
# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACSISTEL

INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

# Implementación de un laboratorio WISP para la aplicación de técnicas de balanceo de carga y optimización del ancho de banda

**Natanael Isaias Rios Huacon**

**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 Macas, Mgtr.
**DOCENTE ESPECIALISTA**

Ing. Luis Amaya Fariño, Mgtr.
**DOCENTE GUÍA UIC**

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 el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **Rios Huacon Natanael Isaias**, como requerimiento para la obtención del título de Ingeniero en telecomunicaciones.

La Libertad, a los 03 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, **Rios Huacon Natanael Isaias**

## DECLARO QUE:

El trabajo de Titulación, **Implementación de un laboratorio WISP para la aplicación de técnicas de balanceo de carga y optimización del ancho de banda,** 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 03 días del mes de agosto del año 2026

**EL AUTOR**

Natanael Rios

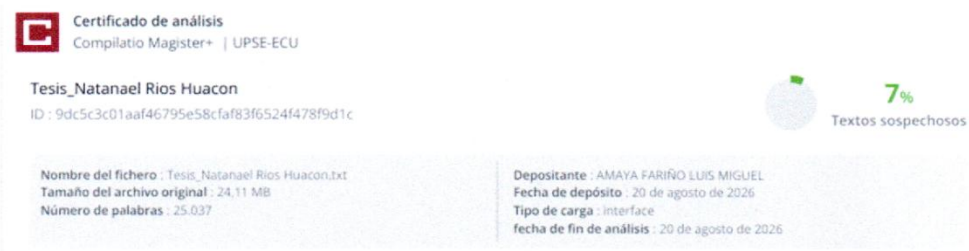
**Rios Huacon Natanael Isaias**

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 un laboratorio WISP para la aplicación de técnicas de balanceo de carga y optimización del ancho de banda**, presentado por el estudiante, **Rios Huacon Natanael Isaias** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 07%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Certificado de análisis
Compilatio Magister+ | UPSE-ECU

Tesis_Natanael Rios Huacon
ID : 9dc5c3c01aaf46795e58cfaf83f6524f478f9d1c

7%
Textos sospechosos

Nombre del fichero : Tesis_Natanael Rios Huacon.txt
Tamaño del archivo original : 24,11 MB
Número de palabras : 25.037

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.**

UPSE

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

## AUTORIZACIÓN

Yo, **Rios Huacon Natanael Isaias**

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

La Libertad, a los 03 días del mes de agosto del año 2026

**EL AUTOR**

Natanael Rios

**Rios Huacon Natanael Isaias**

# AGRADECIMIENTO

*Agradezco primeramente a Dios por darme salud y fortaleza para terminar esta importante etapa académica.*

*Agradezco a la Universidad y a sus docentes, quienes compartieron sus conocimientos y contribuyeron a mi formación profesional.*

*Agradezco profundamente a mi madre por su amor y apoyo incondicional durante todo este proceso; a mis hermanos, por motivarme a no rendirme y brindarme su constante respaldo; y a mi compañera de vida, quien, con su amor, paciencia y palabras de aliento, me ha impulsado a seguir siempre adelante en los momentos más difíciles. Gracias por caminar a mi lado y brindarme el apoyo necesario para terminar esta etapa de mi vida.*

*Finalmente, expreso mi gratitud a todas aquellas personas que estuvieron presentes a lo largo de este camino y aportaron significativamente a mi crecimiento personal y profesional.*

*Natanael Isaias Rios Huacon*

# DEDICATORIA

*Dedico este trabajo de titulación a mi familia por su amor incondicional, sus sacrificios, sus consejos y su apoyo constante durante todo mi proceso de formación académica.*

*A mis seres queridos, quienes, con su cariño, comprensión y palabras de aliento, fueron un pilar fundamental para culminar esta etapa de mi vida.*

*A mi compañera de vida, por compartir conmigo este camino, por estar presente en cada momento y por ser parte de los sueños y metas que deseo alcanzar. Este logro también es parte de nuestra historia.*

*Finalmente, dedico este trabajo a todas aquellas personas que creyeron en mí y que dejaron una huella significativa durante este camino.*

*Natanael Isaias Rios Huacon*

## ÍNDICE GENERAL

## ÍNDICE DE FIGURAS

## ÍNDICE DE TABLAS

## Resumen

El presente proyecto tiene como objetivo diseñar e implementar un laboratorio educativo que permita simular una red WISP, aplicando balanceo de carga, gestión del ancho de banda y segmentación del tráfico mediante VLAN.

La metodología combina enfoques de investigación descriptiva, documental y aplicada, lo que permite analizar las tecnologías involucradas. Se analizaron y compararon las técnicas de balanceo de carga Round Robin, Least Connections, PCC e IP Hashing con el propósito de determinar la alternativa más adecuada para el entorno propuesto. A partir de este análisis, se seleccionó e implementó PCC (Per Connection Classifier), complementado con mecanismos de QoS y VLAN dedicadas a cada tipo de servicio. La implementación se realizó utilizando un *router* MikroTik y un *switch* gestionable TP-Link, y se evaluó el funcionamiento de la red bajo escenarios de tráfico y priorización.

Los resultados evidenciaron una mejora en la eficiencia y estabilidad de la red, lo que permitió validar su funcionalidad para fines educativos. Finalmente, se desarrolló una guía técnica con prácticas y recomendaciones orientadas a estudiantes y docentes para facilitar la replicación del entorno y fortalecer el aprendizaje práctico.


**Palabras clave:** WISP, balanceo de carga, PCC, QoS, VLAN.

## Abstract

This project aims to design and implement an educational laboratory that simulates a WISP network by applying load balancing, bandwidth management, and VLAN-based segmentation.

The methodology combines descriptive, documentary, and applied research approaches, allowing for the analysis of the technologies involved. Round Robin, Least Connections, PCC, and IP Hashing load balancing techniques were analyzed and compared to determine the most suitable alternative for the proposed environment. Based on this analysis, PCC (Per Connection Classifier) was selected and implemented, complemented by QoS mechanisms and VLANs dedicated to each type of service. The implementation was carried out using a MikroTik router and a TP-Link managed switch, and network performance was evaluated under different traffic and prioritization scenarios.

The results showed improvements in network efficiency and stability, which validated the functionality of the proposed environment for educational purposes. Finally, a technical guide containing practical exercises and recommendations for students and instructors was developed to facilitate the replication of the environment and strengthen practical learning.


**Keywords:** WISP, load balancing, PCC, QoS, VLAN.

## Introducción

Hoy en día, el acceso a internet y la gestión eficiente de la red son vitales para ofrecer conectividad de calidad y alto rendimiento, particularmente en entornos corporativos, académicos y rurales. Las redes de proveedores de servicios de internet inalámbricos (WISP) se han consolidado como una solución viable para brindar servicios de internet en lugares donde otras tecnologías son costosas o inviables. Ante este escenario, se hace necesario implementar soluciones que aseguren la disponibilidad continua, la segmentación del tráfico y la administración óptima del ancho de banda.

Los equipos TP-Link y MikroTik son una opción rentable y versátil para implementar técnicas avanzadas de red, como el balanceo de carga, la segmentación por VLAN y la administración de calidad de servicio (QoS). Estas funciones son fundamentales en las redes WISP, ya que permiten distribuir el tráfico de forma inteligente sin provocar saturación y mantener el servicio incluso en caso de fallo de uno de los enlaces.

Este proyecto se desarrolla en un entorno controlado dentro de un laboratorio, donde se simula la implementación de una red WISP con técnicas de balanceo de carga y optimización del ancho de banda. El objetivo es evaluar el comportamiento del balanceo de carga ante fallos de conectividad y verificar la continuidad del servicio en condiciones simuladas.

También se realiza la segmentación lógica de la red mediante VLAN, lo que permite representar la separación del tráfico de distintas áreas funcionales, como servicios VIP, usuarios empresariales y usuarios de la comunidad. Esto permite analizar la contribución de estas técnicas a una gestión del tráfico más segura, organizada y eficiente en redes reales.

La simulación en el entorno de laboratorio permite observar el comportamiento de una infraestructura de red frente a diferentes casos, considerando los aspectos más importantes, como la disponibilidad, la redundancia de enlaces y la recuperación automática ante fallos. Estos factores son fundamentales en el entorno de producción y su estudio en condiciones controladas proporciona un marco ideal para validar su eficacia antes de la implementación real.

Durante este proceso se utilizan dispositivos gestionables que permiten implementar configuraciones avanzadas de equilibrio de carga, segmentación mediante VLAN y control del ancho de banda en el entorno de laboratorio, lo que proporciona una base sólida para el análisis de soluciones aplicables a redes WISP reales [1].

# Capítulo 1. Aspectos introductorios

## 1.1.Antecedentes

Los habitantes de lugares alejados de las ciudades, como pequeños pueblos o comunidades donde el avance tecnológico en las telecomunicaciones aún es limitado, deben recurrir, en muchos casos, a terceros para acceder a estos servicios. A ello se suma el elevado costo de los servicios de internet ofrecidos por las grandes operadoras presentes en el país, lo que dificulta su contratación para determinados sectores de la población.

Ante esta situación, han surgido diversas empresas con el objetivo de brindar acceso a internet a bajo costo, sin dejar de lado la calidad de servicio. En este sentido, los WISP (proveedores de servicios de internet inalámbrico) han sido una solución eficaz por su bajo costo de implementación, flexibilidad y cobertura en lugares donde los operadores tradicionales no llegan [2].

El modelo de redes WISP está orientado al uso de tecnologías inalámbricas con el fin de proporcionar acceso a internet mediante equipos como *routers*, antenas, *switches* gestionables y *software* de administración de tráfico. Sin embargo, para que funcione correctamente, se requiere conocimiento técnico específico, especialmente en temas como el balanceo de carga, la gestión del ancho de banda y la segmentación del tráfico, que permiten optimizar el uso de los recursos disponibles y garantizar una experiencia adecuada al usuario. Aunque las redes WISP desempeñan un papel importante en el sector de las telecomunicaciones, todavía son pocas las universidades que incluyen formalmente su estudio en los programas académicos. Muchos planes de estudio de ingeniería y tecnologías de la información enfatizan los contenidos teóricos y dejan de lado la aplicación práctica de soluciones en entornos controlados. Esta situación abre una brecha entre la

academia y las necesidades del mercado, lo que obliga a los ingenieros a enfrentarse a escenarios con múltiples usuarios, enlaces compartidos y recursos limitados.

Investigaciones anteriores han explorado el uso de técnicas como PCC (Per Connection Classifier), IP *Hashing*, Round Robin y Least Connections para distribuir de forma equitativa el tráfico entre múltiples enlaces. Asimismo, la implementación de políticas de QoS ha sido crucial para priorizar tráfico crítico, como voz o video, frente a servicios menos sensibles a la latencia. La combinación de estas herramientas ayuda a mejorar el rendimiento de las redes, disminuir la congestión y aumentar la calidad de servicio [3].

En cuanto a la segmentación del tráfico, el uso de VLAN dedicadas a cada tipo de servicio ha adquirido relevancia en entornos donde se requiere garantizar la seguridad y el aislamiento del tráfico, como redes empresariales, servicios VIP o redes comunitarias.

El proyecto se alinea con estos avances y propone la creación de un entorno de laboratorio que simule una red WISP bajo condiciones reales. En este entorno se pretende formar a los estudiantes para la gestión práctica de redes inalámbricas, mediante la aplicación de técnicas modernas de balanceo y optimización, con el fin de que adquieran competencias acordes con las exigencias del mundo laboral actual.

## 1.2.Planteamiento del problema

En la formación académica de los estudiantes de telecomunicaciones, el conocimiento práctico sobre redes inalámbricas de proveedores de servicios de internet (WISP) es escaso. Muchos programas educativos se enfocan en conceptos teóricos sin proporcionar suficientes oportunidades para la implementación y optimización de redes en un entorno realista. Esta falta de experiencia práctica crea una brecha entre la educación universitaria y las necesidades del mercado laboral, en el que los ingenieros deben gestionar redes con recursos limitados, optimizar el ancho de banda y aplicar técnicas de balanceo de carga para mejorar la calidad de servicio.

La falta de laboratorios específicos para redes WISP en instituciones académicas impide que los estudiantes desarrollen habilidades esenciales para implementar y mantener este tipo de infraestructuras. Esto se traduce en profesionales con conocimientos insuficientes para diseñar y gestionar redes de manera eficiente en entornos reales, lo cual afecta su desempeño en el campo laboral y la competitividad en el sector de las telecomunicaciones.

## 1.3.Justificación

Hoy en día, el acceso a internet se ha vuelto una necesidad fundamental para el desarrollo educativo, económico y social; sin embargo, muchas zonas rurales y comunidades con infraestructura limitada siguen teniendo graves dificultades para acceder a servicios de conectividad estables y de calidad. Frente a este escenario, las redes WISP (Wireless Internet Service Provider) ofrecen una alternativa viable y eficiente, ya que permiten brindar servicios de internet a través de tecnologías inalámbricas y evitar los elevados costos de cableado y despliegue que implican las soluciones tradicionales [4].

Sin embargo, la gestión de redes WISP conlleva diversos retos técnicos, tales como la optimización del ancho de banda, la distribución equitativa de la carga entre los usuarios o los servicios y la adopción de medidas de seguridad, incluida la segmentación del tráfico mediante VLAN. Estos retos se vuelven más complejos en entornos con recursos limitados, donde los operadores deben optimizar el uso de la infraestructura básica para brindar un servicio de calidad a diferentes tipos de usuarios, desde clientes residenciales hasta empresas o instituciones. En el ámbito académico, la enseñanza sobre redes se limita normalmente a conceptos generales acerca de la conectividad y deja de lado temas más específicos, como la gestión avanzada del tráfico en redes WISP. Esta falta de práctica especializada limita la preparación de los estudiantes para afrontar situaciones reales, en las que la aplicación de técnicas como Round Robin, Least Connections o la segmentación por VLAN resulta indispensable para mantener un servicio eficiente, seguro y escalable [2].

Por ello, el presente proyecto se centra en diseñar e implementar un entorno de laboratorio que permita la simulación de redes WISP reales mediante la aplicación de diversas técnicas de balanceo de carga, control del ancho de banda y segmentación del tráfico. Se emplearán un switch

gestionable y herramientas accesibles con el fin de reproducir condiciones de bajo costo, pero de alto valor didáctico, y permitir que los estudiantes adquieran experiencia práctica directa en la configuración y prueba de redes avanzadas. También se plantea la elaboración de una guía de prácticas y recomendaciones para la enseñanza de estas tecnologías, de manera que el conocimiento generado supere el marco del proyecto y sirva como base de futuros trabajos académicos. Esta guía servirá de apoyo a centros de enseñanza que pretendan actualizar sus laboratorios de redes, lo que favorecerá una enseñanza más completa, práctica y ajustada a las exigencias del mercado laboral actual.

## 1.4.Descripción del proyecto

El objetivo del presente proyecto es diseñar e implementar un entorno de laboratorio para la simulación de redes WISP (Wireless Internet Service Provider), en el que se integren técnicas avanzadas de balanceo de carga, optimización del ancho de banda y segmentación del tráfico mediante VLAN. Este entorno permitirá a los estudiantes de telecomunicaciones adquirir competencias prácticas en la configuración, gestión y análisis de redes inalámbricas de acceso mediante el empleo de equipamiento real y herramientas de software propias del sector.

La solución planteada consiste en utilizar un switch gestionable y un router como núcleo de red, en el cual se analizarán y compararán técnicas de balanceo de carga como PCC (Per Connection Classifier), IP Hashing, Round Robin, ECMP (Equal Cost Multi-Path Routing) y Least Connections, con el propósito de seleccionar la alternativa más adecuada para su implementación. Estas técnicas permitirán distribuir de manera eficiente el tráfico entre diferentes rutas o enlaces simulados, lo que mejorará la utilización de los recursos de red y evitará cuellos de botella [2].

También se implementarán mecanismos de gestión del ancho de banda y de calidad de servicio (QoS) para dar prioridad al tráfico más sensible, como los servicios de voz o video, frente a otros tipos de datos menos críticos. Esta optimización se conseguirá mediante el uso de reglas de priorización y colas de tráfico definidas en el router.

Se realizará la segmentación del tráfico mediante la creación de VLAN independientes según el tipo de usuario o servicio, como clientes VIP, clientes empresariales y usuarios de tipo estándar o comunidad. Esta separación lógica permitirá simular escenarios reales en los que se requiere garantizar la seguridad, la privacidad y la asignación diferenciada de recursos.

Al finalizar, se elaborará una guía técnica y pedagógica que recopile las configuraciones, prácticas y recomendaciones desarrolladas durante el proyecto. Esta guía será un recurso de enseñanza para cursos y talleres especializados en redes WISP, lo que contribuirá a consolidar la formación de los estudiantes en el diseño, implementación y mantenimiento de este tipo de infraestructuras [4].

## 1.5.Objetivos

### 1.5.1. Objetivo general

Diseñar e implementar un entorno de laboratorio para la simulación y optimización de una red WISP, utilizando técnicas avanzadas de balanceo de carga, gestión del ancho de banda y segmentación del tráfico mediante VLAN, con el fin de fortalecer las prácticas de los estudiantes en la gestión y la seguridad de este tipo de redes.

### 1.5.2. Objetivos específicos

- Analizar las principales técnicas de balanceo de carga, optimización del ancho de banda y segmentación del tráfico mediante VLAN en redes WISP, con énfasis en su aplicabilidad en entornos con recursos limitados.
- Configurar y probar un entorno de red basado en un router y un switch gestionable, implementando técnicas como PCC (Per Connection Classifier) para mejorar la gestión del tráfico.
- Evaluar la implementación de VLAN dedicadas a cada tipo de servicio, garantizando la seguridad y la calidad de servicio (QoS) mediante técnicas de priorización y segmentación del tráfico.

- Desarrollar una guía de prácticas y recomendaciones para la enseñanza y aplicación de estas tecnologías, para que los estudiantes adquieran experiencia en la administración de redes WISP con segmentación de servicios.

### 1.6.Alcance del proyecto

El alcance del presente proyecto comprende el diseño, la configuración y la implementación de un entorno de laboratorio funcional que permita simular una red WISP en condiciones similares a las reales, utilizando equipos accesibles, como un switch gestionable y otros dispositivos de red. Este entorno servirá para aplicar y evaluar técnicas de balanceo de carga, gestión del ancho de banda y segmentación del tráfico mediante VLAN, de acuerdo con los objetivos planteados.

Este proyecto permitirá una distribución eficiente del tráfico de red mediante el análisis e implementación de técnicas como PCC (Per Connection Classifier), Round Robin o Least Connections, lo que mejorará la disponibilidad del servicio en escenarios con múltiples usuarios. De igual forma, la implementación de VLAN específicas para los distintos tipos de servicios (empresarial, VIP y estándar) garantizará la seguridad de los datos y la segmentación del tráfico, lo cual contribuirá a una mejor calidad de servicio (QoS) en la red simulada [5].

El proyecto prevé, además, el desarrollo de una guía práctica orientada a estudiantes, con el propósito de extender su alcance más allá del entorno técnico y posibilitar que el conocimiento y la experiencia adquiridos sean reproducidos y utilizados como material didáctico en cursos de redes inalámbricas, telecomunicaciones o infraestructura de red. De este modo, los objetivos específicos del proyecto están directamente alineados con los resultados esperados: por una parte, proveer una experiencia formativa práctica y aplicable y, por otra, proponer soluciones técnicas

viables que puedan ser implementadas en escenarios reales de conectividad con recursos limitados. Se busca generar un impacto educativo y validar técnicamente las soluciones implementadas, lo cual contribuye al fortalecimiento de las capacidades profesionales de los futuros ingenieros.

## 1.7.Metodología

La metodología del presente proyecto combina tres enfoques de investigación: descriptivo, documental y aplicado, lo que permite abordar el estudio desde una perspectiva integral que conecte la teoría con la práctica en el contexto de redes WISP. Esta combinación metodológica facilitará la caracterización, el análisis y la implementación de soluciones técnicas y didácticas en escenarios simulados con recursos limitados.

### 1.7.1. Investigación descriptiva

Este tipo de investigación pretende detallar y caracterizar los fenómenos, procesos o sistemas tal y como se presentan, lo que permite entender su estructura, funcionamiento y componentes sin modificarlos. En este proyecto se empleará para caracterizar las principales técnicas de balanceo de carga, optimización del ancho de banda y segmentación del tráfico que se utilizan actualmente en redes WISP.

Se estudiará el impacto que estas técnicas tienen sobre el rendimiento, la estabilidad y la eficiencia de las redes inalámbricas. También se describirán los elementos básicos de una red WISP, su funcionamiento general y los problemas más comunes que presenta, especialmente en zonas rurales o con recursos limitados.

### 1.7.2. Investigación documental

La investigación documental se basa en la revisión y análisis de fuentes bibliográficas y técnicas, con el objetivo de sustentar teóricamente el proyecto y tomar decisiones fundamentadas

en la información existente. En este caso, se llevará a cabo mediante el análisis de artículos científicos, manuales técnicos, normas y documentación oficial de fabricantes como MikroTik y TP-Link.

Esta etapa permitirá identificar buenas prácticas, configuraciones recomendadas y antecedentes relevantes en la implementación de técnicas como balanceo de carga, QoS y segmentación mediante VLAN. La información recopilada será clave para fundamentar el diseño del entorno de laboratorio y sus aplicaciones didácticas [6].

### 1.7.3. Investigación aplicada

La investigación aplicada utiliza conocimientos teóricos para la resolución de problemas prácticos mediante el desarrollo de soluciones que puedan ser aplicadas y evaluadas en contextos reales o simulados. En el proyecto se diseñará e implementará un entorno de laboratorio que simule una red WISP real. En este entorno se analizarán y compararán técnicas como PCC, IP Hashing, Round Robin, ECMP (Equal Cost Multi-Path Routing) y Least Connections, y se implementará la técnica seleccionada de acuerdo con los criterios definidos para el proyecto, así como mecanismos de gestión del ancho de banda mediante QoS y segmentación del tráfico mediante VLAN. Posteriormente, se realizarán pruebas de desempeño bajo diferentes escenarios de tráfico para evaluar la eficiencia y estabilidad de las configuraciones implementadas. Asimismo, se desarrollará una guía técnica paso a paso dirigida a los estudiantes, como herramienta educativa para reforzar su aprendizaje en materia de gestión y seguridad de redes inalámbricas [1].

# Capítulo 2. Marco teórico y conceptual

## 2.1. Fundamentos de las redes WISP

Un WISP es un proveedor de servicios de internet que utiliza tecnologías de comunicación inalámbrica para ofrecer conectividad a usuarios finales, principalmente en áreas rurales, remotas o de difícil acceso, donde la infraestructura tradicional de cableado (como fibra óptica o cable coaxial) es costosa, inviable o inexistente. Mediante el uso de enlaces punto a punto (PtP) y punto a multipunto (PtMP), estos proveedores proporcionan cobertura de red utilizando frecuencias licenciadas o libres del espectro radioeléctrico e implementando una topología que puede adaptarse según la geografía y la densidad poblacional de la zona de cobertura.

Las redes WISP se han convertido en una solución efectiva en los últimos años para cerrar la brecha digital, especialmente en países en vías de desarrollo; sin embargo, el rápido aumento de la demanda de ancho de banda y del número de usuarios conectados plantea importantes desafíos técnicos relacionados con la calidad de servicio (QoS), la estabilidad de la red y la eficiencia en la utilización de los recursos disponibles. Estos desafíos adquieren especial relevancia porque muchos WISP operan con infraestructura y recursos económicos limitados, además de estar expuestos a condiciones ambientales que pueden afectar el rendimiento de los enlaces inalámbricos.

Entre los principales problemas operativos que enfrentan las redes WISP se encuentran:

### Saturación de enlaces troncales

En horas pico, el tráfico agregado de múltiples clientes puede superar la capacidad disponible de los enlaces principales, lo que provoca latencia elevada, pérdida de paquetes y reducción de la velocidad efectiva de navegación.

**Mala calidad de servicio (QoS)**

La imposibilidad de priorizar adecuadamente ciertos tipos de tráfico, como voz sobre IP (VoIP) o videoconferencias, puede traducirse en una experiencia deficiente para el usuario y afectar la percepción del servicio.

**Caídas de red por mal direccionamiento del tráfico**

En redes con múltiples salidas hacia internet (por ejemplo, varios proveedores), la ausencia de una estrategia de distribución de tráfico puede generar inestabilidad, interrupciones o uso ineficiente del ancho de banda contratado.

**Dificultad para distribuir la carga entre varios enlaces**

Muchos WISP utilizan más de un proveedor de internet o combinan diferentes tecnologías (fibra, radioenlaces, LTE), pero, sin un sistema de balanceo de carga adecuado, algunos enlaces pueden estar sobrecargados mientras otros permanecen infrautilizados.

Frente a esta situación, la aplicación de técnicas de balanceo de carga y gestión del ancho de banda constituye una estrategia clave para mejorar el rendimiento general de la red, asegurar la disponibilidad del servicio y brindar una experiencia de usuario más estable y satisfactoria. Estas técnicas permiten optimizar la utilización de múltiples rutas o enlaces disponibles, redistribuir el tráfico de manera inteligente y establecer mecanismos de priorización y reserva de recursos, y contribuyen así a una red más robusta, escalable y adaptable a las exigencias del entorno [7].

## 2.2. Balanceo de carga

El balanceo de carga es un mecanismo utilizado para distribuir de forma equitativa o estratégica el tráfico de datos entre varios recursos disponibles, como enlaces de internet,

servidores, nodos de red o puertas de enlace. Tiene como objetivo principal optimizar el uso de los recursos, mejorar el rendimiento global del sistema, minimizar los tiempos de respuesta y garantizar la alta disponibilidad de los servicios, de modo que se evita que un solo recurso se sature mientras otros permanecen infrautilizados.

En la práctica, el balanceo de carga permite gestionar de forma eficiente múltiples flujos de datos, asignando cada petición o paquete de información al recurso más adecuado en función de criterios como la carga actual, la latencia, el tipo de tráfico o la capacidad del enlace. Esta distribución inteligente y dinámica del tráfico contribuye a que la red sea más estable y fiable, y a mejorar la experiencia del usuario [8].

Entre los beneficios más importantes del balanceo de carga se destacan:

**Optimización del uso de recursos disponibles:** se aprovecha la totalidad de la capacidad de múltiples enlaces o equipos, de modo que se evitan los cuellos de botella.

**Incremento del rendimiento y la velocidad:** al evitar la saturación de un solo canal, se garantiza que el tráfico circule de manera más eficiente y rápida.

**Reducción de fallos y aumento de la disponibilidad:** en caso de que uno de los enlaces o servidores falle, el sistema puede redirigir automáticamente el tráfico hacia otros recursos funcionales.

**Escalabilidad:** permite añadir más enlaces o servidores de forma modular sin necesidad de reconfigurar la red desde cero.

El balanceo de carga adquiere mayor relevancia en las redes WISP, que normalmente operan con varios enlaces de distinta índole y capacidad (fibra óptica dedicada, radio punto a

punto, LTE, varios proveedores de internet de respaldo, etc.). En estos entornos, esta técnica ayuda a solucionar problemas de saturación y asegura un uso eficaz del ancho de banda disponible.

### 2.2.1. Escenarios de aplicación del balanceo de carga

Los principales escenarios en los que se aplica el balanceo de carga en redes WISP incluyen:

**Múltiples enlaces WAN (Wide Area Network):** la salida a internet de un router puede estar conformada por varios proveedores o tecnologías. El balanceador determina a través de qué enlace debe dirigirse cada conexión o tipo de tráfico.

**Diferentes torres base:** en una red WISP que cubre grandes zonas geográficas, puede ser necesario distribuir la carga entre torres o nodos de acceso inalámbrico para evitar sobrecargas en puntos específicos.

**Nodos intermedios en redes malladas:** en topologías mesh (malla), donde múltiples rutas pueden conectar un cliente con la red troncal, el balanceo permite seleccionar la ruta óptima según métricas como la congestión, la pérdida de paquetes o la interferencia.

Implementar balanceo de carga en una red WISP no solo mejora la eficiencia técnica, sino que también representa una ventaja competitiva para el proveedor, ya que permite ofrecer un servicio más confiable y de mayor calidad, incluso en condiciones adversas o de alta demanda [8].

## 2.3. Técnicas de balanceo de carga en redes WISP

El balanceo de carga puede implementarse mediante diversas técnicas, diferenciadas por el criterio empleado para distribuir las conexiones o el tráfico entre los enlaces disponibles. Estas técnicas permiten establecer diferentes mecanismos de clasificación y asignación del tráfico, de acuerdo con las características de las conexiones, parámetros de la comunicación y las condiciones

de los enlaces utilizados. En este contexto, la selección de una técnica determinada depende de las características de la red y de los requerimientos del escenario en el que se implementa. Algunas técnicas se basan en la clasificación de las conexiones a partir de determinados parámetros del tráfico, la distribución de paquetes o la selección de rutas de igual costo. Por ello, cada mecanismo presenta características particulares que deben considerarse al momento de diseñar una solución de balanceo para una red WISP. Entre las principales técnicas se encuentran PCC (Per Connection Classifier), NTH Load Balancing, ECMP (*Equal Cost Multi-Path*), IP Hashing y Least Connections, cuyas características y mecanismos de funcionamiento, ventajas y desventajas se describen a continuación [3].

### 2.3.1. PCC (Per Connection Classifier)

El Per Connection Classifier (PCC) es una técnica de balanceo de carga muy utilizada en los routers MikroTik y otros sistemas de gestión de tráfico. Esta técnica examina las características de cada conexión nueva, tales como las direcciones IP de origen y destino, los puertos involucrados y el protocolo utilizado (TCP/UDP), y la clasifica de acuerdo con un conjunto predefinido de reglas.

Una vez establecida, la conexión se mantiene en el mismo enlace WAN durante toda su vida útil, evitando saltos entre enlaces que podrían provocar pérdida o desorden de paquetes. PCC funciona mejor en escenarios donde existen varios enlaces con capacidades similares, ya que asigna las conexiones de forma equilibrada sin necesidad de monitorear constantemente la carga [9].

En la Tabla 1 se presentan las ventajas y desventajas de la técnica de balanceo PCC.

***Tabla 1.*** *Ventajas y desventajas del PCC.*

| Ventajas | Desventajas |
|---|---|
| Buena estabilidad de conexión: se garantiza la coherencia de la ruta de la sesión. | No toma en cuenta la carga real de cada enlace. |
| Evita el desorden de paquetes, especialmente en protocolos como TCP. | Distribución ineficiente en escenarios de tráfico asimétrico. |
| Distribución eficiente en escenarios con tráfico uniforme. | No es ideal si los enlaces tienen diferentes capacidades. |

*Nota.* Elaboración propia.

### 2.3.2. NTH Load Balancing

La técnica NTH (*Nth Packet Load Balancing*) funciona mediante la distribución por turnos de los paquetes a las interfaces disponibles, siguiendo un método similar al *Round Robin*. Es decir, se puede configurar el sistema para que, cada cinco paquetes, uno se dirija por el segundo enlace, otro por el tercero, y así sucesivamente. Es un método relativamente sencillo de implementar y funciona bien cuando el tráfico es constante y los enlaces tienen capacidades y latencias similares. Sin embargo, cuando los enlaces son asimétricos o presentan grandes diferencias de velocidad, esta técnica puede provocar congestión en los enlaces más lentos y un aprovechamiento ineficiente de los más rápidos [9].

En la Tabla 2 se presentan las ventajas y desventajas de la técnica NTH Load Balancing.

***Tabla 2.*** *Ventajas y desventajas de NTH.*

| Ventajas | Desventajas |
|---|---|
| Distribución equitativa a nivel de paquetes. | No mantiene la coherencia de la sesión, por lo que no es recomendable para tráfico TCP. |
| Fácil de configurar. | Bajo rendimiento si los enlaces no son equivalentes en velocidad o calidad. |
| Útil en entornos donde no es crítico mantener la integridad de cada conexión, como en tráfico UDP o masivo. | Inestable para protocolos sensibles, como HTTPS, VoIP o SSH. |

*Nota.* Elaboración propia.

### 2.3.3. ECMP (*Equal Cost Multi-Path*)

ECMP (Equal Cost Multi-Path Routing) es un método que se emplea principalmente en protocolos de enrutamiento dinámico, tales como OSPF o BGP. Esta técnica permite utilizar simultáneamente varias rutas con el mismo costo métrico para transmitir tráfico. En redes WISP, esta técnica puede aplicarse en la capa de enrutamiento para equilibrar el tráfico entre varias rutas hacia un mismo destino, siempre que tengan la misma métrica. Es decir, el algoritmo considera que existen dos o más rutas igualmente viables y reparte de forma equitativa el tráfico entre ellas [10].

En la Tabla 3 se presentan las ventajas y desventajas de esta técnica de balanceo de carga.

***Tabla 3.*** *Ventajas y desventajas de ECMP.*

| Ventajas | Desventajas |
|---|---|
| Escalabilidad en redes grandes con múltiples rutas. | Requiere que las rutas tengan exactamente el mismo costo. |
| Compatible con protocolos dinámicos de enrutamiento. | Presenta menor flexibilidad cuando los enlaces tienen diferentes características y capacidades. |
| Buena distribución de tráfico cuando los enlaces son homogéneos. | Su distribución del tráfico es menos adecuada cuando los enlaces no son homogéneos. |

*Nota.* Elaboración propia.

### 2.3.4. IP Hashing

El IP Hashing es una técnica de balanceo que aplica una función hash a determinados campos del encabezado IP (como la IP de origen o destino) para determinar por qué enlace debe dirigirse una conexión o flujo de datos. Este método garantiza que todas las conexiones provenientes del mismo cliente o dirigidas al mismo servidor seguirán siempre la misma ruta, manteniendo así la coherencia de la sesión. Es especialmente útil para aplicaciones que requieren persistencia en la conexión, como llamadas VoIP, videoconferencias y servicios de *streaming* [11].

En la Tabla 4 se presentan las ventajas y desventajas del IP Hashing.

***Tabla 4.*** *Ventajas y desventajas de IP Hashing.*

| Ventajas | Desventajas |
|---|---|
| Coherencia en las rutas de conexión. | No considera la carga en tiempo real. |
| Recomendado para tráfico sensible a la latencia o la pérdida de paquetes. | Distribución desigual si un usuario genera un volumen elevado de tráfico. |
| Compatible con balanceadores de alto rendimiento. | Dependencia del algoritmo de hash. |

*Nota.* Elaboración propia.

### 2.3.5. Least Connections

El algoritmo Least Connections (menor número de conexiones activas) asigna las nuevas conexiones al enlace o servidor que tenga menos sesiones activas en ese momento. Es una estrategia dinámica que evalúa continuamente la carga de trabajo de cada recurso y toma decisiones basadas en el número de conexiones actuales, no en el volumen de tráfico. Esta técnica es ampliamente utilizada en los balanceadores de carga de servidores web, pero también puede aplicarse en routers avanzados o controladores de tráfico en redes WISP, especialmente en escenarios con un elevado número de usuarios concurrentes, donde se busca distribuir el tráfico de forma más equitativa [12].

En la Tabla 5 se presentan las ventajas y desventajas de esta técnica de balanceo.

***Tabla 5.*** *Ventajas y desventajas de Least Connections.*

| Ventajas | Desventajas |
|---|---|
| Distribución dinámica y adaptativa. | Puede requerir *hardware* con capacidad de procesamiento adicional. |
| Mejora el rendimiento bajo condiciones de alta carga. | No siempre refleja el volumen real de tráfico por enlace, ya que una conexión puede consumir más recursos que muchas conexiones pequeñas. |
| Reduce el riesgo de saturar un solo enlace. | No es recomendable para redes pequeñas o con tráfico constante. |

*Nota.* Elaboración propia.

## 2.4. Técnicas de balanceo de ancho de banda

En las redes WISP, el balanceo de ancho de banda es una estrategia esencial para asegurar un uso eficiente de los recursos de red y brindar un nivel de calidad de servicio aceptable a los usuarios, especialmente en situaciones de conectividad limitada o cuando varios clientes compiten

por los recursos disponibles. A diferencia del balanceo de carga, que distribuye conexiones, el balanceo de ancho de banda asigna porciones del ancho de banda disponible en función de las prioridades, el tipo de tráfico o los usuarios. Esta gestión resulta fundamental para redes inalámbricas rurales, donde los enlaces troncales pueden ser escasos, costosos o afectados por interferencias. A continuación, se detallan algunas de las técnicas más relevantes para implementar este tipo de balanceo en entornos WISP [11].

### 2.4.1. QoS (calidad de servicio)

La calidad de servicio (QoS) es un conjunto de mecanismo de gestión del tráfico que operan en el nivel de aplicación de políticas, mediante los cuales se establecen prioridades para ciertos tipos de servicios o usuarios. En un escenario WISP, en el que coexisten diversos tipos de tráfico (navegación, videollamadas, descargas, etc.), la QoS se vuelve indispensable para que servicios sensibles a la latencia, como VoIP, videoconferencias o juegos en línea, tengan prioridad frente a aplicaciones que admiten mayor retraso, como archivos de actualizaciones [7].

La QoS se puede implementar mediante colas simples (*Simple Queues*), que se configuran por IP o por interfaz y permiten limitar o garantizar determinados anchos de banda a usuarios específicos. Las colas jerárquicas (HTB, Hierarchical Token Bucket) permiten crear estructuras complejas de prioridades en las que se pueden definir clases padre e hijo, estableciendo no solo límites máximos y mínimos, sino también prioridades relativas entre flujos de tráfico.

#### Beneficios de QoS

La implementación de QoS ofrece diversos beneficios relacionados con la gestión eficiente del tráfico y la priorización de los servicios de red. Entre los principales beneficios de su aplicación se encuentran los siguientes:

- Mejora la experiencia del usuario al priorizar tráfico crítico.
- Evita la saturación de la red por aplicaciones no prioritarias.
- Permite ofrecer diferentes niveles de servicio.

### 2.4.2. Burst (modo ráfaga)

El modo ráfaga (*Burst*) es una técnica que permite a los usuarios exceder temporalmente su límite de ancho de banda asignado, siempre y cuando la red tenga capacidad disponible. Esta técnica mejora significativamente la percepción de velocidad, especialmente durante tareas de corta duración, como cargar una página web, abrir un video o iniciar una descarga. Los umbrales de ráfaga (burst-threshold) establecen las condiciones necesarias para habilitar el modo ráfaga, generalmente relacionadas con el uso promedio del cliente [13].

En la Tabla 6 se presentan las ventajas y desventajas del Burst o modo ráfaga aplicado al balanceo de ancho de banda.

***Tabla 6.*** *Ventajas y desventajas de Burst.*

| Ventajas | Desventajas |
|---|---|
| Ofrece una mejor experiencia a usuarios residenciales. | No garantiza velocidad sostenida. |
| Permite mantener límites sostenidos mientras mejora el rendimiento en tareas puntuales. | Puede saturar el enlace si muchos usuarios utilizan el modo ráfaga simultáneamente. |
| Reduce las quejas de los usuarios en redes con limitaciones de capacidad sin comprometer el control general. | Requiere configuración precisa. |

*Nota.* Elaboración propia.

### 2.4.3. Balanceo por prioridades de tráfico

El balanceo por prioridades de tráfico permite dirigir diferentes tipos de tráfico hacia los enlaces disponibles, con base en criterios definidos por el administrador de red. Por ejemplo, un enlace de mejor calidad puede reservarse para tráfico VoIP o videoconferencias, mientras que el tráfico de navegación o streaming puede enrutarse por enlaces secundarios [14].

Esta técnica suele requerir una configuración avanzada mediante herramientas de marcado de tráfico, como las siguientes:

**Mangle:** permite identificar y clasificar paquetes por tipo de protocolo, puerto, dirección IP, etc.

**Routing Marks:** se utilizan junto con *Mangle* para aplicar rutas específicas a diferentes tipos de tráfico.

**Multiple routing tables:** permiten definir rutas específicas para distintos tipos de servicios.

#### Aplicaciones comunes

El balanceo por prioridad de tráfico puede aplicarse en diferentes escenarios de una red, de acuerdo con las características y necesidades de los servicios que utilizan los enlaces disponibles. Entre las principales aplicaciones de esta técnica se encuentran las siguientes:

- Separación de tráfico empresarial y residencial.
- Uso eficiente de enlaces según el perfil del tráfico.
- Aseguramiento de calidad en servicios sensibles.

## 2.5. Arquitectura de redes WISP

La arquitectura de las redes WISP comprende el conjunto de elementos físicos, lógicos y de comunicación que permiten proporcionar acceso a internet mediante tecnologías inalámbricas. A diferencia de los proveedores tradicionales, que dependen principalmente de una estructura cableada, las redes WISP utilizan enlaces de radiofrecuencia para transportar datos.

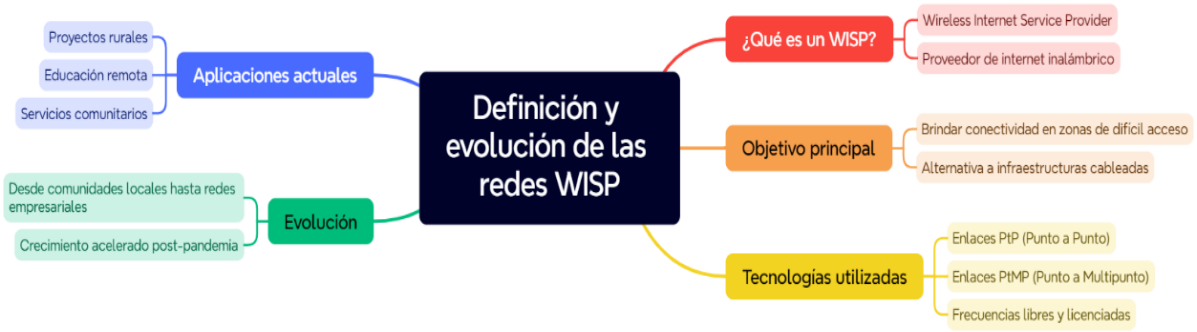
### 2.5.1. Definición y evolución de las redes WISP

A diferencia de los proveedores tradicionales de internet, los WISP no generan tráfico de datos, sino que lo transportan desde un proveedor *upstream* o mayorista hacia los usuarios finales. Este modelo permite que los WISP operen con una infraestructura más liviana, pero también les plantea desafíos importantes en términos de estabilidad del servicio, capacidad de ancho de banda disponible y condiciones ambientales que afectan los enlaces inalámbricos.

Desde su aparición, las redes WISP han experimentado una evolución significativa gracias a los avances en tecnologías inalámbricas. Inicialmente, ofrecían servicios con velocidades limitadas y conexiones inestables. Sin embargo, con la llegada de estándares como Wi-Fi 5 y Wi-Fi 6, y de tecnologías como LTE y 5G aplicadas a soluciones fijas, los WISP han logrado un avance sustancial en la calidad de sus servicios, con velocidades competitivas y una mayor fiabilidad. Este desarrollo también ha sido posible gracias a la reducción de los costos de los equipos, la facilidad de instalación y una gestión remota más eficiente. Estos avances han facilitado que los proveedores amplíen su cobertura hacia zonas marginales mediante modelos de negocio sostenibles, que permiten recuperar la inversión inicial en menor tiempo y ofrecer soluciones más rápidas y personalizadas a los usuarios [2].

En la Figura 1 se presenta un mapa conceptual que proporciona una representación simplificada y estructurada de la definición y evolución de las redes WISP, lo que permite visualizar de forma clara las relaciones entre los conceptos principales.

***Figura 1.*** *Definición y evolución de las redes WISP.*




*Nota.* Elaboración propia.

### 2.5.2. Componentes de una red WISP

Las redes WISP suelen estar conformadas por cuatro componentes principales: torres y mástiles de transmisión, antenas punto a punto (PtP) y punto a multipunto (PtMP), routers, radios inalámbricos y equipos de red, y enlaces de *backhaul*. Estos elementos permiten establecer, distribuir y gestionar la conectividad inalámbrica de la red. La arquitectura de red debe ser sólida y capaz de gestionar el tráfico de datos de manera eficiente.

Los nodos WISP deben afrontar problemas relacionados con la interferencia en las señales, el control del tráfico, la distribución de la capacidad del ancho de banda, la calidad de servicio (QoS) y la optimización de los recursos disponibles. La eficiencia operativa de una red WISP está muy condicionada por su infraestructura física y tecnológica, que debe diseñarse para brindar conectividad estable, escalabilidad y una cobertura adecuada en ambientes geográficamente

dispares. A continuación, se describen los componentes más importantes que forman una red WISP.

### Torres y mástiles de transmisión

Las torres y mástiles son estructuras básicas en la arquitectura de una red WISP, ya que permiten elevar los equipos de transmisión (antenas y radios) por encima de obstáculos naturales o artificiales, como árboles, edificios o accidentes geográficos. La altura de estas estructuras es determinante para obtener líneas de vista despejadas (LoS, Line of Sight) entre los puntos de transmisión y recepción, algo esencial en enlaces inalámbricos de alta capacidad. Según su construcción, las torres pueden ser autoapoyadas, arriostradas o instaladas sobre edificaciones existentes; la elección de una u otra dependerá del presupuesto, la ubicación geográfica, la carga estructural que deban soportar y la cobertura requerida. Es primordial realizar estudios topográficos y de propagación antes de instalarlas para garantizar un rendimiento óptimo del enlace.

