidad desarrollar un entorno de pruebas en un ambiente controlado enfocado en la optimización de la Unidad Máxima de Transmisión (MTU) como variable clave del rendimiento. A partir de una topología jerárquica con un router núcleo y varios segmentos de accesos, se diseñó y configuro una infraestructura que permite evaluar el impacto de distintos valores de MTU sobre parámetros como latencia, throughput, tasa de fragmentación y retransmisiones.

La metodología se desarrolló en tres fases de diseño y simulación en GNS3, implementación física en un entorno controlado de laboratorio y medición comparativa de resultados. En la simulación se validaron el direccionamiento IP, el enrutamiento y los valores de MTU, la topología fue replicada sobre hardware real para observar el comportamiento del tráfico con cargas y escenarios más cercanos a la práctica.

Los resultados evidencian que una MTU correctamente configurada, apoyada por mecanismos como MSS clamping y Path MTU Discovery (PMTUD), aumenta la estabilidad de la red al mitigar la fragmentación y disminuir las retransmisiones, mejorando así la eficiencia en entornos controlados. Se concluye que el ajuste de MTU, combinado con una adecuada planificación de la topología y segmentación de la red, constituye una estrategia viable y de bajo costo para optimizar el desempeño de redes de datos académicas y de pequeña escala.

Palabras clave: MTU, entornos controlados, optimización de red, redes.

ABSTRACT

This project aims to develop a controlled test environment focused on optimizing the Maximum Transmission Unit (MTU) as a key performance variable. Using a hierarchical topology with a core router and several access segments, an infrastructure was designed and configured to evaluate the impact of different MTU values on parameters such as latency, throughput, fragmentation rate, and retransmissions.

The methodology was developed in three phases: design and simulation in GNS3, physical implementation in a controlled laboratory environment, and comparative measurement of results. The simulation validated IP addressing, routing, and MTU values. The topology was replicated on real hardware to observe traffic behavior under loads and scenarios closer to real-world use.

The results demonstrate that a correctly configured MTU, supported by mechanisms such as MSS clamping and Path MTU Discovery (PMTUD), increases network stability by mitigating fragmentation and reducing retransmissions, thus improving efficiency in controlled environments. It is concluded that MTU tuning, combined with proper network topology planning and segmentation, constitutes a viable and low-cost strategy to optimize the performance of small-scale academic data networks.

Keywords: MTU, controlled environments, network optimization.

ÍNDICE

ÍNDICE DE IMÁGENES

ÍNDICE TABLAS

ÍNDICE DE ABREVIATURAS

ABREVIATURA	SIGNIFICADO
MTU	Maximum Transmission Unit – Unidad Máxima de Transmisión
VLAN	Virtual Local Area Network – Red de Área Local Virtual
TCP	Transmission Control Protocol – Protocolo de Control de Transmisión
UDP	User Datagram Protocol – Protocolo de Datagramas de Usuario
Wireshark	Herramienta de análisis de tráfico de red
IP	Internet Protocol – Protocolo de Internet
PDU	Protocol Data Unit – Unidad de Datos de Protocolo
ACK	Acknowledgment – Confirmación de recepción de datos
DHCP	Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Host
DNS	Domain Name System – Sistema de Nombres de Dominio
BANDWIDTH	Ancho de Banda – Capacidad de transmisión de datos en una red
TTL	Time to Live – Tiempo de Vida

NAT	Network Address Translation – Traducción de Direcciones de Red
QoS	Quality of Service – Calidad de Servicio
IPSec	Internet Protocol Security – Seguridad de Protocolo de Internet
SLA	Service Level Agreement – Acuerdo de Nivel de Servicio
RARP	Reverse Address Resolution Protocol – Protocolo de Resolución Inversa de Direcciones
NTP	Network Time Protocol – Protocolo de Tiempo de Red
FTP	File Transfer Protocol – Protocolo de Transferencia de Archivos
HTTP	HyperText Transfer Protocol – Protocolo de Transferencia de Hipertexto
HTTPS	HyperText Transfer Protocol Secure – Protocolo de Transferencia de Hipertexto Seguro
SSL	Secure Sockets Layer – Capa de Conexión Segura
TLS	Transport Layer Security – Seguridad de Capa de Transporte
BGP	Border Gateway Protocol – Protocolo de Puerta de Enlace de Frontera
OSPF	Open Shortest Path First – Primer Camino Abierto más Corto
SNMP	Simple Network Management Protocol – Protocolo Simple de Gestión de Red

CAPÍTULO I

1.1. Antecedentes

La Unidad Máxima de Transmisión (MTU) ha sido objeto de estudio desde los primeros desarrollos de las redes de datos, particularmente en el estándar Ethernet que fijo en 1500 bytes define el tamaño máximo de las tramas transmitidas sin fragmentación[1]. Este parámetro se consolidó como un elemento esencial para garantizar la eficiencia en la transmisión de paquetes y evitar que se originen pérdidas de rendimiento en diferentes capas de la arquitectura de red.

Con el tiempo, diversos estudios han demostrado que una configuración inadecuada de la MTU puede causar problemas de fragmentación, aumentando de la latencia y desaprovechando el ancho de banda disponible. Por ello, una investigación reciente demuestra que una configuración inadecuada de la MTU puede provocar fragmentación, incrementar la latencia y desaprovechar ancho de banda, mientras MTU grandes optimizan procesamiento y throughput, como se vio en los modos de bonding 802.3ad vs Round-Robin bajo diferentes tamaños de MTU[2].

Este parámetro es esencial para garantizar la eficiencia en la transmisión de paquetes y prevenir pérdidas de rendimiento en distintas capas de la arquitectura de red. Protocolos como PPPoE reducen el tamaño de MTU a 1492 bytes para incluir la sobrecarga de encapsulamiento. [3]

A nivel de la capa 3 (red) los paquetes IP que superan la MTU de la interfaz de salida también se fragmentan, generando sobrecarga adicional, es fundamental que ambos niveles, enlace de datos y la red estén configurados correctamente para asegurar una transmisión eficiente entre nodo[4].

La configuración y optimización de la MTU ha adquirido especial relevancia en redes inalámbricas abiertas, como las redes mesh y la infraestructura del internet de las cosas (Iot), factores como perdida de paquetes, interferencias y ruido ambiental pueden generar retransmisiones que afectan el rendimiento, ajustar la MTU según las condiciones de la red y su topología permite mejorar la eficiencia del tráfico y minimizar retrasos[5].

Diversos estudios también han evaluado el desempeño de protocolos como TCP y UDP en aplicaciones de videovigilancia sobre redes LTE, especialmente en zonas rurales o controladas. Los resultados muestran UDP ofrece menor latencia y jitter en comparación con TCP y que la configuración de la MTU es determinante para optimizar el rendimiento, reducir la perdida y asegurar la calidad de transmisión de video en redes con alta demanda de tráfico[6] .

1.2.Descripción del proyecto

El proyecto se centra en abordar las dificultades prácticas en la gestión de tráfico de datos en un ambiente controlado, centrándose en la problemática relacionada con la configuración y optimización de MTU en redes de telecomunicaciones. Para lograrlo, se estudiarán los protocolos que operan por encima de la MTU (IP, TCP, UDP, ICMP) considerando su interacción con las capas inferiores de la red y el efecto que tiene diferente tamaño de MTU sobre la latencia, el Throughput, el jitter, la fragmentación y la perdida de paquetes.

La red se configurará utilizando una topología jerárquica compuesta inicialmente por cinco equipos lo que permite una administración escalonada y estructurada del tráfico, este diseño facilita el ajuste dinámico de la MTU según las condiciones de la red y el tipo de enlace, minimizando la fragmentación y optimizando la eficiencia en la transmisión de datos. Esta lógica se extiende a un escenario físico con un router, un punto de accesos inalámbrico cuatro laboratorios cableados manteniendo el mismo criterio de segmentación y control

Los roles están organizados en fases jerárquicas, donde cada fase cumple una función específica para el análisis del comportamiento de la MTU.

- Fases de jerarquía: equipo central que administra globalmente el tráfico de manera global.
- Fase de administración: el equipo encargado de supervisar el tráfico en el tiempo real, identificando problemas de fragmentación y latencia.
- Fase de control: dos equipos que simulan condicionen variables de tráfico mediante la transmisión y recepción de datos configurados con diferentes valores de MTU.
- Fase de seguridad: punto de diagnóstico que verifica la integridad de la red identificando fallas y generando reportes técnicos.

Para el análisis de los resultados, se utilizará la herramienta de monitoreo de tráfico Wireshark, que permite realizar pruebas bajo diversas cargas de tráfico y

capturas de los paquetes transmitidos, facilitando la observación de parámetros críticos como la fragmentación, latencia y rendimiento de la red [7].

1.3.Objetivos

1.3.1. Objetivo general

- Implementar una red utilizando equipos Ros con un enfoque en la optimización de la unidad máxima de transmisión, evaluando su impacto en el rendimiento de la red.

1.3.2. Objetivos específicos

- Analizar los fundamentos teóricos, normativas y estudios actuales relacionados con la optimización de MTU en redes de telecomunicaciones.
- Implementar la red controlada en un ambiente de pruebas, aplicando la configuración de MTU optimizados.
- Evaluación de la unidad máxima de transmisión para medir el rendimiento de la red y la optimización de la nueva red del laboratorio de telecomunicaciones.

1.4.Problemática

En laboratorios de telecomunicaciones universitarios, enfrentan dificultades de interoperabilidad de equipos de diferentes fabricantes especialmente en lo referente a la configuración de la unidad máxima de transmisión (MTU). La falta de uniformidad en la MTU puede provocar fragmentación de paquetes, aumentado la latencia, desaprovechamiento del ancho de banda y afectando negativamente la eficiencia de las prácticas de laboratorio[8].

Un tamaño de MTU adecuado no solo incrementa la relación carga útil-encabezado, si no también mejorar el rendimiento de acceso directo a memorias (DMA) entre la interfaz de red (NIC) y la CPU del host. Cuando un paquete IP sufre fragmentación al atravesar una red cuya MTU es menor que el tamaño de su paquete transmitido, lo que reduciría considerablemente el rendimiento de reenvío. Como se observa en la Figura 1, un tamaño de MTU mayor permite que los paquetes se transmitan de manera más eficiente, reduciendo la carga de procesamiento y los efectos adversos de fragmentación.

Diversos estudios como ¿Is Large MTU Beneficial to Cellular Core Networks? (2023), que muestran que MTU elevadas mejoran la eficiencia al reducir la cantidad de encabezados procesados, disminuir la fragmentación y optimizar el desempeño general de la red[8].

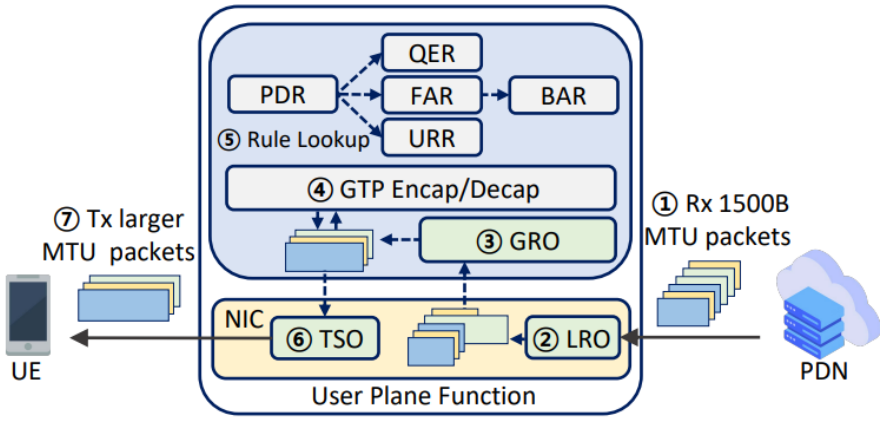


Figura 1 Arquitectura UDPF [8]

Los protocolos de comunicación como IP, TCP, UDP e ICMP dependen directamente de una correcta configuración de MTU para garantizar la transmisión eficiente. En entornos controlados la fragmentación ocurre cuando un paquete excede el MTU de algunos dispositivos en la ruta de transmisión, afectando el desempeño de los protocolos. En redes IPv6 la fragmentación esta deshabilitada, los paquetes demasiados grandes son destacados, lo cual incrementa el riesgo de pérdida de información[9].

La fragmentación se produce principalmente en la capa de red (capa 3 del modelo OSI), donde los paquetes IP se dividen fragmentos más pequeños para travesar enlaces con restricciones de tamaño, esto resulta especialmente crítico duarnte el handshake de TCP (SYN, SYN-ACK, ACK) ya que, si estos mensajes exceden de la MTU, se generan sobrecargas en los dispositivos de red aumentando la latencia y el consumo de recursos[10].

Este proyecto plantea la optimizar la configuración de la MTU en un ambiente controlado, mediante el diseño e implementación una red con MTU optimizada para evaluar su desempeño mediante herramientas como Wireshark para el análisis de tráfico. Se espera que la optimización de la MTU permita reducir la fragmentación, mejorar la eficiencia de flujo de datos y aumentar la estabilidad de la red asegurando que los objetivos del proyecto sean verificables y medibles[11].

1.5. Justificación

En el ámbito de las telecomunicaciones, comprender la conmutación de paquetes es esencial para el diseño, implementación y optimización de redes de comunicación. Este proceso consiste en fragmentar los datos en paquetes enviados a través de redes LAN, WAN e Internet, haciendo posible la gestión efectiva del trabajo y asegurando la confiabilidad de comunicación para que los estudiantes y profesionales desarrollen una comprensión sólida de los conceptos y su aplicación práctica, es crucial contar con un laboratorio especializado que permita simular, analizar y configurar redes de conmutación de manera detallada[12].

Las herramientas como GNS3, ampliamente utilizada para simular entornos de red reales al integrar Routers y switches ya sean virtuales o físicos, se ha consolidado como una de las más relevantes en entornos académicos y profesionales. Otras plataformas como EVE-NG (Emulated virtual Environmet), Wireshark, Mininet, NS3 (Network Simulator 3) también son utilizadas en entornos académicos y de investigación brindando entornos controlados para el análisis y validación de configuraciones[13].

La configuración de la MTU es determinante en la eficiencia de la red ya que define el tamaño máximo de los paquetes que pueden transmitirse sin fragmentación, si la MTU está configurada requiere fragmentación aumentado la sobrecarga, afectando el rendimiento y elevando la latencia. Según el IETF RFC 9268 [14], la fragmentación de paquetes a menudo reduce la confiabilidad de comunicaciones en internet, al aumentar la MTU significativamente por encima de los valores estándar 1500 bytes se observó una mejora notable en el rendimiento y reducción de la latencia en redes celulares del core al disminuir la calidad de paquetes fragmentados[8].

Estudios han demostrado que la configuración optima de la MTU (unidad máxima de transmisión) reduce significativo la latencia y mejora el rendimiento global de la red[15]. Este proyecto resulta viable gracias a la disponibilidad de bases teóricas solidad, recursos técnicos adecuados y un tiempo razonable para implementar la configuración optima del MTU en un entorno controlado.

La relevancia de esta investigación radica en la necesidad de establecer estrategias que optimicen el rendimiento de la red en escenarios de transmisión intensiva, como en entornos IoT móviles, ajustes de red como el tamaño de los paquetes y la configuración de transmisión han demostrado un efecto directo sobre la eficiencia energética y la latencia en redes MEC-IoT [16]. Esto respalda la idea de que configurar correctamente la MTU puede evitar fragmentaciones, reducir retardo y mejorar la eficiencia en redes de nueva generación.

Por lo tanto, el presente proyecto busca demostrar cómo la correcta configuración de la MTU influye de manera positiva en la transmisión de datos, aportando un referente práctico y teórico que respalde futuras investigaciones orientadas a la optimización de redes en telecomunicaciones.

1.6. Alcance del proyecto

Este proyecto de titulación tiene como objetivo principal diseñar e implementar un sistema de red orientado a la optimización de la Unidad Máxima de Transmisión (MTU) en un ambiente controlado. Se emplearán equipos de telecomunicaciones y simulaciones, configurando diferentes tamaños de MTU con el fin de evaluar su impacto en el rendimiento de la red, permitiendo gestionar y monitorear la configuración de la MTU garantizando un análisis detallado de su influencia en la eficiencia y estabilidad de la red[16].

La implementación del sistema incluirá el desarrollo de una infraestructura de comunicación local y remota mediante el unos de protocolos de red avanzados y equipos especializados para configurar y optimiza de MTU. Esta infraestructura funcionará como nodo de referencia para trasmisión de datos entre diferente dispositivo, facilitando el monitoreo y control remoto desde ubicaciones externas, se integrará la sincronización y ajuste dinámico de parámetros en tiempo real con el fin de optimizar el rendimiento, reducir la latencia y evitar la fragmentación innecesaria[17].

En materia de seguridad, se desarrollarán interfaces de usuario y plataformas de monitoreo, utilizando tecnologías de comunicación seguras como VPN y SSH, La VPN proporciona una red privada virtual que permite establecer una conexión segura a través de Internet, protegiendo el tráfico mediante protocolos de cifrado robustos como IPSec o SSL/TLS, los cuales garantizan la privacidad e la integridad de los datos en redes.

La tecnología SSH (Secure Shell) se empleará para el acceso remoto seguro a los dispositivos de la red, cifrando la comunicación entre cliente y el servidor mediante algoritmos de encriptación como AES y RSA, asegurando que la autenticidad e integridad en los procesos de administración remota

Una parte esencial del proyecto será la optimización de protocolos de transmisión de datos y la evaluación del rendimiento de la red bajo distintas configuraciones de MTU, se realizarán pruebas exhaustivas que permitan comprobar el comportamiento del sistema bajo diferentes cargas de tráfico y

condiciones de red, asegurando precisión y estabilidad en un entorno cercano al de producción real. Esto incluirá la simulación de escenarios reales de tráfico de red y la implementación de diversas configuraciones para evaluar el impacto en el rendimiento de la red.

Uno de los primeros escenarios que se puede implementar es el de alta latencia, simulado a través de conexiones WAN, donde los paquetes grandes deben ser fragmentados. Este escenario permite observar cómo la fragmentación puede aumentar la latencia en redes con grandes distancias. Además, se puede evaluar un escenario de alta carga, en el que múltiples dispositivos transmiten datos simultáneamente, lo que permite estudiar la capacidad de la red para manejar grandes volúmenes de tráfico sin causar congestión o pérdida[17].

Finalmente, se desarrollarán prácticas de laboratorio orientadas a la implementación y configuración de redes utilizando equipos ROS y herramientas de simulación como GNS3. Estas prácticas ofrecerán una experiencia práctica a estudiantes y profesionales, proporcionando conocimientos sobre la configuración, optimización de la MTU, y el análisis de rendimiento en redes controladas.

El objetivo es no solo implementar una solución de automatización efectiva, sino también fomentar el aprendizaje y la adopción de tecnologías avanzadas en el campo de las telecomunicaciones y las redes de alta velocidad.

1.7. Metodología

Este proyecto se sustenta en una combinación de métodos que permiten abordar de manera integral el análisis técnico de la Unidad Máxima de Transmisión (MTU) garantizando el cumplimiento de los objetivos planteados.

Investigación Descriptiva

Se evaluará el impacto de diferentes configuraciones de MTU sobre el tráfico de datos en un entorno de simulación. Este análisis permitirá identificar las relaciones existentes entre las variantes de estudio como la latencia, perdida de paquetes y eficiencia en el uso de los recursos de red[16].

Estudios previos sobre la optimización de MTU, demostrando como la configuración adecuada puede mejorar significativamente el rendimiento de las redes LAN / WAN. Estudios han demostrado que una MTU más alta en beneficiosa en condiciones de baja perdida de paquetes y alta latencia mientras que configuraciones más pequeñas pueden ser ideales para entornos con tráfico denso o condiciones en la topología simples han permitido identificar patrones en comportamiento del tráfico bajo diferentes configuraciones[8].

Investigación Documental

Se analizará trabajos previos y literatura científica relacionada con redes de telecomunicaciones y la optimización de protocolos, especialmente en lo referente a la configuración de la MTU. Esta etapa permitirá identificar ventajas, limitaciones y tendencias actuales en el ajuste de la MTU, así como examinar tecnologías emergentes aplicables en entornos controlados. Los estudios revisados muestran que una MTU más alta resulta beneficiosa en condiciones de baja pérdida de paquetes y alta latencia, mientras que valores más reducidos pueden ser más adecuados en escenarios de tráfico denso o con topologías simples.

Investigación Aplicada

La implementación en un entorno controlado permitirá evaluar en la práctica el impacto de diferentes configuraciones de MTU en el rendimiento de la red, empleando herramientas como GNS3 y equipos ROS para prueba física [17].

Se medirá el efecto de los valores de MTU sobre indicadores de desempeño, tales como latencia, pérdida de paquetes y throughput. Este análisis práctico permitirá proponer configuraciones óptimas que contribuyan a mejorar la eficiencia y la gestión de redes.

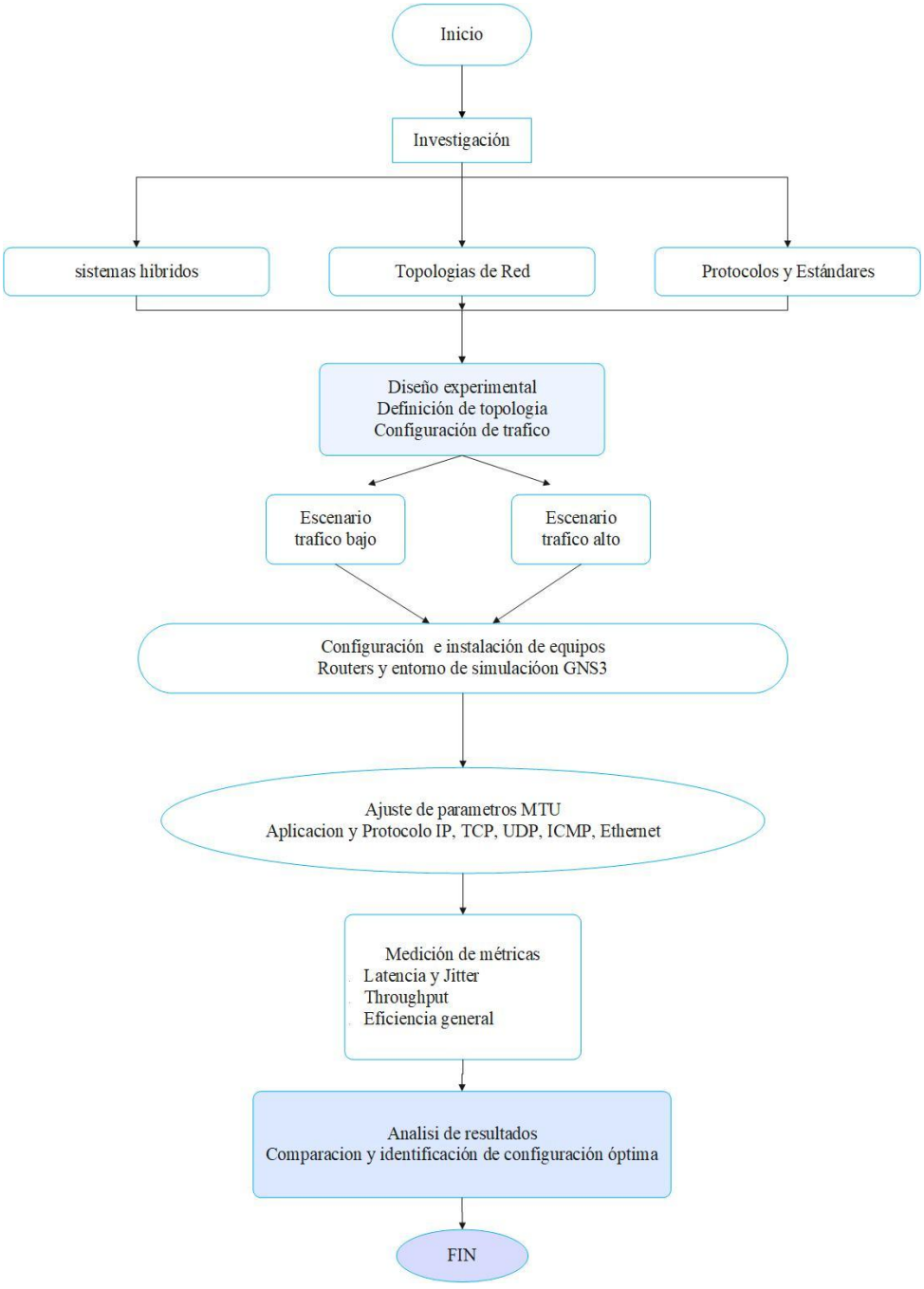


Figura 2 Diagrama de flujo de la metodología propuesta.

CAPITULO II

2. FUNDAMENTOS TEÓRICOS DE LA PROPUESTA

2.1.Marco contextual

En este capítulo se explora los fundamentos teóricos necesarios para comprender el contexto de la Unidad Máxima de Transmisión (MTU) y su incidencia directa en el rendimiento de las redes de telecomunicaciones. El estudio en entornos controlados permite probar, ajustar y validar configuraciones optimas, esto resulta especialmente relevante en actividades de laboratorios académicos y en investigación aplicadas orientada al desempeño de redes.

