UNIVERSIDAD ESTATAL

PENÍNSULA DE SANTA ELENA

FACSISTEL

INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

Implementación de una arquitectura dinámica con enrutamiento OSPF y seguridad perimetral para la gestión de infraestructura crítica.

Tomalá Pozo Gabriela Aracely

Dirigido por:

Ing. Luis Miguel Amaya Fariño, Mgtr.

LA LIBERTAD 2026

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. Ronald Rovira Jurado, Ph.D.
DIRECTOR DE LA CARRERA

Ing. Luis Amaya Fariño, Mgtr.
TUTOR

Ing. Fernando Chamba, Mgtr.
DOCENTE ESPECIALISTA

Ing. Corina Gonzabay De La A, Mgtr.
SECRETARIA

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 la cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **Tomalá Pozo Gabriela Aracely**, como requerimiento para la obtención del título de Ingeniero en telecomunicaciones.

La Libertad, a los 04 días del mes de agosto del año 2026

TUTOR

Ing. Luis Miguel Amaya Fariño, Mgtr.

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Tomalá Pozo Gabriela Aracely**

DECLARO QUE:

El trabajo de Titulación, **Implementación de una Arquitectura de Red Dinámica con Enrutamiento OSPF y Seguridad Perimetral para la Gestión de Infraestructura Crítica** de un 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 04 días del mes de agosto del año 2026

EL AUTOR

Gabriela Tomalá

Tomalá Pozo Gabriela Aracely
C.I 2450298308

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Tomalá Pozo Gabriela Aracely**

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 04 días del mes de agosto del año 2026

EL AUTOR

Gabriela Aracely

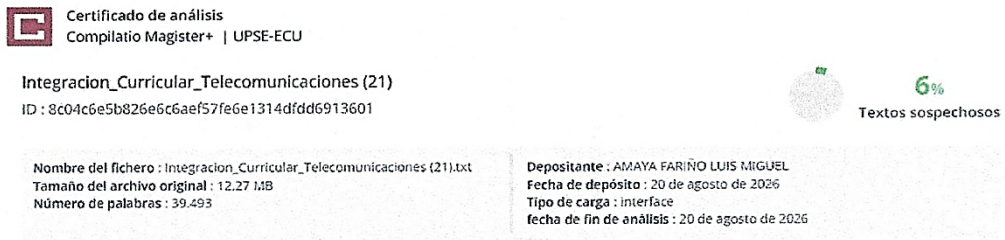
Tomalá Pozo Gabriela Aracely
CI. 245028308

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **Implementación de una arquitectura de red dinámica con enrutamiento OSPF y seguridad perimetral para la gestión de infraestructura crítica**, presentado por la estudiante Tomalá Pozo Gabriela Aracely, fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 06% por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Certificado de análisis
Compilatio Magister+ | UPSE-ECU

Integracion_Curricular_Telecomunicaciones (21)
ID : 8c04c6e5b826e6c6aef57fe6e1314dfdd6913601

6%
Textos sospechosos

Nombre del fichero : Integracion_Curricular_Telecomunicaciones (21).txt
Tamaño del archivo original : 12.27 MB
Número de palabras : 39.493

Depositante : AMAYA FARIÑO LUIS MIGUEL
Fecha de depósito : 20 de agosto de 2026
Tipo de carga : interface
fecha de fin de análisis : 20 de agosto de 2026

TUTOR

Ing. Luis Miguel Amaya Fariño, Mgtr.

AGRADECIMIENTO

Agradezco a Dios por ser mi guía y mi fortaleza a lo largo de toda esta etapa académica, por darme la sabiduría necesaria para superar cada obstáculo y por permitirme culminar con éxito mi formación profesional.

A mi mamá, Catalina Pozo, y a mi papá, Juan Tomalá, por su apoyo incondicional, por su esfuerzo diario y por creer siempre en mis capacidades, incluso en los momentos en que yo dudaba de ellas.

A mis hermanos Richard, Cristián y María, por su cariño, sus palabras de aliento y por acompañarme de forma incondicional en cada etapa de este proceso.

A mis compañeros y amigos, por su compañía, su apoyo y por hacer de este camino un proceso mucho más llevadero, incluso en los momentos de mayor exigencia.

A mi tutor, Mgtr. Luis Amaya Fariño, por su valiosa guía, su paciencia y por compartir generosamente sus conocimientos, los cuales fueron fundamentales para el desarrollo y la culminación de este trabajo de titulación.

Al Ing. Fernando Chamba, especialista de este proyecto, por su tiempo, sus observaciones oportunas y sus aportes técnicos, que enriquecieron significativamente el resultado final de esta investigación.

Gabriela Tomalá Pozo.

DEDICATORIA

A Dios por sostenerme con su fortaleza en cada noche de desvelo, por ser la luz que guio mi camino cuando todo parecía incierto y por ser el aliento que nunca faltó cuando las fuerzas parecían agotarse.

A mi madre, Catalina Pozo, cuyo amor incondicional ha sido el motor silencioso de cada uno de mis logros. Gracias por tus manos siempre dispuestas a sostenerme, por tus palabras de aliento en cada tropiezo y por creer en mí incluso cuando yo misma dudaba; sin tu sacrificio nada de esto sería posible.

A mi padre, Juan Tomalá, por enseñarme con su ejemplo que el esfuerzo constante y el trabajo honesto siempre encuentran su recompensa.

A mis hermanos, Richard, Cristián y María, por ser mi refugio en los días difíciles y mi impulso en los días de duda. Gracias por cada palabra de aliento, por cada muestra de cariño y por caminar junto a mí en cada etapa de este proceso.

A Iván González, por su paciencia infinita, por sostener mi mano en los momentos de cansancio y por creer en mí incluso en las noches en que yo dejaba de creer. Gracias por ser mi calma en medio del caos de este proceso.

Y a ti, Fabián Pozo, que hoy me acompañas desde el cielo, aunque la distancia entre nosotros ya no se mide en kilómetros, tu recuerdo sigue tan presente como el primer día. Cada página de este trabajo lleva un pedazo de tu memoria, y sé que, donde estés, celebras este logro conmigo.

Gabriela Tomalá Pozo.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El Laboratorio de Telecomunicaciones de la Universidad Estatal Península de Santa Elena contaba con una infraestructura de red estática, sin protocolos de enrutamiento dinámico, sin un servicio de asignación automática de direcciones IP y sin mecanismos de seguridad perimetral. Estas limitaciones afectaban tanto su operatividad técnica como su valor formativo.

Ante esta problemática, el proyecto tuvo como objetivo implementar una arquitectura de red dinámica mediante la configuración del protocolo OSPF, el servicio DHCP y mecanismos de seguridad perimetral basados en firewall y listas de control de acceso (ACL) sobre equipos MikroTik. La implementación se realizó mediante un router principal y cinco módulos de red identificados como A, B, C, D y E.

Con un enfoque experimental, el proyecto se desarrolló en cuatro fases: diseño de la arquitectura, simulación en GNS3, implementación física y validación mediante pruebas de conectividad.

Las pruebas de convergencia demostraron que OSPF recalcula automáticamente las rutas ante la caída de un enlace, sin requerir intervención manual. Asimismo, las políticas de firewall y las ACL bloquearon eficazmente el tráfico no autorizado. Se concluye que la integración de estos componentes permitió satisfacer la necesidad de disponer de una red robusta, estable, dinámica y segura.

Palabras clave: OSPF, DHCP, seguridad perimetral, MikroTik, redes dinámicas, ACL, infraestructura de red.

ABSTRACT

The Telecommunications Laboratory at the Universidad Estatal Península de Santa Elena relied on a static network infrastructure that lacked dynamic routing protocols, automatic IP address assignment services, and perimeter security mechanisms. These limitations hindered both its technical operations and its educational value.

To address these issues, the project aimed to implement a dynamic network architecture by configuring the OSPF protocol, DHCP services, and perimeter security mechanisms—specifically firewalls and access control lists (ACLs) using MikroTik equipment. The implementation involved a main router and five network modules designated as A, B, C, D, and E.

Adopting an experimental approach, the project was carried out in four phases: architecture design, simulation in GNS3, physical implementation, and validation through connectivity testing.

Convergence tests demonstrated that OSPF automatically recalculates routes in the event of a link failure, without requiring manual intervention. Additionally, firewall policies and ACLs effectively blocked unauthorized traffic. The study concludes that integrating these components successfully met the need for a robust, stable, dynamic, and secure network.

Keywords: OSPF, DHCP, perimeter security, MikroTik, dynamic networks, ACL, network infrastructure.

INTRODUCCIÓN.

Con el paso de los años, el aumento de equipos y usuarios conectados comenzó a evidenciar que la red ya no respondía a las exigencias del presente: el direccionamiento IP se seguía asignando manualmente a cada equipo y las rutas de comunicación entre dispositivos no contaban con ningún mecanismo que permitiera ajustarse automáticamente ante cambios en la topología. A esto se sumaba la falta de controles de seguridad en el perímetro, un escenario que hacía cada vez más evidente la necesidad de cambiar la arquitectura desde sus bases.

Al revisar la situación, se comprobó que estas limitaciones afectaban tanto el desarrollo de las prácticas académicas como la administración diaria de la red. El primer problema fue la ausencia de un protocolo de enrutamiento dinámico: cualquier modificación en la topología requería intervención manual, con el consiguiente riesgo de errores.

A esto se sumaba la falta de un servicio DHCP, que generaba conflictos de direccionamiento por asignaciones manuales o duplicadas. Tampoco existían mecanismos de seguridad perimetral que filtraran el tráfico entrante y saliente, lo que dejaba al laboratorio vulnerable frente a accesos no autorizados.

Con base en este diagnóstico, se planteó como objetivo general diseñar e implementar una arquitectura de red dinámica que integrara el protocolo OSPF para el enrutamiento dinámico, el servidor DHCP para la asignación automática de direcciones IP y un sistema de seguridad perimetral basado en firewall y ACLs. El proyecto se desarrolló en dos etapas: primero, mediante simulación, para validar la lógica de enrutamiento y las políticas de seguridad sin riesgo; después, implementando la solución en los equipos físicos del laboratorio.

CAPÍTULO I

1.1. Identificación del problema.

Con el paso de los años, el incremento de equipos y usuarios conectados evidenció que la red ya no respondía a las exigencias actuales. El direccionamiento IP continuaba asignándose manualmente a cada equipo y las rutas de comunicación entre los dispositivos no disponían de un mecanismo que permitiera ajustarlas automáticamente ante cambios en la topología de red. A ello se sumaba la ausencia de controles de seguridad perimetral, lo que hacía evidente la necesidad de rediseñar la arquitectura de red desde sus bases.

El análisis de la situación permitió determinar que estas limitaciones afectaban tanto el desarrollo de las prácticas académicas como la administración diaria de la red. El primer problema identificado fue la ausencia de un protocolo de enrutamiento dinámico, ya que cualquier modificación en la topología requería intervención manual y aumentaba el riesgo de errores de configuración.

Además, la falta de un servicio DHCP ocasionaba conflictos de direccionamiento debido a asignaciones manuales incorrectas o duplicadas. Tampoco existían mecanismos de seguridad perimetral que filtraran el tráfico entrante y saliente, lo que dejaba al laboratorio expuesto a accesos no autorizados.

Con base en este diagnóstico, se planteó como objetivo general diseñar e implementar una arquitectura de red dinámica que integrara el protocolo OSPF para el enrutamiento dinámico, el servicio DHCP para la asignación automática de direcciones IP y mecanismos de seguridad perimetral basados en firewall y listas de control de acceso (ACL). El proyecto se desarrolló en dos etapas. En primer lugar, se utilizó una simulación para validar la lógica de enrutamiento y las políticas de seguridad sin comprometer la infraestructura física. Posteriormente, la solución se implementó en los equipos del laboratorio.

1.2. Antecedentes.

El desarrollo de las tecnologías de la información y la comunicación ha transformado la gestión de redes en instituciones educativas a nivel global. En este contexto, Ponce Guerrero (2024) en un artículo publicado en Journal TechInnovation, señala que la seguridad en las redes LAN no se limita a restringir el acceso, sino que también comprende la

protección de los datos y la defensa frente a intrusiones lógicas, como programas maliciosos y ataques de *hackers*. Asimismo, plantea la necesidad de implementar una estrategia integral que contemple medidas de seguridad física, lógica y de infraestructura para garantizar el estado de la red. [1].

A nivel regional, la situación también presenta importantes desafíos. Según Seguridad & Defensa, la incorporación del Internet Industrial de las Cosas (IoT) y la integración de tecnologías digitales en entornos operativos han generado nuevas oportunidades de ataque contra las redes institucionales. Esta situación hace necesario que los espacios académicos dedicados a la formación en telecomunicaciones cuenten con infraestructuras que incorporen y demuestren buenas prácticas de seguridad [2].

En la Universidad Nacional Autónoma de México (UNAM) se implementó un firewall perimetral para caracterizar el comportamiento de una red LAN bajo distintas condiciones de filtrado. Además de controlar el tráfico entrante y saliente, el dispositivo asumió funciones de servidor DHCP para asignar direcciones IP de forma automática a los equipos conectados a la red local [3].

En la Pontificia Universidad Católica del Ecuador (PUCE), se documentó el uso de un firewall perimetral con configuración de interfaces LAN y mecanismos de control de comunicaciones no autorizadas. Este tipo de implementación evidencia la posibilidad de integrar servicios de seguridad y administración de red en un mismo dispositivo, lo cual resulta pertinente para laboratorios e instituciones de educación superior [4].

Desde una perspectiva técnica, el protocolo OSPF se caracteriza por calcular rutas de manera automática mediante el algoritmo SPF (*Shortest Path First*). A diferencia de RIP, OSPF utiliza un modelo de estado de enlace y difunde actualizaciones cuando se producen cambios relevantes en la topología, en lugar de enviar periódicamente la tabla de enrutamiento completa. Esto permite reducir el tráfico de control y optimizar el uso del ancho de banda disponible [5].

Un estudio realizado en la Universidad Católica de Oriente analizó la integración de una red privada virtual (VPN), un firewall y un sistema de detección de intrusiones (IDS). Sus resultados evidenciaron que la combinación de estas herramientas fortalece la seguridad

de las redes institucionales al establecer capas complementarias de defensa frente a accesos no autorizados. Este enfoque de defensa en profundidad constituye un referente para la arquitectura de seguridad propuesta en el presente proyecto [6].

En el ámbito normativo, la protección de infraestructuras críticas de red ha cobrado mayor relevancia institucional; se indica que los estándares como el NERC-CIP, aplicados en varios países latinoamericanos incluyendo Ecuador, establecen controles específicos de seguridad para redes de datos críticas, promoviendo la adopción de modelos de segmentación mediante firewalls perimetrales y controles de acceso como mecanismos de defensa fundamentales frente a amenazas tanto internas como externas [7].

La seguridad en tecnologías de la información también ha sido abordada por estudios sobre protocolos de seguridad informática aplicados en laboratorios de carreras tecnológicas. Estos trabajos identifican que la ausencia de políticas claras de control de acceso y una configuración inadecuada de la red constituyen vulnerabilidades que pueden afectar tanto la disponibilidad de los servicios como la integridad de los equipos [8].

Respecto de la implementación práctica, diversos trabajos confirman la idoneidad de OSPF para redes institucionales de telecomunicaciones. Un proyecto de diseño e implementación de una red WAN basada en OSPF comprobó que este protocolo facilita la adaptación de las rutas ante fallos de enlace y contribuye a una administración más eficiente del enrutamiento. Estas características son especialmente relevantes en entornos donde la continuidad del servicio resulta crítica para las operaciones institucionales [9].

En Ecuador, la Universidad Nacional de Loja identificó limitaciones en sus mecanismos de seguridad y desarrolló una propuesta de mejora para su firewall perimetral. El estudio señala que una estrategia centrada únicamente en el filtrado de puertos y direcciones IP puede resultar insuficiente frente a las amenazas cibernéticas actuales. Por ello, propone una configuración más avanzada, con reglas específicas de control de acceso para gestionar de manera más efectiva el tráfico entrante y saliente de la red institucional [10].

En la Universidad Estatal Península de Santa Elena se realizó un estudio de vulnerabilidades en una red LAN de la provincia de Santa Elena mediante herramientas de

hacking ético. Los resultados evidenciaron que configuraciones incorrectas, controles insuficientes y una gestión inadecuada de la red pueden incrementar la exposición a accesos no autorizados, tanto internos como externos [11].

Finalmente, Fortinet destaca que las soluciones modernas de seguridad de red contemplan simultáneamente el control de accesos mediante firewalls y ACLs, la gestión dinámica del tráfico y la identificación de activos tecnológicos como componentes interdependientes de una arquitectura segura y eficiente [12]. Ese enfoque integrado es precisamente el que sustenta la propuesta del presente trabajo de titulación.

1.3. Descripción del proyecto.

El proyecto consiste en el diseño e implementación de una arquitectura de red dinámica para el Laboratorio de Telecomunicaciones, construida sobre siete equipos MikroTik y configurada mediante la herramienta WinBox. La solución integra tres componentes complementarios: el protocolo de enrutamiento OSPF, el servicio DHCP y mecanismos de seguridad perimetral basados en firewall y listas de control de acceso (ACL).

El entorno de simulación GNS3 se utilizó como herramienta de validación previa, lo que permitió verificar el comportamiento de las configuraciones antes de su implementación en la infraestructura física.

El protocolo OSPF es responsable del enrutamiento dinámico dentro de la red. Como protocolo de estado de enlace, cada router mantiene una representación de la topología de red y calcula automáticamente las rutas más eficientes mediante el algoritmo SPF (*Shortest Path First*). Ante cambios en la topología, como la caída de un enlace o la incorporación de un nuevo dispositivo, OSPF propaga la información actualizada y recalcula las rutas sin requerir intervención del administrador.

El servicio DHCP automatiza la asignación de parámetros de red. Una vez configurado en el router administrador, asigna automáticamente la dirección IP, la máscara de subred, la puerta de enlace predeterminada y los servidores DNS a los dispositivos que se conectan a la red. Esta configuración reduce el tiempo requerido para incorporar nuevos equipos y evita conflictos de direccionamiento derivados de asignaciones manuales incorrectas o duplicadas.

La seguridad perimetral se implementa mediante las capacidades nativas de firewall de RouterOS, complementadas con reglas de filtrado que funcionan como listas de control de acceso. El firewall inspecciona el tráfico entrante y saliente de cada módulo según políticas predefinidas, mientras que las ACL determinan qué direcciones IP, protocolos y puertos están autorizados para comunicarse con cada segmento de la red.

1.4. Objetivo del proyecto.

1.4.1. Objetivo general.

Implementar una arquitectura de red dinámica en el Laboratorio de Telecomunicaciones mediante la configuración del protocolo OSPF, el servicio DHCP y un sistema de seguridad perimetral basado en firewall y ACLs sobre equipos MikroTik, con el fin de garantizar la disponibilidad, eficiencia y protección de la infraestructura de red frente a fallos de topología y accesos no autorizados.

1.4.2. Objetivos específicos.

- Diagnosticar el estado actual de la infraestructura de red del Laboratorio de Telecomunicaciones, identificando las deficiencias en el enrutamiento y la asignación de direcciones IP.
- Configurar el protocolo de enrutamiento OSPF y el servicio DHCP sobre los equipos, definiendo la topología de red, el esquema de direccionamiento IP y las áreas de enrutamiento para garantizar la conectividad dinámica entre los segmentos del laboratorio.
- Implementar políticas de seguridad perimetral mediante firewall y listas de control de acceso (ACLs) en los equipos MikroTik, estableciendo reglas de filtrado de tráfico que impidan el acceso de dispositivos y redes no autorizadas a la infraestructura del laboratorio.

1.5. Justificación.

La implementación de este proyecto responde no solo a una necesidad técnica, sino también a una necesidad formativa. Un laboratorio de telecomunicaciones que opera con una red estática, sin servicio DHCP y sin mecanismos de seguridad perimetral, limita las oportunidades de aprendizaje práctico de los estudiantes. En cambio, una infraestructura que

integra enrutamiento dinámico, asignación automática de direcciones IP y controles de seguridad permite desarrollar prácticas alineadas con escenarios reales de administración de redes.

Un estudio desarrollado en la Facultad de Informática de la Universidad Autónoma de Sinaloa destaca la implementación de OSPF en equipos MikroTik como una alternativa para la gestión de redes con múltiples routers y rutas dinámicas. Asimismo, la plataforma RouterOS ofrece herramientas de configuración y administración que pueden facilitar las prácticas de implementación en contextos académicos [13].

En síntesis, el proyecto puede generar un impacto técnico, académico e institucional. Desde el punto de vista técnico, contribuye a mejorar la administración, disponibilidad y seguridad de la red. En el ámbito académico, fortalece las condiciones del laboratorio para el desarrollo de prácticas relacionadas con enrutamiento dinámico, DHCP y seguridad perimetral. A nivel institucional, puede aportar al fortalecimiento de la infraestructura tecnológica destinada a la formación en telecomunicaciones.

Desde una perspectiva técnica, la selección de MikroTik como plataforma de implementación se sustenta en investigaciones previas que documentan la utilidad de RouterOS para aplicar políticas de seguridad. Palate y Avila (2021), mediante un caso de estudio sobre mitigación de vulnerabilidades en la red central de un proveedor de servicios de Internet, identificaron medidas como el uso de reglas de firewall, el control de conexiones y la restricción de servicios de administración remota para mitigar amenazas y preservar la estabilidad de la red [14].

En un artículo publicado en *Journal TechInnovation*, Ponce Guerrero (2024) señala que la seguridad en redes LAN requiere un enfoque integral que incluya la protección de datos, el control de accesos y la consideración de elementos físicos, lógicos y de infraestructura. Esta perspectiva respalda la decisión de integrar OSPF, DHCP y controles de seguridad perimetral en una única arquitectura, ya que permite abordar de manera coordinada las necesidades de conectividad, administración de direcciones IP y protección de la red del laboratorio [1].

1.6. Alcance del proyecto.

El presente proyecto abarca el diseño, la configuración y la implementación de una arquitectura de red dinámica en el Laboratorio de Telecomunicaciones. La infraestructura está compuesta por siete equipos MikroTik con RouterOS: un router administrador, un switch de distribución y cinco módulos independientes, identificados como A, B, C, D y E.

A diferencia de una red plana basada en direccionamiento estático, la arquitectura propuesta integra enrutamiento dinámico, asignación automática de direcciones IP y controles de seguridad perimetral como elementos articulados. Cada módulo funciona como un segmento de red diferenciado y puede comunicarse con los demás segmentos de acuerdo con las rutas dinámicas y las políticas de acceso configuradas. De esta manera, los cambios admisibles en la topología pueden ser atendidos mediante los mecanismos de convergencia del protocolo de enrutamiento, sin requerir una reconfiguración manual de las rutas.

El alcance técnico también comprende la implementación del servicio DHCP para la asignación automática de direcciones IP en cada módulo. Asimismo, se configura la entrega de los servidores DNS públicos 8.8.8.8 y 1.1.1.1 a los dispositivos conectados a la red. Esta configuración incluye las cámaras IP PTZ compatibles con la aplicación Yi IoT que se encuentran integradas en el laboratorio.

Asimismo, se configurarán los servidores DNS que se entregarán a los clientes a través de DHCP y los rangos de direcciones que utilizará cada servidor. De manera complementaria, el proyecto abarca la implementación de seguridad perimetral mediante reglas de firewall y listas de control de acceso (ACL) configuradas directamente sobre el sistema operativo RouterOS del equipo MikroTik, siguiendo las funcionalidades de enrutamiento, filtrado y control de tráfico que este sistema ofrece de manera nativa [15].

1.7. Delimitación del proyecto.

El presente estudio se delimita exclusivamente a la infraestructura física de red LAN instalada dentro del Laboratorio de Telecomunicaciones de la UPSE, por lo que no contempla la implementación de redes inalámbricas como parte central de la arquitectura, más allá de la conectividad puntual requerida por las cámaras IP incluidas en el proyecto.

Asimismo, el alcance no incluye la integración de servicios en la nube, la administración de infraestructura externa a las instalaciones del laboratorio, ni la implementación de esquemas de seguridad perimetral avanzados como firewalls de nueva generación (NGFW), sistemas IDS/IPS dedicados o soluciones de filtrado, ya que el proyecto se enfoca específicamente en las capacidades de enrutamiento dinámico, asignación de direcciones y control de acceso que ofrece el equipo MikroTik dentro de su propio sistema operativo.

En cuanto al alcance temporal, el proyecto comprende las fases de diseño, configuración, implementación y validación de la arquitectura de red durante el periodo establecido para el desarrollo del trabajo, sin contemplar un monitoreo continuo o mantenimiento posterior a la entrega del proyecto ante el Laboratorio de Telecomunicaciones.

De esta manera, el alcance definido garantiza que los objetivos planteados sean medibles, verificables mediante evidencia de tráfico real y ejecutables dentro de los recursos técnicos y de tiempo disponibles para la institución.

1.8. Metodología.

1.8.1. Enfoque de la investigación.

El proyecto se desarrolló bajo un enfoque de investigación mixto, al integrar métodos cuantitativos y cualitativos. La selección de este enfoque se fundamenta en la naturaleza del problema de estudio, que comprende una dimensión técnica susceptible de medición objetiva y una dimensión contextual que requiere interpretación y análisis crítico.

El componente cuantitativo se orientó a evaluar el desempeño de la arquitectura de red implementada mediante indicadores técnicos verificables. Se consideraron los tiempos de convergencia del protocolo OSPF ante la interrupción de un enlace, el porcentaje de asignaciones DHCP realizadas correctamente, el número de conexiones bloqueadas por las reglas de firewall y las listas de control de acceso (ACL), y los resultados de las pruebas de conectividad de extremo a extremo entre los módulos. Los resultados obtenidos permiten determinar el grado de cumplimiento de los requerimientos técnicos establecidos para la infraestructura de red.

1.8.2. Metodología descriptiva.

Durante la fase de diagnóstico se aplicó una investigación de tipo descriptiva, orientada a caracterizar el estado inicial de la infraestructura de red del Laboratorio de Telecomunicaciones. Para ello, se realizaron actividades de observación directa y levantamiento técnico de los equipos MikroTik existentes. Estas actividades permitieron documentar la topología física de la red, el esquema de direccionamiento IP, las configuraciones vigentes, la ausencia de protocolos de enrutamiento dinámico y las vulnerabilidades de seguridad identificadas.

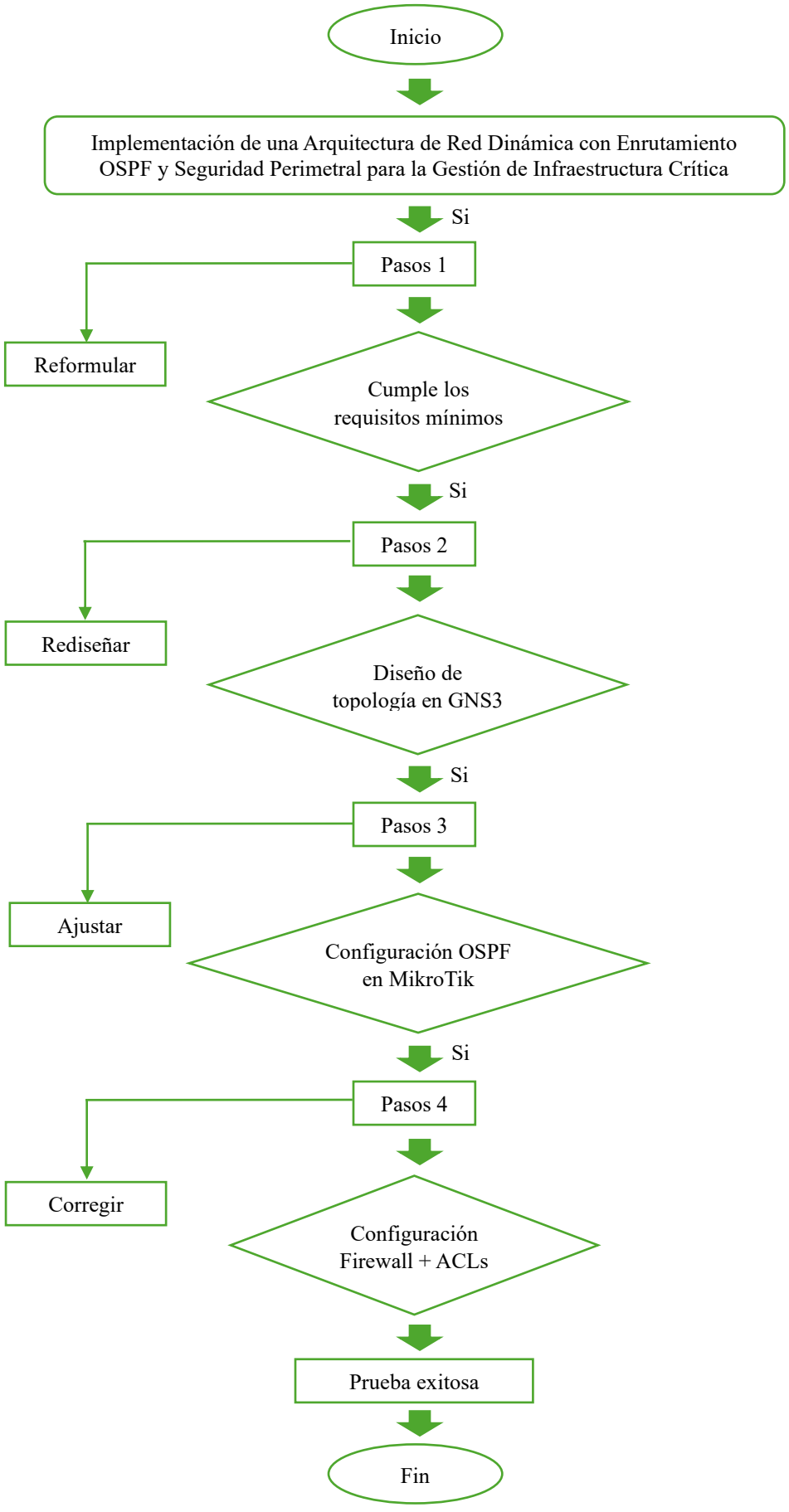
1.8.3. Metodología experimental.

El componente experimental se desarrolló durante la fase de implementación y evaluación; en esta etapa se realizaron configuraciones controladas sobre los equipos MikroTik, se manipularon variables técnicas como parámetros OSPF, rangos DHCP y reglas de firewall, se ejecutaron pruebas sistemáticas para observar y medir el comportamiento de la red bajo diferentes condiciones. La simulación de fallos de enlace para verificar la convergencia de OSPF, las pruebas de asignación DHCP y las pruebas de filtrado de tráfico con las ACLs son ejemplos concretos del carácter experimental de esta fase del trabajo.

1.8.4. Fase metodológica del proyecto.

El proyecto se desarrolló en cuatro fases consecutivas para diseñar, implementar y validar una red dinámica con OSPF y seguridad perimetral. Cada fase incluyó verificaciones y ajustes antes de avanzar a la siguiente etapa.

1. El diseño de la arquitectura, que incluyó la topología lógica en GNS3, el esquema de direccionamiento IP y las políticas de seguridad.
2. La implementación sobre los equipos físicos, configurando cada módulo según el diseño establecido.
3. La validación mediante pruebas de conectividad, verificación de adyacencias OSPF y comprobación del funcionamiento de las reglas de firewall y ACLs.
4. La configuración de la seguridad perimetral, mediante la implementación de reglas de firewall y listas de control de acceso (ACLs), para restringir el tráfico no autorizado y proteger la infraestructura de red.


Inicio
Implementación de una Arquitectura de Red Dinámica con Enrutamiento OSPF y Seguridad Perimetral para la Gestión de Infraestructura Crítica
Si
Pasos 1
Reformular
Cumple los requisitos mínimos
Si
Pasos 2
Rediseñar
Diseño de topología en GNS3
Si
Pasos 3
Ajustar
Configuración OSPF en MikroTik
Si
Pasos 4
Corregir
Configuración Firewall + ACLs
Prueba exitosa
Fin

CAPÍTULO II

2.1. Marco contextual.

Las universidades ecuatorianas atraviesan un proceso de modernización de sus infraestructuras tecnológicas que, en muchos casos, no ha alcanzado aún a los laboratorios de práctica.

Bermeo (2025), en un artículo publicado por la editorial Tecnocientífica América, señala que buena parte de las instituciones de educación superior del país presenta una infraestructura tecnológica insuficiente para sostener ecosistemas digitales, que resulta más marcada en los espacios de formación técnica que en las áreas administrativas [16].

El laboratorio de telecomunicaciones de la UPSE no era la excepción: su infraestructura de red presentaba las limitaciones propias de un esquema de gestión manual: dependencia total de la intervención del administrador ante cualquier cambio en la topología, ausencia de políticas formales de seguridad perimetral y un sistema de asignación de direcciones IP propenso a conflictos.

Esta situación no solo afectaba la operación cotidiana del espacio, sino que reducía sus posibilidades como entorno de aprendizaje para tecnologías de red avanzadas. La implementación de una arquitectura dinámica con OSPF, DHCP y seguridad perimetral responde directamente a estas limitaciones.

2.2. Marco teórico

2.2.1. Fundamentos de redes.

Los fundamentos en redes comprenden el conjunto de principios, dispositivos, protocolos y modelos de comunicación que permiten la interconexión entre equipos informáticos para compartir datos, servicios y recursos. Una red informática se basa en la conexión de dos o más dispositivos capaces de intercambiar información, mientras que los protocolos establecen las reglas necesarias para que dicha comunicación se realice de forma ordenada [17].

Las redes de computadoras constituyen la base tecnológica sobre la que se sustenta la comunicación digital moderna. En la Universidad de Huánuco, las redes de

telecomunicaciones han evolucionado hacia arquitecturas más complejas y escalables, donde la eficiencia en el enrutamiento y la seguridad de los datos son pilares fundamentales para garantizar la continuidad operativa de cualquier institución [9].

Desde el punto de vista de su alcance geográfico, las redes se clasifican en redes de área local (LAN), que conectan dispositivos dentro de un mismo edificio o campus; redes de área metropolitana (MAN), que abarcan una ciudad o región; y redes de área amplia (WAN), que permiten la interconexión a nivel nacional o internacional.

La arquitectura implementada en este proyecto corresponde a una red LAN en el laboratorio de telecomunicaciones, con capacidad de expansión hacia una WAN mediante la integración del protocolo OSPF.

2.2.2. Seguridad perimetral en redes.

La seguridad perimetral informática hace referencia al conjunto de medidas, tecnologías y políticas orientadas a proteger los recursos de una red interna frente a amenazas provenientes de redes externas o no confiables. En un artículo publicado en la *Revista de* Ingeniería: Ciencia, Tecnología e Innovación, definen la seguridad perimetral como todos los sistemas destinados a proteger de intrusos el perímetro de la red privada, siendo el firewall su componente fundamental [18].

2.2.3. Lista de control de acceso en comunicaciones seguras.

Las Listas de Control de Acceso (ACLs) son conjuntos de reglas que permiten al administrador de red definir qué tráfico está permitido o denegado en función de criterios como dirección IP de origen a destino, el protocolo, puerto TCP/UDP o interfaz de red.

En el proyecto de grado Diseño e implementación de una red FTTH utilizando el estándar G.984.X configurando Queue-Tree y ACL, se demostró la implementación de ACLs en routers permitiendo un control del tráfico de red, restringiendo el acceso a servicios específicos y reduciendo la superficie de ataque de la infraestructura, se analizó que las ACLs definen exactamente los dispositivos que pueden comunicarse con cada segmento, impidiendo de manera efectiva que equipos o redes no autorizadas puedan integrarse o interferir con la infraestructura del laboratorio [19].

Las ACLs son esencialmente un conjunto de reglas o configuraciones que determinan qué paquetes de red pueden fluir a través de un dispositivo y cuáles deben bloquearse para hacer cumplir las políticas de seguridad, restringir el acceso no autorizado y mitigar posibles amenazas a la seguridad al definir qué tráfico está permitido o denegado según criterios específicos.

2.2.4. Estándares de seguridad aplicables.

El marco de seguridad del NIST (National Institute of Standards and Technology) organiza la gestión de la ciberseguridad en cinco funciones: identificar, proteger, detectar, responder y recuperar. Las medidas implementadas en este proyecto contribuyen principalmente a las funciones de proteger y detectar; el firewall y las ACLs protegen la infraestructura limitando el acceso no autorizado, mientras el monitoreo del tráfico en tiempo real permite detectar comportamientos anómalos.

La norma ISO/IEC 27001:2022, por su parte, orienta el diseño de las políticas de seguridad perimetral mediante sus principios de confidencialidad, integridad y disponibilidad; en su versión más reciente, establece los requisitos para un sistema de gestión de seguridad de la información (SGSI).

- **Gestión y protección: NIST CSF.**

Ante el panorama de amenazas explicado, la comunidad internacional ha desarrollado marcos normativos y estándares de gestión de la seguridad que orientan a los operadores de infraestructura crítica en la implementación de controles y prácticas de protección. Los dos estándares más ampliamente adoptados a nivel global son el marco de seguridad del NIST (NIST CSF) y la norma ISO/IEC 27001.

- **Norma ISO/IEC 27001.**

La norma ISO/IEC 27001 establece los requisitos para implementar, mantener y mejorar continuamente, un sistema de gestión de seguridad de la información (SGSI). Según su versión vigente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), incorpora 93 controles de referencia organizados en cuatro categorías: controles organizativos, controles de personas, controles físicos y controles

tecnológicos, complementados por la guía de implementación de la norma ISO/IEC 27002 [20].

A diferencia del NIST CSF, la ISO/IEC 27001 es una norma certificable, lo que implica que las organizaciones pueden obtener una certificación independiente que acredita el cumplimiento de sus requisitos. Esta característica la hace especialmente relevante para los operadores de infraestructura crítica de telecomunicaciones que necesitan demostrar conformidad ante reguladores, clientes y socios comerciales.

La publicación Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience propone el marco InfraGuard para evaluar la ciberresiliencia de infraestructuras críticas. El modelo integra NIST CSF, ISO/IEC 15504 y COBIT mediante una evaluación multidimensional de capacidades relacionadas con la gestión de riesgos, la defensa activa y la recuperación ante incidentes. Este enfoque evidencia la importancia de combinar estándares y modelos de madurez para fortalecer la protección de sistemas críticos [21].

- **Modelo OSI.**

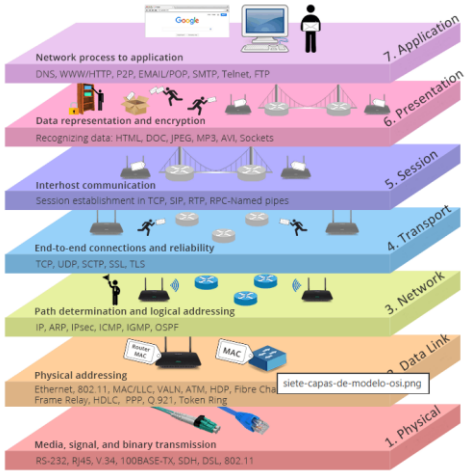
El modelo de referencia OSI (Open Systems Interconnection), desarrollado por la ISO, establece una arquitectura de siete capas para estandarizar la comunicación entre sistemas heterogéneos: la capa física, enlace de datos, red, transporte, sesión, presentación y aplicación.

El protocolo OSPF opera en la capa de red (capa 3) del modelo OSI, lo que le permite tomar decisiones de enrutamiento basadas en el estado de los enlaces de datos. Para ello, utiliza un algoritmo de estado de enlace para calcular las rutas más cortas y eficientes en una red; cada router OSPF mantiene una base de datos de estado de enlace que contiene información sobre los routers vecinos [22].

La Figura 1, se muestra el funcionamiento de analizar la interacción entre las distintas capas del modelo OSI y el proceso de transmisión de datos a través de la red. El protocolo IP cumple la función de encaminar los paquetes de datos entre diferentes redes; el protocolo TCP asegura una entrega confiable de la información entre dispositivos mediante mecanismos de verificación y retransmisión, mientras que UDP prioriza la velocidad sobre

la confiabilidad, siendo utilizado en aplicaciones que requieren transmisión en tiempo real [23].

Figura 1. *Protocolos de red básicos en la comprensión del modelo OSI.*



Nota. Es la representación de los protocolos de la red básica en el modelo OSI; mostrando la interacción entre capas y protocolos, con esto permite comprender con mayor profundidad el funcionamiento del modelo OSI [23].

Como se muestra en la Tabla 1, el modelo OSI se divide en siete capas, cada una de las cuales cumple un papel importante dentro de la pila de redes y se comunica con otras capas mediante el intercambio de unidades de datos de protocolo [24].

Tabla 1. *Descripción de las siete capas del modelo OSI, sus funciones principales.*

N°	Capas.	Función principal.	PDU.	Sistema asociado.
7	Aplicación.	Interfaz directa con el usuario final; gestiona servicios de red como correo, navegación web y transferencia de archivos.	Datos.	Servidor PC.
6	Presentación.	Traduce, cifra y comprime los datos para que sean interpretables entre sistemas distintos.	Datos.	Gateway.

5	Sesión.	Establece, gestiona y finaliza las sesiones de comunicación entre aplicaciones.	Datos.	Gateway.
4	Transporte.	Garantiza la entrega de datos extremo a extremo con control de errores y flujo mediante TCP o UDP.	Segmento / Datagrama.	Gateway.
3	Capa de red.	Enrutamiento y direccionamiento lógico de paquetes a través de la red; aquí opera OSPF.	Paquete.	Enrutador.
2	Enlace de datos.	Direccionamiento físico mediante direcciones MAC; control de acceso al medio y detección de errores.	Trama.	Switch.
1	Capa física.	Transmisión de bits en forma de señales eléctricas, ópticas o de radio a través del medio físico.	Bit.	Hub y cables.

Nota. La comunidad de red en las siete capas cumple cada función específica, desde la transmisión física de bits hasta la interacción con el usuario.

2.2.5. Tipos de redes.

Las redes de computadoras pueden clasificarse bajo distintos criterios: por su topología, por su medio de transmisión o por su alcance geográfico, siendo esta última la clasificación más utilizada en la literatura técnica y académica.

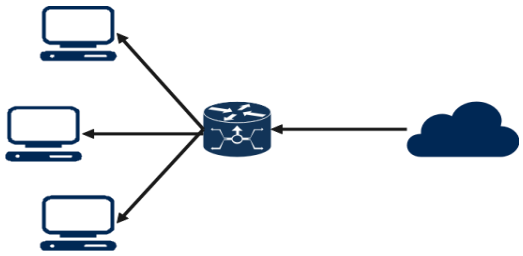
Las redes de computadoras pueden clasificarse en LAN, MAN y WAN, esto debido a su tamaño y alcance, siendo las LAN (Red de área local) de extensión pequeña, las MAN (Red de área metropolitana) de tamaño medio y por último, las WAN (Red de área amplia) las más grandes y completas, siendo Internet el ejemplo más representativo.

- **Red de área local (LAN Local Area Network).**

Una red LAN es un grupo de computadoras y dispositivos periféricos que están conectados en un área limitada, como una escuela, un laboratorio, una casa o un edificio de oficinas. Es especialmente útil para compartir recursos como archivos, impresoras, aplicaciones y otros servicios.

En general, consta de menos de 5000 dispositivos interconectados en varios edificios; es una red privada y opera a una velocidad relativamente mayor en comparación con otros sistemas WAN [25].

Figura 2. *Red de área local (LAN)*



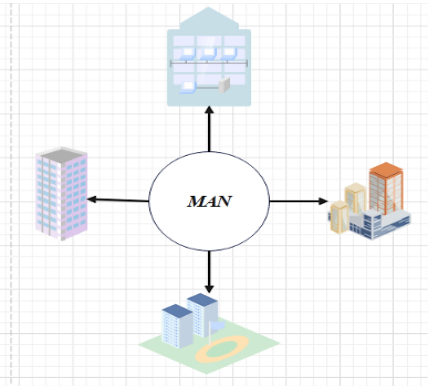
Nota: Es una infraestructura esencial en las comunicaciones actuales, porque facilita la conexión entre dispositivos próximos de forma ágil, confiable y segura, permitiendo el intercambio de datos y recursos.

- **Red de área metropolitana (MAN — Metropolitan Area Network).**

Las redes MAN son una tecnología que permite la interconexión de múltiples dispositivos y recursos en una zona geográfica extensa, como una ciudad, área metropolitana o campus universitario.

Se caracterizan por tener altas velocidades de transmisión de datos y una notable capacidad de ancho de banda para soportar el tráfico de múltiples usuarios y aplicaciones. Entre sus ventajas destacan el alto rendimiento, la conectividad confiable gracias a su infraestructura y la escalabilidad para agregar nuevos dispositivos [25].

Figura 3. *Una red de área metropolitana (MAN).*

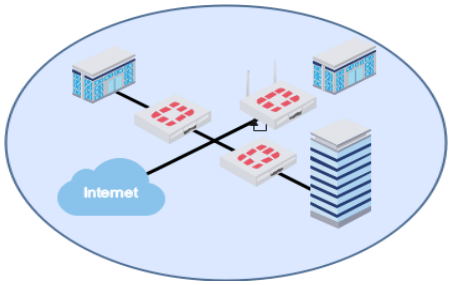


Nota. Es un sistema de comunicación que enlaza dispositivos y redes situadas en distintas áreas geográficas, facilitando la transferencia de datos e información entre diferentes ciudades, países e incluso continentes.

- **Red de área amplia (WAN — Wide Area Network).**

Los dos tipos más comunes son la red de área local (LAN) y la red de área amplia (WAN). Una LAN es una infraestructura de red que proporciona acceso a usuarios y dispositivos finales en un área geográfica, mientras que las WAN conectan redes en grandes extensiones, definidas por el tamaño del área que abarcan, la cantidad de usuarios conectados, los tipos de servicios disponibles y el área de responsabilidad [25].

Figura 4. *Red área ampliada (WAN).* .



Nota. Es un tipo de red de comunicación que permite interconectar dispositivos, oficinas, edificios o redes ubicadas en diferentes países. Su objetivo principal es facilitar la transmisión de datos y la comunicación a largas distancias.

La Tabla 2, se muestran las redes WAN, LAN y MAN se diferencian principalmente por sus enlaces, velocidad y forma de administración.

Tabla 2. *Análisis multidimensional de los tres principales tipos de redes.*

Características.	**LAN.**	**MAN.**	**WAN.**
Alcance.	Laboratorio.	Ciudad/Campus.	Limitada.
Distancias máximas.	5 km.	10 a 50 km.	Millones.
Velocidad típica.	100 Mbps – 10 Gbps.	30 Mbps – 10 Gbps.	Variable.
Latencia.	Muy baja (< 1ms).	Baja (1 – 10 ms).	Alta (10 – 500 ms).

Propietario.	Privado institucional.	Preveedor/IPS.	IPS/Operadora.
Medio de transmisión.	Ethernet, Wi-Fi.	Fibra óptica/MPLS.	Satélite, fibra, BGP/MPLS.
Administración.	Interna.	Proveedor/mixta	Proveedor externo.

Nota. Análisis comparativo multidimensional de los tres principales tipos de redes (LAN, WAN, MAN) en cuanto a cobertura, velocidad, costo y aplicaciones.