### Antenas punto a punto (PtP) y punto a multipunto (PtMP)

Las antenas son los dispositivos encargados de emitir y recibir las señales inalámbricas dentro de la red. Existen principalmente dos configuraciones:

### Antenas punto a punto (PtP)

Estas antenas se utilizan para conectar dos ubicaciones fijas, como la torre principal con un nodo de distribución remoto. Suelen ser altamente direccionales (parabólicas o de panel) y operan en bandas como 5 GHz o frecuencias licenciadas (por ejemplo, 6 GHz, 11 GHz o superiores), lo que permite enlaces de larga distancia con alta capacidad y baja latencia.

### Antenas punto a multipunto (PtMP)

Estas antenas están diseñadas para conectar una estación base con múltiples clientes finales. Emplean antenas sectoriales u omnidireccionales, dependiendo del área de cobertura, y operan comúnmente en bandas de 2,4 GHz o 5 GHz, aunque también pueden usar frecuencias licenciadas para evitar interferencias en ambientes saturados. La elección entre PtP y PtMP depende de la topología de red, el número de usuarios, el ancho de banda requerido y las condiciones ambientales del entorno [15].

### Routers, radios inalámbricos y equipos de red

Los routers y radios inalámbricos son el núcleo de procesamiento y gestión del tráfico dentro de una red WISP. Se encargan de enrutar los datos, establecer conexiones seguras, gestionar la calidad de servicio (QoS) y monitorear el rendimiento de los enlaces. Entre las marcas más utilizadas por los WISP se encuentran las siguientes:

**MikroTik:** reconocida por su versatilidad, bajo costo y funcionalidades avanzadas mediante su sistema operativo RouterOS.

**Ubiquiti:** amplia presencia en el mercado WISP gracias a sus soluciones integradas como AirMax y UniFi, que ofrecen buena relación calidad-precio.

**Cambium Networks:** preferida en implementaciones más profesionales y exigentes, con soluciones robustas y escalables como ePMP y PMP 450.

Estos dispositivos suelen incluir funciones como control de ancho de banda, *firewall*, NAT y monitoreo remoto, lo que permite una administración centralizada de la red [15].

### Enlaces de backhaul

El backhaul es el componente que conecta la red de acceso inalámbrico con la red troncal o el proveedor upstream de internet. Este puede ser:

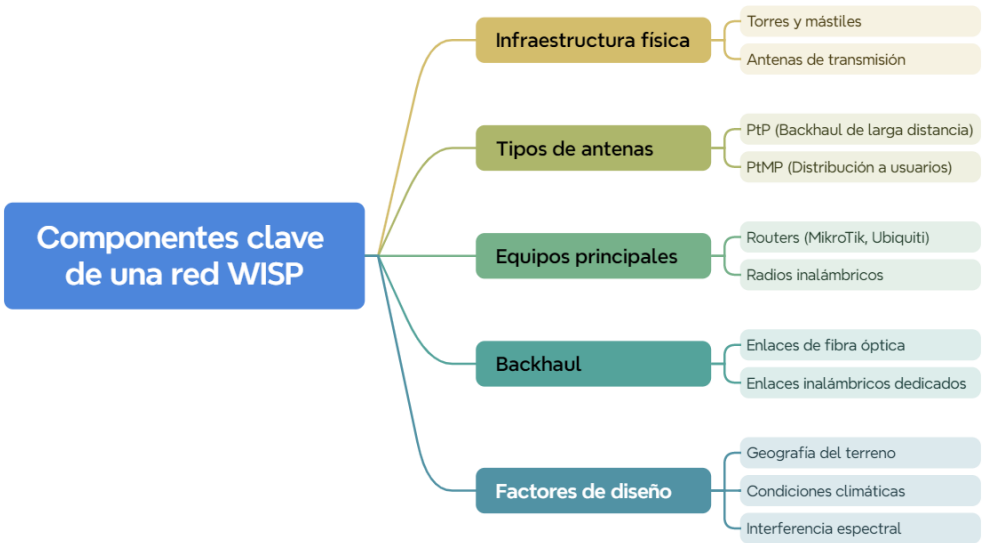
**Backhaul de fibra óptica:** ofrece alta capacidad, baja latencia y mayor confiabilidad. Es ideal cuando se dispone de infraestructura terrestre accesible.

**Backhaul inalámbrico:** se utiliza en zonas donde la fibra no está disponible. Emplea enlaces PtP de alta capacidad sobre bandas licenciadas o libres y puede cubrir distancias que superan los 20 o 30 kilómetros, dependiendo del entorno y los equipos.

El diseño del backhaul debe considerar la redundancia, la protección contra interferencias y la capacidad suficiente para soportar el tráfico agregado de todos los usuarios conectados a la red [15].

En la Figura 2 se muestra la relación entre los componentes clave de una red WISP, lo que permite realizar un análisis más claro.

***Figura 2.*** *Componentes clave de una red WISP.*




*Nota.* Elaboración propia.

### 2.5.3. WISP frente a ISP tradicionales

Los proveedores de servicios de internet inalámbrico han emergido como una alternativa viable y eficiente frente a los proveedores de servicios de internet tradicionales (ISP), especialmente en áreas rurales y de difícil acceso. A continuación, se detallan las principales ventajas y limitaciones de los WISP en comparación con los ISP convencionales.

#### Ventajas de los WISP

**Menor costo de implementación:** los WISP requieren inversiones iniciales menores que los ISP tradicionales, ya que no dependen de infraestructura física basada en cables de fibra óptica o coaxiales. Esta característica les permite prestar servicios a precios más competitivos, lo que facilita el acceso a internet en comunidades con recursos limitados.

**Rápida escalabilidad:** la naturaleza inalámbrica de las redes WISP permite una expansión rápida y eficiente. La instalación de nuevos puntos de acceso o la ampliación de la cobertura puede llevarse a cabo en períodos reducidos, lo que facilita la adaptación a las necesidades cambiantes de los usuarios y al crecimiento de la demanda.

**Cobertura flexible:** los WISP pueden proporcionar conectividad en lugares a los que los ISP tradicionales no llegan debido a barreras geográficas o económicas. Mediante el uso de tecnologías inalámbricas, pueden sortear obstáculos físicos y brindar servicios en zonas montañosas, selváticas o escasamente pobladas, lo cual contribuye a reducir la brecha digital.

**Adaptabilidad tecnológica:** los WISP tienden a incorporar tecnologías emergentes más rápidamente, como el empleo de bandas de frecuencia no licenciadas y equipos de última

generación, lo que les permite brindar servicios innovadores y adaptarse a las tendencias del mercado con mayor flexibilidad [16].

**Limitaciones de los WISP**

**Dependencia de la línea de visión (LoS):** las conexiones inalámbricas necesitan una línea de visión clara entre el transmisor y el receptor para garantizar una señal fuerte y estable. El servicio puede verse afectado por obstáculos tales como edificaciones, árboles o accidentes geográficos que interfieran con la señal.

**Interferencias y sobrecarga de espectro:** los WISP que utilizan bandas de frecuencia no licenciadas están expuestos a interferencias de otros dispositivos y redes, lo cual puede afectar el rendimiento de la conexión. La saturación del espectro es un problema habitual en las zonas urbanas muy pobladas.

**Limitaciones en el ancho de banda:** aunque los WISP han mejorado sus capacidades, aún enfrentan restricciones en cuanto al ancho de banda disponible, especialmente en comparación con las conexiones de fibra óptica ofrecidas por los ISP tradicionales. Esto puede limitar la velocidad y la cantidad de datos que los usuarios pueden transmitir simultáneamente.

**Desafíos regulatorios y legales:** en algunos países, los WISP enfrentan obstáculos relacionados con la obtención de licencias, regulaciones estrictas y falta de reconocimiento legal, lo que puede dificultar su operación y expansión.

**Dependencia de condiciones ambientales:** factores como el clima, la humedad y las condiciones atmosféricas pueden afectar la calidad de las conexiones inalámbricas, y provocan interrupciones o disminuciones en la velocidad del servicio [17].

### Comparativa con ISP tradicionales

Los ISP tradicionales ofrecen conexiones más estables y de mayor capacidad, pero su despliegue en zonas remotas se ve limitado por los altos costos de infraestructura. Por su parte, los WISP pueden llegar a comunidades desatendidas gracias a su enfoque inalámbrico, aunque con ciertas restricciones técnicas. Las redes WISP constituyen una solución eficaz para extender el acceso a internet en zonas donde los ISP tradicionales no pueden operar eficientemente; sin embargo, es fundamental afrontar sus limitaciones mediante la inversión en tecnología, capacitación y marcos regulatorios adecuados, a fin de garantizar un servicio de calidad y sostenible en el tiempo [16].

En la Figura 3 se presenta el mapa conceptual de las ventajas y limitaciones de las redes WISP, el cual facilita la comprensión del tema al mostrar de manera clara la relación entre ambos aspectos.

***Figura 3.*** *Ventajas y limitaciones.*


*Nota.* Elaboración propia.

### 2.5.4. Modelos de topología en redes WISP

Las redes WISP utilizan diversas topologías para proporcionar conectividad inalámbrica eficiente y adaptada a las necesidades específicas de cada entorno. Entre las configuraciones más comunes se encuentran las topologías punto a punto (PtP) y punto a multipunto (PtMP), así como combinaciones híbridas que integran ambas para optimizar el rendimiento y la cobertura.

#### Topología punto a punto (PtP)

La topología PtP establece una conexión directa entre dos nodos, normalmente para enlaces de backhaul que conectan estaciones base con la red troncal de internet. Esta configuración es adecuada para transmitir grandes volúmenes de datos a largas distancias con alta fiabilidad y baja latencia. Equipos como el Ubiquiti AirFiber AF-5XHD permiten velocidades superiores a 1 Gbps mediante tecnologías avanzadas como MIMO y modulación de alta densidad para maximizar el rendimiento en enlaces PtP [18].

#### Topología punto a multipunto (PtMP)

En la topología PtMP, una estación base central se conecta simultáneamente con varios equipos terminales de cliente (CPE, *customer premises equipment*), lo cual permite una distribución eficiente del servicio en zonas con gran densidad de usuarios. Esta configuración es típica en entornos urbanos y suburbanos, donde existe la necesidad de conectar a varios usuarios finales desde un solo punto de acceso. Ubiquiti, con su serie LTU, ha mejorado significativamente el rendimiento de las redes PtMP, y ha proporcionado mayor capacidad de modulación y flexibilidad en la asignación de frecuencias.

### Implementaciones híbridas: combinación de PtP y PtMP

Desde 2022, se observa una tendencia creciente hacia el uso de topologías híbridas que combinan enlaces PtP y PtMP. Esta estrategia permite a los WISP adaptar sus redes a las características topográficas y a las demandas de tráfico de cada zona. Por ejemplo, se pueden utilizar enlaces PtP para conectar estaciones base en ubicaciones remotas o de difícil acceso, mientras que las configuraciones PtMP pueden emplearse para proporcionar el servicio a múltiples usuarios en áreas densamente pobladas. El uso de tecnologías como el AirFiber MLO de Ubiquiti, con soporte para operaciones de múltiples enlaces y velocidades superiores a 5 Gbps, ha facilitado la implementación de estas arquitecturas híbridas.

### Consideraciones para la selección de la topología

La elección entre topologías PtP, PtMP o híbridas depende de varios factores, entre los que se incluyen los siguientes:

**Geografía del área de cobertura:** terrenos montañosos o con obstáculos pueden requerir enlaces PtP para garantizar la calidad de la señal.

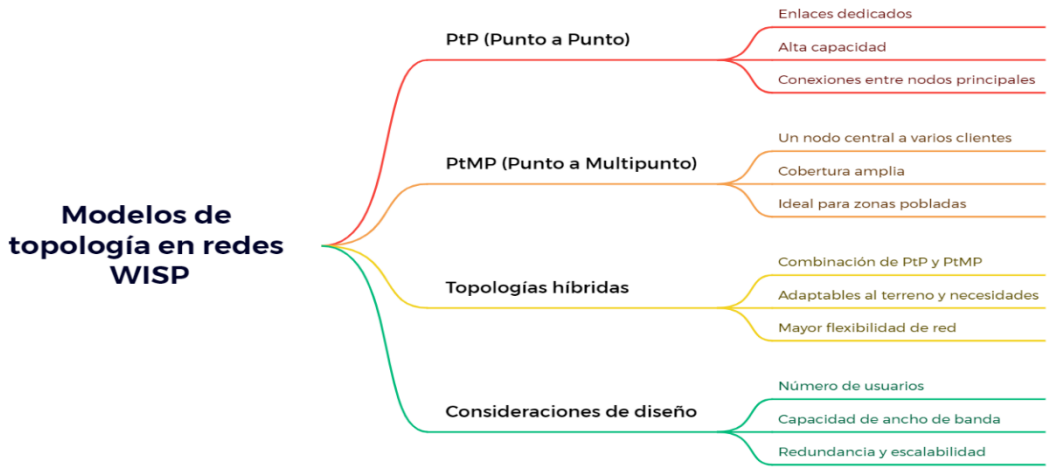
**Densidad de usuarios:** áreas con alta concentración de usuarios pueden beneficiarse de configuraciones PtMP para optimizar el uso del espectro.

**Requerimientos de ancho de banda:** aplicaciones que demandan alta capacidad de transmisión pueden necesitar enlaces PtP dedicados.

**Presupuesto y recursos disponibles:** las soluciones híbridas ofrecen flexibilidad para balancear costos y rendimiento según las necesidades específicas. La implementación de topologías adecuadas es esencial para el éxito de las redes WISP. La combinación estratégica de

enlaces PtP y PtMP permite a los proveedores ofrecer servicios de alta calidad, adaptándose a las condiciones particulares de cada entorno y satisfaciendo las crecientes demandas de conectividad. En la Figura 4 se presenta de forma simplificada el modelo de la topología de las redes WISP.

***Figura 4.*** *Modelos de topología en redes WISP.*




*Nota.* Elaboración propia.

### 2.6. Fundamentos matemáticos del balanceo de carga

El balanceo de carga se fundamenta en algoritmos matemáticos que permiten distribuir el tráfico de la red de manera eficiente entre múltiples enlaces de internet. Estos modelos buscan optimizar el uso del ancho de banda, reducir la congestión y mejorar la disponibilidad del servicio. En este apartado se presentan los fundamentos matemáticos de las principales técnicas de balanceo de carga y su aplicación en entornos WISP.

#### 2.6.1. PCC y su implementación práctica

El método PCC (Per Connection Classifier) permite determinar el enlace WAN al que se asigna una conexión a partir de determinados parámetros de esta, como las direcciones IP de origen y destino y los puertos utilizados. Para ello, los parámetros de la conexión se procesan mediante una función hash y posteriormente, se aplica una operación módulo en función del número de

enlaces WAN disponibles. De esta manera, el resultado permite identificar el enlace al que será asignada la conexión.

Matemáticamente, se puede expresar como una función hash modular:

$$H = f(IP_{origen}, IP_{destino}, Puerto_{origen}, Puerto_{destino}) mod\ N. \quad (1)$$

donde:

$\boldsymbol{f}$: función hash que combina los parámetros de la conexión.

**IP de origen**: dirección IP del equipo que inicia la conexión.

**IP de destino**: dirección IP del servidor o equipo de destino.

**Puerto de origen**: puerto de origen de la comunicación.

**Puerto de destino**: puerto del servicio de destino.

**mod N**: operador módulo, que devuelve el residuo de la división.

**N**: número total de enlaces WAN disponibles.

Esta ecuación permite determinar a qué enlace WAN se asigna una nueva conexión, de forma que todas las conexiones asociadas a una sesión, como una sesión TCP, se mantengan en el mismo enlace.

Ejemplo:

- **IP de origen**: 192.168.1.100
- **IP de destino**: 8.8.8.8
- **Puerto de origen**: 50874

- **Puerto de destino**: 443
- **Enlaces WAN disponibles**: 3 (N = 3)

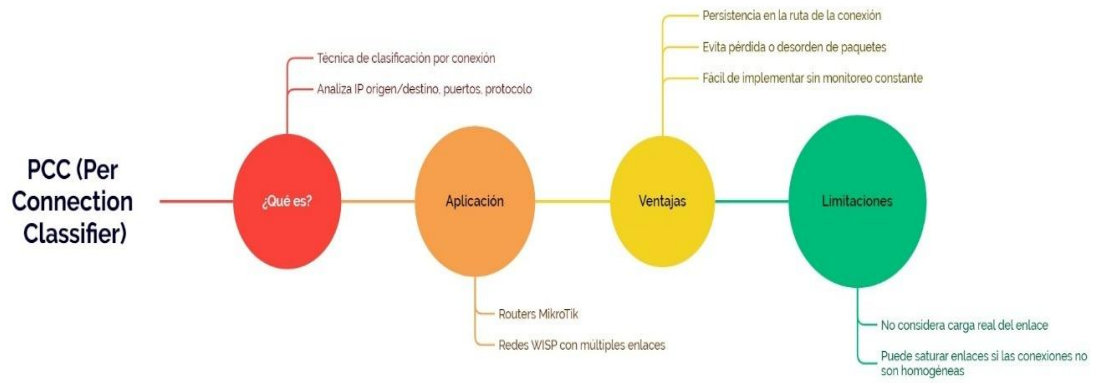
Si el valor hash resultante de esta combinación es 17, entonces:

$$17\ mod\ 3\ =\ 2$$

La conexión se asigna al enlace 3, considerando que la numeración inicia desde 0 (0 = enlace 1, 1 = enlace 2 y 2 = enlace 3).

A continuación, la Figura 5 muestra de forma simplificada la estructura del PCC (Per Connection Classifier).

***Figura 5.*** *Mapa conceptual del PCC.*




*Nota.* Elaboración propia.

### 2.6.2. Round Robin: simplicidad y aplicación

Round Robin distribuye las conexiones de forma secuencial entre varios enlaces: la primera conexión se asigna al enlace 1, la segunda al enlace 2 y así sucesivamente. Es una técnica sencilla, pero efectiva cuando las conexiones son de tamaño y duración similares.

En redes WISP, Round Robin resulta útil cuando se dispone de enlaces equilibrados en capacidad y latencia. No tiene en cuenta el peso del tráfico, pero resulta adecuado para entornos de laboratorio, demostraciones educativas o para pequeñas redes. Su fórmula matemática es:

$$Ei = (CmodN) + 1 \quad (2)$$

donde:

$\boldsymbol{Ei}$: enlace seleccionado.

$\boldsymbol{C}$: contador de conexiones o solicitudes.

$\boldsymbol{N}$: número de enlaces disponibles.

$\boldsymbol{mod}$: operador módulo.

$+1$: hace que la enumeración de los enlaces empiece en uno.

**Finalidad**

Permite asignar conexiones de manera secuencial y equitativa entre varios enlaces, independientemente de la dirección IP o el tipo de tráfico.

**Aplicación**

- Se cuenta el número total de conexiones (C) en orden de llegada.
- Se aplica la operación módulo considerando el número de enlaces disponibles.
- Se suma 1 para iniciar la numeración desde el enlace 1 y no desde 0.

Ejemplo:

- Número de conexión: C = 10
- Enlaces WAN: N = 3

$$Ei = (10 mod 3) + 1 = 1 + 1 = 2$$

Esta conexión se asigna al enlace 2.

Como se muestra en la Figura 6, el mapa conceptual presenta una visión simplificada del Round Robin, sus características y aplicaciones.

***Figura 6.*** *Mapa conceptual de Round Robin.*


*Nota.* Elaboración propia.

### 2.6.3. IP Hashing y persistencia

La técnica de IP Hashing utiliza funciones hash aplicadas a campos como las direcciones IP de origen y destino para determinar el enlace que se utilizará. Esta técnica resulta adecuada para mantener la coherencia de la ruta durante toda la sesión, lo cual es fundamental para aplicaciones como videollamadas, VoIP o juegos en línea.

Matemáticamente, se expresa como:

$$H = Hash(IP_{origen}, IP_{destino}) \quad (3)$$

$$Ei = (H \ mod \ N) + 1$$

donde:

$\boldsymbol{H}$: valor hash generado a partir de las direcciones IP.

$\boldsymbol{N}$: número de enlaces disponibles.

$\boldsymbol{Ei}$: enlace seleccionado.

Se genera un valor hash a partir de las direcciones IP involucradas y se aplica la operación módulo para determinar el enlace correspondiente.

Ejemplo:

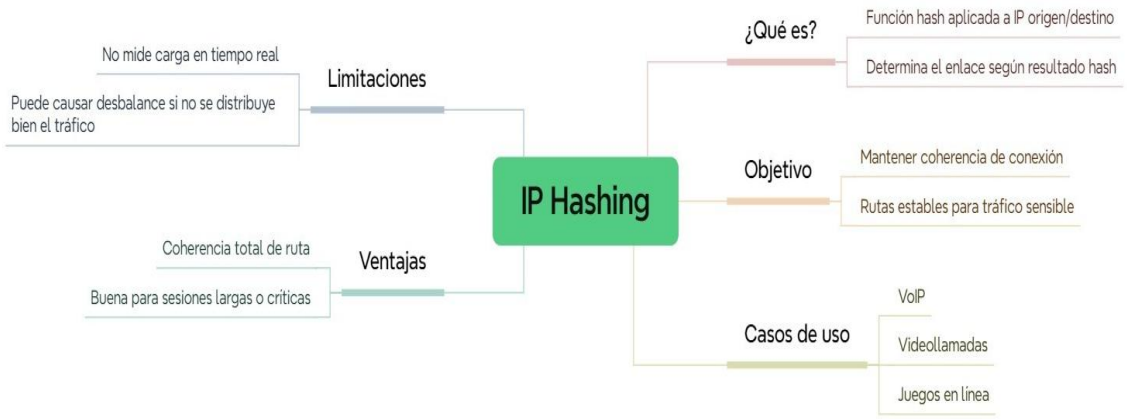
- **IP de origen**: 10.1.1.25
- **IP de destino**: 8.8.8.8
- **Valor hash simulado**: H = 12
- **Enlaces**: N = 4

$$Ei = (12 mod 4) + 1 = 0 + 1 = 1$$

La conexión se asigna al enlace 1.

La Figura 7 muestra de forma esquemática el funcionamiento del IP Hashing, lo que facilita su comprensión.

***Figura 7.*** *Mapa conceptual de IP Hashing.*




*Nota.* Elaboración propia.

### 2.6.4. Least Connections en entornos variables

Esta técnica asigna nuevas conexiones al enlace que tiene el menor número de sesiones activas en tiempo real. Es un enfoque dinámico adecuado para situaciones en las que los flujos de tráfico presentan un comportamiento variable.

En redes WISP con múltiples enlaces de distinta capacidad y carga, Least Connections puede constituir una estrategia efectiva. Su principal ventaja radica en que esta técnica es más adaptativa que Round Robin en la distribución del tráfico, aunque puede requerir dispositivos con mayor capacidad de procesamiento. La selección del enlace con menos conexiones activas se representa con la siguiente ecuación:

$$Ei = min\{C_1, C_2, \ldots . C_n\} \quad (4)$$

Donde:

$\boldsymbol{Ei}$ : enlace seleccionado.

$\boldsymbol{C_1}$: número de conexiones activas en el enlace.

**n**: número de enlaces disponibles.

Esta técnica se emplea consultando el número de conexiones activas de cada enlace y seleccionando aquel que presente la menor cantidad en ese instante, como se muestra en la Tabla 7

***Tabla 7.*** *Conexiones activas por enlace.*

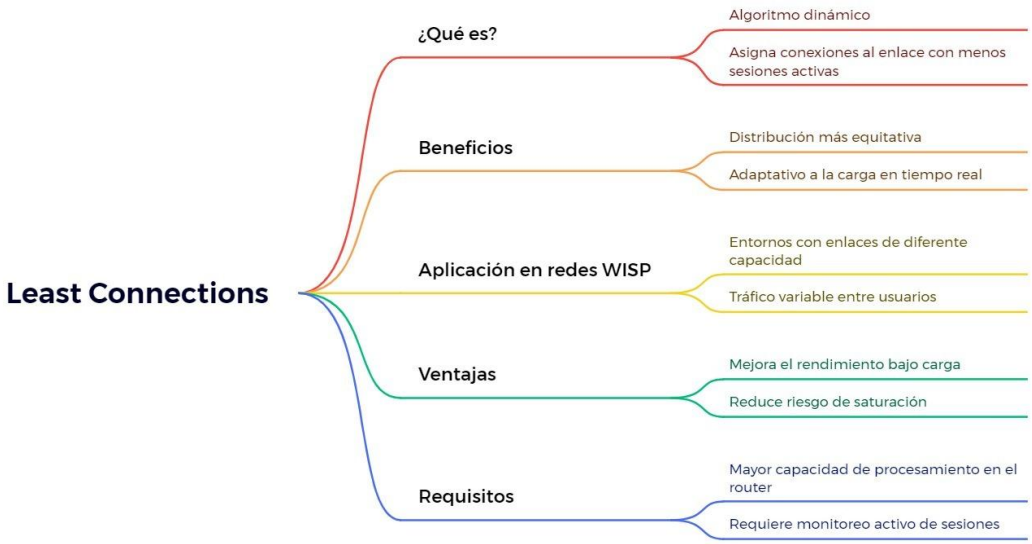
| Enlace | Conexiones activas |
|---|---|
| WAN1 | 20 |
| WAN2 | 15 |
| WAN3 | 18 |

*Nota.* Elaboración propia.

WAN2 es el enlace con el menor número de conexiones, con un total de 15 conexiones activas.

En la Figura 8 se presenta un mapa mental que facilita la comprensión de Least Connections, sus ventajas y sus aplicaciones.

***Figura 8.*** *Mapa mental de Least Connections.*




*Nota.* Elaboración propia.

## 2.7. Fundamentos matemáticos de técnicas de optimización del ancho de banda

Las técnicas de optimización del ancho de banda se sustentan en principios matemáticos que permiten administrar de manera eficiente los recursos disponibles en una red. Estas técnicas buscan priorizar el tráfico, reducir la congestión y mejorar el rendimiento de las comunicaciones.

### 2.7.1. QoS aplicada al tráfico priorizado

La calidad de servicio (QoS) permite clasificar, priorizar y controlar el tráfico de red de acuerdo con las necesidades de cada tipo de servicio. En redes WISP, esta gestión permite establecer diferentes niveles de prioridad y asignar el ancho de banda disponible entre las distintas clases de tráfico.

Para representar matemáticamente la proporción de ancho de banda asignada a cada clase de tráfico, se utiliza la siguiente expresión:

$$Pt = \frac{Wt}{\sum_{i=1}^{n} Wi} \quad (5)$$

donde:

**Pt**: proporción del ancho de banda asignada al tráfico de tipo t.

**Wt**: peso o prioridad del tráfico de tipo t.

**Wi:** peso de cada clase de tráfico.

**n**: número total de clases de tráfico.

En la Figura 9 se presenta de forma simplificada la calidad de servicio, sus aplicaciones y su fórmula.

***Figura 9.*** *Mapa conceptual de calidad de servicio (QoS).*


*Nota.* Elaboración propia.

### 2.7.2. Uso de colas HTB y Simple Queues

Las colas de tráfico son herramientas esenciales para limitar y garantizar el uso del ancho de banda. En MikroTik, las más utilizadas son las siguientes:

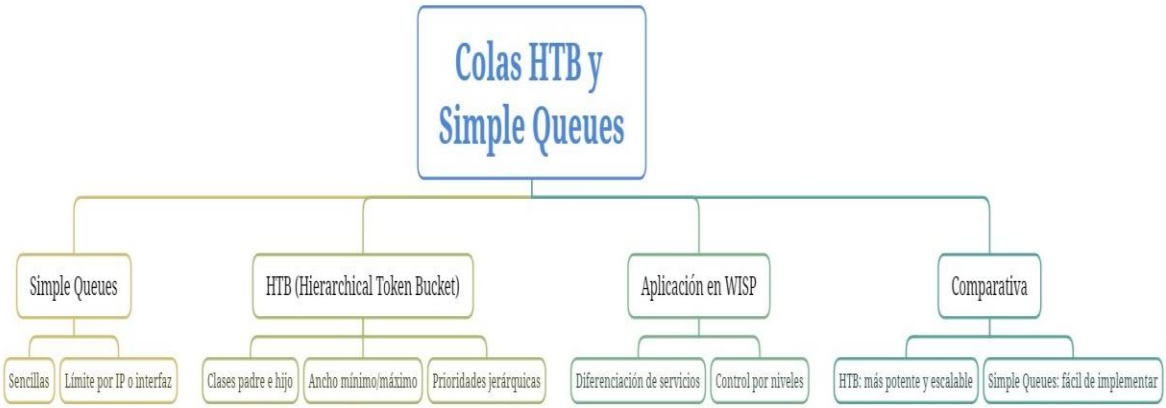
**Simple Queues**: se aplican por IP o interfaz. Son sencillas, pero menos escalables.

**HTB (Hierarchical Token Bucket)**: permite crear árboles de prioridad con clases padre e hijo, configurando valores mínimo y máximo de ancho de banda, así como una prioridad relativa.

HTB resulta adecuado para redes WISP que requieren ofrecer planes diferenciados o garantizar valores mínimos de ancho de banda para servicios críticos.

En la Figura 10 se muestra, mediante un mapa conceptual, la relación entre los elementos fundamentales del uso de colas HTB, lo que permite realizar un análisis más claro y organizado.

***Figura 10.*** *Mapa conceptual de colas HTB y Simple Queues.*




*Nota.* Elaboración propia.

### 2.7.3. Técnica Burst

La técnica Burst permite incrementar temporalmente la velocidad de transmisión de un usuario cuando se cumplen determinadas condiciones de consumo y existe capacidad disponible de red. En redes WISP, esta función puede utilizarse para mejorar el rendimiento percibido en actividades de corta duración, como la carga de páginas web o el inicio de una descarga.

Para representar los parámetros asociados al funcionamiento de la ráfaga, se utiliza la siguiente expresión matemática:

$$Tb = \frac{Blimit - Baverage}{Rburst - Rlimit} \qquad (6)$$

Donde:

**Tb**: tiempo máximo de la ráfaga.

**Blimit**: límite de datos de la ráfaga.

**Baverage**: consumo promedio de ancho de banda.

**Rburst**: velocidad máxima de la ráfaga.

**Rlimit**: velocidad normal asignada al usuario.

En la Figura 11 se presentan de forma simplificada los aspectos clave de la técnica Burst.

***Figura 11.*** *Mapa conceptual de Burst.*


*Nota.* Elaboración propia.

### 2.7.4. Mangle y Routing Marks

En redes WISP, la combinación de *Mangle* y *Routing Marks* permite clasificar el tráfico y asociarlo con rutas específicas según los criterios establecidos. De esta manera, los diferentes tipos de tráfico pueden distribuirse entre los enlaces WAN disponibles de acuerdo con sus requerimientos de servicio. Por ejemplo, el tráfico de VoIP puede dirigirse al enlace de menor latencia, el tráfico de streaming al enlace de mayor capacidad, y las actualizaciones o descargas, a un enlace secundario.

La asignación del tráfico a una ruta determinada puede representarse mediante la siguiente expresión:

$$L(t) = Rk \tag{7}$$

Donde:

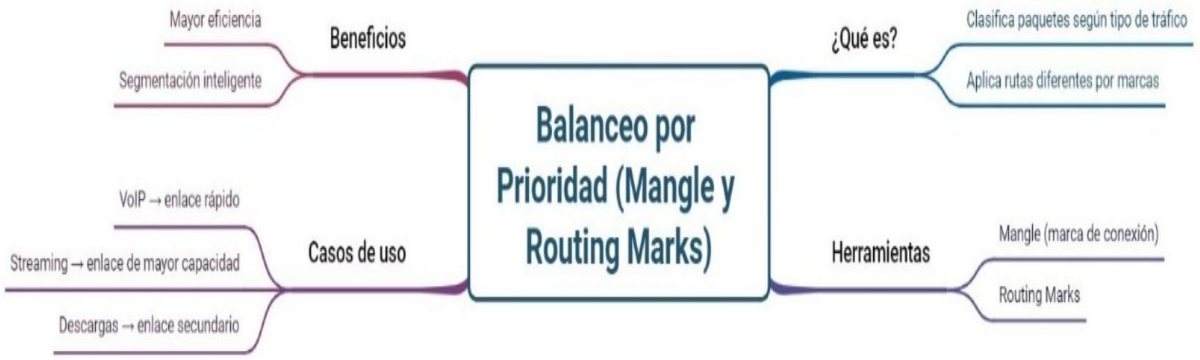
$\boldsymbol{L(t)}$: enlace WAN asignado al tráfico de tipo t.

$\boldsymbol{t}$: tipo o clase de tráfico.

$\boldsymbol{Rk}$: ruta o enlace WAN seleccionado mediante la marca de enrutamiento correspondiente.

La Figura 12 muestra de forma simplificada los beneficios y herramientas del balanceo por prioridad.

***Figura 12.*** *Mapa conceptual de balanceo por prioridad.*




*Nota.* Elaboración propia.

## 2.8. Estrategias para optimizar redes WISP

La optimización de una red WISP requiere la aplicación de estrategias que garanticen un funcionamiento estable y eficiente. Estas prácticas permiten mejorar la disponibilidad del servicio, minimizar las interrupciones y facilitar el crecimiento de la infraestructura. En este apartado se presentan las principales estrategias orientadas a fortalecer el rendimiento y la estabilidad de la red WISP.

### 2.8.1. Redundancia y respaldo de enlaces WISP

Las redes WISP deben estar preparadas para enfrentar fallos de conectividad o interrupciones en el servicio. Para ello, se implementan mecanismos de redundancia que aseguran

la continuidad del servicio ante eventos inesperados, como la caída de un proveedor de internet o la falla de un equipo.

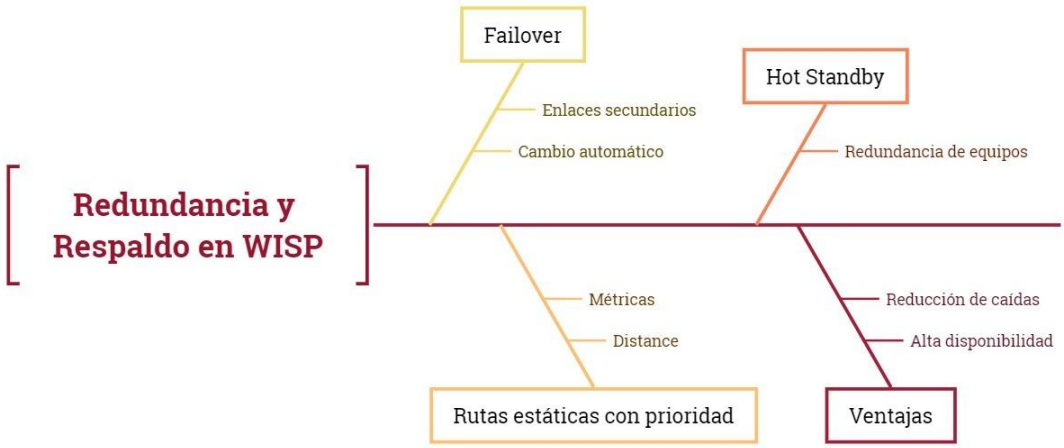
Entre las estrategias más comunes se encuentran:

- Failover entre enlaces WAN (cambio automático al respaldo).
- Rutas estáticas con prioridades (distancia o métrica).
- *Hot Standby* Routers y configuraciones dual WAN.

Estas técnicas permiten reducir el tiempo de inactividad y mantener la operatividad del sistema con mínima intervención humana.

En la Figura 13 se presentan, mediante un mapa conceptual, los principales aspectos relacionados con la redundancia y el respaldo en redes WISP.

***Figura 13.*** *Mapa conceptual de redundancia y respaldo.*




*Nota.* Elaboración propia.

### 2.8.2. Gestión del espectro e interferencias

Las redes WISP operan en su mayoría en el espectro libre (2,4 GHz y 5 GHz), el cual es compartido por múltiples dispositivos y redes. Esto hace que sean susceptibles a interferencias, lo que puede afectar la estabilidad y la velocidad del enlace. Para minimizar las interferencias, se aplican prácticas como el análisis de espectro para seleccionar los canales menos congestionados, el ajuste de potencias de transmisión, el uso de antenas sectoriales o direccionales y la separación física y lógica de frecuencias. Estas estrategias permiten mantener la calidad de la transmisión, mejorar la cobertura y reducir las colisiones.

En la Figura 14 se muestra de forma clara la relación entre los conceptos principales de la gestión del espectro en redes WISP.

***Figura 14.*** *Mapa conceptual de gestión del espectro en WISP.*


*Nota.* Elaboración propia.

### 2.8.3. Diseño escalable de redes WISP

Un diseño escalable garantiza que una red pueda crecer sin comprometer su rendimiento. En redes WISP, esto implica estructurar la red en capas jerárquicas, donde cada segmento cumple una función específica.

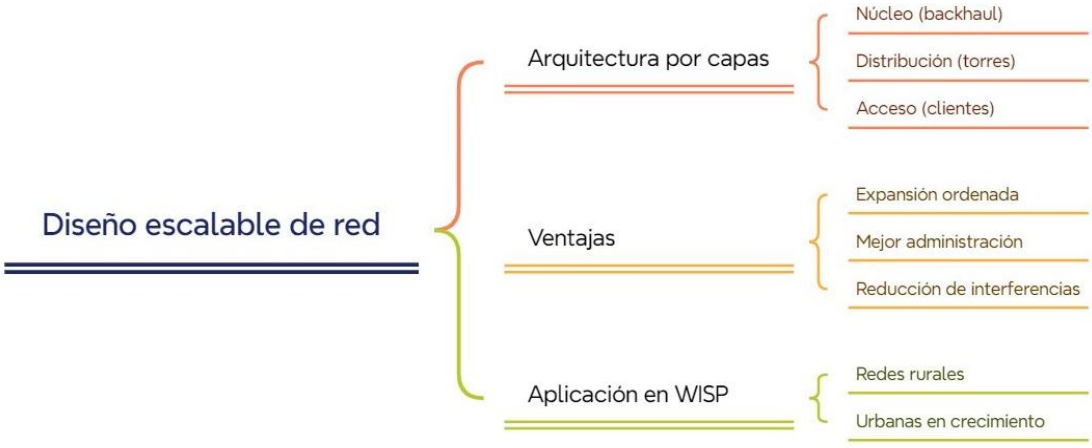
**Modelo de red jerárquica**

- Capa de núcleo: enlaces de backhaul o backbone.
- Capa de distribución: enlaces entre torres y repetidores.
- Capa de acceso: conexión final a los clientes.

Este diseño permite balancear mejor el tráfico, simplificar la administración y facilitar la expansión futura sin rediseñar toda la red.

En la Figura 15 se presenta de forma simplificada el diseño escalable de una red, entendido como la capacidad de esta para crecer y adaptarse a nuevas demandas sin perder rendimiento, estabilidad ni seguridad.

***Figura 15.*** *Mapa conceptual de diseño escalable de la red.*




*Nota.* Elaboración propia.

### 2.8.4. Administración y monitoreo preventivo

Una red WISP no solo debe estar bien configurada, sino también bien administrada y monitoreada. La implementación de políticas preventivas reduce el tiempo de respuesta ante fallos, mejora la experiencia del usuario y optimiza los recursos.

Las buenas prácticas incluyen:

- Monitoreo proactivo con alertas y registros.
- Control de usuarios y conexiones simultáneas.
- Respaldos periódicos de configuraciones.
- Auditorías internas de rendimiento y seguridad.

Una gestión eficiente evita que pequeños errores se conviertan en fallos críticos. A continuación, en la Figura 16 se presentan de forma concreta los principales aspectos de la administración y el monitoreo, entendidos como el conjunto de procesos, herramientas y prácticas utilizadas para supervisar, analizar y gestionar el rendimiento, la disponibilidad y la seguridad de los recursos de red.

***Figura 16.*** *Mapa conceptual de administración y monitoreo.*


*Nota.* Elaboración propia.

## 2.9. Métodos de segmentación y aislamiento de red

En el diseño y gestión de infraestructuras WISP, la segmentación de red es una estrategia fundamental que permite dividir la red en dominios lógicos o virtuales, lo que mejora la seguridad, el control del tráfico y la eficiencia operativa. Mediante distintas tecnologías, se pueden aislar grupos de usuarios, servicios o flujos de datos, lo que permite aplicar políticas específicas según los requerimientos del proveedor o del cliente. En este apartado se describen las tecnologías VLAN y VPN, y su aplicación en entornos WISP.

### 2.9.1. VLAN (Virtual Local Area Network)

La tecnología VLAN es una solución que permite dividir una red física en diferentes dominios lógicos de *broadcast*. Opera en la capa 2 del modelo OSI y está basada en el estándar IEEE 802.1Q, que incluye un identificador de VLAN en la cabecera de la trama Ethernet. Esta técnica permite aislar el tráfico entre diferentes grupos de usuarios o servicios sin necesidad de infraestructura física adicional. Cada VLAN actúa como una subred lógica independiente, lo que permite aplicar políticas diferenciadas de calidad de servicio (QoS), seguridad y gestión. En un

entorno WISP, las VLAN se utilizan para separar el tráfico de los clientes del tráfico de gestión, lo que favorece una administración eficiente y una mayor protección de la red.

### 2.9.2. VPN (Virtual Private Network)

Una VPN establece un túnel cifrado entre dos o más puntos en una red pública, como internet. Trabaja desde la capa 3 (red) hasta la capa 5 (sesión) del modelo OSI, dependiendo del protocolo empleado (IPsec, SSL/TLS o OpenVPN). Su objetivo principal es garantizar la confidencialidad, la integridad y la autenticación del tráfico transmitido. En una red WISP, las VPN permiten que sitios remotos, repetidoras o clientes privilegiados se conecten de forma segura, incluso a través de redes no confiables. El encapsulamiento del tráfico y el cifrado hacen de esta tecnología un elemento esencial para preservar la privacidad de los datos y mantener la seguridad de la infraestructura.

# Capítulo 3. Desarrollo de la propuesta

## 3.1. Descripción general del sistema

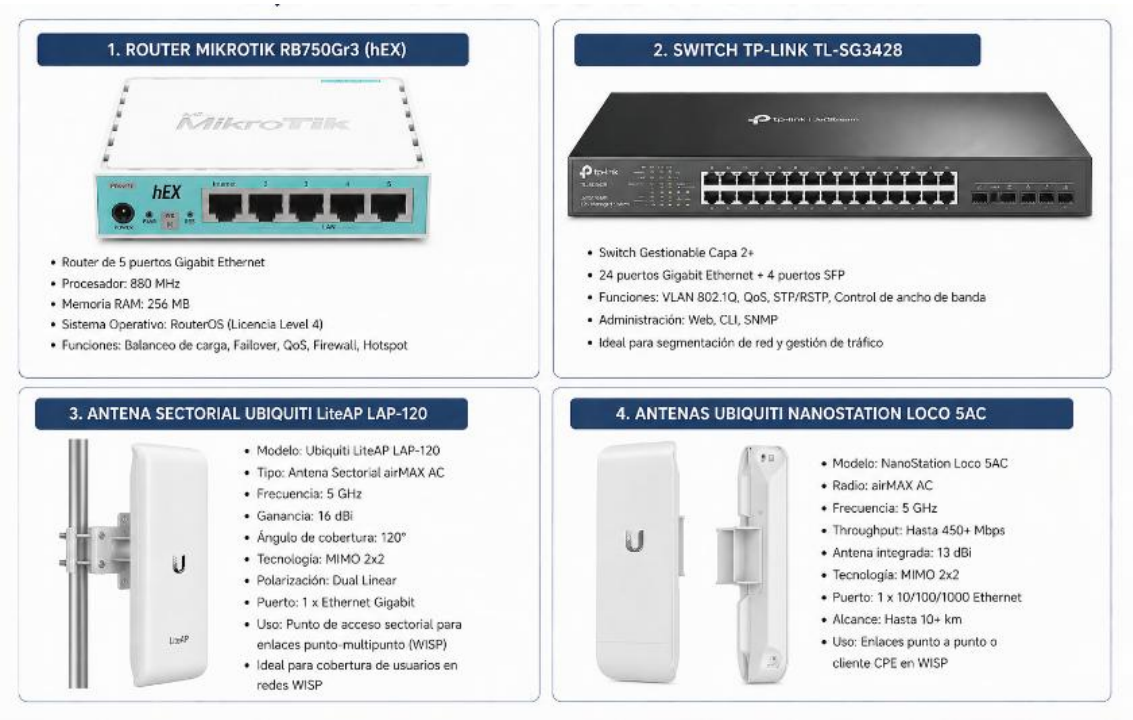
El presente proyecto propone el diseño e implementación de una red basada en tecnología WISP, orientada a la optimización del ancho de banda y la mejora del rendimiento del servicio mediante técnicas de balanceo de carga, segmentación de red y calidad de servicio (QoS). El sistema se desarrolla en un entorno de laboratorio que simula condiciones reales de operación, lo que permite analizar el comportamiento de la red ante distintos escenarios de tráfico y demanda de los usuarios. La arquitectura está conformada por un router principal MikroTik RB750Gr3 hEX, un switch gestionable TP-Link TL-SG3428 y dispositivos de acceso inalámbrico, los cuales trabajan de forma conjunta para garantizar la conectividad y la gestión eficiente del tráfico.