2.1.Conceptos fundamentales de MTU

2.1.1. Definición y características principales

La unidad máxima de transmisión (MTU) corresponde al tamaño máximo de un paquete que puede transmitirse por una interfaz sin requerir fragmentación. En redes Ethernet, el valor de referencia para muchas implementaciones es 1500 bytes a nivel capa 3 aunque este puede variar según el tipo de interfaz, medio físico y mecanismo de encapsulación empleado [18].

Determinando mecanismos de encapsulación modifican la MTU disponible para la carga útil, tecnologías como PPPoE añade 8 bytes de cabecera (6 bytes de PPPoE+2 bytes de PPP), reduciendo la MTU típica a 1492 si no se ajusta explícitamente, lo que puede inducir fragmentación/reensamblado con paquetes mayores[19].

En IPv6, los routers intermedios no fragmentan paquetes si un paquete excede de la MTU del siguiente salto, es descartado y se notifica al emisor, para mejorar la señalización de la MTU mínima a lo largo del camino, el RFC 9268 introduce una opción Hop-by-Hop lo que permite registra la PMTU mínima en el trayecto y permite retroalimentarla a la fuente[20].

2.1.2. Eficiencia de carga útil según el tamaño de la MTU

El tamaño de la MTU influye en la relación entre la carga útil y la sobrecarga de cabecera, a mayor MTU el porcentaje del paquete corresponde a datos útiles aumentando así la eficiencia de transmisión [8].

La eficiencia puede calcularse mediante la expresión:

$$Eficiencia = \frac{carga\ útil}{MTU} \times 100$$

Considerando una cabecera IPv4+TCP de 40 bytes y la cabecera IPv4+UDP de 28 bytes, en la Tabla 1 presenta valores representativos de carga útil y eficiencia para diferentes tamaños de MTU.

Tabla 1
Eficiencia de carga útil en función de la MTU para IPv4+TCP e IPv4+UDP

MTU (bytes)	**Carga útil IPv4+TCP (bytes)**	**Eficiencia IPv4+TCP (%)**	**Carga útil IPv4+UDP (bytes)**	**Eficiencia IPv4+UDP (%)**
256	216	84,38	228	89,06
512	472	92,19	484	94,53
1024	984	96,09	996	97,27
1280	1240	96,88	1252	97,81
1500	1460	97,33	1472	98,13

Con base en estos valores, la Figura 3 muestra cómo, conforme aumenta la MTU cree la proporción de datos útiles por paquetes, lo que se traduce en una mejor utilización del ancho de banda disponible.

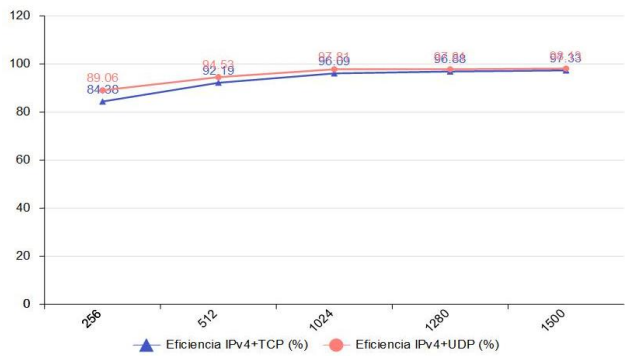


Figura 3 Eficiencia de carga vs tamaño de MTU

2.1.3. Impacto del Overhead por encapsulación

Al introducir encapsulaciones adicionales como VLAN, PPPoE, GRE o VXLAN se introduce overhead adicional, reduce la MTU efectiva disponible para la carga útil. En la Tabla 2 se resume el overhead típico en bytes y la MTU resultante asumiendo una MTU ethernet de 1500 bytes.

Tabla 2
Overhead de encapsulación y MTU IP efectiva sobre Ethernet

Tecnología de encapsulación	Overhead adicional (bytes)	MTU IP efectiva (bytes)
VLAN 802.1Q	4	1496
PPPoE	8	1492
GRE IPv4	24	1476
VXLAN (IPv4)	50	1450
VXLAN (IPv6)	70	1430

A partir de estos valores se construye la Figura 4, que representa de forma gráfica el overhead añadido por cada encapsulación. Se observa los valores orientativos de bytes adicionales: VLAN (802.1Q) =4 B, PPPoE = 8 B, GRE =24 B, VXLAN (IPv4) 50 B, VXLAN (IPv6) = 70 B[21].

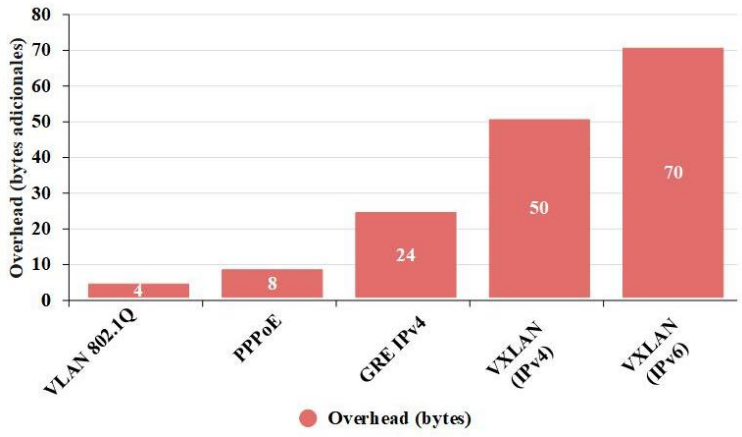


Figura 4 Overhead típico de encapsulación por tecnología

Esto implica que, aunque el enlace físico soporte una MTU de 1500 bytes en el tamaño máximo de los paquetes IP debe reducirse para evitar fragmentación cuando se utiliza esta tecnología, por ejemplo, en el enlace Ethernet como PPPoE si se envía paquetes de 1500 bytes sin ajustar a 1492 se producirá fragmentación o descarte de paquetes generando retransmisión y degradando el rendimiento de TCP y UDP.

2.2. Impacto de la MTU en rendimiento de la Red

El tamaño de la MTU influye de manera directa en la latencia, el throughput y la fragmentación, su configuración determina la eficiencia con la que los dispositivos procesan paquetes, el aprovechamiento del ancho de banda y la estabilidad del tráfico en diferentes entornos de red.

- Una MTU demasiado pequeña genera un mayor número de paquetes lo que incrementa la sobrecarga de cabeceras, el procedimiento en los dispositivos de red y el tamaño de las colas lo que reduce la eficiencia global.
- Una MTU excesivamente grande no es soportada por todos los dispositivos de la ruta, lo que produce fragmentación y pérdida de rendimiento[9].

En entornos de alta demanda de tráfico, como los data centers y las redes de almacenamiento (SAN), el uso de Jumbo Frames (MTU hasta 9000 bytes) permite mejorar la eficiencia de transmisión hasta en un 20 – 30 %, al reducir interrupciones al procesador y optimizar el uso del ancho de banda[22].

En escenarios de redes IoT o enlaces inalámbricos, una MTU elevada puede aumentar la probabilidad de retransmisiones cuando el canal tiene interferencias por lo que valores más bajos resultan más estables[10] De hecho, investigaciones recientes muestran que una MTU adaptativa puede reducir la pérdida de paquetes hasta en un 15 % y mejorar la latencia en un 10 % en entornos virtualizados [20].

La Tabla 3 se muestran los efectos de diferentes tamaños de MTU en distintos entornos de red destacando tanto sus impactos positivos como los riesgos o limitaciones asociados.

Tabla3
Efecto de la MTU en diferentes entornos

Entorno	MTU típica	Impacto positivo	Riesgo / Limitación
Ethernet estándar	1500 B	Compatibilidad universal	Fragmentación si se superan 1500 B
SAN / Data center (Jumbo)	9000 B	+30 % throughput	Requiere soporte total de equipos
VPN / GRE / VXLAN	1550–9000 B	Reducción de Overhead por encapsulación	Fragmentación si no se ajusta MTU subyacente
IoT inalámbrico	500–1280 B	Estabilidad bajo ruido e interferencia	Menor eficiencia por Overhead alto
Núcleo 5G / 4G LTE	2000–4500 B	Reducción de latencia y CPU load	Incompatibilidad con routers antiguos

2.3. Fundamentos teóricos de la optimización de redes.

La optimización del rendimiento en redes se basa en ajuste de parámetros como la MTU, la topología y los protocolos de transporte, un principio clave es la teoría de la capacidad de canal de Shannon-Hartley, que define la tasa máxima de transmisión libre de error en un canal con ruido. Esta teoría del rendimiento depende del ancho de banda y la relación señal/ruido (SNR) [23], configurar adecuadamente la MTU reduce overhead y minimizan retransmisiones por fragmentación aprovechando mejor el canal

En redes virtualizadas como VLAN, VXLAN o GRE exigen aumentar la MTU subyacente de lo contario se generan fragmentaciones que incrementan la latencia y disminuyen el throughput [16]. Mecanismos como el PMTUD y

PLPMTUD permiten detectar dinámicamente la MTU mínima de un trayecto, incluso cuando se bloquean mensajes ICMP [20].

Estudios en redes de alta demanda, como núcleos 5G y sistemas de almacenamiento, evidencian que el uso de Jumbo Frames (≥ 9000 bytes) reduce la fragmentación casi cero y mejora la eficiencia de procesamiento hasta un 30 % [22].

En entornos de baja latencia (videovigilancia, IoT, VoIP), ajistar correctamente la MTU es fundamental para mantener la calidad de servicio (QoS). Investigaciones recientes demuestran que una MTU optima puede reducir la latencia en un 10 % y mejorar la estabilidad de aplicaciones críticas[10].

2.4. Efectos de la configuración de MTU

La MTU configurada incorrectamente puede inducir fragmentación, incrementar la latencia y provocar perdida de paquetes, afectando aplicaciones sensibles al retardo, en tecnologías virtualizadas como VXLAN o GRE una MTU inadecuada intensifica la sobrecarga. Configuraciones óptimas pueden reducir pérdida de paquetes hasta en un 15% y mejorar la latencia en un 10% lo que es fundamental para aplicaciones como videovigilancia, conferencias en tiempo real y NFV[24].

El ajuste dinámico de la MTU se logra con herramientas como PMTUD y su versión mejorada DPLPMTUD, optimizando ancho de banda y reduciendo retransmisiones, especialmente en protocolos modernos como QUIC y SCT[25].

La Tabla 4 se compara el impacto de una MTU incorrecta versus una optimizada en un escenario de alta demanda.

Tabla 4
Impacto de la MTU en la latencia y la pérdida de paquetes

Escenario de MTU	Latencia (ms)	Pérdida de paquetes (%)
MTU inadecuada	115	8
MTU optimizada	107	6,8

En la Figura 5 muestra como una MTU configurada incorrectamente genera una mayor latencia y una mayor pérdida de paquetes en comparación con una MTU optimizada, estos resultados resaltan la importancia de un ajuste adecuado de la MTU mediante mecanismos como PMTUD Y DPLPMTUD.

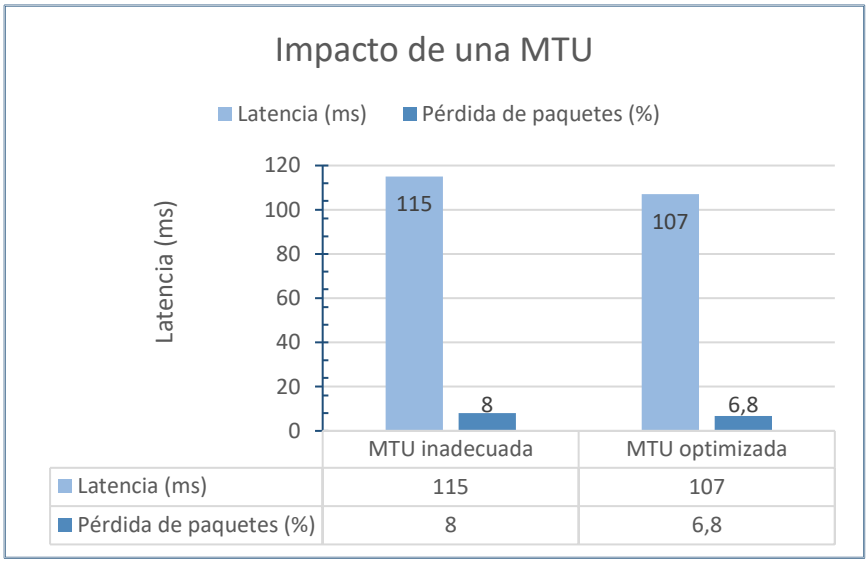


Figura 5 Impacto de una MTU inadecuada vs configurada correctamente en redes de alta demanda.

En términos prácticos una MTU incorrecta se asocia con incremento en latencia (115 ms) y una pérdida de paquetes del 8 %, mientras que una MTU ajustada adecuadamente reduce estos valores a 107 ms y 6,8 %, respectivamente evidenciando la relevancia del ajuste automatizado en redes modernas.

2.5. Marco conceptual

2.5.1. Variable de estudio

Para analizar este comportamiento en la presente investigación, se han definido variables claves que permiten medir el impacto de diferentes configuraciones de MTU sobre el rendimiento de la Red.

La siguiente tabla 5 se detalla las variables claves utilizadas para evaluar el impacto de diferentes configuraciones de MTU sobre el rendimiento de la red, así como su forma de medición en el entorno se simulación *[9], [26]*.

Tabla 5
Definición de variables de estudio

Variable	Tipo de variable	Indicador	Forma de medición
Tamaño de MTU	Independiente	Bytes por paquetes	Configuración en simulación GNS3(1500 bytes, 9000 bytes)
Latencia	Dependiente	Tiempo de respuesta	Ping e ICMP con opción *Don't Fragment*
Throughput	Dependiente	Volumen de datos transmitidos	Iperf / pruebas de carga controlada
Fragmentación	Dependiente	Numero de paquetes fragmentados	Conteo de paquetes fragmentados durante la transmisión

Estas variables permiten evaluar como las distintas configuraciones de MTU afectan la eficiencia, la latencia y estabilidad de la red.

2.6. Estudios recientes sobre MTU

En redes locales, la MTU Ethernet estándar de 1500 bytes resulta suficiente para la mayoría de aplicaciones, teniendo en cuenta que en redes virtualizadas con tecnologías como VLANs, VXLANs y GRE, la encapsulación agrega sobrecarga en los encabezados, lo que puede llevar a la fragmentación, latencia y perdida de rendimiento.

La Tabla 6 muestra como varia la MTU recomendada según el tipo de encapsulamiento utilizado en redes virtualizadas, así como su efecto sobre la fragmentación y latencia.

Tabla 6
Impacto de la MTU según tipo de encapsulación en redes virtualizadas

Tipo de Encapsulación	**MTU Recomendada**	**Efecto sobre fragmentación**	**Impacto en Latencia**
Ethernet estándar sin encapsulación	1500 bytes	Mínima	Baja, sin retraso significativo
VLAN (IEEE 802.1Q)	1522–1600 bytes	Baja a moderada	Ligera, debido a sobrecarga de encabezados
VXLAN	1600–9000 bytes	Moderada si no se ajusta	Media, por fragmentación y procesamiento adicional
GRE	1550–9000 bytes	Moderada a alta si no se ajusta	Media-alta, causada por fragmentación y retransmisiones

Como se observa en Ethernet estándar la fragmentación es mínima, mientras que, en la VLAN, VXLAN y GRE el ajuste de MTU es crítico para evitar retraso. Estudios recientes han demostrado que una configuración adecuada de MTU puede mejorar la eficiencia hasta en un 20%, reducir la latencia y optimizar aplicaciones criticas como (NFV) y el almacenamiento en la nube[27].

2.7. Avances tecnológicos y normativas

2.7.1. Normativas IETF y Modelos de gestión NETCONF, YANG

Los avances tecnológicos, así como las normativas de organismos como el IETF, han sido fundamentales para la evolución de la configuración de la MTU en particular los modelos de gestión de red como el YANG permiten un ajuste dinámico y preciso de la MTU optimizando el rendimiento en redes complejas como WAN y entornos virtualizados.

Una configuración inadecuada de la MTU puede generar fragmentación innecesaria afectando el desempeño de protocolos como TCP y UDP. En TCP si el

Maximun Segment Size (MSS) supera el valor de la MTU se produce retransmisiones y aumento de latencia mientras que en UDP una MTU demasiado pequeña puede provocar perdida de datos hasta que se ajuste la configuración.

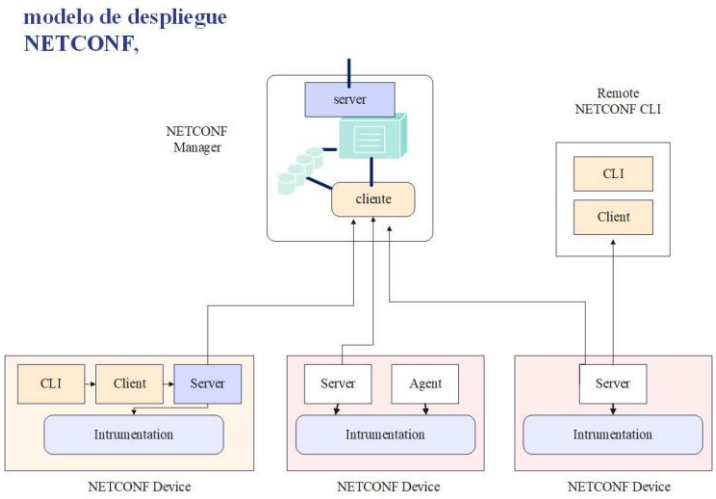


Figura 6 Modelo de despliegue NETCONF.

Esta Figura 6 se presenta un modelo de despliegue NETCONF, que muestra la interaccion entre cliente, servidor y dispositivos de red. Esta representación permite complender cómo los estandares IETF y modelos de gestion como YANG permitiendo la configuracion dinamica de parametros criticos como la MTU.

2.7.2. Soluciones prácticas basadas en estándares

La optimización de la MTU en redes IP se basa en mecanismos estandarizados definidos por el IETF, orientados a evitar la fragmentación excesiva. Uno de los enfoques más utilizados es el Path MTU Discovery (PMTUD) descrito en el RFC 8201 [28], donde el host emite datagramas con el bit Don't Fragment (DF) activado. Si un router intermedio detecta un paquete demasiado grande, envía un mensaje ICMP indicando la MTU máxima posible [29]. En entornos donde el tráfico ICMP está bloqueado o filtrado el mecanismo puede fallar, limitando su eficacia.

Para superar las limitaciones, el RFC 4821 introdujo el Packetization layer Path MTU Discovery (PLPMTUD) permite a protocolos de transporte como TCP determinar de forma activa la MTU mínima de la ruta, sin depender exclusivamente

del ICMP, esto lo hace más robusto en entornos con firewalls o políticas restrictivas [30].

En el caso de IPv6 el RFC 9268 propone la opción Hop-by-Hop-option, que introduce un encabezado adicional en los paquetes[4]. Esto permite que los routers intermedios notificar cambios en la MTU de la ruta de forma automática facilitando la adaptación de la transmisión a enlaces con menor capacidad y reduciendo la fragmentación.

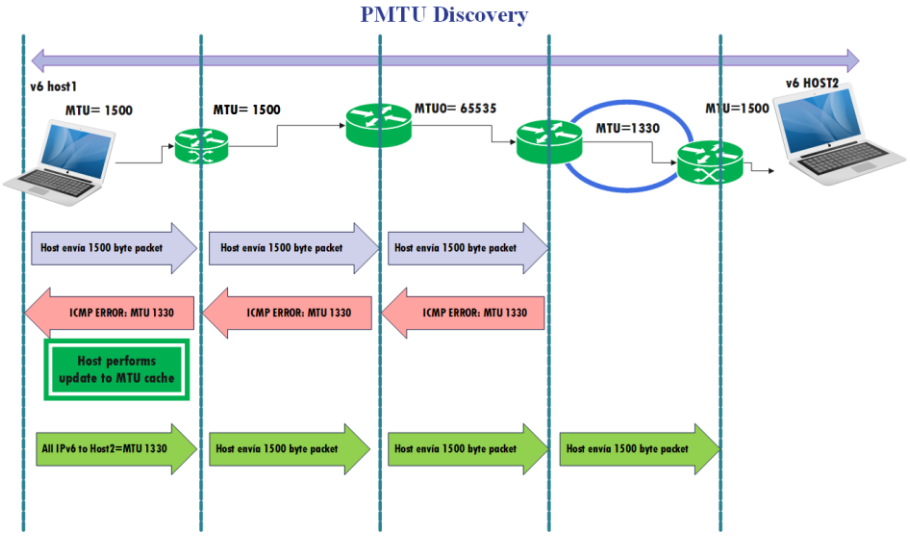


Figura 7 Procesos de descubrimiento de MTU mínima en IPv6

La Figura 7 ilustra el proceso de descubrimiento de MTU mínima en IPv6 donde los routers intermedios actualizan dinámicamente el valor de la MTU. Esta representación permite comprender visualmente como se optimiza la transmisión de datos y se mejora la eficiencia en entornos de red heterogéneos.

2.8. Metodología de implementación

2.8.1. Diseño de la topología de red para pruebas

El diseño de la topología de red es clave para replicar escenarios de tráfico real y configurar de forma óptima la Unidad Máxima de Transmisión (MTU) en un entorno controlado [31]. Para simular redes LAN y WAN de forma efectiva se incluyen routers, switches, servidores y dispositivos finales, conectados según una topología que permita activar un enlace bajo prueba por vez.

Este diseño debe permitir crear diferentes escenarios experimentales diversos, permitiendo evaluar el rendimiento de la red bajo diferentes configuraciones, flujo de datos y tamaño de MTU.

2.8.2. Topologías aplicadas

La red se implementa bajo un modelo jerárquico híbrido en estrella extendida estructurada en tres capas: núcleo, distribución, acceso, permitiendo simular diferentes escenarios de tráfico y evaluar el impacto de la MTU en la eficiencia de la red.

En la siguiente tabla 7, se describe las topologías más utilizadas y su relación con la MTU resaltando sus funciones y ventajas en diferentes escenarios.

Tabla 7
Topologías implementadas y su relación con MTU.

Topología	Función / Ventaja	Relación con MTU
Estrella extendida	Conexión centralizada de nodos	Configuración uniforme de MTU en todos los enlaces [8], [26]
Jerárquica	Tres capas: núcleo (centraliza), distribución (segmenta), acceso (conecta usuarios y servidores)	Permite segmentar tráfico y optimizar flujo por capa
Cliente-servidor	Servidores proporcionan servicios y bases de datos, clientes generan solicitudes	Facilita la evaluación de fragmentación y eficiencia en aplicaciones críticas [28].
Híbrida	Combina jerárquica y cliente-servidor; incluye nodos adicionales.	Permite evaluar MTU en distintos escenarios y tipos de tráfico LAN/WAN

Este tipo de topología permite:

- Controlar y segmentar el tráfico según las capas de acceso, distribución y núcleo, facilitando la medición precisa de throughput, latencia y fragmentación.
- Simular escenarios reales de interacción cliente-servidor y comunicación entre nodos.
- Ofrecer flexibilidad para agregar nodos y variar condiciones de prueba, permitiendo analizar el impacto de la MTU en distintos contextos de tráfico.
- Implementar tramas y flujos diferenciados (RTP/UDP, TCP transaccional, ICMP, VLAN) y evaluar cómo cada tipo de tráfico responde a la optimización de la MTU.

2.8.3. Topología en estrella extendida.

La figura 8 muestra la topología en estrella extendida donde los nodos de acceso usuarios y dispositivos finales se conectan a switches intermedios, los cuales a su vez se enlazan con un nodo central [32].

Esta estructura permite un control centralizado del tráfico en puntos bien definidos, asegurando que los parámetros de la MTU se configuren de manera homogénea en los enlaces principales y de acceso.

La configuración facilita la detección de fragmentación y perdida, optimizado la transmisión de datos entre los servidores y los clientes, el diseño de laboratorio, se emplea servidores para la simulación de aplicaciones críticas y los dispositivos de acceso están configurados para generar tráfico y evaluar cómo afecta la optimización de la MTU en la red.

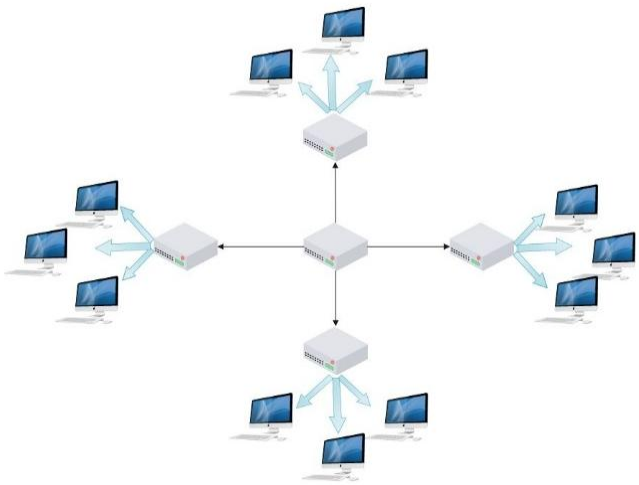


Figura 8 topología en estrella extendida

2.8.4. Topología jerárquica

La figura 9 presenta un modelo de topología jerárquica organizada en tres capas lógicas como núcleo, distribución y acceso. El núcleo concentra el tráfico agregado, la capa de distribución segmenta y aplica políticas de enrutamiento y la capa de acceso conecta los usuarios, servidores y dispositivos finales[33].