2.2.6. Topologías en red.

El término topología de red hace referencia a la disposición física o lógica de los nodos y los enlaces que conforman una red de comunicaciones. En telecomunicaciones, se distinguen dos perspectivas complementarias para el análisis de la topología; se pueden observar en la Tabla 3.

Tabla 3. *Se muestra lo comparativo de la topología de la red.*

Topología	Ventajas	Desventajas
Bus.	-Bajo costo de cable. -Fácil instalación inicial. -Adecuado para redes pequeñas.	- Si falla un nodo o el cable principal, se afecta toda la red. -Difícil diagnóstico de fallas.
Anillo.	-Rendimiento determinado. -Anillo dual: protección ante fallos. -Latencia controlada.	-Falla un nodo interrumpe el anillo simple. -Para agregar más nodos, se requiere una interrupción.
Estrella.	-La falla de un solo nodo no afecta los demás. -Fácil instalación y mantenimiento. -Escalabilidad sencilla a los puertos.	-Dispositivo central, punto crítico. -La capacidad está limitada por los puertos del dispositivo central
Malla.	-Máxima tolerancia a fallos. -Sin punto único de fallas. -Distribución entre cargas a nuevas rutas, -Alta disponibilidad.	-Eleva el costo de implementación. -El número de enlaces crece cuadráticamente.

Híbrida	-Máxima flexibilidad de diseño. -Redundancia selectiva por segmento. -Escalabilidad muy alta. -Optimización de la relación costo-beneficio por zona.	-Mayor complejidad de diseño y gestión. -Costo de implementación elevado. -Más difícil diagnóstico de fallas.

Nota. Comparativo de las principales topologías de la red (bus, anillo, malla, estrella) evaluando sus ventajas, desventajas y escenario de aplicaciones.

- **Enrutamiento.**

El enrutamiento es el proceso mediante el cual los dispositivos de red determinan la ruta más adecuada para enviar paquetes desde un origen hasta un destino. La obra Introducción al protocolo OSPF distingue dos paradigmas principales de enrutamiento: el estático, en el que el administrador configura manualmente las rutas, y el dinámico, en el que los dispositivos intercambian información sobre la topología de red y calculan automáticamente las rutas disponibles de acuerdo con las métricas del protocolo. [26].

El enrutamiento dinámico resulta especialmente adecuado en entornos institucionales donde la topología de red puede cambiar con frecuencia. En un trabajo académico sobre OSPFv2 desarrollado en el Instituto Tecnológico de las Américas, Chevalier (2025), afirma que los protocolos de enrutamiento dinámico comparten una estructura común: utilizan mensajes de protocolo para intercambiar información de rutas, construyen estructuras de datos (tablas de enrutamiento) y aplican algoritmos de enrutamiento para seleccionar el mejor camino disponible [27].

- **Redes estáticas.**

Una red estática es aquella cuya configuración de rutas, tablas de reenvío, parámetros de calidad de servicio y asignación de recursos se define de manera manual y permanece invariable a lo largo del tiempo, salvo intervención explícita del administrador. En este modelo, cada dispositivo de red (router, switch, servidor) opera con parámetros predefinidos que no se modifican automáticamente en respuesta a eventos del entorno.

En el contexto del enrutamiento, la modalidad estática implica que el administrador configura manualmente cada ruta en la tabla de encaminamiento del dispositivo. En las redes

tradicionales, las políticas de red son difíciles de implementar en todos los dispositivos de la red de forma simultánea, lo que refleja la rigidez operativa característica de los entornos estáticos.

- **Redes dinámicas.**

Una red dinámica es aquella capaz de adaptar automáticamente su configuración, rutas y parámetros operativos en respuesta a cambios en el estado de la red, sin requerir intervención manual del administrador. Este comportamiento adaptativo se logra mediante protocolos de enrutamiento dinámico, mecanismos de señalización y, en las arquitecturas más modernas, mediante la separación del plano de control del plano de datos a través de tecnologías como SDN (Software-Defined Networking) y NFV (Network Functions Virtualization).

Desde la perspectiva del enrutamiento, los protocolos dinámicos, como OSPF, EIGRP y BGP, permiten intercambiar información de enrutamiento y actualizar automáticamente las rutas ante cambios en la topología de red. Estas características hacen que sean adecuados para entornos IPv6 que requieren continuidad de servicio, tolerancia a fallos y adaptación dinámica del tráfico. La evidencia específica sobre su desempeño frente a configuraciones estáticas debe sustentarse en el estudio seleccionado de Future Internet [28].

- **Redes estáticas vs. redes dinámicas.**

La distinción entre redes estáticas y redes dinámicas constituye uno de los ejes conceptuales fundamentales para comprender la evolución de las arquitecturas de red. Esta clasificación no solo describe la manera en que se configuran y gestionan los elementos de la red, sino que también determina la capacidad de adaptación de la infraestructura ante cambios en el tráfico, en la topología o en los requisitos de los servicios.

La Tabla 4, se muestran los protocolos IGP, aquellos utilizados para encaminar el tráfico dentro de un sistema autónomo o dentro de la infraestructura de una misma empresa. Entre los protocolos IGP existen dos categorías: los de vector distancia, que se basan en una dirección y un sentido para decidir la ruta hacia la red de destino, entre los que destacan RIP y EIGRP; y los de estado de enlace, que verifican el estado de las adyacencias entre vecinos de forma periódica y calculan el costo de cada enlace [29].

Tabla 4. *Comparación de los protocolos de enrutamiento BGP, OSPF y EIGRP.*

Parámetro	IGP	EGP
Ámbito de uso.	Dentro de un sistema autónomo (AS).	Entre sistemas autónomos distintos.
Administración.	Una sola organización.	Múltiples organizaciones / ISP.
Protocolos principales.	RIP, EIGRP, OSPF, IS-IS	BGP
Métrica.	Costo, saltos, ancho de banda.	Políticas de rutas.
Escalabilidad.	Redes medianas y pequeñas.	Redes a escala de Internet.

Nota. El protocolo BGP es el único protocolo de puerta de enlace exterior funcional en la actualidad, al punto de que, en la práctica, los ingenieros utilizan ambos términos de manera indistinta.

2.2.7. Protocolo de enrutamiento OSPF.

- **OSPF (Open Shortest Path First).**

El uso de áreas en OSPF está optimizado para el manejo eficiente de recursos en redes de gran escala: cada área es un conjunto lógico de routers que comparten la misma base de datos de estado de enlace. De acuerdo con la guía técnica de González (2023), OSPF es ampliamente utilizado en redes IP debido a su eficiencia en la actualización dinámica de rutas y su capacidad de adaptación a distintos tamaños de red, lo que lo convierte en una opción adecuada tanto para redes empresariales pequeñas como para infraestructuras más complejas, como la desarrollada en el presente proyecto [30].

Cuando se produce una falla en un enlace o se incorpora un nuevo router, los dispositivos OSPF intercambian información actualizada y recalculan las rutas en cuestión de segundos, sin necesidad de intervención manual del administrador de red [22].

La Tabla 5 muestra que OSPF es un protocolo de enrutamiento eficiente, seguro y escalable que nos permite aprovechar el mejoramiento de las direcciones IP, seleccionar rutas en el mejor costo de los enlaces y reaccionar rápidamente ante el cambio de la red.

Tabla 5. *Principales características del protocolo OSPF: soporte para VLSM y CIDR.*

Parámetro	Descripción
Sin clases	Soporta VLSM y CIDR para un uso eficiente del espacio de direcciones.
Convergencia rápida	Propaga cambios de topología de forma inmediata sin actualizaciones periódicas.
Métrica por costo	Calcula rutas en función del ancho de banda de los enlaces.
Sin bucles	El algoritmo SPF garantiza rutas libres de bucles de enrutamiento.
Autenticación	Permite autenticar el intercambio de información entre routers.
Escalabilidad	Se adapta eficientemente a redes de pequeña, mediana y gran escala.

Nota. Las principales características del protocolo OSPF, destacando su diseño sin clase con soporte para VLSM y CIDR, su capacidad de convergencia rápida ante cambios en la topología

- **Definición y características de OSPF.**

Las redes conectadas y los costos asociados a cada enlace de información se intercambian entre routers mediante paquetes LSA, permitiendo que cada dispositivo construya un mapa completo de la topología de la red. En el artículo de “Blazar Networks” se comenta que cada router OSPF mantiene una base de datos de estado de enlace (LSDB) que contiene información detallada de cada router vecino [22].

Según CCNA Desde Cero, se agrupa tradicionalmente en dos grandes familias según el algoritmo que utilizan para calcular las rutas: los protocolos de vector distancia y los protocolos de estado de enlace. Los primeros determinan el mejor recorrido a partir de la distancia (métrica) y la dirección (vector) hacia una red de destino; para ello envían periódicamente a sus vecinos la tabla de enrutamiento [31].

Este enfoque tiene consecuencias directas sobre la eficiencia y estabilidad de la red: mientras los protocolos de vector distancia son más sencillos de configurar, pero más propensos a bucles de enrutamiento y a una convergencia lenta, los protocolos de estado de enlace ofrecen una visión más precisa de la topología y se adaptan con mayor rapidez a los cambios.

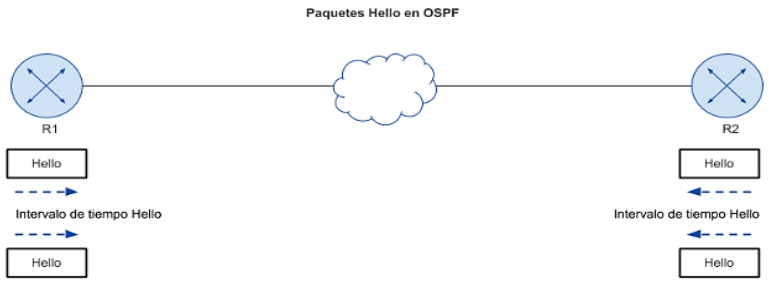
- **Enrutamiento OSPF.**

Para que la información de los routers se sincronice entre sí, cada uno forma una adyacencia completa únicamente con el DR, que recibe las actualizaciones de todos y las redistribuye al resto del segmento. Esto minimiza la cantidad de información repetitiva que se reenvía en la red, ya que OSPF envía todos los mensajes al router designado [32].

El DR cumple dos funciones principales: originar los anuncios de enlace en nombre de esa red y establecer adyacencias con todos los routers del segmento, participando así en la sincronización de las bases de datos de estado de enlace [33].

En la Figura 5, se muestra el funcionamiento del Router Designado (DR) dentro de un segmento de red multiacceso, aplicado al contexto de la arquitectura de red implementada.

Figura 5. *Intercambio de bases de datos*



Nota. El segmento envía su información de enrutamiento, representada mediante flechas dirigidas únicamente hacia el DR y su respectivo respaldo, el BDR, en lugar de comunicarse directamente con todos los demás routers. El router designado se encarga de recopilar dicha información y redistribuirla al resto de los dispositivos.

Dentro de una red que implementa el protocolo OSPF (Open Shortest Path First), desempeñan distintos roles según su ubicación dentro de la topología y su función específica en el intercambio de información de enrutamiento. Estos roles no son mutuamente

excluyentes: un mismo dispositivo físico puede cumplir más de una función simultáneamente, dependiendo de cómo estén configuradas sus interfaces.

El intercambio directo de información entre cada par de dispositivos generaría un volumen considerable de tráfico de control, así como una carga de procesamiento innecesaria. Para resolver esta problemática, OSPF elige un router designado (DR) por cada segmento multiacceso, cuya función se resume en dos aspectos principales: por un lado, centraliza el intercambio de información al establecer adyacencias completas con todos los routers del segmento y por otro, origina el anuncio de red (Network LSA) correspondiente a dicho segmento [34].

1. **Router interno (IR):** Es aquel cuyas interfaces se encuentran conectadas exclusivamente dentro de una misma área OSPF. Mantiene una única base de datos de estado de enlace (LSDB) correspondiente a dicha área, sin tener visibilidad directa sobre el resto de la topología.
2. **Router fronterizo de área (ABR):** Es el router que conecta dos o más áreas OSPF, una de las cuales debe ser obligatoriamente el área troncal o backbone (área 0). Este mantiene una base de datos de estado de enlace independiente por cada área a la que está conectado, y se encarga de generar los anuncios de resumen que permiten propagar las rutas de un área hacia los demás sin necesidad de compartir el detalle completo de su topología interna.
3. **Router fronterizo de sistema autónomo (ASBR):** Corresponde al router que actúa como punto de conexión entre el dominio OSPF y una red externa que emplea un protocolo de enrutamiento distinto, como EIGRP, BGP o rutas estáticas. Su función principal es redistribuir dichas rutas externas hacia el dominio OSPF mediante LSA de tipo 5, permitiendo que los routers internos reconozcan los destinos que no pertenecen originalmente a la red OSPF.
4. **Router troncal (BR):** Es todo router que posee al menos una interfaz conectada directamente al área troncal. Cabe recordar que todo ABR es, por definición, un router troncal cumple necesariamente el rol de ABR.
5. **Router designado (DR):** En los segmentos de multiacceso, como las redes LAN, OSPF elige un router designado con el propósito de centralizar el intercambio de

información de enrutamiento. Origina el anuncio de red (Network LSA) en representación del segmento y establece adyacencias completas con todos los demás routers presentes en él, evitando así que cada dispositivo deba sincronizarse de manera independiente con sus vecinos.

6. **Router designado de respaldo (BDR):** Es el router que obtiene la segunda prioridad más alta durante el proceso de elección del segmento multiacceso. Su función es actuar como respaldo inmediato del DR, manteniendo sincronizada su propia base de datos con la del resto del segmento, de modo que pueda asumir el rol de router designado sin necesidad de una nueva elección completa en caso de que el DR falle.

   La Tabla 6 presenta los principales tipos de routers OSPF y sus funciones dentro de la red.

Tabla 6. *Los cuatro tipos de enrutadores OSPF y su rol dentro de la red.*

Tipos de router	Siglas	Función principal
Enrutador interno.	IR	Todas sus interfaces pertenecen a una sola área; solo enruta tráfico dentro de ella.
Red troncal del enrutador.	BR	Tiene al menos una interfaz en el área 0; forma parte de la columna vertebral OSPF.
Router de Frontera de área.	ABR	Conecta dos o más áreas OSPF; genera LSA tipo 3 para comunicación entre áreas.
Router de frontera del sistema autónomo.	ASBR	Conecta la red OSPF con otros sistemas autónomos o protocolos de enrutamiento.

Nota. Clasificación de los cuatro tipos de enrutadores OSPF (IR, ABR, ASBR, BR) y descripción de su rol funcional dentro de la jerarquía de área.

- **OSPF en MikroTik routerOS**

Santana (2024), docente de la Facultad de Informática en la Universidad Autónoma de Sinaloa, documenta en su blog académico que la implementación de OSPF en plataformas MikroTik routerOS proporciona un equilibrio óptimo entre funcionalidad y control administrativo, permitiendo gestionar eficientemente entornos dinámicos con múltiples rutas. El autor destaca que routerOS soporta las versiones OSPFv2 (para IPv4) y OSPFv3 (para

IPv6), con soporte completo para configuración de áreas, tipos de redes, prioridades de router y filtros de rutas [13].

Adicionalmente, el Instituto Tecnológico Universitario UNCUYO, señala que OSPF ofrece opciones de respaldo mediante la redistribución de rutas, lo que permite integrarlo con otros protocolos o sistemas de enrutamiento, y que el protocolo soporta tanto VLSM (Variable Length Subnet Masking) como CIDR (Classless Inter-Domain Routing), brindando mayor flexibilidad en el diseño del esquema de direccionamiento IP de la red [35].

- **Algoritmo de Dijkstra.**

El algoritmo de Dijkstra es una herramienta que permite responder una pregunta muy práctica: ¿cuál es el camino más corto para llegar de un punto a otro dentro de una red? Para lograrlo, recorre de manera ordenada, comparando en cada paso las distancias posibles y quedándose siempre con la opción que representa el menor costo hasta ese momento. Se trata de un enfoque simple, pero muy eficiente, razón por la cual se ha convertido en una pieza fundamental dentro de la ingeniería de telecomunicaciones.

Gracias a este mecanismo, cuando ocurre un cambio en la topología de la red: por ejemplo, la caída de un enlace entre módulos o la incorporación de un nuevo segmento, cada router recalcula automáticamente sus rutas utilizando Dijkstra, garantizando que el tráfico siempre se enrute por el camino más eficiente disponible. Esta característica resulta especialmente valiosa en un entorno de infraestructura crítica, donde la disponibilidad y la rapidez de convergencia de la red son determinantes para mantener la continuidad operativa.

En términos de eficiencia computacional, cuando la dimensión es grande, conviene apoyar esta selección en una cola de prioridad implementada mediante un mínimo (*min-heap*), estructura que permite obtener en tiempo reducido el próximo nodo a procesar sin necesidad de recorrer linealmente todos los candidatos [36].

El protocolo OSPF se basa en el algoritmo Shortest Path First (SPF), basado en el algoritmo de Dijkstra. Para ello, cada router construye y mantiene una base de datos de estado de enlace (Link-State Database, LSDB**);** a partir de esta base de datos, el router calcula el árbol de caminos de menor costo, considerando la métrica asignada a cada enlace, la cual generalmente está relacionada con el ancho de banda disponible. De esta forma, OSPF

selecciona automáticamente la ruta más eficiente para alcanzar cada red de destino y actualiza sus tablas de enrutamiento cuando se producen cambios en la topología, garantizando una convergencia rápida y un uso eficiente de los recursos de la red [37].

En la Universidad de Huánuco, se investigó el proceso de cálculo OSPF, que consiste en tres etapas principales; en primer lugar, se establece la adyacencia con routers vecinos mediante el intercambio de paquetes *"Hello".* En segundo lugar, la sincronización de la base de datos de estado de enlace (LSDB) a través de paquetes DBD, LSR y LSU; y en tercer lugar, la ejecución del algoritmo SPF para determinar la ruta de menor costo hacia cada destino [9].

La Tabla 7, se muestra que el funcionamiento de OSPF se desarrolla en tres etapas principales: primero, cada router crea un mapa de la red; después, calcula las rutas más cortas mediante el algoritmo SPF; finalmente, guarda las mejores rutas en su tabla de enrutamiento para enviar los paquetes correctamente.

Tabla 7. *Etapas del proceso que ejecuta OSPF mediante el algoritmo de Dijkstra.*

Etapa	Nombre	Descripción
1	Construcción de la LSDB.	Cada router recopila información de todos los enlaces mediante el intercambio de LSA con sus vecinos, construyendo un mapa completo de la topología.
2	Ejecución del algoritmo SPF.	Cada router aplica el algoritmo de Dijkstra sobre su LSDB para calcular el árbol de rutas más cortas, siendo él mismo la raíz del árbol.
3	Actualización de la tabla de enrutamiento.	Las rutas calculadas se instalan en la tabla de enrutamiento del enrutador, que las utiliza para reenviar los paquetes hacia su destino.

Nota. El proceso que ejecuta OSPF para determinar las rutas óptimas mediante el algoritmo de Dijkstra se desarrolla en tres etapas principales, en las que se refleja el funcionamiento general de los protocolos de enrutamiento en la red [38].

2.2.8. Protocolo DHCP (Dynamic Host Configuration Protocol).

El servicio DHCP, Dynamic Host Configuration Protocol, permite que los dispositivos de una red obtengan direcciones IP, además de la información necesaria, proporcionada por un servidor autorizado, para asignar máscaras de subred, gateway y demás parámetros de red, en un proceso denominado direccionamiento dinámico [39].

El protocolo DHCP permite la distribución automática de direcciones IP en una red; el servidor cumple la función básica de asignar a cada cliente solicitante una dirección IP junto con la información del servidor DNS. Cabe destacar que las direcciones IP asignadas de forma estática no se someten a verificación (ping) por parte del servidor, a diferencia de las direcciones dinámicas [40].

Antes de configurar el servidor DHCP, la interfaz debe contar con una dirección IP estática, que servirá como puerta de enlace para los clientes DHCP, y esa misma dirección no debe incluirse en el rango del pool de direcciones distribuidas a los clientes [41].

En cuanto al comportamiento con respecto al transporte, DHCP utiliza UDP como protocolo de capa de transporte: los mensajes del cliente hacia el servidor se envían al puerto del "servidor DHCP", mientras que los mensajes del servidor hacia el cliente se envían al puerto del "cliente DHCP" [42].

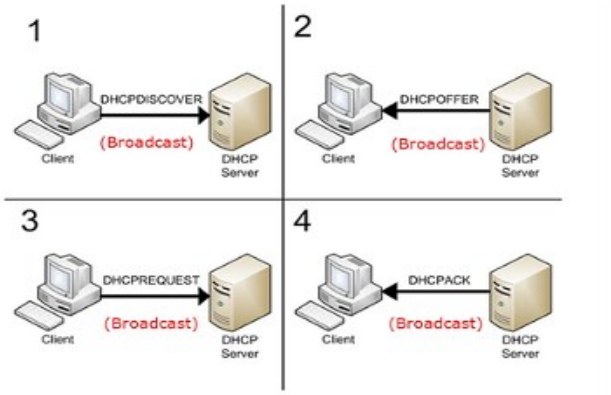
- **Tipos de asignación de direcciones IP.**

Entre las principales ventajas del servicio DHCP, la guía de funcionamiento del protocolo destaca la facilidad para incorporar nuevos equipos a la red y simplificar los cambios en la configuración general. No obstante, la misma fuente advierte que DHCP utiliza mensajes que, en su configuración básica, no incorporan mecanismos de autenticación robustos. Por ello, puede estar expuesto a amenazas como la conexión de dispositivos no autorizados o la suplantación de un servidor DHCP.

Además, debido al uso de mensajes de difusión durante determinadas etapas del proceso de asignación de direcciones IP, un volumen elevado de solicitudes puede afectar el desempeño de la red. Por esta razón, el módulo de seguridad perimetral contempla controles adicionales para mitigar estas vulnerabilidades, tales como reglas de firewall, segmentación de la red y políticas de control de acceso [43].

En la Figura 6 muestra que el protocolo DHCP utiliza una arquitectura cliente-servidor para asignar automáticamente la configuración de red a los dispositivos.

Figura 6. *Funcionamiento del intercambio de mensajes DHCP.*



Nota. Adaptado de Funcionamiento del protocolo [43].

El protocolo DHCP soporta tres modalidades de asignación de direcciones IP, cada una adecuada para distintos escenarios y requerimientos de red:

- **Asignación dinámica:** El servidor asigna una dirección IP del pool disponible por un tiempo determinado *(lease time)*. Es la modalidad más común en redes con dispositivos móviles o de alta rotación, como redes inalámbricas corporativas y redes de acceso a Internet.
- **Asignación automática o estática por MAC (reserva DHCP):** El servidor asigna siempre la misma dirección IP a un dispositivo específico identificado por su dirección MAC. La dirección queda registrada permanentemente en la base de datos del servidor y no está disponible para otros clientes.
- **Asignación manual:** El administrador configura explícitamente la dirección IP que debe recibir un dispositivo concreto, pero el mecanismo de distribución sigue siendo el protocolo DHCP.

El servidor mantiene una base de datos de direcciones IP disponibles y las asigna a los clientes conforme son solicitadas, registrando en todo momento qué dispositivo posee cada dirección, durante cuánto tiempo y en qué momento fue asignada.

- **Proceso de asignación DORA.**

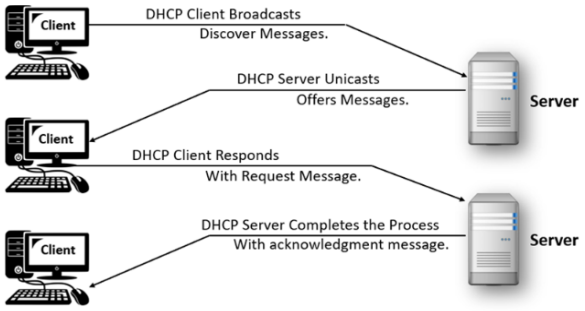
Es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo conectado, permitiéndoles comunicarse con otras redes IP.

El cliente transmite un mensaje "discover" en broadcast para localizar servidores disponibles; el servidor responde con un "offer" que incluye una dirección IP disponible; el cliente envía un "request" confirmando la aceptación; y, finalmente, el servidor envía un "acknowledgment" confirmando la asignación y proporcionando todos los parámetros de configuración [44].

En la Figura 7 muestra que el proceso de asignación DHCP sigue el proceso de DORA *(Discover, Offer, Request, Acknowledgment).*

Figura 7. *Funcionamiento del protocolo DHCP para la asignación IP en DORA.*

.



Nota. Se muestra el diagrama del proceso DORA del protocolo DHCP que ilustra las cuatro etapas: Discover, Offer, Request y Acknowledgment para la asignación dinámica de direcciones IP.

- **DHCP-DISCOVER:** El cliente recién conectado a la red, sin conocer ningún parámetro de red, envía un mensaje de broadcast solicitando la presencia de un servidor DHCP disponible. Este mensaje se envía a la dirección de broadcast 255.255.255.255 desde la dirección IP de origen 0.0.0.0.
- **DHCP-OFFER:** El servidor recibe el mensaje de descubrimiento y responde con una oferta de configuración, que incluye una dirección IP disponible del pool gestionado por el servidor, junto con los demás parámetros de red.

- **DHCP-REQUEST:** El cliente selecciona la oferta recibida (en caso de haber múltiples servidores DHCP en la red) y envía un nuevo mensaje de broadcast indicando formalmente que acepta la configuración ofrecida por el servidor elegido.
- **DHCP-ACK (Acknowledgement):** El servidor confirma la asignación enviando un mensaje DHCPACK al cliente, que contiene la configuración de red definitiva y el tiempo de arrendamiento acordado. El cliente aplica la configuración y puede comenzar a comunicarse en la red.

Cuando el cliente y el servidor DHCP se encuentran en segmentos de red lógicos diferentes, un agente de retransmisión DHCP actúa como reenviador y envía los paquetes de difusión entre ambos segmentos. El proceso DORA se ejecuta cada vez que un dispositivo se conecta a la red LAN del laboratorio; el equipo MikroTik RouterOS designado como servidor DHCP gestiona este proceso de forma automática, asignando los parámetros de red configurados por el administrador [42].

CAPÍTULO III

3.1. Desarrollo de la propuesta.

El desarrollo de este capítulo implicó un proceso previo de análisis y diseño que no siempre resulta visible en el documento. Antes de conectar el primer cable o abrir WinBox por primera vez, fue necesario identificar con claridad los recursos disponibles en el laboratorio, las necesidades de la infraestructura y la arquitectura de red más adecuada para abordar dichas necesidades de manera coherente.

El diagnóstico inicial reveló tres problemas principales: la ausencia de enrutamiento dinámico, la inexistencia del servicio DHCP y la falta de mecanismos de seguridad perimetral.

La solución diseñada integra el protocolo de enrutamiento OSPF, el servicio DHCP y mecanismos de seguridad perimetral basados en firewall y listas de control de acceso (ACL). Todos estos componentes se implementaron sobre siete equipos MikroTik hEX S disponibles en el laboratorio. Antes de extender la configuración a la infraestructura física, el diseño completo fue validado en el entorno de simulación GNS3, lo que permitió verificar el

comportamiento de los protocolos e identificar posibles inconsistencias sin comprometer la red real.

La arquitectura también integra tres cámaras IP conectadas a través de los módulos de videovigilancia. Esta incorporación añade un componente práctico al proyecto, ya que el laboratorio no solo permite demostrar el funcionamiento de los protocolos de red, sino también gestionar tráfico real generado por dispositivos de monitoreo. A lo largo de este capítulo se presenta el detalle de cada componente, desde los equipos físicos hasta la configuración final de cada módulo.

3.2. Componentes de la propuesta.

3.2.1. Componentes físicos.

- MikroTik hEX S (RB760iGS)

El MikroTik hEX S es el equipo que asume el rol de router administrador o maestro, dentro de la arquitectura implementada. Se trata de un router Gigabit compacto de cinco puertos diseñado para entornos donde no se requiere conectividad inalámbrica, pero sí capacidades avanzadas de enrutamiento y seguridad [45].

En la Figura 8, se muestra un router Gigabit de alto rendimiento diseñado para administrar redes pequeñas y medianas. Su procesador de doble núcleo, memoria RAM de 256 MB y cinco puertos Ethernet permiten gestionar el tráfico de manera rápida y estable; se pueden mostrar en la Tabla 8.

Figura 8. *El MikroTik heX S (RB760iGS).*

Nota. Interfaz del simulador de red utilizado para la simulación y prueba de la topología de la red antes de la implementación.

Tabla 8. *Especificaciones técnicas del MikroTik hEX S (RB760iGS) [45].*

Parámetro	Especificaciones
Arquitectura CPU	MMIPS – MediaTek MT7621A.
Frecuencia CPU	880 MHz, Dual Core (2 núcleos, 4 hilos).
Chip de conmutación	MT7621A (integrado).
Memoria RAM	256 MB.
Puerto Ethernet	5 × 10/100/1000 Mbps (Gigabit) – ether1 a ether5.
PoE de entrada	Pasivo + 802.3af/at (12–57 V).
PoE de salida	Puerto ether5 – PoE pasivo hasta 57 V, máx. 500 mA.
Puerto USB	1 × USB 2.0 Tipo A.

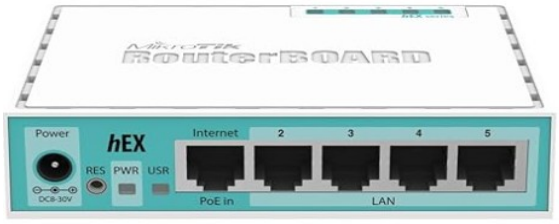
Nota. Especificaciones técnicas del MikroTik hEX S (RB760iGS): procesador, memoria RAM, puertos Ethernet, rendimiento y características de conectividad.

- MikroTik routerBOARD hEX RB750Gr3

Es una versión de la familia hEX optimizada para funciones de módulo secundario, su función se asignada a cada módulo, y su diseño compacto facilita la instalación en los tableros de práctica del laboratorio. [46].

La Tabla 9, se muestran las especificaciones; que resultó especialmente útil durante la implementación fue la compatibilidad total con routerOS. Todos los equipos de la arquitectura comparten el mismo sistema operativo y la misma herramienta de administración y en la Figura 9 se muestra el diseño de implementación.

Figura 9. *Mikrotik heX RB750Gr3 [46].*



Nota. Vista del dispositivo MikroTik hEX RB750Gr3 empleado como módulo secundario en la red de laboratorio para segmentación y control de tráfico

Tabla 9. *Especificaciones técnicas del MikroTik heX S (RB750iGr3).*

Parámetros	Especificaciones
CPU	MT7621A — Doble núcleo 880 MHz, 4 hilos.
RAM	256 MB.
Almacenamiento	16 MB Flash + ranura microSD.
Puerto Ethernet	5 × Gigabit (10/100/1000 Mbps).
Entradas	Jack DC + PoE pasivo.
Sistema operativo	RouterOS (licencia nivel 4).
Funciones	VLAN, QoS, VPN, balanceo de carga, firewall.
Dimensiones	113 × 89 × 28 mm.
Temperatura de operación	-40 °C a 60 °C.

Nota. Especificaciones técnicas del MikroTik hEX RB750Gr3: procesador, memoria, interfaces Gigabit Ethernet, rendimiento de enrutamiento y consumo de energía.

- Conector RJ45

El conector RJ45, técnicamente denominado conector modular 8P8C (8 posiciones, 8 contactos), es la interfaz física estandarizada universalmente utilizada para la terminación de cables de par trenzado (UTP/STP) en redes Ethernet [47].

En la Figura 10, se muestra el conector RJ45 se utiliza para conectar dispositivos en redes Ethernet; cuenta con ocho pines que organizan cuatro pares de cobre según las normas T568A o T568B con Cat6. Puede transmitir datos a velocidad; en la Tabla 10 se dan las especificaciones más detalladas.

Figura 10. *Conectores Cambo Plug RJ45.*

Nota. Conector Cambo Plug RJ45 Cat6 utilizados para la terminación de cables de red en la infraestructura física del laboratorio.

Tabla 10. *Especificaciones técnicas del conector RJ45 / 8P8C.*

Designación técnica	8P8C – 8 posiciones, 8 contactos
Norma de cableado	ANSI/TIA-568 (T568A y T568B).

Número de pines	8 pines (4 pares de cobre trenzado).
Velocidad máxima (Cat6)	1 Gbps (hasta 10 Gbps en distancias ≤ 55 m).
Frecuencia máxima (Cat6)	250 MHz por par.

Nota: Especificación del conector RJ45/8P8C: categoría de cable compatible, impedancia, temperatura operativa, número de pines y aplicaciones.

- Cable UTP de par trenzado para-Gigabit

El cable de categoría 6 (Cat6) es un estándar de cableado de par trenzado para redes ethernet Gigabit y otros protocolos de la capa física de redes, definido en la norma ANSI/TIA/EIA-568-B.2-1 [48].

En la Figura 11 se muestra un cable de red de categoría 6, utilizado como medio de transmisión en redes Ethernet de alta velocidad. Este tipo de cable opera con un ancho de banda de hasta 250 MHz y permite enlaces de hasta 1 Gbps hasta 100 metros, según las condiciones del enlace y la categoría del cableado.

Figura 11. *Cable De Red Par Trenzado.*

Nota. Cable de red par trenzado (UTP Cat6) empleado para las conexiones físicas entre los dispositivos de la arquitectura implementada.

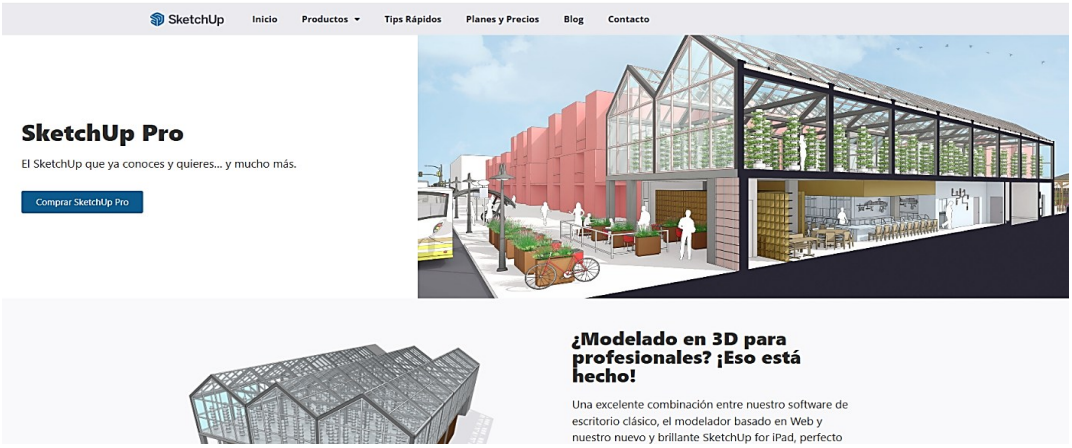
3.2.2. Componentes lógicos.

- **SketchUp**

El laboratorio está organizado en siete módulos distribuidos sobre estructuras verticales: módulo principal, módulo switch y módulos A, B, C, D y E. Esta distribución no es arbitraria; responde a criterios de flujo de tráfico, distancias de cableado y accesibilidad para las actividades de práctica y mantenimiento.

En la Figura 12, se muestra el programa ejecutable para la planificación del espacio físico del laboratorio, Utilicé SketchUp Studio 2026; la representación 3D permitió definir la distribución de los tableros de práctica, la ubicación de los equipos en cada módulo [49].

Figura 12. *Software de modelado 3D para diseño arquitectónico.*



Nota. Es la interfaz del Software SketchUp empleado para el diseño tridimensional del laboratorio de telecomunicaciones y la planificación del espacio físico.

Tabla 11. *Características técnicas de SketchUp.*

Características	Descripción
Desarrollador	Originalmente Last Software (2000) y Google (2006).
Sistema operativo	Windows 10/11, macOS 11+ (Pro); Navegador web (Free/Go).
Análisis energético	Integración con Sefaira para evaluación energética de edificios.

Nota. Características técnicas de SketchUp: versión empleada, sistema operativo compatible, capacidades de modelado 3D y herramientas de diseño disponibles.

- **GNS3 (Graphical Network Simulator-3).**

Mediante la simulación se validó previamente el esquema de direccionamiento, evitando que un error de configuración se replicara directamente en los equipos reales, lo cual habría implicado reconfigurar varios módulos.

GNS3 permite simular el comportamiento de los dispositivos MikroTik con una fidelidad muy superior a la de los simuladores convencionales, ya que ejecuta el sistema operativo RouterOS real sobre máquinas virtuales, garantizando que los resultados obtenidos sean representativos del comportamiento esperado en la implementación física. [50].

En la Figura 13, se muestra un software gráfico de código abierto utilizado para diseñar y simular redes informáticas. Permite trabajar con equipos virtuales de fabricantes y en la Tabla 12 muestra sus características.

Figura 13. *GNS3 Graphical Network Simulator3).*

Nota. Programa ejecutable de GNS3 el proceso de diseño, implementación y validación de una arquitectura de red dinámica sobre el entorno de simulación GNS3.

Tabla 12. *Características técnicas de GNS3.*

Características	Descripción
Tipo de software.	Emulador/Simulador gráfico de redes – código abierto (Open Source).
Sistema operativo.	Windows 7/10/11 (64 bits), macOS, Linux (Ubuntu, Debian).
Fabricantes soportados.	Cisco, MikroTik, Juniper, Fortinet, Aruba, Arista, Vyatta, y más.
Integración con Wireshark.	Captura de tráfico directamente desde cualquier enlace de la topología.

Nota: Muestra las características técnicas de GNS3 versión utilizada, plataformas soportadas, tipos de emuladores compatibles y requerimientos del sistema para la simulación.

- **Winbox**

Es la interfaz gráfica oficial de MikroTik para la configuración y administración de dispositivos RouterOS. Durante toda la implementación WinBox v4, la versión multiplataforma compatible con Windows, que ofrece una interfaz renovada con mejor manejo de múltiples sesiones simultáneas [51].

En la Tabla 13 se muestran las características técnicas del programa y en la Figura 14 se muestra el diseño del programa.

Figura 14. *Herramienta gráfica de administración y gestión de RouterOS.*

Nota. Herramienta WinBox utilizada para la administración y gestión de los routers MikroTik mediante interfaz gráfica.

Tabla 13. *Características técnicas de Winbox.*

Desarrollador	**Winbox**
Versiones disponibles.	v3 (solo Windows, legada) / v4 (multiplataforma: Windows, macOS, Linux).
Sistemas operativos.	Windows 10/11 (v3 y v4), macOS 11+ (v4), Linux (v4).
Protocolo de conexión.	MAC-based (Winbox Protocol) o TCP/IP (dirección IP + puerto 8291).
Compatibilidad RouterOS.	RouterOS v6.x y v7x.
Monitoreo en tiempo real.	Tráfico por interfaz, uso de CPU/RAM, vecinos OSPF, DHCP, logs.

Nota: Características técnicas de WinBox: versión, sistemas operativos compatibles, protocolos de conexión soportados y funcionalidades principales de administración.

- **Wireshark**

Es el analizador de protocolos de red de código abierto más utilizado en el mundo; fue desarrollado como el primer analizador de protocolos open source con amplia aceptación en la comunidad de redes y telecomunicaciones. Permite capturar, inspeccionar y analizar el tráfico de datos que circula por una interfaz de red en tiempo real [52].

En la Figura 15, se muestra Wireshark, un analizador de protocolos de red que permite capturar, observar y estudiar los paquetes que circulan por una red en tiempo real. Dispone de filtros para localizar información específica y puede integrarse con GNS3 para analizar el tráfico de redes virtuales, por lo que es muy útil para detectar fallas. La Tabla 14, muestra sus características técnicas por una interfaz de red en tiempo real.

Figura 15. *Analizador de protocolos de red.*

Nota. Programa ejecutable, donde se muestra el tráfico de la red en tiempo real en cada puerto en los módulos A, B, C, D y E.

Tabla 14. *Características técnicas de Wireshark.*

Desarrollador original	**Wireshark**
Tipo de software.	Analizador de protocolos de red (sniffer / packet analyzer).
Sistemas operativos.	Windows, macOS, Linux, FreeBSD, Solaris y otros Unix.
Interfaz gráfica.	GTK+ / Qt (GUI multiplataforma).
Modo de captura.	Promiscuo (captura todo el tráfico del segmento) o no-promiscuo.
Filtros de captura.	Sintaxis BPF (Berkeley Packet Filter) – filtrado en tiempo de captura.

Nota. Características técnicas de Wireshark versión, plataformas compatibles, protocolos analizados, capacidades de filtrado y formatos de archivo de captura.

3.3. Arquitectura de la red implementada.

3.3.1. Diseño lógico del laboratorio.

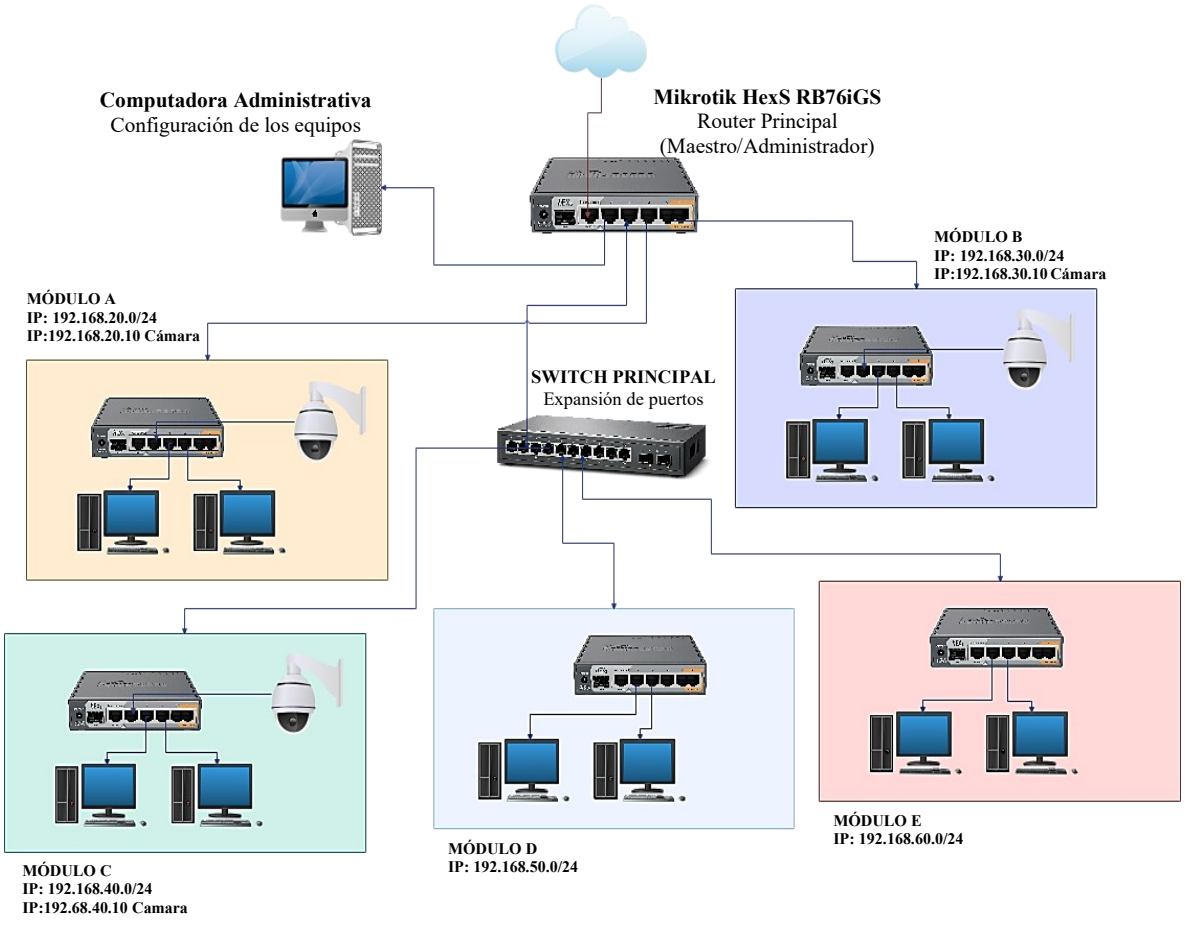
La topología implementada sigue un modelo híbrido extendido que combina dos estructuras complementarias: una topología en estrella para conectar los módulos subordinados al switch principal y al router administrador, y una estructura jerárquica que se extiende desde el módulo principal hacia los módulos A, B, C, D y E. Esta combinación permite centralizar la administración.

En la Figura 16 se muestra el router administrador, un MikroTik hEX S modelo RB760iGS. Este equipo constituye el núcleo de la arquitectura, ya que gestiona el tráfico entre segmentos de red, proporciona el servicio DHCP a los dispositivos que lo solicitan,

implementa las políticas de seguridad perimetral y participa en el proceso de enrutamiento dinámico mediante OSPF.

El switch principal, un MikroTik RB2011, actúa como equipo de distribución y amplía la disponibilidad de puertos para conectar los módulos C, D y E. Esta función resulta necesaria debido a que el MikroTik hEX S dispone de cinco puertos, uno de los cuales se utiliza como interfaz WAN. Los módulos A y B se conectan directamente a los puertos ether4 y ether5 del router administrador, mientras que los módulos C, D y E se conectan a través del switch principal.

Figura 16. *Esquema físico de las conexiones.*

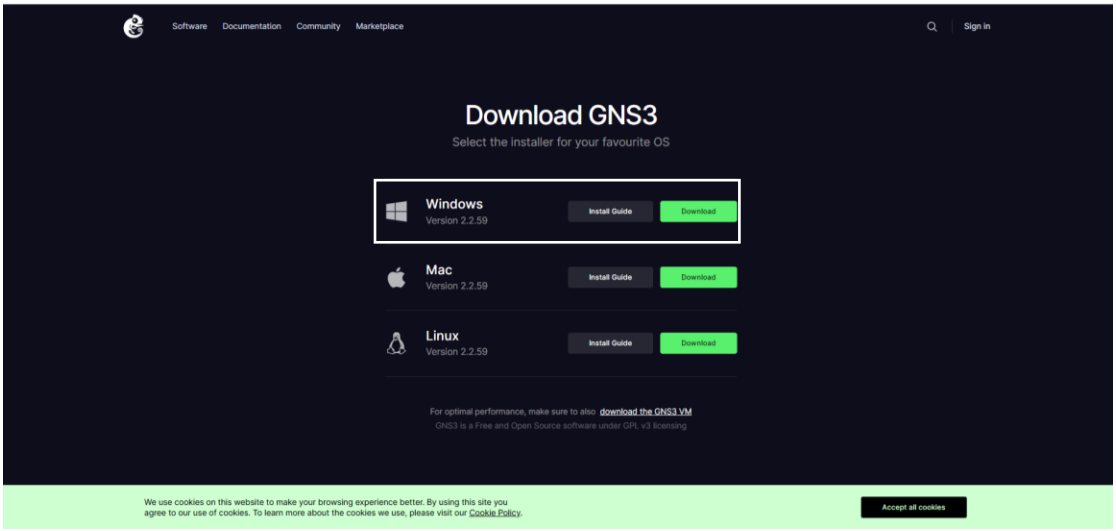


Nota. El equipo MikroTik HexS RB760iGS, que actúa como router maestro y es el cerebro de toda la red, a él se conecta también la PC Administrativa para gestionar los equipos. Desde el router baja al Switch Central, que multiplica los puertos disponibles para llegar a todos los módulos.