La red se segmenta mediante cuatro VLAN: una VLAN de administración y tres VLAN destinadas a los servicios empresarial, VIP y estándar. Para optimizar el rendimiento, se implementan técnicas de balanceo de carga que permiten distribuir el tráfico entre múltiples enlaces de salida a internet, lo que reduce la congestión y mejora la disponibilidad. Asimismo, se aplican políticas de QoS para priorizar el tráfico crítico y controlar el consumo de ancho de banda, lo que contribuye a mejorar indicadores como la latencia y la pérdida de paquetes.

### 3.1.1. Selección y justificación de equipos

Para la implementación del sistema WISP propuesto, se seleccionaron dispositivos de red que ofrecen un equilibrio entre rendimiento, funcionalidad y costo. A continuación, se describen los equipos utilizados, sus principales características y la justificación de su elección dentro del diseño de la red. La Figura 17 recoge el conjunto de equipos empleados.

***Figura 17.*** *Equipos utilizados en la implementación de la red WISP.*




*Nota.* Elaboración propia.

### 3.1.2. Router principal

El sistema emplea un router MikroTik RB750Gr3 hEX como dispositivo principal, el cual funciona bajo el sistema operativo RouterOS, ampliamente utilizado en entornos de redes profesionales. Este equipo dispone de cinco puertos Ethernet Gigabit y admite múltiples conexiones simultáneas, lo que permite gestionar el tráfico de forma eficiente. El router cumple un rol fundamental dentro de la red, ya que se encarga del enrutamiento del tráfico, la implementación del balanceo de carga y la aplicación de políticas de control del ancho de banda.

La elección de este equipo se fundamenta en su capacidad para implementar diversas técnicas de balanceo de carga y optimizar el uso del ancho de banda, características que lo convierten en una solución adecuada para entornos WISP que requieren estabilidad y rendimiento. En la Tabla 8 se presentan las especificaciones técnicas del router principal.

***Tabla 8.*** *Especificaciones técnicas del router principal MikroTik RB750Gr3 hEX.*

| **Parámetro** | **Valor** | **Aplicación en el proyecto** |
|---|---|---|
| CPU | 880 MHz (Dual Core) | Permite procesar reglas de balanceo |
| RAM | 256 MB | Soporta múltiples conexiones simultáneas |
| Puertos | 5 puertos Gigabit Ethernet | Permite la conexión de múltiples enlaces WAN y LAN |
| Sistema operativo | RouterOS | Permite la configuración de balanceo de carga, VLAN y QoS |
| NAT | Compatible | Permite la salida a internet de múltiples usuarios |
| Capacidad de conexiones | Alta | Gestión de tráfico en entornos WISP |

*Nota.* Elaboración propia.

### 3.1.3. Asignación de puertos en el router

La implementación del balanceo de carga se realiza mediante la técnica PCC (Per Connection Classifier) configurada en el router MikroTik. El tráfico de los usuarios ingresa al router a través de la interfaz LAN conectada al switch gestionable. Previamente, el tráfico es segmentado mediante VLAN y, posteriormente, el router procesa las conexiones a través de reglas de Mangle para clasificarlas y distribuirlas entre los enlaces WAN disponibles.

Los puertos Ethernet 1 y Ethernet 5 se configuran como enlaces WAN para la salida a internet y participan en el esquema de balanceo de carga PCC. Por otro lado, el puerto Ethernet 3 se utiliza como enlace troncal (*trunk*) hacia el switch, lo que permite la comunicación con las VLAN implementadas en la red. En la Tabla 9 se detalla la asignación de puertos del router principal.

***Tabla 9.*** *Asignación de puertos.*

| Puerto | Tipo de interfaz | Función de red | Descripción |
|---|---|---|---|
| Ethernet 1 | WAN | Enlace de internet 1 | Participa en el balanceo PCC como enlace de salida a internet |
| Ethernet 2 | Libre | Futura expansión | Disponible para futuras configuraciones o pruebas |
| Ethernet 3 | LAN | Conexión al switch | Recibe tráfico segmentado |
| Ethernet 4 | Libre | Futura expansión | Disponible para futuras configuraciones o pruebas |
| Ethernet 5 | WAN | Enlace de internet 2 | Participa en el balanceo PCC como enlace de salida a internet |

*Nota.* Elaboración propia.

### 3.1.4. Switch de distribución

Para la capa de distribución, se emplea un switch gestionable TP-Link diseñado para operar en capa 2 con funciones de capa 3 (L2+) del modelo OSI. Este dispositivo permite gestionar el tráfico mediante segmentación lógica y ofrece una alta capacidad de interconexión gracias a sus múltiples puertos Gigabit y al soporte de enlaces de fibra. Su función principal dentro del sistema es organizar y segmentar el tráfico mediante VLAN, lo que permite separar los usuarios en diferentes grupos: empresarial, VIP y estándar. Esto evita la mezcla de datos, mejora la seguridad y permite aplicar políticas diferenciadas.

El switch también gestiona los puertos en modo *trunk* y *access*, lo que permite transportar múltiples VLAN hacia el router a través del enlace. De esta forma, el tráfico llega correctamente organizado para su posterior procesamiento. La implementación de estas funciones en la capa de distribución permite optimizar el rendimiento del sistema, ya que el switch se encarga de la segmentación, mientras que el router se enfoca en tareas más avanzadas como el balanceo de carga y el control del tráfico. En la Tabla 10 se presentan las especificaciones técnicas del switch de distribución.

***Tabla 10.*** *Especificaciones técnicas del switch de distribución TP-Link TL-SG3428.*

| **Parámetro** | **Valor** | **Aplicación en el proyecto** |
|---|---|---|
| Puertos | 24 Gigabit + SFP | Conexión de múltiples dispositivos |
| Capa | L2+ | Segmentación mediante VLAN |
| VLAN | 802.1Q | Separación de usuarios |
| LACP | Compatible | Permite agregación de enlaces |
| QoS | Básico | Priorización inicial del tráfico |
| Capacidad de conmutación | Alta | Gestión eficiente del tráfico |

*Nota.* Elaboración propia.

### 3.1.5. Dispositivos de acceso inalámbrico

En este proyecto, la capa de acceso está formada por dispositivos inalámbricos encargados de establecer la comunicación entre la red y los usuarios finales. Para ello, se utilizan equipos CPE Ubiquiti NanoStation Loco5AC y una antena sectorial que funciona como punto de acceso principal. Estos equipos permiten transmitir y recibir datos a través de enlaces inalámbricos en la banda de 5 GHz, que ofrece ventajas en términos de velocidad y menor interferencia respecto de otras bandas de frecuencia.

El sistema se basa en una arquitectura punto a multipunto, donde una antena sectorial configurada en modo access point actúa como nodo central, mientras que los equipos CPE instalados en las ubicaciones de los usuarios operan en modo station.

#### Configuración y operación

La configuración de los dispositivos inalámbricos incluye aspectos fundamentales, como la definición del SSID, la selección del canal de operación, el ancho de banda del canal (20, 40 u 80 MHz) y el mecanismo de seguridad. Estos elementos aseguran una correcta comunicación entre

el punto de acceso y los clientes, así como la protección de la red. El tráfico generado por los usuarios es transmitido desde los CPE hacia la antena sectorial y, posteriormente, enviado al switch de distribución, donde es segmentado mediante VLAN antes de ser procesado por el router principal.

A continuación, en la Tabla 11 se presentan las principales especificaciones técnicas de los dispositivos de acceso inalámbrico utilizados en el sistema y su aplicación dentro de la arquitectura propuesta.

***Tabla 11.*** *Especificaciones técnicas de las antenas Ubiquiti NanoStation.*

| **Parámetro** | **Valor** | **Aplicación en el proyecto** |
|---|---|---|
| Frecuencia | 5 GHz | Menor interferencia y mayor velocidad |
| Ganancia | 13 dBi | Mayor alcance y mejor direccionamiento |
| Tecnología | AirMax AC | Eficiencia en enlaces punto-multipunto |
| MIMO | 2 × 2 | Incrementa la capacidad de transmisión de datos |
| Velocidad | Hasta 450 Mbps | Soporta tráfico de múltiples usuarios |
| Interfaz de red | Ethernet Gigabit | Conexión directa al switch |
| Modo de operación | Station (cliente) | Permite la conexión de los usuarios |
| Alimentación | PoE | Facilita la instalación en exteriores |
| Sistema operativo | AirOS | Configuración y monitoreo del enlace |

*Nota.* Elaboración propia.

### 3.2. Diseño de la red

La red propuesta está diseñada con una topología en estrella extendida, que se caracteriza por centralizar la gestión del tráfico en un dispositivo principal. Esta topología es adecuada para entornos WISP, ya que permite una mayor organización, control y escalabilidad de la red.

En este caso, el router principal MikroTik RB750Gr3 hEX es el nodo central de la red y cumple el rol de administrador. Toda la información generada por los usuarios se dirige a este dispositivo, lo que permite aplicar de manera eficiente políticas de enrutamiento, balanceo de carga y control de ancho de banda. Esta centralización permite gestionar el tráfico con mayor rapidez y utilizar de manera más eficiente los recursos disponibles. La elección de una topología en estrella extendida se justifica porque permite que los dispositivos intermedios, como el switch de distribución, organicen el tráfico antes de enviarlo al router, lo que contribuye a evitar la congestión y mejorar el rendimiento general del sistema. Además, este tipo de topología permite la implementación de técnicas como VLAN, QoS y balanceo de carga, las cuales requieren un punto de control centralizado.

En líneas generales, el flujo de comunicación comienza en los usuarios finales, pasa por los dispositivos de acceso inalámbrico, continúa hacia el switch de distribución y, finalmente, llega al router principal, donde se ejecutan las funciones críticas de gestión del tráfico.

El diseño se estructura en tres niveles funcionales:

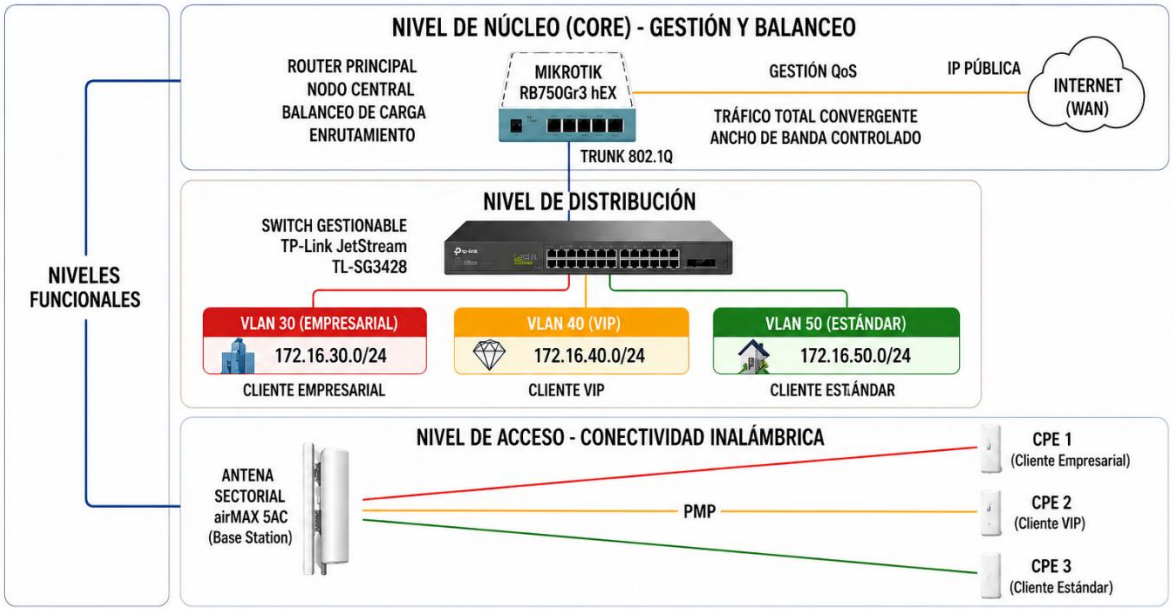
**Nivel de acceso:** dispositivos inalámbricos, como la antena sectorial y los equipos del cliente, encargados de proporcionar conectividad a los usuarios.

**Nivel de distribución:** switch gestionable TP-Link TL-SG3428 JetStream, cuya función es segmentar el tráfico mediante VLAN y clasificar a los usuarios en diferentes grupos (empresarial, VIP y estándar).

**Nivel de núcleo:** router principal, encargado de procesar el tráfico, aplicar el balanceo de carga y gestionar el acceso a internet.

En la Figura 18 se muestran los niveles funcionales de la topología de la red WISP.

***Figura 18.*** *Niveles de funcionalidad.*




*Nota.* Elaboración propia.

### 3.2.1. Segmentación de red

La segmentación de red constituye un elemento fundamental dentro del diseño del sistema propuesto, ya que permite organizar el tráfico de los usuarios, mejorar la seguridad y optimizar el uso del ancho de banda. La segmentación se realiza mediante el uso de redes virtuales locales

(VLAN), las cuales permiten separar lógicamente el tráfico dentro de una misma infraestructura física.

### Descripción de las VLAN

La segmentación de la red mediante VLAN se implementa con el objetivo de separar el tráfico de los usuarios en diferentes grupos, lo que permite aplicar políticas específicas de control del ancho de banda y prioridades. Esta estrategia mejora la organización del tráfico, reduce la congestión y optimiza el rendimiento general del sistema.

En el presente proyecto se definen tres VLAN principales: usuarios empresariales, usuarios VIP y usuarios estándar. Cada una responde a distintas necesidades y servicios, por lo que se le asignan políticas específicas.

### VLAN 10 – Administración

Esta VLAN está destinada a la gestión de los equipos de infraestructura de la red, como routers, switch, antenas y radios inalámbricos, por lo que requiere un acceso controlado y un nivel adecuado de seguridad para evitar acceso no autorizado. A esta VLAN se le asigna una prioridad alta, con el fin de garantizar una administración estable de los dispositivos y facilitar las tareas de configuración, monitoreo y mantenimiento de la red.

### VLAN 30 – Usuarios empresariales

Esta VLAN está destinada a usuarios con un consumo moderado de recursos, como navegación, uso de aplicaciones en la nube y servicios administrativos, por lo que requiere un equilibrio entre rendimiento y uso eficiente del ancho de banda. A esta VLAN se le asigna una prioridad media con el fin de garantizar un servicio estable sin afectar a los usuarios VIP.

**VLAN 40 – Usuarios VIP**

Esta VLAN está destinada a usuarios que requieren un servicio de alta calidad, como aplicaciones críticas, videoconferencias o servicios empresariales sensibles a la latencia. Se busca garantizar la estabilidad, la baja latencia y la alta disponibilidad del servicio. Se le asigna una cola de alta prioridad para asegurar que este tráfico sea atendido antes que el tráfico de menor prioridad en situaciones de congestión.

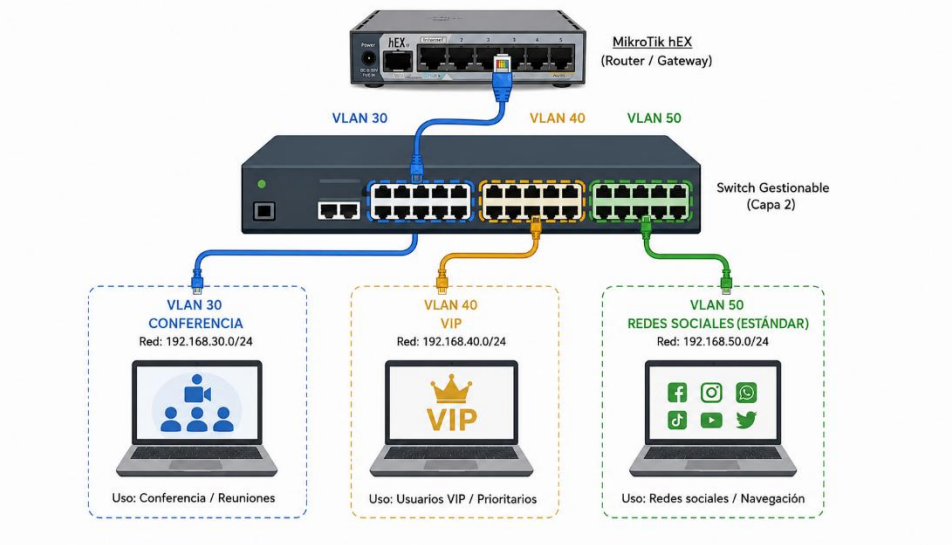
**VLAN 50 – Usuarios estándar**

Esta VLAN está destinada a usuarios de menor prioridad que realizan actividades como el acceso general a internet o uso recreativo, con el fin de optimizar el ancho de banda sin impactar en los servicios críticos. Se le asigna una cola de baja prioridad para limitar el ancho de banda en caso de congestión.

La implementación de VLAN permite no solo segmentar el tráfico, sino también aplicar políticas diferenciadas de calidad de servicio (QoS) y balanceo de carga, lo que contribuye a una gestión eficiente de los recursos de red y a una mejor experiencia del usuario según el tipo de servicio.

La Figura 19 muestra la representación gráfica de la segmentación lógica de la red mediante VLAN y la forma en que el switch gestionable divide una misma infraestructura física en diferentes redes virtuales.

***Figura 19.*** *Implementación de VLAN.*




*Nota.* Elaboración propia.

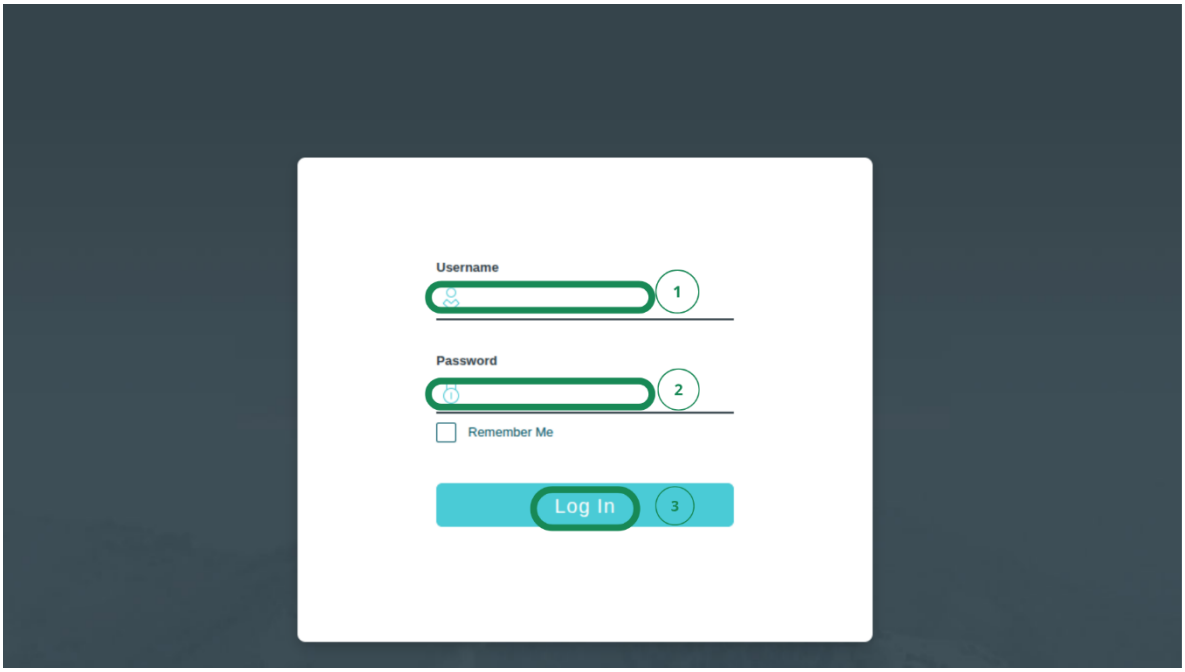
### 3.3. Configuración de los equipos

La configuración de las VLAN en el switch gestionable se realiza mediante su interfaz web, lo que permite definir redes lógicas independientes dentro de una misma infraestructura física.

#### 3.3.1. Creación de VLAN en el switch

En primer lugar, se accede a la interfaz web del switch mediante la dirección IP asignada y se procede a crear las VLAN correspondientes al sistema.

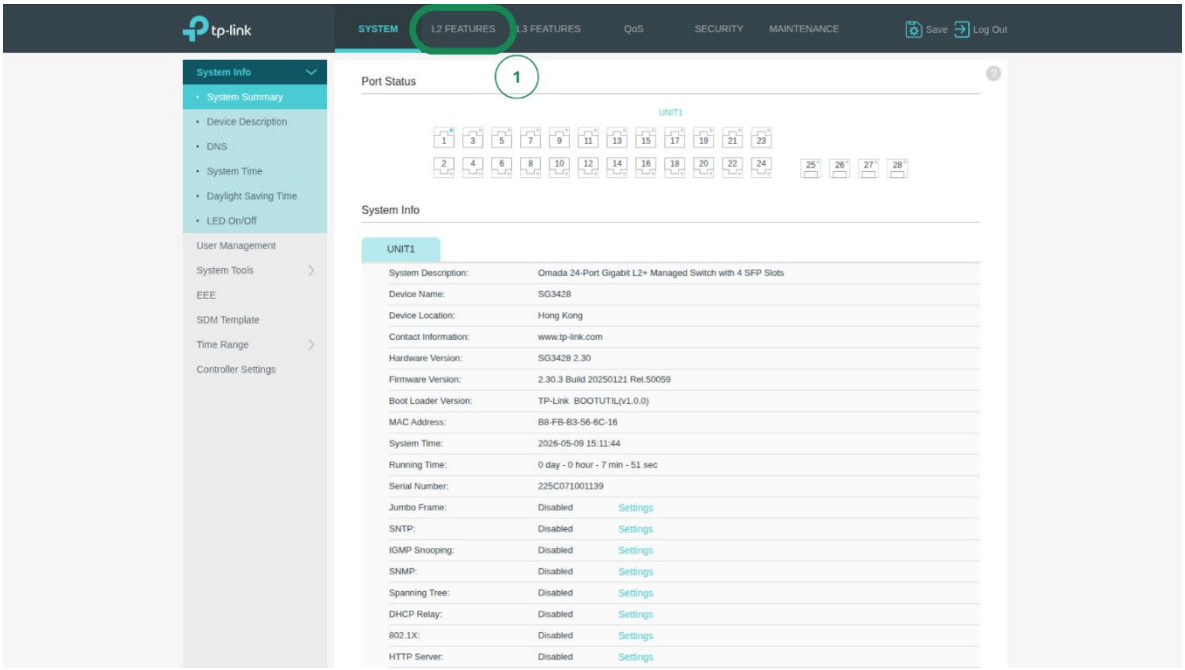
***Figura 20.*** *Usuario y contraseña del switch.*




*Nota.* Elaboración propia.

En la Figura 20 se muestra la configuración de un usuario y una nueva contraseña, ya que el equipo no tenía credenciales configuradas. En este caso, se configuró admin como usuario y Wisp2026 como contraseña para acceder al switch.

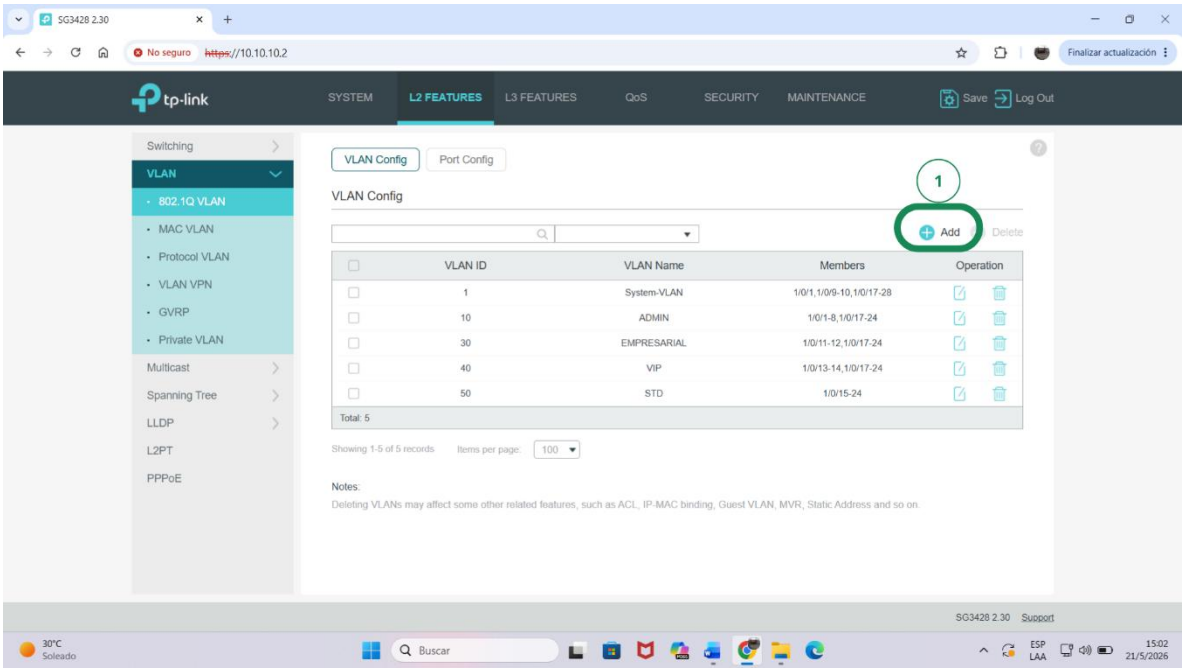
***Figura 21.*** *Interfaz gráfica web.*




*Nota.* Elaboración propia.

La Figura 21 muestra la interfaz gráfica web del switch. En el menú principal se selecciona la opción L2 Features.

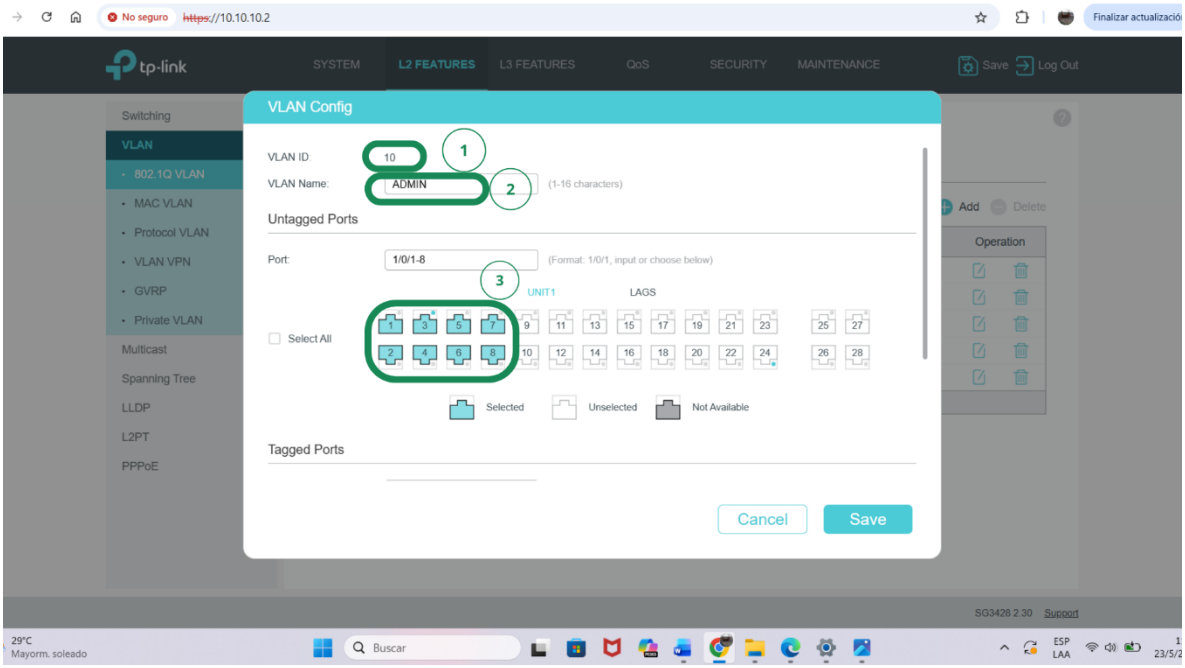
***Figura 22.*** *Apartado VLAN.*




*Nota.* Elaboración propia.

En la Figura 22 se muestra la ventana en la que se encuentra el apartado de VLAN, desde el cual se realiza la creación de cada VLAN mediante la opción Add.

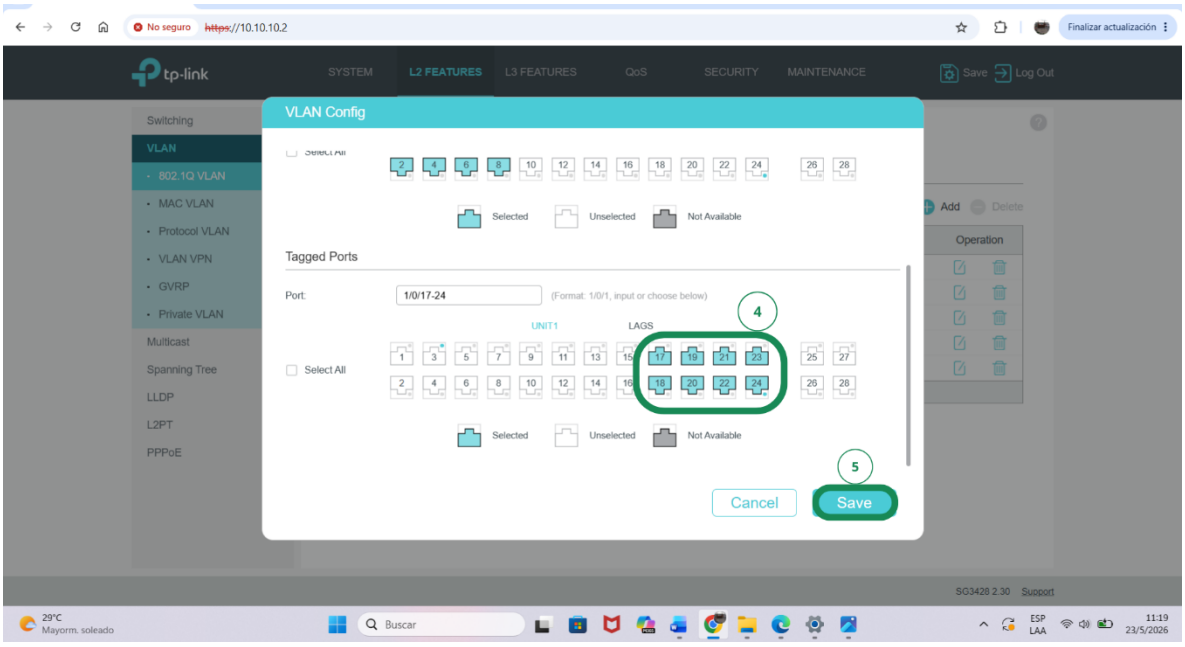
***Figura 23.*** *VLAN 10.*




*Nota.* Elaboración propia.

En la Figura 23 se observa la ventana VLAN Config, en la que se creó la primera VLAN, correspondiente a la VLAN 10 de administración. En el campo VLAN ID se asignó el identificador 10 y, en VLAN Name, el nombre ADMIN; posteriormente, se seleccionaron los puertos 1 al 8 como pertenecientes a esta VLAN.

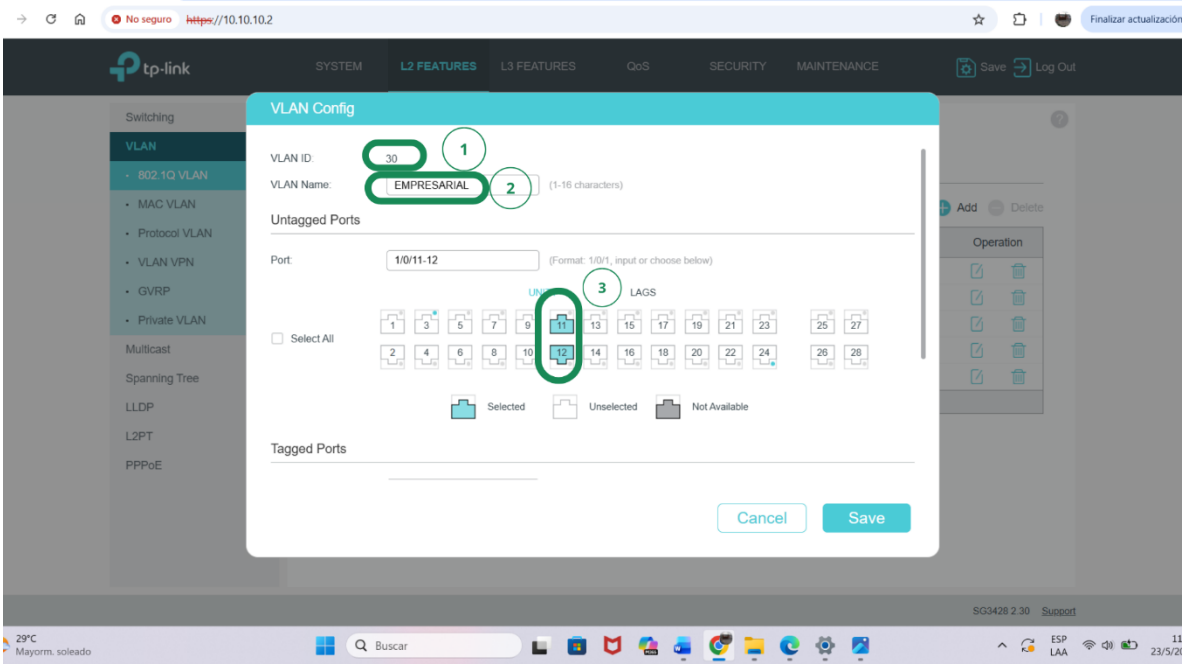
***Figura 24.*** *Selección de puertos troncales.*




*Nota.* Elaboración propia.

En la Figura 24 se presenta el apartado de selección de los puertos troncales, asignados en este caso del 17 al 24. Finalmente, se guarda la configuración mediante la opción Save.

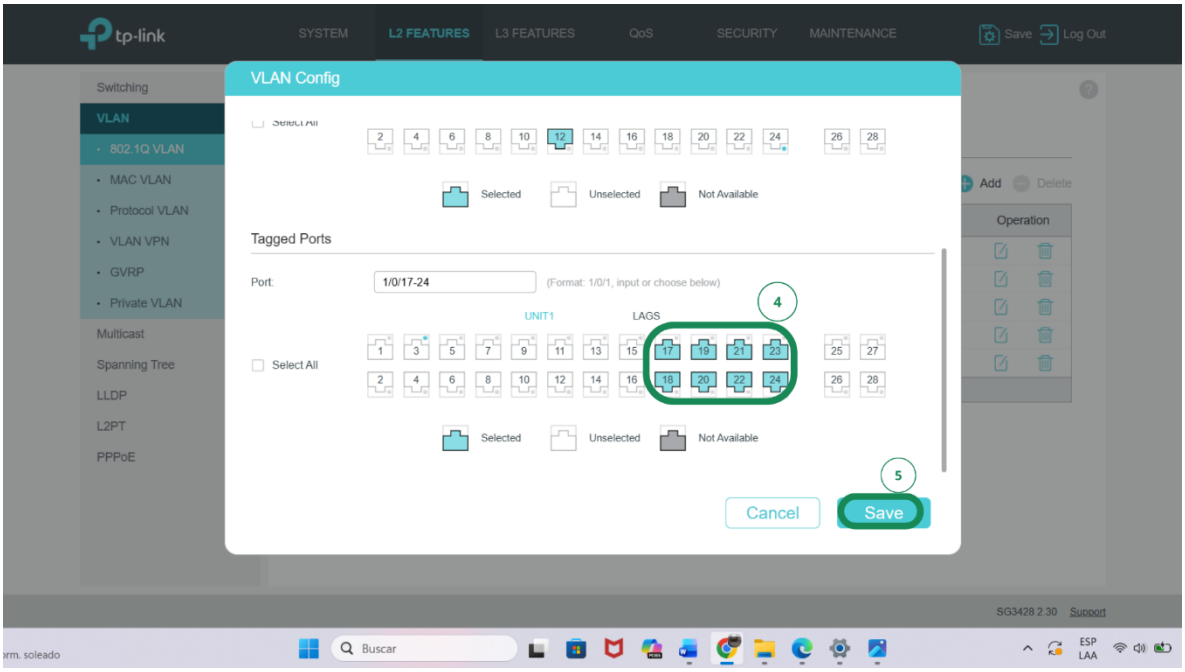
***Figura 25.*** *VLAN 30.*




*Nota.* Elaboración propia.

La Figura 25 muestra la creación de la VLAN 30, destinada al servicio empresarial. En el campo VLAN ID se configuró el identificador 30 y, en VLAN Name, el nombre empresarial; posteriormente, se seleccionaron los puertos 11 y 12 como pertenecientes a esta VLAN.

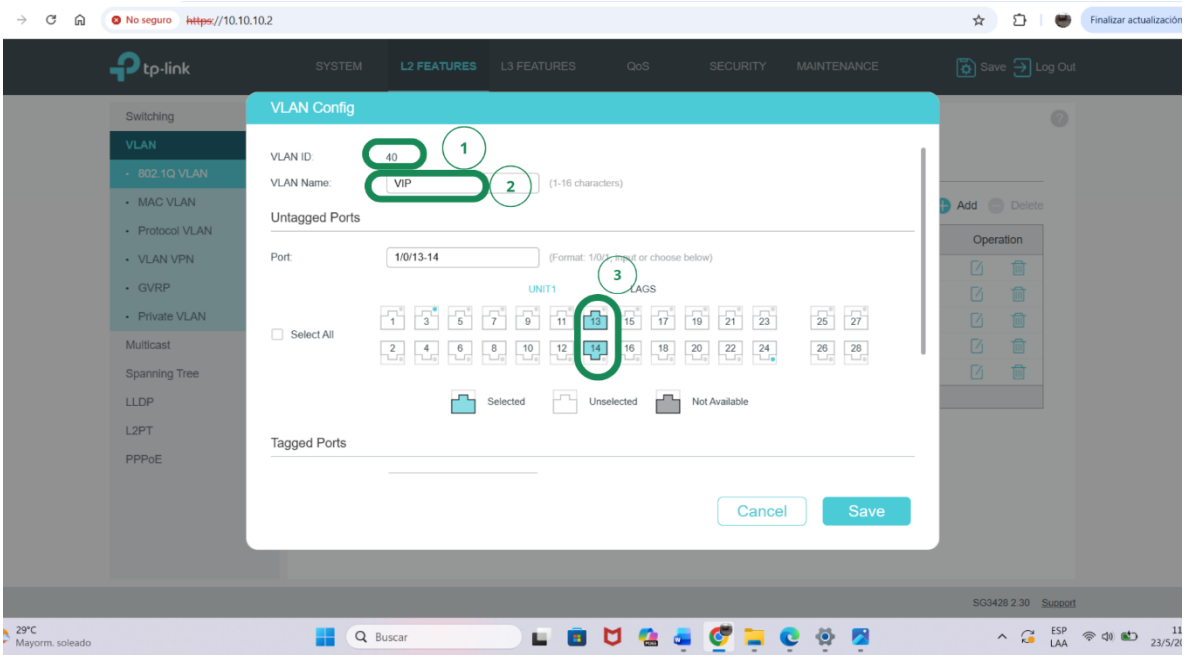
***Figura 26.*** *Selección de puertos troncales de VLAN 30.*




*Nota.* Elaboración propia.

La Figura 26 muestra los puertos troncales asignados a la VLAN empresarial, correspondientes a los puertos del 17 al 24; la configuración se guarda mediante la opción Save.

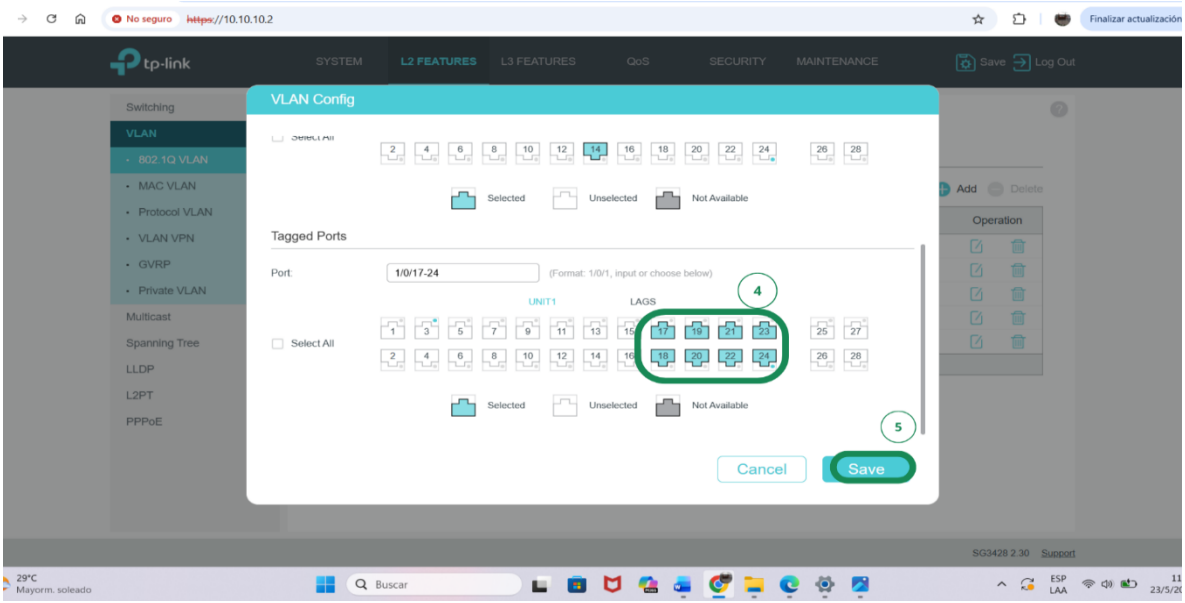
***Figura 27.*** *VLAN 40.*




*Nota.* Elaboración propia.

La Figura 27 muestra la creación de la VLAN 40, destinada al servicio VIP. En el campo VLAN ID se configuró el identificador 40 y, en VLAN Name, el nombre VIP; posteriormente, se seleccionaron los puertos 13 y 14 como pertenecientes a esta VLAN.

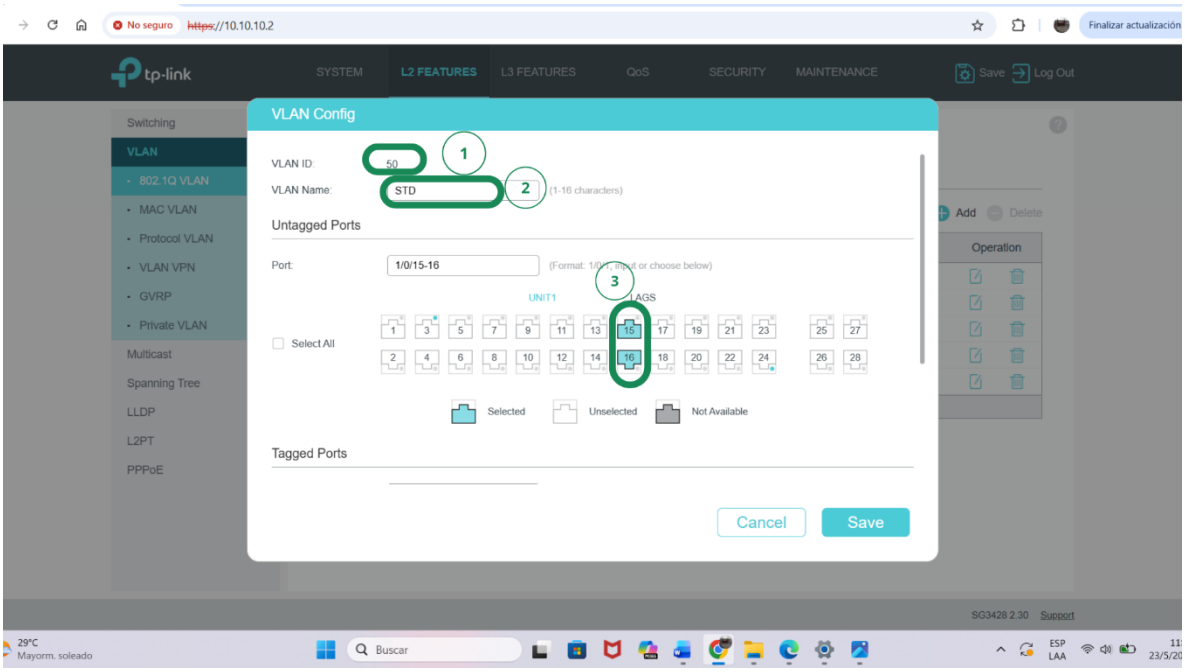
***Figura 28.*** *Selección de puertos troncales de VLAN 40.*




*Nota.* Elaboración propia.

En la Figura 28 se seleccionaron los puertos troncales de esta VLAN, correspondientes a los puertos del 17 al 24, y se guardó la configuración mediante la opción Save.