Este diseño se adapta perfectamente el análisis de la MTU ya que permite observar como la fragmentación y la latencia varía en función del tamaño de los paquetes en cada capa, en los entornos de laboratorios se simula servidores en la capa de accesos que generan tráfico de diversas aplicaciones mientras que el tráfico de datos se segmenta y optimiza en capas superiores.

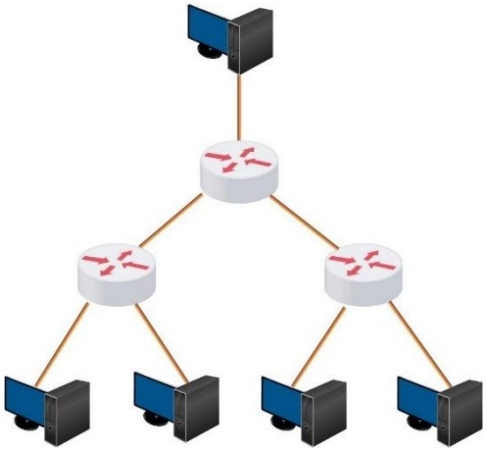


Figura 9 Topología jerárquica de tres capas (núcleo, distribución y acceso).

2.8.5. Topología cliente-servidor e híbrida.

La figura 10 muestra la topología cliente-servidor e híbrida en la que diferentes laboratorios generan solicitudes simultáneas a servidores que proporcionan aplicaciones, base de datos y contenidos multimedia [34].

La red esta segmentada en VLAN para optimizar el tráfico y gestiona la MTU de manera eficiente y el punto central de control actúa como el núcleo de la red interconectando los diferentes nodos y permitiendo simular condiciones LAN y WAN lo cual facilita la evaluación del impacto de la MTU sobre la fragmentación, latencia y el rendimiento general de la red [35]

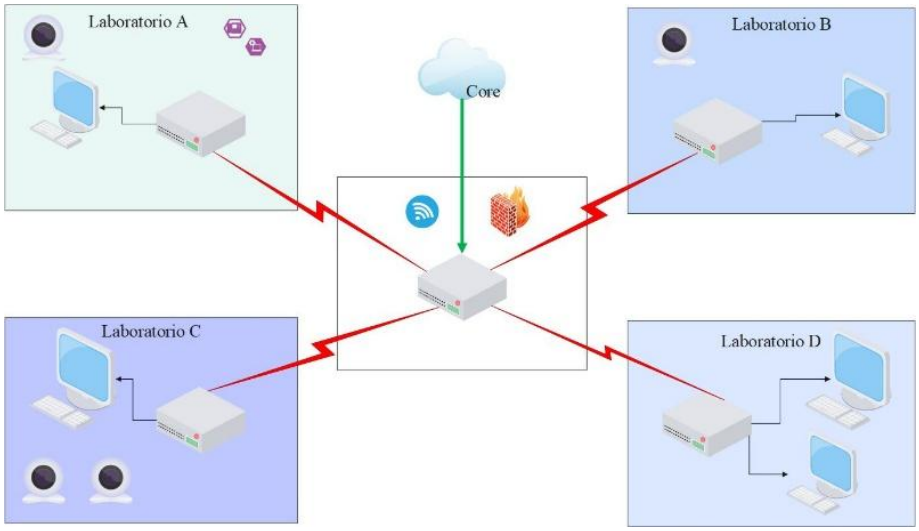


Figura 10 Topología híbrida

2.9. Tipo de tráfico en la topología de pruebas

En la topología propuesta se manejan diferentes tipos de tramas y flujos de tráfico de acuerdo con la función de cada capa, permitiendo evaluar de manera controlada como impacta la optimización de la MTU en cada flujo de datos, desde la generación de información en la capa de acceso hasta la agregación de tráfico en el núcleo[9].

Las principales categorías de tráfico consideradas

- ✓ Tráfico en tiempo real RTP/UDP
  - Flujo orientado a aplicaciones sensibles de la latencia, como VoIP o trasmisión multimedia.

- Evaluación del impacto de la fragmentación y la variación de jitter al ajustar la MTU.

✓ Tráfico transaccional
- Paquetes TCP utilizados en consultas y respuestas de base de datos.
- Aplicaciones web HTTP y servicios de trasferencia de archivos FTP.
- Escenarios de comunicación cliente-servidor bajo protocolos confiables TCP.

✓ Tráfico de conectividad y pruebas.
- Mensaje ICMP para pruebas de conectividad y verificación de MTU máxima mediante la opción Don´t Fragment.
- Flujos UDP de prueba para medir latencia y pérdida de paquetes en transmisiones multimedia.

✓ Trama de conectividad y administración
- Protocolos de señalización y gestión como la resolución de direcciones (ARP) y asignación dinámica de dirección IP (DHCP)

✓ Tráfico segmentación de VLANs
- Tramas como etiquetas 802.1Q VLAN Tagging que añaden 4 bytes a cada trama Ethernet
- Permite separar y analizar de manera independiente el tráfico de laboratorio, servidores y nodos de acceso, manteniendo un entorno controlado para la optimización de la MTU.

2.9.1. Implementación de redes controladas basadas en la optimización de MTU

La topología de red y caracterizado el tipo de tráfico se implementa la optimización de la MTU en el entorno controlado. El proceso consiste en ajustar los parámetros de cada dispositivo de red incluyendo routers y conmutadores administrables para garantizar que los paquetes de datos se transmitan. Una MTU correctamente configurada permite minimiza la fragmentación y mejora el rendimiento general de la red[36].

Para determinar el valor de MTU más adecuado se emplearon métodos de descubrimiento dinámico, como PMTUD y PLPMTUD. PMTUD utiliza ICMP

Fragmentation Needed, mientras que PLPMTUD no depende únicamente de ICMP, por lo hace eficaz con UDP y en redes donde esos mensajes puedan estar bloqueados [37].

La optimización busca mitigar la fragmentación, cuando un paquete excede el MTU de un enlace intermedio, el router debe dividirlo, lo que agrega sobrecarga, latencia y potencial perdida de paquetes.

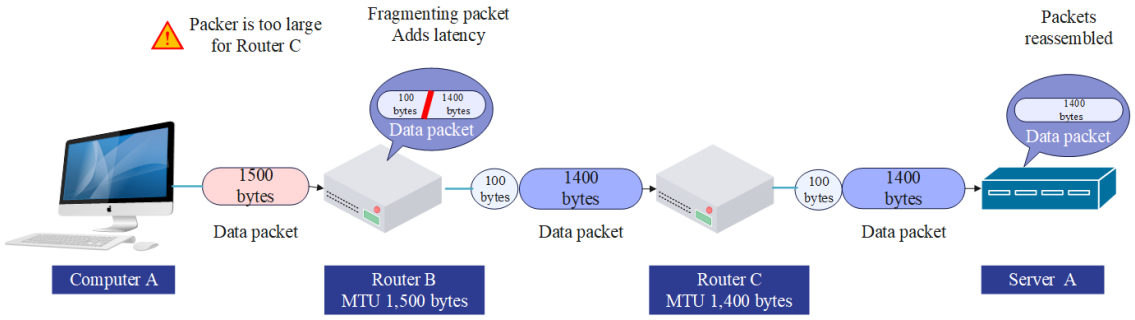


Figura 11 Fragmentación de paquetes en la red

En la Figura 11 ilustra un ejemplo de cómo un paquete de 1500 bytes enviado desde el origen se divide en dos fragmentos (por ejemplo, 1400 y 100 bytes) al atravesar un enlace con MTU reducida.

Se suele realizar pruebas de MTU mediante ping con DF y se empleó Wireshark para registrar métricas clave: latencia, throughput, jitter y tasa de fragmentación, antes y después de aplicar los ajustes[38]. Los valores obtenidos permitieron ajustar la MTU de cada enlace considerando la capacidad de los dispositivos, la naturaleza del tráfico y la prioridad de aplicaciones sensibles a tiempo real.

La Tabla 8 se presenta los componentes utilizados en la implementación de la optimización de la MTU dentro del entorno controlado, detallando la función de cada elemento y su relación con el proceso de ajuste de MTU y análisis de rendimiento.

Tabla 8
Componentes empleados en la implementación de la optimización de MTU

Componente	Función / Descripción
Dispositivos de enrutamiento	Soportan protocolos dinámicos como OSPF y BGP, permiten analizar el comportamiento de la MTU en distintos escenarios de enrutamiento.
Conmutadores administrables	Configurados para redes virtualizadas (VLAN, VXLAN), permiten evaluar la fragmentación y ajuste de MTU en entornos virtualizados.
Servidores y dispositivos finales	Emulan fuentes y destinos de tráfico, generando patrones de carga y latencia variables.
Enlaces simulados	Representan distintos tipos de conexión (fibra óptica, Ethernet, enlaces de baja capacidad), incluyendo variaciones en la MTU para replicar escenarios heterogéneos.

Como se observa en la Tabla 8, los routers permiten evaluar la interacción entre MTU, MSS y PMTUD, mientras que los enlaces simulados reproducen condiciones reales, incluyendo enlaces con MTU reducida que inducen fragmentación

2.9.2. Análisis de las limitaciones en los métodos de configuración basados en MTU

La optimización de la Unidad Máxima de trasmisión (MTU) es un aspecto clave para la eficiencia de las redes IP, ya que influye directamente en el tamaño de los paquetes transmitidos, el nivel de fragmentación y la utilización de los recursos de red. Los métodos de ajuste de MTU presentan ciertas limitaciones técnicas y operativas que deben ser consideradas en escenarios de implementación en entornos reales.

De acuerdo con lo establecido en los estándares RFC 1191[39] y RFC 8201, las principales limitaciones identificadas se resumen en la Tabla 9.

Tabla 9
Limitaciones en la configuración basada en MTU

Limitación	Detalle	Impacto
Infraestructura heterogénea	Diferentes equipos soportan distintos tamaños de MTU.	Paquetes se fragmentan al pasar por routers o switches antiguos[40].
Fragmentación oculta (ICMP bloqueado)	Fallo en Path MTU Discovery cuando ICMP está bloqueado.	Paquetes se pierden sin notificación, degradando rendimiento[41].
Impacto en protocolos de capa superior	TCP y otras aplicaciones sensibles a la latencia pueden sufrir.	Retransmisiones, aumento de sobrecarga y latencia.
Sobrecarga administrativa	Requiere monitorización y ajuste constante.	Mayor complejidad en redes corporativas o multi-sitio[42].
Encapsulamientos adicionales (VPN, GRE, IPSec)	Cabeceras extra reducen MTU efectiva.	Fragmentación en túneles VPN o GRE, afectando throughput.
Tráfico dinámico poco adaptable	Flujos variables como multimedia o IoT sufren fragmentación.	Latencia y jitter en videollamadas o alertas IoT[14].

En la Tabla 9**,** evidencias las principales limitaciones al configurar la MTU en redes IP. Destaca factores como la heterogeneidad de los dispositivos, fragmentación oculta causada por el bloqueo de ICMP, los efectos en protocolos sensibles al retardo como TCP, la sobrecarga administrativa en redes extensas, los encapsulamientos adicionales utilizan VPN y la baja adaptabilidad de planificar cuidadosamente la configuración de la MTU y complementar sus ajustes con herramientas dinámicas como PMTUD y PLPMTUD[40].

2.10. Herramienta y equipos de implementación

2.10.1. Software de simulación GNS3

GNS3 es una plataforma de simulación y emulación de redes que permite replicar topologías reales en entornos virtualizados, integrando imágenes de sistemas operativos de red como Cisco IOS y MikroTik RouterOS. Esta ofrece un entorno controlado para realizar pruebas de configuraciones complejas sin depender de hardware físico.

La investigación sobre MTU, GNS3 permite evaluar de manera precisa el impacto de distintos tamaños de paquetes en flujos de tráfico y topologías variadas, garantizando resultados reproducibles y extrapolables a escenarios reales[43].

La Tabla 10 presenta una comparativa entre GNS3 y otras plataformas de simulación, destacando sus características y ventajas para la implementación.

Tabla 10
Comparativa con otras plataformas de simulación

Característica	**GNS3**	**Packet Tracer**	**EVE-NG**
Realismo	Emula sistemas operativos reales (Cisco IOS, MikroTik RouterOS), permitiendo pruebas cercanas a producción.	Simula dispositivos Cisco mediante representaciones virtuales; adecuado para aprendizaje conceptual.	Ejecuta imágenes reales de múltiples fabricantes, facilitando laboratorios complejos y heterogéneos.
Compatibilidad	Soporta múltiples fabricantes y tipos de dispositivos, permitiendo redes heterogéneas.	Solo dispositivos Cisco; limitado para integración multi-vendor.	Amplia compatibilidad con diversos proveedores, ideal para entornos de prueba avanzados.
Facilidad de uso	Requiere configuración técnica de imágenes y topologías; aprendizaje más profundo.	Interfaz intuitiva, configuración sencilla y rápida para estudiantes.	Demanda conocimientos técnicos en gestión de imágenes y virtualización.

La elección de GNS3 se fundamenta en tres aspectos clave:

- ✓ Realismo: La capacidad de ejecutar sistemas operativos reales permite que las pruebas de MTU reflejen con precisión el comportamiento en entornos de producción.
- ✓ Compatibilidad multi-vendor: Facilita la integración de dispositivos de distintos fabricantes, lo que permite estudiar redes heterogéneas con configuraciones complejas.
- ✓ Escenarios controlados y reproducibles: La plataforma permite crear topologías complejas y ajustar parámetros críticos como la MTU, lo que la hace ideal para laboratorios de investigación y estudios académicos.

GNS3 se integra eficientemente con herramientas de análisis de tráfico como Wireshark y con equipos reales o virtuales MikroTik, aumentando la fidelidad de las pruebas y proporcionando un entorno robusto para evaluar la optimización de la MTU y su impacto en el rendimiento de la red.

2.10.2. Equipos MikroTik

MikroTik se seleccionó como dispositivo de red principal por su flexibilidad, escalabilidad y costo accesible, características que lo hacen ideal para entornos de laboratorio. Su compatibilidad con GNS3 permite integrar pruebas híbridas (virtual-físico), mientras que sus capacidades de configuración detallada de MTU lo convierten en una herramienta de análisis robusta.

Características principales y capacidades de configuración

- ✓ Enrutamiento y conmutación avanzados: Soporte para protocolos dinámicos (OSPF, BGP, RIP) y configuraciones de VLAN, QoS y NAT.
- ✓ Control detallado de interfaces: Permite establecer MTU por interfaz física o lógica, incluyendo túneles PPPoE, VLAN y VPN, ajustando el tamaño de paquetes según el tipo de tráfico.

- ✓ Seguridad y monitoreo: Incluye firewall avanzado, herramientas de análisis de tráfico y monitoreo detallado del rendimiento.
- ✓ Integración con simuladores: Compatible con GNS3 y EVE-NG para entornos híbridos (virtual-físico).

Especificaciones técnicas del MikroTik hEX S

La Tabla 11 detalla las especificaciones técnicas del dispositivo MikroTik hEX S (RB760iGS) utilizado en la investigación para avaluar el rendimiento de la MTU en redes de laboratorio [44].

Tabla 11
Especificaciones técnicas del MikroTik hEX S (RB760iGS)

Característica	Detalle
Código de producto	RB760iGS (hEX S)
CPU	Dual-core 880 MHz
RAM	256 MB
Almacenamiento	16 MB FLASH
Licencia RouterOS	Nivel 4
Puertos Ethernet	5 × Gigabit Ethernet
Ranura SFP	1 × SFP (1.25 Gbps)
PoE-In	802.3af/at, 12–57 V
PoE-Out	Puerto 5, pasivo, hasta 57 V / 500 mA
Consumo energético	6 W promedio, 24 W máximo
Conectividad adicional	1 × USB 2.0 tipo A, ranura microSD
Funciones avanzadas	Aceleración IPsec, monitoreo de voltaje/temperatura
Rango de temperatura	–40 °C a +70 °C

Comparativa con otros dispositivos de red

La Tabla 12 compara el MikroTik Hex RB760Gr3 con otros dispositivos de red utilizados para pruebas de laboratorio, destacando las cualidades más relevantes para las pruebas.

Tabla 12
Comparativa de equipos para pruebas de laboratorio.

Equipo	Cualidades destacadas para la implementación
MikroTik Hex RB760Gr3	Configuración avanzada de MTU y VLANs; integración con GNS3 y Wireshark.
Ubiquiti EdgeRouter	Interfaz web accesible y CLI tipo Linux; adecuado para entornos pequeños; soporte limitado para ajustes de MTU; menor compatibilidad con simulaciones académicas[44].
Cisco Small Business (RV260)	Alta fiabilidad y seguridad; menor flexibilidad para pruebas académicas.
TP-Link Archer C6	Fácil de instalar y usar; recomendable para redes domésticas o PYMES con requerimientos básicos; no permite ajustes de MTU ni simulación detallada [44].

La elección de MikroTik Hex RB760Gr3 se fundamenta en su balance entre flexibilidad, escalabilidad y compatibilidad con herramientas académicas, superando las limitaciones de otros dispositivos para entornos de laboratorio y simulaciones de red [44]

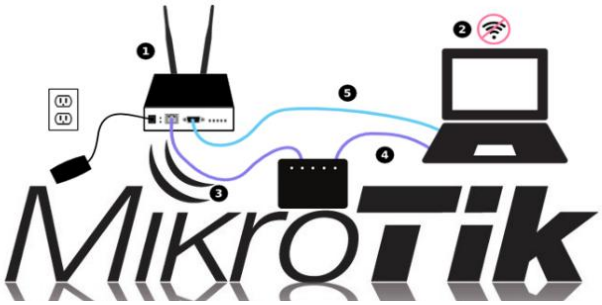


Figura 12 MikroTik Hex RB760Gr3 [48]

Su capacidad para ajustar MTU, gestionar VLANs y túneles, y monitorizar el tráfico de manera detallada garantiza que los experimentos sean reproducibles y confiables, cumpliendo con los objetivos de la investigación y proporcionando resultados aplicables a escenarios profesionales.

2.11. Identificación de cuello de botella y limitaciones

En redes de datos, un cuello de botella es un punto de la infraestructura donde la capacidad de transmisión o procesamiento es menor que la demanda. En entornos con encapsulación múltiple, como túneles VXLAN o redes superpuestas, MTU mal configuradas pueden causar fragmentación excesiva y degradar el desempeño[45].

Investigaciones en pilas de red señala que, en enlaces de alta velocidad, otro factor de limitación es el procesamiento interno de paquetes en los hosts, especialmente por transferencia entre buffers o interrupciones, lo cual puede saturar la CPU o el bus del sistema, limitando el throughput incluso en enlaces de alta velocidad[46].

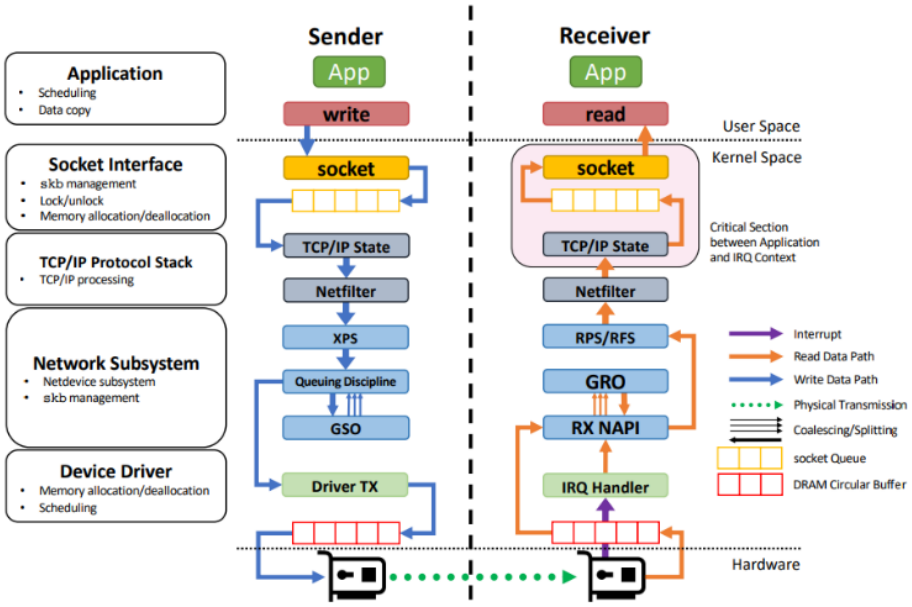


Figura 13 Arquitectura [49]

Como se observa en la Figura 13, tanto en el transmisor como en el receptor existen múltiples capas (aplicación, interfaz de sockets, protocolo TCP/IP,

subsistema de red y controlador de dispositivo) que pueden convertirse en cuellos de botella. Cada una de ellas requiere gestión de memoria, interrupciones y transferencia de datos, lo que en escenarios de alta carga puede afectar el rendimiento.

Una analogía sencilla para comprender el fenómeno es la del embudo si el flujo de agua (datos) excede la capacidad de la abertura del embudo (enlace o dispositivo) se genera congestión. De manera similar, cuando un punto de la red procesa menos información de la que recibe, se origina un cuello de botella.

La Tabla 13 resume los principales puntos susceptibles a generar limitaciones en la infraestructura.

Tabla 13
Los posibles cuellos de botella identificados en la red

Punto de la red	**Causa del cuello de botella**	**Efecto en la red**
Enlaces de agregación	MTU mínima insuficiente o tráfico elevado	Retrasos y pérdida de paquetes
Interfaces mixtas	Topologías jerárquicas + cliente-servidor	Fragmentación de paquetes
Dispositivos de baja capacidad	CPU o memoria limitada	Procesamiento lento y retrasos
Buffers saturados	Llegada de más paquetes de los que pueden enviar	Colas largas y latencia alta

Esta identificación permite focalizar esfuerzos en la optimización de la MTU y la configuración de la infraestructura, minimizando los impactos negativos sobre el flujo de datos y mejorando el desempeño de la red en escenarios controlados.

El desarrolló los fundamentos teóricos necesarios para comprender la importancia de la MTU en el rendimiento de redes de telecomunicaciones, abordando conceptos clave como fragmentación, eficiencia de carga útil,

encapsulaciones, mecanismos de descubrimiento de MTU y limitaciones inherentes a configuraciones incorrectas. Asimismo, se revisaron normativas IETF, modelos de gestión modernos, tecnologías de virtualización y factores que influyen en la aparición de cuellos de botella.

Estos elementos proporcionan el sustento conceptual que permitirá, en los capítulos posteriores, diseñar la metodología de implementación, realizar las pruebas experimentales y analizar el impacto real de la optimización de la MTU en un entorno de laboratorio controlado.

CAPÍTULO III

3. DESARROLLO DE LA PROPUESTA

3.1. Contexto general de la propuesta

En este capítulo se presenta la implementación de una red optimizada mediante el ajuste de la Unidad la Máxima de Transmisión (MTU), con el uso de equipos MikroTik y la herramienta GNS3[47]. Se detallan las etapas de diseño, configuración, simulación y validación y prueba de la infraestructura de red tanto en el entorno simulado como en el entorno físico.

Se describe la topología de red aplicada en el entorno simulado y su posterior traslado a la implementación física, se detallan los objetivos de la prueba de rendimiento con el ajuste de la MTU y como la configuración física se valida mediante la prueba de laboratorios A, B, C y D.

3.2. Componentes de la propuesta

La propuesta tiene como objetivo mejorar el desempeño de la red mediante la optimización de la Unidad Máxima de Transmisión ajustando configuraciones específicas de red en un entorno de prueba. El ajuste adecuado de la MTU es crucial ya que una configuración inapropiada puede generar perdida de paquetes, fragmentación innecesaria y aumento de la latencia.

3.2.1. Importancia de la implementación práctica en entornos reales y simulados

El diseño e implementación de redes no debe limitarse únicamente al plano teóricos. Por esta razón la propuesta integra tanto entornos de simulación (GNS3 en Ubuntu) como la implementación física con router MikroTik.

La simulación previa en GNS3 permite anticipar errores de configuración y analizar el comportamiento del tráfico bajo diferentes condiciones de carga antes de desplegar la red física, reduciendo el riesgo operativo y aumentando la tasa de éxito de la implementación[43]. La combinación de escenarios reales y virtuales

ofrece un marco integral de validación, garantizando que los resultados sean reproducibles y aplicables en entornos académicos y profesionales

3.3. Componentes y funcionamiento operativo de la red

Para garantizar el correcto funcionamiento, se seleccionaron componentes lógicos y físicos que permiten implementar, configurar y validar la red en un ambiente controlado.

3.3.1. Componentes lógicos:

1. Ubuntu

   - Sistema operativo estable y de código abierto, empleado como plataforma base para ejecutar GNS3 y Wireshark debido a su compatibilidad y flexibilidad en configuraciones de red.

Figura 14 Ubuntu[50]

2. GNS3

   - Plataforma de simulación que permite emular redes a partir de imágenes de dispositivos. Se utiliza para diseñar la topología, validando el diseño antes de implementar en equipos físicos[43].