3.3.2. Diseño lógico en GNS-3.

Para diseñar la simulación utilizamos el programa GNS3. El primer paso que realicé fue descargar los archivos necesarios desde el sitio oficial; para esto se abrió el navegador oficial de la página: https://www.gns3.com/software/download. En la Figura 17 se muestra la ventana de instalación del programa.

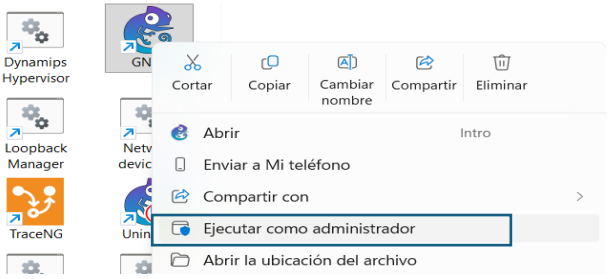
Figura 17. *Instalador principal del cliente GNS3 para Windows.*



Nota. Ventana del instalador principal del cliente GNS3 para sistemas Windows, con los componentes disponibles para la instalación.

Una vez que los archivos terminaron de descargarse, instalé en el escritorio de GNS3. Ubiqué el archivo "*GNS3-all-in-one.exe"* en mi carpeta de descargas; lo ejecuté con doble clic, como se muestra en la Figura 18.

Figura 18. *Archivo descargado en GNS3.*



Nota. Archivo de instalación descargado de GNS3, previo a la ejecución del proceso de instalación en el entorno de simulación.

Cuando el sistema pregunta si deseaba permitir que el programa hiciera cambios en el dispositivo, hice clic en *"Sí"* para continuar. Se abre el asistente de instalación (Setup Wizard), leemos los términos de la licencia y al estar de acuerdo, hice clic en "I Agree".

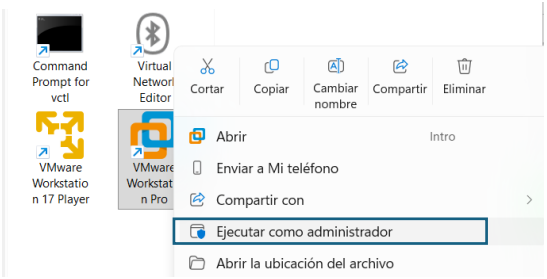
En la Figura 19, se muestra en segundo plano la instalación de GNS3 VM en VMware; componente fundamental, que es una máquina virtual preconfigurada que permite ejecutar dispositivos con mayor rendimiento que el modo local.

Figura 19. *Máquina virtual de GNS3 para VMware.*

Nota. Configuración de la máquina virtual de GNS3 para VMware, necesaria para la ejecución de imágenes de dispositivos de red en el simulador.

Elegimos una carpeta de destino fácil de localizar, como el escritorio, y extraje el contenido; al finalizar, encontré dentro un archivo con extensión que es el formato de imagen de máquina virtual. En la Figura 20 se muestra el ejecutable del programa.

Figura 20. *Ejecutamos el programa.*

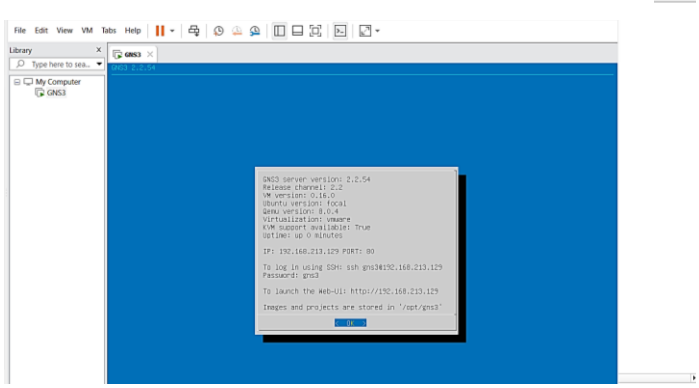


Nota. Ejecución del programa GNS3 mostrando la interfaz inicial del simulador lista para comenzar la configuración de la topología de red.

En la pantalla principal, seleccioné la opción "Open a Virtual Machine" VMware me mostró los detalles de la máquina virtual a importar. Hice clic en "Import" para iniciar el proceso con el programa GNS3 VM en ejecución; el siguiente paso fue configurar el cliente de escritorio para que se comunicara correctamente con la máquina virtual.

En la Figura 21, se observa el importado; GNS3 VM apareció en mi lista de máquinas virtuales. La inicié haciendo clic en "Play virtual machine" la máquina virtual arrancó y mostró en pantalla su dirección IP local, la cual necesitaré para conectarla con el cliente de GNS-3.

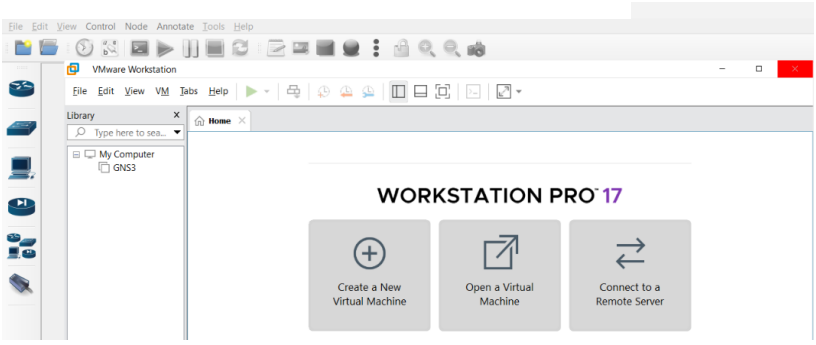
Figura 21. *Instalación de GNS3 y VMware.*



Nota. Se ve el proceso de instalación conjunta de GNS3 y VMware Workstation, integrando el motor de virtualización con el simulador de red.

Al terminar el asistente, la interfaz principal de GNS3 quedó lista para su uso y desarrollo del programa. Pude observar en la Figura 22, la pantalla que el estado de la GNS3 VM aparecía como *"Connected"* lo que confirmó que la instalación fue exitosa.

Figura 22. *Instalación completa del programa.*

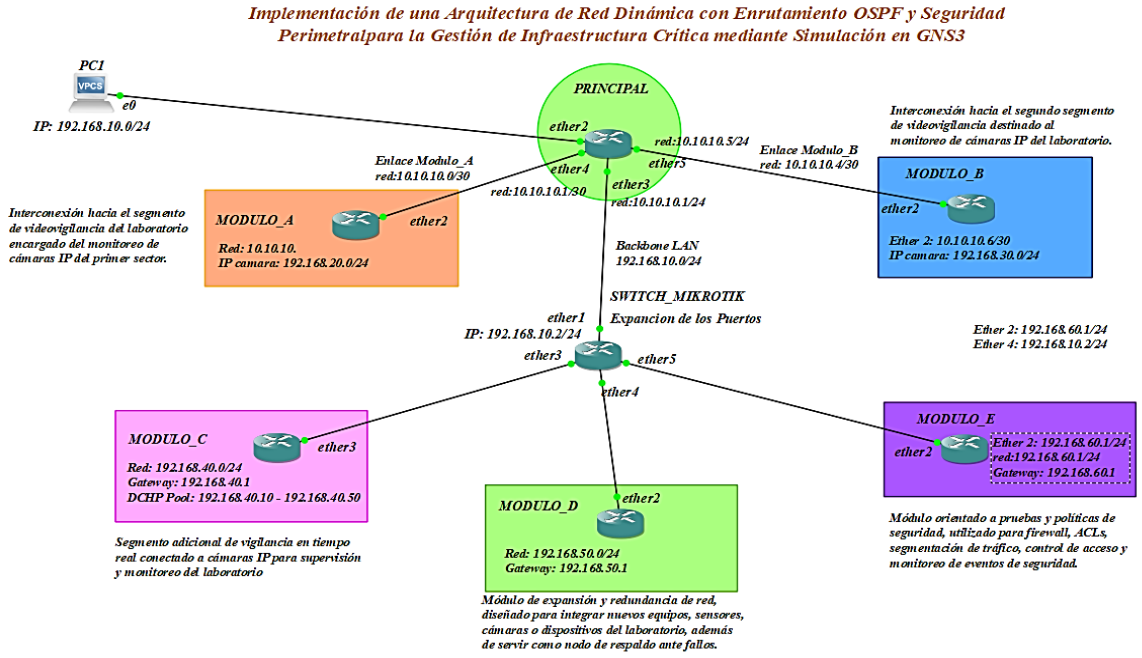


Nota. Interfaz de inicio de VMware Workstation, mostrando las opciones para crear, abrir o conectarse a una máquina virtual.

La topología implementada sigue un modelo híbrido extendido, en el cual un enrutador MikroTik actúa como núcleo principal de la red y concentra la comunicación hacia los demás segmentos a través de un switch configurado en modo bridge switch.

En la Figura 23, se ve que la arquitectura se divide en siete módulos (módulo principal, el switch, módulo a, módulo b, módulo c, módulo d, módulo e) con roles claramente diferenciados, cada uno orientado a una función específica dentro de la red.

Figura 23. *Simulación en GNS3.*



Nota. Lista de la simulación de la topología de red en GNS3, representando la arquitectura diseñada con los módulos MikroTik interconectados.

La Tabla 15, se muestra la descripción en direcciones IP del programa GNS3 en su ejecutable función de cada módulo implementado en la red.

Tabla 15. *Descripción Funcional de los Módulos.*

Módulo	Red	Función
MÓDULO A	192.168.20.0/24	Videovigilancia zona 1 — cámaras del primer sector.
MÓDULO B	192.168.30.0/24	Videovigilancia zona 2 — cámaras del laboratorio.
MÓDULO C	192.168.40.0/24	Videovigilancia en tiempo real + servidor DHCP (reparte IPs del .10 al .50).

MÓDULO D	192.168.50.0/24	Expansión y respaldo — para nuevos equipos o nodo de redundancia.
MÓDULO E	192.168.60.0/24	Seguridad perimetral — firewall, ACLs, control de acceso y monitoreo.

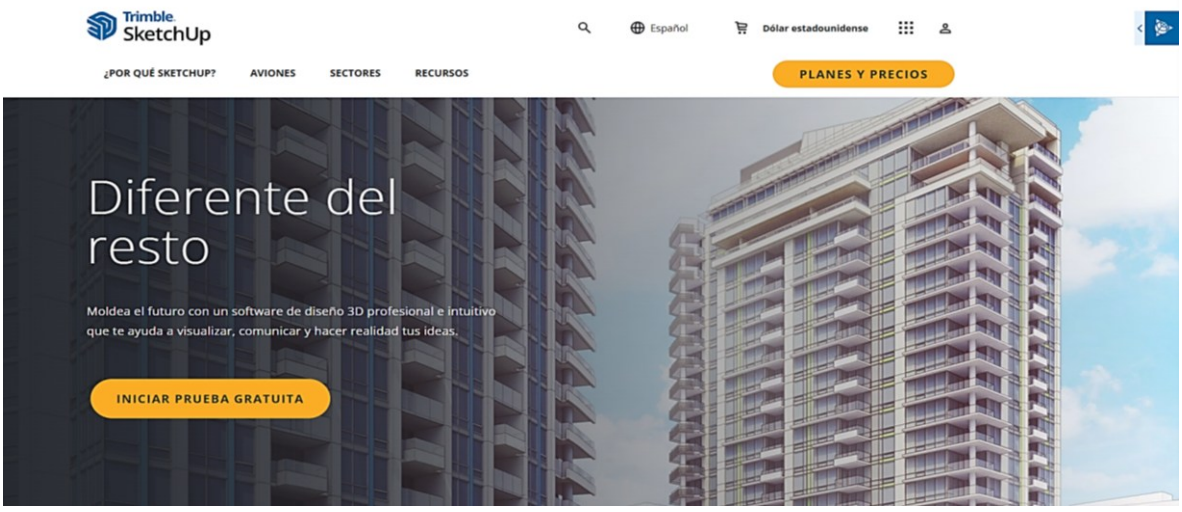
Nota. Descripción funcional de los cinco módulos de la arquitectura, detallando el propósito, segmento IP asignado y equipos conectados a cada uno.

3.3.3. Diseño implementado en SketchUp.

Para el desarrollo del presente proyecto, se diseñó un escenario físico correspondiente al laboratorio de telecomunicaciones, cuya distribución fue modelada mediante el software SketchUp 2026, herramienta que permitió representar de manera tridimensional la organización y disposición de los elementos que conforman el entorno de trabajo.

En la Figura 24, se muestra la instalación del software; se ejecuta un navegador web y se acceder al sitio oficial de SketchUp, disponible en la dirección electrónica: https://sketchup.trimble.com/en/download/all. Una vez ingresado al sitio oficial, se localiza la sección de descargas y se selecciona la versión SketchUp Studio

Figura 24. *Imagen generada por el programador.*

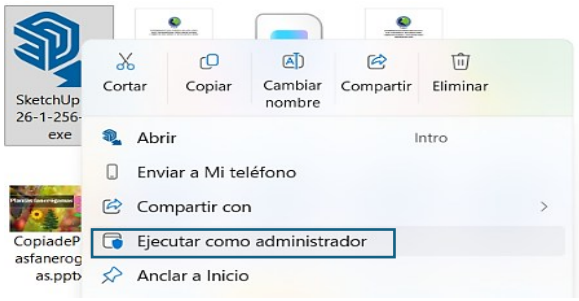


Nota. Se muestra la ventana de navegación de la página oficial de Sketchup para la implementación del proyecto.

Al finalizar la descarga, se dirige a la carpeta donde fue almacenado el archivo instalador y se ejecuta haciendo doble clic sobre él. En el sistema operativo Windows 11

puede solicitar permisos de administrador, ante lo cual se selecciona la opción *"Sí"* para continuar con el proceso; así se muestra en la Figura 25.

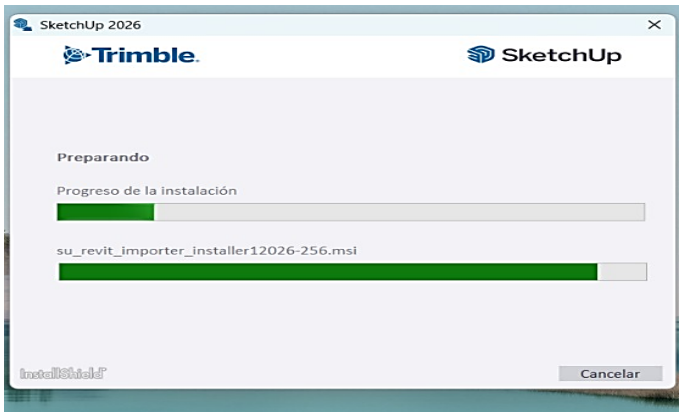
Figura 25. *Imagen generada por el programador.*



Nota. Archivo de instalación de SketchUp descargado desde el sitio oficial, listo para ejecutar el proceso de instalación en el equipo.

Una vez iniciado, se aceptan los términos y condiciones de uso del software y se selecciona la ruta de instalación deseada en el equipo. Una vez finalizada la instalación, se hace clic en *"Finalizar"* para cerrar el asistente que se muestra en la Figura 26.

Figura 26. *Instalación de programa en el ordenador.*

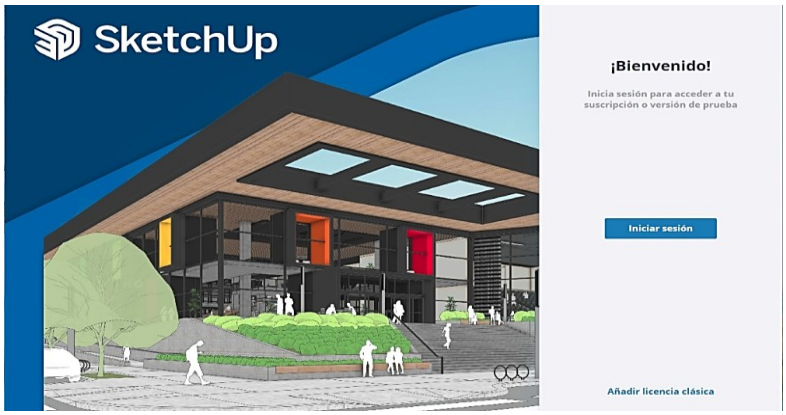


Nota. Proceso de instalación de SketchUp en el ordenador, mostrando las opciones de configuración del asistente de instalación.

Una vez iniciado el asistente de instalación, se aceptan los términos y condiciones de uso del software y se selecciona la ruta de instalación deseada en el equipo; se recomienda mantener la ruta predeterminada sugerida por el instalador.

En la fFgura 27 se muestra la finalización de la instalación; se hace clic en *"Finalizar"* para cerrar el asistente. A continuación, se abre SketchUp Studio desde el acceso directo creado en el escritorio o desde el menú de inicio de Windows 11.

Figura 27. *Programador instalado.*

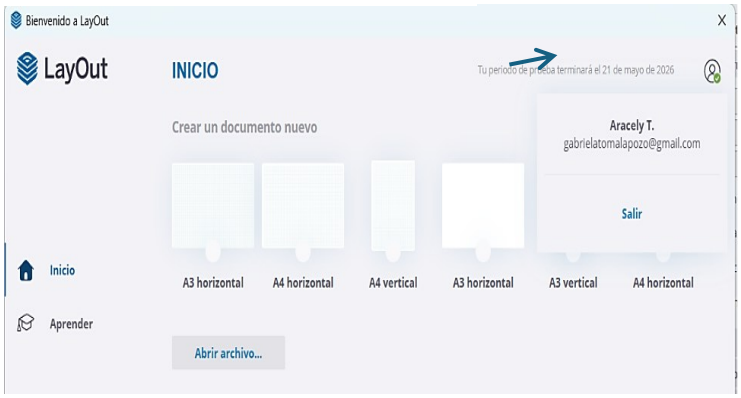


Nota. Programa de instalación de SketchUp en el ordenador, mostrando las opciones de configuración del asistente.

Al ejecutar el programa por primera vez, se solicita iniciar sesión con una cuenta de Trimble o crear una nueva; se ingresan las credenciales correspondientes para activar la licencia de SketchUp Studio y acceder a todas las funcionalidades del software.

En la Figura 28, se visualiza la interfaz de SketchUp con la sesión iniciada, mostrando el entorno de trabajo 3D donde se realizó el diseño del laboratorio.

Figura 28. *Sesión iniciada en el programa SketchUp.*



Nota. Para instalar LayOut, primero se descarga el instalador oficial de SketchUp correspondiente al sistema operativo.

El Laboratorio de Telecomunicaciones fue elaborado mediante el software SketchUp Studio 2026, herramienta que permitió representar de manera detallada la distribución física y funcional de los elementos que conforman el escenario de trabajo.

Como se puede observar en la Figura 29, en el laboratorio los tableros se clasifican en siete módulos de trabajo, denominados de la siguiente manera: módulo A, módulo B, módulo C, módulo D, módulo E y el módulo principal junto con el switch, siendo este último el encargado de gestionar y coordinar las actividades de los demás módulos durante el desarrollo de las prácticas.

Figura 29. *Implementación del diseño del laboratorio de telecomunicaciones.*

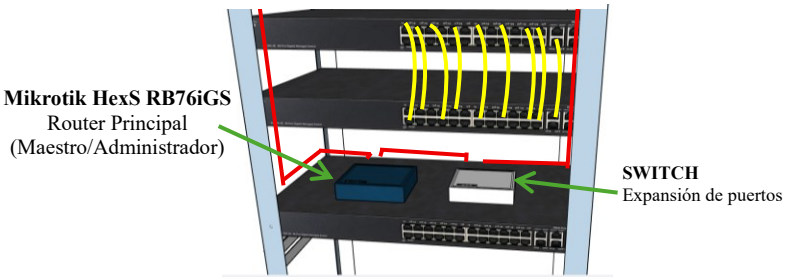
Nota. Se muestra el diseño 3D del laboratorio de telecomunicaciones implementado en SketchUp, con la distribución de los equipos y el espacio físico.

3.3.4. Estructura y función del administrador.

El Módulo principal constituye el núcleo central de administración y gestión de la red del laboratorio de telecomunicaciones; este se encuentra conformado por tres elementos fundamentales que trabajan de manera conjunta para garantizar la conectividad, el control y la administración de toda la infraestructura de red.

En la Figura 30, se muestra el flujo de conexión del switch principal; se describe de la siguiente manera: router principal mikroTik hEX S RB760iGS, switch principal MikroTik RB750Gr3 → Módulo C, Módulo D, Módulo E.

Figura 30. *Ubicación de Router Administrador.*



La Tabla 16, se muestra la distribución de puertos del router principal que organiza la comunicación de la topología híbrida.

Tabla 16. *Especificaciones de puertos del router principal.*

Puertos	Función	Descripción
SFP	Reservado / Expansión futura.	Sin conexión en esta implementación disponible para futuras ampliaciones mediante fibra óptica o enlaces de alta velocidad.
Ethernet 1	Entrada WAN / Internet.	Recibe la conexión del proveedor ISP. Configurado como interfaz WAN para acceso externo y salida a Internet.
Ethernet 2	Administración.	Equipo central de administración y enrutamiento encargado de la gestión de tráfico, segmentación de red, balanceo de carga, políticas de seguridad y comunicación entre todos los módulos de la topología híbrida extendida.
Ethernet3	Switch principal.	Dispositivo de conmutación encargado de ampliar la cantidad de puertos disponibles y centralizar la interconexión entre el MikroTik principal y los módulos C, D y E dentro de la arquitectura híbrida extendida.
Ethernet 4	Enlace Módulo A.	Interconexión hacia el Módulo A, encargado del monitoreo de cámaras IP del primer segmento del laboratorio.
Ethernet 5	Enlace Módulo B.	Interconexión hacia el Módulo B, destinado al monitoreo de cámaras IP del segundo segmento del laboratorio.

Nota. Se muestra las especificaciones de los puertos del router administrador asignación de interfaces, segmentos IP configurados y función de cada puerto en la red.

- **Distribución de los puertos del Switch.**

La Tabla 17, se muestran los puertos del switch que actúa como concentrador central de la red, encargado de interconectar el router MikroTik principal con los distintos módulos del laboratorio; permite la segmentación y distribución del tráfico de datos hacia cada segmento de red de forma ordenada y eficiente.

Tabla 17. *Switch Distribución de puertos.*

Puertos	Función	Descripción
Puerto 1	Enlace al MikroTik principal	Conectado al MikroTik principal.
Puerto 2	Disponible	Sin conexión en esta implementación. Disponible para futuras amplificaciones.
Puerto 3	Enlaces Módulo C	Nodo secundario activo conectado a una cámara IP para monitoreo en tiempo real de un área adicional del laboratorio. Se integra a la arquitectura dinámica mediante OSPF y DHCP, con políticas de seguridad aplicadas a través de Firewall y ACLs.
Puerto 4	Enlaces Módulo D	Módulo de expansión y redundancia de red, diseñado para integrar nuevos equipos, sensores, cámaras o dispositivos del laboratorio, además de servir como nodo de respaldo ante fallos de otros módulos.
Puerto 5	Enlaces Módulo E	Destinado a pruebas de firewall, ACLs, control de acceso, segmentación de tráfico y monitoreo de eventos de seguridad. Permite validar políticas de red en un entorno controlado antes de aplicarlas en producción

Nota. Distribución de puertos del switch principal asignación de cada interfaz a los módulos y dispositivos de la infraestructura del laboratorio.

La Tabla 18, presenta el esquema de direccionamiento IP asignado a los cinco módulos (A–E) de la red. Para cada módulo se detalla: la IP del enlace punto a punto OSPF configurada en el propio módulo y su contraparte en el mikroTik principal.

Tabla 18. *Direcciones IP de los módulos A hasta el módulo E.*

Módulo	IP de enlace OSPF del módulo	IP del MikroTik Principal	Red interna del módulo	Gateway del módulo	Cámara IP
Módulo A	10.10.10.2/30	10.10.20.1/30	192.168.10.0/24	192.168.10.1	192.168.20.10
Módulo B	10.10.10.6/30	10.10.20.5/30	192.168.20.0/24	192.168.20.1	192.168.30.10
Módulo C	10.10.20.14/30	10.10.20.13/30	192.168.50.0/24	192.168.50.1	192.168.40.10
Módulo D	10.10.30.14/30	10.10.10.13/30	192.168.40.0/24	192.168.40.1	No aplica
Módulo E	10.10.20.10/30	10.10.20.9/30	192.168.60.0/24	192.168.60.1	No aplica

Nota: Se muestra las redes de los módulos A, B, C, D y E en el punto de enlace a la red.

La tabla 19, se muestras las cámaras IP de los módulos A, B y C utilizan direcciones estáticas dentro de redes independientes. Cada cámara se comunica mediante la puerta de enlace correspondiente a su módulo, lo que permite enviar el tráfico hacia otras redes y hacia el MikroTik principal.

Tabla 19. *Segmentación de cámaras IP.*

Cámara	Módulo	Dirección IP	Gateway
Cámara Módulo A	Módulo A	192.168.20.10	192.168.20.1
Cámara Módulo B	Módulo B	192.168.30.10	192.168.30.1
Cámara Módulo C	Módulo C	192.168.40.10	192.168.40.1

Nota. Se muestran las direcciones IP de las cámaras asignadas en cada módulo A, módulo B, módulo C.

- **Distribución de las redes por segmento del laboratorio.**

La Tabla 20 se muestra la administración principal, mientras que cada módulo cuenta con su propia red y puerta de enlace. Esta organización reduce el tráfico innecesario, facilita la identificación de los dispositivos y mejora el control, la seguridad y el enrutamiento entre los distintos módulos.

Tabla 20. *Segmentación general de la red.*

Segmento	Red	Máscara	Gateway	Uso principal
Red de administrativa	192.168.10.0/24	255.255.255.0	192.168.10.1	Administración del MikroTik principal, PC de gestión y acceso a la red.
Módulo A	192.168.20.0/24	255.255.255.0	192.168.20.1	Dispositivos del módulo A y cámara IP.
Módulo B	192.168.30.0/24	255.255.255.0	192.168.30.1	Dispositivos del módulo B y cámara IP.
Módulo C	192.168.40.0/24	255.255.255.0	192.168.40.1	Dispositivos del módulo C y cámara IP.
Módulo D	192.168.50.0/24	255.255.255.0	192.168.50.1	Dispositivos del módulo D.
Módulo E	192.168.60.0/24	255.255.255.0	192.168.60.1	Dispositivos del módulo E

Nota. Se muestra la segmentación IP de la arquitectura implementada subredes asignadas a cada módulo con su máscara de red, gateway predeterminado y rango de hosts disponibles.

La Tabla 21, se muestran los enlaces entre el MikroTik principal y los módulos A, B, C, D y E que utilizan redes con direcciones IP. Esta distribución aprovecha eficientemente las direcciones disponibles, evita conflictos y permite establecer conexiones punto a punto para el intercambio de rutas mediante OSPF.

Tabla 21. *Segmentación de enlaces OSPF.*

Enlace	Router ID	Dirección vecina	Adyacente
Módulo A.	2.2.2.2	10.10.20.10	Establecida
Módulo B.	5.5.5.5	10.10.20.6	Establecida

Módulo C.	3.3.3.3	10.10.20.14	Establecida
Módulo D.	4.4.4.4	10.10.30.14	Establecida
Módulo E.	6.6.6.6	10.10.20.10	Establecida

Nota. Se ve las direcciones de enlaces OSPF en un punto a punto para la comunicación del MikroTik administrador en cada módulo.

3.3.5. Ubicación y etiquetados.

El etiquetado de la infraestructura de red implementada en el laboratorio de telecomunicaciones se rige bajo la normativa ANSI/TIA-606-C, la cual establece los requisitos mínimos para la identificación y administración de la infraestructura.

Esta normativa define un sistema de etiquetado jerárquico que permite identificar de manera única cada elemento físico y lógico de la red, incluyendo puertos, enlaces, equipos y módulos, garantizando la estabilidad de las conexiones y facilitando las tareas de mantenimiento, expansión y resolución de problemas.

- **Módulo A (Videovigilancia Zona 1).**

El Módulo A corresponde al nodo de videovigilancia del primer segmento del laboratorio; sus puertos están etiquetados conforme a la función que cada enlace cumple dentro de la arquitectura OSPF implementada, justificando la asignación física de cada conexión.

La Tabla 22, se muestran las características y la descripción del módulo A, la configuración de puertos a una arquitectura funcional orientada a la escalabilidad y segmentación del tráfico.

Tabla 22. *Características de los puertos asignados al módulo A.*

Puerto	Etiqueta (TIA-606-C)	Dirección IP	Función	Descripción/Justificación
SFP	N/A	Reserva	Expansión	Puerto disponible para futuras ampliaciones de la red.
Ether1	MOD-A	10.10.10.2/30	Enlace OSPF.	Comunicación entre el Módulo A con en MikroTik principal.

Ether2	MOD-A-CAM1	192.168.20.0/24	Acceso de la cámara.	Puerto interno donde se conecta la cámara IP del primer sector, recibiendo dirección dentro del segmento.
Ether3	MOD-A	10.10.10.2.30	Reservado	Reservado para conectar una computadora de mantenimiento y realizar tareas de configuración o diagnóstico.
Ether4	MOD-A	192.168.20.0/24	Red interna.	Reservado para conectar una computadora de mantenimiento y realizar tareas de configuración o diagnóstico.
Ether5	MOD-A-LAN-[2–4]	192.168.20.0/24	Expansión del módulo.	Puerto destinado a la integración futura de sensores, dispositivos IoT o equipos adicionales.

Nota. Se detallan los puertos del equipo asignado al primer segmento de videovigilancia para cada interfaz, su etiqueta según la norma ANSI/TIA-606-C, la dirección IP asignada.

- **Módulo B (Videovigilancia Zona 2).**

El Módulo B gestiona el segundo segmento de videovigilancia del laboratorio; la conexión al enrutador principal se realiza mediante ether2 como enlace; los puertos internos se agrupan en un bridge para la LAN de cámaras IP.

La Tabla 23, se muestran los puertos del módulo B junto con las direcciones IP en cada descripción que se va a realizar.

Tabla 23. *Características de los puertos asignado al módulo B.*

Puerto	Etiqueta (TIA-606-C)	Dirección IP	Función	Descripción / Justificación
SFP	MOD-B-SFP1	N/A	Fibra óptica (Reserva).	Puerto disponible para futuras implementaciones de enlaces de alta velocidad mediante fibra óptica.
Ether1	MOD-B	192.168.20.1/24	Enlace ascendente hacia el Router Maestro.	Permite la integración del módulo B con la red de distribución del laboratorio, facilitando la comunicación.

Ether2	MOD-B-CAM1	10.10.10.6/30	Enlace OSPF hacia el MikroTik Principal.	Puerto destinado al intercambio dinámico de rutas mediante OSPF, permitiendo la comunicación entre el Módulo B y el Router Principal.
Ether3	MOD-B	192.168.30.0/24	Cámara IP.	Conexión de la segunda cámara IP implementada en el laboratorio para las pruebas de videovigilancia y monitoreo del tráfico de red.
Ether4	MOD-B	192.168.30.0/24	PC de monitoreo.	Conexión de un equipo de monitoreo encargado de visualizar y administrar la cámara IP del segundo segmento.
Ether5	MOD-B	192.168.30.0/24	Expansión.	Puerto reservado para la integración futura de dispositivos adicionales o nuevas pruebas de laboratorio.

Nota. Se implementa una arquitectura escalable y de administración dinámica, donde el enlace ascendente se establece mediante DHCP hacia el router administrador.

- **Módulo C (Vigilancia con OSPF y DHCP).**

El Módulo C integra una cámara IP con políticas de seguridad mediante firewall y ACLs; sus interfaces fueron renombradas funcionalmente para reflejar su rol dentro del bridge local, siguiendo la nomenclatura de la ANSI/TIA-606-C.

La Tabla 24, se observan las características y las funciones del módulo C.

Tabla 24. *Características de los puertos asignado al módulo C.*

Puerto	Etiqueta (TIA-606-C)	Dirección IP	Función	Descripción / Justificación
Ether1	MOD-C	N/A	Reserva	Puerto disponible para futuras ampliaciones o nuevos dispositivos.
Ether2	MOD-C CAM1	192.168.40.0/24	Cámara IP de monitoreo.	Puerto directo para la cámara IP del área adicional. Las

				ACLs y el firewall del módulo restringen el tráfico no autorizado hacia este segmento.
Ether3	MOD-C-UPLINK	Asignada por (segmento) 10.10. 10.10/30	Enlace de distribución.	Conecta el módulo C al puerto 3 del switch principal estado activo garantiza la integración automática del módulo en la arquitectura dinámica.
Ether4	MOD-C	192.168.40.0/24	Gateway del bridgeLocal.	Destinado a la incorporación de equipos adicionales de monitoreo o administración.
Ether5	MOD-C-LAN- [2–4]	192.168.40.0/24	Reservado / Expansión.	Puertos libres dentro del bridgeLocal, disponibles para futuras ampliaciones del segmento de vigilancia o integración de nuevos dispositivos.

Nota. Es el direccionamiento dinámico mediante un enlace de distribución basado en DHCP, garantizando su integración automática con la infraestructura principal

- **Módulo D (Expansión y Redundancia).**

El Módulo D opera con direccionamiento estático, lo que garantiza su identificación permanente dentro de la infraestructura. Su enlace al switch central se realiza por ether2 conectado al puerto 4 del Switch Principal.

La Tabla 25, se observan las características del módulo D junto con los puertos y la descripción de cada una de ellas.

Tabla 25. *Características de los puertos asignado al módulo D.*

Puerto	**Etiqueta (TIA-606-C)**	**Dirección IP**	**Función**	**Descripción / Justificación**
Ether1	MOD-D	192.168.60.2/24	Red de Enrutamiento	Red utilizada para el intercambio de rutas dinámicas entre el módulo D y el principal.

Ether2	MOD-D	10.10.10.14/30	Enlace OSPF	Comunicación punto a punto con el mikroTik principal mediante OSPF.
Ether3	MOD-D	192.168.50.0/24	Gateway LAN	Puerta de enlace de la red local del módulo D.
Ether4	MOD-D	192.168.50.0/24	Reserva	Puerto disponible para futuras ampliaciones o nuevos dispositivos.
Ether5	MOD-D	192.168.40.0/24	Segmento de usuarios.	Red destinada para la conexión de nuevos equipos, cámaras, sensores y dispositivos de expansión.

Nota. Proporcionando un punto de conexión estable y permanente con la red principal. La configuración del bridge_D utiliza la dirección 192.168.60.2 como puerta de enlace predeterminada y el servicio DNS externo 8.8.8.8 para la resolución de nombres, eliminando la dependencia de mecanismos de asignación dinámica

- **Módulo E (Seguridad y Pruebas).**

El Módulo E está destinado a la validación de políticas de seguridad: pruebas de firewall, ACLs, control de acceso y segmentación de tráfico. Su etiquetado refleja esta función diferenciada dentro de la arquitectura híbrida extendida.

La Tabla 26, se observan las funciones a las que está destinado el módulo E, junto con las descripciones y características.

Tabla 26. *Características de los puertos asignado al módulo E.*

Puerto	Etiqueta (TIA-606-C)	Dirección IP	Función	Descripción / Justificación
Ether1	MOD-E	N/A	Enlace de distribución.	Puerto disponible para futuras expansiones o conexión de dispositivos adicionales.
Ether2	MOD-E	10.10.10.18/30	Equipos de prueba / PC. de monitoreo	Conecta el módulo E al puerto 5 del switch principal, permitiendo la validación de políticas de firewall, ACLs y segmentación de tráfico.

Ether3	MOD-E	192.168.60.0/24	Gateway del segmento.	Pruebas de ACLs, control de acceso y monitoreo de eventos de seguridad, permitiendo validar configuraciones sin afectar el resto de la infraestructura.
Ether4	MOD-E	192.168.60.0/24	Reservado	Puerto no utilizado en la implementación actual.
Ether5	MOD-E	192.168.60.0/24	Reservado	Puerto no utilizado en la implementación actual.

Nota: Se ha diseñado como un entorno de pruebas y validación de seguridad dentro de la arquitectura de red, operando sobre el segmento. La dirección se establece como puerta de enlace, permitiendo la centralización del monitoreo y la gestión de eventos de seguridad.

El sistema de etiquetado aplicado garantiza que cada puerto y enlace de la infraestructura pueda ser identificado, verificado y documentado de forma indiscutible, cumpliendo con los requisitos establecidos por la normativa ANSI/TIA-606-C y facilitando las tareas de operación, mantenimiento y expansión del laboratorio de telecomunicaciones.

3.3.6. Módulos y redes.

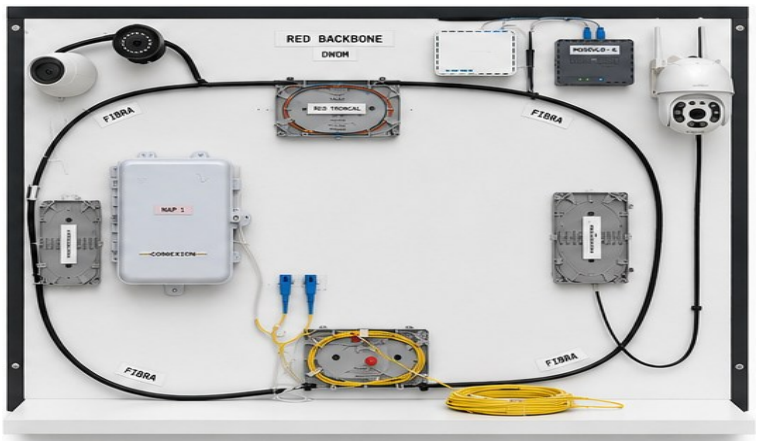
- **Tablero 1 y Módulo A.**

El módulo A opera bajo el protocolo de enrutamiento dinámico OSPF, configurado con un Router ID, IP de enlace, Gateway/LAN y red OSPF. Este protocolo de enlace permite el intercambio automático de tablas de enrutamiento entre los routers del laboratorio, calculando la ruta más eficiente, lo que asegura una distribución óptima del tráfico y una convergencia rápida ante cualquier cambio en la topología.

Adicionalmente, mediante el monitoreo de las interfaces del módulo A, se supervisa en tiempo real el tráfico generado por las cámaras IP del primer segmento, asegurando la disponibilidad, estabilidad y seguridad de toda la infraestructura de red del laboratorio.

En la Figura 31, se muestra el diseño tridimensional del Módulo A, elaborado mediante el software SketchUp 3D; este modelo permite visualizar la distribución física de los equipos de red, el sistema de cableado y la ubicación de los dispositivos.

Figura 31. *Módulo A.*



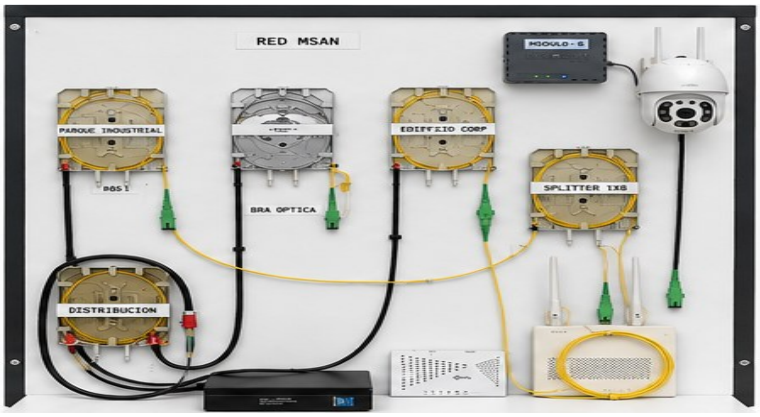
Nota. Dentro de tu arquitectura de red dinámica con OSPF, el módulo A cumple la función de uno de los nodos remotos de la topología, integrado al router principal mediante un enlace y anunciado dinámicamente por OSPF.

- **Tablero 2 y Módulo B.**

El Módulo B está configurado como un nodo de red independiente dentro del laboratorio, con el propósito específico de gestionar el segmento de cámaras IP y videovigilancia. En su estructura interna se configura un bridge que forma la red local donde se conectan las cámaras IP y demás equipos del segmento.

En la Figura 32, el diseño 3D del módulo B, elaborado permite visualizar la distribución física de los equipos de red, el sistema de cableado y la ubicación de los dispositivos.

Figura 32. *Módulo B.*



Nota: El Módulo B permite verificar el correcto enrutamiento dinámico entre nodos, la estabilidad de la comunicación bajo el esquema OSPF implementado, y el comportamiento de redirección de tráfico dentro de la topología, aportando evidencia empírica al desempeño general de la arquitectura de red diseñada.

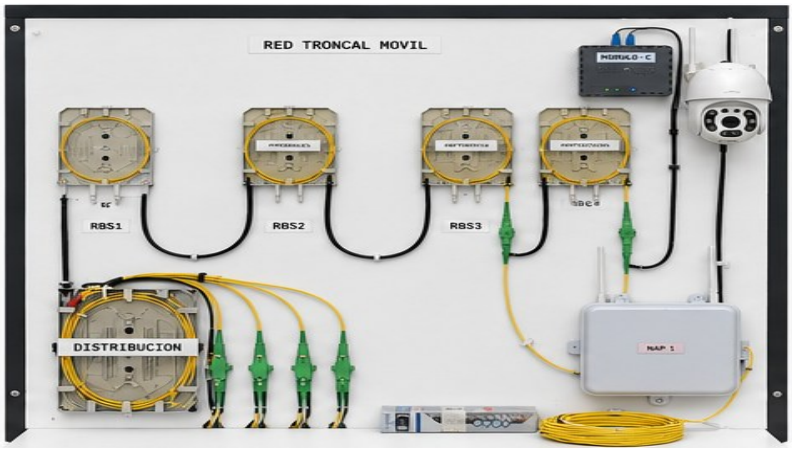
- **Tablero 3 y Módulo C.**

El módulo C está dentro de la red del laboratorio con el propósito de crear un segmento dedicado a la vigilancia, integrando una cámara IP que permite el monitoreo en tiempo real de las instalaciones.

Para lograr que el módulo C cumpla con su función, se integró la interfaz renombrada para facilitar su administración, la configuración interna del módulo que agrupa todos los puertos bajo una misma red local, garantizando la comunicación fluida entre los dispositivos conectados entre ellos. Además, se habilitó un cliente DHCP para que el módulo reciba direccionamiento IP automáticamente al conectarse al switch principal.

En la Figura 33, El Módulo C, nos permite visualizar la distribución física de los equipos de red, el sistema de cableado y la ubicación de los dispositivos.

Figura 33. *Módulo C.*



Nota. El Módulo C cumple un doble propósito dentro de la arquitectura de nodo remoto con su propio segmento de dispositivos finales; sirvió como caso de estudio práctico para demostrar la capacidad de diagnóstico y corrección de fallas de enrutamiento dinámico, evidenciando cómo un error de configuración en el router principal.

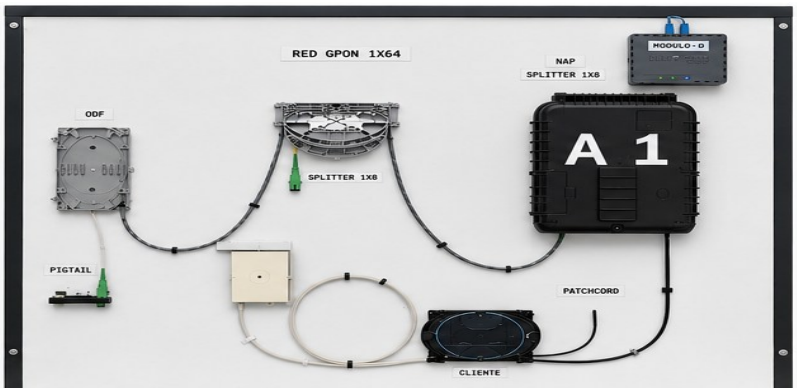
- **Tablero 4 y Módulo D.**

El módulo D fue implementado como un nodo de red autónomo dentro del laboratorio; para facilitar su reconocimiento dentro de la arquitectura general, la conexión hacia la red principal se establece a través del puerto ether2, enlazado directamente al puerto ether4 del switch central, integrando dentro del módulo.

Este puerto actúa como el punto de entrada y salida del tráfico entre el módulo y el resto de los segmentos de red, permitiendo que todos los dispositivos conectados al módulo compartan el mismo segmento de comunicación de forma ordenada y centralizada.

En la Figura 34, el módulo D, es la distribución física de los equipos de red, el sistema de cableado y la ubicación de los dispositivos.

Figura 34. *Módulo D.*



Nota. El módulo D cumple el rol de nodo remoto dentro de la arquitectura OSPF, validando la correcta propagación de rutas dinámicas hacia un segmento con direccionamiento.

- **Tablero 5 y Módulo E.**

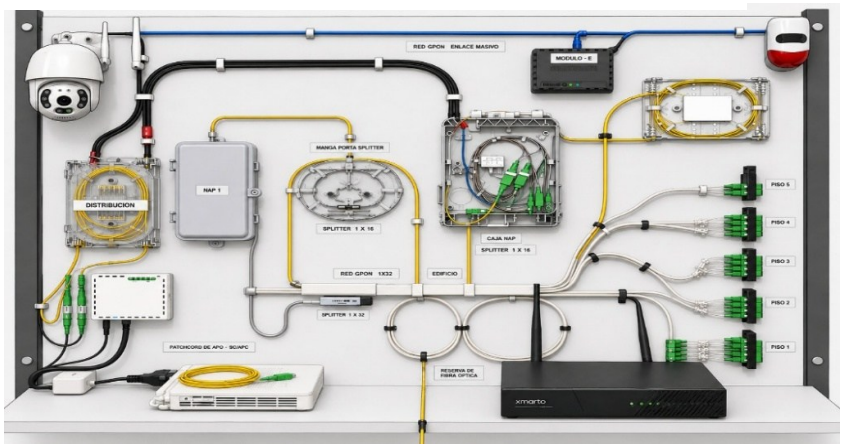
El módulo E está destinado a las pruebas de firewall, listas de control de acceso (ACL), segmentación de tráfico y monitoreo de eventos de seguridad; funciona como un entorno de laboratorio aislado dentro de la infraestructura de red.

Su principal objetivo es permitir la configuración y evaluación de políticas de seguridad, verificando el comportamiento del tráfico y detectando posibles vulnerabilidades antes de que dichas configuraciones sean implementadas en la red operativa. De esta manera, se minimizan los riesgos de interrupción del servicio y se garantiza una mayor estabilidad en la infraestructura.

La implementación de este módulo permite llevar a cabo pruebas, filtrado de paquetes y validación de reglas de seguridad en un entorno controlado, donde es posible simular diferentes escenarios de operación y ataques informáticos.

En la Figura 35, se muestra la seguridad y la capacidad de administración de la red ante futuros requerimientos tecnológicos. Su diseño escalable permite incorporar nuevos dispositivos.