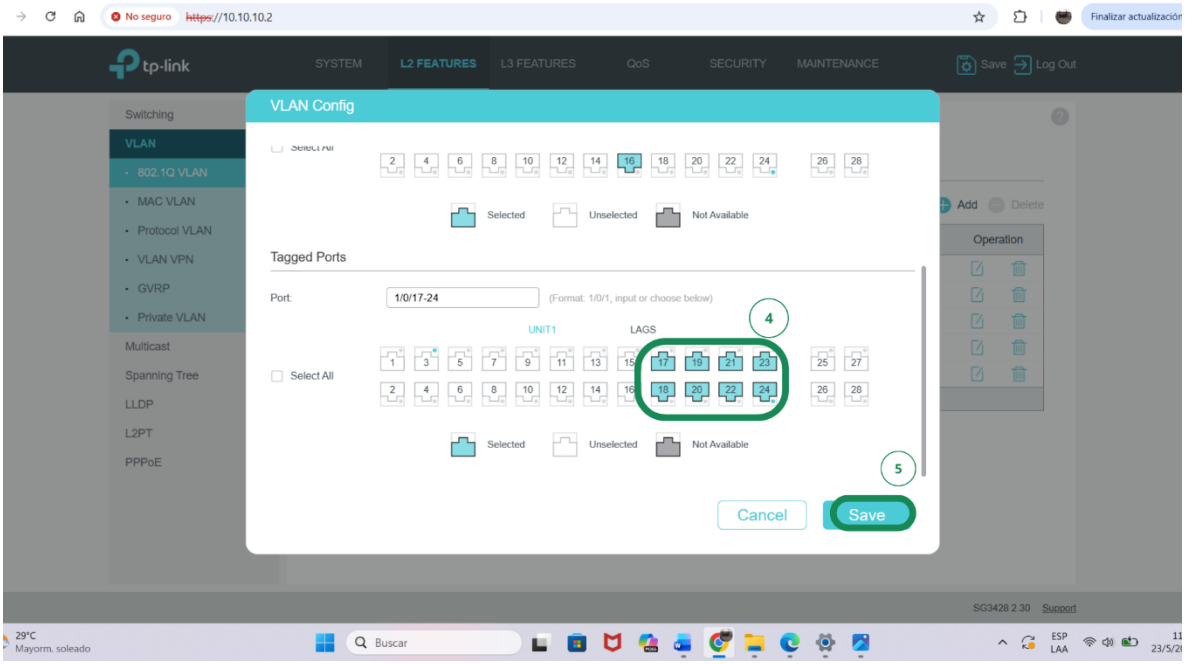
***Figura 29.*** *VLAN 50.*




*Nota.* Elaboración propia.

La Figura 29 muestra la creación de la VLAN 50, destinada a los usuarios estándar. Se configuró el identificador 50 y el nombre STD y, posteriormente, se seleccionaron los puertos 15 y 16 como pertenecientes a dicha VLAN.

**Figura 30.** *Selección de puertos troncales de VLAN 50.*




*Nota.* Elaboración propia.

En la Figura 30 se seleccionaron los puertos troncales de esta VLAN, correspondientes a los puertos del 17 al 24. Finalmente, se guardó la configuración mediante la opción Save. De esta manera, se completó la creación de todas las VLAN sobre las que opera el sistema.

Esta configuración es esencial para transportar el tráfico etiquetado hacia el router, donde se aplicarán las políticas de enrutamiento, balanceo de carga y QoS. Una vez implementadas las VLAN, el switch se encarga de identificar el tráfico según el puerto de entrada y asignarlo a la VLAN correspondiente. Posteriormente, este tráfico se envía al router a través del enlace trunk y conserva el etiquetado 802.1Q. Esta implementación permite separar los diferentes tipos de usuarios en la red, lo que facilita la aplicación de políticas específicas y mejora la eficiencia del sistema.

### 3.3.2. Integración con el router

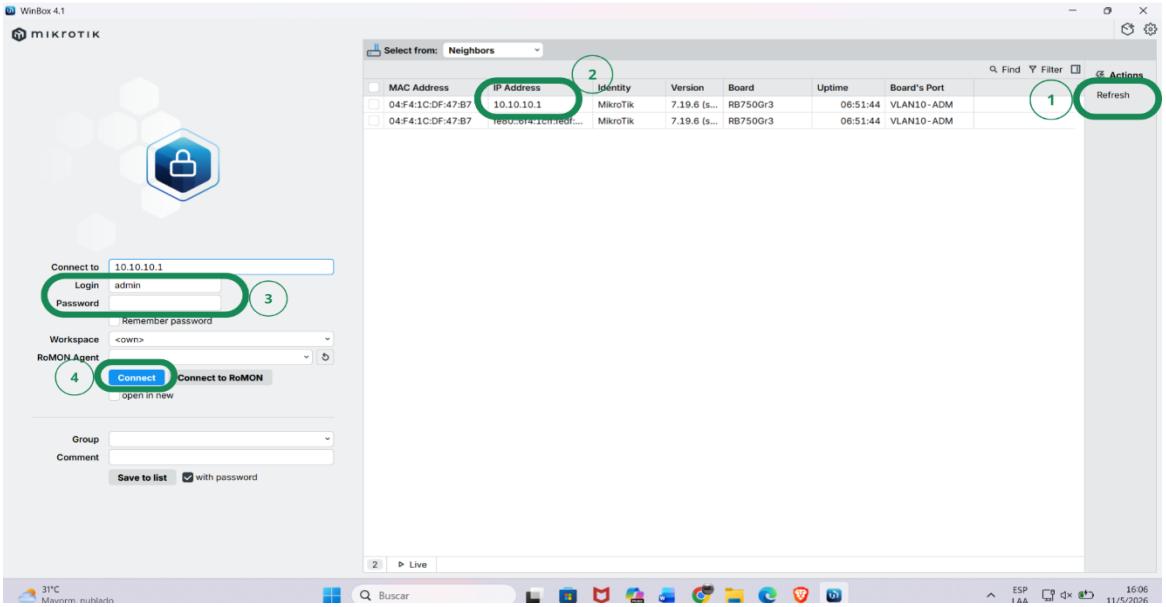
Una vez que el tráfico ha sido segmentado en el switch, se envía al router principal MikroTik RB750Gr3 hEX mediante un enlace trunk. En este dispositivo se realiza el procesamiento principal de la red, ya que se aplican las políticas de enrutamiento, balanceo de carga y calidad de servicio (QoS). La configuración del router se lleva a cabo a través de la herramienta de administración WinBox, la cual permite gestionar de manera gráfica e intuitiva todos los parámetros del sistema.

### 3.3.3. Configuración en el router

Para lograr la correcta integración con el switch y el funcionamiento del sistema, se realiza la siguiente configuración:

**Configuración para el acceso a internet**

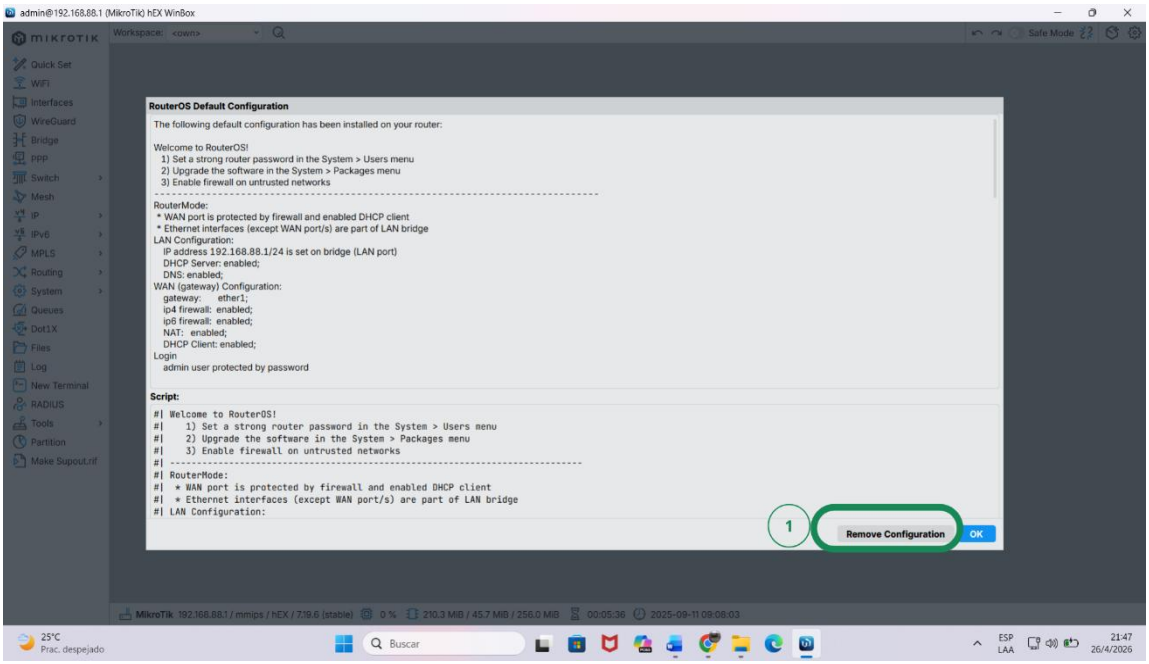
***Figura 31.*** *Interfaz del WinBox.*




*Nota.* Elaboración propia.

La Figura 31 muestra el acceso inicial a la interfaz gráfica WinBox. Para establecer la conexión, se actualizó la ventana, se seleccionó la dirección IP 10.10.10.1, se introdujeron las credenciales del router (usuario y contraseña) y se confirmó mediante la opción Connect.

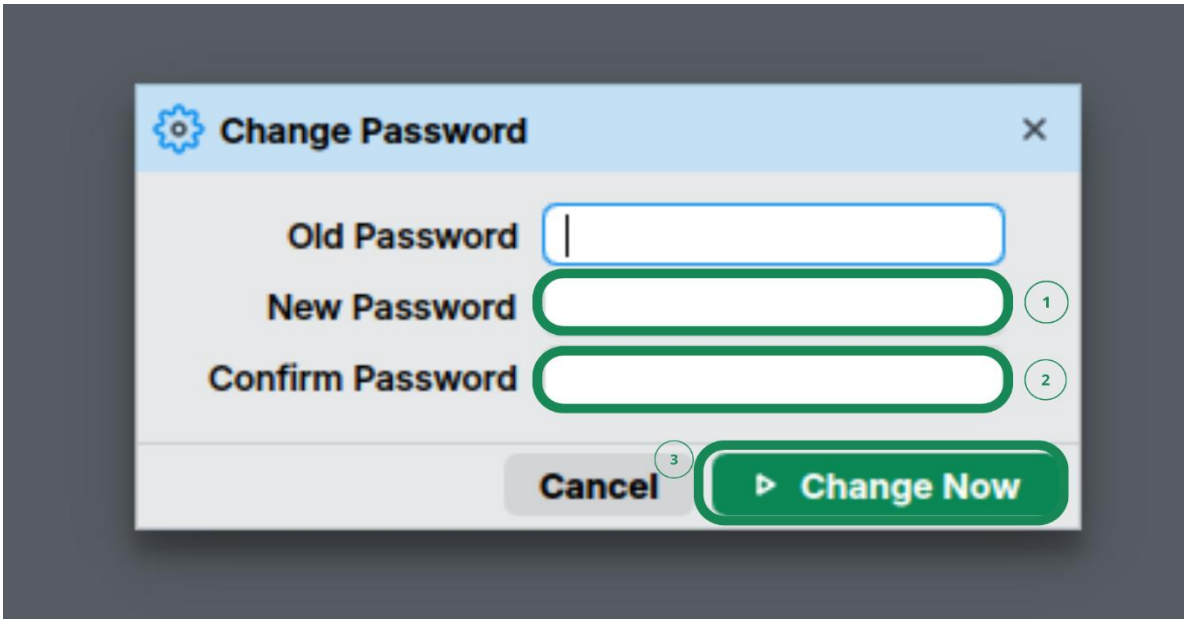
***Figura 32.*** *Configuración de fábrica.*




*Nota.* Elaboración propia.

En la Figura 32, una vez que se ha ingresado a la interfaz, se debe eliminar la configuración de fábrica del dispositivo para establecer una nueva.

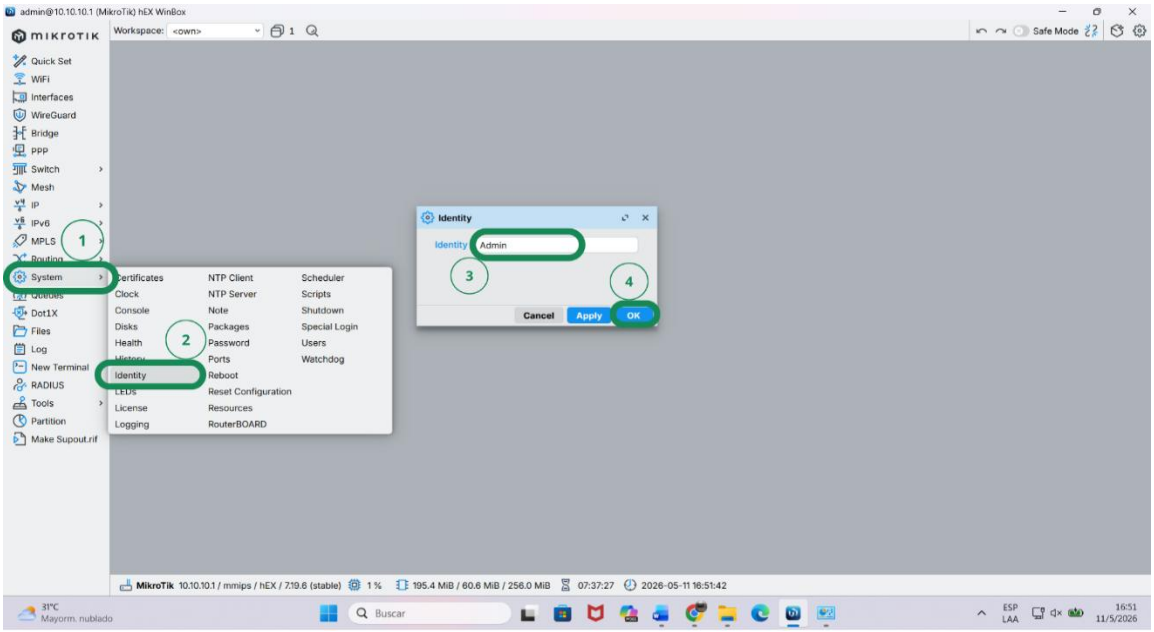
***Figura 33.*** *Nueva contraseña.*




*Nota.* Elaboración propia.

En la Figura 33 se muestra el nuevo acceso a WinBox, en el que el sistema solicita establecer una nueva contraseña; en este caso, se asignó la contraseña Wisp2026.

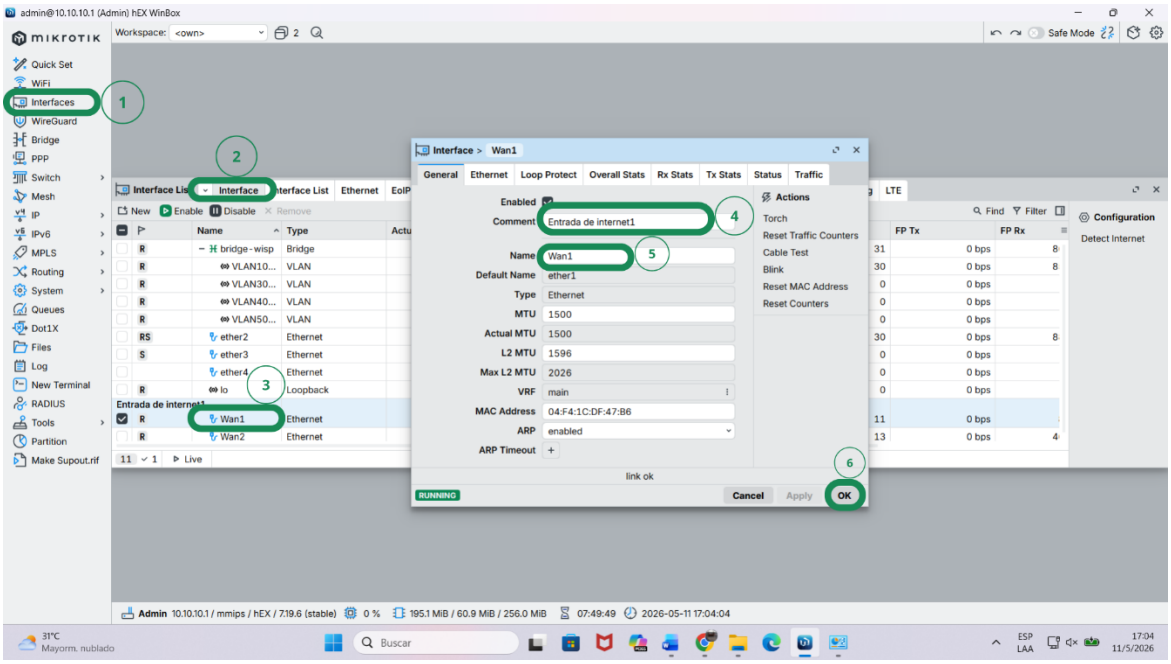
***Figura 34.*** *Asignación de nombre al dispositivo.*




*Nota.* Elaboración propia.

En la Figura 34 se asignó un nombre al dispositivo. Para ello, se accedió a System > Identity, se reemplazó el nombre MikroTik por Admin y se confirmó mediante la opción OK.

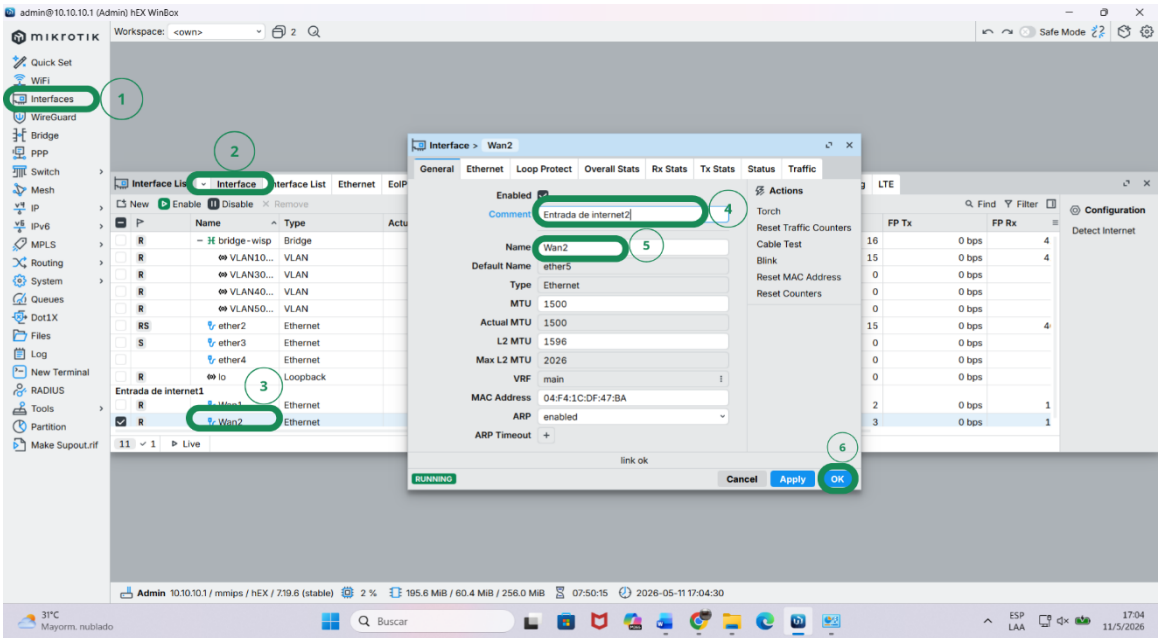
***Figura 35.*** *Interfaz como WAN1.*




*Nota.* Elaboración propia.

En la Figura 35 se identifican las interfaces del router. La interfaz WAN1 (ether1) corresponde al primer proveedor de internet; para su configuración se accedió al apartado Interfaces, se seleccionó la interfaz ether1, se asignó el comentario “entrada de internet 1” y el nombre WAN1, y se confirmó con la opción OK. De esta manera, las interfaces quedan debidamente identificadas.

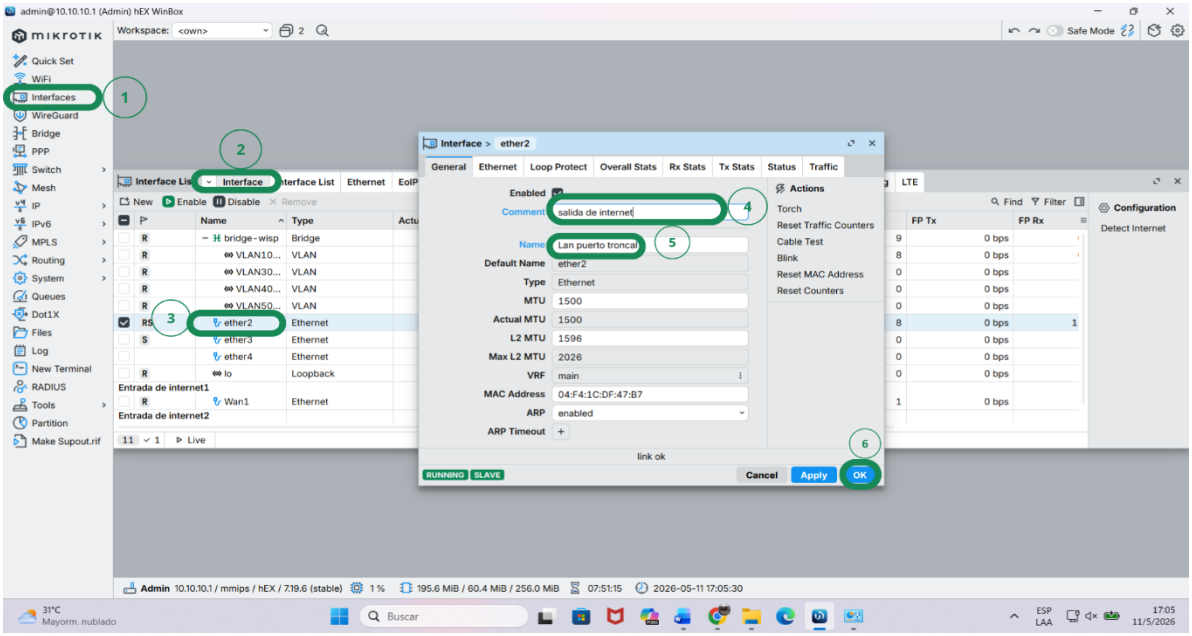
***Figura 36.*** *Interfaz como WAN2.*




*Nota.* Elaboración propia.

En la Figura 36 se repite el mismo procedimiento para la interfaz WAN2: en la ventana Interface se seleccionó ether5, se asignó el comentario “entrada de internet 2” y el nombre WAN2, y se confirmó con la opción OK.

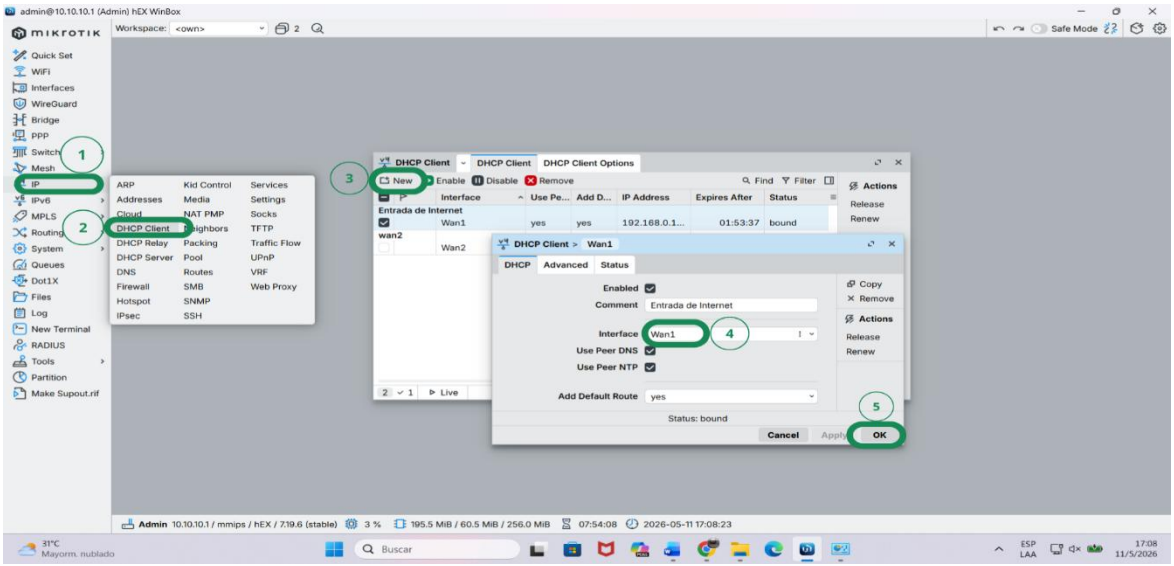
***Figura 37.*** *Salida de internet.*




*Nota.* Elaboración propia.

En la Figura 37, dentro de la misma ventana Interface, se seleccionó la interfaz ether2, a la cual se le asignó el comentario “salida de internet” y el nombre LAN (puerto troncal), dado que este puerto se encarga de la comunicación con todas las VLAN. Finalmente, se confirmó la configuración mediante la opción OK.

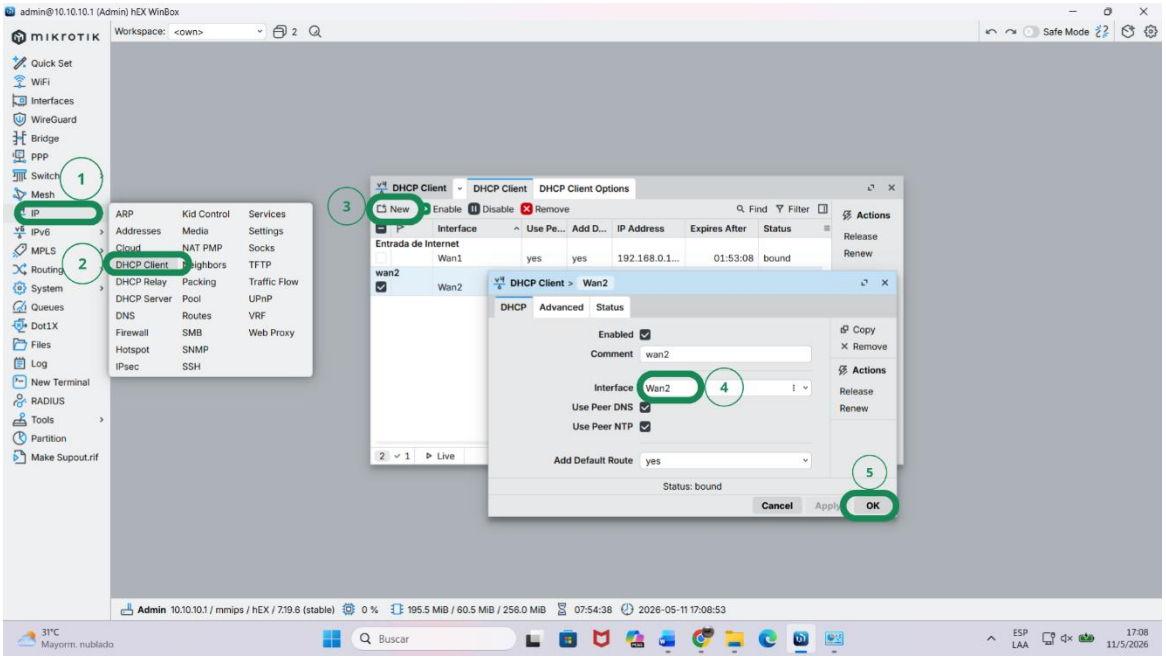
***Figura 38.*** *Configuración en DHCP client.*




*Nota.* Elaboración propia.

En la Figura 38 se presenta la configuración del DHCP Client, necesaria para que las interfaces WAN reciban una dirección IP del proveedor de internet. Para ello, se accedió a IP > DHCP Client, se seleccionó la opción New, se asignó la interfaz WAN1 y el comentario “entrada de internet”, y se confirmó con la opción OK.

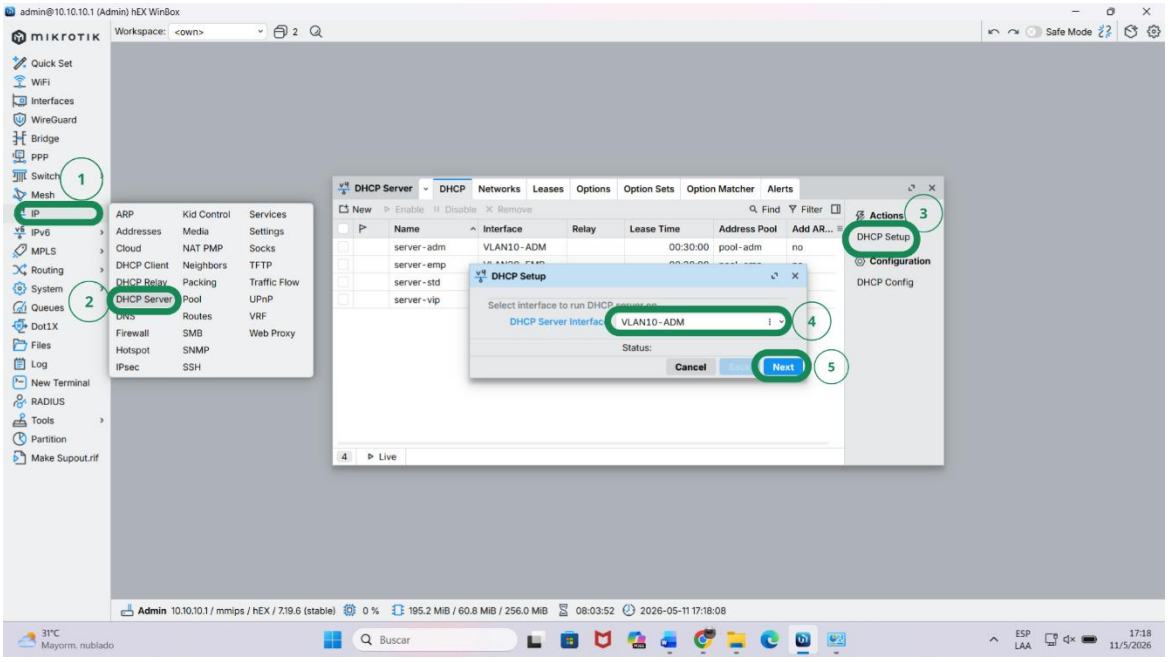
***Figura 39.*** *Configuración del cliente DHCP para WAN2.*




*Nota.* Elaboración propia.

En la Figura 39 se aplicó el mismo procedimiento a la interfaz WAN2: en la ventana DHCP Client se seleccionó la opción New, se asignó la interfaz WAN2 y se confirmó con la opción OK.

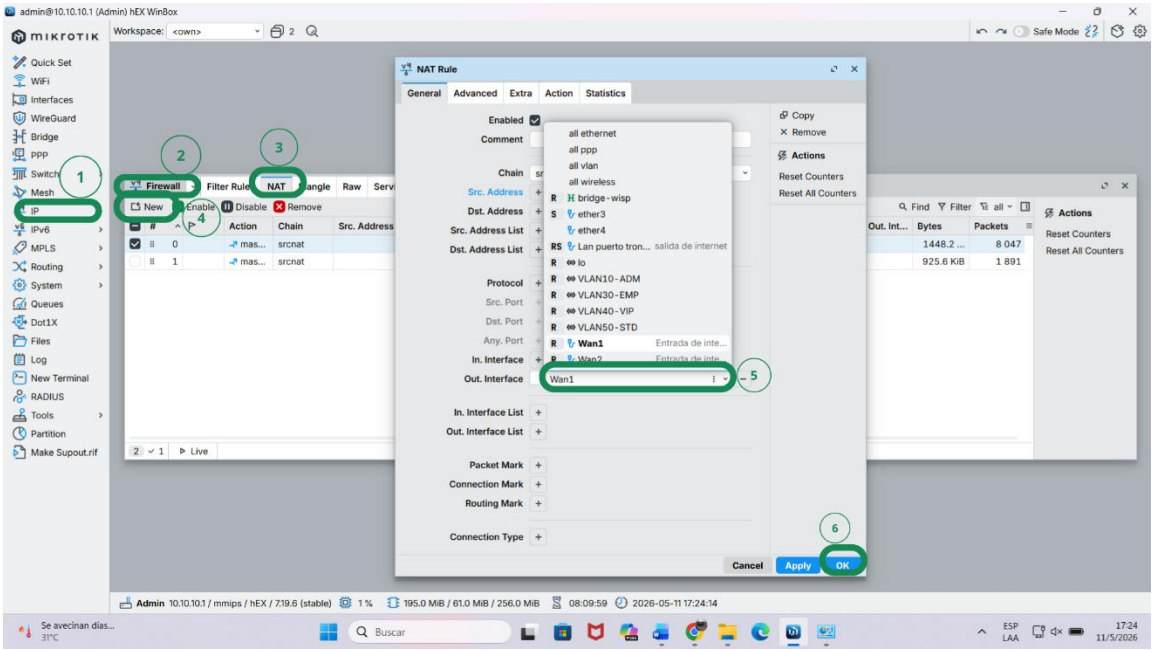
***Figura 40.*** *Configuración del DHCP Server.*




*Nota.* Elaboración propia.

En la Figura 40 se presenta la configuración del DHCP Server mediante el asistente DHCP Setup sobre la interfaz LAN, lo que permite que los dispositivos reciban automáticamente sus direcciones IP.

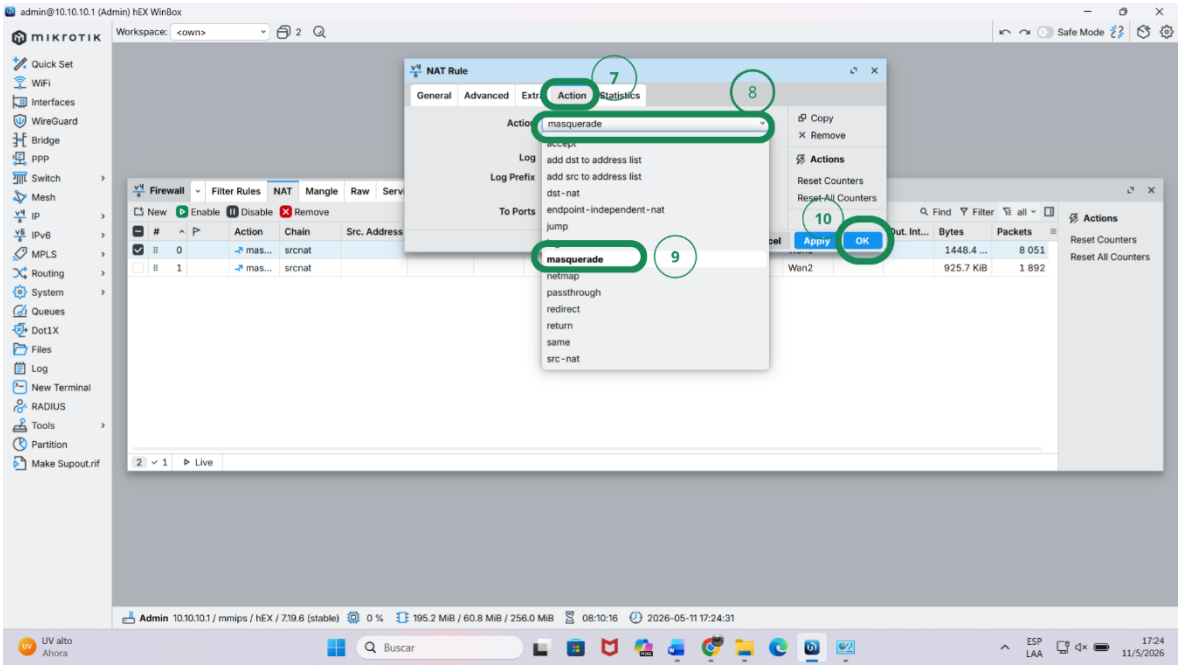
***Figura 41.*** *Configuración del NAT.*




*Nota.* Elaboración propia.

En la Figura 41 se presenta, finalmente, la configuración del NAT, necesaria para que los dispositivos conectados al router dispongan de acceso a internet. Se accedió a IP > Firewall > NAT y se creó una regla con la cadena srcnat, en la que se definió la red local y se seleccionó como interfaz de salida WAN1.

***Figura 42.*** *Selección masquerade.*



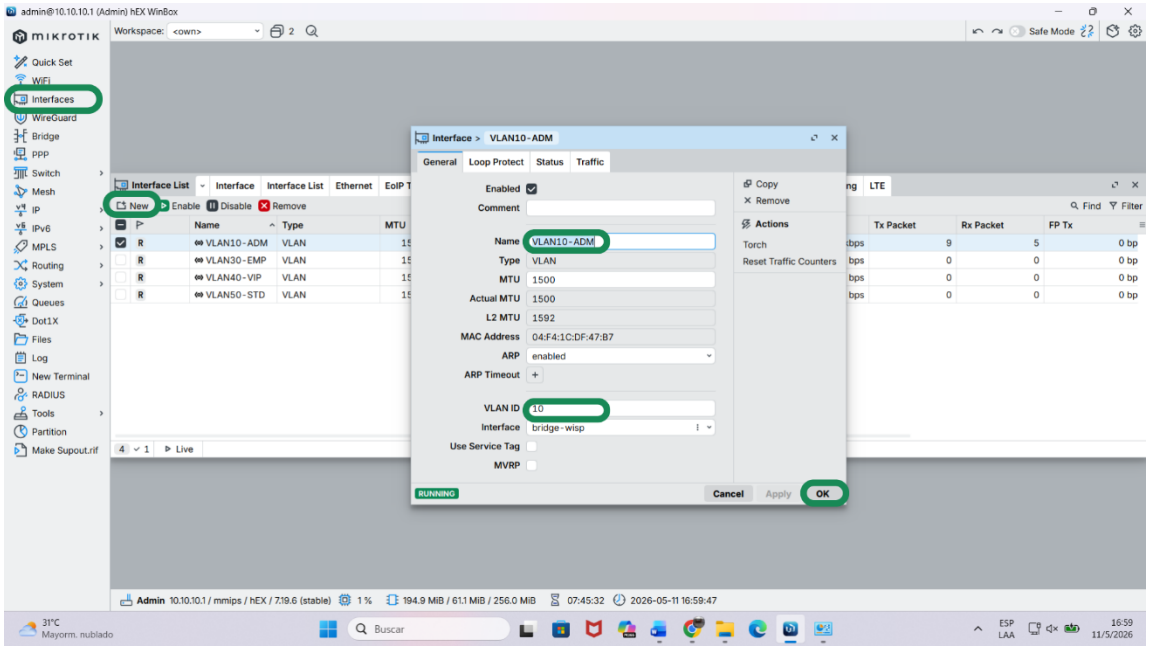

*Nota.* Elaboración propia.

En la Figura 42, en el apartado Action, se seleccionó la opción masquerade y se guardó la configuración mediante la opción OK.

### 3.3.4. Creación de VLAN en el router

En el router se crean interfaces virtuales asociadas al puerto físico conectado al switch mediante un enlace trunk. Esto permite identificar el tráfico según la VLAN de origen.

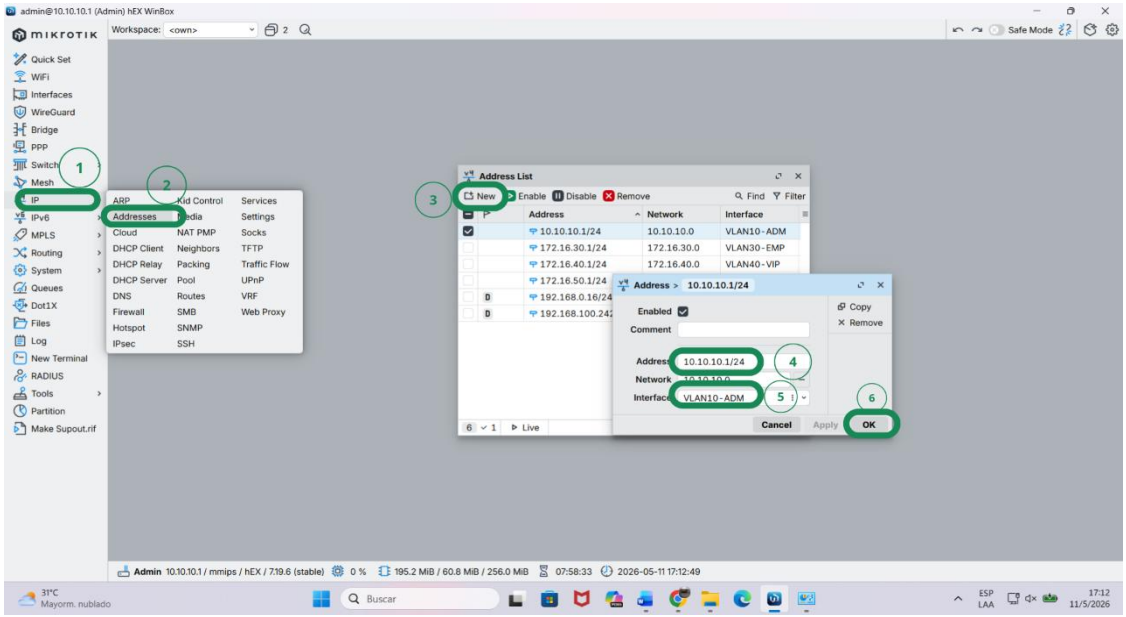
***Figura 43.*** *Creación de interfaz de VLAN.*




*Nota.* Elaboración propia.

La Figura 43 muestra la creación de la interfaz correspondiente a la VLAN 10 de administración. En el campo VLAN ID se configuró el identificador 10 y se asoció la interfaz al puerto troncal correspondiente. El mismo procedimiento se aplica a las demás VLAN del sistema.

***Figura 44.*** *IP para red LAN.*




*Nota.* Elaboración propia.

En la Figura 44 se presenta la creación de la red LAN. Para ello, se accedió a IP > Address, se seleccionó la opción New, se asignó la dirección 10.10.10.1/24 a la interfaz correspondiente a la VLAN 10 de administración y se guardó la configuración con la opción OK.

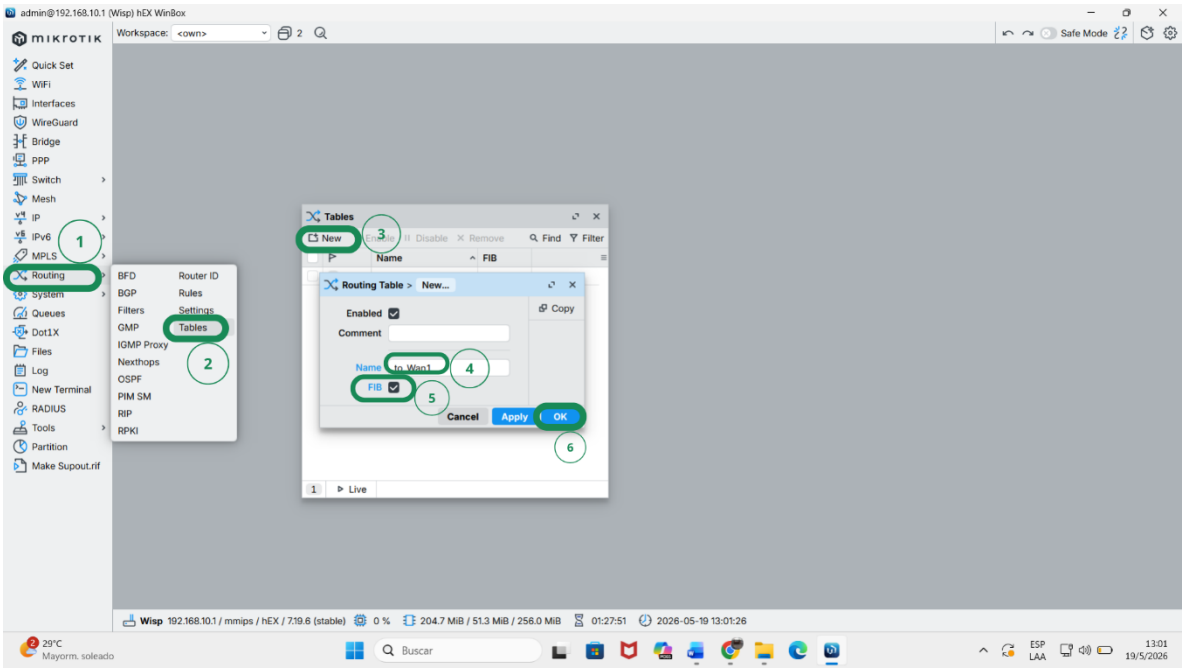
### 3.3.5. Implementación del balanceo de carga PCC

En esta etapa se implementa el balanceo de carga mediante la técnica PCC (Per Connection Classifier) en el router MikroTik, con el objetivo de distribuir el tráfico de los usuarios entre los enlaces de internet disponibles. Esta configuración permite optimizar el uso del ancho de banda, mejorar la estabilidad de la conexión y mantener la persistencia de las sesiones activas.

La implementación del PCC se realiza sobre el tráfico que ingresa desde la interfaz LAN/troncal, de modo que las conexiones provenientes de las VLAN configuradas puedan ser clasificadas y distribuidas entre los enlaces WAN. Para ello, se configuran reglas de Mangle, marcado de conexiones, marcado de rutas y rutas de salida hacia cada proveedor de internet.