Figura 15 GNS3[51]

3. Wireshark
    - Herramienta de análisis de protocolos que permite capturar y diagnosticar el tráfico en tiempo real, útil para identificar fragmentación y medir parámetros como latencia, jitter y pérdida de paquetes[20].

Figura 16 Wireshark [52]

4. Winbox
    - Aplicación creada por MikroTik para la configuración gráfica de sus routers, se utiliza tanto en la simulación como en la implementación física facilitando ajustes de MTU, reglas de firewall y parámetros avanzados de red.

Figura 17 Winbox[53]

3.3.2. Componentes físicos:

5. Mikrotik hEX
    - Modelo profesional (RB750Gr3) con 5 puertos Gigabit Ethernet, soporte para VLANS, firewall, VPN y enrutamiento avanzado

esencial en el proyecto por su capacidad de ajustar manualmente la MTU en cada interfaz y manejar tráfico de alta velocidad sin comprometer rendimiento.

Figura 18 MikroTik hEX (RB750Gr3) [54]

6. Conector RJ-45
   - Permiten interconectar los cables Ethernet con los dispositivos físicos. Su correcta crimpación es crucial para evitar errores que puedan afectar la transmisión de datos y la validación de la MTU.

Figura 19 RJ-45

7. Cable de red categoría 6
   - Soporta velocidades de hasta 1 Gbps con ancho de banda de 250 MHz, adecuado para garantizar estabilidad en la transmisión de tramas cercanas al valor máximo de la MTU, reduciendo interferencias y pérdidas de señal.

3.4. Diseño lógico de la solución

La solución se diseñó de forma jerárquica donde MikroTik Principal funciona como núcleo central interconectando todos los laboratorios A, B, C y D. cada laboratorio actúa como escenario de prueba independiente y representa un caso

de uno especifico como red de acceso simple, VLAN básica, VLAN múltiples y escenarios de usuario final con tráfico de video.)

En todos los casos el tráfico atraviesa siempre en MikroTik Principal permitiendo centralizar la gestión de MTU, aplicar métricas homogéneas de latencia, throughput, jitter y fragmentación y comparar de forma objetiva el comportamiento de la red entre la configuración estándar y optimizada.

3.5. Entorno de simulación en GNS3

La simulación en GNS3 permite reproducir la arquitectura lógica definida en un entorno controlado previo a la implementación física, se evalúan diferentes configuraciones de MTU, midiendo su efecto sobre la latencia, el throughput, el jitter, la fragmentación y la perdida de paquetes utilizando router MikroTik virtualizados y herramientas de pruebas con ping, iperf3 y Wireshark.

La simulación sirve como etapa intermedia entre el diseño teórico y el despliegue físico, ya que permite validar el direccionamiento, el enrutamiento y los valores de MTU antes de aplicar cambios en los equipos reales.

3.5.1. Diagrama de red GNS3

La topología simulada en GNS3 replica el diseño jerárquico descrito en el diseño lógico, en el MikroTik Principal se ubica en el router que se representa los laboratorios A, B, C y D e incorporando un enlace hacia el nodo que representa la red gestionable desde la cual se administra el escenario de prueba.

En esta topología:

- El MikroTik Principal concentra el enrutamiento entre todas las subredes de laboratorio.
- Cada laboratorio se modela como un router independiente, con su propia subred /24 y, en los casos necesarios, VLAN internas.
- El tráfico de prueba se genera desde hosts conectados a cada laboratorio (PCs o VPCS), lo que permite medir el comportamiento extremo a extremo entre laboratorios y hacia la red de gestión.

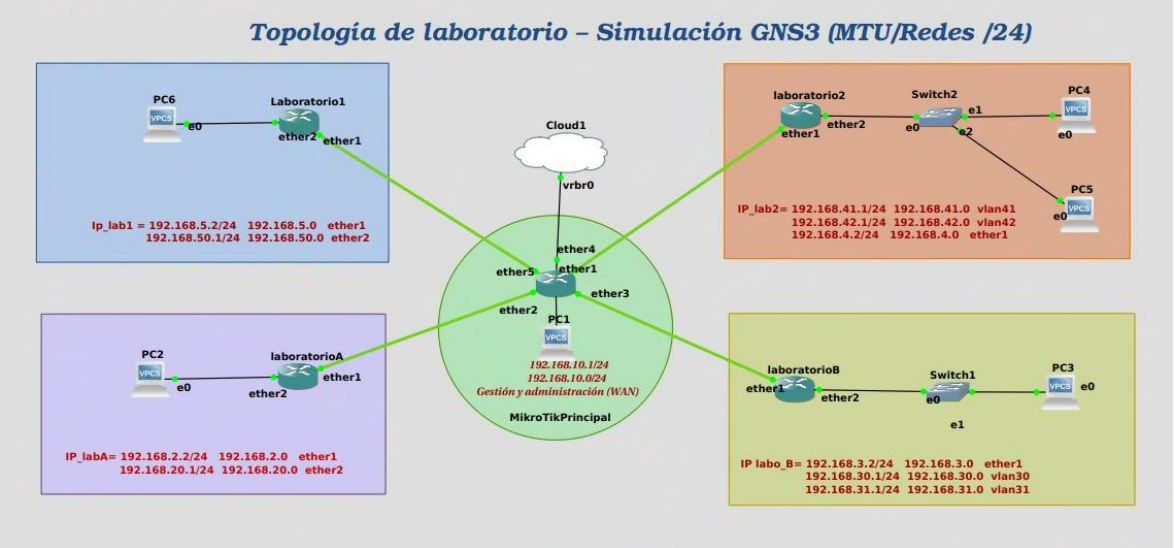


Figura 20 Simulación en GNS3

En la Figura 20, muestra la topología híbrida diseñada en el simulador GNS3, donde se aprecia el MikroTik Principal como núcleo y los cuatro routers de laboratorio como nodos de acceso.

3.5.2. Configuración inicial en GNS3

La configuración inicial tuvo como propósito dejar operativo el escenario de simulación con una base estable sobre la cual aplicar los cambios de MTU. Se realizaron las siguientes acciones generales.

- Asignación de direcciones IP estáticas a cada interfaz de los routers.
- Verificación de conectividad básica mediante *ping* entre el MikroTik principal y cada laboratorio.
- Configuración de rutas estáticas iniciales para garantizar el alcance entre todas las subredes.
- Comprobación del funcionamiento de las herramientas de prueba (Wireshark, *ping*).

Una vez validado el correcto funcionamiento del escenario base, se procedió a aplicar los ajustes de MTU en los diferentes enlaces y a registrar su impacto en las métricas de desempeño.

3.5.3. Plan de direccionamiento IP de la simulación en GNS3

En la simulación de GNS3 se implementa un esquema jerárquico de direccionamiento IP, donde cada laboratorio (A, B, C, D) tiene una red /24 independiente. El MikroTik principal actúa como núcleo de interconexión entre todas las redes de los laboratorios y se distribuye el tráfico a través de las interfaces correspondientes.

A continuación, la Tabla 14 muestra el direccionamiento del MikroTik Principal, con las interfaces correspondientes a cada enlace hacia los laboratorios y la red de gestión.

Tabla 14
Direccionamiento del MikroTik Principal

Interfaz	Dirección IP / Máscara	Subred	Gateway	Descripción
ether1	192.168.122.32/24	192.168.122.0/24	192.168.122.1	Conexión a la nube Cloud1 (gestión y administración)
ether2	192.168.2.1/24	192.168.2.0/24		Enlace con Laboratorio A
ether3	192.168.3.1/24	192.168.3.0/24		Enlace con Laboratorio B
ether4	192.168.4.1/24	192.168.4.0/24		Enlace con Laboratorio C
ether5	192.168.5.1/24	192.168.5.0/24		Enlace con Laboratorio B

El MikroTik principal concentra el enrutamiento entre las redes /24 y el acceso administrativo mediante la red 192.168.122.0/24.

Laboratorio A (MT2)

El Laboratorio A constituye una red interna de usuarios conectada al MikroTik Principal a través de la subred 192.168.2.0/24. Su objetivo es generar tráfico ICMP y TCP controlado desde equipos virtuales, con el fin de analizar la eficiencia de la transmisión bajo condiciones de MTU estándar y MTU optimizada.

La Tabla 15 se presenta el direccionamiento IP para el router del Laboratorio A, detallando las interfaces y la subred local interna.

Tabla 15
Direccionamiento del router Laboratorio A

Interfaz	Dirección IP / Máscara	Subred	Gateway	Descripción
ether1	192.168.2.2/24	192.168.20.0/24	192.168.20.1	Enlace principal con MikroTik Principal
ether2	192.168.20.1/24	192.168.2.0/24		Red local interna del laboratorio (PC de prueba)

Laboratorio B (MT3)

El Laboratorio B simula una red secundaria orientada a la medición de latencia y pérdida de paquetes en condiciones de tráfico mixto TCP/UDP. Se conecta al MikroTik Principal mediante la subred 192.168.3.0/24 y utiliza VLAN interna para segmentar el tráfico.

La tabla 16 el direccionamiento IP del router del Laboratorio B, con las interfaces y VLAN internas configuradas.

Tabla 16
Direccionamiento IP del router Laboratorio B

Interfaz	Dirección IP / Máscara	Subred	Descripción
ether1	192.168.3.2/24	192.168.3.0/24	Enlace con MikroTik Principal
vlan30	192.168.30.1/24	192.168.30.0/24	VLAN 30 – red interna de prueba
vlan31	192.168.31.1/24	192.168.31.0/24	VLAN 31 – red interna de prueba

Laboratorio B permite observar el impacto de la MTU sobre tramas etiquetadas, al agregar bytes adicionales de encabezado VLAN (IEEE 802.1Q).

Laboratorio C (MT4)

El Laboratorio C está enlazado al MikroTik Principal por la red 192.168.4.0/24 y contiene dos VLAN (vlan41 y vlan42), este diseño reproduce un entorno segmentado donde se prueban valores de MTU altos en redes con múltiples dominios lógicos.

La Tabla 17 se presentan las interfaces de direcciones IP para el router laboratorio C, con sus respectivas VLAN configuradas.

Tabla 17
Direccionamiento IP del router Laboratorio C

Interfaz	Dirección IP / Máscara	Subred	Descripción
ether1	192.168.4.2/24	192.168.4.0/24	Enlace con MikroTik Principal
vlan41	192.168.41.1/24	192.168.41.0/24	VLAN 41 – tráfico de datos interno
vlan42	192.168.42.1/24	192.168.42.0/24	VLAN 42 – tráfico de prueba optimizado

Este laboratorio se utiliza para validar la efectividad de la MTU extendida (9000 bytes) sobre tráfico de VLANs

Laboratorio D (MT5)

El Laboratorio D es el nodo final de la simulación, conectado al MikroTik Principal por la red 192.168.5.0/24, dispone de una subred local 192.168.50.0/24 destinada a equipos de usuario (PC6 o VPCS) y cámara IP utilizada en las pruebas de tráfico.

La Tabla 18se presenta el direccionamiento IP del router Laboratorio D, con las interfaces correspondientes a los dispositivos finales del laboratorio.

Tabla 18
Direccionamiento IP del router Laboratorio D

Interfaz	Dirección IP / Máscara	Subred	Descripción
ether1	192.168.5.2/24	192.168.5.0/24	Enlace con MikroTik Principal
ether2	192.168.50.1/24	192.168.50.0/24	Red local del laboratorio (PC/cámara IP)

Este segmento se utiliza para pruebas finales de throughput y comparación entre escenarios con MTU estándar (1500 bytes) y optimizada (9000 bytes) utilizando flujo de datos sostenidos y tráfico de video en tiempo real.

El direccionamiento IP adoptado en el entorno de simulación permite la comunicación bidireccional entre el MikroTik Principal y los laboratorios, garantizando la independencia lógica de cada dominio. Este modelo facilita la observación directa del impacto de la MTU en cada subred y ofrece una estructura modular adaptable para futuras pruebas de escalabilidad o enrutamiento dinámico.

3.6. Protocolos, estándares y flujo de tráfico

La simulación en GNS3 implementó varios estándares clave, incluyendo IEEE 802.3 Ethernet, IEEE 802.1Q (VLAN) y IPv4 (RFC 791). Estos protocolos son fundamentales para entender cómo los ajustes de MTU afectan la eficiencia de la red.

El entorno se diseñó bajo los principales estándares de comunicación definidos por el Institute of Electrical and Electronics Engineers (IEEE) y el Internet Engineering Task Force (IETF), garantizando que la simulación sea coherente con una red IP real, configurando las interfaces Ethernet, las VLAN, el direccionamiento IPv4 y los protocolos de transporte ICMP, TCP y UDP. Esto permite medir de forma precisa el impacto de los cambios en la MTU.

La Tabla 19 presenta un resumen de los protocolos y estándares aplicados en cada capa del modelo OSI. Estos forman la base técnica sobre la cual se generó y analizó el tráfico en la simulación.

Tabla 19
Estándares y protocolos aplicados

Capa OSI	Protocolo / Estándar	Descripción técnica	Aplicación en la simulación
Capa 1 (Física)	IEEE 802.3 (Ethernet)	Define los parámetros físicos y eléctricos de la red LAN (tramas de 1500 bytes).	Implementado en las interfaces Ethernet de los routers MikroTik y enlaces virtuales de GNS3.
Capa 2 (Enlace de datos)	IEEE 802.1Q (VLAN)	Permite la segmentación del tráfico mediante etiquetado de tramas VLAN.	Usado en Laboratorio B (vlan30, vlan31) y Laboratorio 2 (vlan41, vlan42).
Capa 3 (Red)	IPv4	Protocolo base para el direccionamiento y enrutamiento de paquetes en redes IP.	Cada subred /24 utiliza direccionamiento IPv4 estático para garantizar el control de las pruebas.
Capa 4 (Transporte)	ICMP / TCP / UDP	ICMP para pruebas de eco y conectividad, TCP y UDP para simulación de tráfico real.	ICMP en pruebas de ping, TCP/UDP en pruebas de iperf3.
Capa 7 (Aplicación)	Wireshark	Herramientas para la generación, captura y análisis de tráfico.	Implementadas en nodos finales Linux para medir rendimiento y observar fragmentación.

3.6.1. Estándares IEEE y IETF aplicados

En la simulación, se trabajó con una red real en la capa física y de enlace utilizando Ethernet (IEEE 802.3) como tecnología base, y IEEE 802.1Q para la creación de VLAN, considerando el overhead de 4 bytes que introduce el etiquetado y su efecto directo sobre la MTU disponible.

En la capa de red, se empleó IPv4, aprovechando sus campos de longitud total y las banderas DF/MF para identificar cuándo un paquete debía fragmentarse. En esta capa, se configuró ICMP para pruebas de conectividad y descubrimiento de

la MTU efectiva, TCP para flujo confiable y UDP para tráfico de baja latencia, especialmente en las pruebas de video.

De este modo, el entorno GNS3 reproduce una pila de protocolos basados en estándares IEEE/IETF adecuados para analizar el impacto de la MTU desde la capa física hasta la capa de transporte.

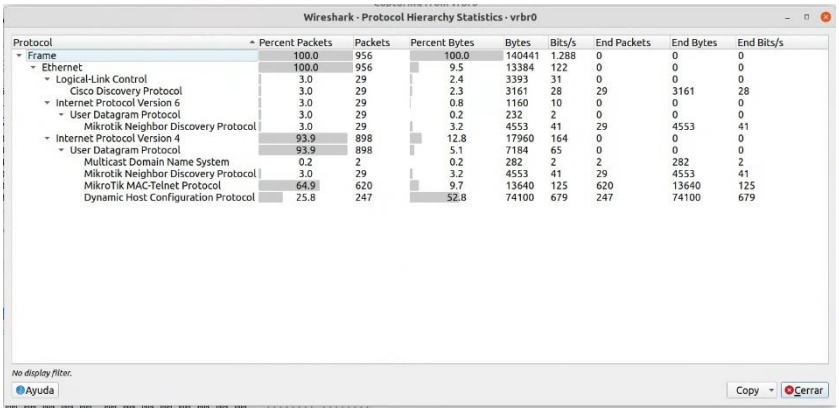


Figura 21 Estadísticas de jerarquía de protocolos capturados con Wireshark

En la Figura 21 muestra las estadísticas de jerarquía de protocolos capturados con Wireshark en la interfaz virbr0 donde se aprecia el predominio de tráfico Ethernet IPv4 y paquetes UDP.

3.6.2. Tipo de tráfico generado

En la simulación se utilizaron los mismos tipos de tráfico definido en el Capítulo II, pero ahora enfocados en su comportamiento dentro del entorno de GNS3. Se generaron paquetes de ICMP para comprobar la conectividad y medir la latencia entre MikroTik principal, en los laboratorios el flujo TCP usando iperf3 para evaluar el throughput sostenido don MTU estándar y optimizada y tráfico UDP para analizar el jitter y la perdida de paquetes en escenarios más sensibles al retardo.

Además, en los laboratorios incorporan una cámara IP se añadió tráfico de video en tiempo real lo que permitió emular el uso de las aplicaciones reales sobre la red esto se empleó como carga de prueba para comparar el comportamiento de la red con MTU de 1500 bytes frente a MTU de 9000 bytes observando como cada tipo de tráfico reacciona ante los cambios en el tamaño máximo de transmisión.

3.6.3. Flujo de tráfico entre laboratorio y núcleo de enrutamiento

El flujo de tráfico en la simulación se organiza alrededor del MikroTik Principal que actúa como núcleo de enrutamiento, todos los paquetes que se intercambian entre los laboratorios A, B, C Y D esto permite medir de forma homogénea el efecto de MTU sobre la latencia, el throughput, el jitter y la fragmentación.

El flujo de tráfico se organiza en tres tipos principales

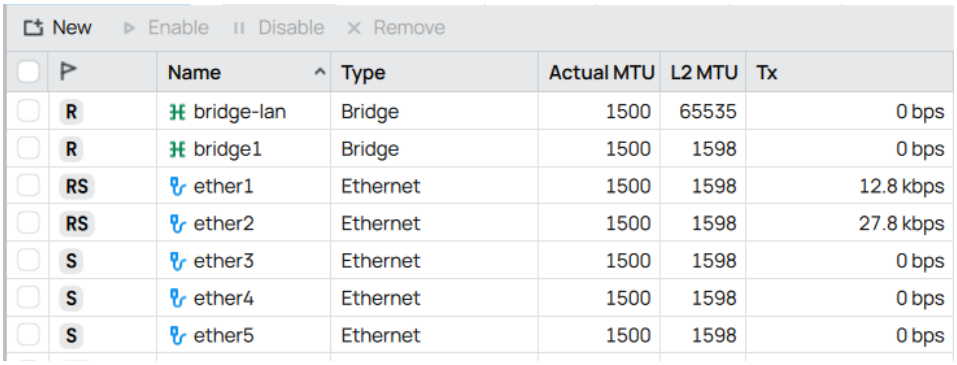
1. Tráfico de gestión, entre el host de administración (Cloud1) y el MikroTik Principal, utilizado para configurar los equipos y lanzar las pruebas sin interferir con el tráfico de usuario.
2. Tráfico de pruebas entre laboratorios: Genera con ICMP, TCP, y UDP para evaluar el impacto de la MTU en los enlaces de tránsito entre los laboratorios y en las rutas extremo a extremo. Se analiza cómo cada tipo de tráfico se ve afectado por los diferentes tamaños de MTU configurados (1500 bytes frente a 9000 bytes).
3. Tráfico de usuario interno: Emula aplicaciones reales especialmente video en tiempo real que se transmite desde las cámaras IP hacia las PCs de medición en los laboratorios. Este flujo de tráfico es fundamental para evaluar el impacto de la MTU en el rendimiento de las aplicaciones críticas que requieren transmisión continua de datos y baja latencia.

3.7.Escenarios de prueba y metodología experimental.

En esta sección se definen dos escenarios globales de prueba diferenciados por el tamaño de la MTU: 1500 bytes y 9000 bytes. Estos escenarios se aplican a los laboratorios A, B, C, y D cada laboratorio representa un caso de uso distinto: red de acceso, VLAN simples, VLAN múltiples, y tráfico de usuario final con video. La variable principal de comparación es el tamaño de la MTU configurada en los enlaces de tránsito.

3.7.1. Escenario estándar

En el escenario base se utilizó la MTU estándar de 1500 bytes, tal como suele encontrarse en redes Ethernet convencionales. Esta configuración se aplicó en los enlaces entre el MikroTik Principal y los laboratorios, manteniendo sin cambios el direccionamiento IP, la topología y los tipos de tráfico generados.



	Name	Type	Actual MTU	L2 MTU	Tx
R	bridge-lan	Bridge	1500	65535	0 bps
R	bridge1	Bridge	1500	1598	0 bps
RS	ether1	Ethernet	1500	1598	12.8 kbps
RS	ether2	Ethernet	1500	1598	27.8 kbps
S	ether3	Ethernet	1500	1598	0 bps
S	ether4	Ethernet	1500	1598	0 bps
S	ether5	Ethernet	1500	1598	0 bps

Figura 22 configuración MTU estándar (1500 bytes)

En la Figura 22 se muestra la configuración de MTU estándar (1500 bytes) aplicada y como se establece en redes Ethernet convencionales. Esta configuración de MTU es la utilizada en los enlaces de tránsito para todos los laboratorios, sin cambios en el direccionamiento IP ni en la topología, sirviendo como referencia para el escenario base.

3.7.2. Escenario optimizado

En el escenario optimizado se configuró una MTU de 9000 bytes en los mismos enlaces de tránsito, habilitando el uso de tramas jumbo. El objetivo fue comprobar si el aumento del tamaño máximo de transmisión permite reducir la fragmentación y mejorar el rendimiento general de la red.

Para garantizar una comparación justa con el escenario base:

- Se mantuvo la misma topología y el mismo plan de direccionamiento.
- Se generaron los mismos tipos de tráfico (ICMP, TCP, UDP y vídeo).
- Se repitieron las mismas pruebas de latencia, *throughput*, *jitter* y pérdida de paquetes.

De esta forma, cualquier diferencia observada entre ambos escenarios puede atribuirse principalmente al cambio en la MTU, y no a modificaciones en la estructura de la red.

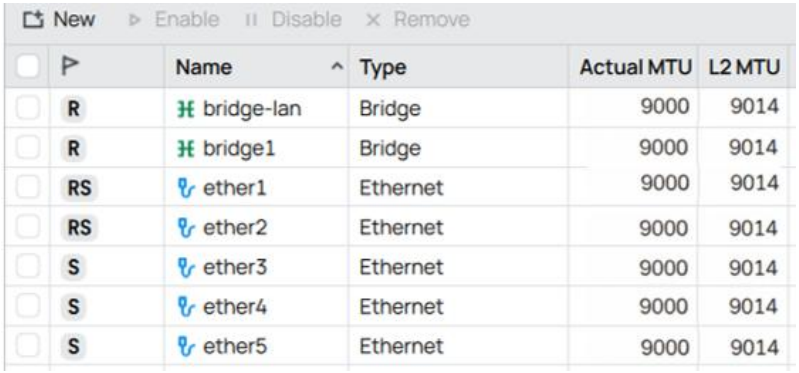


Figura 23 configuración MTU optimizada (9000 bytes)

La Figura 23 ilustra la configuración de MTU extendida (9000 bytes) sobre los mismos enlaces, correspondiente al escenario optimizado empleado para las pruebas con tramas *jumbo*.

3.7.3. Herramienta de medición

En ambos escenarios, se utilizaron herramientas conocidas y fácilmente reproducibles para obtener datos precisos sobre el comportamiento de la red bajo diferentes configuraciones de MTU. Estas herramientas incluyen.

- ✓ ping / ping con DF (Don't Fragment). Para verificar conectividad, medir la latencia y detectar la MTU efectiva en cada ruta activando el bit DF y ajustando el tamaño de los paquetes.
- ✓ iperf3 (TCP y UDP)
  - En TCP, para medir el throughput sostenido entre el núcleo y los laboratorios.
  - En UDP, para analizar jitter y pérdida de paquetes bajo distintas tasas de tráfico.
- ✓ Wireshark

  Para capturar y analizar los paquetes, verificando tamaño, encabezados IP y presencia de fragmentación.

El uso combinado de estas herramientas permitió obtener una visión completa del comportamiento de la red bajo cada configuración de MTU, proporcionando datos clave sobre el rendimiento de la red.

3.7.4. Mecanismo de transmisión, fragmentación y PMTUD

El análisis también consideró cómo la MTU influye en la forma en que los paquetes se transmiten y se fragmentan en la red:

- Con MTU 1500 bytes, cualquier paquete IP que supera este tamaño puede ser fragmentado por el router, lo que aumenta el número de fragmentos y la sobrecarga de procesamiento.
- Cuando se activa el bit Don't Fragment (DF), los routers dejan de fragmentar esos paquetes: si superan la MTU del enlace, se descartan y se genera un mensaje ICMP del tipo "Fragmentation Needed", lo que constituye la base del mecanismo Path MTU Discovery (PMTUD).