Figura 35. *Módulo E.*



Nota. Cumple una función diferenciada dentro de la arquitectura: además de operar como nodo remoto de la topología, es el módulo destinado a las pruebas de seguridad perimetral (firewall, ACLs, segmentación y bloqueo de tráfico).

3.4. Software Winbox diseño de los módulos.

El presente capítulo describe el procedimiento de implementación de una arquitectura de red dinámica en el Laboratorio de Telecomunicaciones, utilizando equipos MikroTik hEX S configurados a través de la herramienta WinBox.

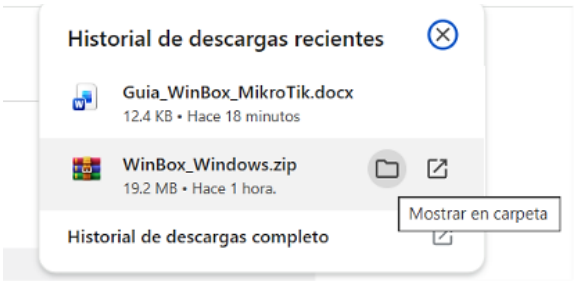
Para poder comenzar a trabajar con el programa, lo primero que se hizo fue abrir un navegador web y dirigirse directamente a la página oficial de WinBox, ingresando la dirección https://mikrotik.com/download/winbox. En la Figura 36, se muestra la plataforma WinBox; es la herramienta oficial de MikroTik.

Figura 36. *Ingresa a la página oficial de descarga.*

Nota. Archivo de instalación descargado de GNS3, previo a la ejecución del proceso de instalación en el entorno de simulación.

Ya dentro del sitio, se buscó el apartado de descargas y se seleccionó la versión WinBox v4.1, que es la versión oficial disponible para su descarga. Como se muestra en la Figura 37, es el historial de descarga de la página oficial de MikroTik en Winbox en el navegador.

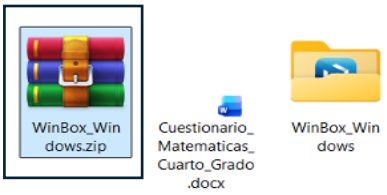
Figura 37. *Ventana de descarga en el mostrador de carpeta.*



Nota: El historial de descargas recientes del navegador, donde se visualiza el archivo comprimido "WinBox_Windows.zip" correspondiente a la aplicación de gestión WinBox y su guía de uso, descargados previamente para la configuración de los equipos MikroTik.

Al terminar la descarga, se busca en los archivos de Windows (tecla Windows + E) y se navega a la carpeta Descargas. Allí encontrarás el archivo Winbox64.exe. Cómo se visualiza la Figura 38.

Figura 38. *Carpeta de descargas en los archivos.*

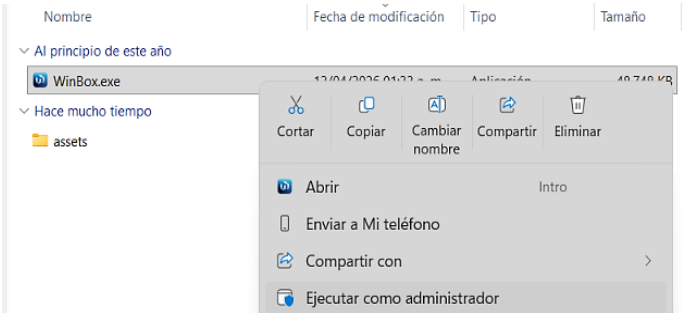


Nota. Ejecución del programa GNS3 mostrando la interfaz inicial del simulador lista para comenzar la configuración de la topología de red.

Para iniciar WinBox, se hizo doble clic sobre el archivo *winbox64.exe*. Al tratarse de un archivo ejecutable descargado desde Internet, el sistema operativo Windows presentó una ventana de advertencia de seguridad solicitando confirmación para la ejecución.

En la Figura 39, se muestra la opción "Ejecutar de todas formas" o "Sí" para permitir la apertura del programa; permite iniciar el programa con privilegios administrativos, lo que facilita el acceso a todas las funciones del software.

Figura 39. *Ejecutar programa.*



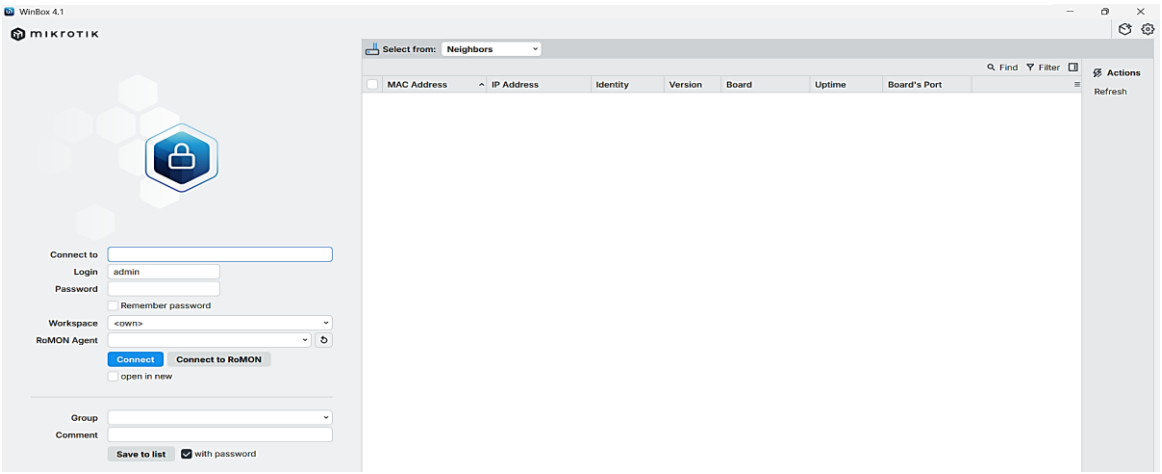
Nota: La imagen muestra el archivo ejecutable "WinBox.exe" dentro del explorador de archivos, con el menú contextual desplegado. Se selecciona la opción "Ejecutar como administrador" para iniciar la aplicación con los permisos necesarios para gestionar los dispositivos MikroTik.

Una vez hecha la ejecución del programa utilizado, podemos visualizar la administración y configuración de dispositivos mikroTik. La pantalla inicial de Winbox corresponde al panel de conexión, desde el cual el administrador puede establecer sesión con cualquier equipo mikrotik accesible en la red. Esta interfaz se compone de los siguientes elementos principales:

- Connect To: Permite ingresar la dirección IP o MAC del equipo MikroTik al que se desea conectar.
- Login: Nombre de usuario de acceso al equipo (por defecto: admin).
- Password: Contraseña de acceso (por defecto: vacía en equipos de fábrica).
- Managed: Lista de equipos MikroTik previamente conectados o guardados en WinBox.
- Neighbors: Lista de equipos MikroTik detectados automáticamente en la red local mediante el protocolo de descubrimiento de vecinos (Neighbor Discovery Protocol).
- Connect: Inicia la sesión con el equipo seleccionado o con la dirección ingresada manualmente.
- Connect To RoMON: Permite la conexión a través de RoMON (Router Management Overlay Network), mecanismo de administración avanzado fuera del alcance de este documento.

En la Figura 40, se muestra el programa instalado y ya accesible para la configuración de los equipos (Módulos A, B, C, D, E).

Figura 40. *Pantalla principal del software Winbox.*



Nota. Pantalla de inicio de WinBox, con los campos connect to, login y password, las pestañas managed y neighbors.

3.4.1. Configuración del equipo MikroTik administrador.

La arquitectura implementada en el modelo de red garantiza que toda política de seguridad, regla de enrutamiento o configuración de servicios definida en el núcleo se aplique de manera uniforme en todos los segmentos de la red.

El router administrador se conecta físicamente a los switches de distribución mediante enlaces troncales que transportan múltiples VLAN. Estos switches, a su vez, extienden la conectividad hacia los dispositivos finales, como estaciones de trabajo, servidores y cámaras IP de vigilancia. Estas últimas constituyen un elemento diferenciador de la arquitectura propuesta.

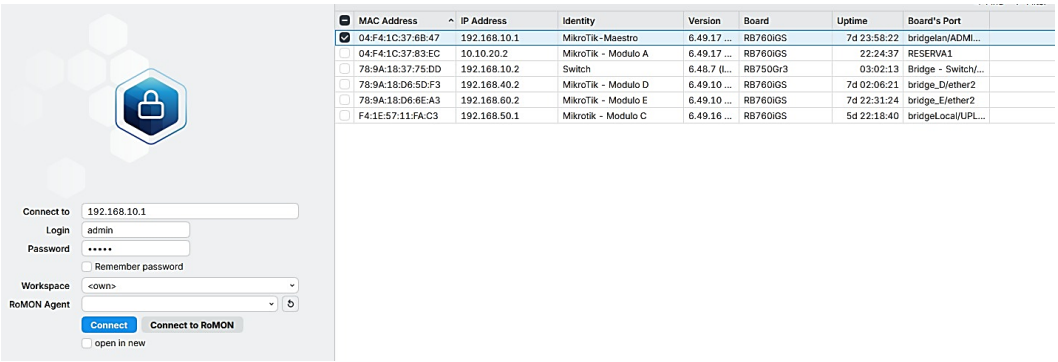
Desde el punto de vista lógico, la red se segmenta en subredes independientes que se comunican entre sí exclusivamente a través del router MikroTik. Esta segmentación cumple un doble propósito: por un lado, limita el dominio de difusión y mejora el rendimiento general de la red; por otro, permite aplicar políticas de seguridad diferenciadas según el tipo de tráfico y los recursos a los que acceden los usuarios o dispositivos.

Para iniciar la configuración del enrutador, se realiza la conexión física del dispositivo MikroTik hEX S, modelo RB760iGS, mediante un cable UTP de categoría 6. Una vez establecida la conexión física, se abre el programa Winbox para acceder al dispositivo.

Se selecciona el dispositivo mediante su dirección MAC; luego, se ingresan las credenciales de acceso en los campos Login y Password. Finalmente, se hace clic en Connect para acceder al panel de administración.

En la Figura 41, se muestra la ventana principal del programa Winbox, herramienta utilizada para la administración de los dispositivos MikroTik.

Figura 41. *Ventana principal de Winbox para acceder el administrador.*

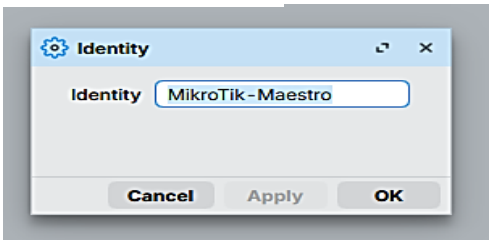


Nota: Ventana principal de Winbox utilizada para la administración de equipos MikroTik.

Para identificar correctamente el dispositivo, procedemos a asignarle un nombre personalizado dentro del panel de administración correspondiente al nombre del equipo. Escribimos MikroTik - Maestro, que será la identidad con la que este enrutador se identificará en la red.

Una vez ingresado el nombre, se debe hacer clic en *Apply* y luego en *OK* para guardar los cambios. La Figura 42, muestra la identidad del equipo administrador.

Figura 42. *Identidad del equipo.*

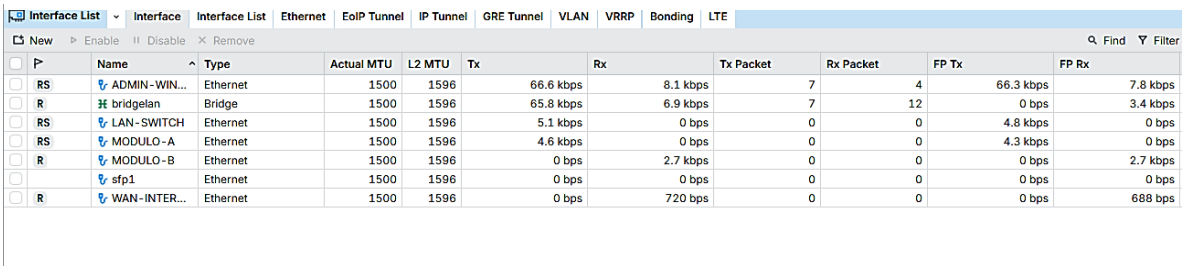


Nota. Configuración de la identidad del equipo administrador, asignando el nombre MikroTik – Maestro.

Con el objetivo de facilitar la administración y la identificación visual de cada puerto durante las configuraciones, renombramos las interfaces físicas del equipo. Para ello, en Winbox, nos dirigimos al menú Interfaces, donde se despliega la lista completa de puertos disponibles en el MikroTik hEX S.

En la Figura 43, se muestra la interfaz desde la cual se abre la ventana de propiedades. Allí se localiza el campo Nombre, que contiene el nombre predeterminado de la interfaz.

Figura 43. *Renombrar las interfaces del router.*



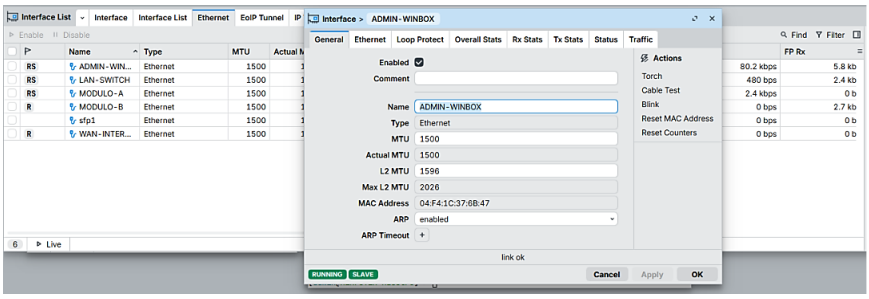
		Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet	Rx Packet	FP Tx	FP Rx
	RS	ADMIN-WIN...	Ethernet	1500	1596	66.6 kbps	8.1 kbps	7	4	66.3 kbps	7.8 kbps
	R	bridgelan	Bridge	1500	1596	65.8 kbps	6.9 kbps	7	12	0 bps	3.4 kbps
	RS	LAN-SWITCH	Ethernet	1500	1596	5.1 kbps	0 bps	0	0	4.8 kbps	0 bps
	RS	MODULO-A	Ethernet	1500	1596	4.6 kbps	0 bps	0	0	4.3 kbps	0 bps
	R	MODULO-B	Ethernet	1500	1596	0 bps	2.7 kbps	0	0	0 bps	2.7 kbps
		sfp1	Ethernet	1500	1596	0 bps	0 bps	0	0	0 bps	0 bps
	R	WAN-INTER...	Ethernet	1500	1596	0 bps	720 bps	0	0	0 bps	688 bps

Nota. Menú Interfaces de WinBox con la lista de puertos físicos disponibles en el MikroTik hEX S, antes de renombrar cada interfaz.

Para establecer la comunicación entre el enrutador y los diferentes segmentos de la red, se asignan las direcciones IP correspondientes a cada interfaz mediante Winbox. Para ello, se accede al menú *IP → Addresses* y se hace clic en el botón *"+"* para agregar cada dirección.

Se configuraron tres direcciones IP, según se muestra a continuación. La Figura 44, presenta el procedimiento para renombrar los puertos del MikroTik administrador y asignar las direcciones IP correspondientes.

Figura 44. *Direccionamiento de IP en el programador.*



Nota. Renombrado de las interfaces del router administrador y asignación de direcciones IP a cada una.

Se hace clic en el botón *"+"*, se ingresa la dirección IP 10.10.10.1/30 y se selecciona la interfaz módulo A. Posteriormente, se hace clic en *Apply → OK* para guardar la configuración.

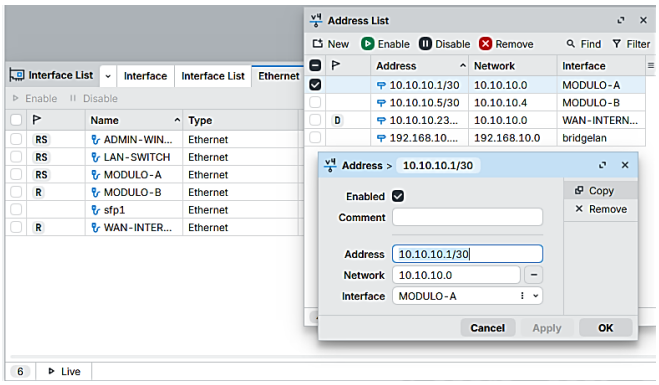
Esta dirección corresponde al enlace punto a punto hacia el primer módulo remoto. La máscara /30 proporciona cuatro direcciones en total, de las cuales dos son utilizables para los dispositivos del enlace.

A continuación, se vuelve a hacer clic en el botón *"+"*, se ingresa la dirección IP 10.10.10.5/30 y se selecciona la interfaz módulo B. Después, se selecciona *Apply → OK* para guardar los cambios.

De igual manera, se agrega la dirección IP correspondiente a la interfaz bridge_Lan y se guardan los cambios mediante *Apply → OK.*

En la Figura 45, se muestra la asignación de direcciones IP a las interfaces del router administrador, con la cual se definen los segmentos de red correspondientes a cada módulo.

Figura 45. *Asignación de direcciones IP.*



Nota. Direcciones IP asignadas a las interfaces del router administrador: 10.10.10.1/30 para el enlace hacia el módulo A, 10.10.10.5/30 para el enlace hacia el módulo B y [dirección IP/prefijo] para la interfaz bridge_Lan. Estas direcciones definen los segmentos de red correspondientes a cada módulo.

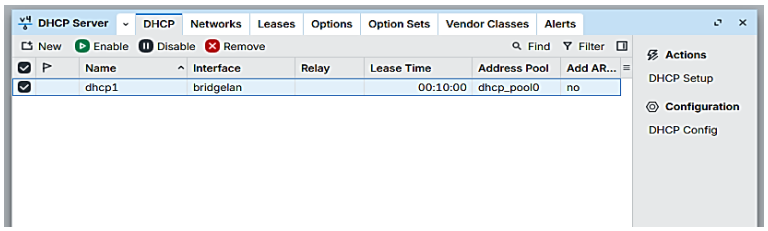
Con esta configuración, los dispositivos conectados a la red local pueden obtener una dirección IP de forma automática mediante el servicio DHCP, siempre que estén configurados como clientes DHCP. Esto incluye computadoras, cámaras IP, dispositivos de monitoreo y otros equipos conectados a la red LAN.

A continuación, se configura el servidor DHCP en el router MikroTik hEX S. Desde Winbox, se accede al menú *IP → DHCP* Server. En lugar de realizar la configuración manualmente campo por campo, se utiliza el asistente integrado mediante el botón DHCP Setup, el cual guía de forma secuencial la definición de los parámetros necesarios.

Durante el proceso, el asistente solicita la interfaz en la que funcionará el servidor DHCP. En este caso, se selecciona la interfaz bridge_Lan, correspondiente a la red LAN principal, desde la cual se asignarán direcciones IP a los dispositivos conectados.

En la Figura 46, se muestra que el asistente detecta automáticamente la red asociada a la interfaz seleccionada. Se verifica que esta corresponda a la red 192.168.10.0/24.

Figura 46. *Interfaz del servidor DHCP.*



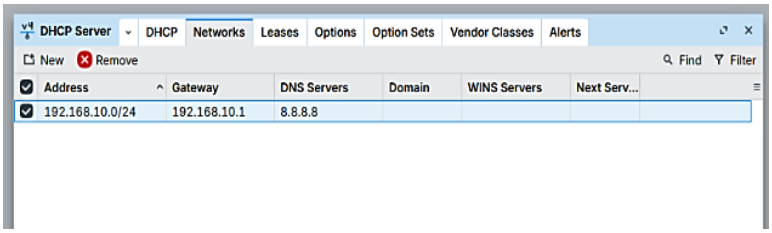
Nota: Asistente DHCP Setup detectando automáticamente la red asociada a la interfaz bridge_Lan: 192.168.10.0/24.

Se confirma que la puerta de enlace predeterminada sea 192.168.10.1, correspondiente a la dirección IP del enrutador en la red LAN. Posteriormente, se define el rango de direcciones IP que el servidor DHCP asignará a los dispositivos conectados.

A continuación, se configuran los servidores DNS. Se puede establecer la dirección 8.8.8.8 como DNS primario y 8.8.4.4 como DNS secundario. Finalmente, se define el tiempo. Para un entorno de laboratorio, puede utilizarse un tiempo de 10 minutos; para un entorno de producción, se recomienda establecer un período de 1 día, según los requisitos de la red.

En la Figura 47, se muestra la configuración de los servidores DNS y del tiempo de arrendamiento de las direcciones IP proporcionadas por el servidor DHCP.

Figura 47. *Servidor DNS.*

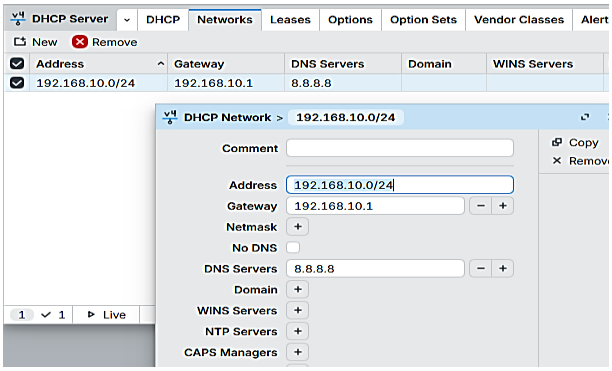


Nota. Configuración de los servidores DNS 8.8.8.8 y 8.8.4.4, así como del tiempo de arrendamiento de las direcciones IP, mediante el asistente DHCP Setup.

Se verifica que la casilla Allow Remote Requests esté habilitada. Esta opción permite que el router actúe como un servidor de caché DNS para los dispositivos de la red local. De esta manera, cuando los clientes reciben la dirección IP del router como servidor DNS mediante DHCP, pueden enviar sus solicitudes de resolución de nombres al MikroTik.

En la Figura 48, se muestra la verificación de que el servicio DNS se encuentra habilitado para atender las solicitudes de los dispositivos conectados a la red local administrada por el router maestro.

Figura 48. *DNS de todos los dispositivos conectados a la red local.*

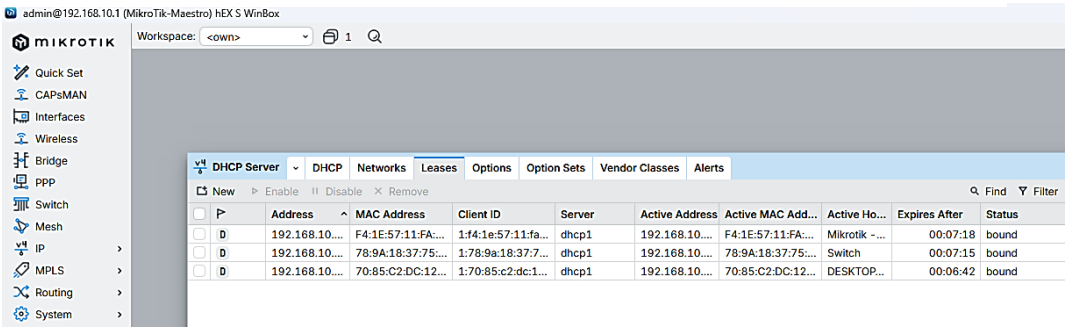


Nota. Activación de la opción que permite al router actuar como servidor DNS local para los dispositivos de la red.

Al finalizar el asistente, se muestra un mensaje que confirma que el servidor DHCP se ha configurado correctamente. A partir de ese momento, los dispositivos que se conecten a la red LAN y estén configurados como clientes DHCP recibirán automáticamente una dirección IP dentro del rango definido.

En la Figura 49, se confirma el estado operativo del servidor DHCP, lo que indica que el servicio se encuentra en ejecución correctamente en el router maestro.

Figura 49. *Funcionamiento del servicio DHCP-Server.*



Nota. Mensaje de confirmación del asistente que indica que el servidor DHCP se configuró correctamente.

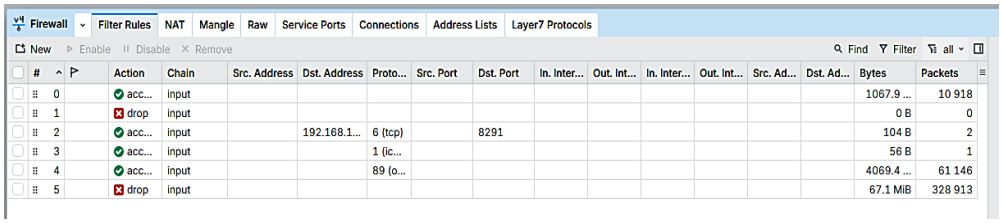
Con el objetivo de proteger la infraestructura de red, se crean las primeras reglas de firewall en el enrutador MikroTik. Estas reglas controlan el tráfico que fluye a través del dispositivo, permitiendo las conexiones autorizadas y bloqueando los accesos no autorizados.

La primera regla permite el tráfico perteneciente a conexiones en estado aprobado o bloqueado. Esta regla es fundamental dentro de la configuración del firewall, ya que permite que las comunicaciones ya establecidas y el tráfico relacionado continúen sin interrupciones.

Una vez creada, la regla aparece en la lista de reglas de filtro y comienza a aplicarse de inmediato al tráfico que atraviesa el enrutador. De esta manera, las sesiones de comunicación activas pueden funcionar con normalidad, sin ser interrumpidas por las reglas de seguridad posteriores.

En la Figura 50, se muestra la configuración inicial del firewall en el MikroTik administrador. Esta configuración permite controlar el acceso a la red y bloquear conexiones no autorizadas.

Figura 50. *Configuración del firewall básico de seguridad.*

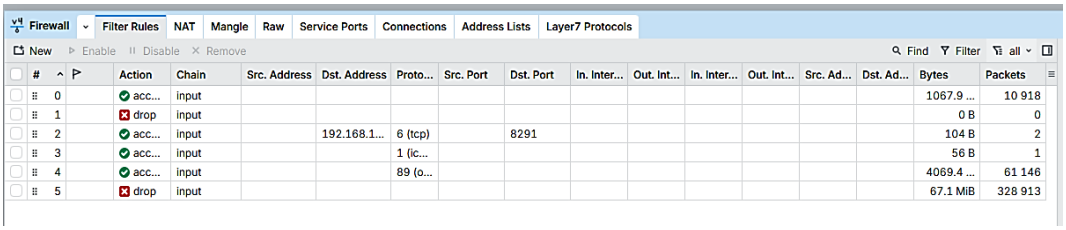


Nota. Regla de firewall activa en el MikroTik administrador que bloquea el tráfico no autorizado hacia la red.

Con esta configuración, el router MikroTik puede intercambiar información de enrutamiento de forma automática con los demás dispositivos de la arquitectura. Para ello, se configura el protocolo OSPF (Open Shortest Path First).

Para verificar el funcionamiento de la interfaz de administración, se realiza un monitoreo en tiempo real. Este evidenció un tráfico estable, con tasas de transmisión y recepción bajas, propias de las tareas de configuración y supervisión. Asimismo, no se identificaron pérdidas de paquetes ni congestión en el enlace, como se observa en la Figura 51.

Figura 51. *Configuración del protocolo OSPF y asignación del ID del enrutador.*

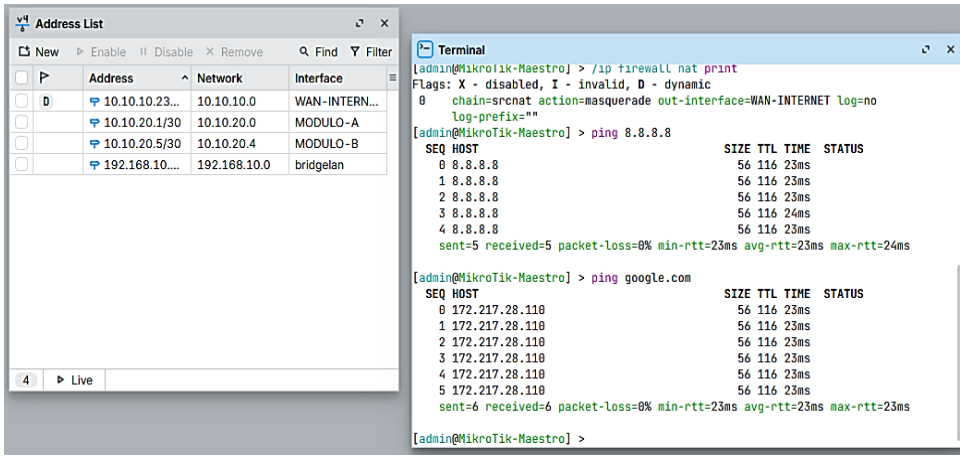


#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
0	acc...	input												1067.9 ...	10 918
1	drop	input												0 B	0
2	acc...	input		192.168.1...	6 (tcp)		8291							104 B	2
3	acc...	input			1 (ic...									56 B	1
4	acc...	input			89 (o...									4069.4 ...	61 146
5	drop	input												67.1 MiB	328 913

Nota. Monitoreo en tiempo real del tráfico de la interfaz de administración, con tasas de transmisión y recepción estables y sin pérdida de paquetes.

En la Figura 52, se muestra la etapa final de configuración del router MikroTik principal, en la que se validan tanto el direccionamiento de la red como la conectividad hacia Internet. En la lista de direcciones se observan las interfaces configuradas.

Figura 52. *Interfaz monitorizada en tiempo real.*



Nota. Etapa final de la configuración del router MikroTik principal, con la interfaz WAN-INTERNET, los enlaces punto a punto hacia los módulos A y B, la interfaz bridge_Lan y la regla de NAT configurada.

En la interfaz WAN-INTERNET, que corresponde a la conexión de salida hacia Internet, se configura una regla de NAT. Esta regla permite que los dispositivos de la red interna accedan a Internet utilizando la dirección IP pública asignada al router.

3.4.2. Configuración del Switch.

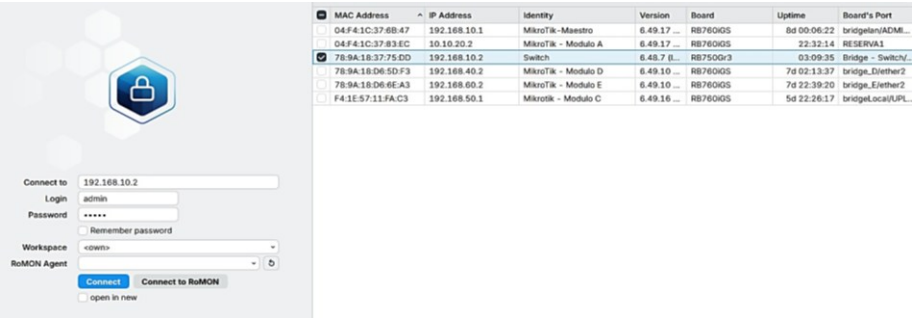
El switch es un dispositivo de capa 2 del modelo OSI que se conecta directamente al router administrador. Su función es ampliar la cantidad de puertos disponibles en la red local.

Debido a que el router administrador MikroTik hEX S cuenta con un número limitado de interfaces físicas, el switch actúa como un elemento de expansión de conectividad. De esta manera, permite integrar un mayor número de dispositivos a la red los cuales se reservan para enlaces WAN, conexiones punto a punto, segmentos de red u otras funciones de enrutamiento.

Para acceder al switch mediante Winbox, se selecciona el dispositivo en la lista de detección. Al seleccionarlo, su dirección MAC se carga automáticamente en el campo Connect To. Posteriormente, se verifican las credenciales de acceso en los campos Login y Password. Finalmente, se hace clic en Connect para ingresar al panel de administración del switch y continuar con la configuración.

En la Figura 53, se muestra la configuración inicial del switch principal, utilizado para ampliar la cantidad de puertos disponibles y habilitar la conectividad entre los módulos del laboratorio.

Figura 53. *Configuración inicial del Switch.*



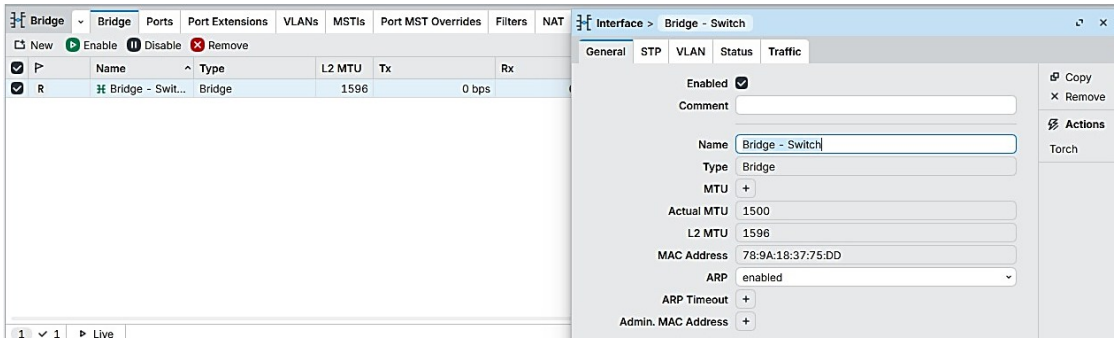
Nota. Configuración del switch principal para ampliar la cantidad de puertos disponibles en la red y habilitar la conectividad entre los módulos del laboratorio.

Para que el switch principal gestione el tráfico de sus puertos físicos como un único segmento de red, primero es necesario crear un bridge. Este funcionará como el núcleo lógico de conmutación dentro del dispositivo MikroTik.

Para crear el bridge, se hace clic en el botón "+" dentro del menú Bridge. A continuación, se abre la ventana de configuración, en la cual se ingresa el nombre bridge-switch. Esta denominación permite identificar el puente dentro del dispositivo y hace referencia a la función del equipo como switch principal de la red, lo que facilita su reconocimiento durante las tareas administrativas posteriores.

En la Figura 54, se muestran los valores predeterminados de la configuración del bridge. En este paso no se requiere realizar ninguna modificación adicional para crear el puente

Figura 54. *Agregar los puertos Bridge.*



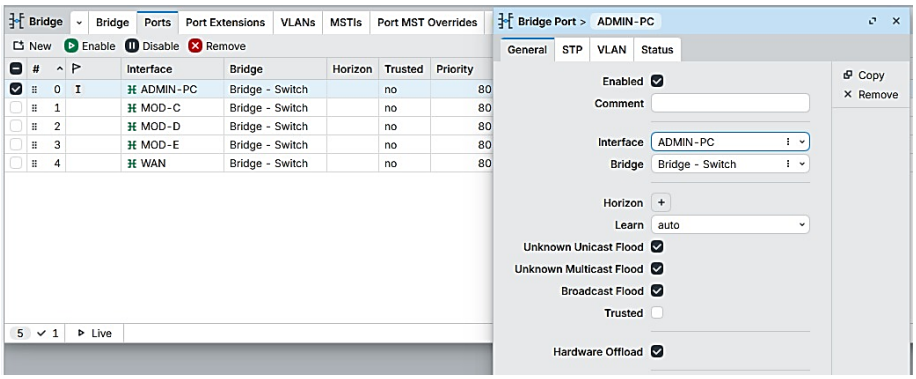
Nota. Creación del bridge bridge-switch con los valores predeterminados en el switch principal.

Una vez creado el bridge bridge-switch, se vinculan los puertos físicos del dispositivo para que funcionen como un único segmento de red conmutado.

Desde Winbox, se accede al menú Bridge y se selecciona la pestaña Ports. A continuación, se hace clic en el botón *"+"* para agregar una interfaz. En el campo Interface, se selecciona el puerto ether2 y, en el campo, se selecciona bridge-switch. Luego, se hace clic en OK para confirmar la configuración.

Posteriormente, se repite el mismo procedimiento para las interfaces ether4 y ether5. De esta manera, los tres puertos quedan asociados al bridge y forman parte del mismo segmento de red. La configuración se muestra en la Figura 54.

Figura 55. *Agregar los puertos físicos al Bridge-Switch.*



Nota. Puertos ether2, ether4 y ether5 vinculados al bridge bridge-switch para formar un único segmento de red conmutado.

Es importante destacar que la interfaz ether1 no se agrega al bridge bridge-switch, ya que cumple la función de enlace de subida hacia el router administrador. Por este motivo, debe mantenerse independiente para permitir la comunicación entre el switch principal y el resto de la arquitectura de red.

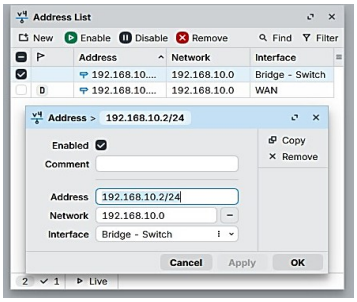
Para que el switch principal pueda administrarse de forma remota y comunicarse con el router administrador dentro de la red local, es necesario asignar una dirección IP a su interfaz de bridge.

Desde Winbox, se accede al menú *IP* → *Addresses* y se hace clic en el botón *"+"* para agregar una nueva dirección IP. En la ventana de configuración, se ingresa la dirección 192.168.10.2/24 y se selecciona la interfaz bridge-switch. Esta dirección corresponde a la IP fija de administración asignada al switch principal dentro de la red local.

Al pertenecer a la subred 192.168.10.0/24, el switch queda en el mismo segmento que el router administrador, cuya dirección IP en la interfaz LAN-switch es 192.168.10.1/24. Esto permite que ambos dispositivos se comuniquen directamente, sin requerir enrutamiento adicional. Finalmente, se hace clic en OK para guardar y confirmar la asignación de la dirección IP.

En la Figura 56, se muestra la asignación de la dirección IP a la interfaz de bridge del switch principal, mediante la cual se establece la identidad de red del dispositivo en la LAN.

Figura 56. *Asignar la dirección IP al Bridge-Switch.*



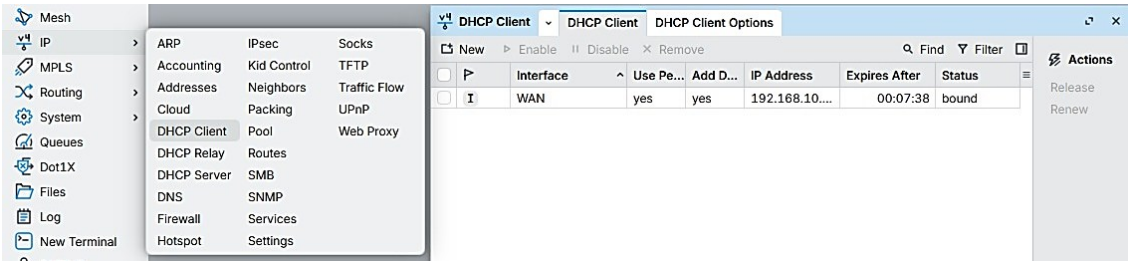
Nota. Asignación de la dirección IP 192.168.10.2/24 a la interfaz de bridge del switch principal, estableciendo su identidad de red en la LAN.

Para que el switch principal obtenga automáticamente los parámetros de red necesarios para comunicarse con el router maestro, se configura un cliente DHCP en la interfaz ether1. Desde Winbox, se accede al menú *IP → DHCP* Client y se hace clic en el botón *"+"* para agregar una nueva entrada.

Al habilitar el cliente DHCP en esta interfaz, el switch solicita automáticamente una dirección IP, una puerta de enlace, servidores DNS y otros parámetros de red al servidor DHCP configurado en el router maestro, cada vez que se establece la conexión entre ambos equipos.

En la Figura 57, se muestra la configuración del cliente DHCP en el switch principal para la obtención automática de parámetros de red desde el router maestro.

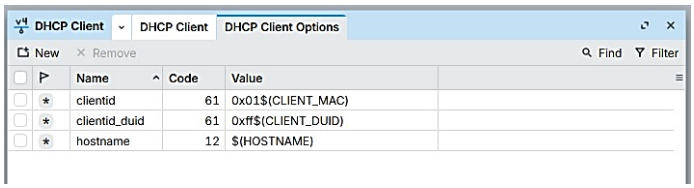
Figura 57. *Configurar el cliente DHCP en el Switch Principal.*



Nota. Configuración del cliente DHCP en el switch principal, habilitado en la interfaz ether1 para obtener automáticamente los parámetros de red desde el router maestro.

En la Figura 58, se muestran los valores predeterminados de configuración del cliente DHCP. En este paso, no es necesario realizar ninguna modificación adicional para su funcionamiento básico.

Figura 58. *DHCP Client.*



Nota. Valores predeterminados del cliente DHCP del switch principal, sin necesidad de realizar una configuración adicional.

A medida que la arquitectura de red crece e incorpora más dispositivos y configuraciones, la administración simultánea de los equipos se vuelve indispensable. Mantener sesiones de administración abiertas en los distintos dispositivos permite supervisar su estado y realizar ajustes de manera coordinada.

Esta modalidad de trabajo facilita la detección y solución de problemas de conectividad entre los módulos, ya que permite observar de forma paralela el comportamiento de la red en todos los dispositivos. De este modo, se agilizan las tareas de monitoreo, verificación y mantenimiento de la infraestructura.

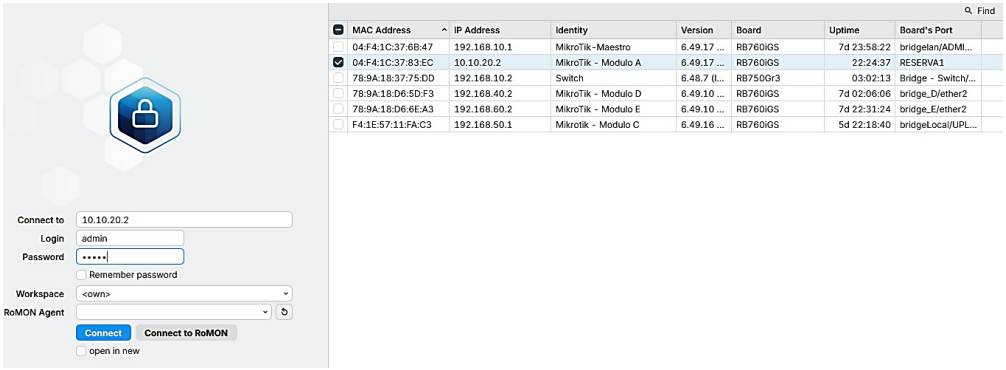
3.4.3. Configuración del Módulo A.

Para iniciar la configuración del enrutador del módulo A, se espera unos segundos hasta que el equipo aparezca en la lista de detección de Winbox. Posteriormente, se selecciona el dispositivo haciendo clic en su dirección MAC.

A continuación, se ingresan las credenciales de acceso en los campos Login y Password. Finalmente, se hace clic en Connect para acceder al panel de administración del dispositivo.

En la Figura 59, se muestra la ventana principal del programa Winbox, utilizada para acceder al enrutador correspondiente al módulo A.

Figura 59. *Acceso al dispositivo mediante WinBox - Módulo A.*

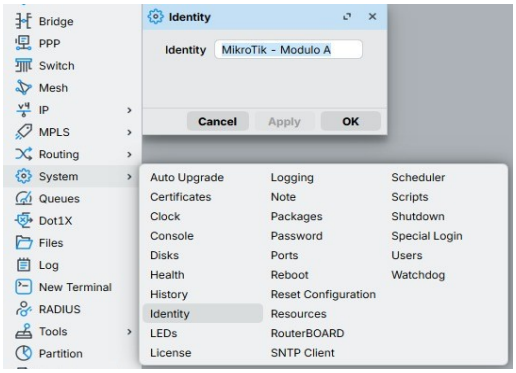


Nota. Ventana de conexión de Winbox utilizada para acceder al enrutador del módulo A.

Una vez dentro del panel de administración, el sistema muestra una ventana de configuración predeterminada. A continuación, desde Winbox, se accede al menú *System* → *Identity,* donde se localiza el campo que contiene el nombre actual del dispositivo.

En este campo, se ingresa el nombre MikroTik-Módulo A, que permite identificar el enrutador dentro de toda la arquitectura de red. El procedimiento se muestra en la Figura 60.

Figura 60. *Identificación del Módulo A.*



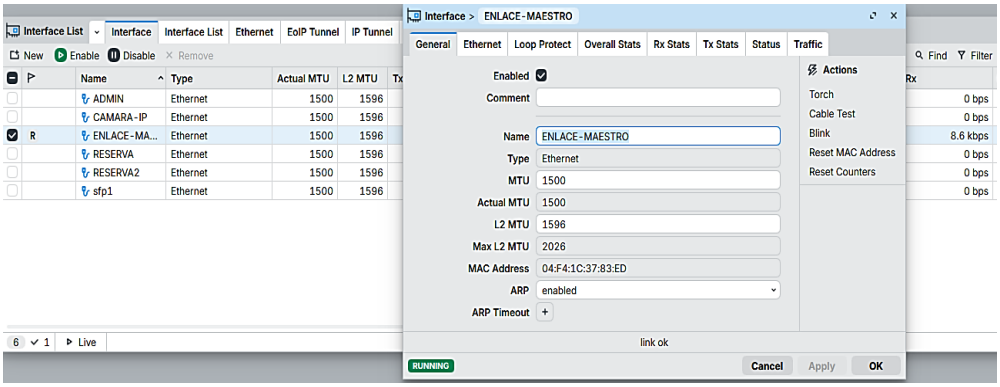
Nota. Configuración de la identidad del módulo A mediante la asignación del nombre MikroTik-Módulo A, con el fin de facilitar su identificación por parte del administrador.

De manera similar al procedimiento realizado en el router maestro, se renombran las interfaces físicas del módulo A para identificar claramente la función de cada puerto dentro de la arquitectura de red. Para ello, desde Winbox, se accede al menú Interfaces, donde se muestra la lista completa de puertos disponibles.

Se hace doble clic sobre cada interfaz y se localiza el campo que contiene el nombre predeterminado. A continuación, se ingresa el nuevo nombre asignado y se confirma la modificación mediante Apply → OK.

En la Figura 61, se muestra el proceso de renombrado de las interfaces del módulo A, lo que permite identificar claramente el puerto CAM-LAN y el enlace de subida o uplink.

Figura 61. *Renombrar las interfaces del Módulo A.*



Nota. Renombrado de las interfaces físicas del módulo A, con identificación del puerto CAM-LAN y del enlace de subida o uplink.

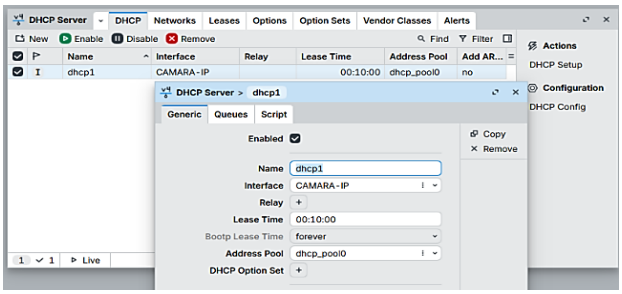
Para asignar la dirección IP a la interfaz de enlace hacia el router maestro, se accede al menú *IP → Addresses*. A continuación, se hace clic en el botón *"+"*, ubicado en la esquina superior izquierda de la ventana, para abrir el formulario de creación de una nueva dirección IP.

En el campo Address, se ingresa la dirección 10.10.10.6/30. Luego, en el campo Interface, se selecciona la interfaz correspondiente al enlace de subida hacia el router maestro. El campo Network se completa automáticamente con la red asociada, 10.10.10.4, de acuerdo con el prefijo /30.