A continuación, se presenta el procedimiento seguido para la configuración del balanceo de carga PCC en el router MikroTik.

***Figura 45.*** *Marcas de rutas.*

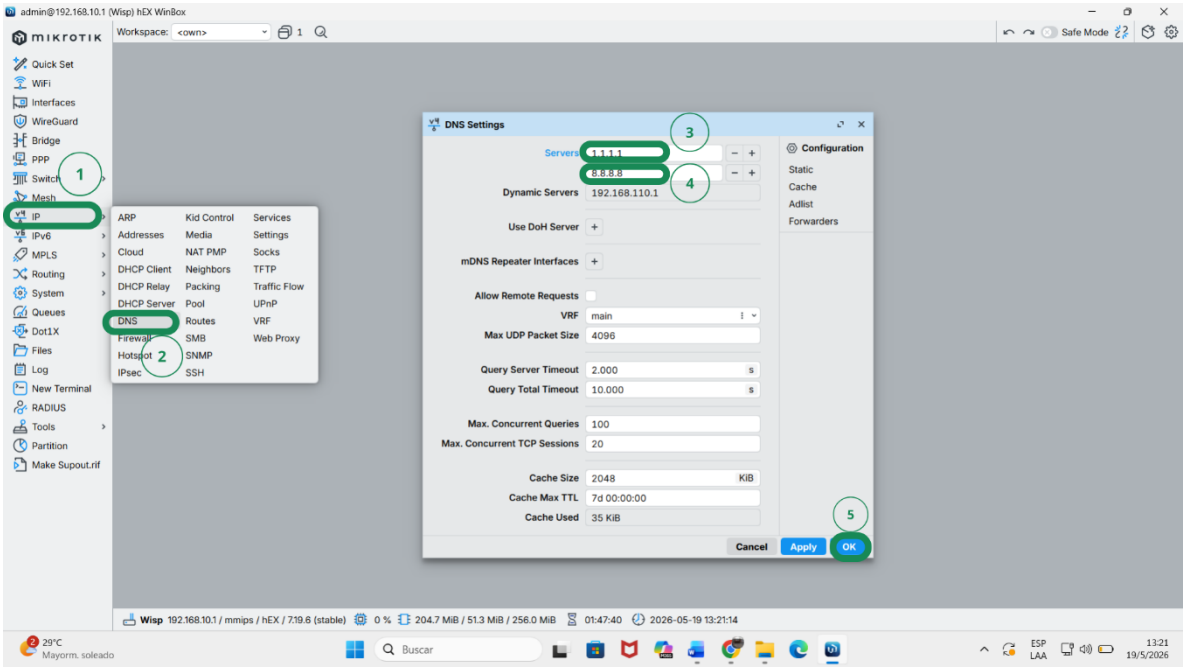



*Nota.* Elaboración propia.

La Figura 45 muestra la creación de las marcas de ruta asociadas a cada enlace WAN. Se accedió a Routing > Tables y, mediante la opción New, se asignó el nombre to_wan1, se habilitó la opción FIB y se confirmó con la opción OK.

El mismo procedimiento se repitió para el enlace WAN2: mediante la opción New, se asignó el nombre to_wan2, se habilitó la opción FIB y se confirmó con la opción OK.

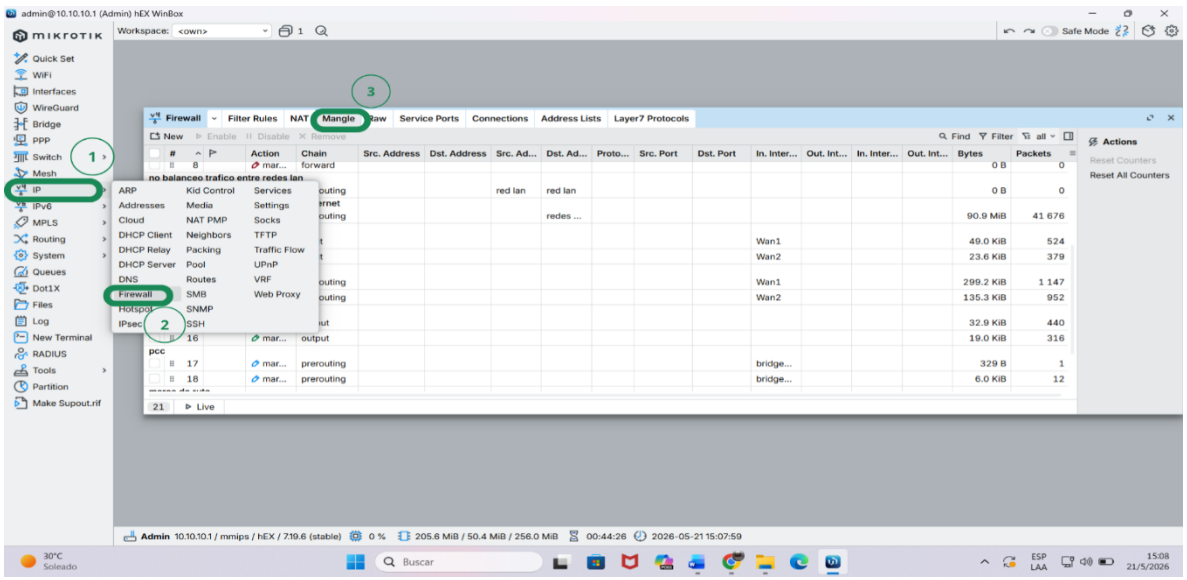
***Figura 46.*** *Configuración de los servidores DNS.*




*Nota.* Elaboración propia.

En la Figura 46 se agregaron los servidores DNS. Para ello, se accedió a IP > DNS y, en el apartado Servers, se configuraron las direcciones 1.1.1.1 y 8.8.8.8 como servidores de resolución de nombres.

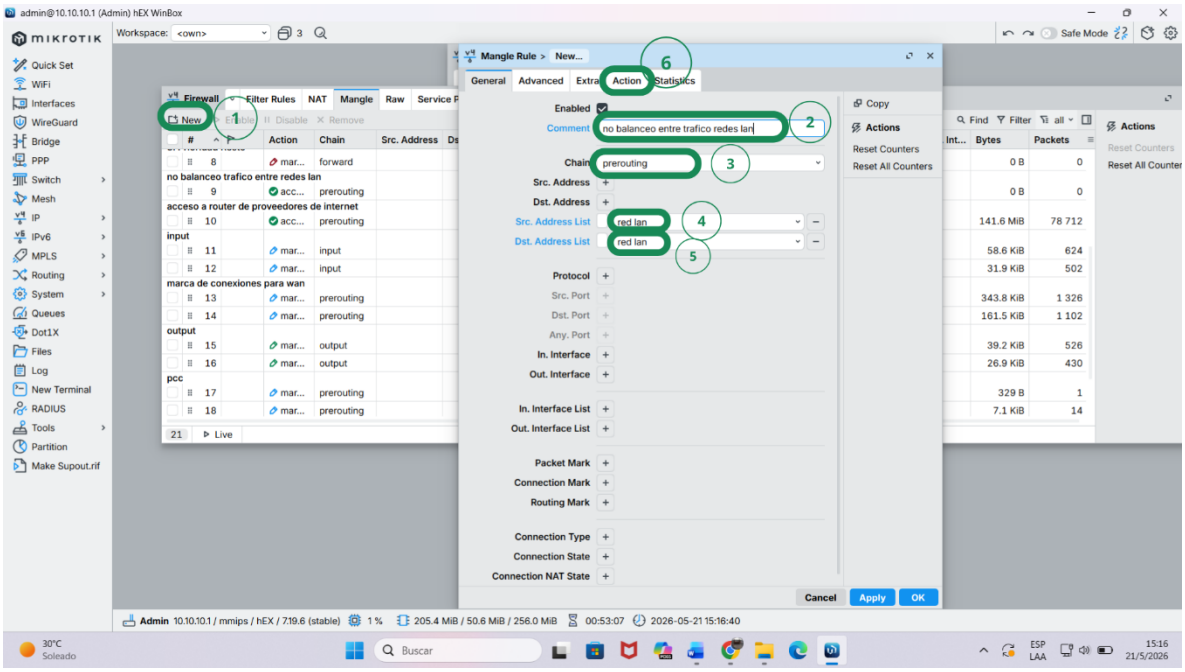
***Figura 47.*** *Acceso al apartado Mangle.*




*Nota.* Elaboración propia.

En la Figura 47 se muestra el acceso a IP > Firewall y, dentro de esa ventana, al apartado Mangle.

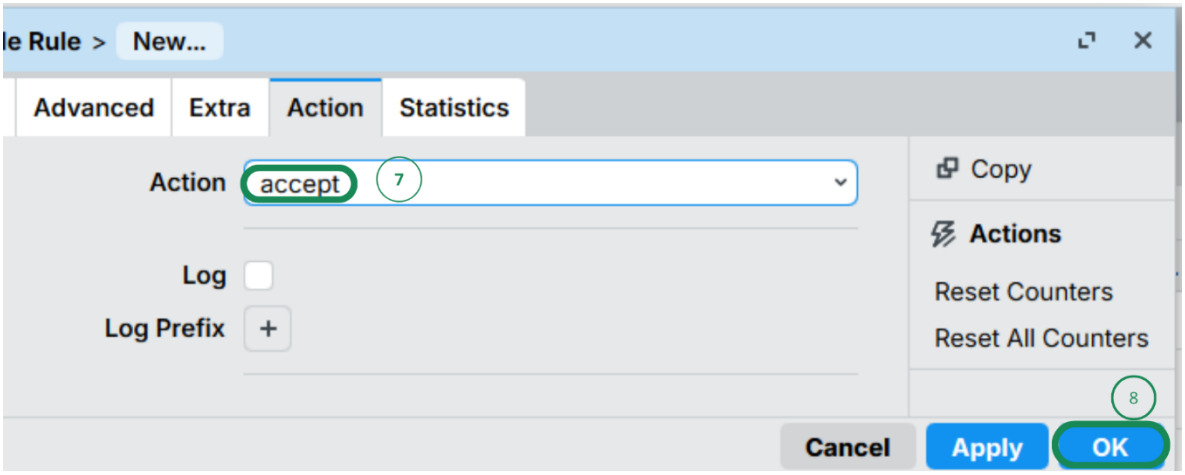
***Figura 48.*** *Configuración para evitar el balanceo entre redes LAN.*




*Nota.* Elaboración propia.

En la Figura 48, dentro del apartado Mangle, se seleccionó la opción New; en el campo Chain se estableció prerouting y, tanto en Src. Address List como en Dst. Address List, se seleccionaron las redes LAN para continuar con la pestaña Action.

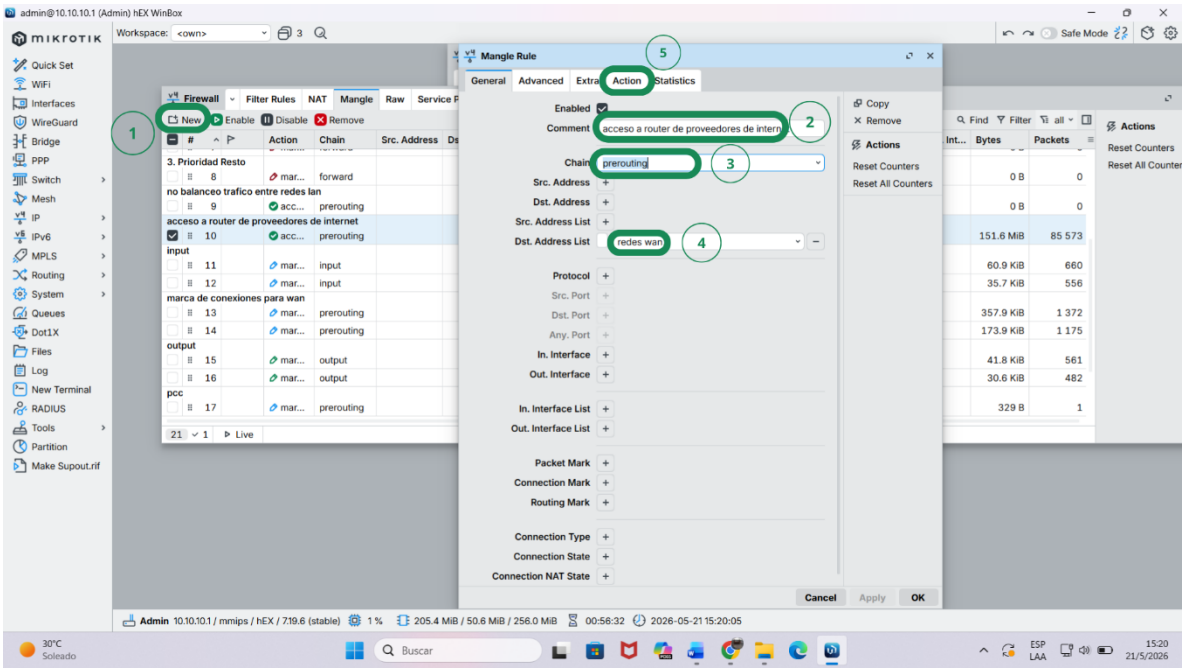
***Figura 49.*** *Apartado Action.*




*Nota.* Elaboración propia.

Como se observa en la Figura 49, se verificó que, en el apartado Action, estuviera seleccionada la opción accept y se confirmó mediante la opción OK. La acción accept evita que el tráfico entre redes LAN sea sometido al balanceo, lo que facilita la gestión local de los equipos.

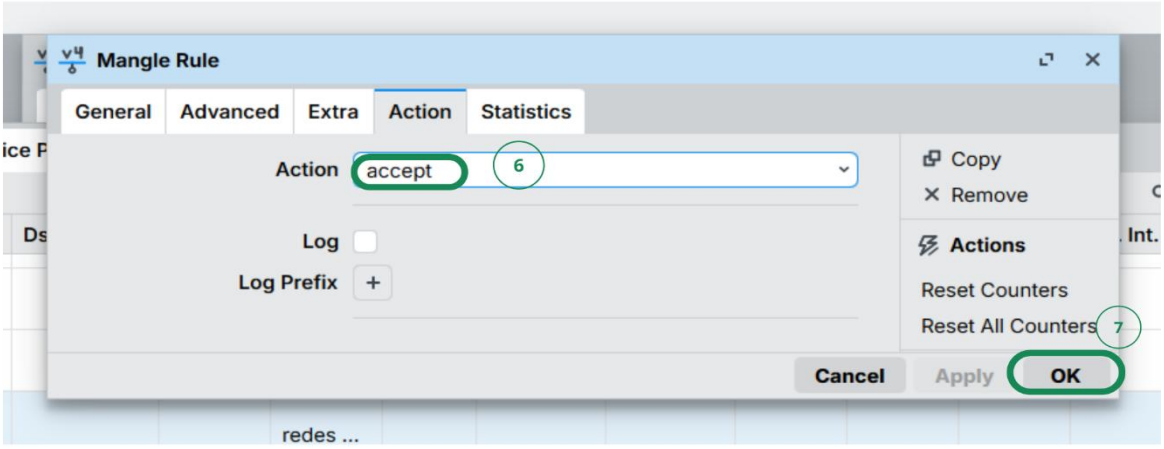
***Figura 50.*** *Regla para el acceso a los routers de los proveedores de internet.*




*Nota.* Elaboración propia.

En la Figura 50 se seleccionó la opción New, con lo que se abrió la ventana Mangle Rule. En el campo Comment se registró la descripción “regla para el acceso a los routers de los proveedores de internet”; en Chain se estableció prerouting; y en Dst. Address List se seleccionaron las redes WAN para continuar con la pestaña Action.

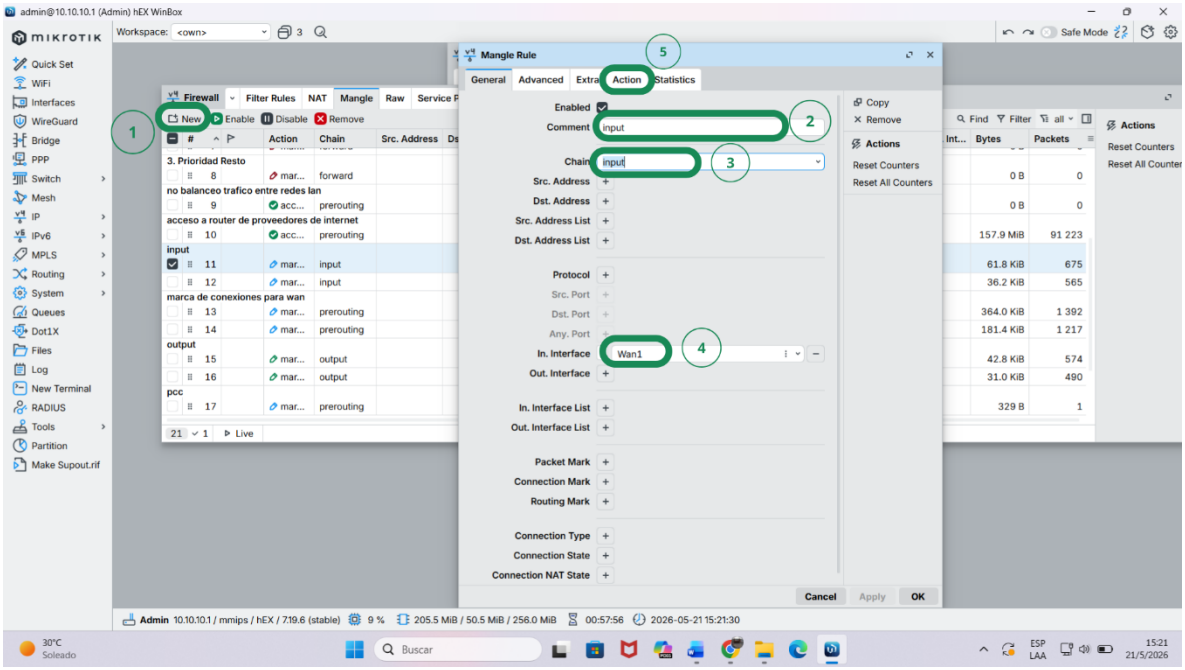
***Figura 51.*** *Pestaña Action.*




*Nota.* Elaboración propia.

En la Figura 51, en el apartado Action, se seleccionó la opción accept y, por último, se confirmó con la opción OK para guardar la configuración.

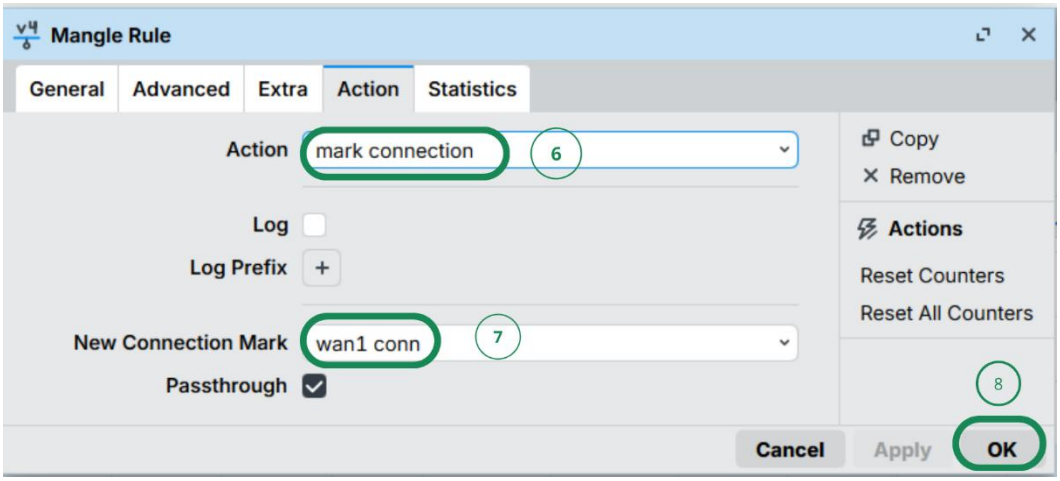
***Figura 52.*** *Regla input.*




*Nota.* Elaboración propia.

En la Figura 52 se creó una nueva regla en la cadena input, la cual identifica las conexiones que ingresan al router a través de la interfaz WAN. En Chain se seleccionó input; en In. Interface se configuró WAN1; y, posteriormente, se definió la acción de marcado de conexión.

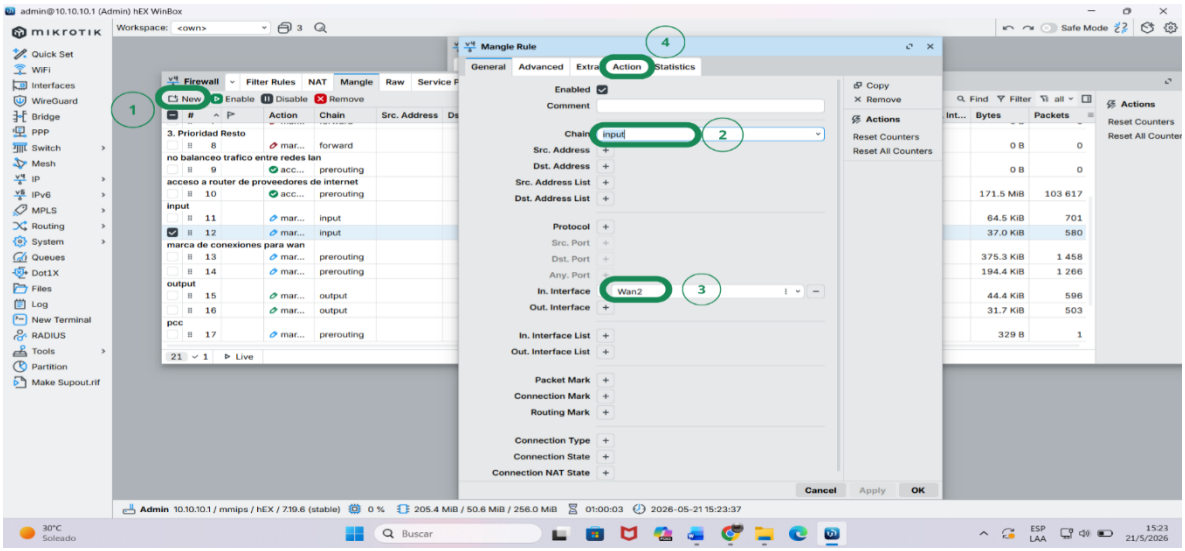
***Figura 53.*** *Pestaña Action: marca de conexión.*




*Nota.* Elaboración propia.

En la Figura 53, en el apartado Action, se seleccionó la opción Mark Connection y, en New Connection Mark, la marca wan1 conn; posteriormente, se confirmó con la opción OK.

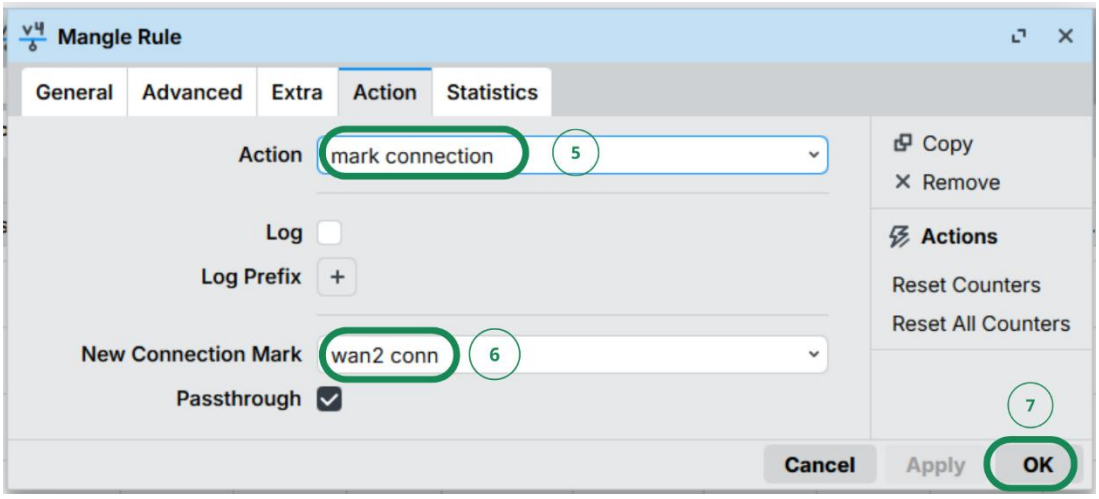
***Figura 54.*** *Regla input para WAN2.*




*Nota.* Elaboración propia.

En la Figura 54 se creó la regla input correspondiente a la interfaz WAN2: mediante la opción New, se estableció la cadena input y, en el apartado Interface, se seleccionó WAN2 para continuar con la pestaña Action.

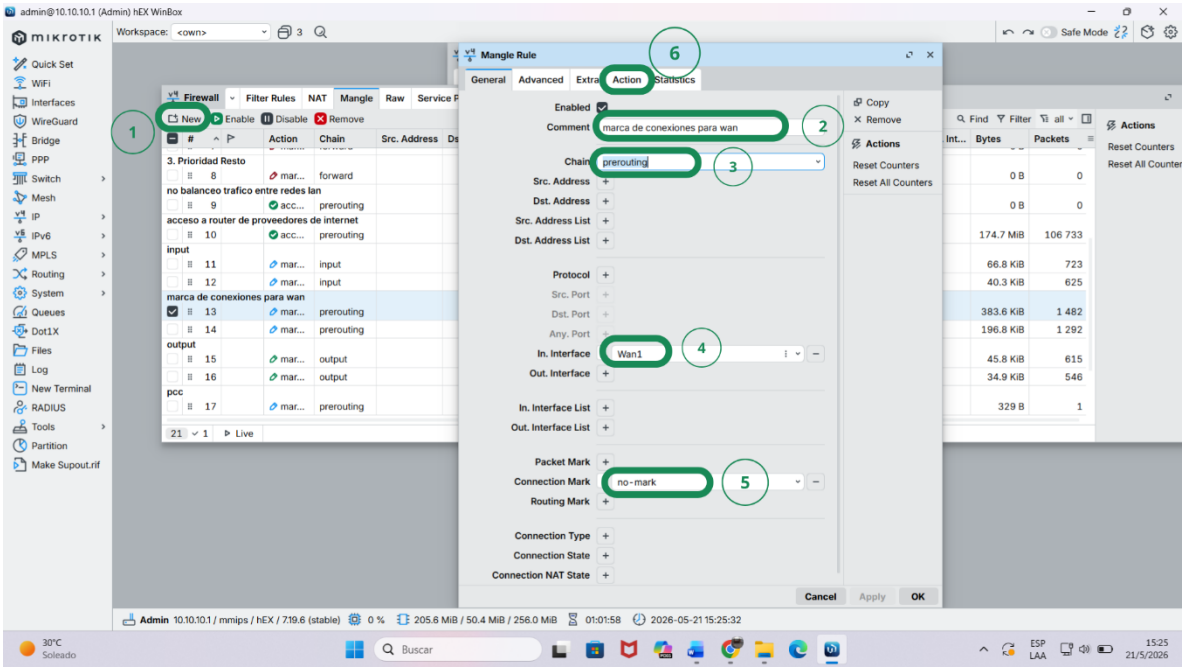
***Figura 55.*** *Pestaña Action: marca de conexión para WAN2.*




*Nota.* Elaboración propia.

En la Figura 55, en el apartado Action, se seleccionó la opción Mark Connection y, en New Connection Mark, la marca wan2 conn; posteriormente, se guardó la configuración con la opción OK.

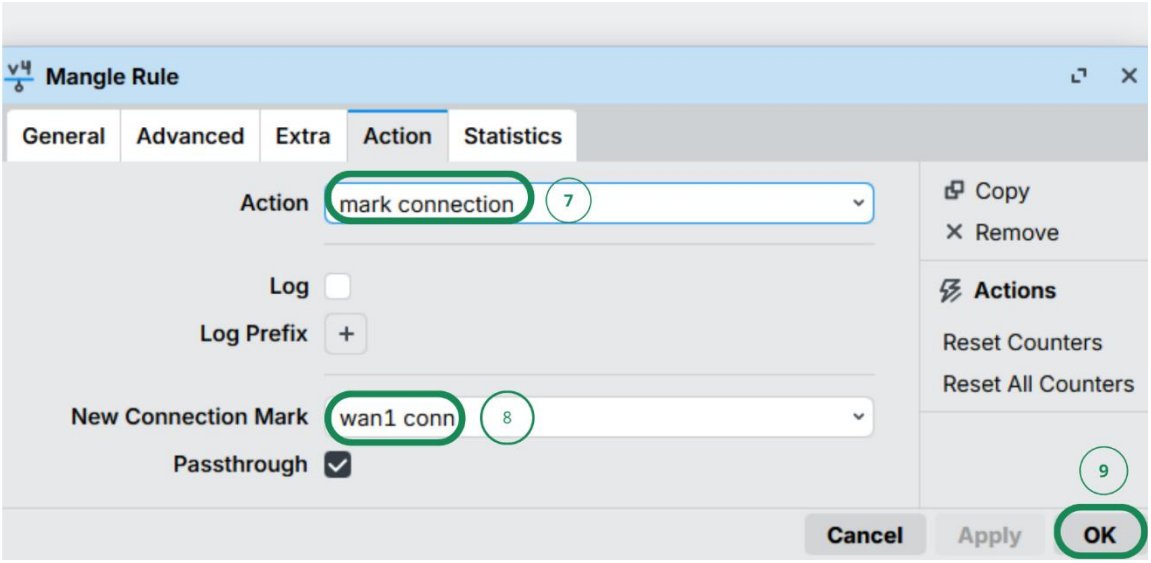
***Figura 56.*** *Marcar las conexiones originadas en internet.*




*Nota.* Elaboración propia.

En la Figura 56 se creó una nueva regla destinada a marcar las conexiones originadas en internet, de modo que el tráfico que ingresa al router por una interfaz WAN salga por esa misma interfaz. Mediante la opción New, se registró el comentario “marca de conexiones para WAN”; en Chain se estableció prerouting; en Interface se seleccionó WAN1; y en Connection Mark, la opción no-mark para continuar con la pestaña Action.

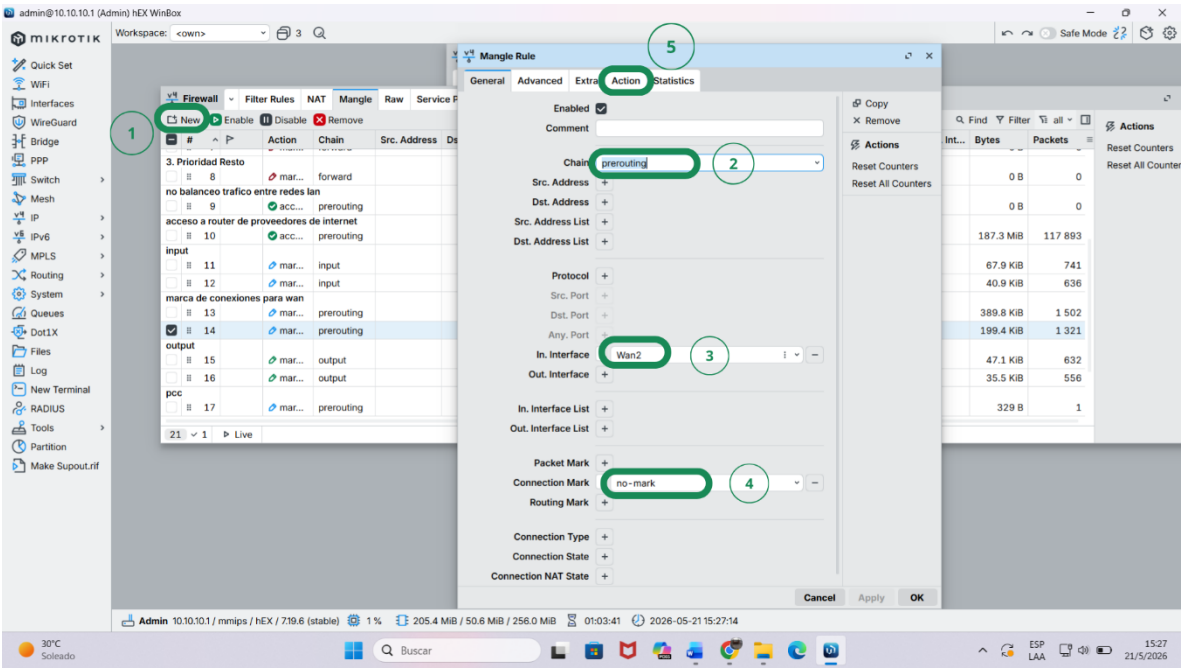
***Figura 57.*** *Pestaña Action: marca de conexión.*




*Nota.* Elaboración propia.

En la Figura 57, en el apartado Action, se seleccionó la opción mark connection y, en New Connection Mark, la marca wan1 conn; posteriormente, se guardó la configuración con la opción OK.

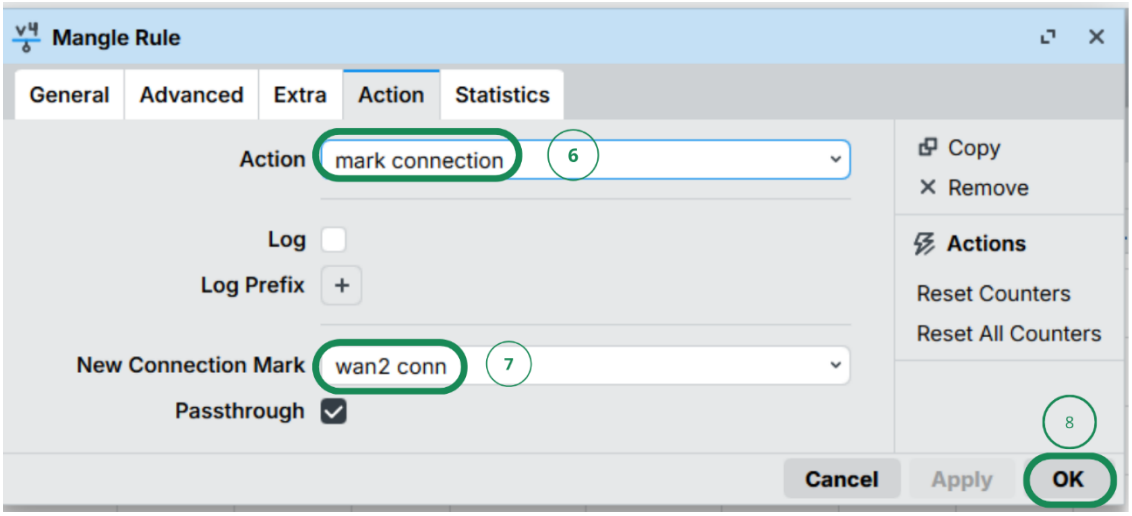
***Figura 58.*** *Marcar las conexiones originadas en internet para WAN2.*




*Nota.* Elaboración propia.

En la Figura 58 se replicó la regla anterior para la interfaz WAN2. Mediante la opción New, se estableció la cadena prerouting; en el apartado Interface, se seleccionó WAN2; y en Connection Mark, la opción no-mark para continuar con la pestaña Action.

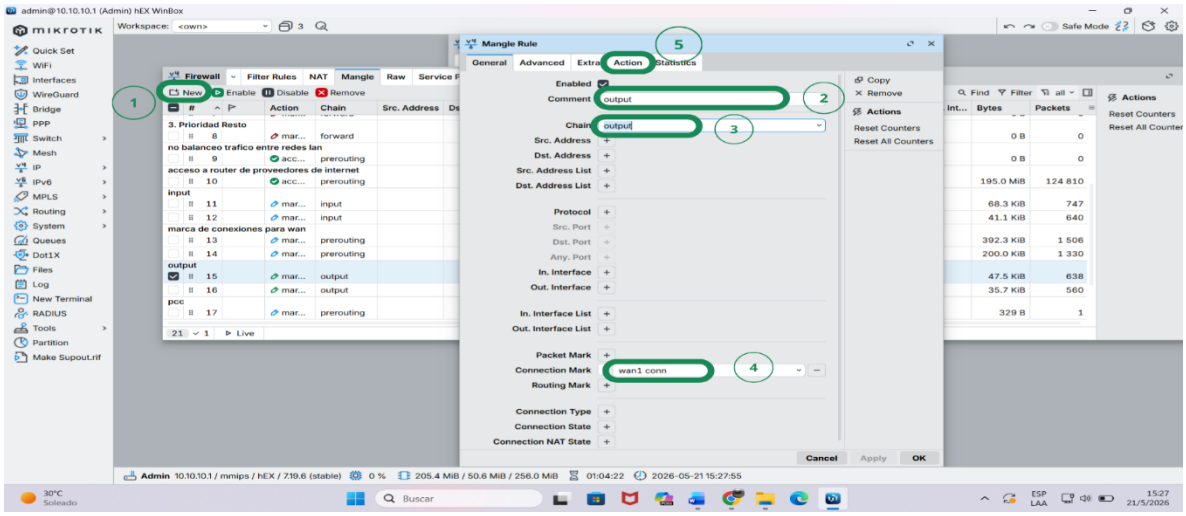
**Figura 59.** *Pestaña Action: marca de conexión para WAN2.*




*Nota.* Elaboración propia.

En la Figura 59, en el apartado Action, se seleccionó la opción mark connection y, en New Connection Mark, la marca wan2 conn; posteriormente, se guardó la configuración con la opción OK.

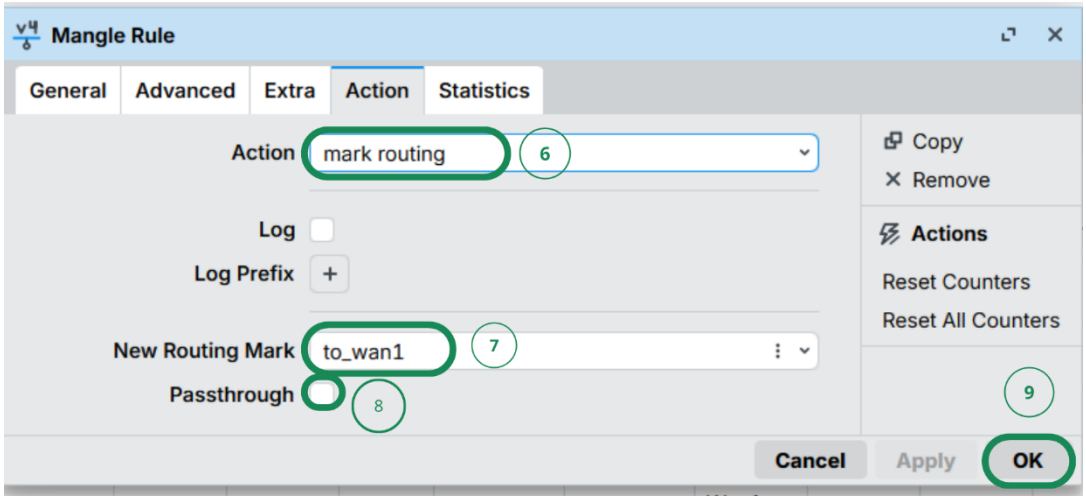
***Figura 60.*** *Regla output para WAN1.*




*Nota.* Elaboración propia.

La Figura 60 muestra la creación de una nueva regla en la cadena output, aplicada al tráfico generado por el propio router y asociado a la marca de conexión wan1 conn. Mediante la opción New, se registró el comentario “output”; en Chain se estableció output; y en Connection Mark se seleccionó wan1 conn para continuar con la pestaña Action.

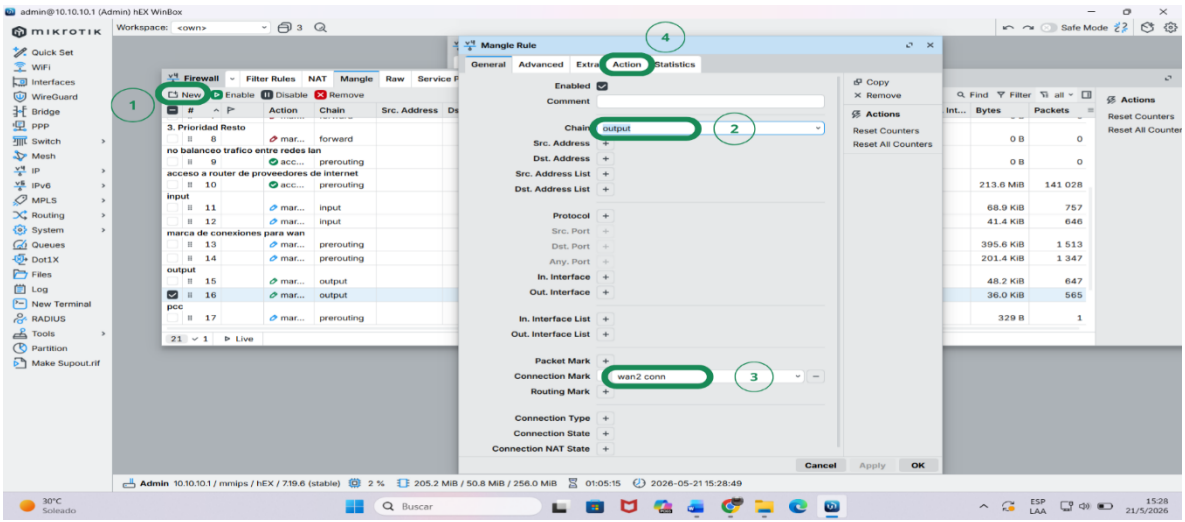
***Figura 61.*** *Pestaña Action.*




*Nota.* Elaboración propia.

En la Figura 61, en el apartado Action, se seleccionó la opción mark routing; en New Routing Mark, la marca to_wan1; y se desactivó la opción Passthrough. Finalmente, se guardó la configuración con la opción OK.

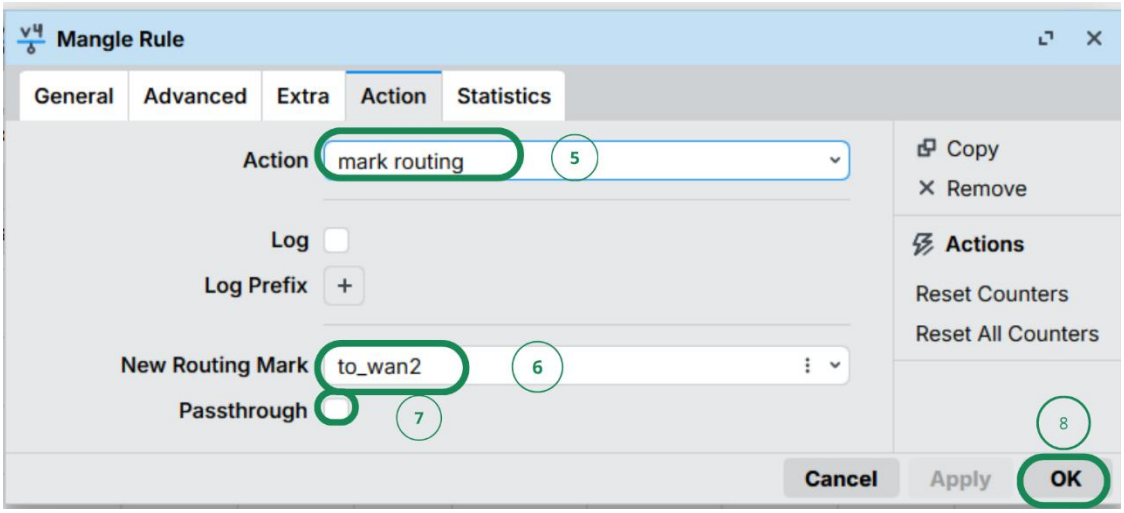
***Figura 62.*** *Regla output para WAN2.*




*Nota.* Elaboración propia.

La Figura 62 muestra la creación de la misma regla aplicada a la interfaz WAN2. Mediante la opción New, se abrió la ventana Mangle Rule, en la que se estableció la cadena output y, en Connection Mark, la marca wan2 conn para continuar con la pestaña Action.

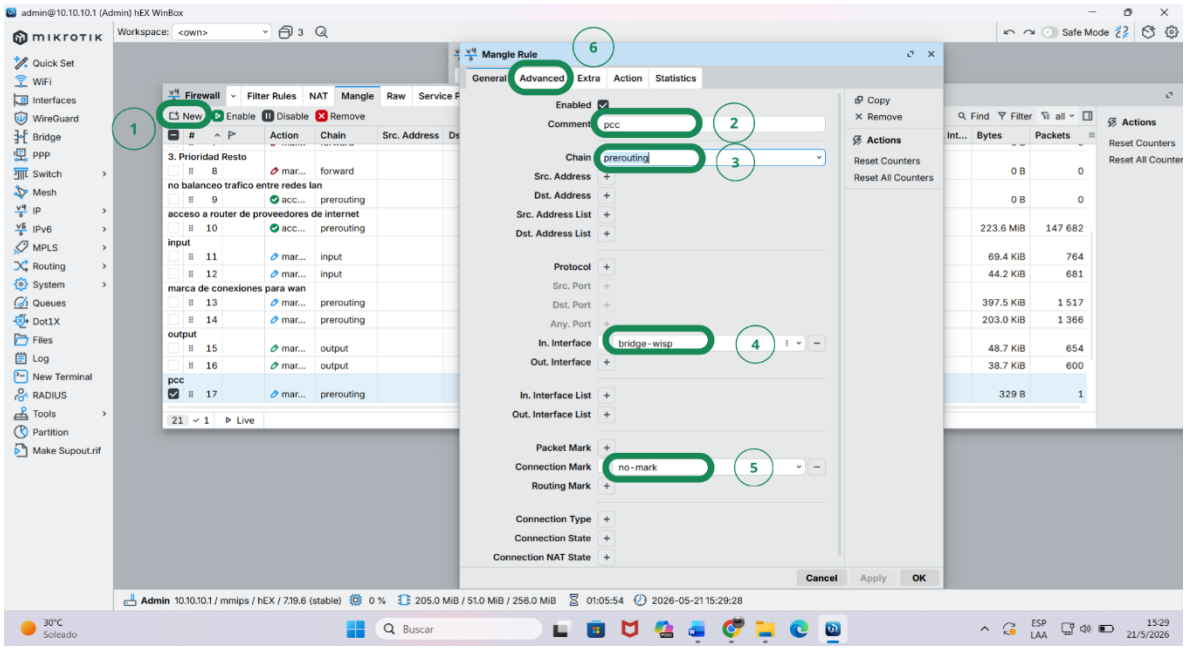
***Figura 63.*** *Pestaña Action: marca de ruta.*




*Nota.* Elaboración propia.