Durante las pruebas se utilizaron pings con DF y tamaños crecientes de paquete para identificar la MTU máxima sin fragmentación entre el núcleo y cada laboratorio. Al mismo tiempo, con Wireshark se revisaron los campos de cabecera IP relacionados con la fragmentación, lo que permitió confirmar, de forma práctica, la diferencia de comportamiento entre el escenario base (1500 bytes) y el optimizado (9000 bytes).

Una vez validados los parámetros de direccionamiento, enrutamiento y los valores de MTU en el entorno virtual GNS3, se procede a replica la topología utilizando hardware físico MikroTik, permitiendo verificar el rendimiento de la red bajo conficiones reales de operación.

3.8. Implementación Física de la red

La implementación física de la red trasladó el diseño validado en la simulación a un entorno real, utilizando un router MikroTik hEX como núcleo de la red cableada, un MikroTik RB2011 como punto de acceso inalámbrico y cuatro routers hEX adicionales para los laboratorios A, B, C y D. La lógica de

direccionamiento, segmentación por VLAN y escenarios de prueba se mantuvieron equivalentes a la definida en el entorno de simulación, a fin de que las mediciones de MTU fueran comparables entre ambos entornos.

3.8.1. Arquitectura física y conexión de los equipos

Los equipos se interconectaron siguiendo una topología de estrella extendida, en el centro de la estructura el router MikroTik hEX actúa como núcleo de enrutamiento y punto de agregación para todas las redes de laboratorio, mientras que el MikroTik RB2011 se configura como punto de acceso inalámbrico, dando servicio tanto a las VLAN de los laboratorios como a la red de invitados.

Desde el hEX principal se distribuyen mediante puertos físicos específicos, los enlaces hacia los segmentos cableados que conforman los laboratorios A, B, C y D. Estos están conectados paralelamente a uno de los puertos del hEX, que se utiliza como troncal 802.1Q para transportar las VLAN de gestión y de acceso inalámbrico hasta el RB2011. Esto facilita centralizar la configuración de la MTU, la asignación de direcciones IP (DHCP) y la aplicación de las políticas de seguridad.

Esto permite mantener la topología jerárquica diseñada previamente en GNS3 y, al mismo tiempo, garantizar que los resultados obtenidos en la simulación puedan compararse de forma directa con los de la implantación real.

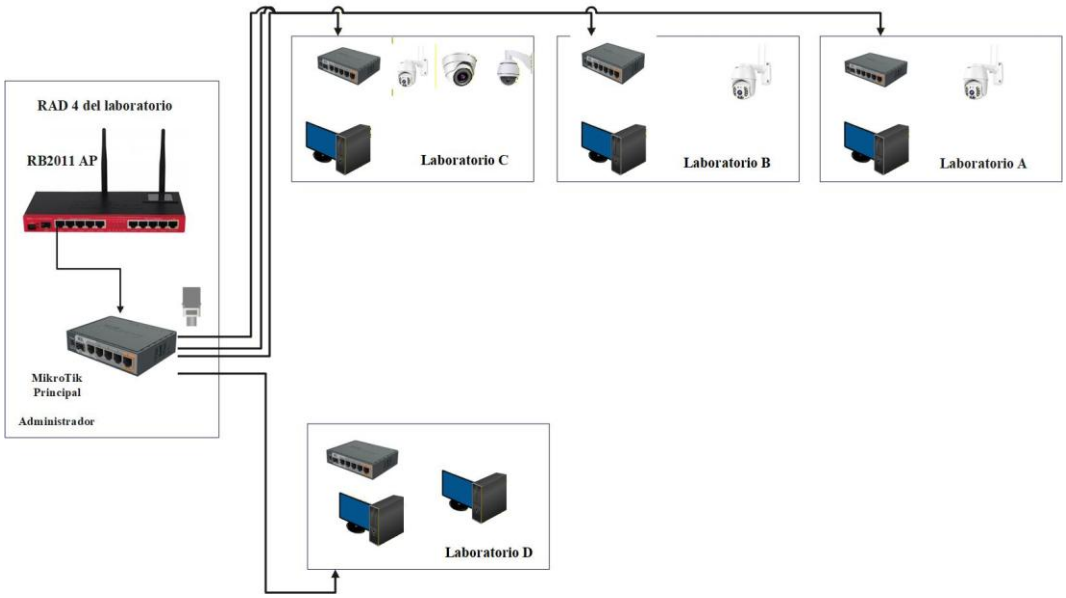


Figura 24 Esquema físico de la conexión de la red.

En la figura 24 se muestra el esquema físico de conexión, donde se observan los enlaces entre el núcleo, el punto de acceso y los laboratorios, así como la ubicación de las PCs de prueba y las cámaras IP.

3.8.2. Plan de Direccionamiento en la implementación física

El plan de direccionamiento en la implementación física mantiene la misma estructura jerárquica utilizada en la simulación, pero ajustando a la infraestructura real. Este direccionamiento está diseñado para garantizar la conectividad adecuada entre los equipos, facilitar la administración de la red y permite mantener la consistencia necesaria para comparar el comportamiento de la MTU entre ambos entornos.

3.8.2.1. VLANs sobre el troncal hEX ⇄ RB2011

Sobre el enlace troncal entre el hEX principal y el RB2011 se implementaron tres VLAN, cada una con un uso específico:

- VLAN 10: tráfico inalámbrico de laboratorio (SSID LAB-V10).
- VLAN 20: tráfico inalámbrico de invitados (SSID INVITADOS-V20).
- VLAN 99: red de gestión para la administración de los equipos.

Cada VLAN disponible de su respectivo gateway en el hEX principal y de un rango de direcciones asignadas mediante DHCP esto permite incorporar dispositivos inalámbricos a los escenarios de prueba sin necesidad de configuraciones manuales.

El RB2011 obtiene su dirección de gestión dentro del VLAN 99 y restringiendo así el acceso administrativo a dicha red.

La Tabla 20 resume el direccionamiento de las VLAN configuradas sobre el troncal entre el hEX y el RB2011. El hEX actúa como Gateway de las VLAN 10, 20 y 99, entregando direcciones mediante DHCP a las redes de laboratorio inalámbrico, invitados y gestión

Tabla 20
Plan de direccionamiento de VLANs sobre el troncal hEX–RB2011

VLAN	Red / Máscara	Gateway (hEX)	Rango DHCP	Uso
10	192.168.10.0/24	192.168.10.1	192.168.10.100–192.168.10.199	SSID LAB-V10 (usuarios lab)
20	192.168.20.0/24	192.168.20.1	192.168.20.100–192.168.20.199	SSID INVITADOS-V20
99	192.168.99.0/24	192.168.99.1	192.168.99.100–192.168.99.199	Gestión y administración

3.8.2.2. Redes de laboratorio

Las redes cableadas de laboratorio se implementan directamente sobre puertos físicos del hEX principal, asignando a cada laboratorio una subred /24.

La Tabla 21 resume el direccionamiento IP de las redes de laboratorio configuradas en el MikroTik Principal, con sus respectivos gateways y rangos DHCP asignado.

Tabla 21
Redes cableadas de laboratorio en el MikroTik Principal

Laboratorio	Red / Máscara	Gateway (hEX Principal)	Rango DHCP	Uso principal
Lab A	192.168.2.0/24	192.168.2.1	192.168.2.100–192.168.2.199	Pruebas de acceso simple (PC/cámara)
Lab B	192.168.3.0/24	192.168.3.1	192.168.3.100–192.168.3.199	Pruebas con VLAN 30/31
Lab C	192.168.4.0/24	192.168.4.1	192.168.4.100–192.168.4.199	Pruebas con múltiples VLAN (41/42)
Lab D	192.168.5.0/24	192.168.5.1	192.168.5.100–192.168.5.199	Escenario de usuario final (PC + cámara IP)

El hEX actúa como Gateway y servidores DHCP para cada una de estas redes permitiendo conectar los equipos de laboratorio sin necesidad de configurar monuelamente se habilita el cliente NTP para sincronizar la hora y se restringe el acceso a SSH/Winbox exclusivamente a la VLAN99 reduciendo la exposición de servicios administrativos. En un entorno de producción real, se recomienda además restringir el acceso a la VLAN de gestión mediante listas de control de acceso (ACL) vinculadas a direcciones MAC específicas, aunque para este laboratorio se limitó por interfaz.

3.8.3. Configuración del RB2011

El equipo MikroTik RB2011 se configuró como punto de acceso inalámbrico, conectado al router hEX principal mediante un enlace troncal 802.1Q, el tráfico de las VLANS 10 laboratorio, 20 invitados y 99 gestión se transportan mediante este troncal manteniendo la segmentación establecida en el plan de direccionamiento.

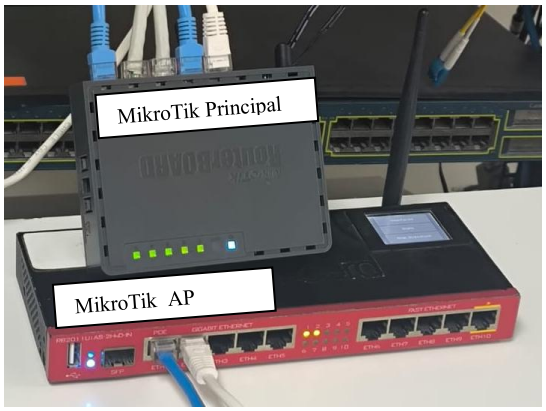


Figura 25 MikroTik RB2011 y hEX Principal conectados en la red.

En la figura 25 el MikroTik RB2011 es utilizado como punto de acceso inalámbrico, mientras que el MikroTik hEX actúa como el núcleo central de la red, gestionando la conexión de los laboratorios y las VLANs.

En la configuración de MikroTik RB2011, se emplea un bridge para gestionar el tráfico de las VLANs a través del enlace troncal, garantizando que cada segmento de la red esté adecuadamente segmentado y que el tráfico sea tratado correctamente. Esto permite no solo segmentar el tráfico de forma eficiente, sino

también asegurar que el tráfico de los laboratorios y de los invitados no interfiera con la administración de la red, mejorando la seguridad y el rendimiento general.

3.8.3.1. Bridge y puerto troncal

1. **Creación del bridge principal**

- Menú: Bridge → Bridge → Add (+)
- Name: br-ap

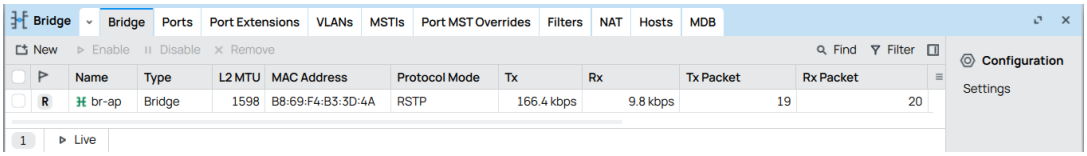


Figura 26 bridge principal br-ap con VLAN Filtering

En la figura 26, se observa la creación del bridge es la base para conectar todas las interfaces físicas del RB2011, y el puerto troncal ether2 será el encargado de llevar el tráfico entre el MikroTik RB2011 y el MikroTik hEX a travez del enlace 802.1Q.

2. **Puerto troncal ether2**

- Menú: Bridge →Ports
- Interface: ether2
- Bridge: br-ap

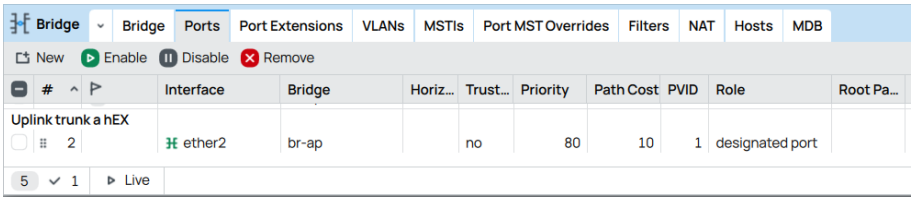


Figura 27 Asociación del puerto troncal ether2 al bridge br-ap en el RB2011

En la figura 27 muestra la asociación del puerto troncal ether2 se asocia al bridge br-ap, permitiendo que el tráfico de las VLANs se gestione correctamente por el dispositivo.

3. **Asociación de SSID al bridge**

- Menú: Bridge → Ports
- Las interfaces wlan1-v10 (SSID LAB-V10) y wlan1-v20 (SSID INVITADOS-V20) se asignan al bridge br-ap.

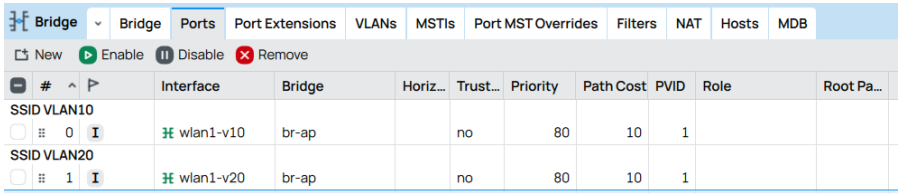


Figura 28 Asociación de SSID al bridge

En la figura 28 se observa la asignación las interfaces virtuales corresponde a los SSID de laboratorio e invitados garantizando que el tráfico inalámbrico se integre correctamente en el enlace troncal y en la segmentación por VLAN.

3.8.3.2. Dirección IP gestión

Configuración de la interfaz VLAN de gestión

- Menú: Interface→ VLAN
- Name: vlan99-mgmt
- VLAN ID: 99
- Interface: br-ap.

Asignación de dirección IP de gestión:

- Menú: IP → Addresses → Add (+)
- Dirección: 192.168.99.2/24
- Interface: vlan99-mgm

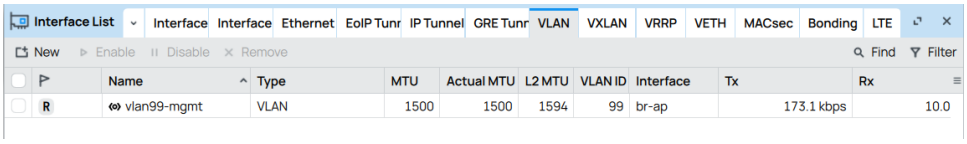


Figura 29 Interfaz de gestión vlan99-mgmt (VLAN 99) creada sobre el bridge br-ap en el RB2011.

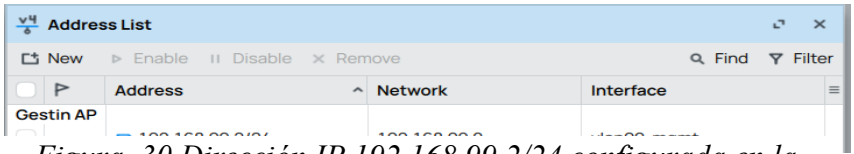


Figura 30 Dirección IP 192.168.99.2/24 configurada en la interfaz vlan99-mgmt del MikroTik RB2011.

En la figura1 29 y 30 muestra la dirección IP configurada en la interfaz vlan99-mgmt del MikroTik RB2011, utilizada exclusivamente para la administración del equipo dentro de la VLAN 99 garantizando seguridad y aislamiento del tráfico administrativo al tráfico de usuario e invitados.

3.9. MikroTik Principal

El router MikroTik hEX se configuró como núcleo de enrutamiento gestionando todas las conexiones entre los laboratorios, las VLAN transportada por el enlace troncal y la red de admiración es el encargado de recibir, procesar y reenviar los paquetes generados en cada escenario de prueba y además se concentran servicios de red como DHCP, DNS y NPT con los ajustes de MTU definidos en el diseño experimental.

3.9.1. Direccionamiento IP de las interfaces de laboratorio

El MikroTik hEX conecta directamente los laboratorios A, B, C y D, asignado a cada laboratorio se asignó una subred /24 para permitir un aislamiento adecuado del tráfico y las interfaces físicas fueron configuradas con direcciones IP estáticas permitiendo identificar claramente cada segmento y facilitar el enrutamiento.

Tabla 22
Direccionamiento IP configurado en el MikroTik Principal (hEX).

Interfaz	Red / Máscara	Dirección IP (gateway)	Uso / Descripción
ether2	192.168.2.0/24	192.168.2.1	Lab A
ether3	192.168.3.0/24	192.168.3.1	Lab B
ether4	192.168.4.0/24	192.168.4.1	Lab C
ether5	192.168.5.0/24	192.168.5.1	Lab D

A continuación, se muestra la configuración en el MikroTik Principal (hEX) donde se asignaron las direcciones IP para cada laboratorio, asegurando la correcta segmentación de tráfico entre los laboratorios y garantizando un acceso eficiente.

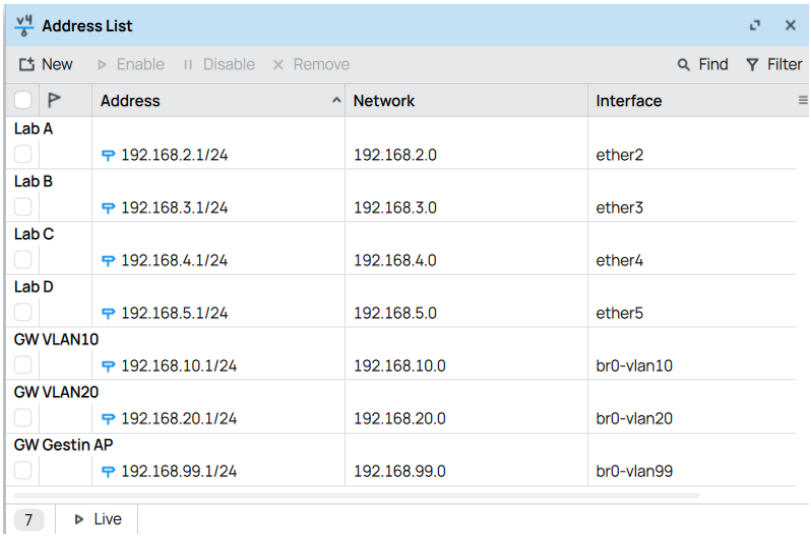


Figura 31 Las interfaces físicas y lógicas en el MikroTik hEX.

La figura 31 ilustra las direcciones IP configuradas en las interfaces del MikroTik, visualizando cómo cada laboratorio está conectado a su respectiva subred /24. Esto facilita la administración y el aislamiento de tráfico entre los laboratorios A, B, C y D

3.9.2. Configuración de VLANs en el MikroTik Principal

En el MikroTik hEX Principal, se configuraron varias VLAN para segmentar el tráfico y mejorar el control y la seguridad de la red. Se creó un bridge denominado br0 para gestionar el tráfico de las VLANs, y se asignaron las direcciones IP correspondientes a cada una de ellas. Además, se habilitó el VLAN Filtering en el bridge para asegurar que solo el tráfico etiquetado con la VLAN correspondiente sea aceptado en cada puerto.

La Tabla 23 se presenta la configuración de las VLANs en el MikroTik Principal.

Tabla 23
VLANs en el bridge del MikroTik Principal

Interfaz	Red / Máscara	Dirección IP (gateway)	Uso / Descripción
br0-vlan10	192.168.10.0/24	192.168.10.1	VLAN 10 – WiFi laboratorio (LAB-V10)
br0-vlan20	192.168.20.0/24	192.168.20.1	VLAN 20 – WiFi invitados (INVITADOS-V20)
br0-vlan99	192.168.99.0/24	192.168.99.1	VLAN 99 – Gestión y administración

Figura 31 se muestra la ventana IP Addresses de Winbox, se muestran las direcciones IP asignadas a las interfaces físicas ether2–ether5 y a las interfaces VLAN br0-vlan10, br0-vlan20, y br0-vlan99, siguiendo el plan de direccionamiento descrito en las Tablas 26 y 27.

3.9.2.1. Bridge y troncal de VLAN en el núcleo

Para permitir la comunicación entre los diferentes segmentos de red y garantizar una correcta integración de las VLANs a través del enlace troncal, se configuró un bridge en el MikroTik Principal (hEX). Este bridge actúa como punto de agregación para las subinterfaces VLAN y el puerto físico que enlaza con el RB2011.

A continuación, se detallan los pasos para la configuración del bridge y el enlace troncal de VLAN en el MikroTik hEX:

1. **Creación del bridge br0 y activación de VLAN Filtering**

- Menú: Bridge → Bridge → Add (+).
- Nombre: br0.

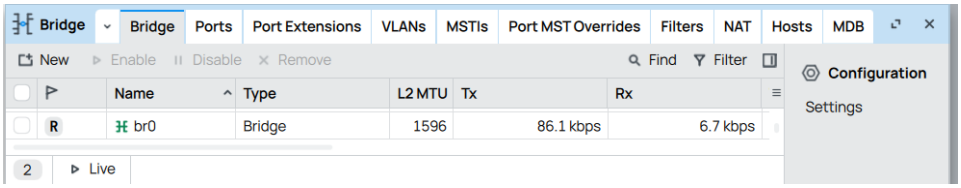


Figura 32 bridge br0

En la figura 32 se muestra la creación de bridge bro en MikroTik hEX, que servirá para gestionar las VLANs en el núcleo de la red, se habilitó la opción VLAN Filtering lo que el bridge pasa a aplicar las reglas de etiquetado y des-etiquetado definidas en la tabla de VLAN.

2. Asociación del puerto troncal al bridge

- Menú: Bridge → Ports → Add (+).
- Interface: ether1 (enlace físico hacia el RB2011).
- Bridge: br0.

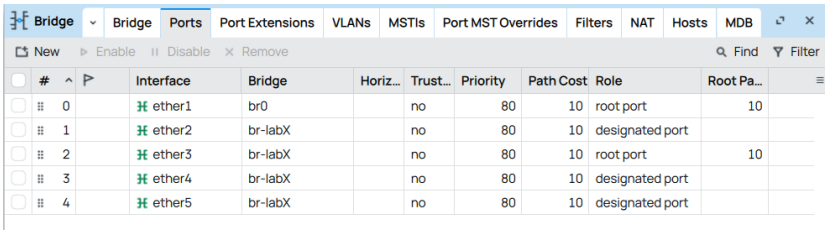


Figura 33 Asociación del puerto troncal al bridge

En la figura 33, Asociación del puerto ether1 al bridge br0 como enlace troncal hacia el RB2011. Los puertos ether2–ether5 forman parte del bridge br-labX, destinado a los laboratorios cableados.

3. Definición de la tabla de VLAN en el bridge

- Menú: Bridge → VLANs → Add (+).

Para cada VLAN se creó una entrada en el bridge br0 según se muestre en la Tabla 24.

Tabla 24
VLAN en el bridge

Interfaz	Bridge	PVID	Rol / Comentario
ether1	br0	1	Uplink troncal hacia RB2011
br0-vlan10	br0	10	Tráfico LAB-V10 (WiFi lab)
br0-vlan20	br0	20	Tráfico INVITADOS-V20
br0-vlan99	br0	99	Tráfico de gestión

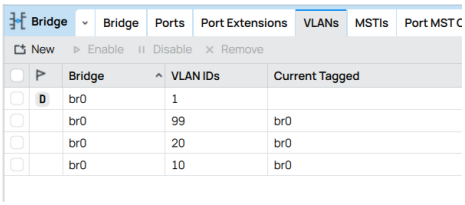


Figura 34 Bridge → VLANs

En la Figura 34 se aprecia que ether1 está unido al bridge br0 como puerto troncal, esta configuración garantiza que el tráfico de laboratorio, invitados y gestión circule de forma segmentada entre el núcleo y el punto de acceso RB2011.

3.9.2.2. Activación de servicio de red en el MikroTik Principal

Se describen los pasos y configuraciones necesarias para habilitar los servicios básicos de red en el MikroTik Principal, lo cual es crucial para garantizar el correcto funcionamiento de la red, así como para proporcionar la conectividad y funcionalidad necesarias durante las pruebas de MTU.

A continuación, se describen los pasos y configuraciones necesarias para habilitar los servicios básicos de red en el MikroTik Principal.

1. Activación del servicio DHCP

El servicio DHCP se configuró para asignar dinámicamente direcciones IP a los dispositivos de los laboratorios y redes asociadas, simplificando la gestión de direcciones y evitando la configuración manual.

- Menú: IP → Pool
- IP → DHCP Server.

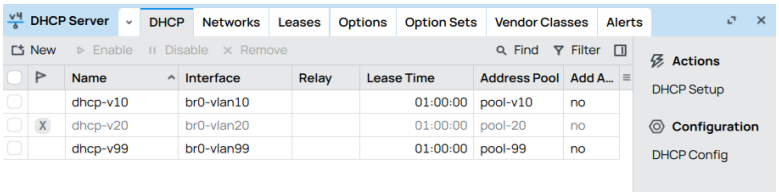


Figura 35 IP → DHCP Server

En la figura 35, los PCs de laboratorio, cámaras IP y dispositivos inalámbricos obtienen automáticamente una dirección válida, su puerta de enlace y parámetros de DNS sin requerir configuración manual.

2. Servicio de DNS local.

El router se configuró como DNS caché local, permitiendo resolver nombres y reducir consultas externas repetidas. Esto simplifica las pruebas de aplicaciones que utilizan nombres de dominio en lugar de direcciones IP.

- Menú: IP → DNS.