Se hace clic en Apply para verificar que los datos sean correctos y, posteriormente, en OK para guardar la dirección IP en la interfaz seleccionada.

En la Figura 62, se muestra la asignación de la dirección IP correspondiente al enlace hacia el router maestro en la interfaz de subida del módulo A.

Figura 62. *IP del enlace hacia Maestro.*

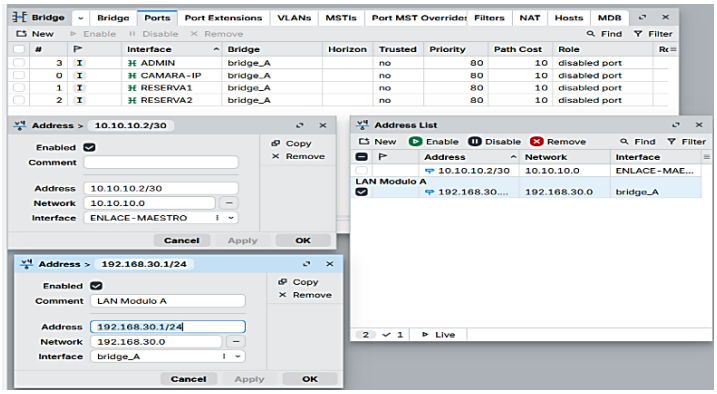


Nota. Asignación de la dirección IP 10.10.10.6/30 a la interfaz de subida ENLACE-MAESTRO del módulo A, correspondiente al enlace hacia el router maestro.

Asimismo, se asigna la dirección IP correspondiente a la red de cámaras en la interfaz CAM-LAN. Para ello, se agrega una nueva dirección IP y se selecciona la interfaz destinada al segmento de videovigilancia del módulo A.

En la Figura 63, se muestra la configuración de la red de cámaras IP del módulo A, correspondiente al segmento dedicado a la videovigilancia de la zona 1.

Figura 63. *Red de Cámara IP.*



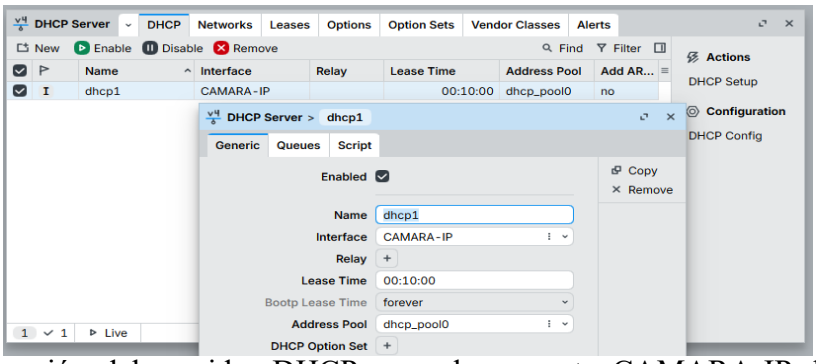
Nota. Configuración de la dirección IP correspondiente al segmento de cámaras IP del módulo A.

Para configurar el servidor DHCP que asignará direcciones IP automáticamente a las cámaras IP conectadas al módulo A, se accede al menú IP → DHCP Server. A continuación, se hace clic en DHCP Setup para iniciar el asistente de configuración guiada, el cual simplifica la creación del servidor DHCP paso a paso.

Al finalizar el asistente, se muestra un mensaje de confirmación indicando que el servidor DHCP se creó correctamente. Posteriormente, desde la lista de DHCP Server, se verifica que el servicio aparezca activo con el estado running en la interfaz configurada.

En la Figura 64, se muestra la configuración del servidor DHCP para el segmento CAMARA-IP del módulo A, lo que permite la asignación automática de direcciones IP a las cámaras conectadas.

Figura 64. *DHCP Server para CAMARA-IP.*



Nota. Configuración del servidor DHCP para el segmento CAMARA-IP del módulo A, habilitando la asignación automática de direcciones IP a las cámaras.

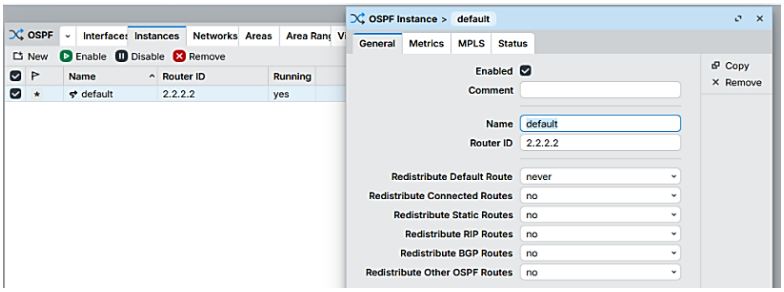
Para configurar el protocolo de enrutamiento dinámico, se hace clic en *Routing* en el menú lateral y se selecciona *OSPF.* A continuación, se abre la ventana principal de configuración, que contiene varias pestañas.

En la pestaña Instances, se localiza el campo Router ID y se ingresa el valor 2.2.2.2. Este valor corresponde al identificador único del módulo A dentro de la topología OSPF del laboratorio.

El identificador debe ser único dentro del dominio OSPF, ya que permite diferenciar el módulo A de los demás routers participantes. Posteriormente, se hace clic en Apply para aplicar los cambios y, finalmente, en OK para guardarlos y cerrar la ventana.

En la Figura 65, se muestra la configuración del protocolo OSPF en el módulo A, con el identificador de router 2.2.2.2.

Figura 65. *Configuración OSPF · Router ID — Módulo A.*



Nota. Configuración del protocolo OSPF en el módulo A, con el identificador de router 2.2.2.2 para su identificación única dentro de la topología dinámica.

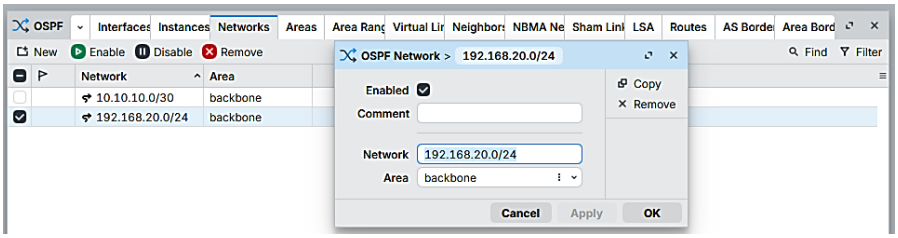
Desde Winbox, se accede al menú *Routing* → *OSPF.* A continuación, se selecciona la pestaña Networks, en la cual se definen las redes que el módulo A anunciará mediante OSPF.

Se hace clic en el botón *"+"* para agregar una nueva entrada de red. En el formulario que se abre, se completan los campos con los valores correspondientes.

En el campo Network, se ingresa la red 10.10.10.0/30, correspondiente al segmento de enlace entre el módulo A y el router administrador. En el campo Área, se selecciona backbone, que corresponde al área principal de OSPF, identificada como Área 0. Esta área centraliza el intercambio de información de enrutamiento entre los dispositivos de la topología.

En la Figura 66, se muestra la configuración de las redes OSPF en el módulo A, mediante la cual se define el segmento que será anunciado al router maestro.

Figura 66. *Configuración de Networks OSPF.*

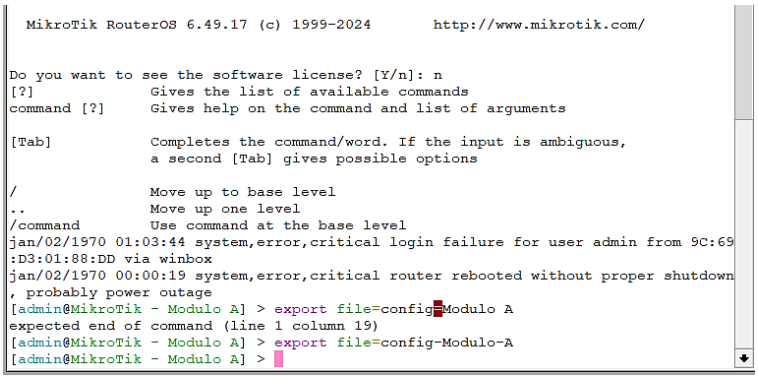


Nota. Configuración de las redes OSPF anunciadas por el módulo A: segmento 10.10.10.4/30 dentro del área backbone o Área 0.

Antes de concluir la sesión de configuración del módulo A, es fundamental realizar una copia de seguridad de los parámetros aplicados durante el proceso. Esta copia permite conservar un respaldo de la configuración y facilita su restauración o consulta posterior.

En la Figura 67, se muestra la exportación de la configuración completa del módulo A mediante la terminal de Winbox, con fines de respaldo y documentación técnica del dispositivo.

Figura 67. *Exportar configuración del Módulo A.*



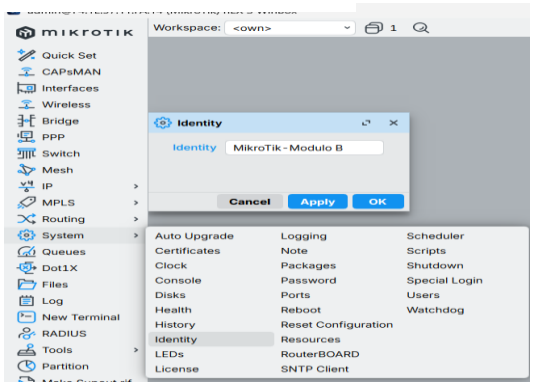
Nota: Exportación de la configuración completa del Módulo A mediante la terminal de WinBox, como respaldo y documentación técnica del dispositivo.

3.4.4. Configuración del Módulo B.

Desde Winbox, se accede al menú *System* → *Identity,* donde se localiza el campo que contiene el nombre actual del dispositivo. En este campo, se ingresa el nombre MikroTik-Módulo B, el cual permitirá identificar el enrutador correspondiente al módulo B dentro de la arquitectura de red.

Una vez ingresado el nombre, se hace clic en *Apply* y luego en *OK* para guardar los cambios. En la Figura 68, se muestra la configuración de la identidad del módulo B en Winbox, mediante la asignación del nombre que permite identificarlo dentro de la arquitectura de red.

Figura 68. *Identificación del Módulo – B.*

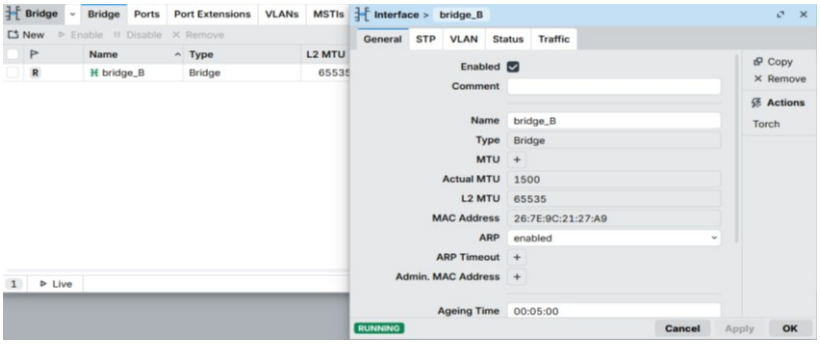


Nota. Configuración de la identidad del módulo B en Winbox, mediante la asignación de un nombre que permite identificarlo dentro de la arquitectura de red.

A continuación, se crea un bridge para el módulo B. El bridge permite agrupar las interfaces físicas destinadas a la red local en un mismo segmento de capa 2. Para facilitar su reconocimiento dentro de la arquitectura, se asigna una denominación que identifica claramente su pertenencia al módulo B y mantiene la convención de nombres aplicada en los dispositivos configurados anteriormente.

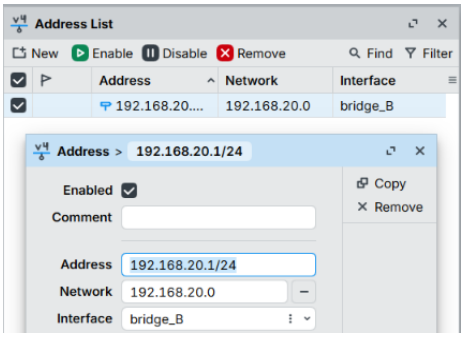
En la Figura 69, se muestra el proceso de creación del bridge en el módulo B, utilizado para agrupar las interfaces y distribuir el tráfico correspondiente a la zona 2. En la Figura 70, se muestra la asignación de la dirección IP del módulo B.

Figura 69. *Crear Bridge en el Módulo B.*



Nota. Creación del bridge del módulo B para agrupar las interfaces físicas de la zona 2 en un único segmento de red conmutado.

Figura 70. *Direcciones IP del Módulo B.*



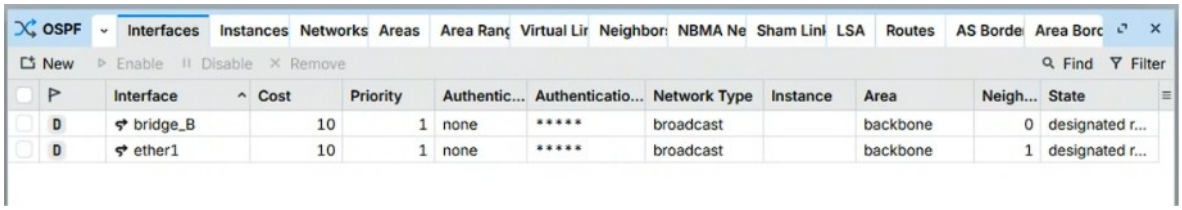
Nota. Dirección IP asignada al módulo B.

En esta etapa, el módulo B se integra al enrutamiento dinámico mediante el protocolo OSPF. Esta configuración permite que el router intercambie automáticamente la información de enrutamiento de sus redes con los demás dispositivos que pertenecen al área OSPF.

De esta manera, se reduce la necesidad de configurar rutas estáticas de forma manual y se facilita la escalabilidad de la topología ante la incorporación de nuevos segmentos o dispositivos de red.

En la Figura 71, se muestra la configuración del enrutamiento dinámico OSPF en el módulo B. Mediante esta configuración, el router puede anunciar sus redes y aprender automáticamente las rutas publicadas por los demás routers participantes.

Figura 71. *Verificar la instancia OSPF.*

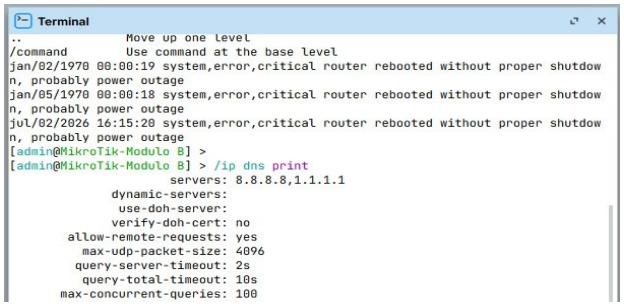


Nota. Configuración del enrutamiento dinámico OSPF en el módulo B, que permite el intercambio automático de rutas con los demás dispositivos del área.

Las redes anunciadas mediante OSPF definen los segmentos que el módulo B debe publicar hacia los demás routers de la topología. De esta manera, los dispositivos participantes pueden aprender automáticamente la ruta necesaria para acceder a la red LAN del módulo B.

En la Figura 72, se muestra la configuración de las redes anunciadas mediante OSPF en el módulo B, junto con la definición de los servidores DNS públicos utilizados para la resolución de nombres de dominio.

Figura 72. *Configurar DNS.*



Nota. Redes anunciadas mediante OSPF y servidores DNS configurados en el módulo B, habilitando la resolución de nombres para los dispositivos de la LAN.

Con todos los parámetros verificados y en estado operativo, el módulo B queda preparado para establecer comunicación con el router administrador. Esto permite la gestión centralizada del tráfico de videovigilancia correspondiente al segundo segmento de red.

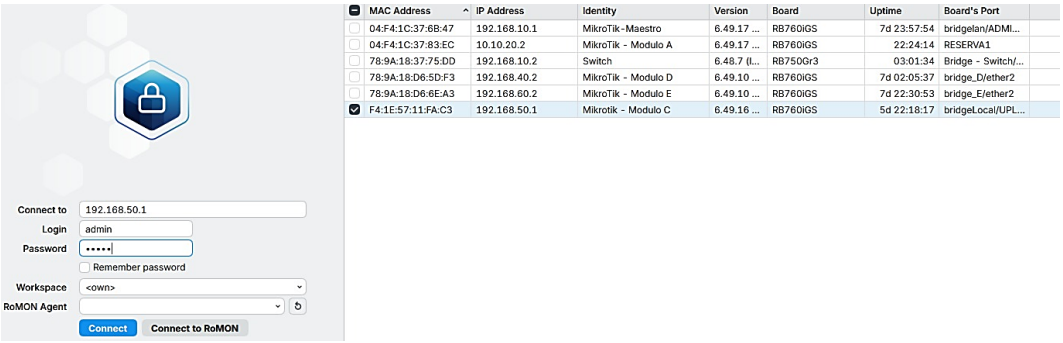
La segmentación aplicada, junto con las políticas de firewall y las ACL definidas, contribuye al aislamiento del tráfico, la protección de los dispositivos conectados y la estabilidad operativa del sistema de monitoreo IP implementado en el laboratorio.

3.4.5. Configuración del Módulo C.

Para iniciar la configuración del módulo C mediante Winbox, se accede a la pestaña Neighbors, donde el programa detecta automáticamente los dispositivos MikroTik disponibles en la red local. Una vez que el equipo aparece en la lista, se selecciona mediante su dirección MAC.

A continuación, se ingresan las credenciales de acceso en los campos *Login* y *Password,* y se hace clic en *Connect* para acceder al panel de administración. El procedimiento se muestra en la Figura 73.

Figura 73. *Acceso al dispositivo mediante WinBox - Módulo C.*



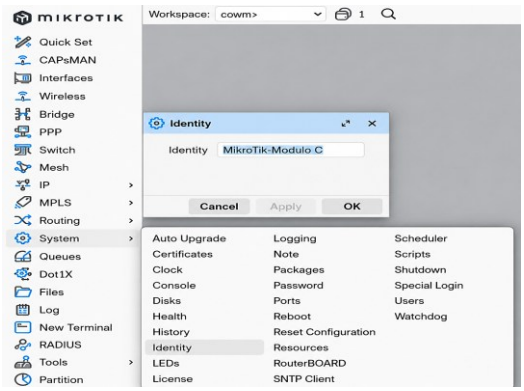
Nota. Ventana de conexión de Winbox que muestra el módulo C detectado en la pestaña Neighbors.

Desde Winbox, se accede al menú System → Identity, donde se localiza el campo que contiene el nombre actual del dispositivo. En este campo, se ingresa el nombre MikroTik-

Módulo C, que permitirá identificar el enrutador correspondiente al módulo C dentro de la arquitectura de red.

Una vez ingresado el nombre, se hace clic en *Apply* y luego en *OK* para guardar los cambios. El procedimiento se muestra en la Figura 74.

Figura 74. *Identidad del Módulo C.*

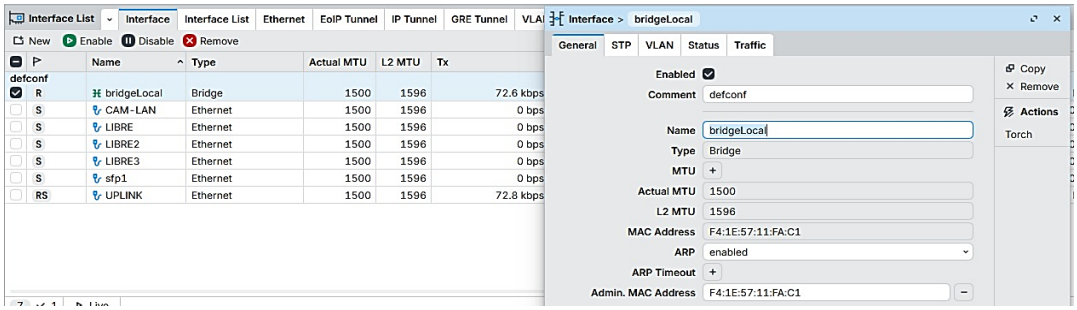


Nota. Configuración de la identidad del módulo C en Winbox, mediante la asignación del nombre MikroTik-Módulo C.

Para mantener una identificación clara y ordenada de cada puerto dentro de la arquitectura, se renombran las interfaces físicas del módulo C. Desde Winbox, se accede al menú Interfaces. A continuación, se hace doble clic sobre cada puerto, se localiza el campo Name, se ingresa el nuevo nombre y se confirma la modificación mediante Apply → OK.

En la Figura 75, se muestran las interfaces del módulo C junto con el bridge creado.

Figura 75. *Renombrar las interfaces del RTR-MÓDULO-C.*

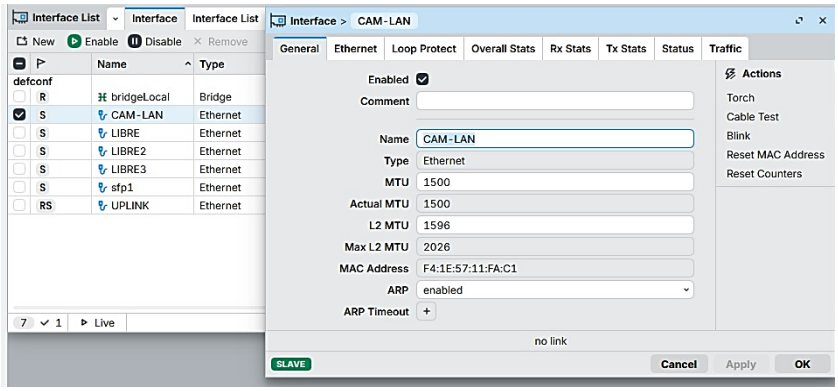


Nota. Interfaces físicas renombradas del módulo C junto con el bridge creado.

Se abre la interfaz ether1 y se cambia su nombre a CAM-LAN. Posteriormente, se hace clic en Apply → OK para guardar los cambios. Este puerto se destina a la conexión de

las cámaras IP y de los dispositivos de videovigilancia correspondientes al módulo C. El procedimiento se muestra en la Figura 76.

Figura 76. *Puerto de la cámara asignada.*

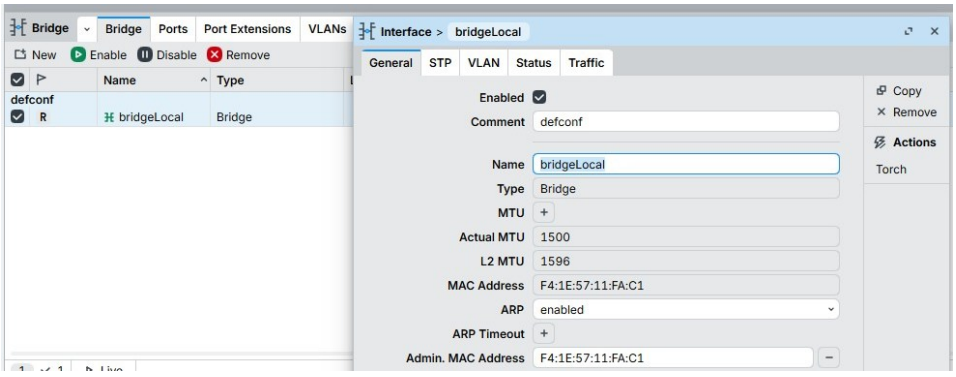


Nota. Renombrado del puerto ether1 a CAM-LAN en el módulo C, destinado a la conexión de cámaras IP y dispositivos de videovigilancia.

Antes de realizar cualquier modificación, se verifican las interfaces asignadas al bridge. Para ello, desde el panel lateral izquierdo de Winbox, se accede al menú Bridge y se selecciona la pestaña Ports. En esta pestaña se muestra la lista de interfaces físicas que se encuentran asociadas actualmente al bridge bridge_Local.

En la Figura 77, se muestra el renombrado de las interfaces vinculadas al bridge bridge_Local, lo que facilita la identificación de los puertos según la función que cumplen dentro de la arquitectura implementada.

Figura 77. *Bridge creado con puerto asignado.*

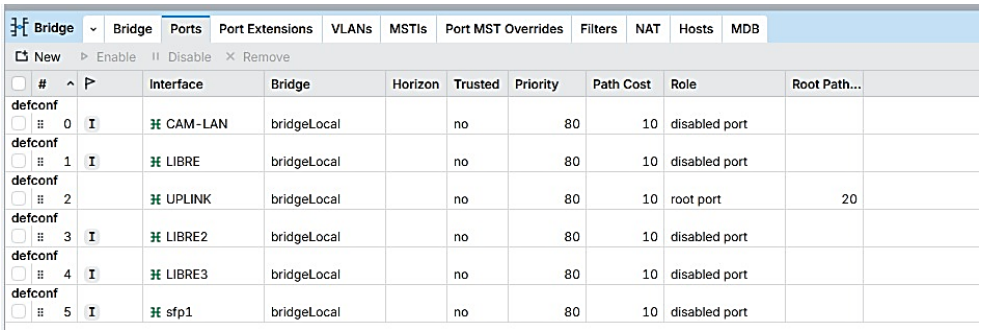


Nota. Renombrado de las interfaces asociadas al bridge bridge_Local del módulo C, con el fin de identificar los puertos según su función dentro de la arquitectura de red.

Se identifican las interfaces activas en la tabla de puertos y se verifica cuáles están asociadas al bridge. En este caso, las interfaces ether2, ether3, ether4 y ether5 se encuentran dentro del bridge bridge_Local, lo que indica que pertenecen al segmento de red LAN del módulo C.

En la Figura 78, se muestra la pestaña Ports con las interfaces asignadas al bridge. Los puertos se identifican como CAM-LAN, Libre, Uplink, Libre2 y Libre3, según la función asignada a cada uno. Esta configuración permite que las interfaces incorporadas al bridge formen parte del mismo segmento de red conmutado, lo que facilita la comunicación y la administración de los dispositivos conectados.

Figura 78. *Puertos asignados en el segmento de la red.*

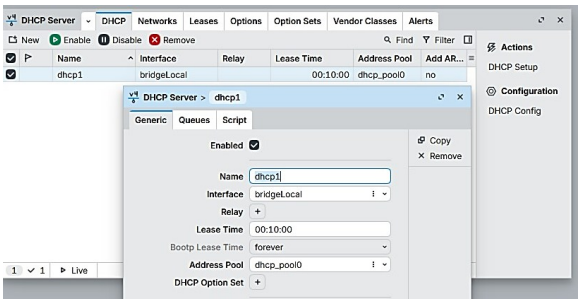


#	Interface	Bridge	Horizon	Trusted	Priority	Path Cost	Role	Root Path...
defconf 0	CAM-LAN	bridgeLocal		no	80	10	disabled port	
defconf 1	LIBRE	bridgeLocal		no	80	10	disabled port	
defconf 2	UPLINK	bridgeLocal		no	80	10	root port	20
defconf 3	LIBRE2	bridgeLocal		no	80	10	disabled port	
defconf 4	LIBRE3	bridgeLocal		no	80	10	disabled port	
defconf 5	sfp1	bridgeLocal		no	80	10	disabled port	

Nota. Puertos CAM-LAN, Libre, Uplink, Libre2 y Libre3 agregados al bridge del módulo C e integrados en un mismo segmento de red.

En la Figura 79, se muestra la verificación del cliente DHCP activo en el módulo C, lo que confirma la obtención correcta de los parámetros de red desde el router maestro.

Figura 79. *Verificación de DHCP server — Módulo C.*

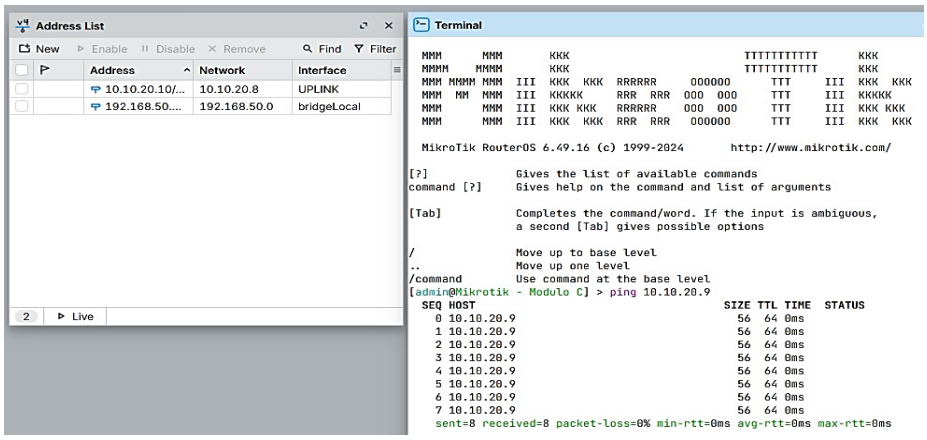


Nota. Verificación del cliente DHCP activo en el módulo C, que confirma la obtención correcta de los parámetros de red desde el router maestro.

Con todos los parámetros verificados y en estado operativo, el módulo C queda integrado a la red general del laboratorio. De esta manera, puede gestionar el tráfico de videovigilancia correspondiente a su segmento de forma centralizada y contribuir al funcionamiento de la infraestructura de monitoreo IP implementada.

En la Figura 80, se muestra la verificación de conectividad desde el módulo C mediante un comando ejecutado en la terminal. Esta prueba permite confirmar la comunicación del módulo con la red y con el router MikroTik principal.

Figura 80. *Conexión la IP al Mikrotik principal junto con el módulo C.*



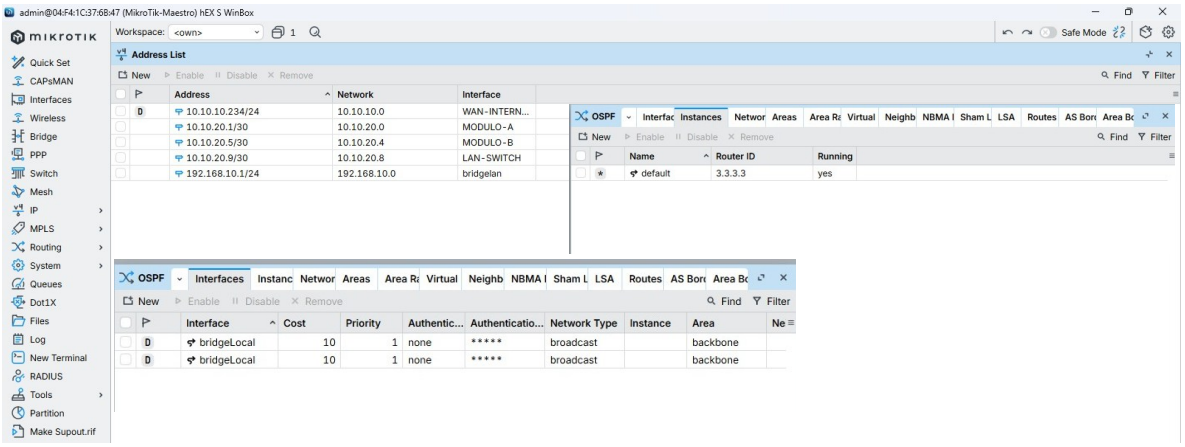
Nota: Prueba de conectividad desde la terminal del módulo C hacia el router maestro.

Una vez verificada la conectividad del módulo C, se configura el protocolo de enrutamiento dinámico OSPF dentro de la arquitectura de red. Para ello, se accede al menú Routing → OSPF y se verifica la existencia de la instancia predeterminada.

Posteriormente, se agregan las redes que participarán en el proceso de enrutamiento dinámico. Se registra la red de interconexión 10.10.20.8/30, utilizada para la comunicación entre el módulo C y el router MikroTik principal, así como la red local 192.168.50.0/24, correspondiente al segmento en el que se conectarán las cámaras IP y los demás dispositivos del módulo.

La configuración de las redes anunciadas mediante OSPF se muestra en la Figura 81.

Figura 81. *OSPF del MikroTik Principal y terminamos de integrar el Módulo C.*

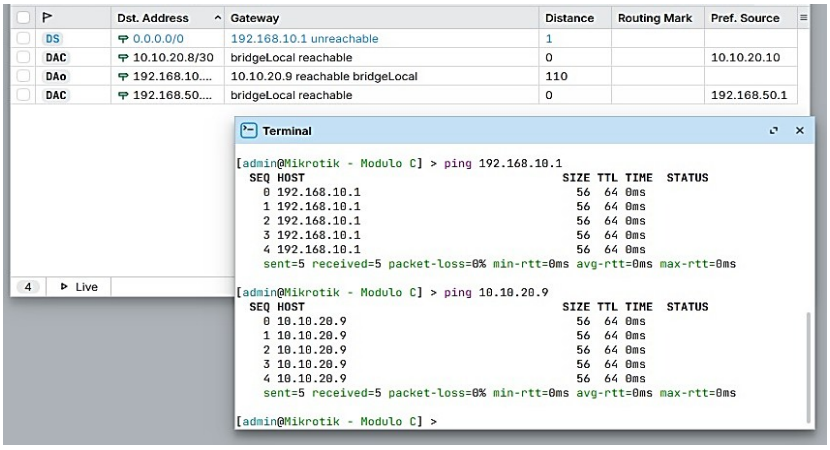


Nota. Configuración de las redes OSPF en el módulo C: enlace de interconexión 10.10.20.8/30 hacia el router MikroTik principal y red local 192.168.50.0/24 correspondiente al segmento de cámaras.

Una vez configurado el protocolo de enrutamiento dinámico OSPF en el módulo C, se verifica su funcionamiento. Para ello, se utiliza el identificador de router 3.3.3.3 y se incorporan al área backbone las redes 10.10.20.8/30 y 192.168.50.0/24.

Posteriormente, se realizan pruebas de conectividad mediante el comando ping para confirmar la comunicación entre el módulo C, el router MikroTik principal y las redes anunciadas. El procedimiento se muestra en la Figura 82.

Figura 82. *Envió y comprobación del módulo C.*



Nota. Prueba de conectividad mediante el comando ping, utilizada para verificar la comunicación IP del módulo C con la red y el funcionamiento del enrutamiento dinámico OSPF, configurado con el Router ID 3.3.3.3.

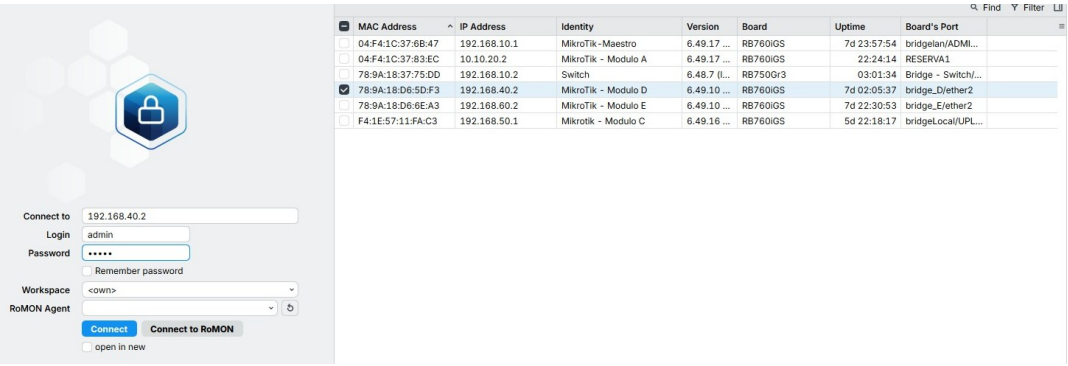
3.4.6. Configuración del Módulo D.

Al abrir Winbox, se muestran los dispositivos detectados en la red dentro de la pestaña Neighbors. Se hace clic en la dirección MAC del dispositivo para cargarla automáticamente en el campo de destino de conexión.

Se establece la conexión mediante la dirección MAC, en lugar de utilizar una dirección IP. A continuación, se ingresan las credenciales de acceso en los campos *Login* y *Password*, y se hace clic en *Connect* para ingresar al panel de administración del enrutador correspondiente al módulo D.

En la Figura 83, se muestra la ventana de conexión de Winbox, utilizada para acceder al enrutador del módulo D.

Figura 83. *Acceso al dispositivo mediante WinBox - Módulo C.*

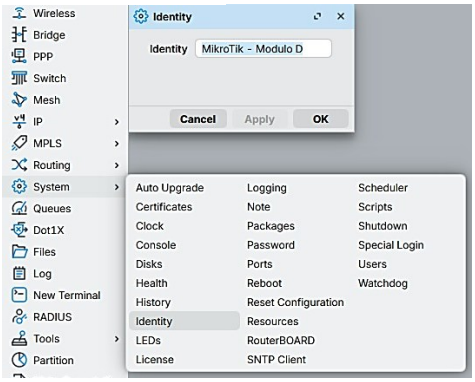


Nota. Renombrado del puerto ether1 a CAM-LAN en el módulo C, destinado a la conexión de cámaras IP y dispositivos de videovigilancia.

Antes de realizar cualquier modificación, se verifican las interfaces asignadas al bridge. Para ello, desde el panel lateral izquierdo de Winbox, se accede al menú Bridge y se selecciona la pestaña Ports. En esta pestaña se muestra la lista de interfaces físicas que se encuentran asociadas actualmente al bridge bridge_Local.

En la Figura 84, se muestra el renombrado de las interfaces vinculadas al bridge bridge_Local, lo que facilita la identificación de los puertos según la función que cumplen dentro de la arquitectura implementada.

Figura 84. *Identificación del Módulo D.*



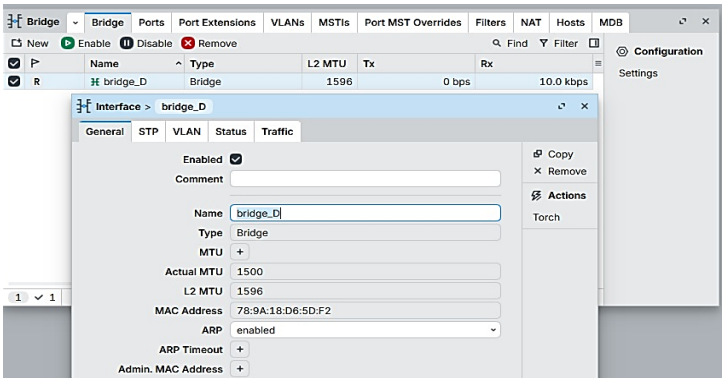
Nota. Ventana de conexión de Winbox utilizada para acceder al enrutador del módulo D.

Una vez establecida la conexión mediante Winbox, se accede al menú *System* → *Identity*. En el campo Name, se elimina el nombre actual del dispositivo y se ingresa la denominación MikroTik-Módulo D.

Posteriormente, se hace clic en *Apply* → *OK* para guardar los cambios y cerrar la ventana. A partir de este momento, el equipo se identifica como MikroTik-Módulo D dentro de la arquitectura de red.

En la Figura 85, se muestra la configuración de la identidad del módulo D en Winbox, mediante la asignación de un nombre identificativo dentro de la red.

Figura 85. *Asignación de los Bridge _D.*



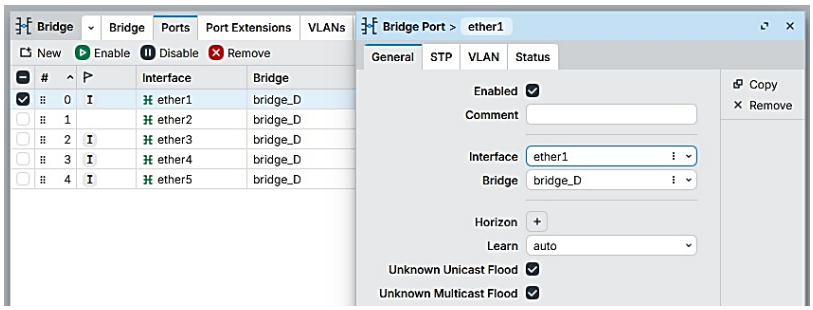
Nota. Creación de un nuevo puente de red (bridge) en el enrutador del módulo D mediante Winbox.

Cada puerto físico que se agregue al puente bridge_D formará parte del mismo segmento de red de capa 2. Por tanto, los dispositivos conectados a dichos puertos podrán comunicarse entre sí mediante conmutación, sin requerir enrutamiento entre ellos.

La dirección IP fija se asigna a la interfaz virtual bridge_D, no a los puertos físicos que la integran. Esta dirección actúa como puerta de enlace predeterminada para los equipos de la red local del módulo D y permite identificar y administrar el equipo MikroTik dentro de la red interna.

En la Figura 86, se muestran las interfaces y los puertos del enrutador, identificados de acuerdo con la función que desempeñan en la arquitectura de red implementada.

Figura 86. *Crear una Bridge_D en el módulo D.*



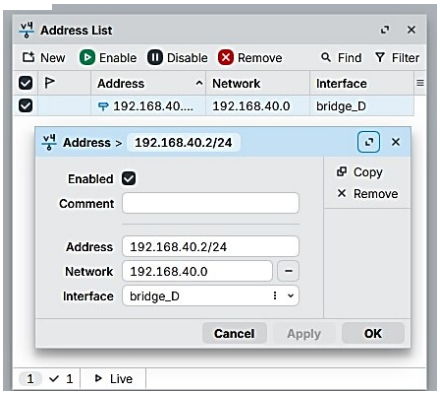
Nota. Interfaces del módulo D renombradas de acuerdo con la función que cumplen dentro de la arquitectura de red.

Una vez aplicada la configuración, el enrutador del módulo D contará con una identidad propia dentro de la red. La dirección IP estática 192.168.40.2/24 se asigna a la interfaz virtual bridge_D, lo que permite acceder y administrar el dispositivo desde los equipos conectados al mismo puente de red.

Para que 192.168.40.2 funcione además como puerta de enlace predeterminada, debe existir una configuración de enrutamiento que permita al módulo D reenviar tráfico hacia otras redes.

En la Figura 87, se muestra la asignación de la dirección IP 192.168.40.2/24 a la interfaz bridge_D del módulo D.

Figura 87. *Asignación de la IP.*



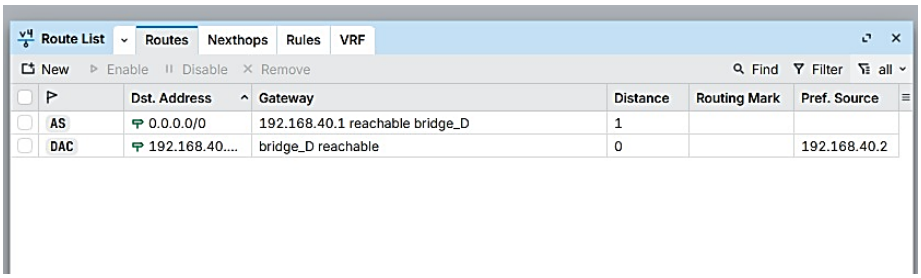
Nota. Asignación de la dirección IP 192.168.40.2/24 a la interfaz bridge_D del módulo D, utilizada como dirección de administración y, según la configuración de enrutamiento, como puerta de enlace para los equipos de la red local.

Una vez configurada la dirección IP, se accede a *IP → Routes* desde el menú lateral de Winbox. Para agregar una nueva ruta, se hace clic en el botón **"+"**.

En el campo Gateway, se ingresa la dirección 192.168.40.1, correspondiente al enrutador principal de la red. Si esta ruta se configura con el destino predeterminado 0.0.0.0/0 valor que puede aparecer por defecto o dejarse vacío al crear la ruta, el módulo D enviará al enrutador principal todo el tráfico cuyo destino no pertenezca a una red directamente conectada o a una ruta más específica.

En la Figura 88, se muestra la tabla de enrutamiento del módulo D, donde se observan las rutas configuradas, incluida la ruta predeterminada a través del gateway 192.168.40.1.

Figura 88. *Asignación de enrutamiento del módulo D.*



Nota: Tabla de enrutamiento del módulo D, con la ruta hacia el gateway 192.168.40.1 configurada.

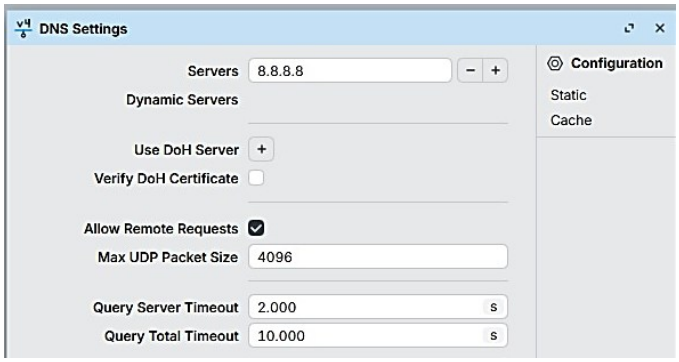
Una vez configurada la ruta predeterminada, el módulo D identifica que los paquetes dirigidos a destinos fuera de la red local 192.168.40.0/24 deben reenviarse hacia la dirección 192.168.40.1.

Esta dirección corresponde al enrutador principal y actúa como siguiente salto para la comunicación con otros módulos de la infraestructura, servidores externos o servicios de Internet.

Sin esta ruta, el módulo D únicamente podrá establecer comunicación entre los equipos conectados a los puertos que pertenecen a bridge_D, dentro de la red local 192.168.40.0/24. Por tanto, permanecerá aislado de las demás redes de la infraestructura y no tendrá una ruta de salida hacia destinos externos.

En la Figura 89, se ilustra que, en ausencia de una ruta predeterminada, los equipos conectados al puente bridge_D pueden comunicarse entre sí, pero no pueden acceder a otras redes ni a recursos externos.

Figura 89. *Configurar el GATEWAY.*



Nota. Configuración del servidor DNS en el enrutador del módulo D para la resolución de nombres de dominio.

Se configura la dirección 8.8.8.8, correspondiente al servicio DNS público de Google, como servidor DNS externo del módulo D. Esta configuración permite que el enrutador consulte dicho servidor para resolver nombres de dominio; es decir, traduce direcciones como *google.com* a sus respectivas direcciones IP.

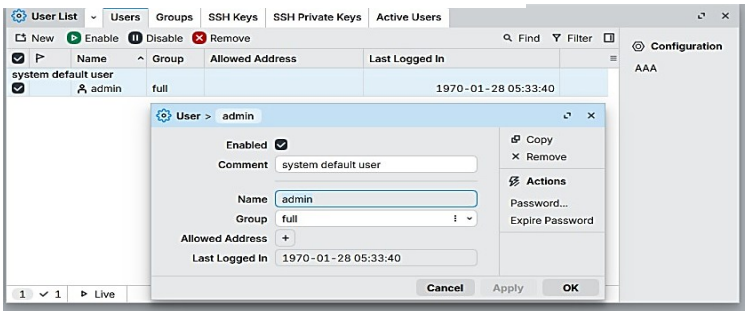
Para que el equipo MikroTik funcione como servidor DNS local para los dispositivos conectados a bridge_D, se habilita la opción *Allow Remote Requests*. De esta manera, el

enrutador recibe las consultas DNS de los clientes, las reenvía al servidor DNS externo configurado y puede almacenar temporalmente las respuestas en caché.

Los sensores, las cámaras IP y los equipos del laboratorio auxiliar deben utilizar la dirección 192.168.40.2 como servidor DNS. Esta configuración puede establecerse manualmente en cada dispositivo o distribuirse automáticamente mediante DHCP, de modo que sus consultas sean atendidas por el módulo D.