En la Figura 63, en el apartado Action, se seleccionó la opción mark routing; en New Routing Mark, la marca to_wan2; se desactivó la opción Passthrough; y se guardó la configuración con la opción OK.

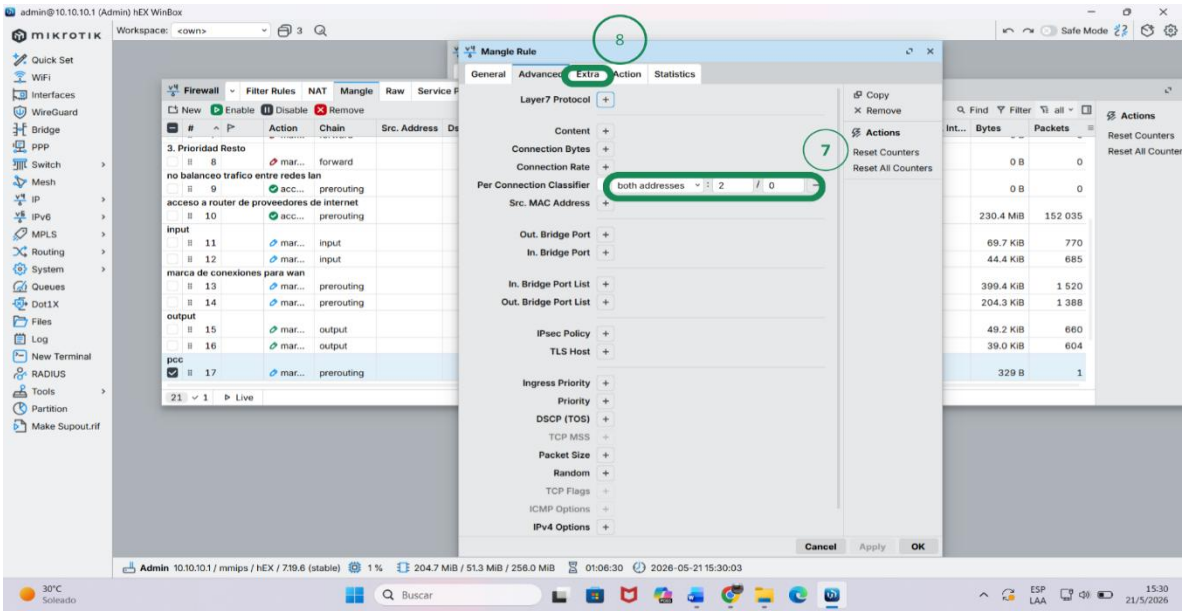
***Figura 64.*** *Inicio del PCC.*




*Nota.* Elaboración propia.

La Figura 64 muestra la creación de la primera regla correspondiente al algoritmo PCC empleado en esta configuración. Mediante la opción New, se abrió la ventana Mangle Rule, en la que se registró el comentario “PCC” y se estableció la cadena prerouting. Además, se seleccionó la interfaz LAN, en este caso *bridge*-wisp, y, en Connection Mark, la opción no-mark para continuar con la pestaña Advanced.

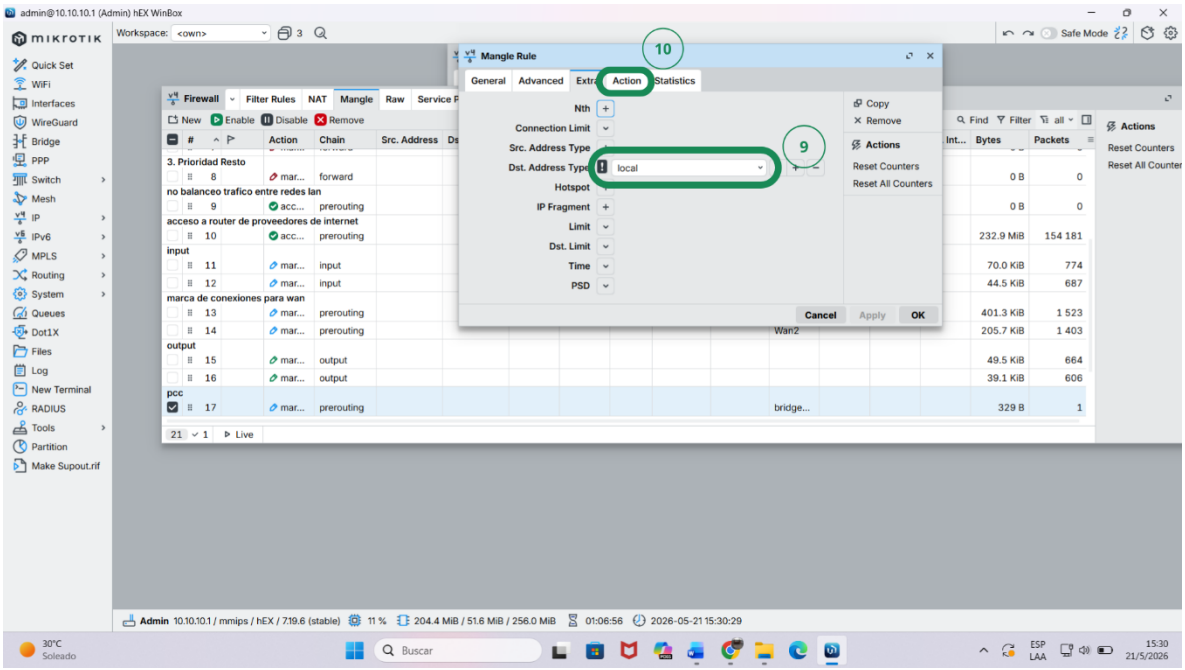
***Figura 65.*** *Configuración en la pestaña Advanced.*




*Nota.* Elaboración propia.

En la Figura 65, en el apartado Per Connection Classifier, se seleccionó la opción both addresses y se configuró un denominador de 2, correspondiente a los dos enlaces de internet balanceados, con índice inicial 0; posteriormente, se continuó con la pestaña Extra.

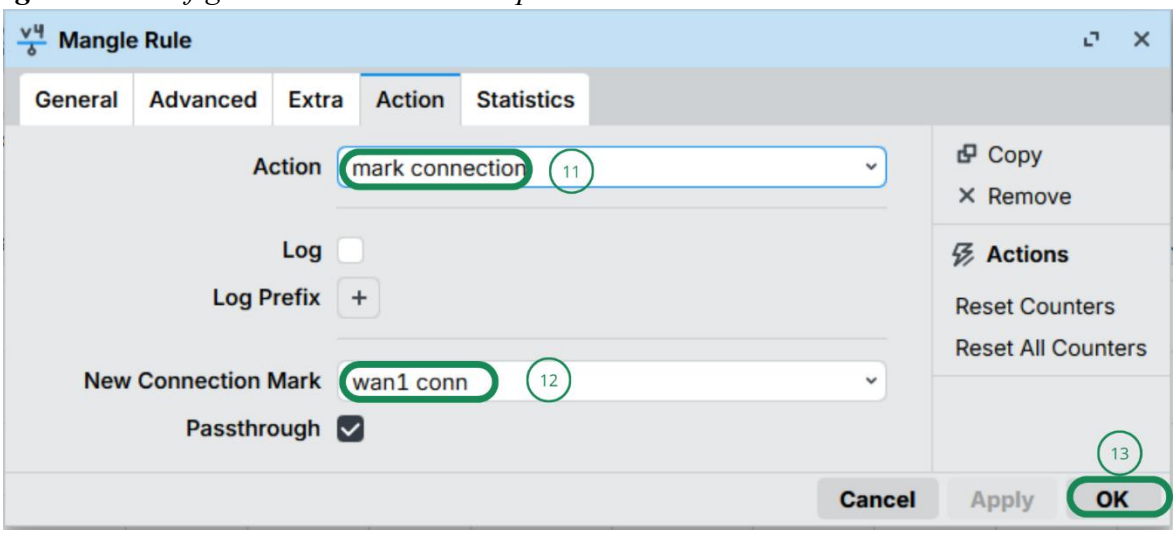
***Figura 66.*** *Configuración en la pestaña Extra.*




*Nota.* Elaboración propia.

En la Figura 66, en el apartado Dst. Address Type, se seleccionó la opción local y se marcó el recuadro correspondiente, con lo que apareció el signo de admiración que niega la condición. De esta manera, la regla se aplica a todo el tráfico de la red, excepto al tráfico local entre redes LAN, que queda excluido de estas políticas. Posteriormente, se continuó con la pestaña Action.

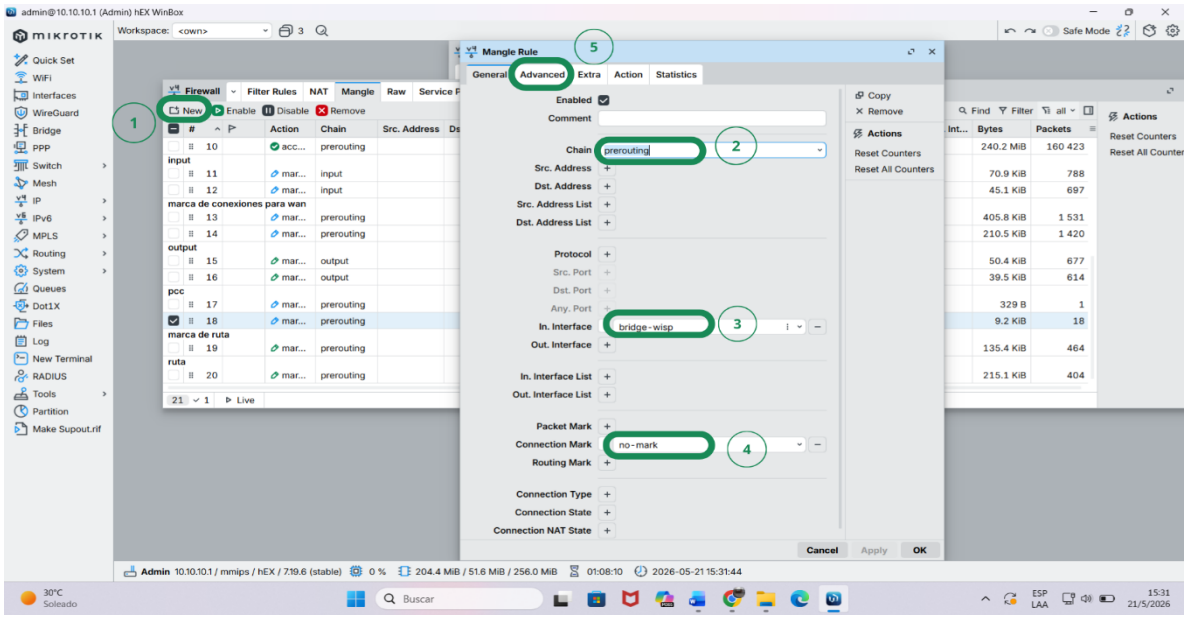
***Figura 67.*** *Configuración del PCC en la pestaña Action.*




*Nota.* Elaboración propia.

En la Figura 67, en el apartado Action, se seleccionó la opción mark connection y, en New Connection Mark, la marca wan1 conn; posteriormente, se guardó la regla con la opción OK.

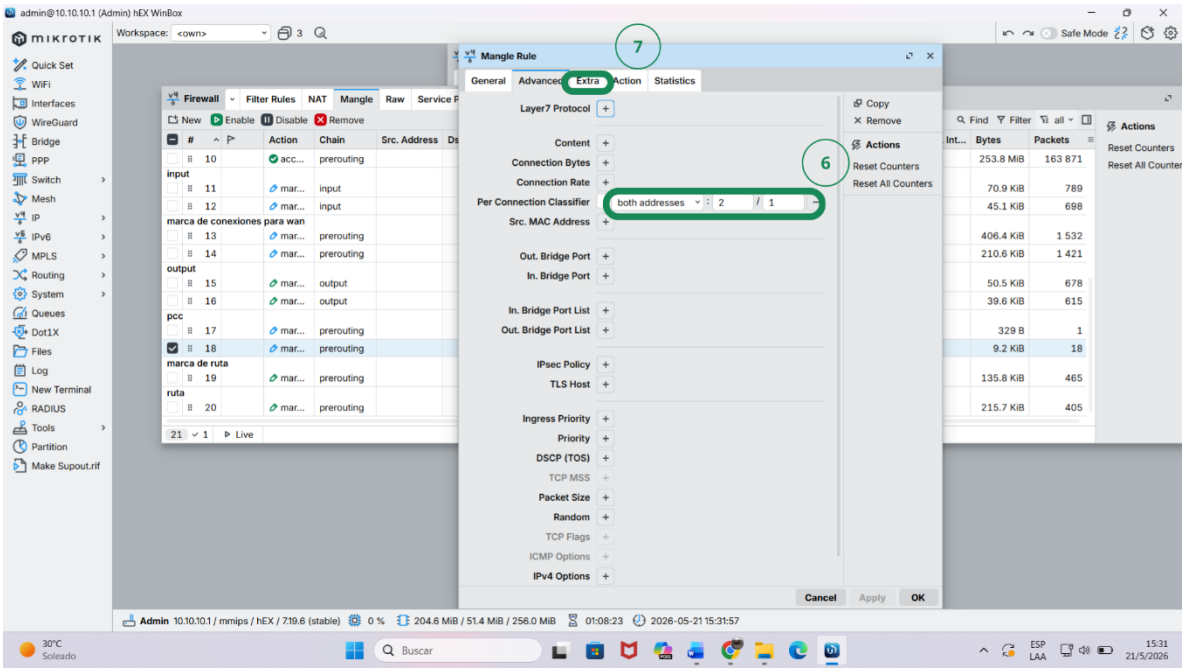
***Figura 68.*** *Regla del PCC para WAN2.*




*Nota.* Elaboración propia.

En la Figura 68 se creó la misma regla del PCC aplicada a la interfaz WAN2. Mediante la opción New, se abrió la ventana Mangle Rule, en la que se estableció la cadena prerouting, se seleccionó la interfaz LAN, en este caso bridge-wisp, y, en Connection Mark, la opción no-mark para continuar con la pestaña Advanced.

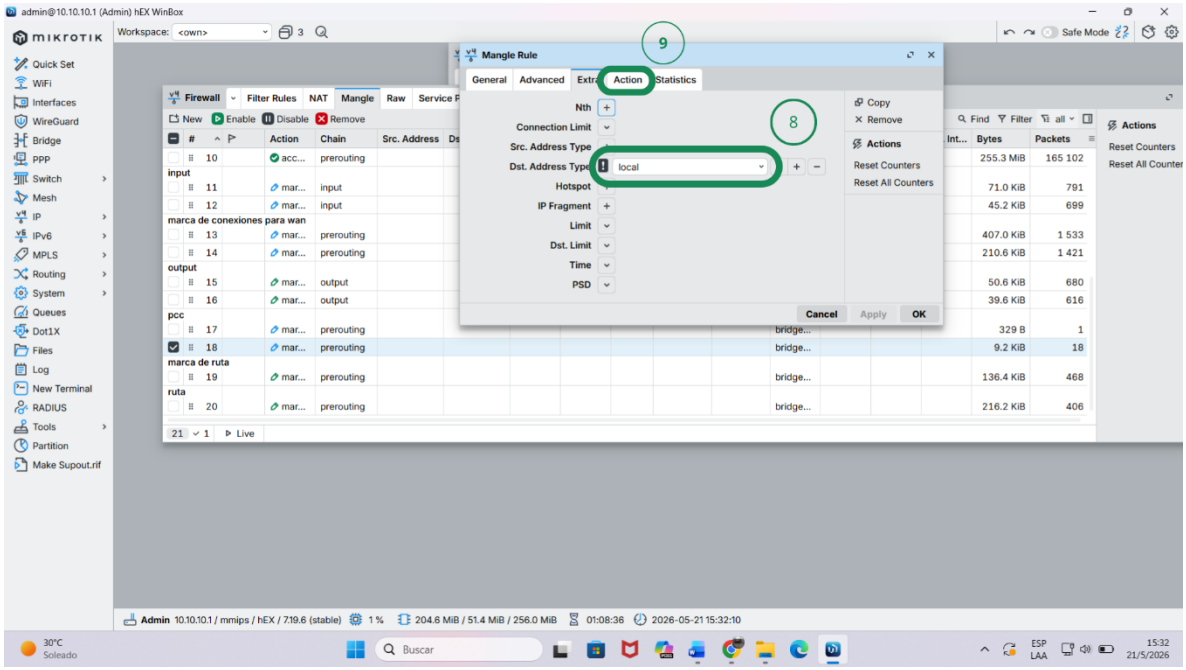
***Figura 69.*** *Configuración del PCC en la pestaña Advanced para WAN2.*




*Nota.* Elaboración propia.

En la Figura 69, en el apartado Per Connection Classifier, se seleccionó la opción both addresses y se mantuvo el denominador de 2, correspondiente a los dos enlaces de internet. En este caso, se asignó el índice 1, correspondiente al segundo enlace WAN; posteriormente, se continuó con la pestaña Extra.

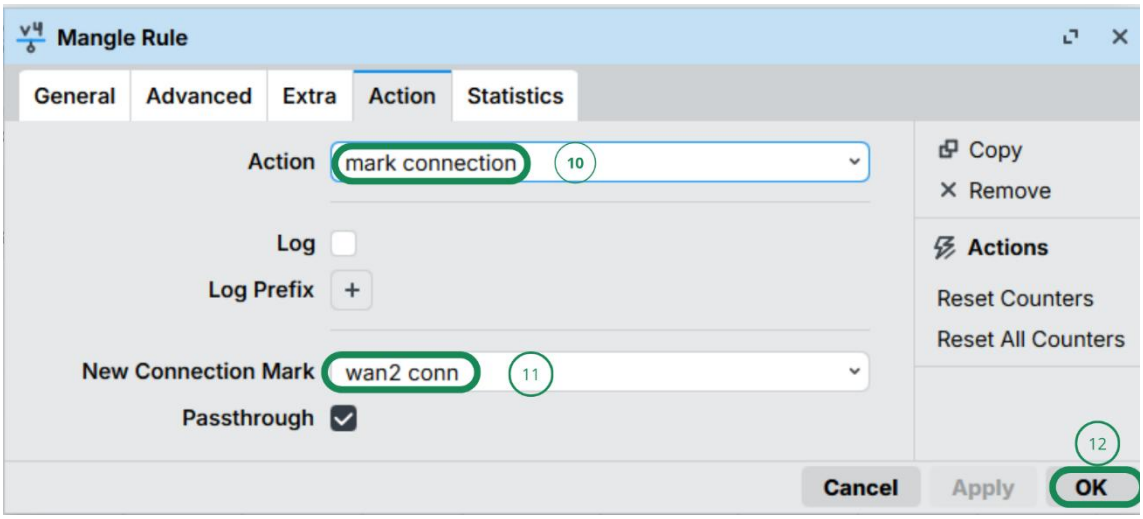
***Figura 70.*** *Configuración del PCC en la pestaña Extra para WAN2.*




*Nota.* Elaboración propia.

En la Figura 70, en el apartado Dst. Address Type, se seleccionó la opción local y se marcó el recuadro correspondiente, con lo que apareció el signo de admiración; posteriormente, se continuó con la pestaña Action.

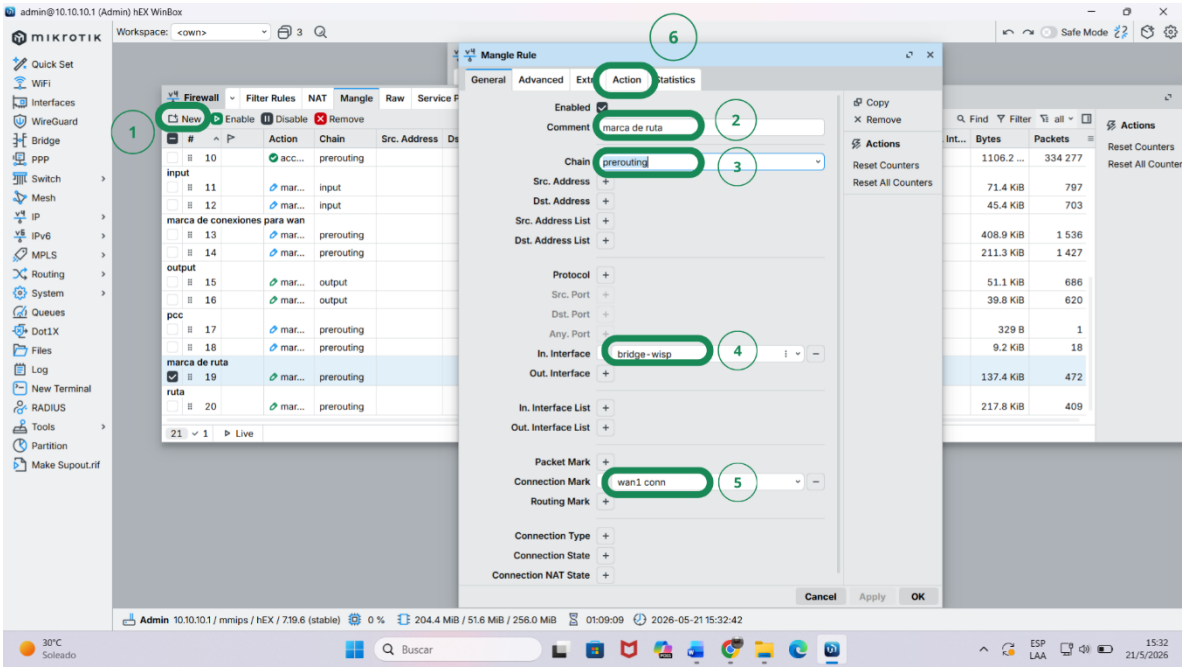
***Figura 71.*** *Configuración del PCC en la pestaña Action para WAN2.*




*Nota.* Elaboración propia.

En la Figura 71, en el apartado Action, se seleccionó la opción mark connection y, en New Connection Mark, la marca wan2 conn; posteriormente, se guardó la regla con la opción OK.

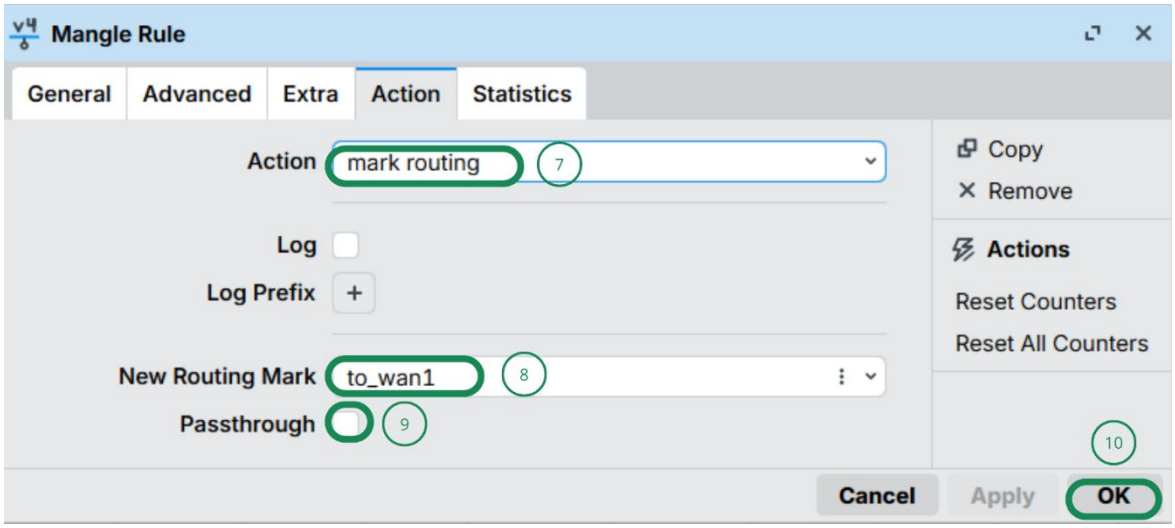
***Figura 72.*** *Configuración de la marca de ruta.*




*Nota.* Elaboración propia.

En la Figura 72 se creó la regla de marca de ruta correspondiente a las conexiones ya marcadas que ingresan por la interfaz LAN. Mediante la opción New, se abrió la ventana Mangle Rule, en la que se registró el comentario “marca de ruta”, se estableció la cadena prerouting, se seleccionó la interfaz LAN, en este caso bridge-wisp, y, en Connection Mark, la marca wan1 conn para continuar con la pestaña Action.

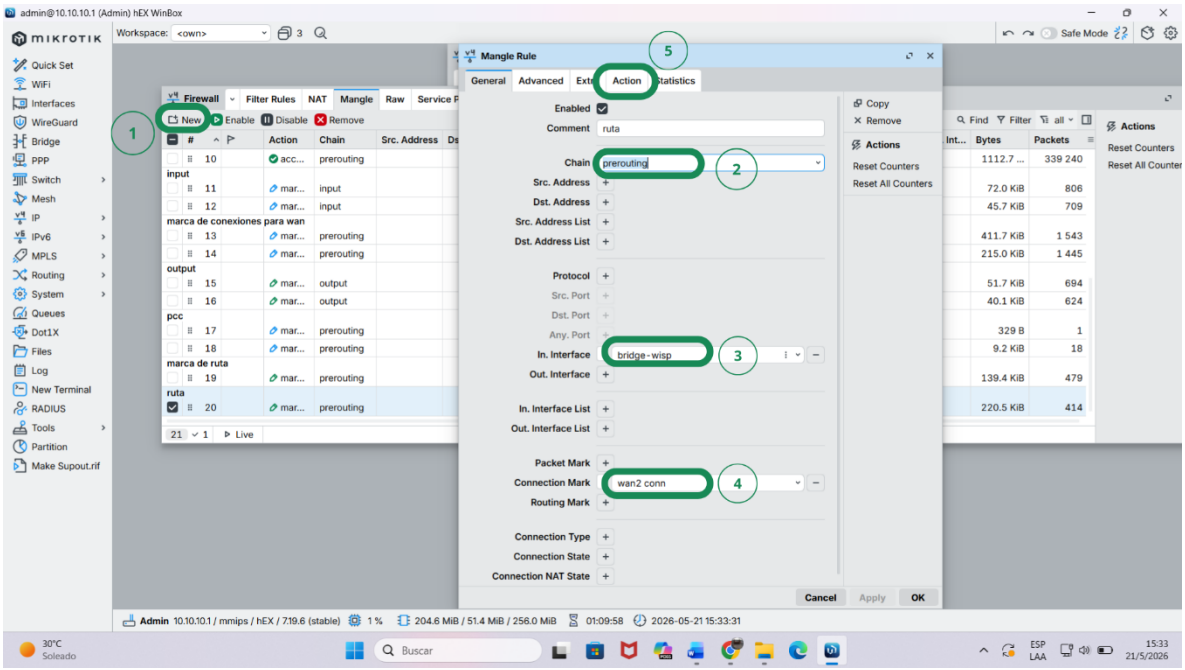
***Figura 73.*** *Configuración de la marca de ruta en la pestaña Action.*




*Nota.* Elaboración propia.

En la Figura 73, en el apartado Action, se seleccionó la opción mark routing; en New Routing Mark, la marca to_wan1; se desactivó la opción Passthrough; y se guardó la regla con la opción OK.

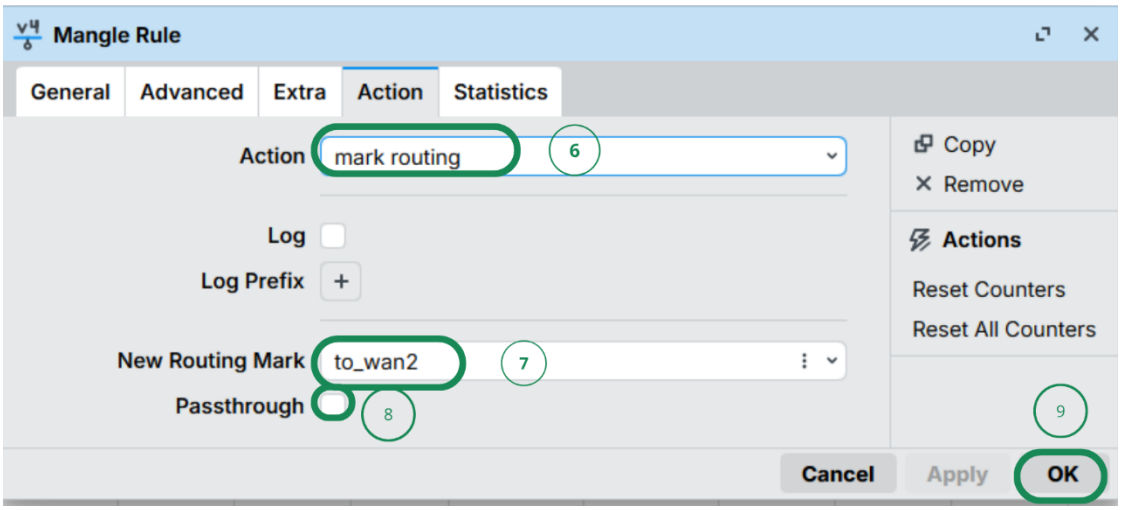
***Figura 74.*** *Configuración de la marca de ruta para WAN2.*




*Nota.* Elaboración propia.

En la Figura 74 se creó la misma regla de marca de ruta aplicada a la interfaz WAN2. Mediante la opción New, se abrió la ventana Mangle Rule, en la que se estableció la cadena prerouting, se seleccionó la interfaz LAN, en este caso bridge-wisp, y, en Connection Mark, la marca wan2 conn para continuar con la pestaña Action.

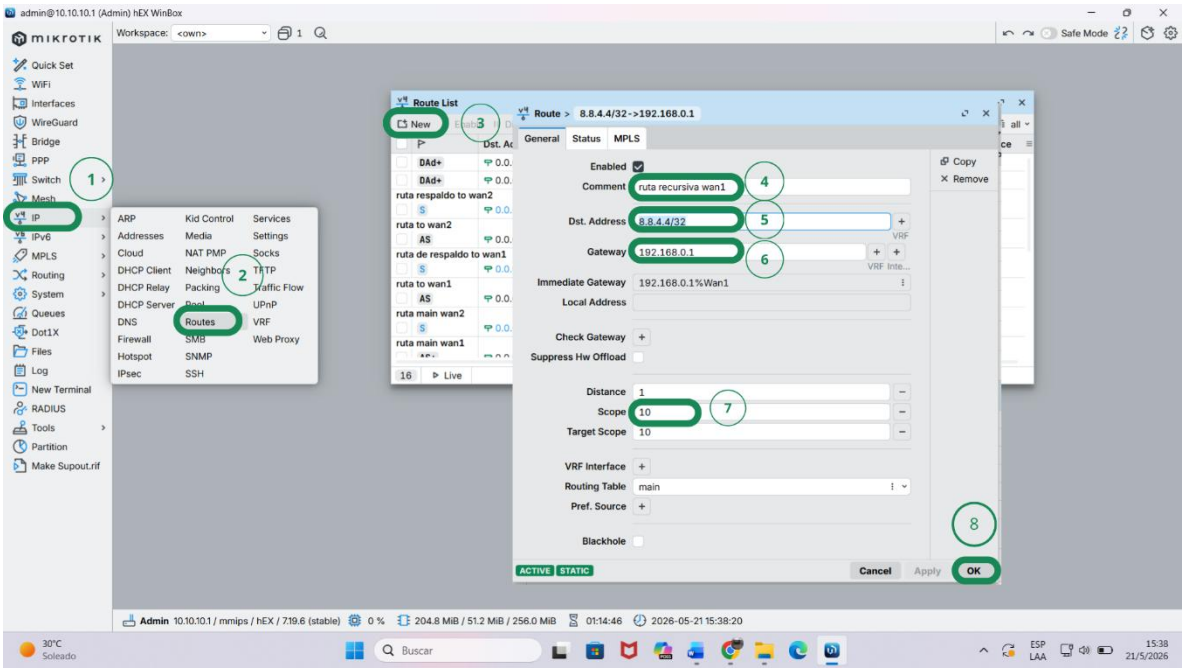
***Figura 75.*** *Configuración de la marca de ruta para WAN2 en la pestaña Action.*




*Nota.* Elaboración propia.

En la Figura 75, en el apartado Action, se seleccionó la opción mark routing; en New Routing Mark, la marca to_wan2; se desactivó la opción Passthrough; y se guardó la regla con la opción OK. Con esta regla se completó la configuración de Mangle, compuesta por un total de doce reglas.

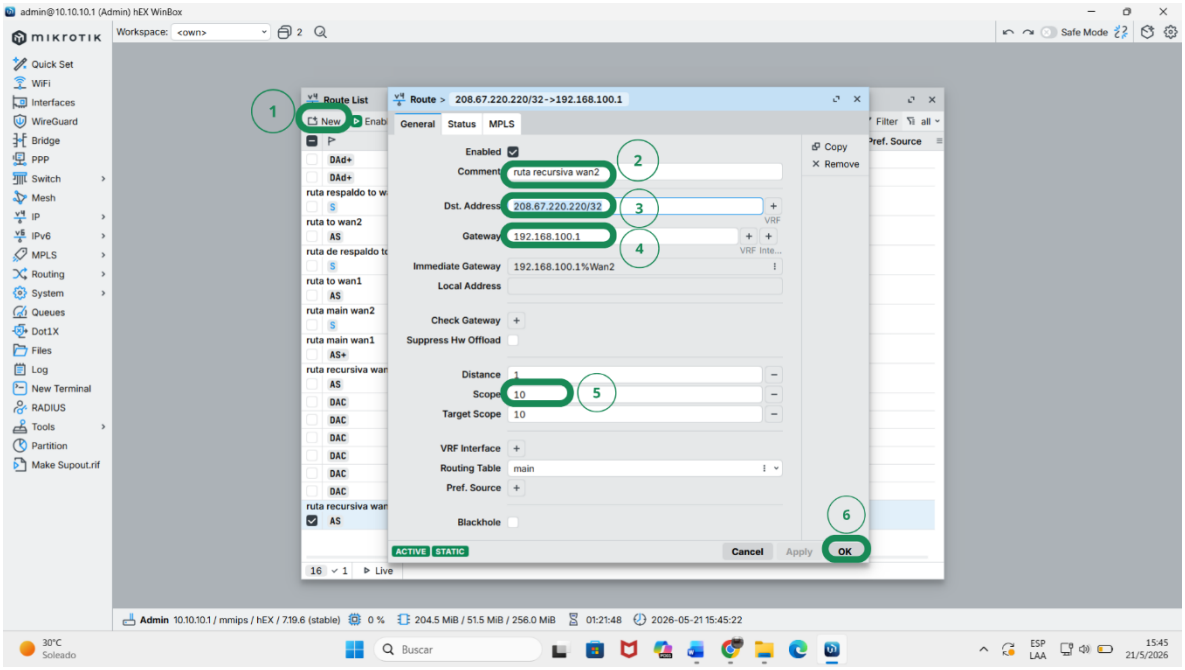
***Figura 76.*** *Creación de rutas estáticas.*




*Nota.* Elaboración propia.

En la Figura 76 se presenta la creación de las rutas estáticas con mecanismo de failover. De esta manera, si uno de los enlaces WAN presenta una falla y queda temporalmente inactivo, el tráfico se redirige automáticamente a través del enlace disponible, lo que permite mantener la continuidad del servicio. Para ello, se accedió a IP > Routes y, mediante la opción New, se registró el comentario “ruta recursiva wan1”; en el campo Dst. Address se configuró la dirección 8.8.4.4, correspondiente al DNS de Google; en Gateway, la dirección 192.168.0.1, correspondiente a la puerta de enlace de WAN1; y en Scope se mantuvo el valor 10. Finalmente, se guardó la configuración con la opción OK.

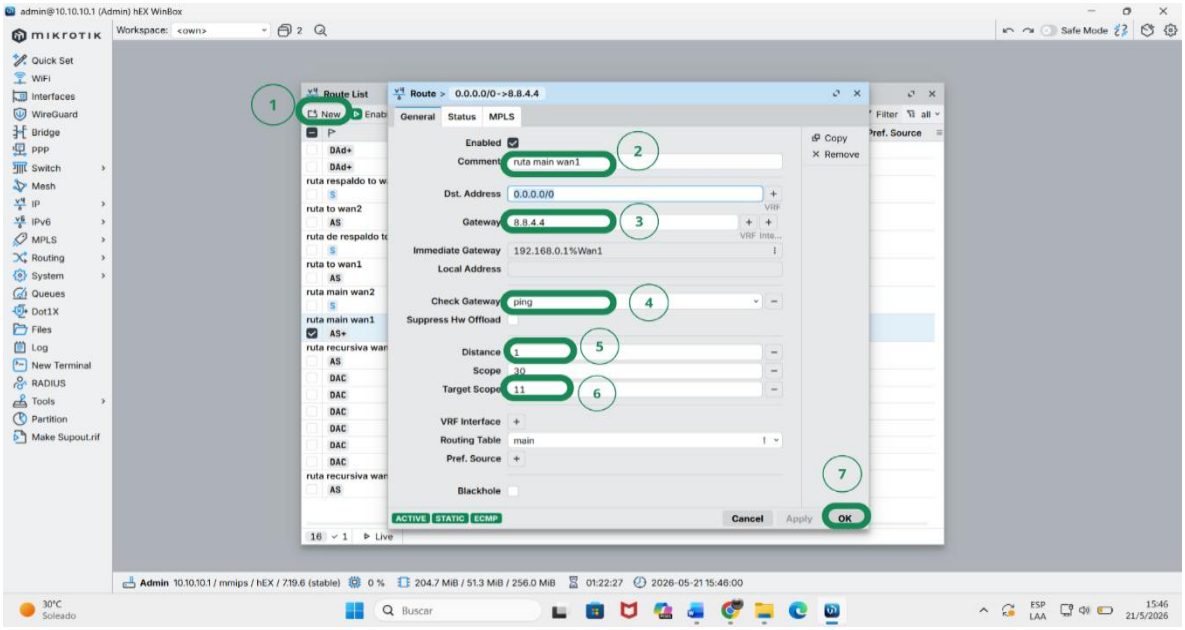
***Figura 77.*** *Creación de rutas estáticas para WAN2.*




*Nota.* Elaboración propia.

En la Figura 77 se repitió el proceso anterior para la interfaz WAN2. Mediante la opción New, se registró el comentario “ruta recursiva wan2”; en el campo Dst. Address se configuró la dirección 208.67.220.220, correspondiente al DNS de OpenDNS; en Gateway, la dirección 192.168.100.1, correspondiente a la puerta de enlace de WAN2; y en Scope se mantuvo el valor 10. Finalmente, se guardó la configuración con la opción OK.

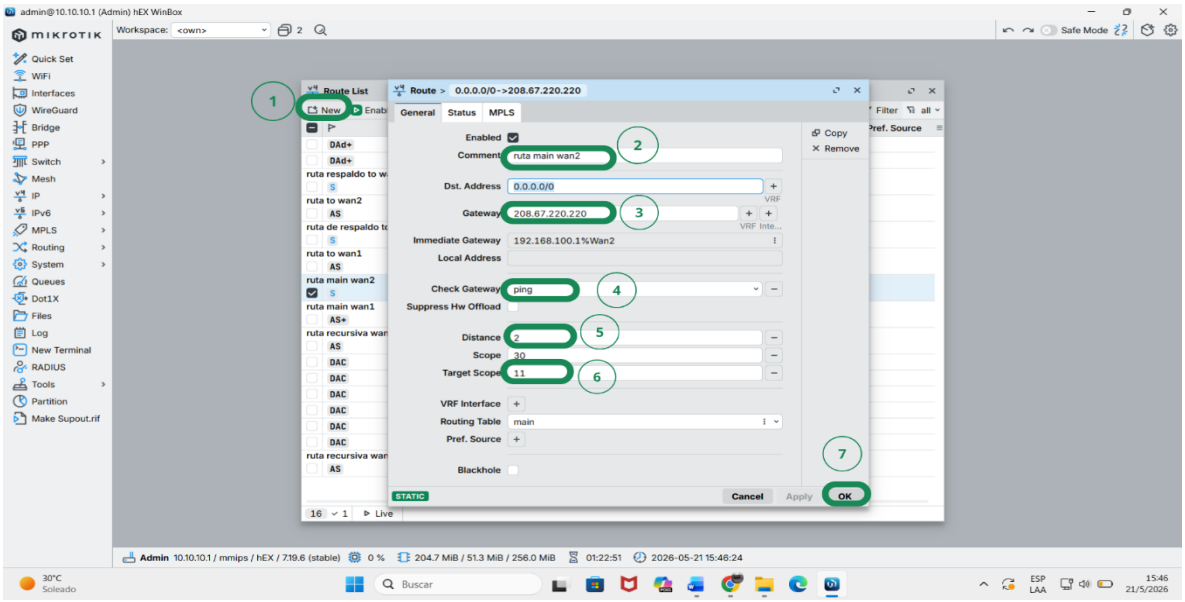
***Figura 78.*** *Regla para la ruta main de la WAN1.*




*Nota.* Elaboración propia.

En la Figura 78 se creó la regla correspondiente a la ruta main de la WAN1. Mediante la opción New, se registró el comentario “ruta main wan1”; en el campo Gateway se configuró la dirección 8.8.4.4; en Check Gateway, la opción *ping*; en Distance, el valor 1; y en Target Scope, el valor 11, superior al Scope empleado en las rutas configuradas previamente. Finalmente, se guardó la configuración con la opción OK.

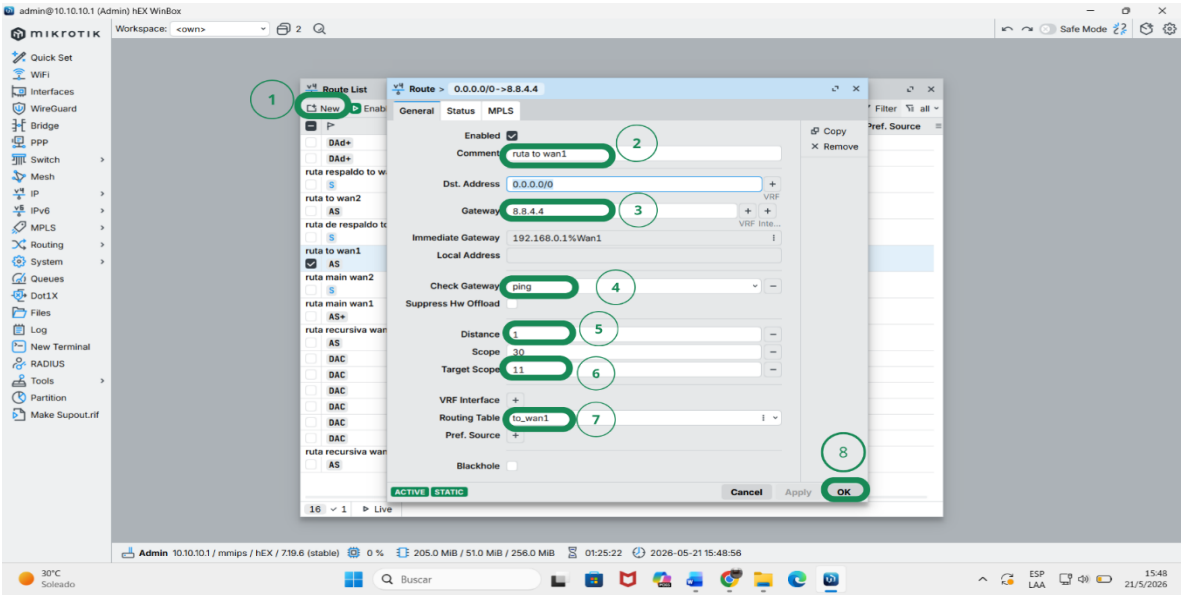
***Figura 79.*** *Regla para la ruta main de la WAN2.*




*Nota.* Elaboración propia.

En la Figura 79 se creó la ruta main correspondiente a la WAN2. Mediante la opción New, se configuró en Gateway la dirección 208.67.220.220; en Check Gateway, la opción ping; en Distance, el valor 2; y en Target Scope, el valor 11. Finalmente, se guardó la configuración con la opción OK.