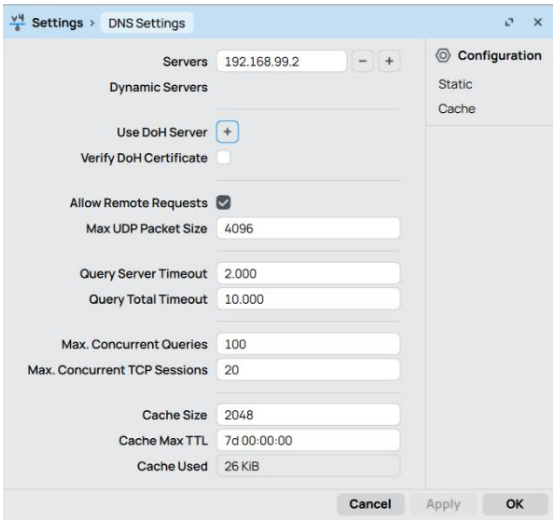


Figura 36 IP → DNS.

La figura 36 muestra cómo se habilitó la opción Allow Remote Requests únicamente para las redes internas, con reenvío hacia servidores DNS públicos, esto reduce el número de consultas externas repetidas y facilita las pruebas de aplicaciones que usan nombres simbólicos en lugar de direcciones IP.

3. **Activación de NTP.**

Se habilitó el cliente NTP apuntando a servidores horarios públicos, con el fin de mantener sincronizado el reloj del dispositivo. La sincronización horaria facilita la interpretación de capturas en Wireshark y la correlación de eventos entre distintos equipos.

- Menú: System → NTP Client

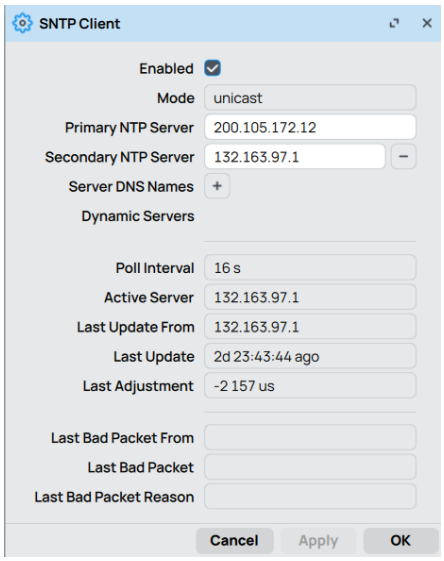


Figura 37 System → NTP Client

La sincronización temporal facilita la interpretación de capturas en Wireshark y la correlación de eventos entre distintos equipos de la red se muestra en la figura 37.

4. **Restricción de acceso administrativo.**

Para reducir la superficie de ataque, se limitaron los servicios administrativos (Winbox, SSH y HTTP) exclusivamente a la red de gestión VLAN 99, bloqueando accesos desde otras subredes mediante reglas de firewall. De esta manera, solo los hosts autorizados en la red 192.168.99.0/24 pueden administrar el hEX y el RB2011.

3.9.2.3. Laboratorio A

En el Laboratorio A, se ha implementado una infraestructura de red que incluye tanto el cableado físico como los dispositivos de prueba para evaluar el rendimiento de la red bajo distintas configuraciones de MTU como se ve en la figura 38. Esta parte del proyecto permite realizar pruebas controladas de conectividad, transmisión de datos y segmentación de tráfico.

Está configurado como una red interna de usuarios, conectada al MikroTik Principal mediante la subred 192.168.2.0/24. En este entorno, se generan tráfico ICMP y TCP controlado desde equipos virtuales, como PCs o dispositivos de prueba, para analizar la eficiencia de la transmisión bajo dos condiciones de MTU:

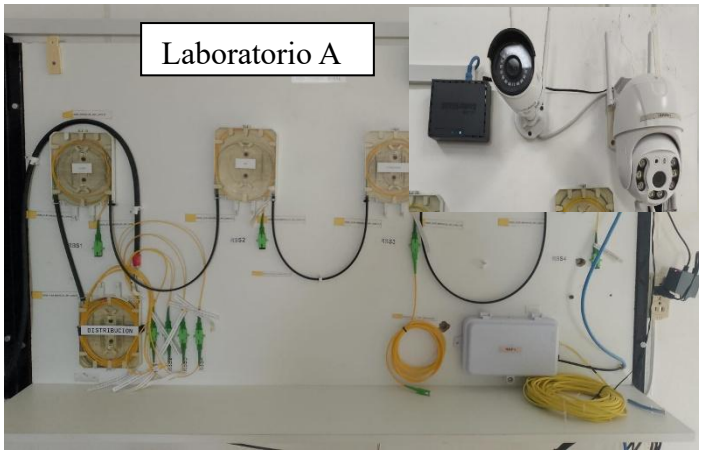


Figura 38 Esquema físico del Laboratorio A

la estándar de 1500 bytes y la optimizada de 9000 bytes. Las pruebas realizadas en este laboratorio son esenciales para observar el impacto de la configuración de la MTU sobre la latencia, el throughput y la fragmentación de los paquetes.

1. Configuración de Interfaces y Dirección IP en MikroTik Principal

En enterfaz gráfica de Winbox, se configuró el MikroTik Principal (hEX) para conectar el Laboratorio A con la subred 192.168.2.0/24. A continuación se detalla el proceso:

Accede a la interfaz de configuración:

- IP > Addresses.
    - Dirección IP a la Interfaz ether2:
    - Asigna la dirección IP 192.168.2.1/24 a la interfaz ether2 (conectada al Laboratorio A).
    - Esto permitirá que el MikroTik Principal actúe como la puerta de enlace para los dispositivos del Laboratorio A.

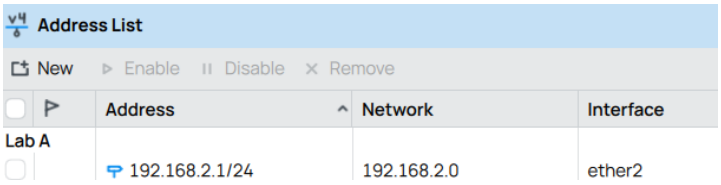


Figura 39 IP_lab A

La figura 39 muestra la infraestructura física del Laboratorio A está compuesta por equipos de red organizados de forma eficiente para asegurar el buen funcionamiento de las pruebas. En la Figura 38, se muestra el esquema físico del laboratorio,

2. Direccionamiento IP

El MikroTik hEX está configurado para gestionar las conexiones de red en el Laboratorio A. en la siguiente Tabla 25, la dirección IP 192.168.2.10/24 está asignada al bridge br-labA del router, lo que permite la conectividad entre los dispositivos conectados al laboratorio.

Tabla 25
Direccionamiento IP

Elemento	**Dirección IP / Rango**	**Máscara de Subred**	**Rango DHCP / Observación**
Gateway (MikroTik Principal)	192.168.2.1	255.255.255.0	Asigna direcciones 192.168.2.100–192.168.2.199 a los dispositivos del laboratorio.
Router Lab A (gestión)	192.168.2.10	255.255.255.0	IP estática sobre el bridge br-labA del MikroTik hEX.
Dispositivos de prueba	192.168.2.100–192.168.2.199	255.255.255.0	Direcciones asignadas dinámicamente mediante DHCP.

3. Configuración de Interfaces y Bridge

El MikroTik hEX en el Laboratorio A está configurado sin VLANs, pero con las interfaces ether2, ether3 y ether4 integradas al bridge br-labA. Este bridge se utiliza para gestionar la conexión de las PCs de prueba y otros dispositivos dentro del laboratorio.

Como se observa en la figura 40, el bridge centraliza el tráfico interno del laboratorio

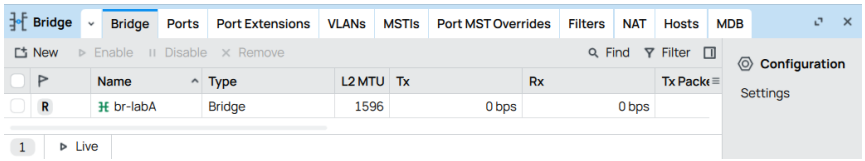


Figura 40 Bridge-br-labA

4. Direcciones IP

La figura 41 muestra el direccionamiento IP en el MikroTik hEX para el Laboratorio A está configurado para garantizar la conectividad entre los dispositivos de prueba, con la asignación de direcciones IP estáticas y dinámicas a través del servidor DHCP.

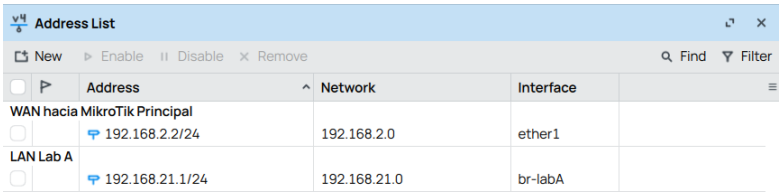


Figura 41 Direccionamiento IP del router Lab A (WAN y LAN)

5. Configuración del Servidor DHCP

La figura 42, el servidor DHCP del MikroTik hEX está habilitado para asignar direcciones IP dinámicamente a los dispositivos conectados al laboratorio. El rango de direcciones IP asignadas por el servidor DHCP es 192.168.2.100 al 192.168.2.199.

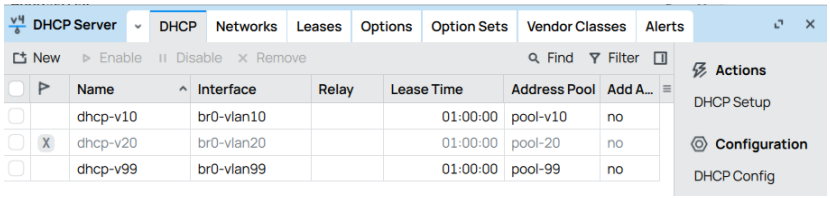


Figura 42 servidor DHCP

En la figura 43 el comando *ping* muestra que hay conexión exitosa entre el dispositivo en el laboratorio A y el MikroTik Principal (192.168.2.1). Todos los paquetes fueron recibidos sin pérdida, con una latencia de 0 ms, lo que indica que la red está operando correctamente y sin problemas de conectividad o fragmentación. Esto confirma que la comunicación entre ambos dispositivos es estable y eficiente.

```
[admin@Lab A] > ping 192.168.2.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.2.1                                56  64 0ms
    1 192.168.2.1                                56  64 0ms
    2 192.168.2.1                                56  64 0ms
    3 192.168.2.1                                56  64 0ms
    4 192.168.2.1                                56  64 0ms
    5 192.168.2.1                                56  64 0ms
    6 192.168.2.1                                56  64 0ms
    7 192.168.2.1                                56  64 0ms
    8 192.168.2.1                                56  64 0ms
    9 192.168.2.1                                56  64 0ms
   10 192.168.2.1                                56  64 0ms
```

Figura 43 Resultado de la prueba de ping desde el Laboratorio A

3.9.2.4. Laboratorio B

La imagen proporcionada muestra al montaje físico del Laboratorio B, que ha sido diseñado para evaluar el impacto de la MTU en redes segmentadas por VLAN. En este laboratorio, las VLAN 30 y 31 están configuradas para analizar

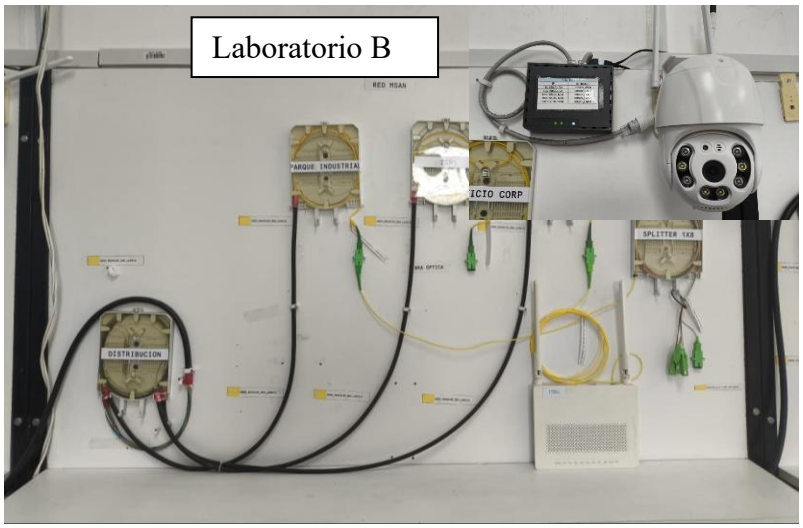


Figura 44 Esquema físico del Laboratorio B

cómo el tráfico etiquetado en VLANs responde a diferentes configuraciones de MTU, observando factores como la latencia, fragmentación y throughput.

El Laboratorio B se implementa con la infraestructura adecuada para realizar pruebas de conectividad bajo condiciones de tráfico con VLAN. El montaje físico, mostrado en la Figura 44, consiste en el siguiente:

- Router MikroTik hEX: Conectado al MikroTik Principal mediante un enlace Ethernet en la interfaz ether1.
- VLAN 30 y VLAN 31: Segmentan el tráfico del laboratorio, permitiendo la prueba de conectividad bajo diferentes configuraciones de MTU.

1. Direccionamiento IP en el Router MikroTik del Laboratorio B

El MikroTik hEX en Laboratorio B está configurado para manejar las interfaces VLAN, además de gestionar el tráfico entre las VLANs y el MikroTik Principal. En la Tabla 26 se presenta la configuración de las direcciones IP en el router del laboratorio B.

Tabla 26
Direccionamiento IP del router del Laboratorio B

Interfaz	Tipo	Dirección IP / Máscara	Red / Descripción
ether1	WAN	192.168.3.2/24	Enlace hacia MikroTik Principal
vlan30	VLAN 30	192.168.30.1/24	Red interna de prueba (VLAN 30)
vlan31	VLAN 31	192.168.31.1/24	Red interna de prueba (VLAN 31)

2. Configuración de Interfaces VLAN

Estas interfaces VLAN permiten segmentar el tráfico y realizar pruebas de conectividad en condiciones controladas como se detalla en la figura 45.

- ether1 tiene la dirección 192.168.3.2/24, que conecta el Laboratorio B al MikroTik Principal.

- vlan30 y vlan31 tienen las direcciones 192.168.30.1/24 y 192.168.31.1/24, respectivamente, que gestionan el tráfico dentro del Laboratorio B para cada VLAN.

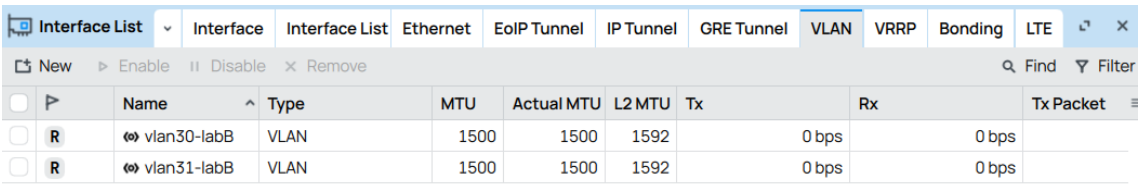


Figura 45 Configuración de las Interfaces VLAN

3. Servidor DHCP en Winbox:

El MikroTik hEX está configurado para proporcionar direcciones IP dinámicas dentro de las VLANs. En Winbox, puedes ver que el servidor DHCP está activo y asignando direcciones dentro de los rangos definidos para vlan30 y vlan31.

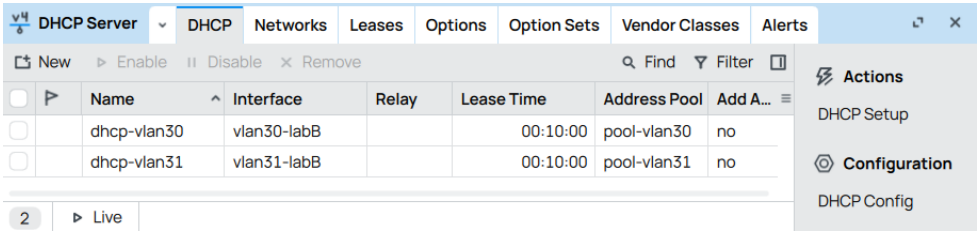


Figura 46 Configuración de DHCP

En esta figura 46 se muestra la configuración del servidor DHCP en Winbox, que asigna direcciones IP dinámicas dentro de las VLANs 30 y 31 del Laboratorio B.

La figura 47 muestra el ping realizado desde el laboratorio B muestra que hay conexión exitosa hacia el MikroTik Principal (192.168.3.1). Todos los paquetes fueron enviados y recibidos correctamente, sin pérdida de paquetes, y con una latencia de 0 ms en cada intento esto confirma que la conectividad es estable y que no existen problemas de fragmentación o retrasos en la transmisión de datos.

```
[admin@Lab B] > ping 192.168.3.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.3.1                                56  64 0ms
    1 192.168.3.1                                56  64 0ms
    2 192.168.3.1                                56  64 0ms
    3 192.168.3.1                                56  64 0ms
    4 192.168.3.1                                56  64 0ms
    5 192.168.3.1                                56  64 0ms
    6 192.168.3.1                                56  64 0ms
    7 192.168.3.1                                56  64 0ms
    8 192.168.3.1                                56  64 0ms
    9 192.168.3.1                                56  64 0ms
   10 192.168.3.1                                56  64 0ms
    sent=11 received=11 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Figura 47 Resultado de la prueba de ping desde el Laboratorio B

3.9.2.5. Laboratorio C

El laboratorio C se conecta al MikroTik Principal mediante la interfaz ether4, implementando dos VLANs: VLAN 41 y VLAN 42. Este escenario simula una red segmentada diseñada para evaluar el comportamiento de la MTU extendida (9000 bytes) sobre tramas VLAN y analizar su rendimiento en redes con múltiples dominios lógicos.

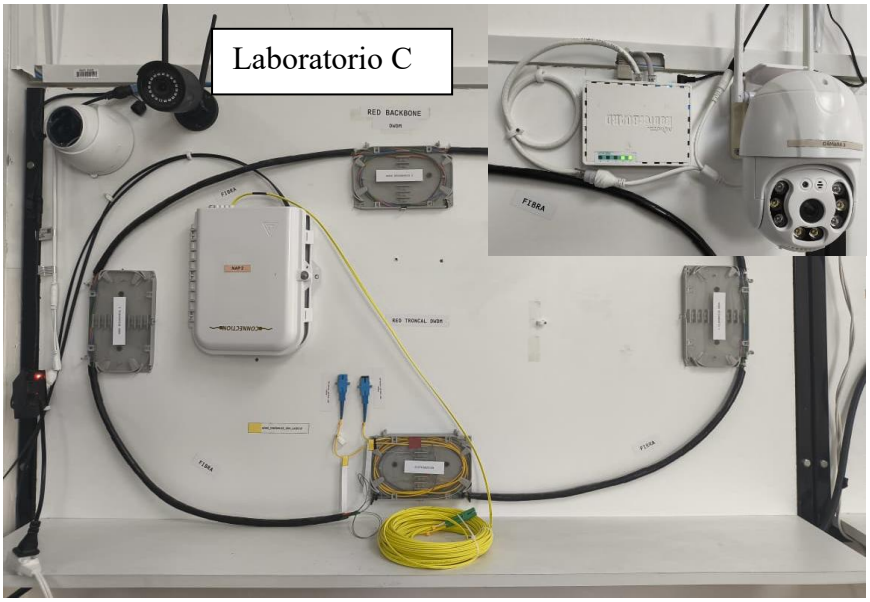


Figura 48 Esquema físico del Laboratorio C

La figura 48 muestra el montaje físico del entorno de laboratorios empleado para las pruebas de rendimiento, donde se integra equipamiento real de la red, cámaras IP y enlaces de fibra óptica.

1. Configuración de interfaces VLAN en el MikroTik Principal

En el MikroTik Principal, las interfaces VLAN asociadas a br0 son configuradas para las VLANs 41 y 42. Se asignan direcciones IP a estas interfaces para facilitar la conectividad entre el MikroTik Principal y los equipos del Laboratorio C.

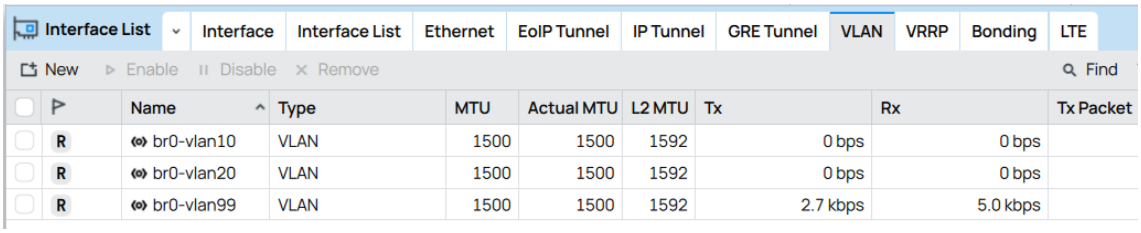


Figura 49 VLAN

Como se observa en la figura 49, estas configuraciones aseguran que los paquetes de datos entre las diferentes VLANs puedan ser correctamente enrutados y gestionados en el MikroTik Principal.

2. Configuración del bridge para el Laboratorio C

El bridge br-labC se configura para gestionar el tráfico interno del laboratorio y conectar las interfaces físicas con las VLANs correspondientes.

Crear un Bridge para el Laboratorio C

- Menú: Bridge
- Asigna el nombre "br-labC".
- Habilita "VLAN Filtering".

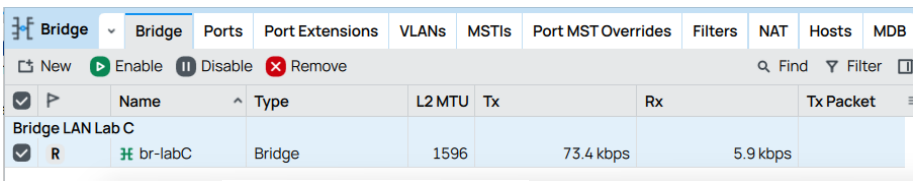


Figura 50 br-labC

Como se observa en la Figura 50, la habilitación de VLAN Filtering permite que el bridge procese únicamente los paquetes etiquetados con la VLAN adecuada, evidenciando el tráfico entre dominios lógicos

1. Agregar las Interfaces VLAN 41 y 42:

- Crea las interfaces VLAN para cada red:
  - VLAN ID: 41
  - VLAN ID: 42

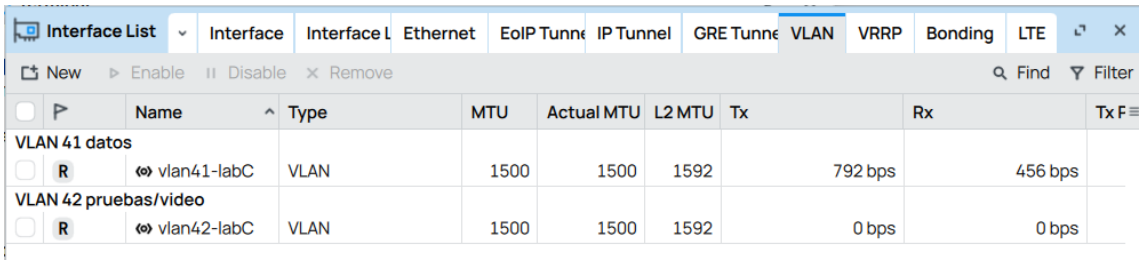


Figura 51 VLAN 41 y 42

La Figura 51 muestra la asignación de la interface VLAN al bridge br-lanC permitiendo que cada VLAN administre su propio dominio de broadcast.

3. **Configuración de la IP para las VLANs del Laboratorio C**

Cada VLAN necesita una dirección IP para garantizar que los dispositivos dentro del laboratorio puedan comunicarse con otros dispositivos en la red. En este caso, las direcciones IP se asignan de la siguiente forma

- Ve a IP > Addresses en Winbox.
  - VLAN 41: 192.168.41.1/24
  - VLAN 42: 192.168.42.1/24

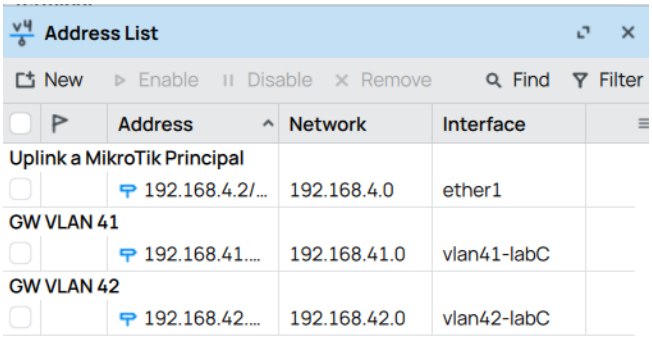


Figura 52 VLAN 41 y VLAN 42.

Se aprecia en la Figura 52, estas direcciones aseguran que cada dispositivo conectado en las VLANs pueda comunicarse correctamente dentro del laboratorio y hacia el MikroTik Principal

4. Cámara IP en el Laboratorio C

En el Laboratorio C se incorporó una cámara IP como generadora de tráfico de vídeo en tiempo real, con el fin de evaluar el impacto de la MTU sobre flujos continuos tipo streaming. La cámara se conectó mediante cable UTP categoría 6 al puerto ether2 del router hEX del laboratorio, configurado como puerto de acceso dentro del bridge br-labC, asociado a la red 192.168.41.0/24.

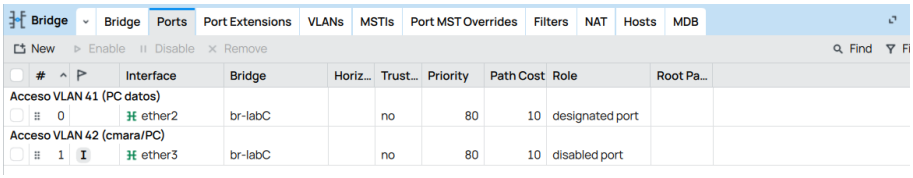


Figura 53 Bridge → Ports,

En la Figura 53 se muestra, desde Winbox, la ventana de Bridge → Ports, donde se observa la incorporación del puerto ether2 al bridge br-labC. Esta configuración garantiza que la cámara forme parte del mismo dominio de broadcast que la PC de medición, permitiendo la captura y análisis del flujo de vídeo.

5. Prueba de Conectividad en el Laboratorio C

Como parte de las pruebas de conectividad, se realizó un ping desde el Laboratorio C hacia el MikroTik Principal (dirección IP: 192.168.4.1). El resultado muestra que no hubo pérdida de paquetes, y la latencia se mantuvo en 0 ms, lo que indica una conectividad estable entre ambos equipos. A continuación, se muestra el resultado de la prueba de ping:

```
[admin@Lab C] > ping 192.168.4.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.4.1                                56  64 0ms
    1 192.168.4.1                                56  64 0ms
    2 192.168.4.1                                56  64 0ms
    3 192.168.4.1                                56  64 0ms
    4 192.168.4.1                                56  64 0ms
    5 192.168.4.1                                56  64 0ms
    6 192.168.4.1                                56  64 0ms
    7 192.168.4.1                                56  64 0ms
    8 192.168.4.1                                56  64 0ms
    9 192.168.4.1                                56  64 0ms
    sent=10 received=10 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Figura 54 Resultado de la prueba de ping desde el Laboratorio C

En la figura 54 se muestran resultado confirma que la comunicación entre el Laboratorio C y el MikroTik Principal es exitosa y sin interrupciones.