En la Figura 90, se muestra la configuración DNS del módulo D, donde el enrutador MikroTik utiliza 8.8.8.8 como servidor DNS externo y actúa como resolvedor DNS local para los dispositivos asociados a bridge_D.

Figura 90. *Configurar un DNS.*



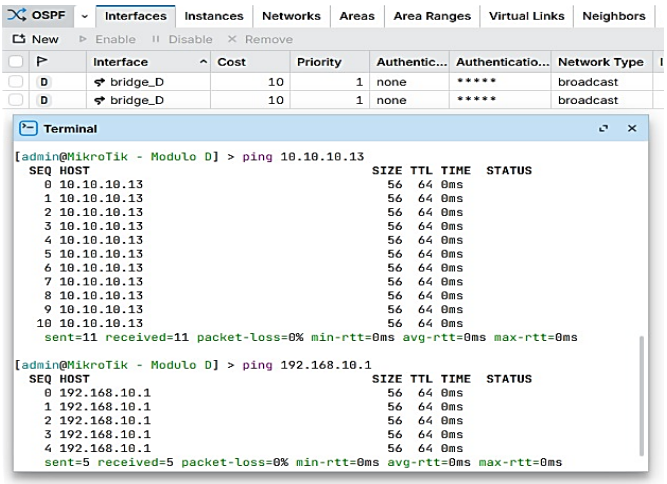
Nota. Configuración del módulo D como servidor DNS local para su red, con el servidor DNS público 8.8.8.8 configurado externo.

Finalmente, se realizan pruebas de validación para comprobar la conectividad entre los dispositivos, el intercambio dinámico de rutas mediante OSPF y el correcto funcionamiento del módulo D dentro de la infraestructura de red.

La validación incluye la comprobación de los vecinos OSPF y de las rutas aprendidas dinámicamente. Una adyacencia OSPF en estado Full indica que los routers han completado la sincronización de su base de datos de estado de enlace y pueden intercambiar información de enrutamiento.

En la Figura 91, se muestran las pruebas de conectividad y la verificación del enrutamiento dinámico OSPF en el módulo D.

Figura 91*. Activamos la seguridad básica.*



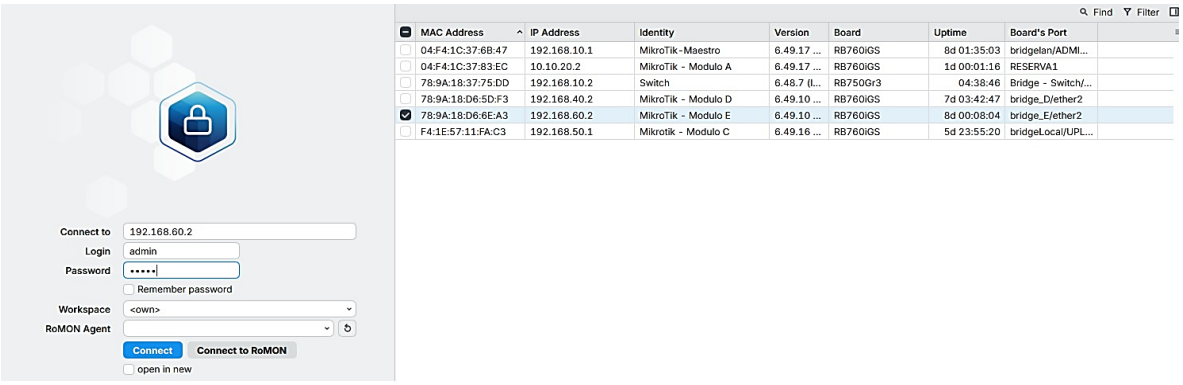
Nota. Pruebas de validación de conectividad y de enrutamiento dinámico OSPF.

3.4.7. Configuración del Módulo E.

Se accede a Winbox para verificar que el equipo se encuentre sin configuraciones previas que puedan interferir con la nueva implementación del módulo E.

En la Figura 92, se muestra la ventana de conexión de Winbox, herramienta utilizada

Figura 92. *Pantalla de winbox del Módulo – E.*



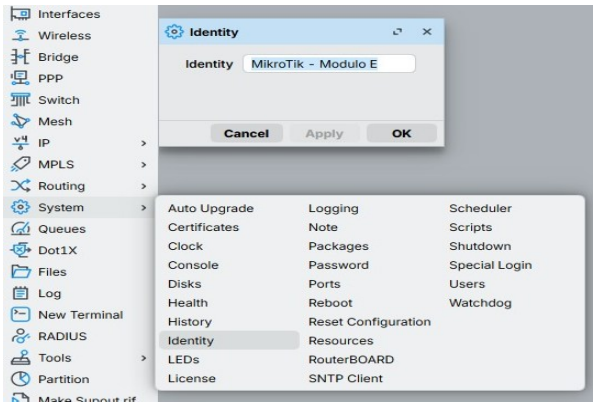
para acceder y administrar el enrutador MikroTik correspondiente al módulo E.

Nota. Ventana de conexión de Winbox utilizada para acceder al enrutador del módulo E.

Una vez establecida la conexión, se accede al menú System → Identity. En el campo Name, se asigna al dispositivo el nombre MikroTik-Módulo_E, el cual permite identificarlo de forma única dentro de la arquitectura de red del laboratorio. Finalmente, se selecciona Apply → OK para guardar los cambios.

En la Figura 93, se muestra la asignación de la identidad al enrutador MikroTik del módulo E, lo que facilita su identificación y administración dentro de la red.

Figura 93. *Identificación del módulo*



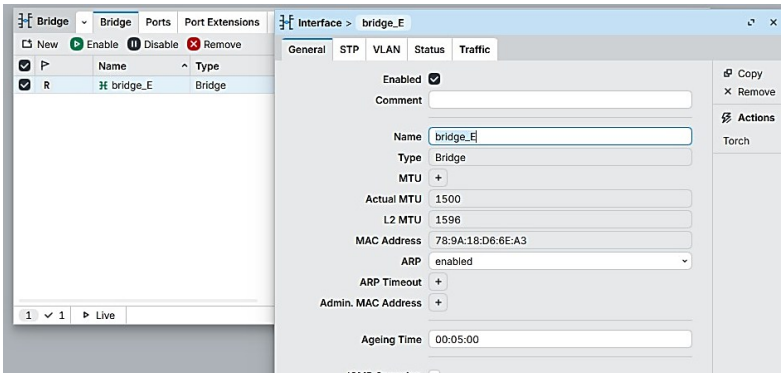
Nota. Ventana de conexión de utilizada para acceder al enrutador del módulo E.

Una vez establecida la conexión, se accede a *System* → *Identity* y se asigna al dispositivo el nombre MikroTik-Módulo_E. Esta identificación permite reconocer el enrutador de forma única dentro de la arquitectura de red del laboratorio.

Para guardar la configuración, se selecciona *Apply* → *OK*.

En la Figura 94, se muestra la asignación de identidad al enrutador MikroTik del módulo E, lo que facilita su identificación y administración dentro de la red.

Figura 94. *Crear una Bridge_E*



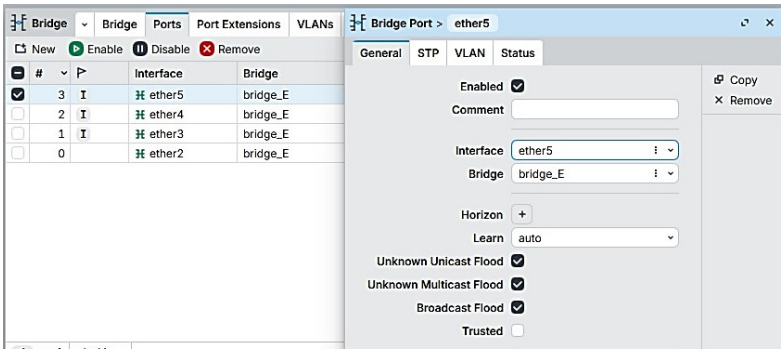
Nota. Creación del bridge_E en el módulo E, que unificará los puertos bajo una misma LAN.

Se accede a *Bridge → Ports* y se agregan las interfaces ether2, ether3, ether4 y ether5 al puente bridge_E. De esta manera, los dispositivos conectados a estos puertos forman parte de la misma red local del módulo E.

La interfaz ether1 no se agrega al bridge, ya que se reserva como enlace ascendente (uplink) hacia el switch principal. Esta separación permite mantener la conexión del módulo E con el resto de la infraestructura y utilizar ether1 como interfaz de salida o administración.

En la Figura 95, se muestra la asignación de los puertos al puente de red bridge_E del módulo E.

Figura 95. *Asignación de los Bridge _D.*



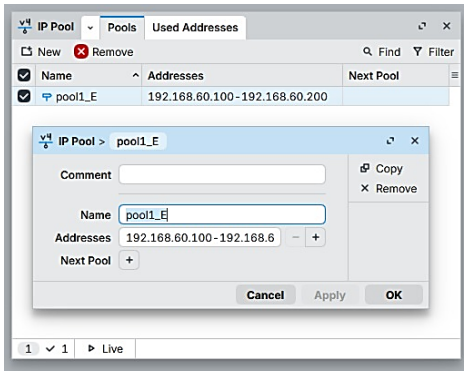
Nota. Puertos ether2, ether3, ether4 y ether5 asignados a bridge_E en el módulo E, mientras que ether1 se reserva como interfaz de enlace ascendente

Posteriormente, se agrega una dirección IP mediante *IP → Addresses → "+"*. Se asigna la dirección 192.168.60.2/24 a la interfaz bridge_E, la cual se utiliza para administrar el módulo E desde Winbox o mediante un navegador web, siempre que el equipo de administración pertenezca al mismo segmento de red.

Mediante el asistente DHCP Setup, se asocia el *pool* pool_E a la interfaz bridge_E. Se configura el espacio de direcciones 192.168.60.0/24 y la puerta de enlace 192.168.60.2, correspondiente a la dirección IP del módulo E. De esta manera, los dispositivos conectados al puente bridge_E reciben automáticamente una dirección IP, máscara de red, puerta de enlace y demás parámetros definidos en el servidor DHCP.

En la Figura 96, se muestra la creación del *pool* de direcciones 192.168.60.100-192.168.60.200 y la configuración del servidor DHCP en la interfaz bridge_E.

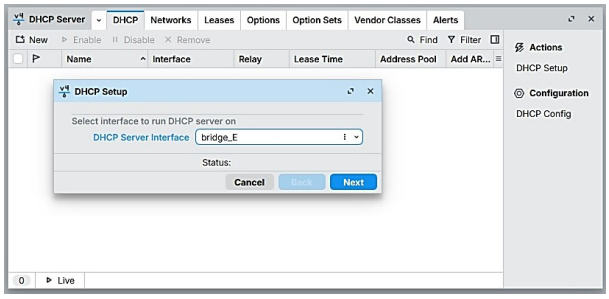
Figura 96. *Configuración del servidor DHCP en el Módulo E.*



Nota: Creación del pool de direcciones IP (192.168.60.100–192.168.60.200) y configuración del servidor DHCP en la interfaz bridge_E para el Módulo E.

En la Figura 97, se crea un nuevo servidor DHCP sobre la interfaz bridge_E, correspondiente al segmento de red del Módulo E. Durante la configuración, se solicita seleccionar la interfaz en la que se ejecutará el servicio; en este caso, ya se encuentra seleccionada la interfaz bridge_E.

Figura 97. *El servidor DHCP del Módulo E está correctamente configurado.*



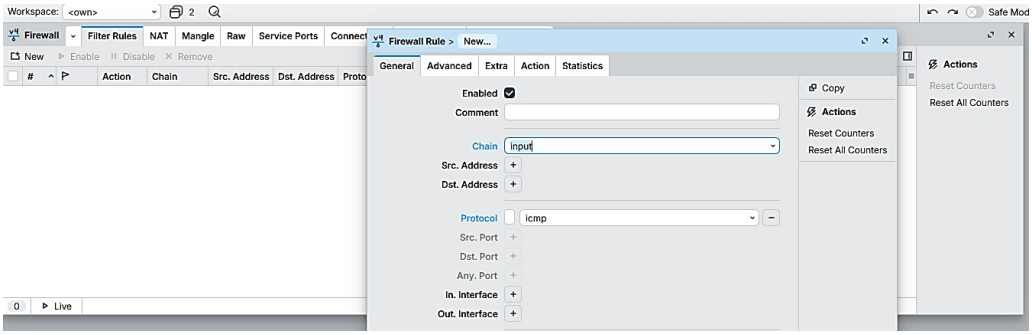
Nota: Selección de la interfaz bridge_E para la creación de un nuevo servidor DHCP correspondiente al Módulo E.

Tras verificar la configuración del servicio DHCP, se procede a configurar el firewall con el fin de controlar el tráfico entrante hacia el router.

Dentro de *IP → Firewall → Filter Rules,* se crea una primera regla en la cadena input que permite el protocolo ICMP. Esta regla habilita únicamente las solicitudes de *ping* hacia el dispositivo, lo cual resulta útil para verificar la conectividad sin exponer otros servicios.

En la Figura 98, se muestra la ventana de creación de una nueva regla de filtrado (*Filter Rule*).

Figura 98. *Se crea una regla de Firewall en la cadena input que acepta tráfico.*



Nota: Ventana de creación de una nueva regla de filtrado (*Filter Rule*) en el firewall de MikroTik, configurada en la cadena input y con el protocolo ICMP habilitado.

CAPÍTULO IV

4.1. Resultado y análisis de la implementación.

Este capítulo presenta y analiza los resultados de las pruebas realizadas sobre la arquitectura de red implementada en el Laboratorio de Telecomunicaciones. El objetivo de estas evaluaciones es verificar de manera integral el correcto funcionamiento del sistema, desde la conectividad entre los distintos módulos hasta el establecimiento de las vecindades OSPF, el aprendizaje dinámico de rutas, la asignación automática de direcciones IP mediante DHCP, el funcionamiento de los dispositivos finales y el comportamiento del tráfico que circula en la red.

Para llevar a cabo las pruebas, se trabajó directamente con los equipos MikroTik mediante comandos ejecutados en la terminal de RouterOS y las herramientas gráficas disponibles en WinBox. Asimismo, se utilizó Wireshark para capturar y analizar el intercambio de paquetes, lo que permitió confirmar la presencia y el comportamiento esperado de los protocolos implementados.

El análisis se estructuró por módulos, respetando las características y funciones específicas de cada uno. En los módulos A, B y C se prestó especial atención a la conectividad y al funcionamiento de las cámaras IP. En los módulos D y E, el enfoque se centró en la

comunicación general de la red, el aprendizaje dinámico de rutas y los mecanismos de administración y seguridad del tráfico.

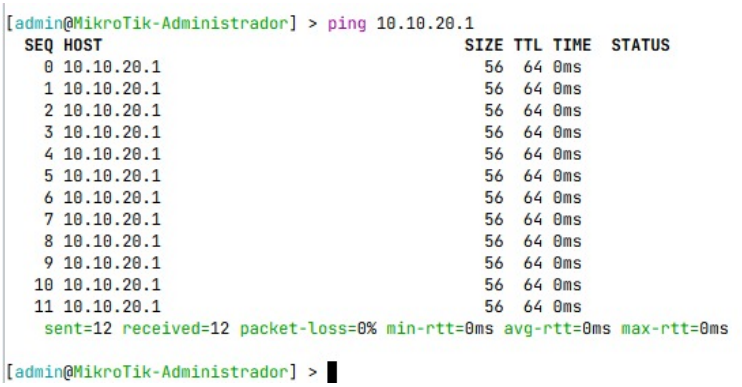
4.1.1. Conectividad del Módulo A.

- **Conectividad con el Router Principal.**

Para verificar la conectividad entre el módulo A y el router administrador, se ejecutó una prueba de ping desde la terminal MikroTik del módulo A hacia la dirección *10.10.20.1*, correspondiente a la interfaz de interconexión del router administrador.

En la Figura 99, se enviaron 12 paquetes ICMP y los 12 llegaron correctamente a destino, lo que se traduce en un 0 % de pérdida de paquetes además, el valor del TTL se mantuvo constante durante toda la prueba, señal de que las respuestas viajaron siempre por la misma ruta.

Figura 99. *Resultado del comando ping hacia 10.10.20.1*



Nota. Prueba de ping desde el Módulo A hacia el router administrador (10.10.20.1): 12 paquetes ICMP enviados y recibidos, con 0% de pérdida.

En cuanto a los tiempos de respuesta, RouterOS reportó un valor de 0 ms. Es importante aclarar que esto no significa que la latencia sea físicamente nula, sino que el tiempo de respuesta fue tan bajo que quedó por debajo de la resolución.

La ausencia de pérdida de paquetes confirma que tanto el enlace físico como la configuración IP entre el módulo A y el router administrador funcionan correctamente. Debido a que la dirección evaluada pertenece a un segmento de interconexión directamente conectado, esta prueba valida principalmente la conectividad del enlace y la configuración IP, pero no el comportamiento del protocolo OSPF.

- **Estado de la vecindad OSPF.**

Para comprobar que las adyacencias OSPF del módulo A se establecieron correctamente, se ejecutó el siguiente comando en la terminal de RouterOS: /*routing ospf neighbor print* esta instrucción permite visualizar en la terminal información clave sobre el vecino OSPF su identificador, la interfaz por la que se establece la comunicación.

Cuando este estado aparece como Full, significa que ambos routers lograron intercambiar por completo su información de estado de enlace y sincronizar correctamente sus bases de datos OSPF.

En la Figura 100, se identificaron 4 routers vecinos a través de la interfaz bridgelan, todos con estado *Full (router-id 5.5.5.5, 3.3.3.3, 2.2.2.2 y 4.4.4.4),* eso indica que la base de datos de enlaces (LSDB) entre el Módulo A y cada vecino está completamente sincronizada.

Figura 100. *Estado de las adyacencias OSPF del Módulo A.*

Nota. Resultado del comando */routing ospf neighbor print* en el Módulo A, mostrando 4 vecinos OSPF en estado Full *(router-id 5.5.5.5, 3.3.3.3, 2.2.2.2 y 4.4.4.4).*

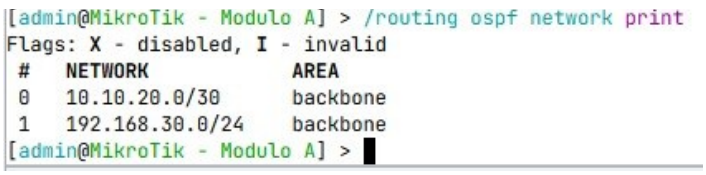
Este resultado confirma que el protocolo OSPF se encuentra activo y funcionando correctamente en el módulo A. La presencia de vecinos en estado Full evidencia que las adyacencias OSPF se han establecido de forma satisfactoria y que las bases de datos de estado de enlace se encuentran sincronizadas entre los routers vecinos

- **Redes anunciadas por OSPF.**

Para comprobar las redes anunciadas por el Módulo A, ejecutamos el comando */routing ospf network print* en la terminal de MikroTik este comando muestra el listado de redes configuradas para ser publicadas dentro del proceso OSPF, junto con el área a la que pertenecen.

En la Figura 101, se observa el Módulo A anuncia dos redes dentro del área backbone la red *10.10.20.0/30*, correspondiente al enlace de interconexión con el router principal, y la red *192.168.30.0/24*, correspondiente a la subred local asignada al Módulo A.

Figura 101. *Redes anunciadas por el Módulo A en OSPF.*



Nota. Redes anunciadas por el Módulo A mediante OSPF: 10.10.20.0/30 (enlace de interconexión) y 192.168.30.0/24 (subred local), dentro del área backbone.

Los resultados evidencian que el módulo A participa correctamente en el proceso de enrutamiento dinámico OSPF, al anunciar tanto su red de interconexión como su red local dentro del área backbone (área 0), conforme al diseño de área.

Esto garantiza que los demás routers de la topología puedan calcular rutas válidas hacia la *subred 192.168.30.0/24* sin necesidad de configuración manual, cumpliendo con el objetivo de dinamismo y escalabilidad planteado para el sistema de comunicaciones seguras.

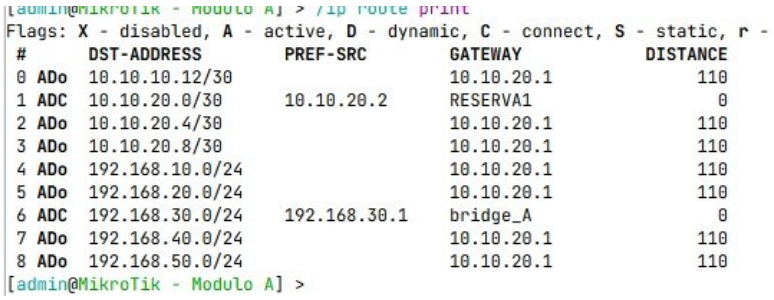
- **Tablas de enrutamiento.**

Para validar el estado de la tabla de enrutamiento, se ejecutó el comando /ip route print en la terminal MikroTik del módulo A. Esta instrucción permite visualizar las rutas registradas en el equipo, su origen, la red de destino, el gateway o interfaz de salida y la distancia administrativa asociada a cada ruta.

Como se muestra en la Figura 102, la tabla de enrutamiento del módulo A registra nueve entradas. Dos corresponden a redes conectadas directamente: 10.10.20.0/30, asociada a la interfaz RESERVA1, y 192.168.30.0/24.

Las siete rutas restantes fueron aprendidas dinámicamente mediante OSPF y se encuentran activas. Estas rutas permiten alcanzar las redes 10.10.10.12/30, 10.10.20.4/30, 10.10.20.8/30, 192.168.10.0/24, 192.168.20.0/24, 192.168.40.0/24 y 192.168.50.0/24 a través del gateway 10.10.20.1, con una distancia administrativa de 110, valor predeterminado para las rutas OSPF.

Figura 102. *Tabla de rutas del Módulo A.*



```
[admin@MikroTik - Modulo A] > /ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r -
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADo  10.10.10.12/30                     10.10.20.1              110
 1 ADC  10.10.20.0/30      10.10.20.2      RESERVA1                  0
 2 ADo  10.10.20.4/30                      10.10.20.1              110
 3 ADo  10.10.20.8/30                      10.10.20.1              110
 4 ADo  192.168.10.0/24                    10.10.20.1              110
 5 ADo  192.168.20.0/24                    10.10.20.1              110
 6 ADC  192.168.30.0/24    192.168.30.1    bridge_A                  0
 7 ADo  192.168.40.0/24                    10.10.20.1              110
 8 ADo  192.168.50.0/24                    10.10.20.1              110
[admin@MikroTik - Modulo A] >
```

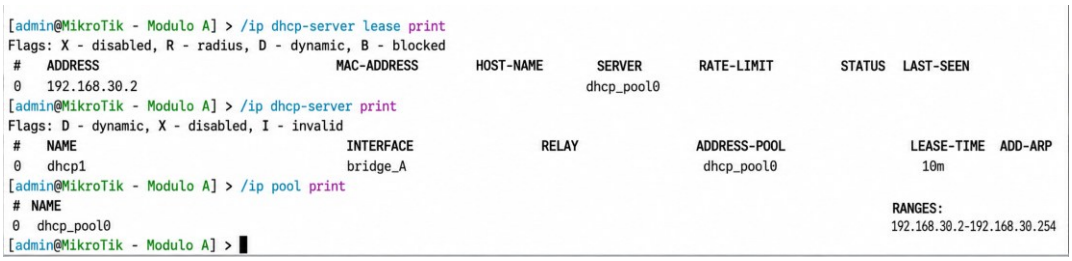
Nota. Tabla de enrutamiento del Módulo A con 9 entradas: 2 redes conectadas directamente y 7 rutas aprendidas por OSPF con distancia administrativa 110.

Los resultados confirman que OSPF calculó e instaló automáticamente en la tabla de enrutamiento las rutas hacia los segmentos remotos de la topología, sin requerir configuración manual de rutas estáticas. La presencia de nueve rutas activas, incluidas las redes directamente conectadas y las rutas aprendidas mediante OSPF, evidencia que el módulo A cuenta con información de enrutamiento para alcanzar las subredes de los demás módulos y los segmentos asociados al router administrador.

- **Funcionamiento del servidor DHCP con cámara.**

En la Figura 103, se muestra el servidor DHCP registró una concesión activa para la cámara IP, asignándole automáticamente la dirección *192.168.30.254* dentro del rango configurado para la subred del Módulo A, sin requerir configuración manual en el dispositivo final.

Figura 103. *Concesión DHCP entregada a la cámara IP.*



```
[admin@MikroTik - Modulo A] > /ip dhcp-server lease print
Flags: X - disabled, R - radius, D - dynamic, B - blocked
 #    ADDRESS          MAC-ADDRESS       HOST-NAME      SERVER       RATE-LIMIT      STATUS  LAST-SEEN
 0    192.168.30.2                                      dhcp_pool0
[admin@MikroTik - Modulo A] > /ip dhcp-server print
Flags: D - dynamic, X - disabled, I - invalid
 #    NAME             INTERFACE          RELAY          ADDRESS-POOL          LEASE-TIME  ADD-ARP
 0    dhcp1            bridge_A                          dhcp_pool0            10m
[admin@MikroTik - Modulo A] > /ip pool print
 # NAME                                                                       RANGES:
 0  dhcp_pool0                                                               192.168.30.2-192.168.30.254
[admin@MikroTik - Modulo A] >
```

Nota. Autorización DHCP activa asignada a la cámara IP del Módulo A (192.168.30.254), dentro del rango configurado.

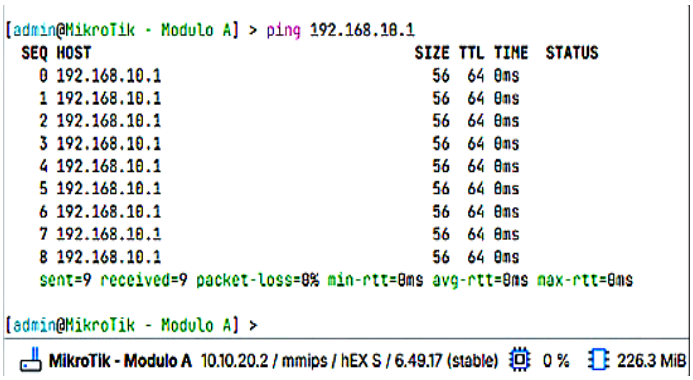
El servicio DHCP opera correctamente en el segmento del módulo A, completando el proceso DORA (*Discover*, *Offer*, *Request*, *Acknowledge*) y entregando direccionamiento dinámico a los dispositivos finales.

Estos resultados validan el objetivo de reducir la configuración manual de direcciones IP planteado en el Capítulo I y demuestran la correcta integración entre el servidor DHCP y la subred 192.168.30.0/24 definida en el diseño de red.

Para confirmar la comunicación bidireccional entre el módulo A y la cámara IP, se ejecutó el comando ping 192.168.10.1 desde la terminal del módulo A hacia la dirección IP asignada a la cámara.

En la Figura 104, la prueba de *ping* registró un 0% de pérdida de paquetes (packet-loss=0 %), lo que confirma que todos los paquetes ICMP enviados fueron respondidos correctamente por la cámara.

Figura 104. *Resultado del ping hacia la cámara IP.*



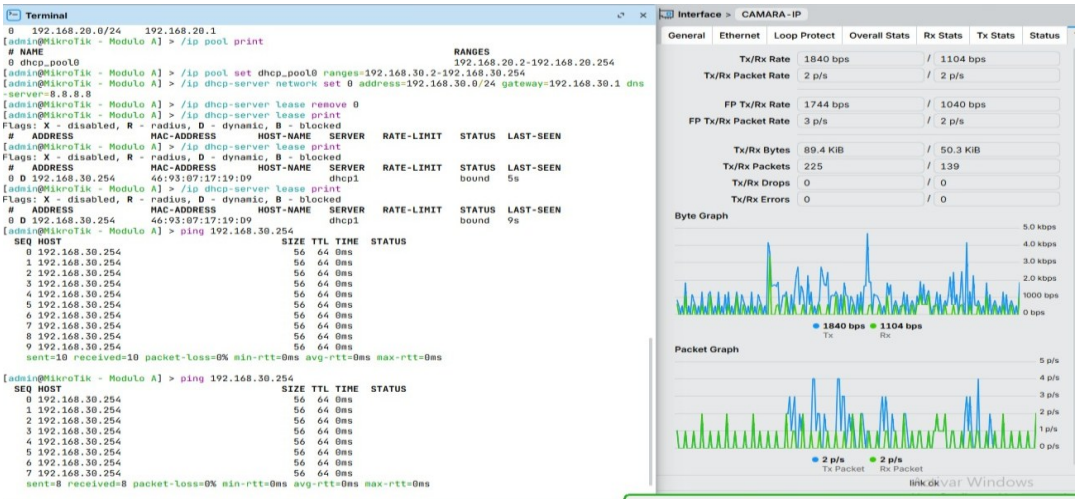
Nota. Prueba de *ping* hacia la cámara IP del módulo A, con 0% de pérdida de paquetes.

- **Tráfico de la interfaz de la cámara.**

La presencia del LSA del módulo B en la base de datos de estado de enlace del router principal evidencia que el intercambio de información de topología entre ambos routers se realizó correctamente. Esto garantiza que el cálculo de rutas mediante el algoritmo SPF refleje de manera adecuada la topología real de la red.

En la Figura 105, la interfaz CAMARA-IP registró tráfico activo de transmisión (Tx) y recepción (Rx), lo que indica un intercambio continuo de datos entre la cámara y el router.

Figura 105. *Gráfico de tráfico Tx/Rx de la interfaz CAMARA-IP.*



Nota. Tráfico de transmisión (Tx) y recepción (Rx) registrado en la interfaz CAMARA-IP del módulo A, que evidencia transmisión activa de datos.

El tráfico bidireccional confirma que la cámara IP no solo se encuentra conectada y direccionada correctamente, sino que también está transmitiendo datos de forma activa a través de la red implementada. Estos resultados validan integralmente el funcionamiento del módulo A como segmento de videovigilancia dentro del sistema de comunicaciones seguro y cierran el ciclo de pruebas para este módulo.

- **Análisis y prueba de tráfico.**

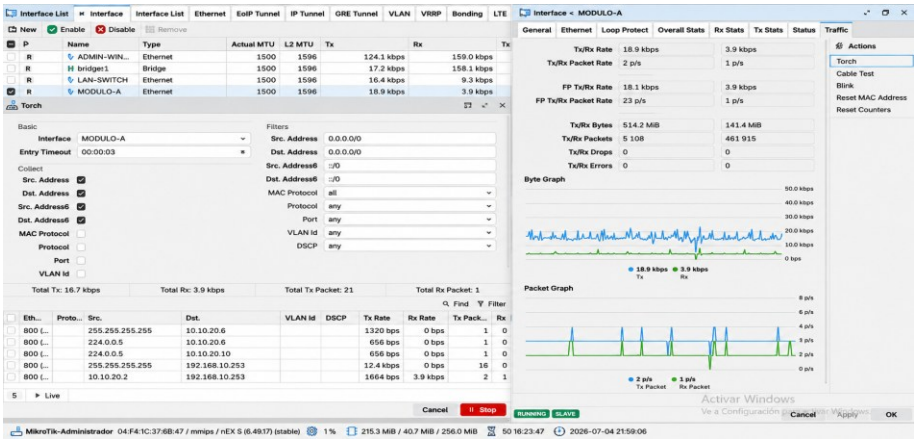
En Interfaz módulo-A, el estado aparece como running, lo que significa que el enlace físico está levantado, también se observa tráfico de transmisión y recepción:

- Tx: aproximadamente 18.9 kbps
- Rx: aproximadamente 3.9 kbps

Esto es importante porque indica que el puerto no está presentando errores físicos ni pérdidas de paquetes el cableado y la conexión Ethernet del Módulo A están funcionando correctamente.

En la figura 106, el módulo A sí tiene tráfico de red, el enlace está activo y no presenta errores. Además, se observa tráfico OSPF, por lo que la comunicación dinámica entre routers está funcionando.

Figura 106. *Análisis del Módulo A.*



Nota. Estado y tráfico de la interfaz del Módulo A (aproximadamente 18.9 kbps Tx y 3.9 kbps Rx), incluyendo tráfico OSPF, confirmando el enlace activo sin errores.

4.1.2. Conectividad del Módulo B.

- **Conexión del Módulo B hasta el administrador.**

Mediante la comunicación directa con el módulo B a través del enlace de interconexión configurado en OSPF, se ejecutó el comando ping 10.10.20.6 desde la terminal del MikroTik principal. Esta dirección IP corresponde al enlace de interconexión con el módulo B y se utilizó para comprobar la disponibilidad y estabilidad de dicho enlace.

La prueba de *ping* registró un 0% de pérdida de paquetes (packet-loss=0 %), lo que confirma que todos los paquetes ICMP enviados fueron respondidos correctamente por el módulo B, como se observa en la Figura 107.

Figura 107. *Resultado del ping desde el Principal hacia 10.10.20.6 (Módulo B)*

```
[admin@MikroTik-Administrador] > ping 10.10.20.6
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.10.20.6                                 56  64 0ms
    1 10.10.20.6                                 56  64 0ms
    2 10.10.20.6                                 56  64 0ms
    3 10.10.20.6                                 56  64 0ms
    4 10.10.20.6                                 56  64 0ms
    5 10.10.20.6                                 56  64 0ms
    6 10.10.20.6                                 56  64 0ms
    7 10.10.20.6                                 56  64 0ms
    8 10.10.20.6                                 56  64 0ms
    9 10.10.20.6                                 56  64 0ms
   10 10.10.20.6                                 56  64 0ms
   11 10.10.20.6                                 56  64 0ms
   12 10.10.20.6                                 56  64 0ms
    sent=13 received=13 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@MikroTik-Administrador] >
```

Nota. Prueba de ping desde el MikroTik Principal hacia el enlace de interconexión con el Módulo B (10.10.20.6), con 0% de pérdida de paquetes.

El resultado confirma que el enlace físico y lógico entre el MikroTik Principal y el Módulo B se encuentra correctamente establecido, sin pérdida de paquetes ni interrupciones, lo que valida la conectividad punto a punto definida en el diseño.

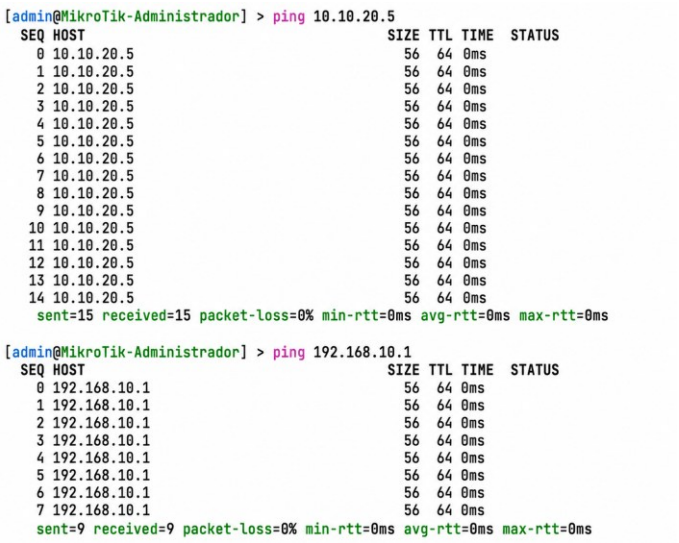
- **Funcionamiento bidireccional del Módulo B.**

Verificar la comunicación bidireccional entre el Módulo B y el MikroTik Principal, tanto a nivel del enlace de interconexión como de la red LAN del Principal desde la terminal del Módulo B ejecutamos dos pruebas de conectividad.

- El primero, el comando *ping 10.10.20.5,* correspondiente a la dirección del enlace de interconexión con el Principal.
- El segundo, el comando *ping 192.168.10.1*, correspondiente a la puerta de enlace de la subred LAN del Principal.

La figura 108, las pruebas de ping obtuvieron respuesta exitosa, confirmando comunicación bidireccional tanto hacia el enlace de interconexión *(10.10.20.5)* como hacia la red LAN del *Principal (192.168.10.1).*

Figura 108. *Resultado del ping bidireccional del módulo B.*



Nota. Se realizaron pruebas de *ping* bidireccionales desde el Módulo B hacia el enlace de interconexión (10.10.20.5) y hacia la LAN del equipo Principal (192.168.10.1), ambas con resultados satisfactorios.

Los resultados confirman que la comunicación entre el Módulo B y el Principal funciona correctamente en ambos sentidos. Esto valida que las rutas calculadas mediante OSPF son simétricas y que no existen restricciones de firewall que bloqueen el tráfico de retorno entre ambos extremos del enlace.

- **Verificar el intercambio de LSAs.**

Se debe confirmar que el MikroTik Principal haya recibido e incorporado correctamente el LSA (*Link-State Advertisement*) correspondiente al Módulo B en su base de datos de estado de enlace (LSDB).

En la Figura 109, el listado de LSAs incluye el Router ID 5.5.5.5, correspondiente al Módulo B. Esto confirma que la información topológica de dicho módulo fue recibida e incorporada correctamente en la LSDB del MikroTik Principal.

Figura 109. *LSA del Módulo B (Router ID 5.5.5.5) en la base de datos OSPF del Principal.*

```
[admin@MikroTik-Administrador] > /routing ospf lsa print
AREA                                    TYPE        ID            ORIGINATOR     SEQUENCE-NUMBER        AGE
backbone                                router      1.1.1.1       1.1.1.1             0x8000001C        762
backbone                                router      2.2.2.2       2.2.2.2             0x80000016        768
backbone                                router      3.3.3.3       3.3.3.3             0x80000016        768
backbone                                router      4.4.4.4       4.4.4.4             0x80000016        768
backbone                                router      5.5.5.5       5.5.5.5             0x80000007        764
backbone                                network     10.10.10.14   4.4.4.4             0x80000013        771
backbone                                network     10.10.20.2    2.2.2.2             0x80000013        773
backbone                                network     10.10.20.6    5.5.5.5             0x80000002        764
backbone                                network     10.10.20.10   3.3.3.3             0x80000013        770
[admin@MikroTik-Administrador] >
```

Nota. Listado de LSAs recibidos por el MikroTik Principal, en el que se muestra el Router ID 5.5.5.5, correspondiente al Módulo B.

La presencia del LSA del Módulo B en la base de datos de la Principal evidencia que el intercambio de información de estado de enlace entre ambos routers se realizó de forma íntegra, lo que garantiza que el cálculo de rutas mediante el algoritmo SPF refleja fielmente la topología real de la red.

- **Verificación de DNS.**

Se debe comprobar que el Módulo B cuente con un servicio de resolución de nombres de dominio (DNS) correctamente configurado. Esto permite traducir nombres de dominio en direcciones IP, de modo que los dispositivos conectados a la red puedan acceder a Internet y a servicios externos sin requerir configuraciones manuales en cada equipo.

Para ello, se ejecuta el comando */ip dns print* en la terminal de WinBox. El resultado confirma que el router tiene configurados dos servidores DNS públicos. Como se muestra en la Figura 110, esta configuración proporciona redundancia: si uno de los servidores no responde, el router puede utilizar el segundo, lo que mejora la disponibilidad y continuidad del servicio de resolución de nombres.

Figura 110. *Verificar resolución DNS.*

```
[admin@MikroTik-ModuLo B] > ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 8.8.8.8                                    56 111 36ms
    1 8.8.8.8                                    56 111 36ms
    sent=2 received=2 packet-loss=0% min-rtt=36ms avg-rtt=36ms max-rtt=36ms

[admin@MikroTik-ModuLo B] > /ip dns print
                      servers: 8.8.8.8,1.1.1.1
             dynamic-servers:
              use-doh-server:
             verify-doh-cert: no
       allow-remote-requests: yes
         max-udp-packet-size: 4096
        query-server-timeout: 2s
         query-total-timeout: 10s
     max-concurrent-queries: 100
max-concurrent-tcp-sessions: 20
                 cache-size: 2048KiB
              cache-max-ttl: 1w
                 cache-used: 25KiB
```

Nota. Se muestran los dos servidores DNS públicos configurados y el parámetro allow-remote-requests habilitado.

El parámetro allow-remote-requests indica que el router está habilitado para aceptar y resolver consultas DNS provenientes de otros dispositivos de la red. De esta manera, los equipos conectados a los módulos A, B, C, D y E pueden utilizar el MikroTik como servidor DNS, sin necesidad de configurar servidores DNS externos de forma individual en cada dispositivo.

- **Verificar enlace físico de la cámara.**

Verificación de enlace físico: Mediante el comando /interface ethernet monitor ether3 once se comprobó el estado del puerto ether3 conectado a la cámara IP. El valor status: link-ok, mostrado en la Figura 111, confirma que el enlace físico Ethernet se encuentra activo. Esta comprobación de capa 1 debe realizarse antes de validar la conectividad IP o el acceso a la cámara.

Figura 111. *Verificar enlace físico de la cámara.*

```
[admin@MikroTik-ModuLo B] > /interface ethernet monitor ether3 once
                     name: ether3
                   status: link-ok
          auto-negotiation: done
                     rate: 100Mbps
              full-duplex: yes
           tx-flow-control: no
           rx-flow-control: no
              advertising: 10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
  link-partner-advertising: 10M-half,10M-full,100M-half,100M-full,1000M-full
[admin@MikroTik-ModuLo B] > /interface bridge host print                                BRIDGE
Flags: X - disabled, I - invalid, D - dynamic, L - local, E - external                  bridge_B
 #       MAC-ADDRESS        VID ON-INTERFACE
 0   DL  F4:1E:57:11:FA:15  _   bridge_B
```

Nota. Estado del enlace físico del puerto ether3 del Módulo B, verificado mediante el comando /interface ethernet monitor ether3 once, con resultado status: link-ok.

El valor rate: 100Mbps confirma que el puerto ether3 opera a una velocidad de 100 Mbps. Esta capacidad es suficiente para el tráfico de video de una cámara IP PTZ en condiciones normales de operación, por lo que el enlace físico no representa un cuello de botella, como se observa en la Figura 112.

La verificación de la capa física debe realizarse antes de evaluar el direccionamiento IP, la conectividad o el acceso a la cámara.

Figura 112. *Estado de conectividad de la cámara.*

Nota. Velocidad de negociación del enlace (rate: 100 Mbps) en el puerto ether3 del Módulo B, conectado a la cámara IP.

- **Análisis y prueba de tráfico.**

Para comprobar que el enlace de interconexión entre el MikroTik Principal y el Módulo B transporta tráfico de red correctamente, se accede a la pestaña **Traffic** de la interfaz correspondiente en WinBox.

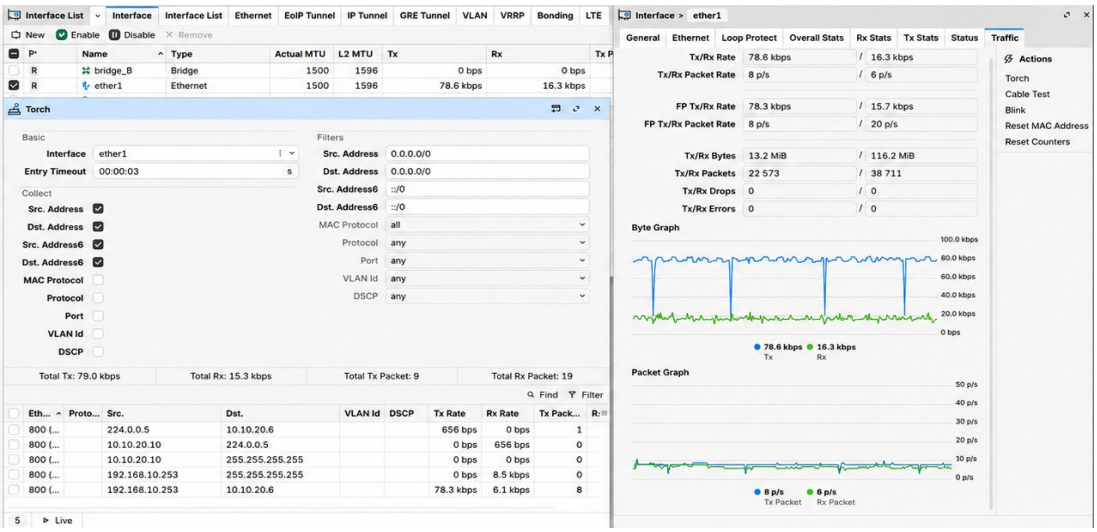
En esta sección se monitorean en tiempo real los valores de transmisión (**Tx**) y recepción (**Rx**), los cuales permiten confirmar la existencia de tráfico bidireccional a través del enlace.

En la ventana de tráfico de la interfaz ether1 se muestran los siguientes valores aproximados:

- Tx Rate: 78.6 kbps
- Rx Rate: 16.3 kbps
- Tx/Rx Packet Rate: 8 p/s y 6 p/s

Se observa en la Figura 113, los valores de Rx y Tx de la interfaz MÓDULO-B se incrementaron de manera consistente durante la ejecución del ping, evidenciando el tránsito activo de paquetes a través del enlace.

Figura 113. *Verificar la ruta por defecto.*



Nota. Tráfico de transmisión y recepción en la interfaz ether1 hacia el Módulo B (Tx: 78.6 kbps, Rx: 16.3 kbps), incrementándose durante la prueba de ping.

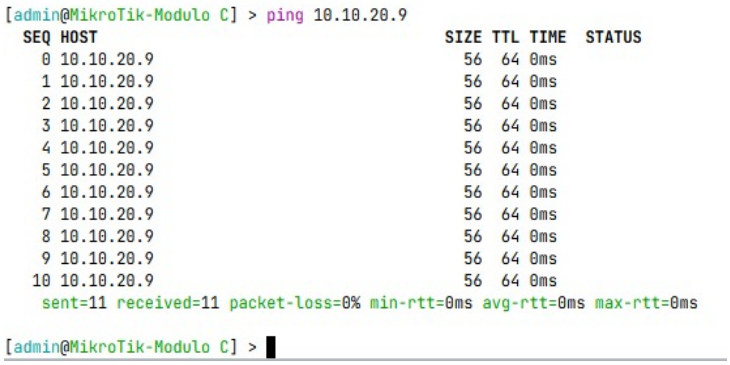
El incremento simultáneo de los contadores Tx y Rx confirma que el enlace físico y lógico entre el Principal y el Módulo B se encuentra plenamente operativo y transportando tráfico bidireccional en tiempo real.

4.1.3. Conectividad del Módulo C.

- **Verificar la comunicación entre el Módulo C y el router principal.**

Mediante el comando ping 10.10.20.9, ejecutado desde el Módulo C, se verificó la disponibilidad del enlace de interconexión con el MikroTik Principal. En la Figura 114, se observa la recepción de 10 de 10 paquetes ICMP, con 0% de pérdida, lo que confirma la conectividad bidireccional entre ambos equipos.