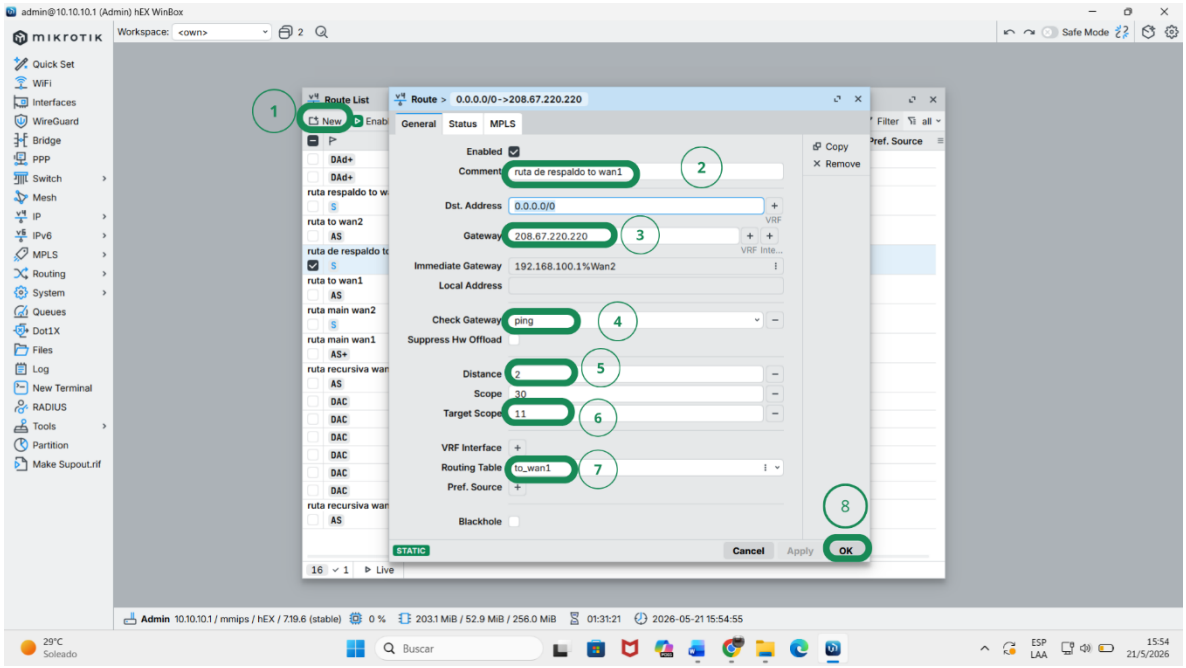
***Figura 80.*** *Regla para la marca de ruta to_wan1.*




*Nota.* Elaboración propia.

En la Figura 80 se creó la regla correspondiente a la marca de ruta to_wan1. Mediante la opción New, se registró el comentario “ruta to wan1”; en Gateway se configuró la dirección 8.8.4.4; en Check Gateway, la opción ping; en Distance, el valor 1; y en Target Scope, el valor 11. Posteriormente, en Routing Table, se seleccionó to_wan1 y se guardó la configuración con la opción OK.

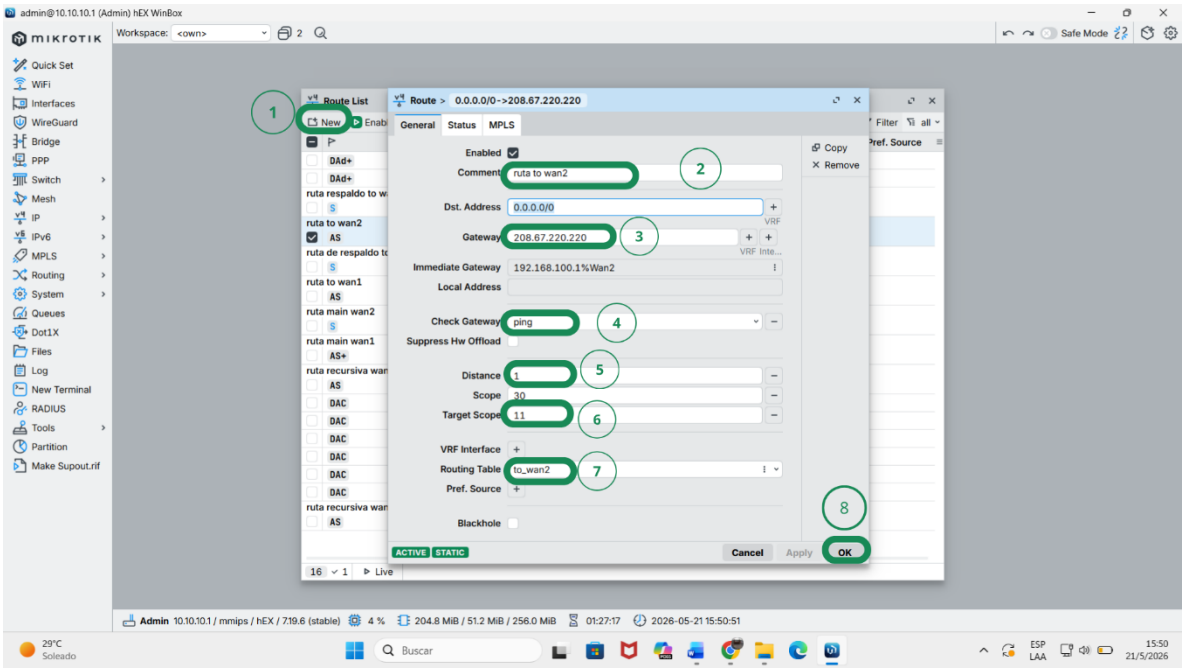
***Figura 81.*** *Creación de la ruta de respaldo para la marca de ruta to_wan1.*




*Nota.* Elaboración propia.

En la Figura 81 se creó la ruta de respaldo para el tráfico asociado a la marca de ruta to_wan1. Mediante la opción New, se abrió la ventana Route, en la que se registró el comentario “ruta de respaldo to wan1”; en Gateway se configuró la dirección 208.67.220.220; en Check Gateway, la opción ping; en Distance, el valor 2; y en Target Scope, el valor 11. Posteriormente, en Routing Table, se seleccionó to_wan1 y se guardó la configuración con la opción OK.

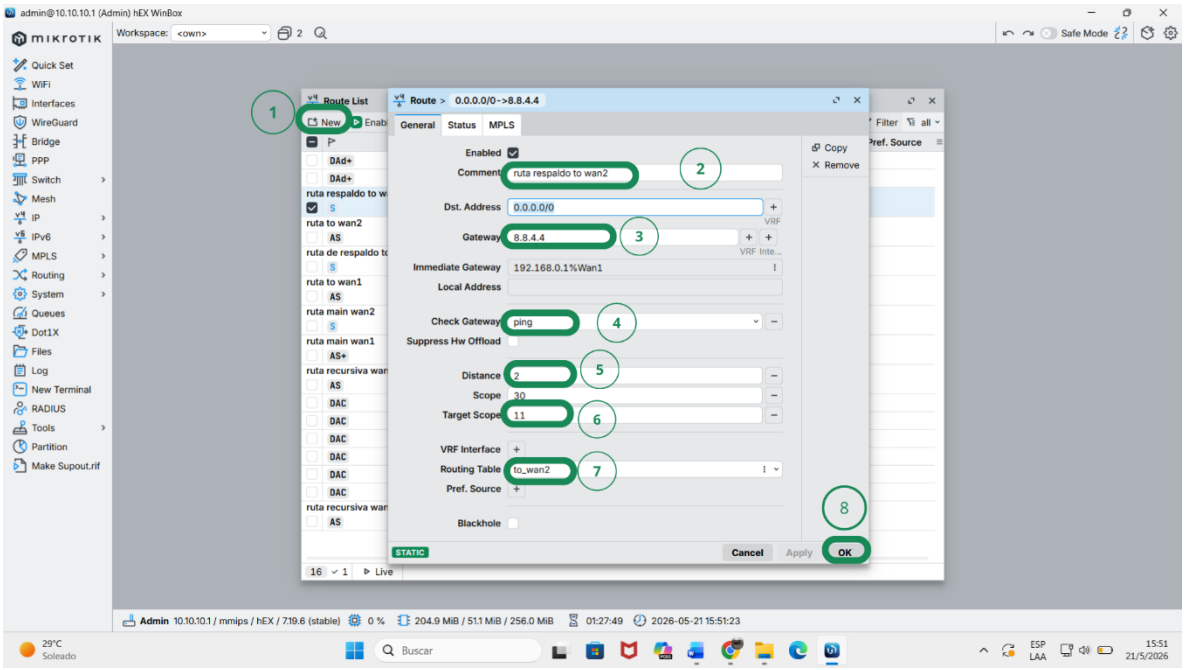
***Figura 82.*** *Regla para la marca de ruta to_wan2.*




*Nota.* Elaboración propia.

La Figura 82 muestra la creación de la regla aplicada a todo el tráfico asociado a la marca de ruta to_wan2. Mediante la opción New, se abrió la ventana Route, en la que se registró el comentario “ruta to wan2”; en Gateway se estableció la dirección 208.67.220.220; en Check Gateway, la opción ping; en Distance, el valor 1; y en Target Scope, el valor 11. Finalmente, en Routing Table, se seleccionó to_wan2 y se guardó la configuración.

***Figura 83.*** *Ruta de respaldo para WAN2.*



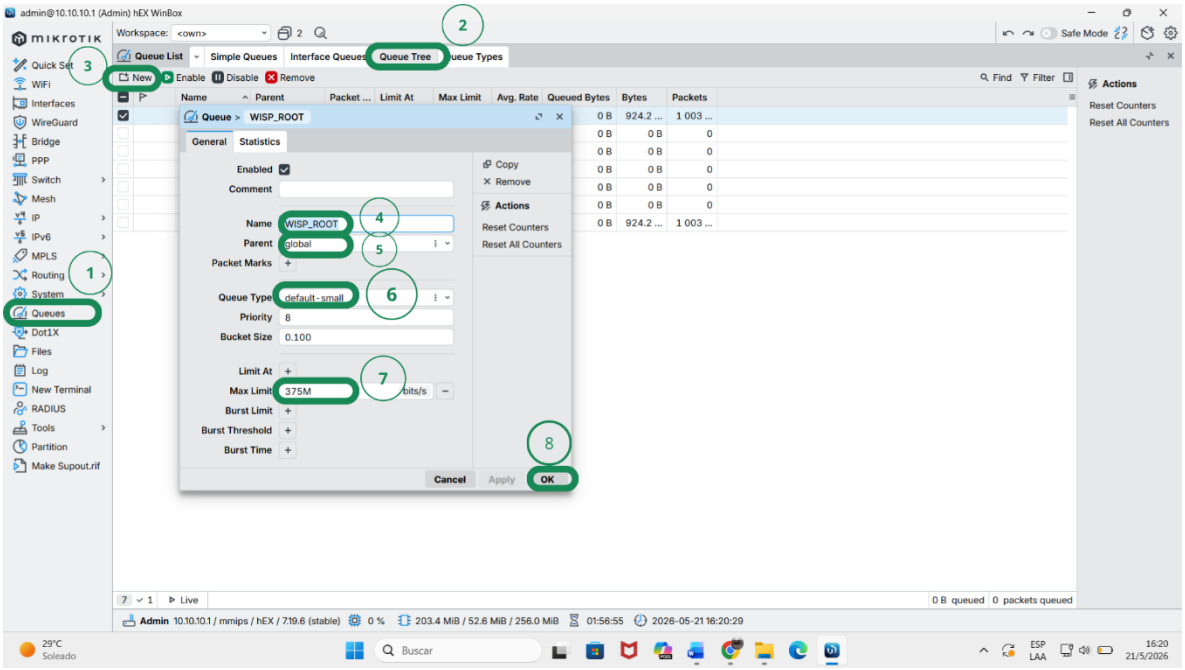

*Nota.* Elaboración propia.

La Figura 83 muestra la ruta de respaldo correspondiente a la WAN2. Mediante la opción New, se abrió la ventana Route, en la que se asignó el comentario “ruta de respaldo to wan2”; en Gateway se estableció la dirección 8.8.4.4; en Check Gateway, la opción ping; en Distance, el valor 2; y en Target Scope, el valor 11. Posteriormente, en Routing Table, se seleccionó to_wan2 y se guardó la configuración.

### 3.3.6. Implementación de la calidad de servicio (QoS)

La calidad de servicio (QoS) se implementa con el objetivo de administrar eficientemente el ancho de banda disponible y establecer diferentes niveles de prioridad para los usuarios de la red. Mediante esta configuración, es posible garantizar un mejor rendimiento para los servicios críticos y optimizar la distribución de los recursos de red según las necesidades de cada grupo de usuarios. A continuación, se presenta la configuración realizada.

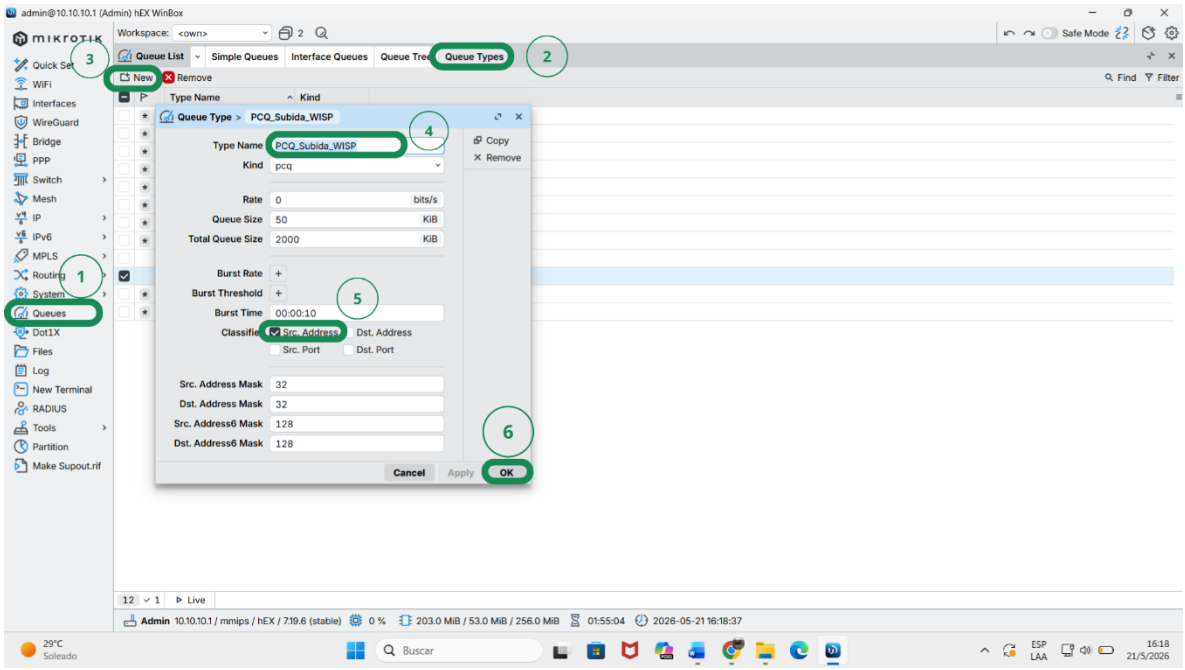
***Figura 84.*** *Configuración Queues.*




*Nota.* Elaboración propia.

En la Figura 84 se presenta la creación de la cola Wisp_Root, la cual funciona como raíz dentro del *Queue Tree*. Para ello, se accedió al apartado Queues y, dentro de Queue Tree, se seleccionó la opción New; en el campo Name se asignó el nombre Wisp_Root; en Parent se seleccionó global; en Queue Type, la opción default; y en Max Limit se configuró un ancho de banda máximo de 375 Mbps. Finalmente, se guardó la configuración con la opción OK.

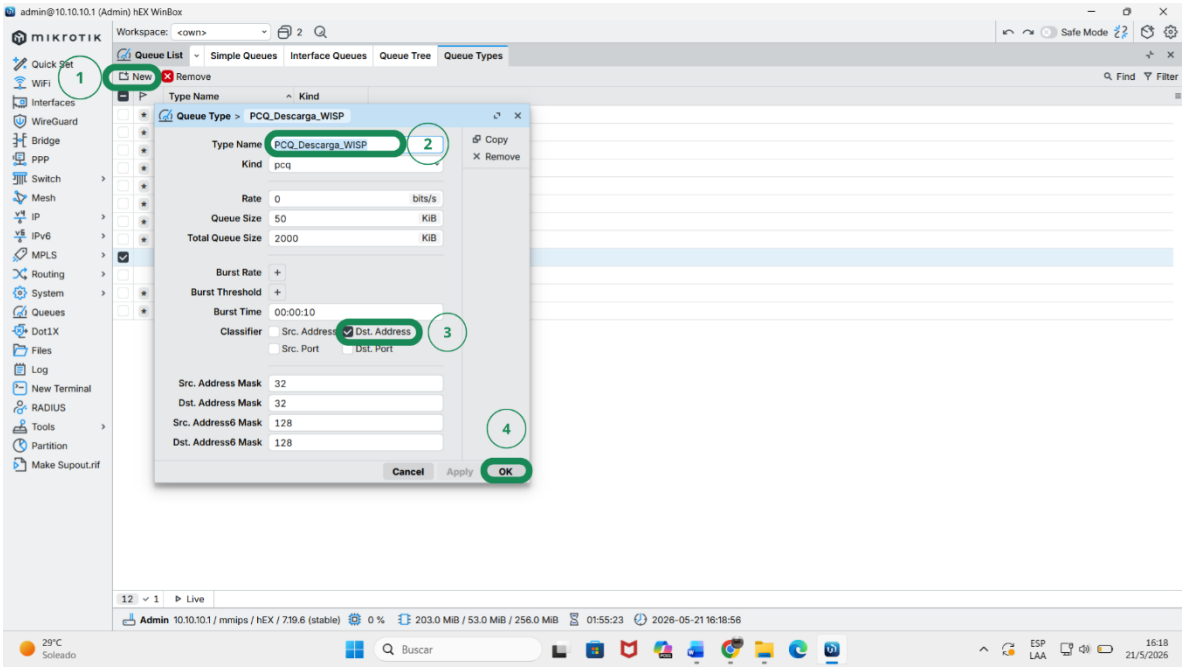
***Figura 85.*** *Queue PCQ de subida.*




*Nota.* Elaboración propia.

En la Figura 85 se presenta la configuración del Queue PCQ (Per Connection Queue), un mecanismo de gestión del ancho de banda que permite crear colas dinámicas para cada usuario. Para ello, se accedió a Queue Type y, mediante la opción New, se asignó en Type Name el nombre PCQ_Subida_Wisp; en Kind, la opción pcq; y en Classifier, el parámetro Src. Address. Finalmente, se guardó la configuración con la opción OK.

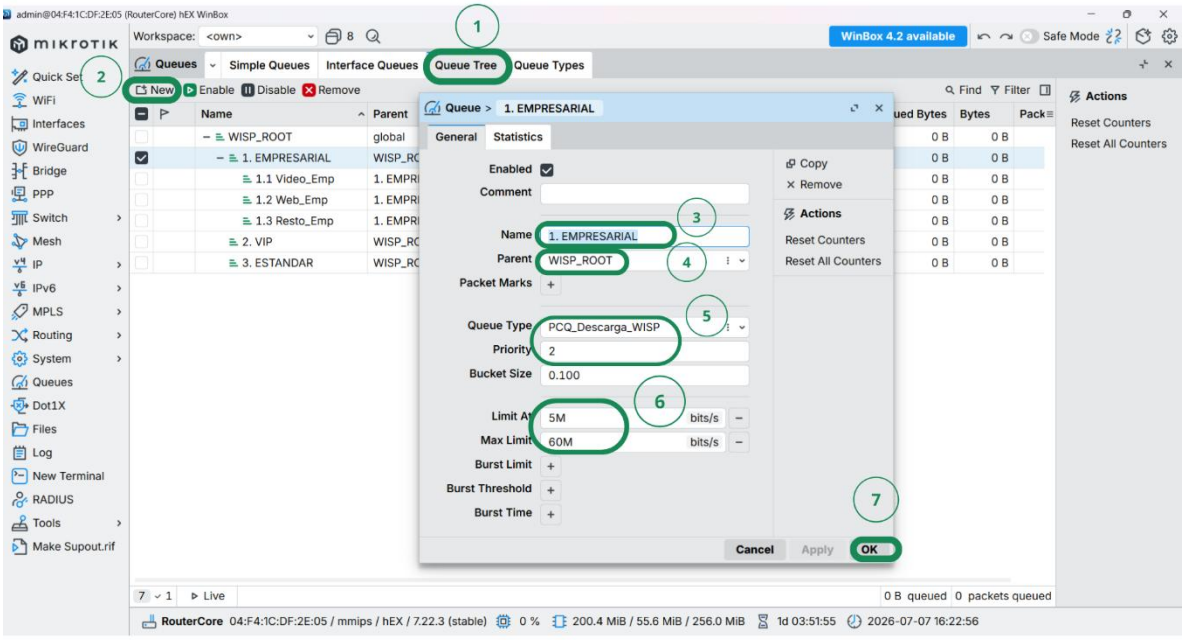
***Figura 86.*** *Queue PCQ de descarga.*




*Nota.* Elaboración propia.

En la Figura 86 se presenta la configuración del Queue PCQ (Per Connection Queue) correspondiente al tráfico de descarga. Mediante la opción New, se asignó en Type Name el nombre PCQ_Descarga_Wisp; en Kind, la opción pcq; y en Classifier, el parámetro Dst. Address. Finalmente, se guardó la configuración con la opción OK.

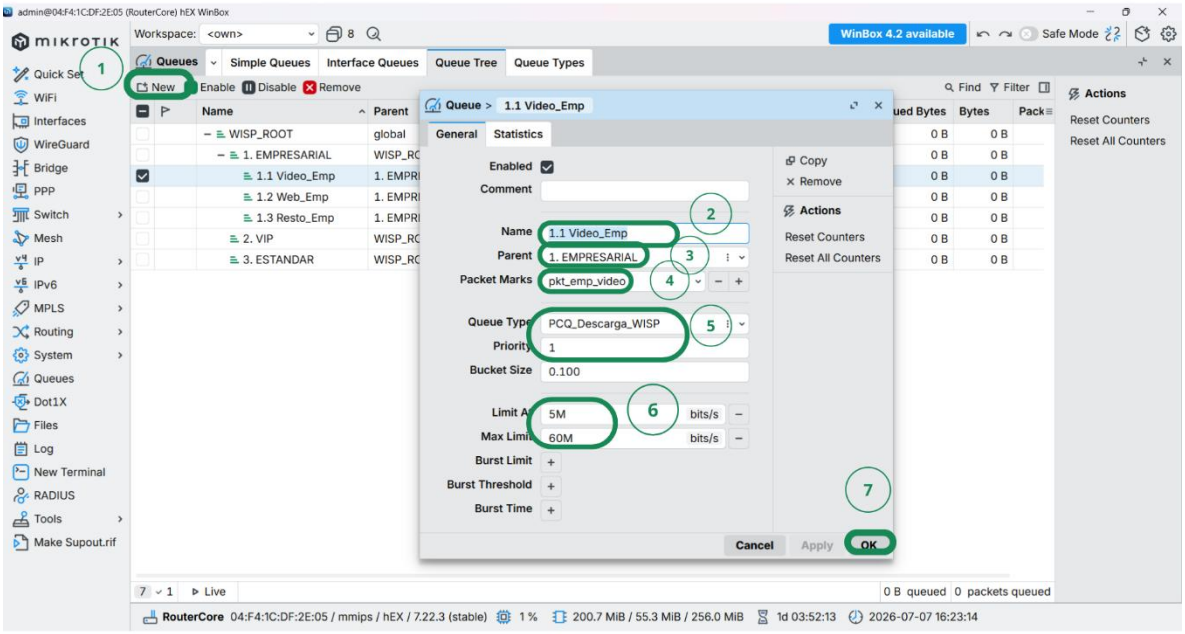
***Figura 87.*** *Cola de servicio empresarial.*




*Nota.* Elaboración propia.

La Figura 87 muestra la configuración de la cola de servicio empresarial, asociada a la cola principal Wisp_Root con el fin de gestionar el tráfico y distribuirlo de forma equitativa entre los usuarios de este plan. Para ello, se accedió a Queue Tree y, mediante la opción New, se asignó en Name el nombre 1. Empresarial; en Parent, la cola Wisp_Root; en Queue Type, la opción PCQ_Descarga_Wisp; y en Priority, el nivel 2. Posteriormente, en Limit At, se estableció un ancho de banda mínimo de 5 Mbps y, en Max Limit, un ancho de banda máximo de 60 Mbps. Finalmente, se guardó la configuración con la opción OK.

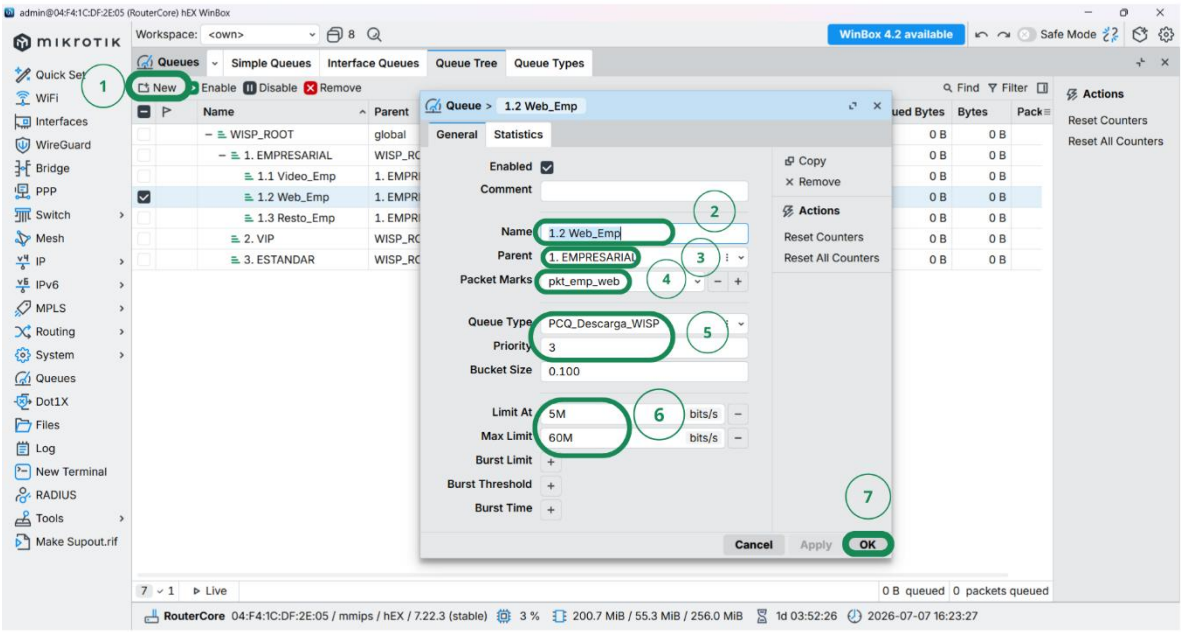
***Figura 88.*** *Cola de servicio de video empresarial.*




*Nota.* Elaboración propia.

En la Figura 88 se presenta la configuración de la cola de servicio de video del plan empresarial, destinada exclusivamente al tráfico de video. Dentro de la ventana Queue Tree, mediante la opción New, se asignó en Name el nombre 1.1 Video_emp; en Parent, la cola 1. Empresarial; en Packet Marks, la marca pkt_emp_video; en Queue Type, la opción PCQ_Descarga_Wisp; y en Priority, el nivel 1. Posteriormente, en Limit At, se estableció un ancho de banda mínimo de 5 Mbps y, en Max Limit, un máximo de 60 Mbps, lo que asegura una adecuada calidad de experiencia en aplicaciones de video. Finalmente, se guardó la configuración con la opción OK.

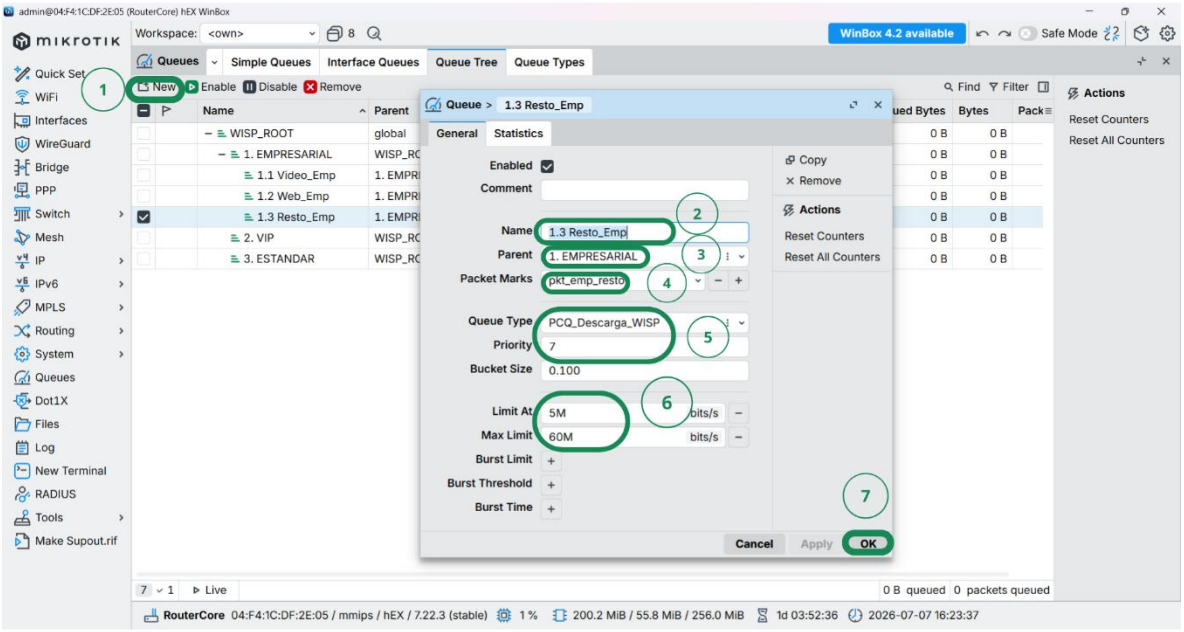
***Figura 89.*** *Cola de servicio web empresarial.*




*Nota.* Elaboración propia.

En la Figura 89 se presenta la creación de la cola de servicio web del plan empresarial, destinada a gestionar el tráfico de navegación. Mediante la opción New, se asignó en Name el nombre 1.2 Web_Emp y, en Parent, la cola 1. Empresarial, con el fin de que esta nueva cola herede las políticas generales de ancho de banda definidas para la categoría empresarial. En Packet Marks se seleccionó la marca pkt_emp_web, creada previamente mediante reglas Mangle para identificar el tráfico de navegación web. En Queue Type se seleccionó la opción PCQ_Descarga_Wisp y, en Priority, el nivel 3 dentro de la jerarquía de colas del plan empresarial. Posteriormente, en Limit At, se estableció un ancho de banda mínimo de 5 Mbps y, en Max Limit, un máximo de 60 Mbps para la navegación web. Finalmente, se guardó la configuración con la opción OK.

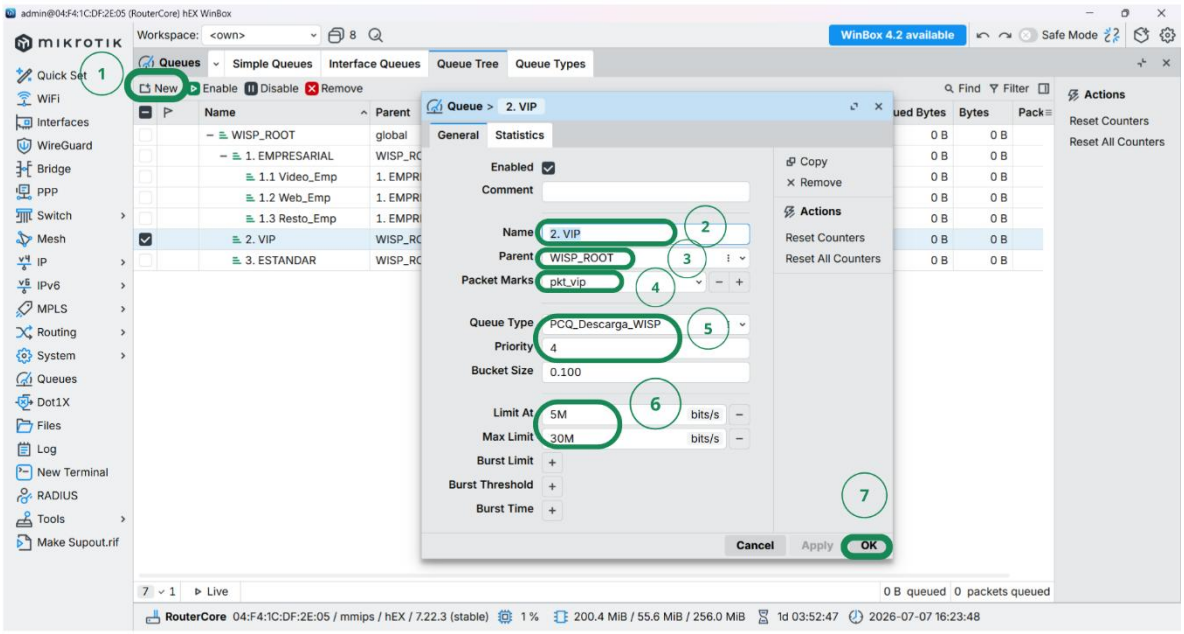
***Figura 90.*** *Cola de servicio Resto_emp.*




*Nota.* Elaboración propia.

En la Figura 90 se presenta la creación de la cola de servicio Resto_emp, destinada a otros tipos de tráfico, como correos, descargas o almacenamiento en la nube. Mediante la opción New, se asignó en Name el nombre 1.3 Resto_Emp y, en Parent, la cola 1. Empresarial, con el fin de mantener las políticas generales de ancho de banda del plan empresarial. En Packet Marks se seleccionó la marca pkt_emp_resto, creada previamente mediante reglas Mangle; en Queue Type, la opción PCQ_Descarga_Wisp; y en Priority, el nivel 7. Posteriormente, en Limit At, se estableció un ancho de banda mínimo de 5 Mbps y, en Max Limit, un máximo de 60 Mbps. Finalmente, se guardó la configuración con la opción OK.

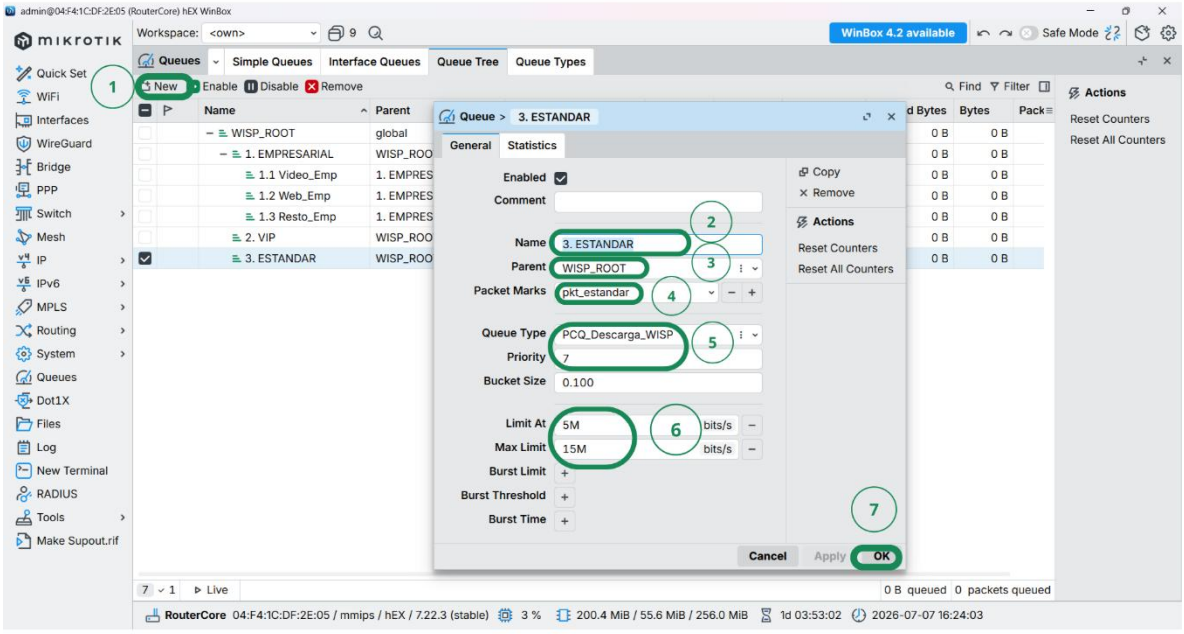
***Figura 91.*** *Cola de servicio VIP.*




*Nota.* Elaboración propia.

En la Figura 91 se presenta la creación de la cola de servicio VIP, destinada a usuarios que requieren mayor prioridad para aplicaciones sensibles a la latencia y una mejor calidad de servicio (QoS). Dentro de la ventana Queue Tree, mediante la opción New, se asignó en Name el nombre 2. VIP y, en Parent, la cola Wisp_Root, de modo que esta cola forme parte de la jerarquía general de administración del ancho de banda. En Packet Marks se seleccionó la marca pkt_vip, creada previamente mediante reglas Mangle; en Queue Type, la opción PCQ_Descarga_Wisp; y en Priority, el nivel 4. Posteriormente, en Limit At, se estableció un ancho de banda mínimo de 5 Mbps y, en Max Limit, un máximo de 30 Mbps. Finalmente, se guardó la configuración con la opción OK.

***Figura 92.*** *Cola de servicio estándar.*




*Nota.* Elaboración propia.

En la Figura 92 se presenta la creación de la cola de servicio estándar, destinada a los usuarios residenciales con requerimientos básicos de conectividad. Mediante la opción New, se asignó en Name el nombre 3. Estándar y, en Parent, la cola Wisp_Root, de modo que forme parte de la jerarquía general de administración del ancho de banda. En Packet Marks se seleccionó la marca pkt_estándar, creada previamente mediante reglas Mangle; en Queue Type, la opción PCQ_Descarga_Wisp; y en Priority, el nivel 7. Posteriormente, en Limit At, se estableció un ancho de banda mínimo de 5 Mbps y, en Max Limit, un máximo de 15 Mbps. Finalmente, se guardó la configuración con la opción OK.

### 3.4. Herramientas para análisis y monitoreo de red

El monitoreo de red representa una actividad fundamental en las infraestructuras de un WISP (proveedor de servicios de internet inalámbrico), ya que permite evaluar el estado, la eficiencia y la confiabilidad de los servicios prestados. Las herramientas diseñadas para este

propósito deben ser capaces de operar en varias capas del modelo OSI, soportar múltiples protocolos y proporcionar análisis tanto activo como pasivo. A continuación, se presenta una revisión técnica de cuatro herramientas ampliamente utilizadas en entornos de telecomunicaciones, haciendo énfasis en su arquitectura, protocolos compatibles, mecanismos operativos y aplicabilidad en escenarios de despliegue reales.

### 3.4.1. Wireshark

Wireshark es una de las herramientas más completas para el análisis pasivo de redes. Trabaja desde la capa de enlace de datos (capa 2) hasta la capa de aplicación (capa 7) del modelo OSI. Su funcionamiento se basa en el *sniffing* de paquetes; es decir, la herramienta captura el tráfico que circula por una interfaz de red e interpreta los paquetes en tiempo real, lo que permite una visualización estructurada por protocolo. Es compatible con más de 200 protocolos, entre los que se incluyen TCP, UDP, HTTP, DNS y TLS. Sus filtros por dirección IP, puerto y tipo de protocolo hacen que esta herramienta resulte adecuada para auditorías de red, detección de intrusiones, análisis de fallos de conexión y validación de servicios en producción [19].

### 3.4.2. PRTG Network Monitor

PRTG es una solución de monitorización activa y pasiva que funciona con un modelo basado en sensores, lo que permite una alta granularidad de supervisión en tiempo real. Trabaja desde la capa de red (capa 3) hasta la capa de aplicación (capa 7) y soporta protocolos como SNMP, NetFlow, sFlow, WMI e ICMP. Los sensores se pueden configurar para medir variables como el uso del ancho de banda, la latencia, la disponibilidad de servicios o la temperatura de los dispositivos. Su arquitectura cliente-servidor permite centralizar la supervisión de múltiples nodos WISP, con alertas, gráficos históricos e interfaces web dinámicas [20].

### 3.4.3. Iperf3

Iperf3 es una herramienta de código abierto ampliamente utilizada para evaluar el rendimiento de redes IP mediante la medición de parámetros como el *throughput*, la pérdida de paquetes, el *jitter* y el ancho de banda disponible entre dos dispositivos. Su funcionamiento se basa en un modelo cliente-servidor, en el que un equipo genera tráfico y el otro lo recibe para calcular el desempeño de la comunicación. Esta herramienta realiza pruebas mediante los protocolos TCP y UDP y, además, es compatible con IPv4 e IPv6, lo que facilita la evaluación del rendimiento bajo diferentes condiciones de transmisión. Debido a su precisión, facilidad de implementación y bajo consumo de recursos, Iperf3 se utiliza ampliamente para validar el desempeño de redes WISP [21].

### 3.4.4. TamoGraph Site Survey

TamoGraph es una herramienta de análisis activo para las capas física (capa 1) y de enlace (capa 2). Su principal función es realizar estudios de sitio (*site survey*) en redes Wi-Fi, lo cual es fundamental en el despliegue de infraestructura WISP basada en enlaces punto a punto o punto a multipunto. Admite los estándares 802.11a/b/g/n/ac/ax/be y permite medir parámetros como SNR, RSSI, throughput y tasas de error. Además, genera mapas de calor que facilitan la planificación de la cobertura y permite evitar interferencias y zonas de sombra. Esta herramienta es especialmente útil en la fase de diseño de redes inalámbricas, en la que el rendimiento de RF constituye un aspecto crítico [22].

En la Tabla 12 se presenta, de forma resumida, la comparativa de las herramientas de gestión de red analizadas.

***Tabla 12.*** *Comparativa de herramientas de gestión de red.*

| **Herramienta** | **Tipo de licencia** | **Capacidades técnicas** | **Protocolos soportados** | **Aplicación en entornos WISP** |
|---|---|---|---|---|
| Wireshark | Gratuita / código abierto | Captura y análisis de paquetes, filtrado por protocolos, inspección profunda | TCP, UDP, ICMP, HTTP, DNS y ARP. | Diagnóstico de tráfico, detección de anomalías, auditoría de red |
| PRTG Network Monitor | Comercial (versión gratuita limitada) | Supervisión del ancho de banda, sensores, alertas, visualización en tiempo real | SNMP, NetFlow, WMI, HTTP y ping. | Monitoreo de enlaces críticos y desempeño de nodos WISP |
| Iperf3 | Gratuita / código abierto | Medición de throughput, jitter, pérdidas de paquetes y ancho de banda mediante pruebas cliente-servidor | TCP, UDP e IPv4/IPv6 | Evaluación de rendimiento de enlaces inalámbricos y optimización del ancho de banda |
| TamoGraph Site Survey | Comercial | Análisis de cobertura Wi-Fi, mapas de calor, simulación de redes inalámbricas | 802.11a/b/g/n/ac/ax | Diseño y optimización de redes de acceso WISP según el entorno físico |

*Nota.* Elaboración propia.

Aunque todas las herramientas analizadas ofrecen funcionalidades importantes para la administración y el diagnóstico de redes, Iperf3 resulta más adecuada para la evaluación del rendimiento, debido a que proporciona mediciones precisas de parámetros como throughput, jitter y pérdida de paquetes. Estos indicadores permiten evaluar de forma objetiva el rendimiento de la red.

### 3.5. Comparativa de técnicas de balanceo

El balanceo de carga en redes WISP (proveedor de servicios de internet inalámbrico) permite distribuir eficazmente el tráfico de datos entre varios enlaces WAN, lo que contribuye a mejorar el rendimiento, disminuir la latencia y garantizar la estabilidad de la red. En este estudio se comparan cuatro técnicas muy utilizadas: PCC (Per Connection Classifier), Round Robin, Least Connections e IP Hashing. La comparación se realiza desde un punto de vista documental, a partir de los valores reportados en la literatura técnica consultada. Para ello, se consideran métricas como la eficiencia de persistencia, el comportamiento ante tráfico variable y la latencia promedio en escenarios típicos de redes inalámbricas comunitarias y empresariales. Se consideran aspectos fundamentales, como la capa del modelo OSI en la que operan, los protocolos que utilizan, su eficiencia técnica y su idoneidad para redes WISP [23].

#### 3.5.1. PCC (Per Connection Classifier)

La técnica Per Connection Classifier (PCC) clasifica el tráfico de red según atributos propios de cada conexión: dirección IP de origen, dirección IP de destino, puertos y protocolos de transporte. Esta técnica funciona principalmente en la capa 3 (red) y la capa 4 (transporte) del modelo OSI. Su lógica se basa en funciones hash que combinan estos atributos para asegurar que todos los paquetes que pertenecen a una misma sesión se enruten por el mismo enlace WAN. Esto evita la fragmentación de sesiones y garantiza una alta persistencia de conexión, característica importante en servicios como videollamadas, juegos en línea o transmisiones en vivo.

Los protocolos que participan en esta técnica son IP, TCP y UDP. Además, PCC presenta una alta efectividad en la gestión de tráfico TCP persistente. En pruebas controladas obtuvo una eficiencia técnica del 96,4 % en estabilidad de sesión con una latencia promedio de 22 ms, convirtiéndose en una de las técnicas más robustas para redes WISP con múltiples rutas activas.