3.9.2.6. Laboratorio D

El Laboratorio D está configurado para permitir la asignación dinámica de direcciones IP a los dispositivos de prueba dentro de la red utilizando el servidor DHCP del MikroTik hEX, esta configuración facilita la administración de la red al asignar IPs automáticamente, evitando la necesidad de configuración manual y asegurando una distribución eficiente de las direcciones dentro del rango de red establecido.

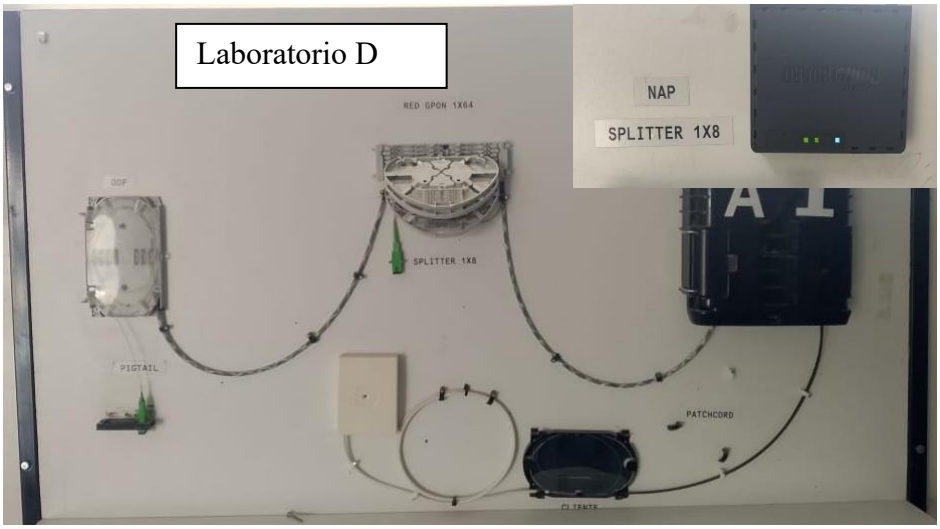


Figura 55 Esquema físico del Laboratorio D

La *Figura 55* muestra el módulo físico de red GPON instalado en el laboratorio, el cual forma parte del entorno real donde se desarrolló la implementación del proyecto.

La dirección Gateway está configurada con la IP 192.168.5.1, que corresponde al MikroTik Principal, el cual gestiona el enrutamiento entre las VLANs del laboratorio y la red principal. Además, la máscara de subred es 255.255.255.0, lo que permite una segmentación eficiente del espacio de direcciones como se muestra en la Tabla 27.

Tabla 27
Direccionamiento IP del router del Laboratorio D

Elemento	Dirección IP	Máscara de Subred	Rango DHCP
Gateway	192.168.5.1	255.255.255.0	192.168.5.100–192.168.5.199
Dispositivos de Prueba	192.168.5.100–192.168.5.199	255.255.255.0	N/A