Figura 114. *Resultado del ping desde el Módulo C hacia 10.10.20.9 (Principal).*



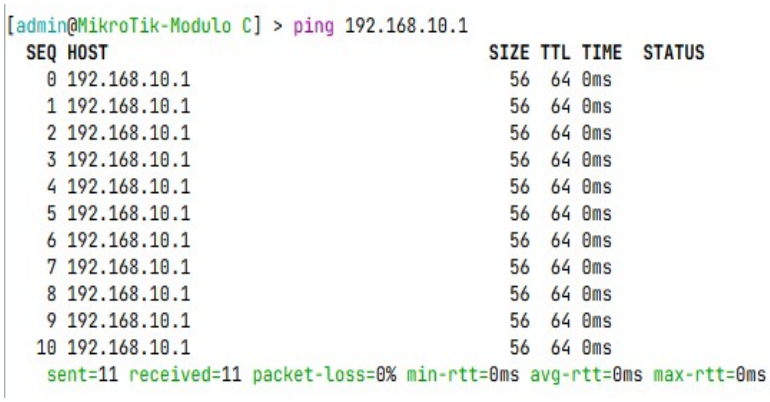
Nota. Prueba de ping desde el Módulo C hacia el MikroTik Principal (10.10.20.9): 10 paquetes enviados y recibidos, con 0% de pérdida.

- **Comunicación con la LAN del Principal.**

Desde la terminal del Módulo C ejecutamos el comando ping 192.168.10.1, correspondiente a la puerta de enlace de la red LAN del Principal verificar que el Módulo C alcanza la subred LAN del MikroTik Principal a través de la ruta calculada por OSPF.

Como se muestra en la Figura 115, la comunicación fue exitosa y no se registró pérdida de paquetes. Este resultado confirma la conectividad entre el Módulo C y la LAN del MikroTik Principal, validando el funcionamiento del enrutamiento dinámico.

Figura 115. *Resultado del ping desde el Módulo C hacia la LAN del Principal 192.168.10.*



Nota. Prueba de ping desde el Módulo C hacia la LAN del Principal (192.168.10.1), con comunicación exitosa y sin pérdida de paquetes.

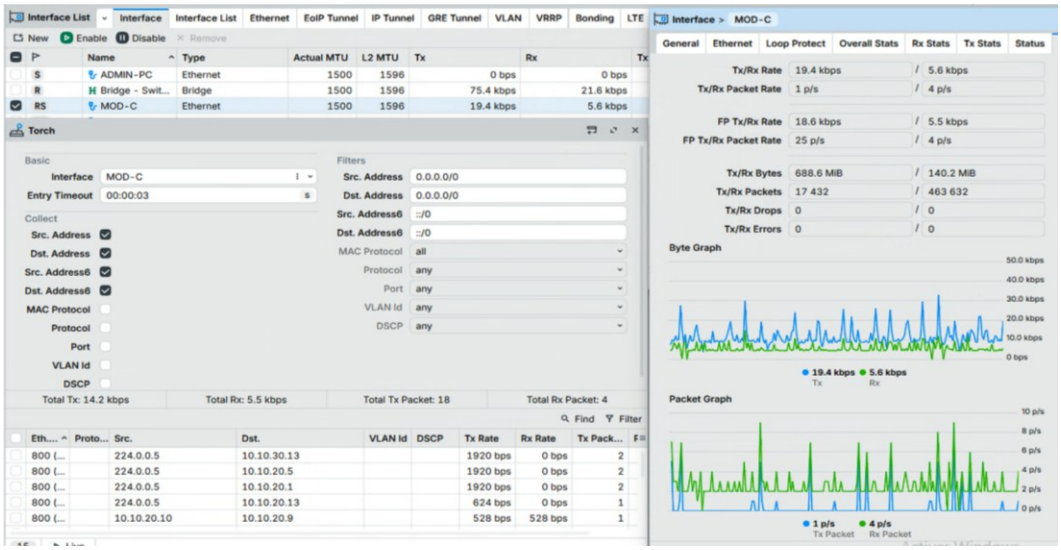
- **Verificar tráfico y estabilidad del enlace.**

Esta prueba tiene como propósito evaluar el comportamiento del tráfico de red en tiempo real sobre la interfaz correspondiente al Módulo C, así como confirmar la actividad del protocolo de enrutamiento dinámico OSPF

- Transmisión (Tx): 19.4 kbps
- Recepción (Rx): 5.6 kbps

Esto demuestra que en la figura 116, no existen paquetes descartados ni errores de transmisión a nivel físico o de enlace, lo cual, valida la calidad del cableado, la correcta negociación ethernet y la estabilidad general del puerto el análisis con Torch aporta la evidencia más significativa: se identifica tráfico dirigido a la dirección *multicast 224.0.0.5,* correspondiente al grupo reservado para el protocolo OSPF *(All OSPF Routers).*

Figura 116. *Tráfico de red en el módulo C.*



Nota. Análisis de tráfico con Torch en el Módulo C, identificando tráfico dirigido a la dirección multicast 224.0.0.5 (All OSPF Routers).

La presencia constante de este tráfico confirma que el Módulo C está enviando y recibiendo actualizaciones de estado de enlace (LSAs) con los routers vecinos, es decir, que la vecindad OSPF se mantiene activa y las tablas de enrutamiento se actualizan dinámicamente.

4.1.4. Conectividad del Módulo D.

- **Verificar el enlace con el MikroTik Principal.**

Desde la terminal del Módulo D se ejecutó el siguiente comando: text/ping 10.10.10.14 count=5. La dirección 10.10.10.14 corresponde al enlace de interconexión con el MikroTik Principal. La prueba permite verificar la conectividad entre ambos equipos a través del enlace punto a punto definido en la topología.

Como se observa en la Figura 117, se enviaron y recibieron correctamente los cinco paquetes ICMP, sin registrar pérdida de paquetes. Este resultado confirma que el enlace de interconexión entre el Módulo D y el MikroTik Principal se encuentra operativo.

Figura 117. *Resultado del ping desde el Módulo D hacia 10.10.30.13*

```
[admin@MikroTik - Modulo D] > ping 10.10.30.13
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.10.30.13                                56  64 0ms
    1 10.10.30.13                                56  64 0ms
    2 10.10.30.13                                56  64 0ms
    3 10.10.30.13                                56  64 0ms
    4 10.10.30.13                                56  64 0ms
    5 10.10.30.13                                56  64 0ms
    6 10.10.30.13                                56  64 0ms
    7 10.10.30.13                                56  64 0ms
    8 10.10.30.13                                56  64 0ms
    9 10.10.30.13                                56  64 0ms
    sent=10 received=10 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Nota. Prueba de ping desde el Módulo D hacia el MikroTik Principal (10.10.10.14): 10 paquetes enviados y recibidos, con 0% de pérdida.

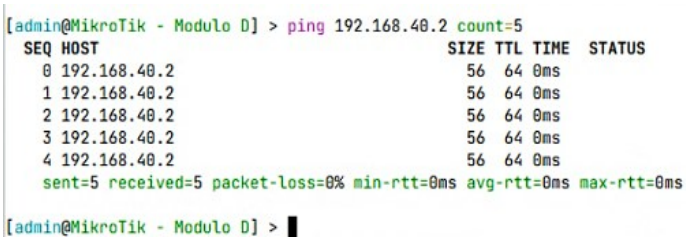
- **Verificar la LAN del Módulo D.**

Para verificar la conectividad de la red LAN del Módulo D, se realizó una prueba de ping hacia un dispositivo conectado a la subred 192.168.40.0/24. La recepción de respuestas ICMP sin pérdida de paquetes confirma la conectividad entre el router y el dispositivo final a través de la interfaz LAN.

La dirección 192.168.40.2/24 corresponde a la interfaz LAN configurada en el propio Módulo D. Como se muestra en la Figura 118, se recibieron correctamente los cinco paquetes ICMP, sin pérdida de paquetes.

Este resultado confirma que la dirección IP de la interfaz LAN se encuentra configurada y activa en el router. RouterOS asocia cada dirección IPv4 a una interfaz específica, lo que permite comprobar su configuración mediante la tabla de direcciones IP

Figura 118. *Resultado del ping hacia la LAN del Módulo D.*



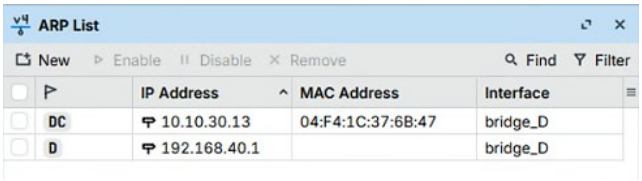
Nota. Prueba de ping hacia la propia interfaz LAN del Módulo D (192.168.40.2), confirmando su correcto funcionamiento.

- **Verificar la tabla ARP.**

Se verificó que el Módulo D reconoce al MikroTik Principal a nivel de capa 2 mediante WinBox, accediendo a la ruta IP → ARP para revisar las asociaciones entre direcciones IP y direcciones MAC.

Como se observa en la Figura 119, la dirección IP 10.10.30.13, correspondiente al MikroTik Principal, aparece asociada a una dirección MAC. Esto confirma que el Módulo D resolvió correctamente la dirección MAC del equipo remoto y que la comunicación de capa 2 en el enlace de interconexión se encuentra operativa

Figura 119. *Tabla ARP del Módulo D.*



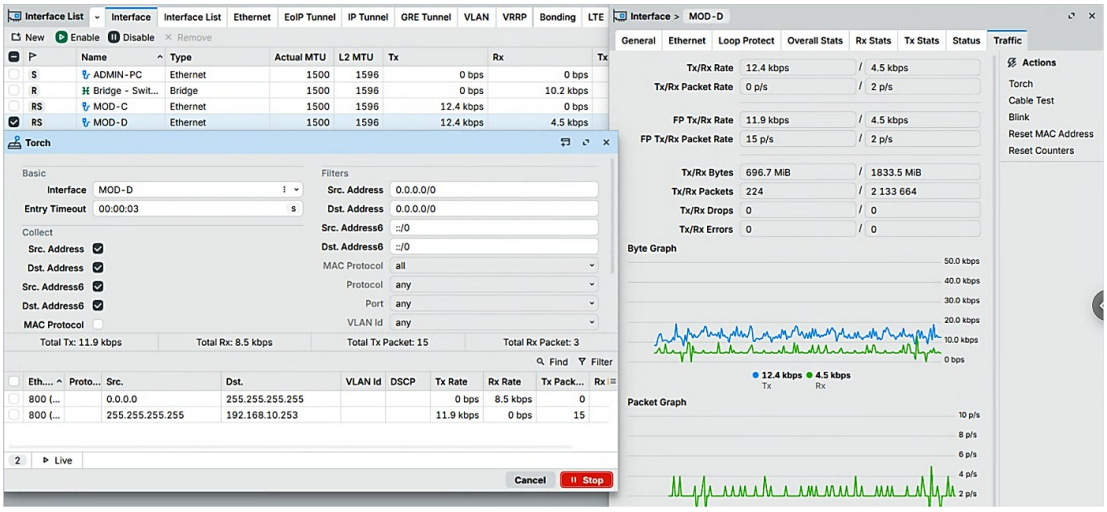
Nota. Tabla ARP del Módulo D con la dirección IP y MAC del MikroTik Principal (10.10.30.13), confirmando el reconocimiento a nivel de capa 2.

- **Verificar el tráfico de la interfaz.**

Se verificó que la interfaz ether2 del Módulo D transporta tráfico hacia el MikroTik Principal mediante WinBox.

Como se muestra en la Figura 120, los contadores de recepción (Rx) y transmisión (Tx) aumentan de forma consistente, lo que evidencia un intercambio activo de datos a través del enlace de interconexión. Esto confirma que la interfaz se encuentra transmitiendo y recibiendo tráfico correctamente

Figura 120. *Tráfico RX/TX de la interfaz.*



Nota. Contadores RX y TX de la interfaz ether2 del Módulo D, incrementándose de forma consistente, evidenciando el intercambio activo de tráfico con el router principal.

4.1.5. Conectividad del Módulo E.

- **Verificación del vecino OSPF.**

Para comprobar que OSPF estableció correctamente la adyacencia entre el Módulo E y el MikroTik Principal, se ejecutó el siguiente comando desde la terminal del Módulo E: text/routing ospf neighbor print. Este comando permite visualizar el estado de vecindad con el router 10.10.20.9. Como se observa en la Figura 125, dicho vecino aparece en estado Full.

Este resultado confirma que la adyacencia OSPF se estableció correctamente y que el intercambio de información de enrutamiento entre ambos routers se realizó de forma satisfactoria.

Figura 121. *Estado de la vecindad OSPF del Módulo E.*

```
[admin@MikroTik - Modulo E] >
[admin@MikroTik - Modulo E] > /routing ospf neighbor print
 0 instance=default router-id=1.1.1.1 address=10.10.20.9 interface=ether2 priority=1 dr-address=10.10.20.9 backup-dr-address=10.10.20.10 state="Full" state-changes=5 ls-retransmits=0 ls-requests=0
   db-summaries=0 adjacency=1w2d4h34m30s
[admin@MikroTik - Modulo E] >
[admin@MikroTik - Modulo E] >
```

Nota. Vecino OSPF del Módulo E (10.10.20.9) en estado Full, mediante el comando */routing ospf neighbor print.*

- **Conectividad con todas las LAN.**

Verificar la comunicación extrema a extremo entre el Módulo E y las redes de los módulos A, B, C y D, desde la terminal del Módulo E: */ping 192.168.10.1*, */ping 192.168.20.1*, */ping 192.168.30.1* y *ping /192.168.40.2,* correspondientes a las puertas de enlace de cada módulo. Las direcciones evaluadas corresponden a las puertas de enlace de las redes LAN de los módulos A, B, C y D. Como se observa en la Figura 122, las cuatro pruebas registraron un packet-loss=0%.

Estos resultados confirman que el Módulo E puede comunicarse correctamente con las redes de los demás módulos, validando la conectividad extrema a extremo en la topología implementada. El comando ping de RouterOS utiliza mensajes ICMP Echo para comprobar la disponibilidad IP de un destino y reporta métricas como paquetes enviados, recibidos y porcentaje de pérdida

Figura 122. *Resultados de ping del Módulo E hacia las LAN de los módulos A, B, C y D.*

```
[admin@MikroTik - Modulo E] > ping 192.168.10.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.10.1                               56  64 0ms
    1 192.168.10.1                               56  64 0ms
    2 192.168.10.1                               56  64 0ms
    3 192.168.10.1                               56  64 0ms
    4 192.168.10.1                               56  64 0ms
    5 192.168.10.1                               56  64 0ms
    sent=6 received=6 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@MikroTik - Modulo E] > ping 192.168.20.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.20.1                               56  63 0ms
    1 192.168.20.1                               56  63 0ms
    2 192.168.20.1                               56  63 0ms
    3 192.168.20.1                               56  63 0ms
    4 192.168.20.1                               56  63 0ms
    5 192.168.20.1                               56  63 0ms
    6 192.168.20.1                               56  63 0ms
    sent=7 received=7 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@MikroTik - Modulo E] > ping 192.168.40.2
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.40.2                               56  63 1ms
    1 192.168.40.2                               56  63 0ms
    2 192.168.40.2                               56  63 0ms
    3 192.168.40.2                               56  63 0ms
    4 192.168.40.2                               56  63 0ms
    5 192.168.40.2                               56  63 0ms
    6 192.168.40.2                               56  63 0ms
    sent=7 received=7 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=1ms
```

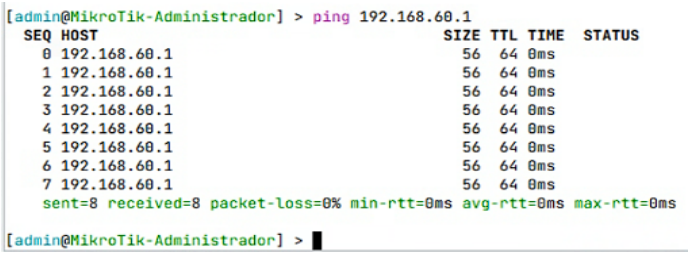
Nota. Pruebas de ping desde el Módulo E hacia las puertas de enlace de los módulos A, B, C y D, todas con 0% de pérdida de paquetes.

- **Conectividad con el Administrador.**

Analizar la comunicación bidireccional entre el Módulo E y el equipo Administrador ejecutamos el comando */ping 192.168.60.1* tanto desde el Módulo E hacia el Administrador, como desde el Administrador hacia el Módulo E, con el fin de validar la conectividad en ambos sentidos.

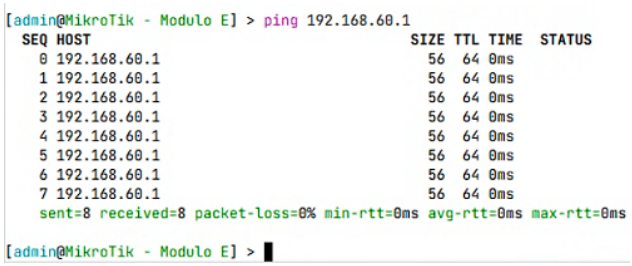
Como se observa en la Figura 123 y la Figura 1284, son ambas pruebas obtuvieron respuesta exitosa, sin pérdida de paquetes este resultado confirma que la comunicación entre el módulo E y el equipo Administrador opera correctamente en ambos sentidos, validando la conectividad bidireccional definida en el diseño de la red.

Figura 123. *Resultado del ping en el Administrador (192.168.60.1).*



Nota: Primera prueba de ping bidireccional entre el Módulo E y el equipo Administrador (192.168.60.1).

Figura 124. *Resultado del ping en el Módulo E (192.168.60.1).*



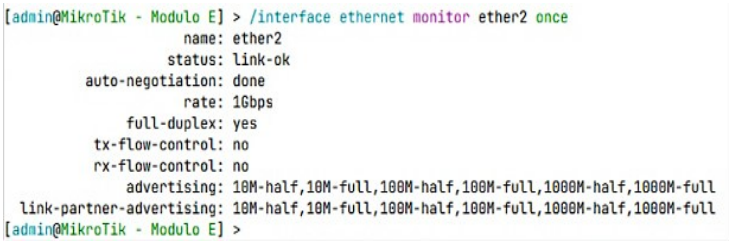
Nota. Segunda prueba de ping bidireccional entre el Módulo E y el equipo Administrador, confirmando la conectividad en ambos sentidos.

- **Verificación del enlace físico.**

Verificar que el enlace físico entre el Módulo E y el equipo Administrador opera con los parámetros esperados de velocidad y dúplex. Desde la terminal del Módulo E ejecutamos el comando /*interface ethernet monitor ether2 once*, con el fin de revisar el estado físico del enlace.

Como se observa en la Figura 125, el enlace mostró *status: link-ok, rate: 1Gbps y full-duplex: yes.* Es el enlace físico entre el módulo E y el equipo administrador opera correctamente a 1 Gbps en modo *Full-Duplex,* confirmando que la capa física no representa una limitante para el rendimiento del sistema implementado.

Figura 125. *Estado físico del enlace ether2 del Módulo E.*



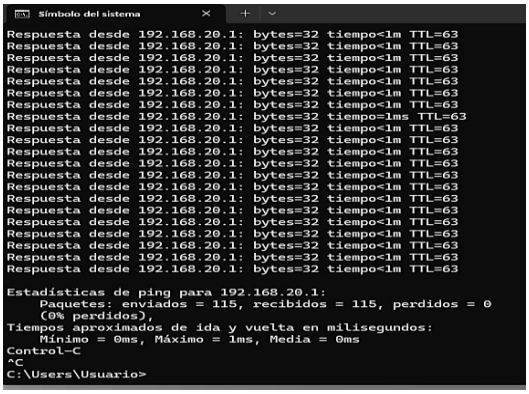
Nota. Estado del enlace físico entre el Módulo E y el equipo Administrador (status: link-ok, rate: 1 Gbps, full-duplex: yes).

4.2. Estudios de tráfico de la red.

4.2.1. Estudio de tráfico del Módulo A.

La red de administración conectada directamente al MikroTik Principal no corresponde a un módulo remoto. La red del Módulo A se identifica mediante la información anunciada por OSPF. Para validar su conectividad, se ejecutó el comando ping 192.168.30.1 desde la consola de Windows; la respuesta exitosa, mostrada en la Figura 126, confirma la comunicación con la puerta de enlace del módulo.

Figura 126. *Comando ejecutable al ping 192.168.30.1.*

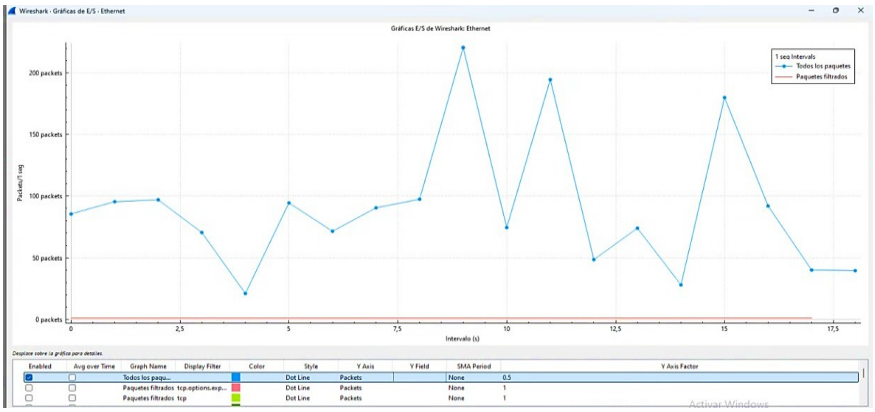


Nota. La captura muestra una prueba de conectividad mediante el comando ping a la dirección IP 192.168.20.1. Se enviaron y recibieron 115 paquetes, sin pérdidas (0 %), con tiempos de respuesta entre 0 y 1 ms. Esto confirma que la conexión con el dispositivo de destino es estable y funciona correctamente.

En la Figura 127, muestra la ventana de gráficas de entrada y salida de Wireshark para una conexión Ethernet la línea azul representa la cantidad total de paquetes capturados en intervalos de un segundo. El tráfico presenta variaciones considerables, con valores

aproximados de entre 20 y 220 paquetes por segundo y varios picos destacados durante la captura.

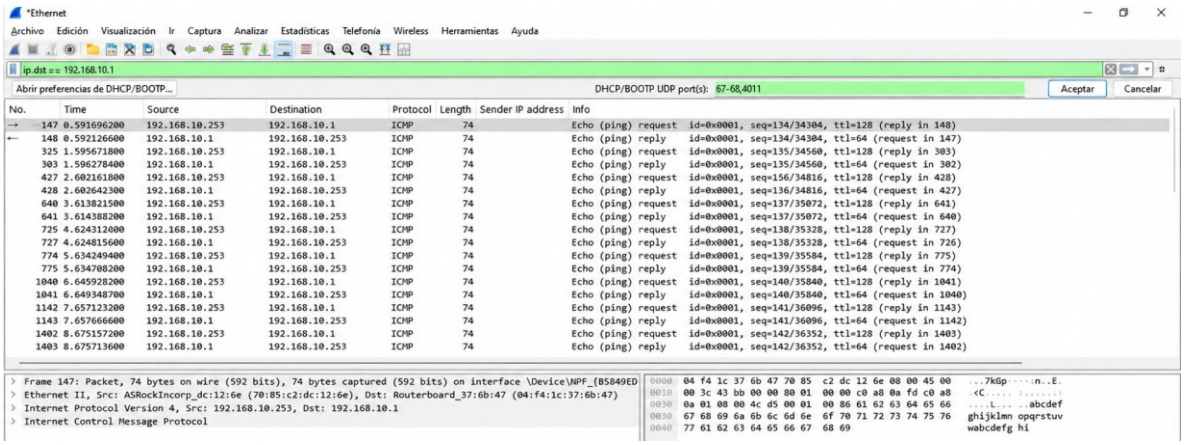
Figura 127. *Análisis del tráfico de red Ethernet mediante Wireshark.*



Nota. La gráfica permite observar el comportamiento del tráfico de red a lo largo del tiempo, identificando periodos de baja actividad y aumentos repentinos en la transmisión de paquetes. Los cambios reflejan una actividad de red variable, sin que la imagen por sí sola confirme fallos o anomalías.

En la Figura 128, muestra una captura de tráfico de red realizada con Wireshark, filtrada por la dirección IP 192.168.10.1, donde se observan solicitudes y respuestas del protocolo ICMP tipo Echo (ping) entre los equipos 192.168.10.253 y 192.168.10.1.

Figura 128. *Análisis de paquetes ICMP.*

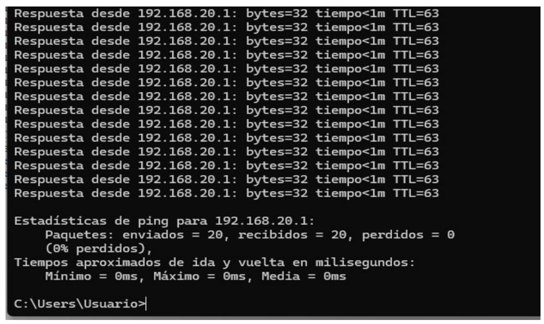


Nota: La captura permite comprobar la comunicación entre ambos dispositivos mediante el intercambio continuo de solicitudes y respuestas ping. Esto indica que existe conectividad entre los equipos durante el periodo analizado.

4.2.2. Estudio de tráfico del Módulo B.

La conectividad del Módulo B con su router administrador se ejecutó una prueba de ping desde línea de comandos (cmd) dirigida al gateway del módulo (192.168.20.1), en simultáneo con una captura de tráfico ICMP en Wireshark, con el fin de obtener tanto la tasa de pérdida de paquetes como el tiempo de ida y vuelta (RTT) con precisión de milisegundos esto se puede observar en la Figura 129.

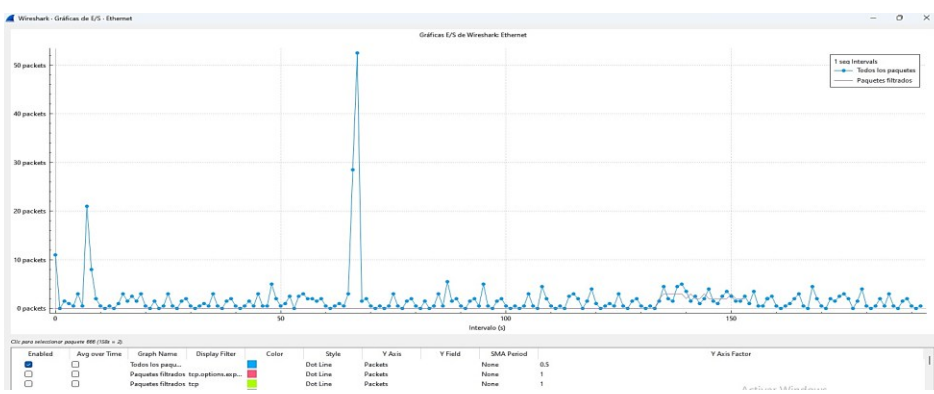
Figura 129. *Resultado del comando ping 192.168.20.1 -n 20 ejecutado desde el host.*



Nota. La imagen muestra una prueba de conectividad realizada desde el Símbolo del sistema mediante el comando ping a la dirección IP 192.168.20.1. Se enviaron y recibieron correctamente 20 paquetes de 32 bytes, sin pérdida de datos (0 %).

En la Figura 130, muestra una gráfica de entrada y salida de Wireshark correspondiente al tráfico de una red Ethernet, donde se representa la cantidad de paquetes capturados en intervalos de un segundo.

Figura 130. *Análisis del tráfico de paquetes en una red.*



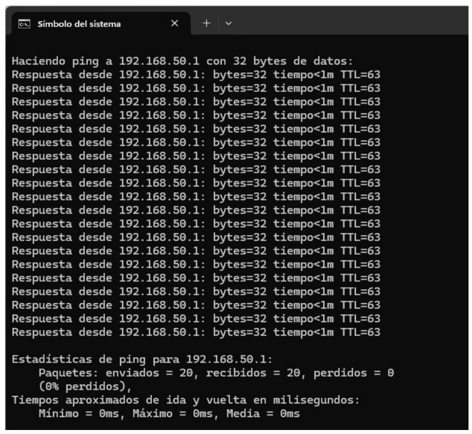
Nota. La gráfica de Wireshark muestra un tráfico generalmente bajo y estable, con dos aumentos importantes en la cantidad de paquetes capturados el pico principal supera los 50 paquetes y representa el momento de mayor actividad de la red durante el periodo analizado

4.2.3. Estudio de tráfico del Módulo C.

Para verificar la conectividad entre el Módulo C y su router administrador, se ejecutó una prueba de ping desde la línea de comandos de Windows hacia la dirección 192.168.60.1.

Como se observa en la Figura 131, el destino respondió correctamente a los 20 paquetes enviados, sin pérdida de paquetes (0%). Los tiempos de ida y vuelta estuvieron entre 0 y 1 ms, lo que evidencia una conexión activa y de baja latencia entre el equipo de origen y el destino.

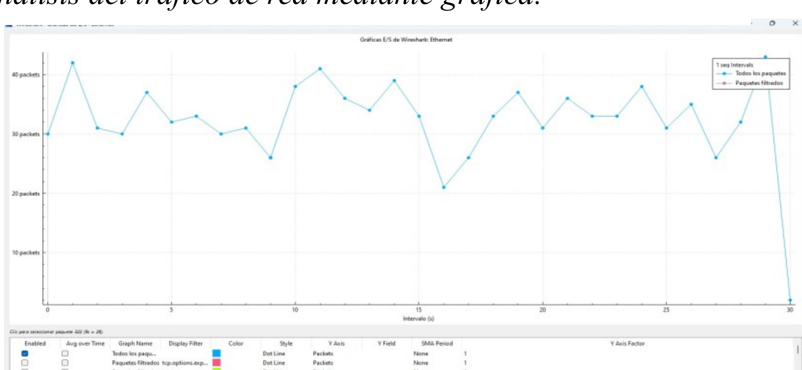
Figura 131. *Verificación de conectividad y latencia mediante paquetes ICMP.*



Nota. La prueba confirma una comunicación estable con el dispositivo 192.168.50.1, ya que los 20 paquetes ICMP fueron enviados y recibidos sin pérdidas. La latencia máxima de 1 ms evidencia una respuesta rápida dentro de la red.

En la Figura 132, se presenta la gráfica de Entrada/Salida generada mediante Wireshark, en la cual se representa el número de paquetes transmitidos por segundo en función del tiempo, correspondiente a un intervalo de captura de 30 segundos con muestreo cada 1 segundo.

Figura 132. *Análisis del tráfico de red mediante gráfica.*



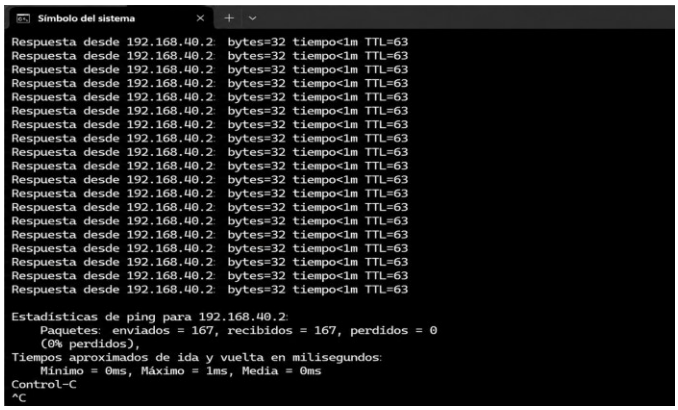
Nota. Se observa que el volumen de tráfico se mantiene la forma constante entre aproximadamente 20 y 42 paquetes por segundo a lo largo de los primeros 30 segundos de captura, sin presentar interrupciones prolongadas ni variaciones abruptas que sugieran fallos en la comunicación

4.2.4. Estudio de tráfico del Módulo D.

Para verificar la conectividad del Módulo D con su router administrador se ejecutó una prueba de ping desde línea de comandos "cmd" dirigida a la interfaz del router del módulo (192.168.40.2), en simultáneo con una captura de tráfico ICMP en Wireshark, con el fin de obtener tanto la tasa de pérdida de paquetes como el tiempo de ida y vuelta (RTT) con precisión de milisegundos.

En la Figura 133 muestra la salida del comando ping ejecutado desde el Símbolo del sistema hacia la dirección 192.168.40.2, correspondiente al gateway del Módulo D dentro de la red implementada.

Figura 133. *Resultado del comando ping 192.168.40.2 ejecutable.*



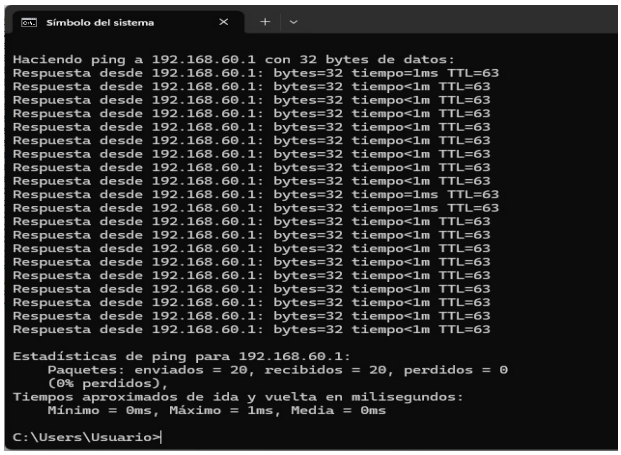
Nota. La captura evidencia una serie continua de respuestas exitosas, cada una con un tamaño de paquete de 32 bytes, tiempo de respuesta menor a 1 milisegundo y un valor de TTL (Time To Live) de 63, lo que indica que los paquetes atravesaron un número reducido de saltos antes de llegar a su destino.

4.2.5. Estudio de tráfico del Módulo E.

Para verificar la conectividad del Módulo E con su router administrador se ejecutó una prueba de ping en la figura 134 presenta la salida del comando ping ejecutado hacia la

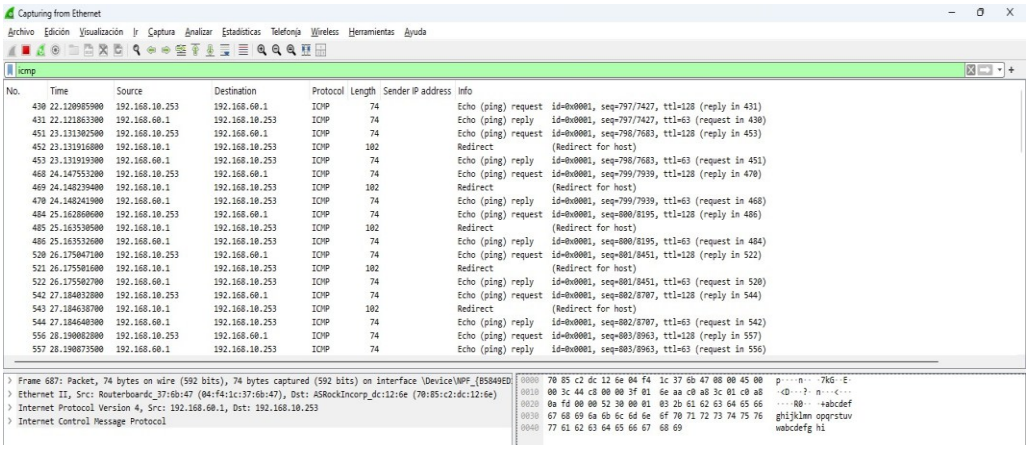
dirección 192.168.60.1, correspondiente al gateway del Módulo E dentro de la red implementada. Se enviaron paquetes de 32 bytes de datos, obteniendo respuesta exitosa en cada uno de ellos, con tiempos de respuesta de 0 a 1 milisegundo.

Figura 134. *Resultado del comando ping 192.168.60.1 ejecutable.*



Nota. Las estadísticas finales de la prueba muestran que se enviaron 20 paquetes, de los cuales se recibieron los 20 de vuelta, registrando un 0% de paquetes perdidos los tiempos de ida y vuelta obtenidos fueron de 0 ms mínimo, 1 ms máximo y 0 ms de media, evidenciando una latencia mínima y estable.

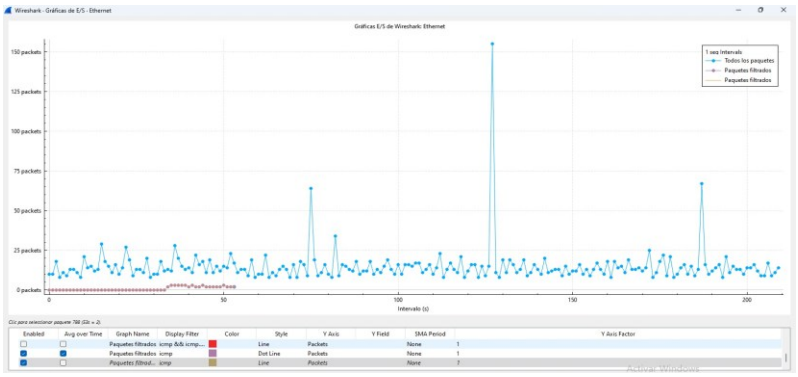
Figura 135. *Prueba de conectividad hacia el Módulo E*



Nota. La captura evidencia la presencia de mensajes *"ICMP Redirect"* enviados desde 192.168.10.1 hacia el equipo de pruebas indican que el gateway local está informando al host que existe una ruta más directa hacia la red de destino (192.168.60.0/24) a través de otro dispositivo de la red.

En la Figura 136, muestra la gráfica de entrada y salida correspondiente a una captura de aproximadamente 220 segundos de duración la serie "Todos los paquetes" (línea celeste) representa el tráfico total de la red, mientras que las series "Paquetes filtrados" (icmp, en tono rosado representan subconjuntos específicos del tráfico correspondientes al protocolo ICMP.

Figura 136. *Tráfico general de red mediante el diseño de gráfica.*



Nota. Estos picos podrían corresponder a eventos puntuales de mayor actividad en la red, como el inicio de pruebas de conectividad o procesos de sincronización, y ameritan una revisión adicional del contenido de los paquetes en esos intervalos para determinar su origen exacto.

4.3. Validación de políticas de seguridad perimetral.

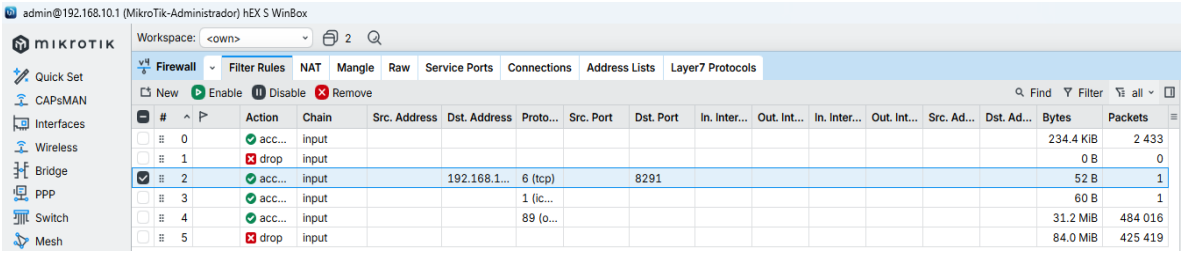
Como parte de la validación del tercer objetivo específico del proyecto, se procedió a evaluar la eficacia del sistema de seguridad perimetral basado en Firewall y Listas de Control de Acceso (ACLs).

El propósito de estas pruebas fue comprobar que la arquitectura implementada es capaz de identificar, registrar y bloquear el tráfico proveniente de dispositivos o segmentos no autorizados, garantizando así la protección y el aislamiento de la infraestructura crítica (cámaras de videovigilancia y equipos de administración).

4.3.1. Prueba de bloqueo de acceso no autorizado

En el Módulo E, el cual fue diseñado estratégicamente como un entorno aislado para la validación de políticas de seguridad, se simuló la generación de tráfico no autorizado. Mediante el envío de solicitudes desde un equipo ubicado en la subred del Módulo E (192.168.60.0/24) hacia la cámara IP del Módulo C (192.168.40.10).

Figura 137. *Punto de acceso no autorizado.*

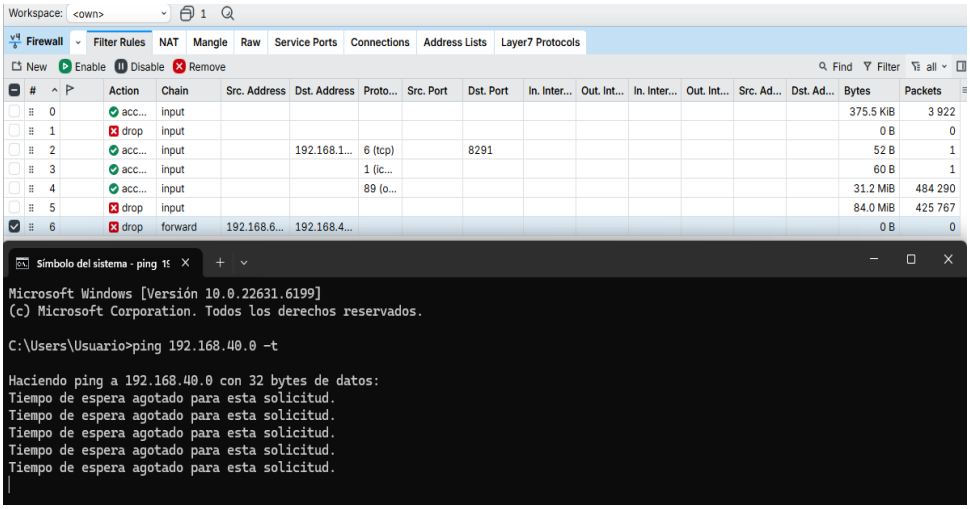


Nota. De acuerdo con el diseño topológico, el acceso a las redes de videovigilancia debe estar restringido estrictamente al segmento de administración.

Previo a la ejecución de la prueba, en el router administrador (Maestro), se verificó una regla de filtrado en la ruta en WinBox, estableciendo la acción de cadena *Forward* para todo el tráfico originado.

Como se observa en la Figura 138, los paquetes ICMP enviados hacia la dirección de la cámara (192.168.40.0) resultaron en un mensaje de "Tiempo de espera agotado para esta solicitud", registrando un 100% de pérdida de paquetes en el origen.

Figura 138. *Tabla de enrutamiento.*



Nota: Se observa el estado de perdida en la conexión de la cámara del módulo C.

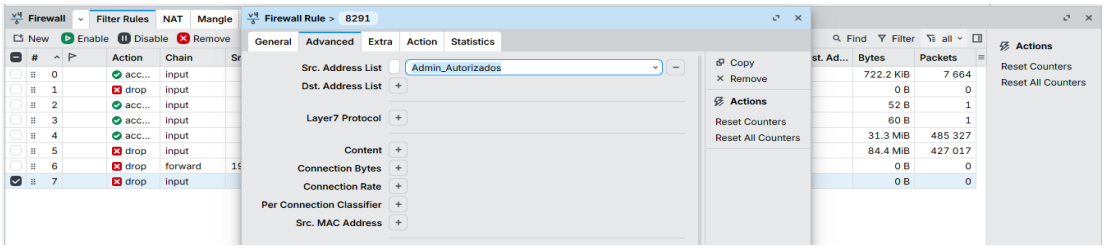
De forma complementaria, al observar la interfaz de WinBox en el router Maestro, se constató que los contadores de "*Bytes*" y "*Packets*" de la regla restrictiva se incrementaron de manera simultánea a los intentos de conexión.

4.3.2. Comprobación de la lista de control de acceso.

La segunda fase de la validación se enfocó en comprobar las Listas de Control de Acceso (ACLs) aplicadas para resguardar el plano de gestión acceso administrativo de los propios enrutadores.

MikroTik, se creó una lista de direcciones lógicas mediante la herramienta "*Address Lists*" denominada *"Admin_Autorizados"* la cual contiene exclusivamente la dirección de red del administrador principal (192.168.10.0/24) se muestra en la Figura 139.

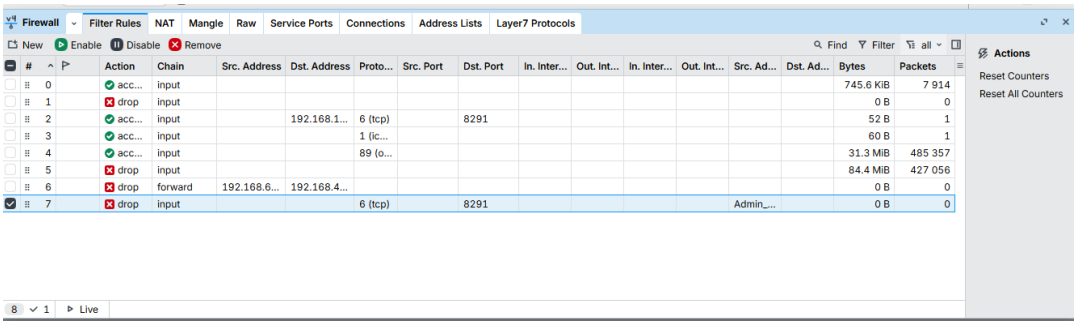
Figura 139. *Lista de administradores autorizados.*



Nota. Se muestra la regla *"Admin_Autorizados"* esta regla implementa control de acceso basado en listas, bloqueando el tráfico entrante que no provenga de una dirección IP incluida en dicha lista, como parte de la política de seguridad perimetral del router administrador.

La Figura 140, el contador de paquetes de la regla 7 permanece en cero. Este resultado no demuestra que un dispositivo no autorizado haya sido bloqueado; indica que la regla no ha recibido tráfico coincidente durante el período observado o que dicho tráfico fue procesado por una regla anterior.

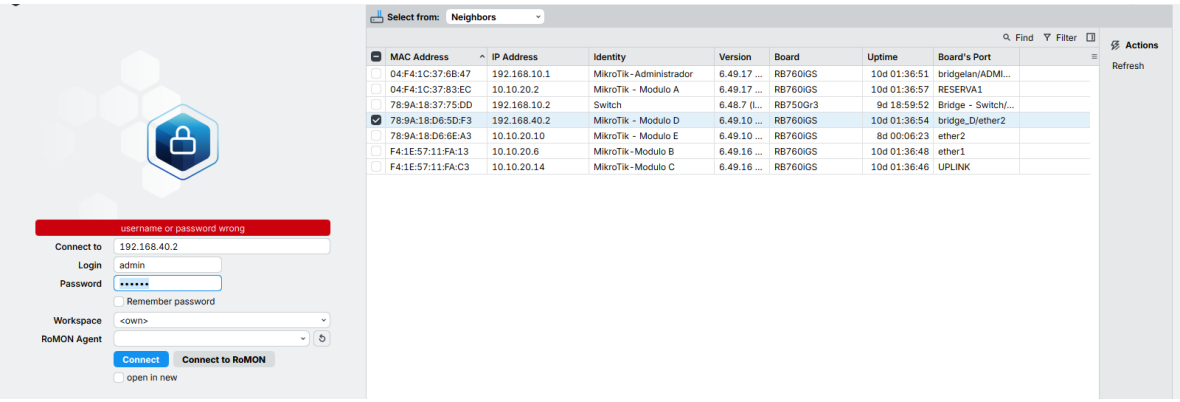
Figura 140. *Regla restrictiva en el Firewall.*



Nota. Vista general de las reglas de firewall (Filter Rules) configuradas en el router administrador MikroTik. Se listan 8 reglas con contador en 0 B / 0 paquetes, lo que indica que aún no se ha registrado tráfico que active dicha regla.

Al intentar establecer una sesión mediante WinBox hacia el router Maestro desde una dirección IP perteneciente al Módulo D red no incluida en la ACL, la solicitud de conexión fue rechazada inmediatamente por el dispositivo así se muestra en la Figura 141.

***Figura 141**. Acceso no autorizado de seguridad.*



Nota. Acceso no autorizado en la computadora secundaria, con esto comprobamos que la prueba de seguridad actuó correctamente.

Esta prueba demuestra que el perímetro lógico de los enrutadores se encuentra debidamente protegido contra intrusiones la aplicación.

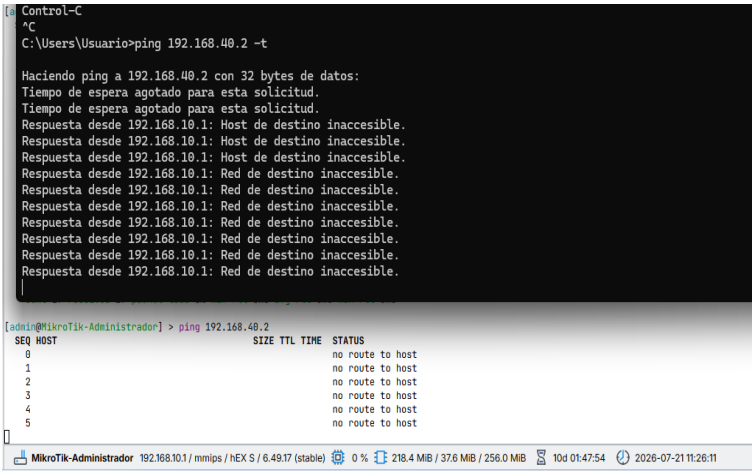
Este control sobre el tráfico fortalece la postura de ciberseguridad del Laboratorio de Telecomunicaciones, disminuyendo el riesgo de manipulaciones internas y cumpliendo a cabalidad con los estándares de protección de infraestructuras críticas abordados en la fundamentación teórica del proyecto.

4.3.3. Simulación de caída de enlace físico.

El escenario de prueba consistió en simular una caída crítica apagando intencionalmente la interfaz de conexión de uno de los módulos remotos para este procedimiento, se seleccionó el enlace de interconexión que comunica al Router Maestro con el Módulo D.

El cual fue diseñado específicamente dentro de la arquitectura como un nodo de expansión y redundancia se procedió a deshabilitar de forma manual la interfaz correspondiente a dicho enlace, simulando así un corte o una falla eléctrica en el dispositivo de extremo la prueba se puede observar en la Figura 142.

Figura 142. *Ejecución de la validación y obtención de evidencia.*

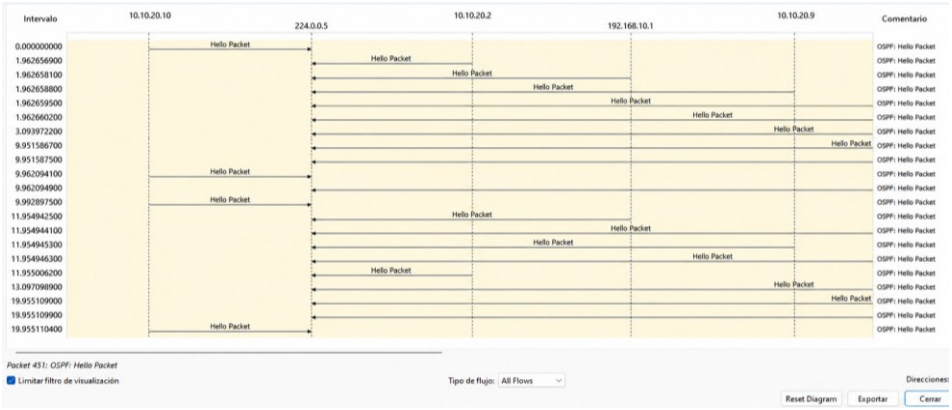


Nota. Al momento de la desconexión, se mantuvo una ventana de terminal abierta ejecutando un ping continuo hacia la dirección IP de la red LAN del Módulo D (192.168.40.2), con el fin de observar el comportamiento de los paquetes en tiempo real.

4.3.4. Recálculo automático en el algoritmo Dijkstra y convergencia OSPF.

Al producirse la interrupción del enlace, el protocolo OSPF detectó de forma inmediata la ausencia de los paquetes *"Hello Packets"* provenientes del Módulo D, al expirar el temporizador de inactividad el Router Maestro invalidó automáticamente la adyacencia y actualizó su Base de Datos de Estado de Enlace (LSDB).

Figura 143. *Lista de control de acceso.*

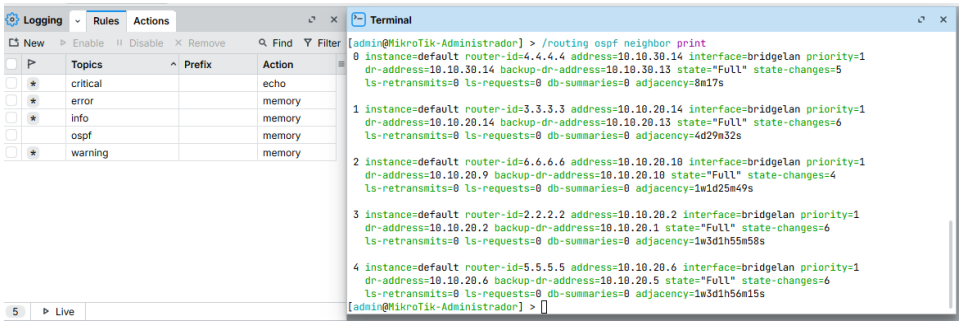


Nota. Los envíos se repiten aproximadamente cada 10 segundos, consistente con el intervalo Hello por defecto del protocolo OSPF, evidenciando el mantenimiento activo de las adyacencias entre el router principal y los módulos de la red.

Esta actualización desencadenó la ejecución del algoritmo *Shortest Path First* (Dijkstra), provocando que la red 192.168.40.0/24 fuera eliminada instantáneamente de la tabla de enrutamiento principal para evitar que el tráfico fuera enviado hacia un camino inexistente.

En la Figura 144, se procedió a rehabilitar la interfaz en WinBox, restaurando la conectividad física en cuestión de milisegundos, OSPF retomó el proceso de descubrimiento, al verificar el estado mediante el comando */routing ospf neighbor print,* se constató cómo la adyacencia pasó rápidamente por los estados hasta alcanzar nuevamente el estado *Full.*

Figura 144*. Línea de desconexión y conexión del tráfico.*



Nota. El estado *"Full"* en las cinco entradas indica que la sincronización de bases de datos de enlace-estado (LSDB) se completó correctamente con todos los vecinos, validando el correcto funcionamiento del protocolo de enrutamiento dinámico en la totalidad de la topología implementada.

4.4. Análisis de latencias por módulos.

Al evaluar el rendimiento de la infraestructura de red implementada, uno de los factores más críticos es la latencia, el tiempo que tardan los paquetes de datos en viajar desde el origen hasta el destino.

Con el fin de comprobar la eficiencia del enrutamiento dinámico mediante OSPF, se realizaron múltiples pruebas de conectividad y análisis de tráfico en cada uno de los módulos, desde el A hasta el E.

4.4.1. Módulo A.

El Módulo A presentó una latencia prácticamente nula durante toda la prueba, con los 20 paquetes enviados regresando sin ninguna pérdida cabe aclarar que este resultado corresponde a la dirección real de este módulo, ya que en una primera prueba se había tomado por error la red administrativa del router principal.

La Tabla 27, se muestra los análisis y presentan los resultados obtenidos en la prueba de conectividad y latencia correspondiente al Módulo A.

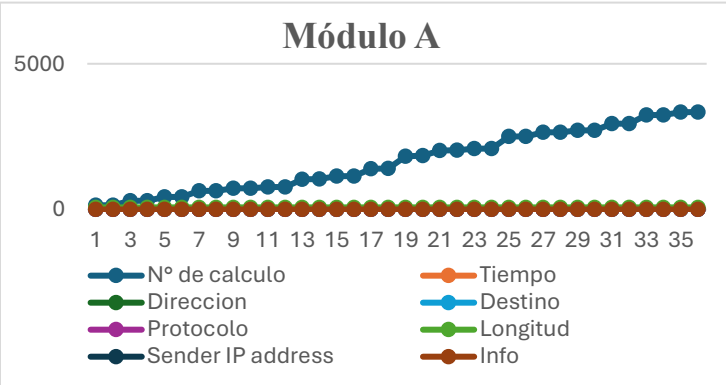
Tabla 27. *Análisis del Módulo A (Videovigilancia Zona 1).*

Parámetros	Valores obtenidos
Paquetes enviados/ recibidos	20/20 paquetes
Pérdida de paquetes	0%
RTT mínimo	0 ms
RTT máximo	1 ms
RTT promedio	0 ms
Observaciones	Prueba realizada hacia la red real del Módulo A (192.168.30.0/24), tras corregir la dirección inicialmente documentada.

Nota. Más bien, el tiempo de respuesta fue tan rápido que quedó por debajo de la resolución que la herramienta puede medir, lo que me indica un enlace sumamente eficiente y sin congestión.

En la Figura 145, se analiza la captura de tráfico entre *192.168.10.253* y *192.168.10.1*, dentro de la misma red local, los análisis contienen 18 ciclos completos de solicitud en respuesta en 36 paquetes en total.

Figura 145. *Análisis del módulo A, valores de los bits.*



4.4.2. Módulo B.

El Módulo B fue el único caso donde se obtuvo el desglose exacto de la latencia directamente, con un promedio de 0.649 ms, un valor considerado muy bajo dentro de una red local la coincidencia entre lo reportado por el símbolo del sistema y lo capturado en la confiabilidad de la medición.

Un detalle que vale la pena resaltar es la presencia de mensajes ICMP esto no indica una falla, sino que el gateway del equipo de pruebas está informando que existe una ruta más directa hacia la red de destino, un comportamiento normal cuando el host de pruebas no está ubicado directamente en el segmento del módulo evaluado.

La Tabla 28, se muestra los análisis y resultados obtenidos en la prueba de conectividad y latencia correspondiente al Módulo B.

Tabla 28. *Análisis del Módulo B (Videovigilancia Zona 2).*

Parámetros	Valores obtenidos
Paquetes enviados / recibidos	20 / 20 - 115 / 115 (prueba extendida)
Pérdida de paquetes	0 %
RTT mínimo	0.430 ms
RTT máximo	0.579 ms
RTT promedio	0.649 ms
Observación	Se detectaron mensajes ICMP Redirect enviados por el gateway local (192.168.10.1).

Nota. La transmisión fue perfecta, logrando un 0% de pérdida de datos, aunque al monitorear de tráfico en ciertos momentos (superando los 50 paquetes por segundo), la latencia se mantuvo estable y no afectó el rendimiento del enlace ni la transmisión de la cámara IP.

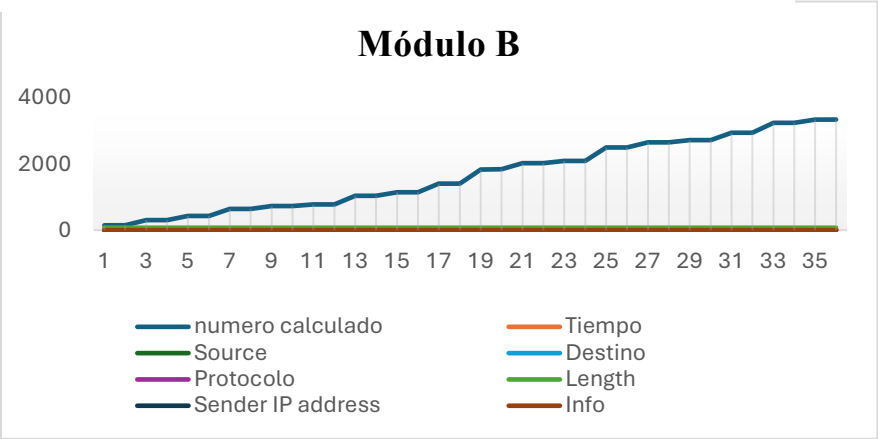
Tabla 29. *Suma de Tiempo por destino*

Destino	Suma de Tiempo (s)	Paquetes	RTT prom.
192.168.10.1	165.2745617	18	0.500 ms
192.168.10.253	165.2835638	18	0.500 ms

Nota. La tabla resume el destino de marcas en tiempo, los 18 paquetes capturados y la cantidad de paquetes correspondiente a cada uno.

El identificador avanza de a 1 en 1 entre un paquete del ping el siguiente avanza según cuántos otros paquetes de la red pasaron en el medio cuando hay más actividad de otros equipos en la red, el salto es más grande como se nota en la Figura 146, entre los puntos donde la curva pega un salto más marcado.

Figura 146. *Explicación del gráfico Módulo B.*



Nota. Este gráfico es el mismo tipo de curva que vimos para el Módulo A, pero acá corresponde a los datos del archivo del Módulo B los 36 paquetes de la captura ICMP.

- **Secciones identificadas.**

La sesión del módulo A concentra el 87% del tráfico MAC-Telnet, lo que sugiere administración activa de ese equipo, mientras la Sesión módulo B tiene actividad más liviana en segundo plano.

Tabla 30. *Paquetes comparativos del módulo A y módulo B*

Sesión	Servidor (MAC)	Paquetes	Bytes	Throughput
Sesión A	f4:1e:57:11:fa:c3	673	288,820	~10.5 KB/s
Sesión B	04:f4:1c:37:6b:47 (Routerboard)	158	33,200	~1.2 KB/s

Nota. La tabla presenta el tráfico de red registrado durante las sesiones de prueba, incluyendo la dirección MAC del servidor, la cantidad de paquetes transmitidos, los bytes transferidos y el throughput aproximado. Los valores corresponden a las mediciones obtenidas durante la prueba de conectividad de la red.

4.4.3. Módulo C.

El Módulo C alcanzó también una latencia mínima, entre 0 y 1 ms una vez resuelto el problema de adyacencia OSPF que inicialmente impedía la comunicación con este segmento esto no afecta el resultado de la prueba simplemente refleja pequeñas diferencias en el número de saltos que atravesó cada paquete de respuesta.

La Tabla 31, se muestra los análisis y resultados obtenidos en la prueba de conectividad y latencia correspondiente al Módulo C.

Tabla 31. *Análisis del Módulo C (Vigilancia con OSPF y DHCP).*

Parámetros	**Valores obtenidos**
Paquetes enviados / recibidos	20 / 20
Pérdida de paquetes	0 %
RTT mínimo	0 ms
RTT máximo	1 ms
RTT promedio	63 – 64 ms
Observación	Se detectaron mensajes ICMP Redirect enviados por el gateway local (192.168.10.1)

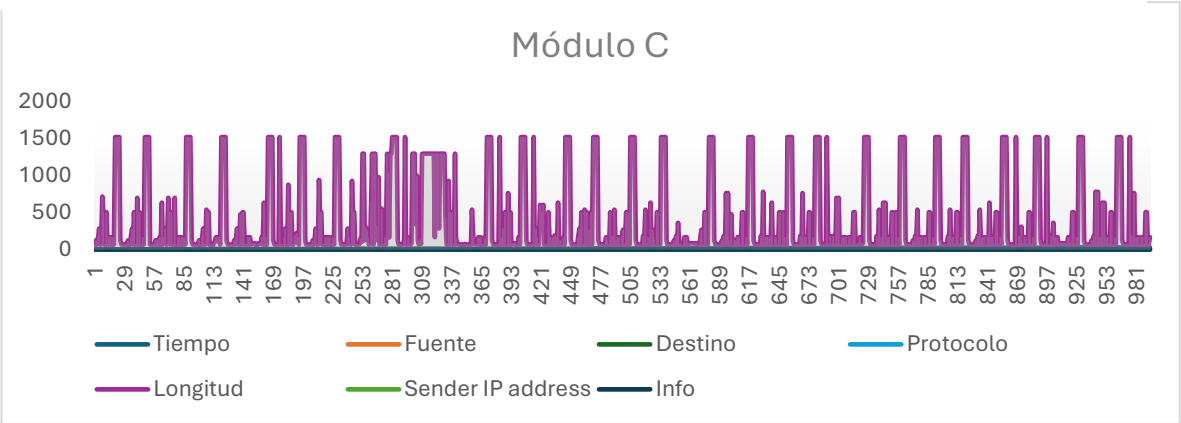
Nota: Esto me confirma que tenemos una conexión activa, muy estable y con una latencia sumamente baja, lo cual es ideal para soportar el tráfico de video en tiempo real de nuestra cámara de seguridad.

Este gráfico muestra la columna Longitud (bytes) de cada uno de los 994 paquetes capturados en el Módulo C, ordenados según su número de captura

A diferencia de los Módulos A y B donde todos los paquetes ICMP median exactamente 74 bytes, acá se ve un patrón mucho más irregular, con picos que llegan hasta ~1,514 bytes intercalados con una base que ronda los 64-164 bytes.

Esto es consecuencia directa de que el Módulo C no es tráfico de ping, sino una sesión de administración remota vía MAC-Telnet.

Figura 147. *Distribución del tamaño de paquete.*



Nota. El gráfico representa la longitud (en bytes) de cada paquete individual de la captura del Módulo C, en el orden en que fue registrado. Los valores oscilan entre 42 y 1,514 bytes, reflejando la alternancia entre paquetes de confirmación

4.4.4. Módulo D.

El Módulo D mostró un comportamiento consistente con el resto de los segmentos todos los paquetes fueron respondidos por debajo de 1 ms y sin pérdidas el valor estable de indica que la ruta de este módulo no presenta cambios ni saltos adicionales entre una prueba y otra, lo cual es un indicio de que la tabla de enrutamiento OSPF se mantiene sin oscilaciones para este destino.

La Tabla 32, se muestra los análisis y resultados obtenidos en la prueba de conectividad y latencia correspondiente al Módulo D.

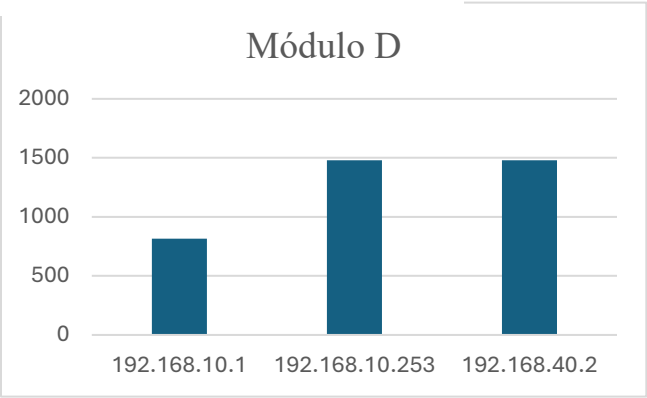
Tabla 32. *Análisis del Módulo D (Expansión y Redundancia).*

Parámetros	**Valores obtenidos**
Paquetes enviados / recibidos	20 / 20
Pérdida de paquetes	0 %
RTT mínimo	0.459 ms
RTT máximo	1.234 ms
RTT promedio	0.768 ms
Observación	Prueba dirigida a la interfaz corregida del módulo (192.168.40.2)

Nota. La respuesta fue continua y totalmente exitosa, registrando tiempos de respuesta menores a 1 milisegundo en cada paquete.

En la Figura 148, agrupa la columna Longitud (bytes) de los 48 paquetes de la captura del Módulo D se suma esos valores por cada IP:

Figura 148. *Suma de Longitud del módulo D.*



Nota. Solicitudes y respuestas de ping, respectivamente), mientras que 192.168.10.1 acumula 816 bytes correspondientes a 8 mensajes ICMP de 102 bytes, emitidos por el router al indicar una ruta más directa hacia la red 192.168.40.0/24.

4.4.5. Módulo E.

El Módulo E cerró el conjunto de pruebas con el mismo patrón de baja latencia observado en los demás módulos mínimo de 0 ms, máximo de 1 ms y promedio de 0 ms al igual que en el Módulo B, aparecieron mensajes ICMP Redirect, lo que confirma que este comportamiento no es un caso aislado, sino una consecuencia normal de la posición del equipo de pruebas dentro de la topología, y no un síntoma de error en el módulo evaluado.

La Tabla 33, se muestra el análisis y resultados obtenidos en la prueba de conectividad y latencia correspondiente al Módulo E.

Tabla 33. *Resultados de la prueba de conectividad (ping) hacia el Módulo E.*

Parámetros	Valores obtenidos
Paquetes enviados / recibidos	20 / 20
Pérdida de paquetes	0 %
RTT mínimo	0 ms
RTT máximo	1 ms
RTT promedio	0 ms

Observación	Se registraron mensajes ICMP Redirect desde 192.168.10.1, igual que en el Módulo E

Nota. Esta latencia mínima y estable me demuestra que las pesadas reglas de firewall y listas de control de acceso (ACLs) que configuré no están generando ningún tipo de cuello de botella o lentitud en el procesamiento de la red

4.5. Verificación de las cámaras de los módulos.

Como parte de la validación integral de la red implementada, se realizó la verificación funcional de las cámaras IP tipo PTZ instaladas en los módulos del Laboratorio de Telecomunicaciones, con el objetivo de comprobar su correcta integración a la red, la disponibilidad del flujo de video en tiempo real y la operatividad de las funciones de control remoto.

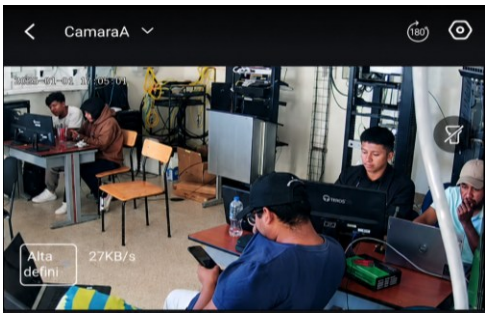
4.5.1. Cámara IP del Módulo A.

Se accedió remotamente a la cámara IP CamaraA, correspondiente al Módulo A, mediante la aplicación de videovigilancia instalada en un dispositivo móvil conectado a la red.

Se verificaron el establecimiento de la conexión, la visualización de video en vivo y la disponibilidad de los controles de panorámica, inclinación y zoom (PTZ).

Como se observa en la Figura 149, la cámara transmite video en tiempo real con una tasa de transferencia de 27 KB/s. La reproducción estable del flujo y la disponibilidad de los controles PTZ confirman la correcta comunicación entre el dispositivo móvil y la cámara dentro de la red del Módulo A.

Figura 149. *Análisis de la Cámara A.*



Nota. Captura de la cámara de la interfaz de video de “Cámara A” del Módulo A, transmitiendo en alta definición con una tasa de transferencia de 27 KB/s.

El encabezado de la interfaz confirma que la conexión está activa, mientras que los controles de desplazamiento y reinicio de posición a 180° evidencian que las funciones de movimiento remoto de la cámara se encuentran operativas.

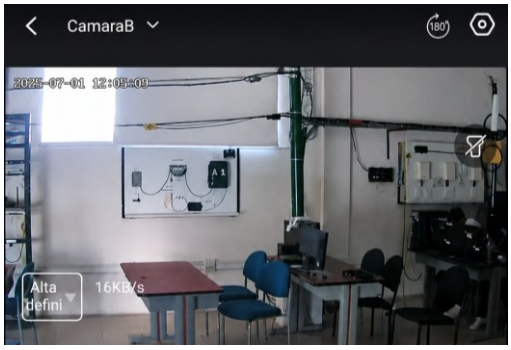
4.5.2. Cámara IP del Módulo B.

De manera análoga, se verificó el funcionamiento de la cámara IP Cámara B, correspondiente al Módulo B, mediante dos capturas realizadas en momentos distintos. La prueba permitió comprobar la estabilidad del flujo de video y el correcto reposicionamiento de la cámara dentro del área monitoreada.

En la primera captura, mostrada en la Figura 154, la cámara registró una tasa de transferencia de 16 KB/s en condiciones de baja luminosidad, permitiendo visualizar el área de trabajo y el tablero de conexiones del módulo.

En la Figura 150, la cámara registró una tasa de transferencia de 17 KB/s y mostró el ambiente desde otro ángulo. La transmisión continua y el reposicionamiento exitoso confirman el funcionamiento estable del video en vivo y de los controles PTZ.

Figura 150. *Análisis de la Cámara B.*



Nota. Captura de la interfaz de video de la cámara IP “Cámara B” del Módulo B, con una tasa de transferencia de 17 KB/s.

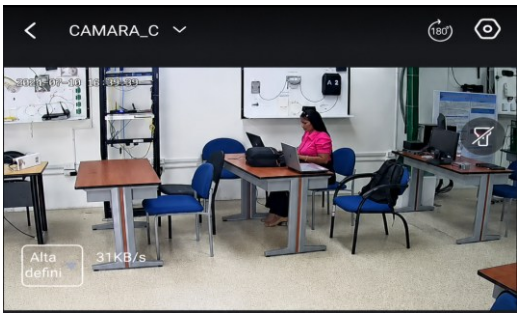
4.5.3. Verificación de la cámara IP del Módulo C.

La cámara IP Cámara C, correspondiente al Módulo C, se encuentra correctamente integrada a la red del laboratorio. Se verificó la transmisión estable de video en vivo y la disponibilidad de los controles remotos de desplazamiento.

La Figura 151, muestra que la Cámara C transmite video en vivo con la conexión activa y los controles PTZ disponibles. Durante la prueba se registró una tasa de transferencia de 31 KB/s, la mayor entre las cámaras evaluadas. Junto con los resultados de los módulos A y B, se confirma el funcionamiento estable del sistema de videovigilancia en los tres módulos verificados.

La interfaz muestra que la conexión permanece activa y que los controles PTZ están disponibles. En conjunto con las pruebas realizadas en los módulos A y B, estos resultados confirman el funcionamiento uniforme del sistema de videovigilancia en los tres módulos verificados.

Figura 151. Análisis de la cámara C.



Nota. Captura de la interfaz de video de la cámara IP “Cámara C” del Módulo C, con una tasa de transferencia de 31 KB/s.

Se espera que la cámara del módulo C transmita video en tiempo real de forma estable, con una tasa de transferencia adecuada al ancho de banda del segmento correspondiente y con el panel de control PTZ disponible, de forma consistente con el comportamiento observado en los módulos A y B.

CONCLUSIONES

- La integración de OSPF, DHCP y reglas de seguridad perimetral permitió resolver de manera conjunta las necesidades de enrutamiento dinámico, asignación automática de direcciones IP y control de acceso en el laboratorio. Las pruebas de conectividad, rutas OSPF y adyacencias en estado Full confirmaron la comunicación entre los cinco módulos sin pérdida de paquetes.
- La implementación de OSPF permitió el intercambio dinámico de información de enrutamiento entre los módulos, facilitando el cálculo automático de rutas y reduciendo la necesidad de configuraciones manuales ante cambios en la topología.
- La validación previa de la topología en GNS3 permitió identificar y corregir posibles inconsistencias antes del despliegue físico. La metodología aplicada diseño, simulación, implementación y validación demostró ser adecuada y replicable para proyectos académicos de infraestructura de red.
- La arquitectura implementada cumple una función técnica y formativa. Además de proporcionar una red organizada, escalable y con controles básicos de seguridad, el Módulo E permite realizar prácticas de firewall y listas de control de acceso en un entorno aislado, sin comprometer la operación de los demás módulos.

RECOMENDACIONES

- Incorporar mecanismos de seguridad complementarios, como IDS/IPS, firewall de próxima generación (NGFW), filtrado web y segmentación adicional mediante VLAN, para fortalecer la protección frente a amenazas más avanzadas.
- Establecer un plan de monitoreo y mantenimiento periódico que incluya la revisión de adyacencias OSPF, tablas de rutas, registros del firewall, uso de ancho de banda, disponibilidad de enlaces y estado de los servicios DHCP y DNS.
- Implementar copias de seguridad automáticas de las configuraciones de los routers MikroTik y documentar un procedimiento de recuperación ante fallos, con el fin de reducir el tiempo de restauración del servicio ante errores de configuración o fallas de hardware.
- Utilizar la topología como recurso didáctico mediante guías de laboratorio para los módulos A–E. Estas prácticas pueden incluir configuración y validación de OSPF,

DHCP, ARP, DNS, reglas de firewall, monitoreo de tráfico y pruebas controladas de seguridad en el Módulo E.

ANEXO.

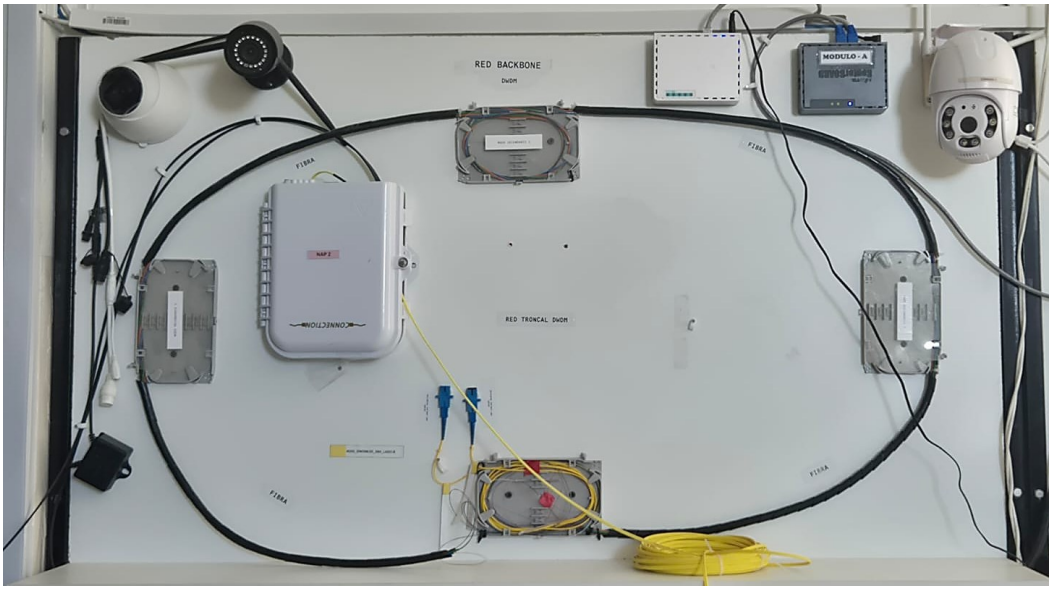
Anexo 1.Clasificación de los equipos Mikrotik.

Anexo 2. Tendido de cable ethernet CAT6 para el laboratorio de Telecomunicaciones.

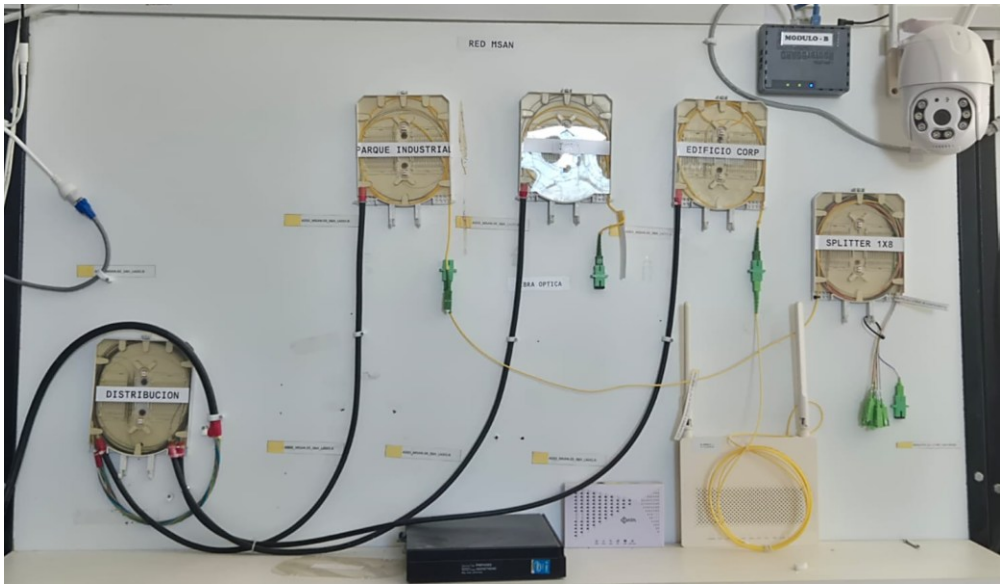
Anexo 3. Mikrotik Administrador junto con el Switch expansión de puertos para los módulos.

Anexo 4. Instalación de los módulos, para la arquitectura de la red.

Anexo 5. Colocación de las cámaras de los módulos A, B y C.

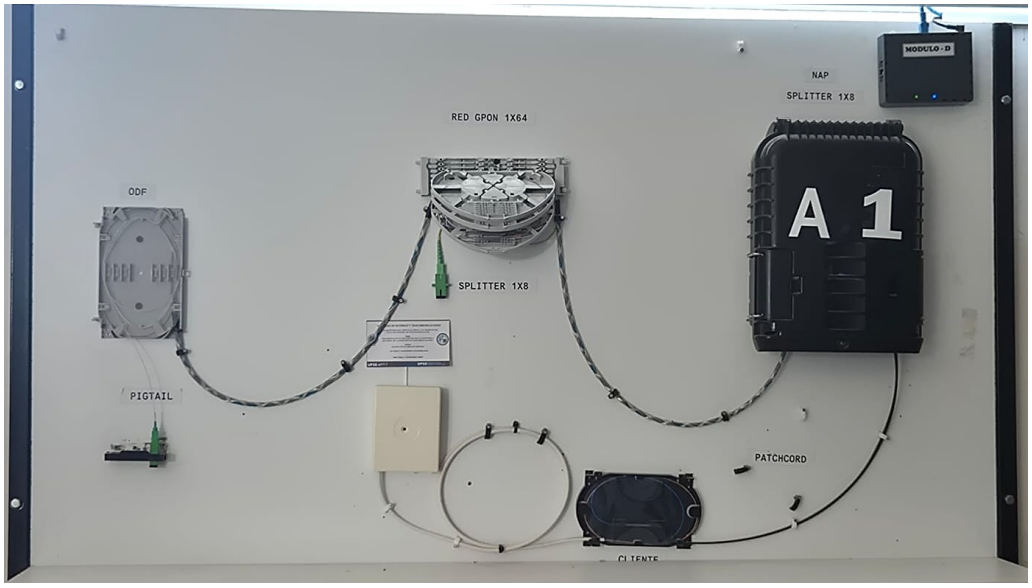


Anexo 6. Escenario del Módulo A junto con su cámara de monitoreo.

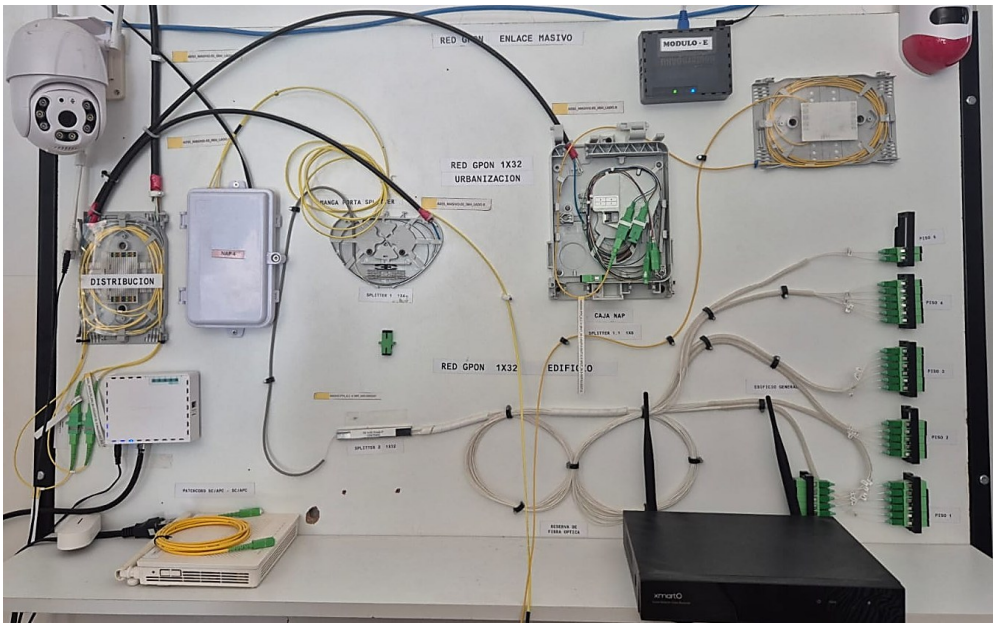


Anexo 7. Escenario del Módulo B junto con su cámara de monitoreo.

Anexo 8. Escenario del Módulo C junto con su cámara de monitoreo.



Anexo 9. Escenario del Módulo D.



Anexo 10. Escenario del Módulo E.

BIBLIOGRAFÍA

[1] J. L. P. Guerrero, «Seguridad en redes LAN: la protección de datos hasta la prevención de intrusiones,» *Journal TechInnovation,* vol. 3, nº 1, p. 14, 1 Junio 2024.

[2] R. Gutter, «Infraestructura crítica en Latinoamérica en riesgo por incremento de ciberataques,» *Seguridad & Defensa,* 23.

[3] F. R. Sala, «Caracterización de un Firewall Perimetral implementado mediante software libre OpenBSD y CentOS,» INSTITUTO DE INVESTIGACIONES EN MATEMÁTICAA APLICADAS EN SISTEMAS, Mexico, 2024.

[4] M. E. C. Chulca, «DISEÑO Y SIMULACIÓN DE UNA RED LOCAL CONECTADA A PROVEEDORES DE SERVICIOS DE INTERNET (ISP) CON POLÍTICAS DE SEGURIDAD Y AUTOMATIZACIÓN DE SUS CONFIGURACIONES,» Quito, 2023.

[5] A. Walton, «Protocolo OSPF: ¿Qué es, Para qué Sirve y Cómo Funciona?,» 23 Octubre 2024. [En línea]. Available: https://ccnadesdecero.es/ospf-open-shortest-path-first/.

[6] John Marín , Alejandro Valencia, Juan Bedoya, «Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS,» *Revista Universidad Católica de Oriente,* vol. 31, nº 45, pp. 33-49, 24 09 2020.

[7] J. M. C. Pardo, «Normatividad para la protección cibernética de la infraestructura crítica en Colombia,» *Ciberespacios, tecnologia e innovación,* vol. 3, nº 5, 30 Junio 2024.

[8] Johan Intriago, Jonathan Quimis, Cristopher Choez, Mario Marcillo, «Protocolos de seguridad informática aplicados en los aboratorios de la carrera tecnologías de la información,» *Journal TechInnovation,* vol. 2, nº 1, pp. 79-84, 1 Junio 2023.

[9] Laura Asenjo, Cristhian Jesus, Macedo Salvatierra, Robert, «Diseño de enlaces WAN para la mejora del QOS de la red de telecomunicaciones en medianas y grandes empresas mediante la interconexión de sedes por tecnología VPLS,» Perú -Lima, 25.

[10] Lindao Fernando, Bravo Pardo, «PROPUESTA DE SEGURIDAD EN EL FIREWALL PERIMETRAL DE LA UNIVERSIDAD NACIONAL DE LOJA",» 2017.

[11] S. Lissette, «ANÁLISIS DE VULNERABILIDADES EN LA RED LAN USANDO HERRAMIENTAS DE HACKING ÉTICO PARA UNA EMPRESA DE LA PROVINCIA DE SANTA ELENA,» La libertad, 2021.

[12] Fortinet, «¿Que es la seguridad en red?,» [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/what-is-network-security.

[13] J. Santana, «MikroTik – OSPF,» 27 Noviembre 2024. [En línea]. Available: https://dsantana.uas.edu.mx/index.php/2024/11/27/mikrotik-ospf/.

[14] D. P. Palate Byron, «Mitigación de vulnerabilidades en la red central de un ISP: Un caso de estudio,» *Ecuadorian Science Journal,* vol. 5, nº 2, 2021.

[15] M. B, «OSPF,» 1 Octubre 2025. [En línea]. Available: https://help.mikrotik.com/docs/spaces/ROS/pages/9863229/OSPF.

[16] L. Bermeo, «La transformación digital como estrategia de gestión educativa en la educación superior: desafíos y oportunidades en América Latina,» *Sinergia Académica,* vol. 8, nº 10, pp. 78-103, 27 Diciembre 2025.

[17] CloudeFlade, «CloudeFlade,» [En línea]. Available: https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/?utm_source=.

[18] Daniel Zapata, Ignacio Gómez, Jhon Acevero, Crithian Obando, David Garcia, «Implementación de un sistema de control y seguridad Informático ENDIAN FIREWALL,» vol. 10, nº 1.

[19] Sanchez Silva, Diego Sebestian; Colcha Guashpa, Luis A, «Diseño e implementación de una red FTTH utilizando el estándar G.984.X configurando Queue-Tree y ACL en el mikrotik RB4011IGS+RM para el ISP Mundotronic en Tollolloma.,» Escuela Superior Policténica De Chimborazo, Riobamba, 2022.

[20] I. O. f. Standardization, 2022. [En línea]. Available: https://www.iso.org/standard/27001?utm_source=.

[21] Lubis, Muharman; Safitra, Muhammad Fakhrul; Fakhrurroja, Hanif; Muttaqin, Alif Noorachmad, «Sensors,» vol. 25, nº 15, 2025.

[22] C. Uc, «Protocolo OSPF,» *Blazar,* 14 Febrero 2024.

[23] T. Tim, «Cisco,» 4 7 2023. [En línea]. Available: https://community.cisco.com/t5/blogs-general/protocolos-de-red-b%C3%A1sicos-en-la-comprensi%C3%B3n-del-modelo-osi/ba-p/4810310.

[24] C. Point, «¿Qué es el modelo OSI? Comprensión de las 7 capas,» [En línea]. Available: https://www.checkpoint.com/es/cyber-hub/network-security/what-is-the-osi-model-understanding-the-7-layers/.

[25] Yana, «LAN vs. MAN vs. WAN: Comprensión de las diferencias en los tipos de red,» 29 7 2024. [En línea]. Available: https://www.qsfptek.com/es/qt-news/lan-vs-man-vs-wan-understanding-the-differences-in-network-types.html?srsltid=AfmBOoo0dfo2ArzfM2dgxTWc4hEx_ZJMVdctGAAhbbskNR_7wnr4aYCI.

[26] Tokio, «Introducción al protocolo OSPF,» *Tokio School,* 18 Febrero 2025.

[27] N. Chevalier, «Eficiencia en Enrutamiento OSPF,» 17 Septiembre 2025. [En línea]. Available: https://www.studocu.com/latam/document/instituto-tecnologico-de-las-americas/sistema-operativo/asignatura-conmutacion-y-enrutamiento-eficiencia-en-enrutamiento-ospf/143044859?sid=29e08846-296b-4a64-acaf-980bf7d499a71783668224.

[28] K. Shahid, S. N. Ahmad y S. T. H. Rizvi, «Network Performance Optimization: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load Sharing and Link Failover Systems,» *Future Internet,* vol. 16, nº 9, p. 339, 20 septiembre 2024.

[29] Sebastian, « Ensayo sobre Tipos de Redes en Sistemas Computacionales,» *Universidad Autonoma De La Lagura,* 24 Septiembre 2024.

[30] I. Gonzalez, «Guía de enrutamiento dinámico OSPF,» *Bienvenido al Centro de Ayuda de Tecnosinergia,* 2023.

[31] M. Suarez, «Vector Distancia y Estado de Enlace,» 10 Agosto 2020. [En línea]. Available: https://ccnadesdecero.com/curso/vector-distancia-estado-enlace/.

[32] «Enrutadores designados,» 2018. [En línea]. Available: https://docs.ruckuswireless.com/fastiron/08.0.60/fastiron-08060-l3guide/GUID-E26414B7-244B-4FCD-BBD2-8D555478C34A.html.

[33] J. Networks, «Guía del usuario de OSPF,» 23 Septiembre 2025. [En línea]. Available: https://www.juniper.net/documentation/us/en/software/junos/ospf/topics/topic-map/configuring-ospf-areas.html#id-ospf-designated-router-overview.

[34] Nicolas J. Tito M. Cypriam m., «Evaluación del rendimiento del enrutamiento mediante OSPF y una arquitectura de red basada en múltiples controladores.,» *Revista Internacional de Redes Informáticas y Seguridad de la Información (IJCNIS),* vol. 13, nº 4.

[35] I. T. Universitario, «Curso taller de MikroTik Routing,» 24 Julio 2016. [En línea]. Available: https://itu.uncuyo.edu.ar/cursos/curso/curso-taller-de-mikrotik-routing.

[36] E. d. Codecademy, «Algoritmo de Dijkstra para encontrar la ruta más corta,» *Equipo de Codecademy,* 2026.

[37] Studysmaster, «modelo TCP/IP,» 19 Septiembre 2024. [En línea]. Available: https://www.studysmarter.es/resumenes/ingenieria/ingenieria-de-telecomunicaciones-ingenieria/modelo-tcpip/.

[38] I. Espinoza, «OSPF: Optimizando el enrutamiento en redes mediante Single Area y Multi Area,» 2 Julio 2026. [En línea]. Available: https://abcxperts.com/ospf-optimizando-el-enrutamiento-en-redes-mediante-single-area-y-multi-area-2/?srsltid=AfmBOopfFCg5MMKnTJsq0oZYfZkuzIBeV0hIBE4q9R0MJyIfplp3r5G5.

[39] Zenarmor, «Tipos de protocolos de enrutamiento,» 15 Agosto 2022.

[40] M. S, «Routers,» 3 junio 2026. [En línea]. Available: https://help.mikrotik.com/docs/.

[41] M. R. Docs, «Configuración básica del servidor DHCP,» 27 Enero 2026. [En línea]. Available: https://mikrotikdocs.fyi/ip/dhcp-server-basic/.

[42] R. Droms, «Dynamic Host Configuration Protocol,» Internet Engineering Task Force, 1997.

[43] G. Albert, «Funcionamiento del protocolo,» 15 junio 2025. [En línea]. Available: https://asir.readthedocs.io/es/latest/TEMA_2_Dhcp/funcionamiento.html.

[44] ManageEngine, «Proceso de DHCP DORA,» 2026. [En línea]. Available: https://www.manageengine.com/products/oputils/tech-topics/dhcp-dora-process.html.

[45] «hEX S,» 2025. [En línea]. Available: https://mikrotik.com/product/hex_s_2025?utm_source=.

[46] Amazon, «MikroTik RB750Gr3 Gigabit Ethernet de 5 puertos,» 2025. [En línea]. Available: https://www.amazon.com/dp/B01MSUMVUB.

[47] «KiWii,» 2023. [En línea]. Available: https://www.kywi.com.ec/conector-rj45-cat6-blindado-10-unidades-lsc-156003/p?srsltid=AfmBOoraIQeYc2567Pvc_mjb9dvhgVUQJGDJ-FgWQh35IUjFktglqHNx#.

[48] «Mercado Libre,» 2026. [En línea]. Available: https://www.mercadolibre.com.ec/cable-de-red-par-trenzado-utppanduit-pfl6x04bu-ceg-305m-color-azul/p/MEC32451072.

[49] Trimble, «Sketchup,» 2026. [En línea]. Available: https://sketchup.trimble.com/en.

[50] GNS3, «GNS3,» 2026. [En línea]. Available: https://gns3.com/.

[51] Wimbox, «Wimbox,» 2026. [En línea]. Available: https://mikrotik.com/download/winbox.

[52] Wireshark, «The world's leading network protocol analyze,» 2026. [En línea]. Available: https://www.wireshark.org/.