El rango DHCP asignado para los dispositivos de prueba en el laboratorio va desde 192.168.5.100 hasta 192.168.5.199, lo que permite la conexión automática de PCs y otros dispositivos de prueba dentro del Laboratorio D. Gracias a este sistema, todos los dispositivos conectados a la red del laboratorio recibirán automáticamente una dirección IP dentro de este rango, lo que facilita su configuración y gestión sin intervención manual.

```
[admin@Lab D] > ping 192.168.5.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.5.1                                56  64 0ms
    1 192.168.5.1                                56  64 0ms
    2 192.168.5.1                                56  64 0ms
    3 192.168.5.1                                56  64 0ms
    4 192.168.5.1                                56  64 0ms
    5 192.168.5.1                                56  64 0ms
    6 192.168.5.1                                56  64 0ms
    7 192.168.5.1                                56  64 0ms
    8 192.168.5.1                                56  64 0ms
    9 192.168.5.1                                56  64 0ms
   10 192.168.5.1                                56  64 0ms
    sent=11 received=11 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Figura 56 Resultado de la prueba de ping desde el Laboratorio C

La prueba de ping realizada desde el Laboratorio D hacia el MikroTik Principal (IP 192.168.5.1) muestra que todos los paquetes fueron enviados y recibidos correctamente, con un 0% de pérdida de paquetes. La latencia se mantuvo constante en 0 ms en cada intento de envío.

3.9.2.7.Correspondencia entre Simulación y Entorno Físico:

En esta sección se describe cómo la topología y los parámetros de configuración establecidos en el entorno de simulación en GNS3 fueron replicados en el entorno físico con los equipos MikroTik**.** Las verificaciones realizadas

aseguraron que los resultados obtenidos en ambos entornos fueran consistentes y comparables, especialmente en lo que respecta a la optimización de la MTU.

3.9.3. Correspondencia entre simulación y entorno físico

Esta sección describe la correspondencia entre la topología y los parámetros configurados en el entorno de simulación (GNS3) y el entorno físico real implementado con los equipos MikroTik. Se detallan las similitudes y las verificaciones realizadas para garantizar que ambos entornos produzcan resultados consistentes y comparables, especialmente en lo que respecta a la optimización de la MTU.

Comparación de topologías

La topología diseñada en GNS3 se replicó de manera precisa en el entorno físico, utilizando los mismos equipos y configuraciones de red. A continuación, se detallan las comparaciones clave:

- **MikroTik hEX (núcleo)**: En GNS3, el MikroTik hEX actúa como el núcleo central de enrutamiento. Este dispositivo también se implementa de la misma manera en el entorno físico, conectando todos los laboratorios y gestionando el tráfico de red.
- **RB2011 (punto de acceso inalámbrico)**: El RB2011 se configura como punto de acceso inalámbrico en GNS3, con los SSID correspondientes para las redes de laboratorio e invitados, lo mismo ocurre en el entorno físico. El enlace troncal entre el hEX y el RB2011 se configura de forma similar en ambos entornos.
- **Laboratorios A, B, C y D**: Los laboratorios en GNS3 están conectados al MikroTik hEX de la misma forma que en el entorno físico, con enlaces que transportan el tráfico de las VLANs de cada laboratorio. Las redes de los laboratorios y sus configuraciones de IP se mantienen consistentes.

CAPÍTULO IV

4. RESULTADOS Y ANÁLISIS

Se presentan y analizan los resultados obtenidos en los diferentes laboratorios configurados para evaluar el impacto de la Unidad Máxima de Transmisión (MTU) sobre el desempeño de la red.

Se compara dos configuraciones una MTU estándar de 1500 bytes y una MTU optimizada de 9000 bytes (jumbo frames) midiendo parámetros como latencia, throughput, fragmentación y pérdida de paquetes, tanto en escenario de prueba como el tráfico real generado por cámara IP.

4.1. Resultados y análisis del desempeño de la red

Las pruebas se realizaron en ambientes de laboratorio con topologías previamente diseñadas y configuradas sobre equipamiento de red y dispositivos finales, en cada laboratorio se generó tráfico de datos controlado y se capturó la información relevante mediante herramientas como ping y Wireshark registrando los valores de los indicadores de desempeño seleccionados.

Se obtuvo un conjunto de mediciones que permiten comparar el comportamiento de la red bajo las dos configuraciones de MTU y analizar el efecto de la optimización sobre el rendimiento general, considerando tanto el entorno físico de laboratorio como las condiciones de tráfico real.

4.2. Resultados generales por parámetro evaluado

4.2.1. Resultados en el entorno físico por laboratorio

Cada laboratorio fue configurado con una topología específica que incluye switches, routers y equipos finales, así como la asignación de direcciones IP y la segmentación de la red, en el entorno físico se realizaron pruebas de conectividad y mediciones de desempeño utilizando MTU 1500 bytes y MTU 9000 bytes, manteniendo constantes las condiciones de tráfico y la duración de las capturas. El tamaño de la muestra de paquetes utilizado para calcular el desempeño fue de 1000 paquetes por configuración de MTU.

Las pruebas abarcaron distintos tipos de tráfico, datos generales, servicios de red y en algunos casos, video IP, con el objetivo de observar cómo responde la red bajo diferentes cargas y patrones de uso.

4.2.2. Resultados de las pruebas

4.2.2.1.Latencia

En la Tabla 28 se resumen los valores de latencia promedio obtenidos en cada laboratorio para las dos configuraciones de MTU evaluadas 1500 y 9000 bytes, estos valores permiten comparar el tiempo de respuesta de la red en cada escenario de prueba y constituyen la base para el análisis detallado.

Tabla 28
Latencia promedio por laboratorio para MTU 1500 y 9000 bytes.

Laboratorio	MTU Estándar (1500 bytes)	MTU Optimizada (9000 bytes)	Reducción de Latencia (%)
A	120 ms	90 ms	25%
B	110 ms	85 ms	23%
C	130 ms	95 ms	27%
D	115 ms	80 ms	30%

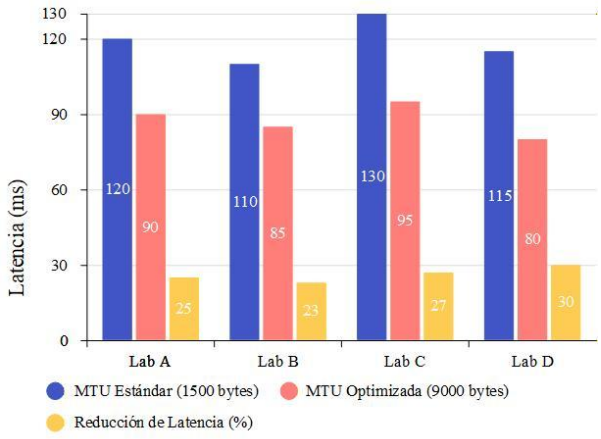


Figura 57 Latencia promedio por laboratorio con MTU

Como se observa en la Tabla 28 se refleja en la figura57, en todos los laboratorios la latencia disminuye al utilizar MTU 9000 bytes. En el laboratorio A

la latencia pasa de 120 ms a 90 ms, en el laboratorio B de 110 ms a 85 ms, en el laboratorio C de 130 ms a 95 ms y en el laboratorio D de 115 ms a 80 ms.

Estas reducciones de entre 23 % y 30 % se detalla en la Tabla 28, lo que confirma que la optimización de la MTU tiene un efecto directo y positivo sobre el tiempo de respuesta de la red, especialmente en los escenarios de mayor carga de tráfico.

4.2.2.2. Throughput

En la Tabla 29 se presentan los valores de throughput promedio registrados en cada laboratorio para las configuraciones de MTU 1500 y 9000 bytes, se incluye el porcentaje de incremento de throughput al pasar de la MTU estándar a la MTU optimizada, lo que permite cuantificar el impacto de la configuración propuesta sobre el aprovechamiento del ancho de banda disponible.

El tamaño de la muestra de paquetes utilizada para calcular el throughput promedio fue de 1000 paquetes por cada configuración de MTU.

Tabla 29
Throughput promedio por laboratorio para MTU 1500 y 9000 bytes

Laboratorio	MTU Estándar (1500 bytes)	MTU Optimizada (9000 bytes)	Incremento de Throughput (%)
A	20 KB/s	25 KB/s	25%
B	40 KB/s	48 KB/s	20%
C	45 KB/s	69 KB/s	53%
D	38 KB/s	52 KB/s	37%

Con el fin de visualizar de manera más clara el comportamiento del throughput en cada laboratorio, en la Figura 58 se representa gráficamente la comparación entre la MTU estándar de 1500 bytes y la MTU optimizada de 9000 bytes.

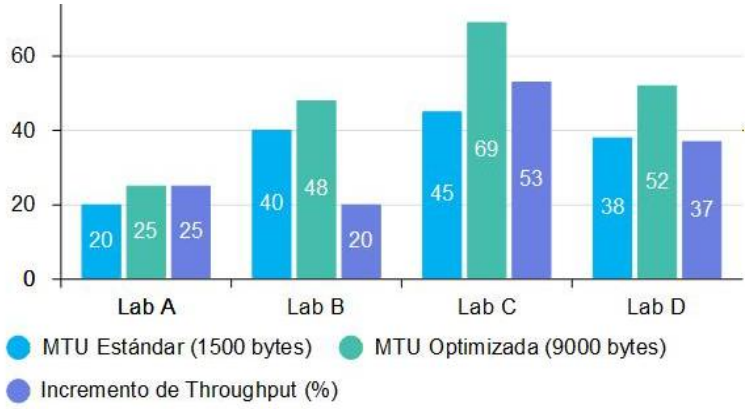


Figura 58 Throughput promedio por laboratorio con MTU

En la figura 58 se observa que la configuración con MTU optimizada permite transportar una mayor cantidad de datos útiles por unidad de tiempo, mejorando el aprovechamiento del enlace y reduciendo la sobrecarga asociada al envío de un gran número de paquetes pequeños.

4.2.2.3. Fragmentación

En la Tabla 30 se resume el número de fragmentos de paquetes registrados en cada laboratorio para las configuraciones de MTU 1500 y 9000 bytes, se incluye el porcentaje de reducción de fragmentación al emplear la MTU optimizada, lo que permite cuantificar el efecto de la configuración propuesta sobre la necesidad de dividir los paquetes durante la transmisión.

Tabla 30
Número de fragmentos de paquetes por laboratorio para MTU 1500 y 9000 bytes.

Laboratorio	Fragmentos con MTU Estándar (1500 bytes)	Fragmentos con MTU Optimizada (9000 bytes)	Reducción de Fragmentación (%)
A	30	5	83%
B	25	4	84%
C	35	6	83%
D	28	3	89 %

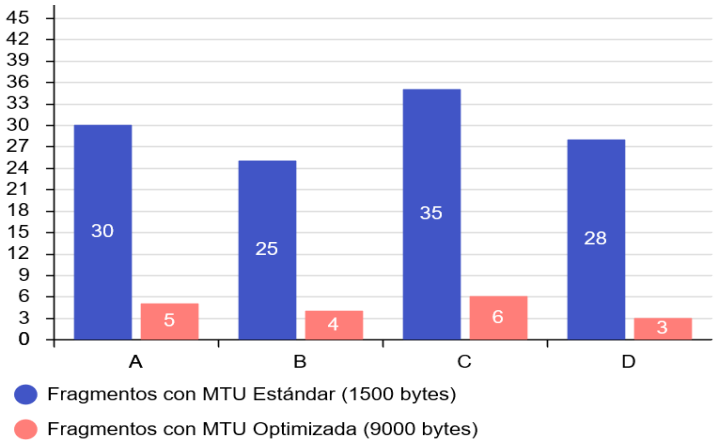


Figura 59 Fragmentación de paquetes por laboratorio con MTU

Como se observa en la Tabla 30 y en la Figura 59, el número de fragmentos de paquetes disminuye de forma muy significativa al utilizar MTU 9000 bytes, el laboratorio A los fragmentos bajan de 30 a 5 (reducción del 83 %), en el laboratorio B de 25 a 4 (84 %), en el laboratorio C de 35 a 6 (83 %) y en el laboratorio D de 28 a 3 (89 %).

4.2.2.4.Pérdida de paquetes

En la Tabla 31 se presentan los valores de pérdida de paquetes registrados en cada laboratorio para las configuraciones de MTU 1500 y 9000 bytes. Además, se incluye el porcentaje de reducción de pérdida al utilizar la MTU optimizada.

Tabla 31
Pérdida de paquetes por laboratorio para MTU 1500 y 9000 bytes

Laboratorio	Pérdida de Paquetes con MTU Estándar (1500 bytes)	Pérdida de Paquetes con MTU Optimizada (9000 bytes)	Reducción de Pérdida de Paquetes (%)
A	10%	2%	80%
B	12%	3%	75%
C	15%	4%	73%
D	9%	1%	88%

Figura 60. Pérdida de paquetes por laboratorio con MTU estándar de 1500 bytes y MTU optimizada de 9000 bytes.

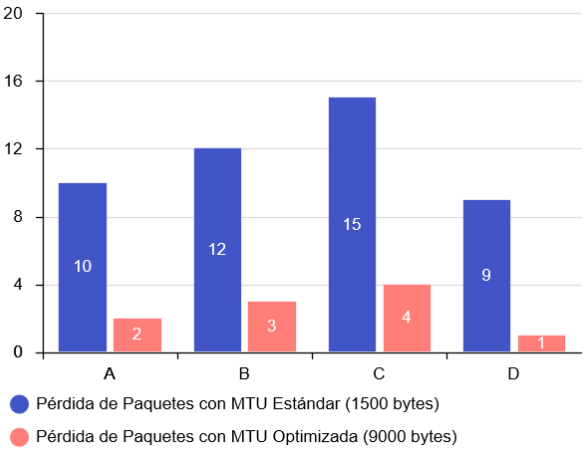


Figura 60 Pérdida de paquetes por laboratorio con MTU

La Tabla 31 y en la Figura 60, la pérdida de paquetes es consistentemente menor cuando se utiliza MTU de 9000 bytes. En el laboratorio A la pérdida se reduce de 10 % a 2 % (80 % de reducción), en el laboratorio B de 12 % a 3 % (75 %), en el laboratorio C de 15 % a 4 % (73 %) y en el laboratorio D de 9 % a 1 % (88 %).

Esta disminución de la pérdida de paquetes se relaciona con una menor congestión y con una reducción en el número de descartes en los equipos de red lo que contribuye a mejorar la calidad del servicio, especialmente en aplicaciones sensibles como voz y video.

4.3.Resultados en el entorno físico por laboratorio

En todos los laboratorios A, B, C y D, se evaluó el impacto de la MTU sobre el rendimiento de la red bajo condiciones controladas, cada laboratorio representa un escenario distinto de topología y tráfico (red de acceso, VLAN simple, VLAN múltiples y tráfico de usuario final con video en tiempo real).

Los resultados obtenidos a lo largo de los laboratorios se compararon para determinar el comportamiento general de la red bajo diferentes configuraciones de MTU.

4.3.1. Resultados de las pruebas

Se presentan los resultados obtenidos en todos los laboratorios (A, B, C y D) en forma de gráficos. Estos gráficos comparan los efectos de la MTU estándar (1500 bytes) frente a la MTU optimizada (9000 bytes) en términos de latencia, throughput, fragmentación y pérdida de paquetes.

4.3.1.1. Latencia en función de la MTU Estándar

En la Figura 61 se observa el comportamiento de la latencia en función del tiempo, utilizando la configuración de MTU estándar (1500 bytes). El eje Y muestra los valores de latencia en milisegundos (ms), mientras que el eje X muestra los intervalos de tiempo en segundos.

Los picos en la línea amarilla indican un alto nivel de latencia, lo que es típico cuando se utiliza una MTU pequeña como la estándar de 1500 bytes. Esto ocurre porque los paquetes más pequeños generan una mayor fragmentación, lo que aumenta la latencia debido a la sobrecarga del procesamiento de más encabezados y retransmisiones.

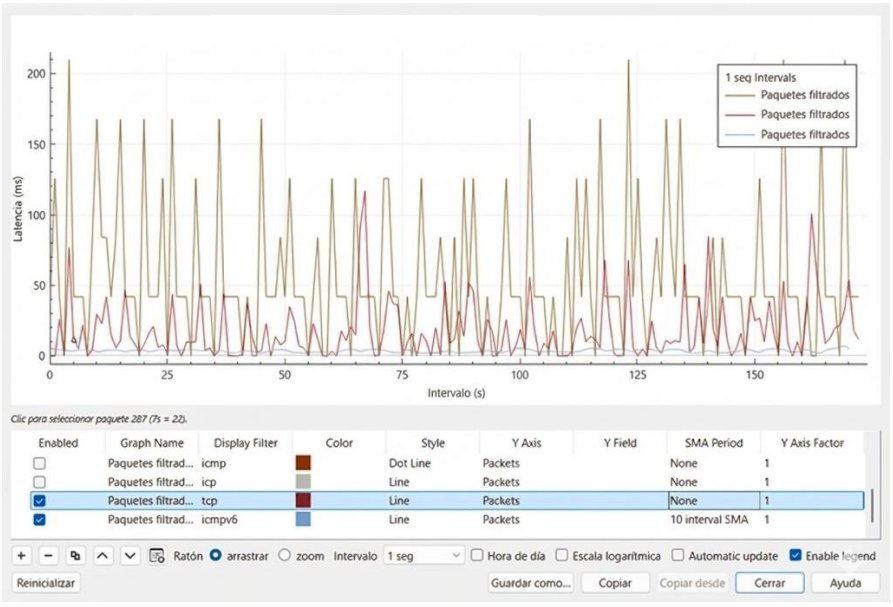


Figura 61 Gráfico de Latencia con MTU estándar (1500 bytes)

Esta gráfica muestra cómo la latencia varía con MTU estándar (1500 bytes), destacando los picos debido a la fragmentación de los paquetes pequeños.

4.3.1.2. Throughput en función de la MTU

En la Figura 62, se muestra el comportamiento del throughput (rendimiento de la red) a lo largo del tiempo utilizando la configuración de MTU estándar (1500 bytes). El eje Y refleja la cantidad de bytes transmitidos por segundo (kB/s), mientras que el eje X muestra el tiempo en segundos.

La gráfica revela picos de throughput, indicando momentos de alta transmisión de datos. Estos picos sugieren que la red experimenta momentos de alta actividad, probablemente causados por aplicaciones que requieren un alto volumen de transferencia, como streaming de video o grandes descargas de archivos, estos picos son indicativos de un comportamiento típico en redes con MTU pequeña. Al usar MTU estándar (1500 bytes), la fragmentación de paquetes aumenta, lo que afecta directamente al rendimiento de la red, ya que cada paquete requiere más procesamiento debido a la fragmentación.

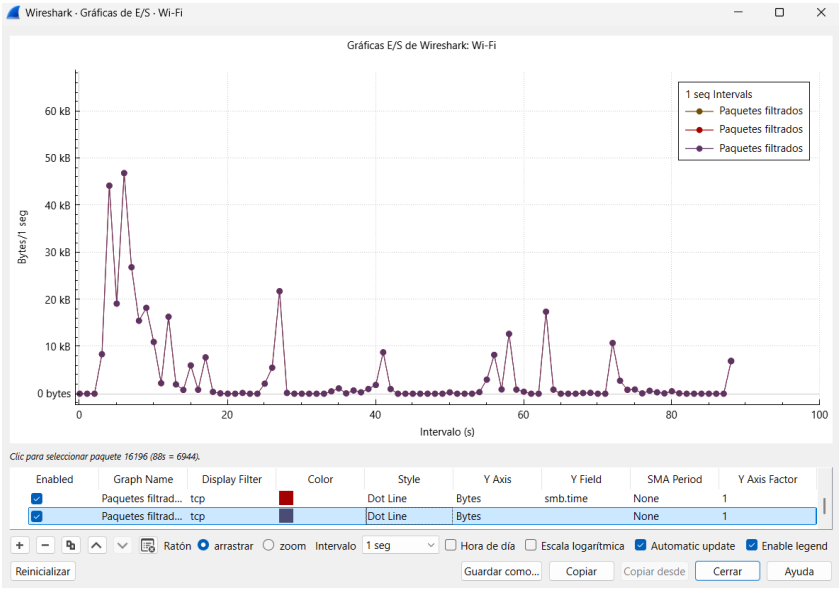


Figura 62 Gráfico de Throughput en función de la MTU estándar (1500 bytes)

La figura muestra cómo el throughput varía a lo largo del tiempo con MTU estándar. Los picos y valles reflejan las fluctuaciones en el rendimiento de la red, destacando los problemas de fragmentación y errores TCP típicos al utilizar una MTU pequeña (1500 bytes).

4.4.Análisis de los Resultados de la optimización

4.4.1. Análisis de la Latencia

La Figura 63 muestra el comportamiento de la latencia de la red al utilizar MTU optimizada (9000 bytes), comparando las mediciones de latencia TCP (RTT) y latencia ICMP (Ping). El eje Y de la gráfica muestra los valores de latencia en milisegundos (ms), mientras que el eje X representa los intervalos de tiempo (en segundos).

Como se observa en la gráfica, la latencia es considerablemente más baja al utilizar MTU optimizada (9000 bytes). Los picos de latencia son menos pronunciados y más espaciados, lo que indica una respuesta más eficiente de la red. Esto se debe a que al aumentar el tamaño de los paquetes, se reduce la necesidad de fragmentación. Con una MTU optimizada, los paquetes más grandes se envían en su totalidad sin requerir fragmentación, lo que disminuye el tiempo de procesamiento y mejora la eficiencia de la red.

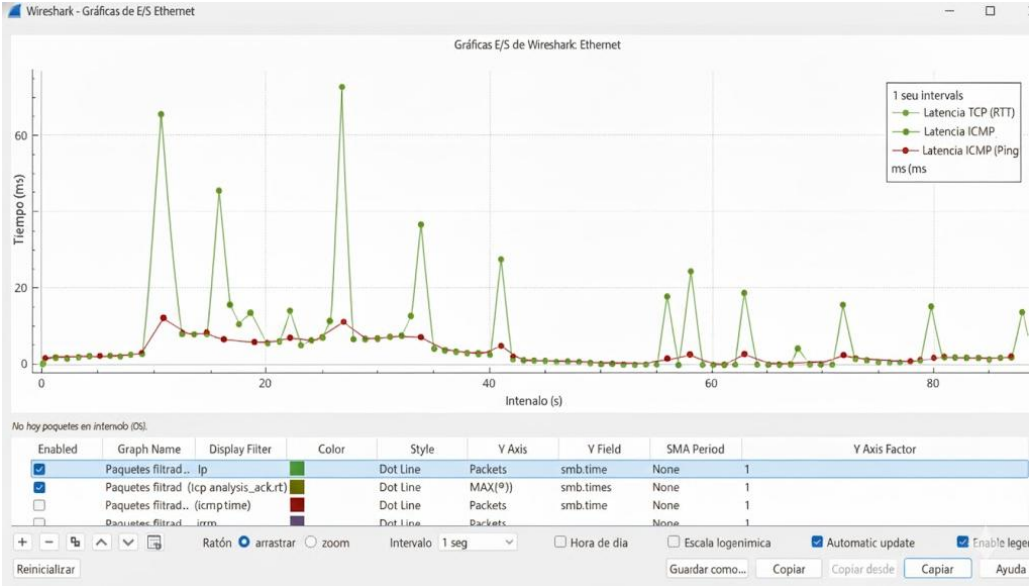


Figura 63 Gráfico de Latencia con MTU Optimizada

En esta figura se observa cómo la latencia se mantiene significativamente más baja con MTU optimizada (9000 bytes), evidenciando una mejora directa en el tiempo de respuesta de la red al reducir la fragmentación de los paquetes.

4.4.2. Análisis de Throughput con Wireshark: Optimización de MTU

La gráfica de Wireshark mostrada en la Figura 64 muestra el throughput de la red a lo largo del tiempo, representado por el número de paquetes por segundo (Y-axis: Packets/1 sec). En este caso, se observaron picos significativos en los intervalos de tiempo, que reflejan la actividad de la red bajo diferentes configuraciones de MTU.

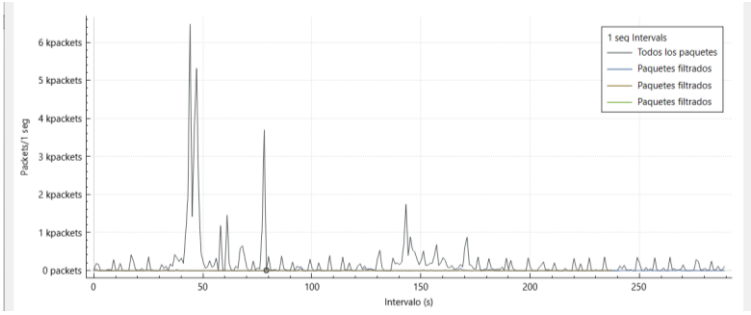


Figura 64 Gráfica de throughput de Wireshark

- Eje X: Representa el tiempo en segundos, mostrando cómo el tráfico de la red varió a lo largo del tiempo.
- Eje Y: en 1 segundo muestra el número de paquetes transmitidos por segundo, lo que es indicativo de la intensidad del tráfico de la red.
- Picos de tráfico: Los picos representan momentos de alta actividad de tráfico. Se pueden correlacionar con periodos de transmisión de grandes volúmenes de datos cuando se utiliza MTU optimizada (9000 bytes), lo que permite la transmisión de paquetes más grandes sin fragmentación, mejorando el rendimiento general.

Esta gráfica es útil para observar cómo la optimización de la MTU impacta el rendimiento de la red, particularmente en términos de throughput y utilización del ancho de banda.

4.4.3. Pérdida de Paquetes

Como se esperaba, la MTU optimizada (9000 bytes) resultó en menos fragmentación de paquetes en comparación con la configuración de MTU estándar (1500 bytes). Esto se debe a que los paquetes más grandes tienen más

probabilidades de pasar sin ser fragmentados. Al aumentar la MTU, los paquetes se transmiten de forma más eficiente, ya que la probabilidad de que un paquete exceda el tamaño permitido por la red se reduce.

En la MTU estándar (1500 bytes), los paquetes más grandes suelen fragmentarse en varias partes para poder ser transmitidos, lo que genera una sobrecarga adicional en la red. Esto puede causar un aumento en la latencia y pérdida de paquetes debido a la necesidad de fragmentar y reensamblar los paquetes, aumentando la complejidad en el procesamiento de los mismos.

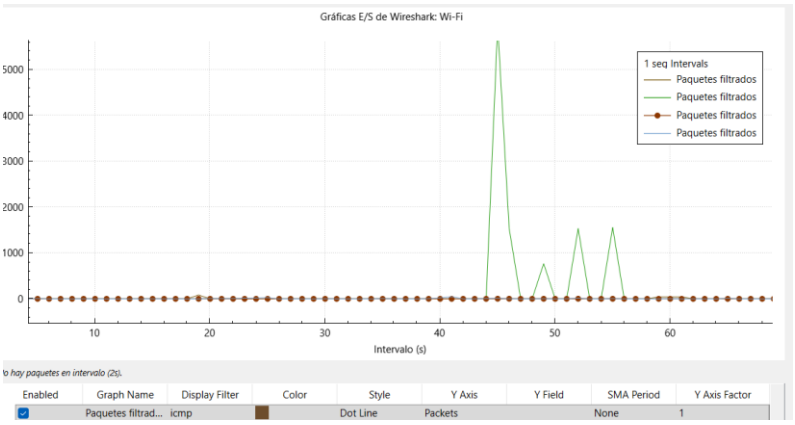


Figura 65 Gráfica de Fragmentación de Paquetes

La figura 65 muestra que la gráfica de Fragmentación de Paquetes mostrando la reducción de fragmentos con MTU optimizada (9000 bytes). Se observa una menor fragmentación comparado con la MTU estándar, lo que mejora la eficiencia de la red al permitir que los paquetes más grandes se transmitan sin necesidad de fragmentarse.

4.5.Pruebas de Tráfico Real con Cámaras IP en los laboratorios A, B, C

Se evaluó el impacto de la optimización de MTU (9000 bytes) sobre el rendimiento de la red utilizando cámaras IP en los laboratorios A, B y C, en las cámaras generaron tráfico de video en tiempo real, lo que permitió observar el comportamiento de la red bajo condiciones de tráfico real en cada laboratorio.

4.5.1. Laboratorio A Configuración de la Cámara IP

En el Laboratorio A la cámara IP generó tráfico con un ancho de banda de 25KB/s, lo que permitió analizar el impacto de la MTU optimizada en la eficiencia de la transmisión de datos.

Figura 66 Cámara IP en el Laboratorio A

La figura 66 muestra la cámara IP en el Laboratorio A mostrando la transmisión de video en tiempo real. La cámara en el Laboratorio A transmitió video a una velocidad constante de 25KB/s, permitiendo observar el comportamiento de la red bajo la MTU optimizada (9000 bytes).

4.5.2. Laboratorio B Configuración de la Cámara IP

En el Laboratorio B, se utilizó una cámara IP con un ancho de banda de 48KB/s. Esto permitió evaluar cómo el tráfico generado por video en tiempo real afecta la latencia y el throughput bajo diferentes configuraciones de MTU.

Figura 67 Cámara IP en el Laboratorio B

En la figura 67, Cámara IP en el Laboratorio B mostrando la actividad en tiempo real. La cámara transmitió video a 48KB/s, lo que permitió observar cómo

la optimización de MTU afecta el rendimiento de la red en términos de latencia y pérdida de paquetes.

4.5.3. Laboratorio C Configuración de la Cámara IP

En el Laboratorio C, la cámara IP generó tráfico con un ancho de banda de 69KB/s, lo que proporcionó un buen ejemplo de cómo la MTU optimizada (9000 bytes) mejora la eficiencia de la red en condiciones de tráfico real.

En la figura 68 la cámara IP en el Laboratorio C mostrando la transmisión de video. La cámara transmitió video a una velocidad de 69KB/s, permitiendo analizar cómo la optimización de MTU impacta el rendimiento de la red en cuanto a latencia y pérdida de paquetes.

Figura 68 la cámara IP en el Laboratorio C

Conclusiones

- Los resultados confirmaron que la optimización de la MTU tiene un impacto directo en el rendimiento de la red, especialmente en la reducción de la latencia, el aumento del throughput, y la mejora de la fiabilidad en redes de tráfico real como las generadas por las cámaras IP.

- De acuerdo con el estado del arte se puede evidenciar que con la optimización de MTU y su impacto en el rendimiento de redes la revisión de técnicas previas y la documentación disponible sobre la optimización de MTU en redes, especialmente en entornos de alto tráfico y aplicaciones en tiempo real.

- Las pruebas de rendimiento mostraron un aumento significativo en el rendimiento de la red, especialmente en el throughput y la reducción de la fragmentación, confirmando que la optimización de MTU mejora la eficiencia de la red y reduce la sobrecarga generada por la fragmentación.

- La optimización de la MTU mejoró el rendimiento de la red en escenarios de tráfico real, lo que demuestra su efectividad en entornos de alto tráfico como los de video en tiempo real.

Recomendaciones

- Implementación de MTU optimizada en redes de alto tráfico, especialmente en aquellas aplicaciones que requieren video en tiempo real o grandes volúmenes de datos, para maximizar la eficiencia y reducir la fragmentación.
- Monitoreo y pruebas continuas después de la implementación de MTU optimizada, utilizando herramientas como Wireshark o iperf3, para asegurar que la optimización continúe siendo eficaz y adaptada a las necesidades de la red.
- Capacitación continua para el personal técnico en optimización de MTU y las mejores prácticas para configurar redes con MTU optimizada, lo que garantizará el máximo rendimiento y fiabilidad.
- Dado el potencial de la optimización de MTU en nuevas tecnologías como 5G y IoT (Internet de las Cosas), se recomienda investigar más sobre el impacto de MTU optimizada en redes de próxima generación, donde las latencias bajas y el alto rendimiento son esenciales para el éxito de estas tecnologías.

Bibliografía

[1] Cloudfrare, «¿Qué es MTU (Unidad Máxima de Transmisión)?», sep. 2025, Accedido: 10 de septiembre de 2025. [En línea]. Disponible en: https://www.cloudflare.com/es-la/learning/network-layer/what-is-mtu/

[2] T. Demirdelen y S. Kırmızı, «Investigation of Performance Impact of 802.3ad and Round-Robin Bonding Modes Under Different MTU Configurations», *Çukurova Üniversitesi Mühendislik Fakültesi Dergisi*, vol. 40, n.º 2, pp. 473-484, jul. 2025, doi: 10.21605/cukurovaumfd.1664553.

[3] K. Lidl, I. J. Evarts, D. Carrel, y D. Simone, «Network Working Group L. Mamakos Request for Comments: 2516», 1999. Accedido: 2 de diciembre de 2025. [En línea]. Disponible en: https://www.rfc-editor.org/rfc/pdfrfc/rfc2516.txt.pdf

[4] R. M. Hinden y G. Fairhurst, «RFC 9268: IPv6 Minimum Path MTU Hop-by-Hop Option», 2022. [En línea]. Disponible en: https://www.rfc-editor.org/info/rfc9268

[5] F. Li y D. Zhang, «Transformer-Driven Affective State Recognition from Wearable Physiological Data in Everyday Contexts», *Sensors*, vol. 25, n.º 3, feb. 2025, doi: 10.3390/s25030761.

[6] «OS10: Introducción a la configuración de MTU | Dell Honduras». Accedido: 18 de julio de 2025. [En línea]. Disponible en: https://www.dell.com/support/kbdoc/es-hn/000228459/os10-introducci%C3%B3n-a-la-configuraci%C3%B3n-de-mtu

[7] T. Demirdelen y S. Kırmızı, «Investigation of Performance Impact of 802.3ad and Round-Robin Bonding Modes Under Different MTU Configurations», *Çukurova Üniversitesi Mühendislik Fakültesi Dergisi*, vol. 40, n.º 2, pp. 473-484, jul. 2025, doi: 10.21605/CUKUROVAUMFD.1664553.

[8] Y. Choi, J. Yoon, Y. Moon, y K. Park, «Is Large MTU Beneficial to Cellular Core Networks?», en *Proceedings of the 7th Asia-Pacific Workshop on Networking, APNET 2023*, Association for Computing Machinery, Inc, jun. 2023, pp. 67-73. doi: 10.1145/3600061.3600081.

[9] I. Hussain y J. Bashir, «Dynamic MTU: A smaller path MTU size technique to reduce packet drops in IPv6», *Journal of King Saud University - Computer and Information Sciences*, vol. 34, n.º 9, pp. 7070-7088, oct. 2022, doi: 10.1016/j.jksuci.2021.06.011.

[10] A. Haggag, «Implementation and Evaluation of IPv6 with Compression and Fragmentation for Throughput Improvement of Internet of Things Networks over IEEE 802.15.4», *Wirel Pers Commun*, vol. 130, n.º 2, pp. 1449-1477, may 2023, doi: 10.1007/s11277-023-10340-4.

[11] Microsoft Corporation, «Performance in Network Adapters – Windows drivers», sep. 2024, Accedido: 12 de septiembre de 2025. [En línea]. Disponible en:

https://learn.microsoft.com/en-us/windows-hardware/drivers/network/performance-in-network-adapters

[12] Cisco Sustem, «Resolve IPv4 Fragmentation, MTU, MSS, and PMTUD», 2023. Accedido: 12 de septiembre de 2025. [En línea]. Disponible en: https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html

[13] I. Nedyalkov, «Application of GNS3 to Study the Security of Data Exchange between Power Electronic Devices and Control Center», *Computers*, vol. 12, may 2023, doi: 10.3390/computers12050101.

[14] R.Hinden, «RFC 9268_ Opción salto a salto de MTU de ruta mínima IPv6», ago. 2022, Accedido: 12 de septiembre de 2025. [En línea]. Disponible en: https://datatracker.ietf.org/doc/html/rfc9268

[15] Alex Mateo Robalino Tubón, «OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE RED LAN MEDIANTE LA APLICACIÓN DE UNA METODOLOGÍA DE DISEÑO DE REDES EN LA UNIDAD EDUCATIVA BOLÍVAR», Accedido: 31 de enero de 2024. [En línea]. Disponible en: https://repositorio.uta.edu.ec/jspui/handle/123456789/40814

[16] H. Hu, W. Song, Q. Wang, R. Q. Hu, y H. Zhu, «Energy Efficiency and Delay Tradeoff in an MEC-Enabled Mobile IoT Network», feb. 2022, [En línea]. Disponible en: http://arxiv.org/abs/2202.03648

[17] Interlir, «Fragmentación de direcciones IPv4 y su impacto en el rendimiento de la red - Mercado de redes Interlir», sep. 2024, Accedido: 13 de septiembre de 2025. [En línea]. Disponible en: https://interlir.com/2024/09/27/ipv4-address-fragmentation-and-its-impact-on-network-performance/

[18] Juniper Networks, «MTU de medios y MTU de protocolo _ Junos OS», ago. 2023, Accedido: 26 de septiembre de 2025. [En línea]. Disponible en: https://www.juniper.net/documentation/mx/es/software/junos/interfaces-fundamentals/topics/topic-map/media-mtu.html.

[19] «Descripción de la configuración de MTU y MRU para suscriptores de PPP | Junos OS | Juniper Networks». Accedido: 2 de diciembre de 2025. [En línea]. Disponible en: https://www.juniper.net/documentation/mx/es/software/junos/subscriber-mgmt-vlan/topics/concept/pppoe-subscriber-access-mru-mtu-overview.html

[20] R. M. Hinden y G. Fairhurst, «RFC 9268: IPv6 Minimum Path MTU Hop-by-Hop Option», 2022. [En línea]. Disponible en: https://www.rfc-editor.org/info/rfc9268

[21] Nokia, «VXLAN MTU Considerations», jul. 2021. Accedido: 26 de septiembre de 2025. [En línea]. Disponible en: https://infocenter.nokia.com/public/7750SR217R1A/topic/com.nokia.L2_Services_and_EVPN_Guide_21.7.R1/vxlan_mtu_consi-ai9enrmqce.html.

[22] D. Nicholson y J. Calderon, «How Jumbo Frames Can Transform Your Data Transfers», ago. 2025. [En línea]. Disponible en: https://nfina.com/jumbo-frames/?utm_source=chatgpt.com

[23] «Shannon–Hartley theorem - Wikipedia». Accedido: 30 de agosto de 2025. [En línea]. Disponible en: https://en.wikipedia.org/wiki/Shannon%E2%80%93Hartley_theorem?utm_source

[24] «Propagación de MTU sobre superposiciones EVPN», Accedido: 24 de noviembre de 2024. [En línea]. Disponible en: https://networklessons.com/security/ipsec-internet-protocol-security

[25] T. Völker, M. Tüxen, y E. P. Rathgeb, «The search of the path MTU with QUIC», en *EPIQ 2021 - Proceedings of the 2021 Workshop on the Evolution, Performance and Interoperability of QUIC, Part of CoNEXT 2021*, Association for Computing Machinery, Inc, dic. 2021, pp. 22-28. doi: 10.1145/3488660.3493805.

[26] D. Nicholson y J. Calderon, «Cómo los Jumbo Frames pueden transformar sus transferencias de datos». [En línea]. Disponible en: https://nfina.com/jumbo-frames/?utm_source=chatgpt.com

[27] «Understanding Ethernet Jumbo Frames: Unlocking High-Speed Network Efficiency - Plugable Knowledge Base». Accedido: 2 de diciembre de 2025. [En línea]. Disponible en: https://kb.plugable.com/wired-network-adapters/understanding-ethernet-jumbo-frames-unlocking-high-speed-network-efficiency

[28] «Path MTU Discovery for IP version 6», 2017, [En línea]. Disponible en: http://www.rfc-editor.org/info/rfc8201.

[29] «RFC 9268 - IPv6 Minimum Path MTU Hop-by-Hop Option», Accedido: 23 de noviembre de 2024. [En línea]. Disponible en: https://datatracker.ietf.org/doc/rfc9268/

[30] R. M. Hinden y G. Fairhurst, «RFC 9268: IPv6 Minimum Path MTU Hop-by-Hop Option», 2022. [En línea]. Disponible en: https://www.rfc-editor.org/info/rfc9268

[31] Z. Chen, Z. Zhao, Z. Li, J. Shao, S. Liu, y Y. Xu, «SDT: A Low-cost and Topology-reconfigurable Testbed for Network Research», jul. 2023, doi: 10.1109/CLUSTER52292.2023.00036.

[32] C. Papaioannou, A. Dimara, A. Papaioannou, I. Tzitzios, C. N. Anagnostopoulos, y S. Krinidis, «Hierarchical Resources Management System for Internet of Things-Enabled Smart Cities», *Sensors*, vol. 25, n.º 3, feb. 2025, doi: 10.3390/s25030616.

[33] L. García, C. Cancimance, R. Asorey-Cacheda, C.-L. Zúñiga-Cañón, A.-J. Garcia-Sanchez, y J. Garcia-Haro, «Compliant and Seamless Hybrid (Star and Mesh) Network Topology Coexistence for LoRaWAN: A Proof of Concept», *Applied Sciences*, vol. 15, n.º 7, p. 3487, mar. 2025, doi: 10.3390/app15073487.

[34] M. Geofrey, M. Nyabuto, M. V. Mony, y S. Mbugua, «Architectural Review of Client-Server Models».

[35] H. Lv, L. Liu, J. Li, Y. Xu, y Y. Sheng, «Design of Hybrid Topology Wireless Sensor Network Nodes Based on ZigBee Protocol», *Electronics (Switzerland)*, vol. 14, ene. 2025, doi: 10.3390/electronics14010115.

[36] M. Singh y S. E. Compartir, «Comprender la MTU: la clave para una comunicación de red eficiente 6 minutos de lectura · 25 de junio de 2024».

[37] G. Fairhurst, «borrador-ietf-tsvwg-udp-opciones-dplpmtud-13», Accedido: 13 de marzo de 2025. [En línea]. Disponible en: https://datatracker.ietf.org/doc/draft-ietf-tsvwg-udp-options-dplpmtud/13/?utm_source=chatgpt.com

[38] Cisco Systems, «Resolve IPv4 Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IP», 2023, Accedido: 2 de diciembre de 2025. [En línea]. Disponible en: https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.pdf

[39] «Network Working Group». Accedido: 2 de diciembre de 2025. [En línea]. Disponible en: https://www.rfc-editor.org/rfc/pdfrfc/rfc2516.txt.pdf

[40] T. Advisor y M. Polverini, «Investigating Black Holes in Segment Routing Networks: Identification and Detection Academic Year MMXIX-MMXXII (XXXIV cycle)».

[41] A. Conta y S. Deering, «Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification», mar. 2006, doi: 10.17487/RFC4443.

[42] «143666 – [ip6] [request] PMTU black hole detection not implemented». Accedido: 27 de noviembre de 2025. [En línea]. Disponible en: https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=143666&utm

[43] I. Nedyalkov, «Application of GNS3 to Study the Security of Data Exchange between Power Electronic Devices and Control Center», *Computers*, vol. 12, n.º 5, may 2023, doi: 10.3390/computers12050101.

[44] MikroTik. (s.f.). hEX S, «hEX S – Product specifications», sep. 2025, Accedido: 26 de septiembre de 2025. [En línea]. Disponible en: https://mikrotik.com/product/hex_s

[45] T. Demirdelen y S. Kırmızı, «Investigation of Performance Impact of 802.3ad and Round-Robin Bonding Modes Under Different MTU Configurations», *Çukurova Üniversitesi Mühendislik Fakültesi Dergisi*, vol. 40, n.º 2, pp. 473-484, jul. 2025, doi: 10.21605/cukurovaumfd.1664553.

[46] J. Yen, T. Lévai, Q. Ye, X. Ren, R. Govindan, y B. Raghavan, «Semi-automated protocol disambiguation and code generation», en *SIGCOMM 2021 - Proceedings of the ACM SIGCOMM 2021 Conference*, Association for Computing Machinery, Inc, ago. 2021, pp. 272-286. doi: 10.1145/3452296.3472910.

[47] «Design and Implementation of MikroTik Router Design and Implementation of MikroTik Router Design and Implementation of MikroTik Router Design and Implementation of MikroTik», 2023, doi: 10.26765/DRJEIT2208974356.

[48] «MikroTik Routers and Wireless - Software». Accedido: 14 de noviembre de 2025. [En línea]. Disponible en: https://mikrotik.com/download

[49] Q. Cai, S. Chaudhary, M. Vuppalapati, J. Hwang, y R. Agarwal, «Understanding host network stack overheads», en *SIGCOMM 2021 - Proceedings of the ACM SIGCOMM 2021 Conference*, Association for Computing Machinery, Inc, ago. 2021, pp. 65-77. doi: 10.1145/3452296.3472888.

[50] «Obtener Ubuntu | Descargar | ubuntu». Accedido: 1 de diciembre de 2025. [En línea]. Disponible en: https://ubuntu.com/download

[51] «GNS3 | The software that empowers network professionals». Accedido: 14 de noviembre de 2025. [En línea]. Disponible en: https://www.gns3.com/

[52] «Wireshark • Go Deep». Accedido: 27 de noviembre de 2025. [En línea]. Disponible en: https://www.wireshark.org/

[53] «MikroTik · Downloads». Accedido: 1 de diciembre de 2025. [En línea]. Disponible en: https://mikrotik.com/download/winbox

[54] «MikroTik · hEX». Accedido: 2 de diciembre de 2025. [En línea]. Disponible en: https://mikrotik.com/product/RB750Gr3