Sin embargo, su implementación requiere conocimientos avanzados sobre la configuración de reglas de enrutamiento y marcado de paquetes, además de un dispositivo que soporte el procesamiento avanzado a nivel de capa de red.

### 3.5.2. Round Robin

Round Robin es una de las técnicas más antiguas y simples para realizar balanceo de carga. Se basa en la asignación por turnos de las nuevas conexiones entre los enlaces WAN disponibles, sin tener en cuenta la carga actual ni el estado de cada ruta. Opera únicamente en la capa 3 del modelo OSI y emplea el protocolo IP como base para el direccionamiento y enrutamiento. No analiza el contenido del paquete ni verifica la integridad de la sesión.

Round Robin es útil en entornos de bajo tráfico, cuando los enlaces disponibles tienen características similares en capacidad y latencia. En escenarios de prueba, esta técnica tuvo una eficiencia técnica del 83,7 %, con una latencia promedio de 38 ms. Su principal ventaja es la facilidad de configuración, ya que no necesita seguimiento de conexiones ni un análisis profundo del tráfico. Sin embargo, dado que no mantiene afinidad de conexión ni se adapta a las diferencias entre enlaces, su uso en redes WISP con tráfico variable o enlaces asimétricos puede provocar pérdida de paquetes, cortes de sesión y bajo rendimiento en servicios sensibles.

### 3.5.3. Least Connections

La técnica Least Connections envía el tráfico al enlace con menos conexiones activas en el momento de recibir una nueva petición. Esta lógica dinámica permite equilibrar la carga en tiempo real y optimizar de forma adaptativa el desempeño de la red.

Actúa principalmente en la capa 4 (transporte), aunque en ocasiones también se aplica a la capa 7 (aplicación), sobre todo cuando se integra con sistemas capaces de interpretar protocolos

como HTTP y HTTPS. Emplea protocolos como TCP y herramientas de monitorización como conntrack o NetFlow para llevar a cabo una contabilización activa de conexiones en cada enlace. En pruebas con tráfico mixto (navegación, video, descargas), Least Connections alcanzó un 89,5 % de eficiencia, con una latencia promedio de 25 ms. Se recomienda en aquellos entornos en los que el tráfico no es constante y se producen momentos puntuales de alta concurrencia.

El mayor inconveniente de esta técnica es que necesita sistemas stateful, es decir, que hagan un seguimiento activo de cada conexión en tiempo real. Esto requiere mayores recursos computacionales, así como un software de red capaz de hacer análisis dinámico.

### 3.5.4. IP Hashing

La técnica IP Hashing asigna conexiones a los enlaces de salida en función de un valor hash generado a partir de las direcciones IP de origen y, opcionalmente, de destino. Esta función determinista asegura que las conexiones de un cliente determinado siempre pasen por el mismo enlace, conservando la integridad de las sesiones en curso.

IP Hashing funciona en la capa 3 del modelo OSI y opera únicamente con el protocolo IP. Su eficacia depende de la estabilidad de las direcciones IP de los clientes, por lo que funciona mejor en entornos con direcciones IP estáticas o cuando se usa DHCP con reservas. Los algoritmos hash más habituales son XOR, CRC32 y MD5, los cuales permiten una distribución uniforme del tráfico siempre que exista una adecuada dispersión de las direcciones IP. En pruebas de laboratorio, el método alcanzó una eficiencia del 91,2 % y una latencia promedio de 29 ms. Es adecuado para aplicaciones como juegos en línea, conexiones bancarias, VPN y otros servicios que requieren mantener la continuidad de la sesión.

Sin embargo, en redes en las que muchos usuarios comparten la misma dirección IP, puede producirse un desequilibrio que sobrecargue un solo enlace, mientras que los demás permanecen infrautilizados. En la Tabla 13 se presenta un resumen de la comparación de técnicas de balanceo.

***Tabla 13.*** *Comparación de técnicas de balanceo de carga en redes WISP.*

| **Técnica** | **Capas OSI** | **Protocolos** | **Mecanismo técnico** | **Eficiencia** | **Latencia** | **Observaciones técnicas** |
|---|---|---|---|---|---|---|
| PCC (Per Connection Classifier) | 3 y 4 (red y transporte) | IP, TCP, UDP | Clasificación por hash de IP y puertos | 96,4 % | 22 ms | Alta persistencia. Adecuado para tráfico en tiempo real. |
| Round Robin | 3 (red) | IP | Asignación secuencial de nuevas conexiones | 83,7 % | 38 ms | Simple, pero poco eficiente con tráfico irregular. |
| Least Connections | 4 (y, opcional, 7) | TCP, conntrack | Asigna al enlace con menos conexiones activas | 89,5 % | 25 ms | Requiere monitoreo y resulta adecuado para tráfico dinámico. |
| IP Hashing | 3 (red) | IP, algoritmo hash | Hash de IP de origen y destino para mantener afinidad | 91,2 % | 29 ms | Eficaz con IP fija. Riesgo de desequilibrio con NAT. |

*Nota*. Las métricas de eficiencia y latencia se presentan como valores de referencia técnica basados en documentación consultada y pueden variar según las condiciones y características de la red.

Según el cuadro comparativo anterior, la técnica PCC (Per Connection Classifier) presenta el mayor grado de precisión y adaptabilidad para redes con múltiples tipos de tráfico y usuarios activos. Aunque su implementación puede resultar compleja en un primer momento, la posibilidad de personalizar los flujos de tráfico la convierte en una opción sólida para su adopción en redes WISP. En cambio, métodos como Round Robin son más adecuados para escenarios básicos,

mientras que Least Connections podría considerarse si se tiene suficiente capacidad de procesamiento para mantener un monitoreo constante.

Por lo tanto, considerando criterios técnicos como la viabilidad de implementación en entornos controlados, la técnica PCC (Per Connection Classifier) resulta la alternativa más adecuada para el entorno analizado. Su flexibilidad, su capacidad de adaptación a distintos patrones de tráfico y un control detallado sobre la distribución hacen de ella una opción adecuada para redes que buscan eficiencia y estabilidad a largo plazo [24].

### 3.6. Resumen del capítulo

En este capítulo se desarrolló la implementación del entorno de laboratorio para la simulación de una red WISP, utilizando equipos de red gestionables y herramientas de configuración que permiten reproducir condiciones similares a las reales. Se realizó la configuración de la conectividad a internet mediante dos enlaces WAN, la creación de VLAN para la segmentación del tráfico y la implementación del balanceo de carga mediante la técnica PCC en un router MikroTik. El balanceo permitió distribuir eficientemente el tráfico hacia los enlaces WAN disponibles. Asimismo, se configuraron políticas de calidad de servicio (QoS) para administrar una capacidad operativa de 375 Mbps de ancho de banda, considerando un margen de seguridad respecto a los 400 Mbps que proporciona el proveedor de internet. De esta capacidad, se asignaron 60 Mbps al servicio empresarial, 30 Mbps al servicio VIP y 15 Mbps al servicio estándar, para un total de 105 Mbps distribuidos entre las diferentes colas de servicio. Los 270 Mbps restantes se mantuvieron como capacidad de reserva para evitar la saturación de la red, absorber variaciones en la demanda de tráfico y contribuir a la estabilidad y continuidad del servicio.

# Capítulo 4. Resultados de la propuesta

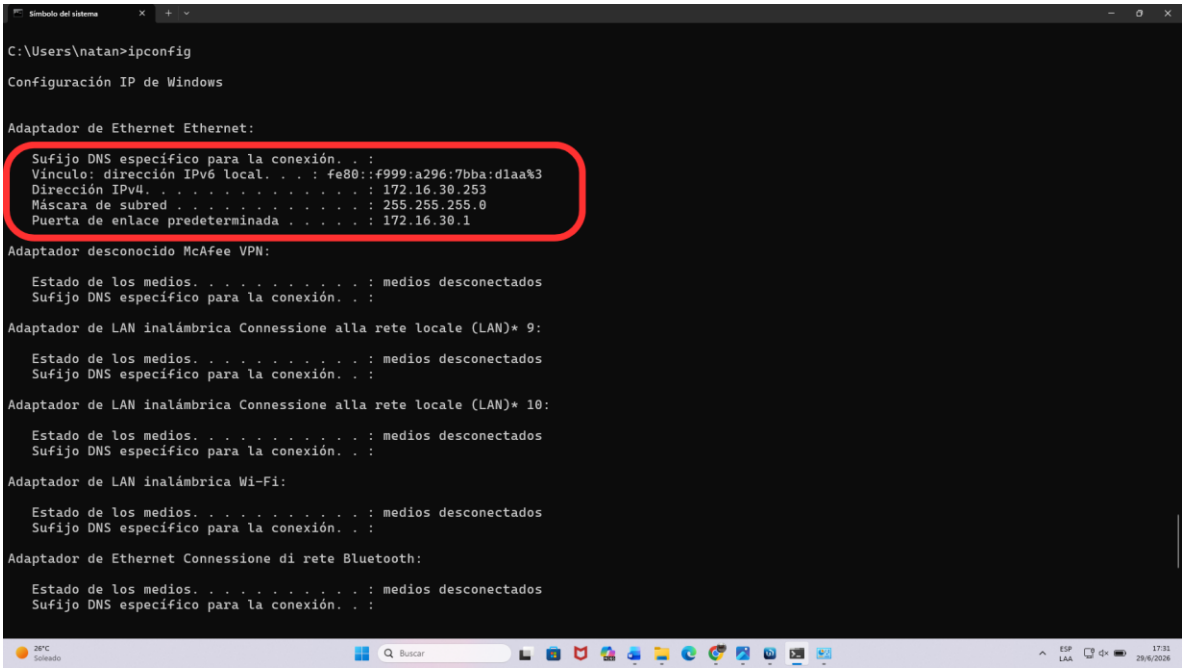
## 4.1. Introducción

En este capítulo se presentan los resultados obtenidos a partir de la implementación del entorno de laboratorio WISP, con el propósito de validar el funcionamiento de la segmentación de red mediante VLAN, el balanceo de carga mediante la técnica PCC y la administración del ancho de banda a través de políticas de calidad de servicio (QoS). Para ello, se realizaron pruebas de conectividad, generación de tráfico y monitoreo de las interfaces del router MikroTik, con el fin de verificar el comportamiento de la red en condiciones de operación similares a las reales. Las pruebas realizadas estuvieron orientadas a comprobar la comunicación entre las VLAN implementadas, la distribución del tráfico hacia los enlaces WAN disponibles mediante el balanceo de carga PCC configurado sobre el enlace troncal y el cumplimiento de los límites de ancho de banda asignados a cada servicio.

## 4.2. Resultado de la segmentación de red mediante VLAN

Con el propósito de validar la implementación de la segmentación de la red mediante VLAN, se realizaron pruebas de conectividad en los equipos clientes pertenecientes a cada uno de los segmentos configurados en el entorno del laboratorio. Inicialmente, se verificó la asignación dinámica de direcciones IP mediante la configuración implementada en el router MikroTik. Se comprobó que cada cliente recibía una dirección IP correspondiente a la VLAN asignada, junto con su respectiva puerta de enlace predeterminada.

***Figura 93.*** *Asignación de dirección IP y puerta de enlace para VLAN 30.*

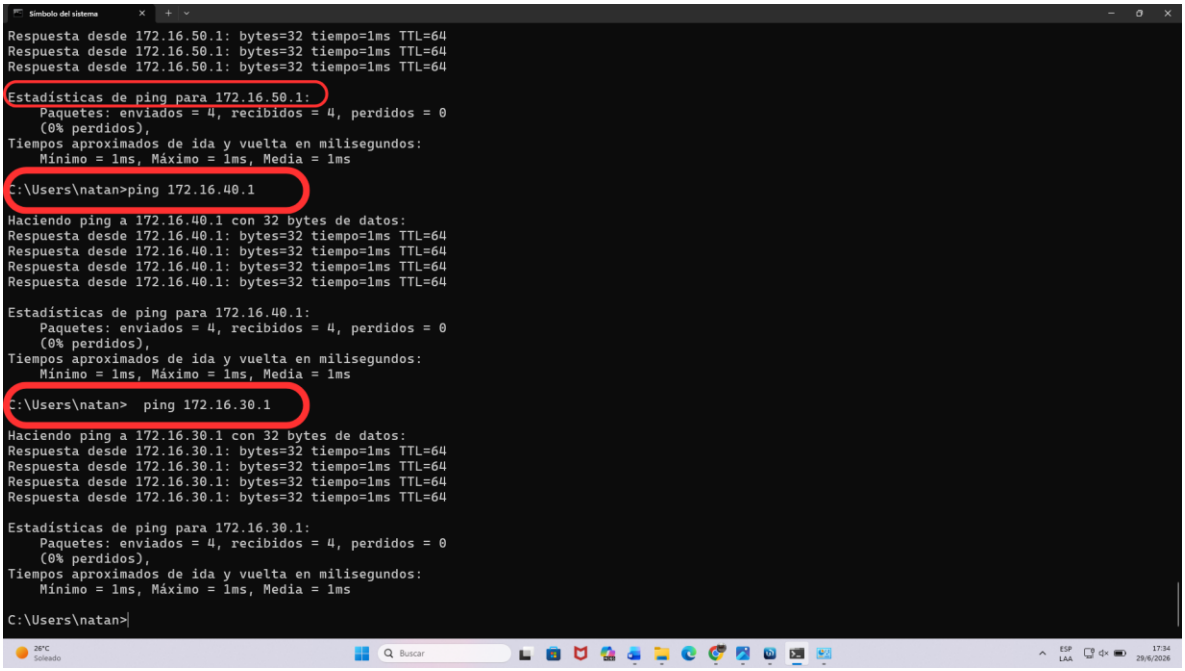



*Nota.* Elaboración propia.

La Figura 93 muestra el resultado obtenido para el equipo conectado a la VLAN 30 (empresarial). En ella se observa la asignación de la dirección IP 172.16.30.253/24 y la puerta de enlace 172.16.30.1. Estos resultados confirman el correcto funcionamiento del servicio y la comunicación entre el switch gestionable y el router MikroTik.

Posteriormente, se realizaron pruebas de conectividad mediante el protocolo ICMP (ping) hacia la puerta de enlace de cada una de las VLAN configuradas. Como se observa en la Figura 94, las respuestas fueron satisfactorias, con un 0 % de pérdidas de paquetes y una latencia promedio de 1 ms, lo que evidencia una comunicación estable entre los equipos.

***Figura 94.*** *Prueba de conectividad mediante ping hacia la puerta de enlace de las VLAN.*




*Nota.* Elaboración propia.

Los resultados obtenidos evidenciaron que la segmentación fue implementada de manera satisfactoria, lo que permitió que cada grupo de usuarios operara dentro de su dominio lógico correspondiente. Con el fin de sintetizar los resultados obtenidos durante las pruebas de conectividad, en la Tabla 14 se presentan los parámetros evaluados para cada VLAN implementada.

***Tabla 14.*** *Resultados de conectividad.*

| VLAN | Dirección IP obtenida | Puerta de enlace | Pérdida de paquetes | Latencia promedio | Estado |
|---|---|---|---|---|---|
| Empresarial 30 | 172.16.30.253 | 172.16.30.1 | 0 % | 1 ms | Correcto |
| VIP 40 | 172.16.40.253 | 172.16.40.1 | 0 % | 1 ms | Correcto |
| Estándar 50 | 172.16.50.253 | 172.16.50.1 | 0 % | 1 ms | Correcto |

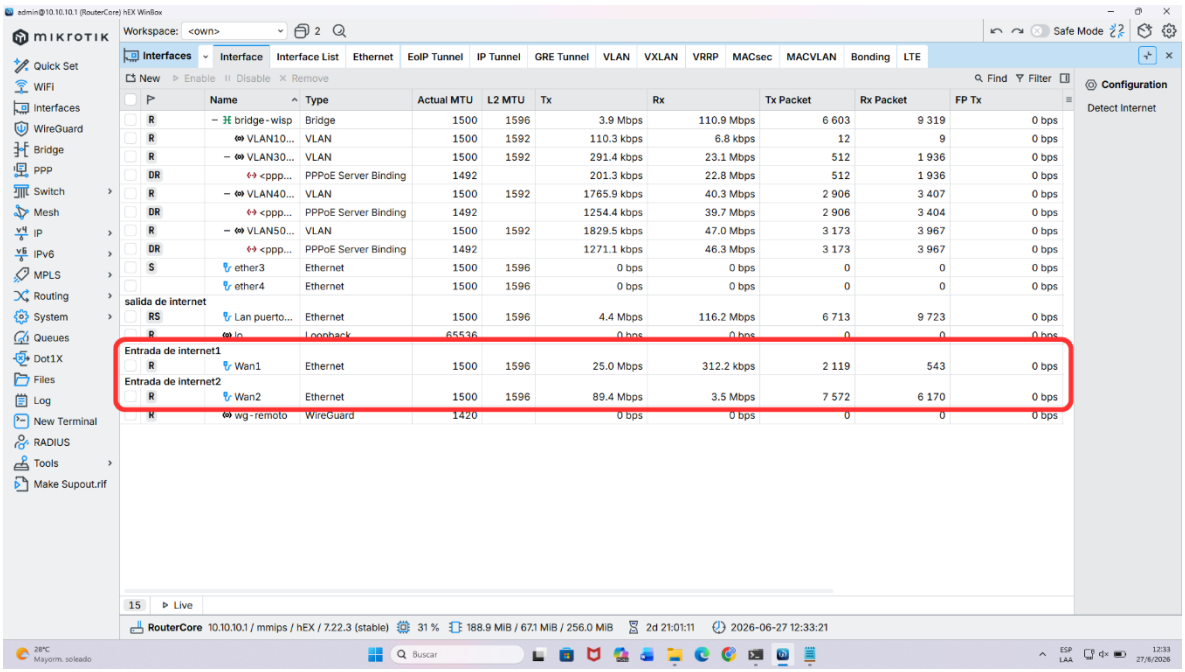
*Nota.* Elaboración propia.

Como se observa en la Tabla 14, las tres VLAN presentaron una conectividad satisfactoria con sus respectivas puertas de enlace, con una pérdida de paquetes del 0 % y una latencia promedio de 1 ms. Estos resultados confirman el correcto funcionamiento de la segmentación de la red y la estabilidad de la comunicación entre los equipos clientes y el núcleo de la red.

### 4.3. Análisis del balanceo de carga mediante PCC

Para evaluar el comportamiento del balanceo, se realizaron pruebas de generación de tráfico desde las diferentes VLAN mediante el software Iperf3, mientras se monitoreaba el consumo del ancho de banda en las interfaces WAN del router, como se muestra en la Figura 95.

***Figura 95.*** *Tráfico balanceado en WAN1 y WAN2.*




*Nota.* Elaboración propia.

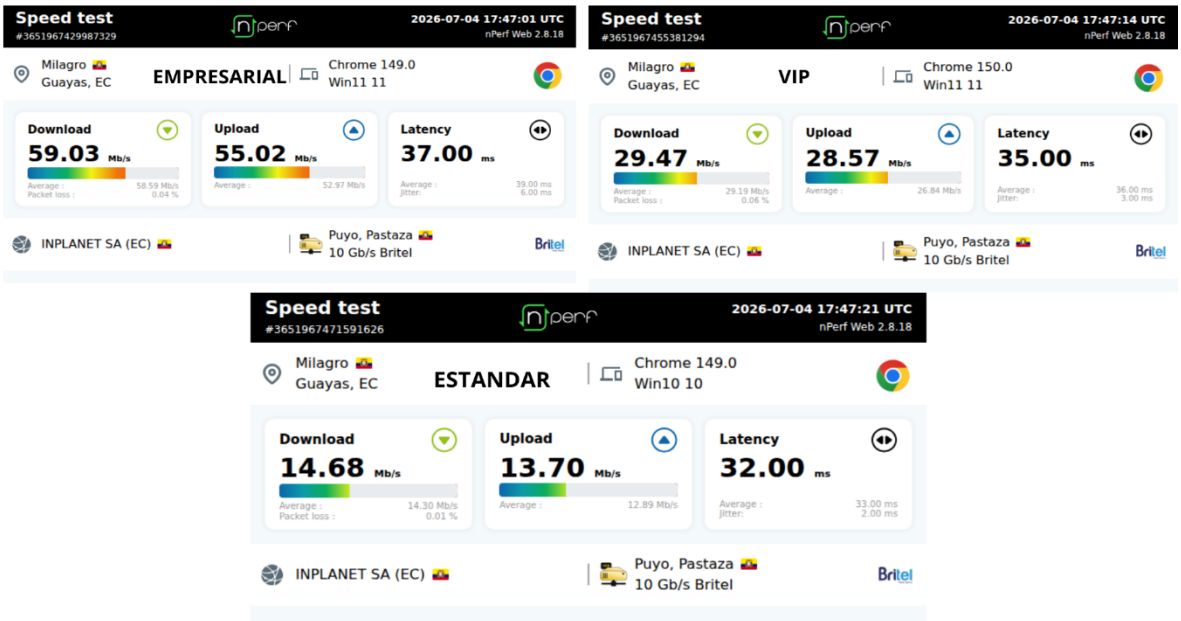
El objetivo fue verificar que las dos WAN trabajaran de manera simultánea y que el tráfico no se concentrara en un solo enlace, de acuerdo con las reglas de clasificación PCC establecidas en el apartado de implementación. También se simuló el fallo de uno de los enlaces mediante su desconexión del router y se verificó que la conexión a internet se mantenía estable a través del

enlace disponible. Esto permitió confirmar que el balanceo PCC funcionó de manera adecuada sobre el enlace troncal, ya que distribuyó las conexiones de los usuarios entre los distintos enlaces de salida a internet y contribuyó a un mejor aprovechamiento de los recursos disponibles.

### 4.4. Resultado de la implementación QoS

Las pruebas realizadas con la herramienta nPerf, utilizada para medir la velocidad de internet, permitieron verificar que las colas de servicio configuradas en el router MikroTik limitaron y priorizaron el tráfico de acuerdo con los valores establecidos. De esta manera, se confirmó que la implementación de la QoS contribuyó a la optimización del ancho de banda y aseguró un tratamiento diferenciado para cada tipo de usuario dentro del entorno WISP simulado.

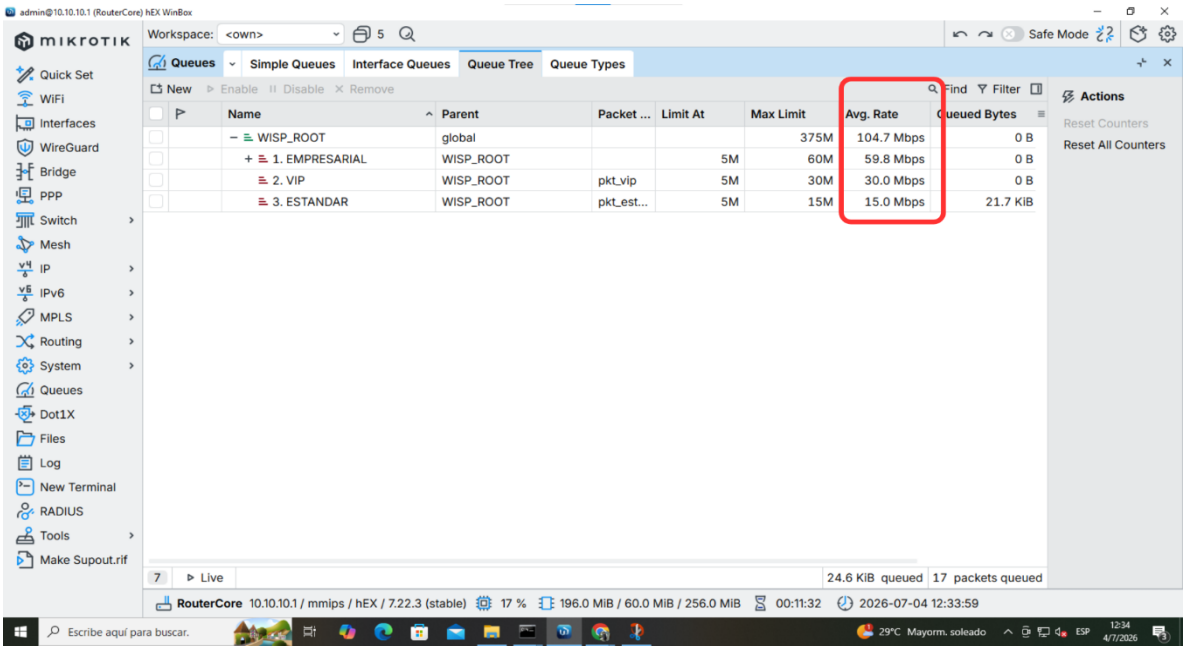
***Figura 96.*** *Prueba de velocidad en nPerf.*




*Nota.* Elaboración propia.

En la Figura 96 se observa una prueba de velocidad realizada de manera simultánea para los tres usuarios, con el fin de verificar que las colas de servicio configuradas no superen los límites establecidos.

***Figura 97.*** *Prueba de QoS.*




*Nota.* Elaboración propia.

La Figura 97 presenta el funcionamiento de las colas configuradas para cada servicio. Se observa que la cola principal Wisp_Root administra un ancho de banda máximo de 375 Mbps, mientras que las colas secundarias tienen un límite máximo de 60 Mbps en el servicio empresarial, 30 Mbps en el servicio VIP y 15 Mbps en el servicio estándar. El tráfico registrado en las tres colas confirma que las políticas de QoS fueron aplicadas correctamente y que la información fue clasificada de acuerdo con el tipo de servicio configurado.

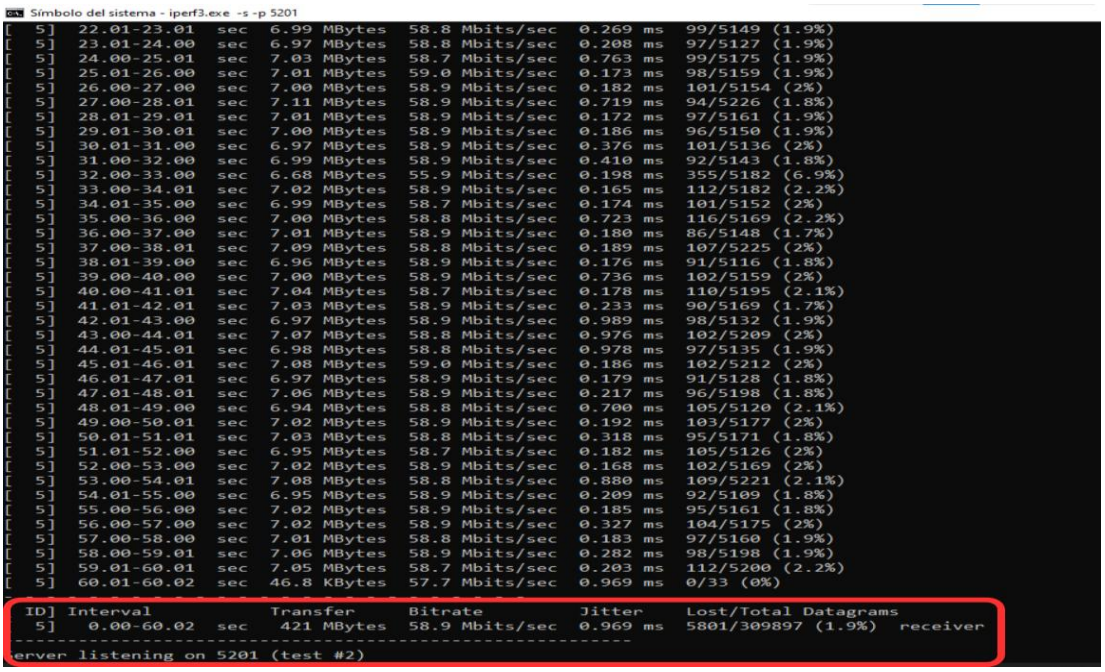
### 4.5. Prueba de tráfico y detección de errores

Con el propósito de validar el comportamiento del sistema bajo condiciones de carga, se realizaron pruebas de tráfico desde las diferentes VLAN mediante herramientas de conectividad y generación de tráfico como Iperf3. Estas pruebas permitieron medir parámetros como la latencia, la pérdida de paquetes y la presencia de errores en las interfaces del router.

### 4.5.1. Análisis de pérdidas de paquetes en VLAN empresarial

Con el fin de evaluar el rendimiento de la red implementada, se realizaron pruebas de generación de tráfico mediante la herramienta Iperf3, la cual permitió medir el throughput, el jitter y la pérdida de paquetes durante la transmisión de datos entre un cliente perteneciente a la VLAN empresarial y el servidor de prueba a través del puerto 5201.

***Figura 98.*** *Pruebas de tráfico en VLAN empresarial.*




*Nota.* Elaboración propia.

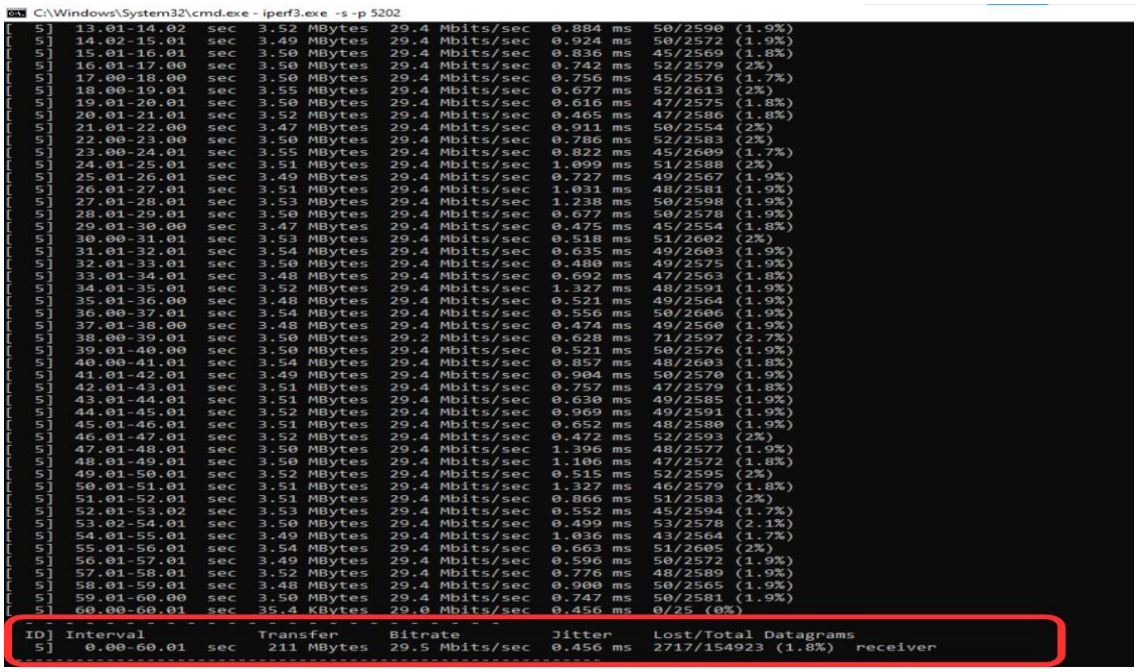
En la Figura 98 se observa la prueba individual de generación de tráfico realizada con el software Iperf3 para analizar el comportamiento de la transmisión de datos. La prueba se realizó en la VLAN empresarial durante una transmisión continua de 60 segundos, en la cual se alcanzó una transferencia total de 421 MB, con un throughput promedio de 58,9 Mbps; asimismo, se registró un jitter de 0,969 ms y una pérdida de paquetes del 1,9 %.

Estos resultados evidencian que la infraestructura implementada mantiene un comportamiento estable durante la transmisión de tráfico, con una elevada tasa de transferencia, una mínima variación temporal y un bajo porcentaje de pérdida de paquetes.

### 4.5.2. Análisis de pérdidas de paquetes en VLAN VIP

Se evaluó el rendimiento de la red mediante la herramienta Iperf3 para medir el throughput, el jitter y la pérdida de paquetes. La transmisión de datos se realizó entre un cliente de la VLAN VIP y el servidor de pruebas a través del puerto 5202.

***Figura 99.*** *Pruebas de tráfico en VLAN VIP.*




*Nota.* Elaboración propia.

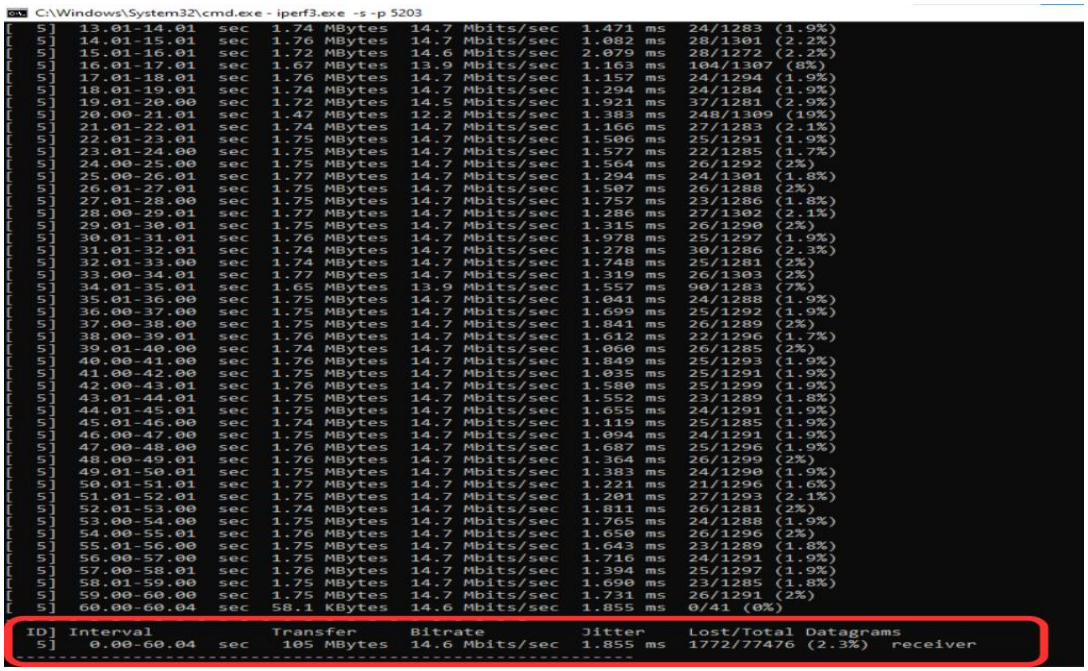
En la Figura 99 se observa una prueba individual de tráfico realizada en la VLAN VIP durante una transmisión continua de 60 segundos, en la cual se alcanzó una transferencia total de 211 MB, con un throughput promedio de 29,5 Mbps; asimismo, se registró un jitter de 0,456 ms y una pérdida de paquetes del 1,8 %.

Estos resultados demuestran que la VLAN VIP mantuvo un desempeño estable durante la transmisión de datos, con una tasa de transferencia cercana al límite de ancho de banda configurado para este servicio. La baja variación temporal y el reducido porcentaje de pérdida de paquetes evidencian el correcto funcionamiento del servicio VIP.

### 4.5.3. Análisis de pérdidas de paquetes en VLAN estándar

Con la finalidad de evaluar el desempeño del servicio correspondiente a la VLAN estándar, se realizó una prueba de generación de tráfico mediante la herramienta Iperf3, con la cual se analizaron indicadores de rendimiento como el throughput, el jitter y la pérdida de paquetes a través del puerto 5203.

***Figura 100.*** *Prueba de tráfico en VLAN estándar.*




*Nota.* Elaboración propia.

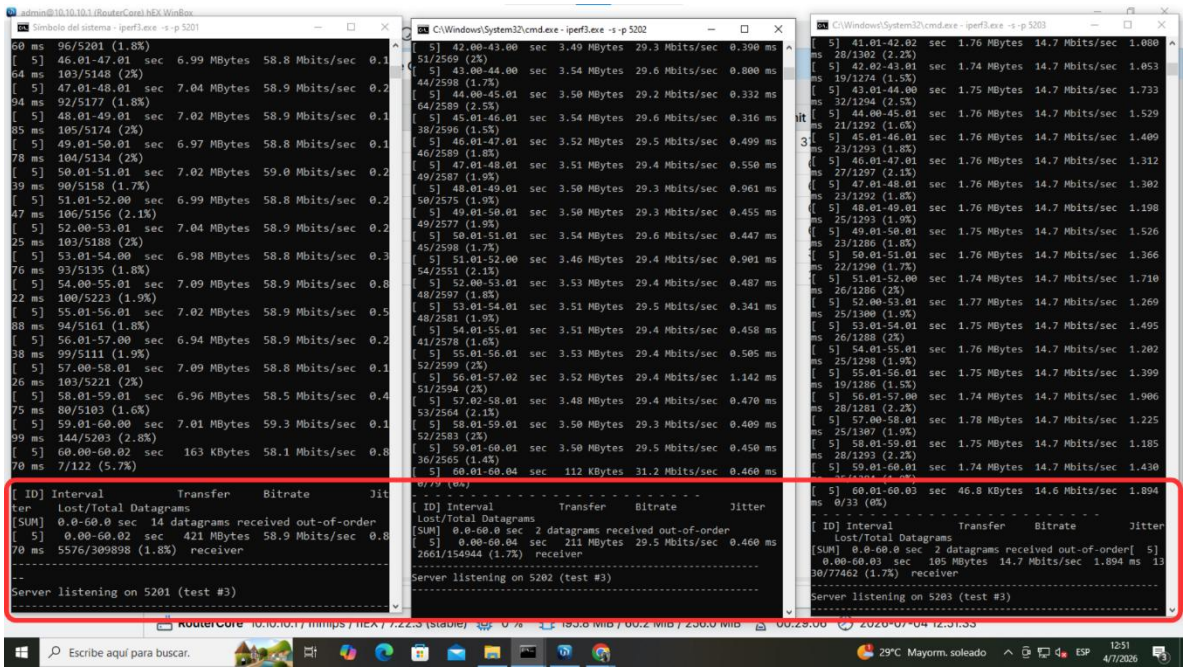
Como se muestra en la Figura 100, durante 60 segundos se transmitieron 105 MB de datos, con un throughput promedio de 14,6 Mbps; asimismo, se registró un jitter de 1,855 ms y una pérdida de paquetes del 2,3 %.

Estos resultados muestran que el ancho de banda alcanzado se mantiene próximo al límite configurado para la cola de servicio estándar, aunque se observó un porcentaje de pérdida de paquetes superior al registrado en los demás servicios. Este comportamiento es coherente con la menor prioridad asignada al tráfico de la VLAN estándar dentro de la estrategia de administración del ancho de banda.

### 4.5.4. Análisis simultáneo de la pérdida de paquetes en las VLAN

Con la finalidad de evaluar el comportamiento de la red bajo condiciones de carga simultánea, se realizaron pruebas de generación de tráfico mediante la herramienta Iperf3. Para ello, se establecieron transmisiones simultáneas correspondientes a los diferentes servicios configurados, lo que permitió analizar el throughput, el jitter y la pérdida de paquetes durante la transferencia de datos.

***Figura 101.*** *Prueba simultánea de tráfico en las VLAN.*



*Nota.* Elaboración propia.

En la Figura 101 se muestran los resultados obtenidos durante la ejecución simultánea de las pruebas. Los tres flujos de tráfico permanecieron activos durante 60 segundos y alcanzaron tasas de transferencia promedio de 58,9 Mbps, 29,5 Mbps y 14,7 Mbps, respectivamente. Asimismo, se registraron valores reducidos de jitter en las tres transmisiones, mientras que la pérdida de paquetes fue baja en relación con el volumen total de datagramas transmitidos. A continuación, se presenta un resumen de los principales parámetros de rendimiento registrados mediante la herramienta Iperf3.

***Tabla 15.*** *Resultados de las pruebas simultáneas.*

| Servicio | Tiempo | Transferencia | Throughput | Jitter | Datagramas perdidos |
|---|---|---|---|---|---|
| Empresarial | 60 s | 421 MB | 58,9 Mbps | 0,800 ms | 1,8 % |
| VIP | 60 s | 211 MB | 29,5 Mbps | 0,460 ms | 1,7 % |
| Estándar | 60 s | 105 MB | 14,7 Mbps | 1,894 ms | 1,7 % |

*Nota.* Elaboración propia.

Como se observa en la Tabla 15, los tres servicios mantuvieron una transmisión estable durante la ejecución simultánea de las pruebas. Los valores de throughput, jitter y datagramas perdidos son consistentes con los resultados presentados en la Figura 101 y permiten comparar cuantitativamente el comportamiento de cada servicio bajo las mismas condiciones de prueba.

## 4.6. Conclusiones

Se diseñó e implementó satisfactoriamente un entorno de laboratorio para la simulación de una red WISP mediante el uso de un router MikroTik y un switch gestionable, lo que permitió recrear condiciones similares a una red real. La infraestructura implementada facilitó el desarrollo de prácticas relacionadas con la segmentación de red, el balanceo de carga y la administración del ancho de banda.

La segmentación de la red mediante VLAN permitió separar correctamente los diferentes tipos de servicio: empresarial, VIP y estándar, lo que garantizó la asignación independiente de direcciones IP y una adecuada comunicación con sus respectivas puertas de enlace. Las pruebas de conectividad realizadas confirmaron el correcto funcionamiento del enlace troncal y el proceso de asignación dinámica de direcciones.

La implementación del balanceo de carga mediante la técnica PCC permitió distribuir las conexiones entre los enlaces WAN de forma estable, mantener la persistencia de las sesiones activas y favorecer un uso más eficiente de los recursos disponibles. Esta técnica demostró ser adecuada para el entorno de laboratorio debido a su estabilidad y capacidad para conservar la continuidad de las sesiones durante las pruebas realizadas.

La configuración de las políticas de calidad de servicio (QoS) permitió administrar el ancho de banda disponible de acuerdo con la prioridad de cada tipo de usuario. Se asignaron 60 Mbps al

servicio empresarial, 30 Mbps al servicio VIP y 15 Mbps al servicio estándar. Las pruebas con Iperf3 evidenciaron que el throughput alcanzado por cada servicio fue consistente con los límites configurados.

Los resultados obtenidos durante las pruebas de rendimiento mostraron bajos valores de latencia, jitter y pérdida de paquetes, además de una utilización moderada de los recursos del router MikroTik. Estos resultados confirman que la solución implementada ofrece un desempeño estable y constituye una alternativa adecuada para fortalecer la formación práctica de los estudiantes en la administración de redes WISP.

### 4.7. Recomendaciones

Implementar futuras pruebas con un mayor número de clientes conectados simultáneamente, con el fin de evaluar el comportamiento del balanceo de carga y de las políticas de calidad de servicio (QoS) en escenarios de mayor demanda.

Ampliar el entorno de laboratorio mediante la incorporación de más dispositivos clientes y diferentes tipos de aplicaciones de red, con el fin de analizar el impacto del balanceo de carga y de la QoS sobre los distintos servicios.

Utilizar el laboratorio como material de apoyo en asignaturas relacionadas con redes de datos, con el propósito de promover el aprendizaje práctico de tecnologías WISP y fortalecer las competencias técnicas de los estudiantes.

**Bibliografía**

[1] Edwin Steven Lima Pozo. (2025, enero) Implementación de una red de distribución de internet con un router MikroTik para balanceo de carga, segmentación por VLANs y gestión de ancho de banda. [Online]. https://repositorio.upse.edu.ec/handle/46000/12740

[2] Andrés Wladimir Párraga Lara. (2021) Análisis, diseño e implementación de módulo WISP como herramienta práctica y demostrativa del manejo de redes inalámbricas para uso en el laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana. [Online]. https://dspace.ups.edu.ec/handle/123456789/20805

[3] Kostiantyn Lisovskyi, Kyryndas Nikita Chyvron Andrii, "servidores web NGINX los principales métodos de balanceo de carga," mayo 2023. [Online]. https://www.researchgate.net/publication/371173423_THE_MAIN_METHODS_OF_LOAD_BALANCING_ON_THE_NGINX_WEB_SERVER

[4] Patricio Germánico Caisaguano Pérez. (2018, abril) Diseño y simulación de un WISP Wireless Internet Service Provider para la ciudad de Pedernales en Manabí Ecuador. [Online]. https://dspace.ups.edu.ec/handle/123456789/15471

[5] Juan Luis Cueto Morelo, "Diseño de un sistema para la optimización de la calidad de servicios y balanceo de carga en redes wifi mediante el controlador Ryu en una red definida por software," June 2025. [Online]. https://repositorio.unicordoba.edu.co/entities/publication/0976baba-bb4a-4e4c-a927-8bdb4360aa3d

[6] TP-Link. Cómo configurar la VLAN 802.1Q en switches inteligentes y administrados. [Online]. https://www.tp-link.com/es/support/faq/2149/

[7] Cristian Oswaldo Taipe Canto, "Implementación de balanceo de carga Per Connection Classifier para la mejora de la calidad de servicio de internet en la empresa Fibergo," mayo 19, 2025. [Online]. https://repositorio.uncp.edu.pe/items/ffd4126b-8d2e-4b7d-8531-b60827a74f46?utm_source=

[8] Carlos Enrique Minda Gilces. (2019) Aplicación de Balanceo De Carga Dinámico Para Servidores, Basada En Redes Definidas Por Software. [Online]. https://dialnet.unirioja.es/servlet/articulo?codigo=7037062

[9] Maman Sulaeman and Agung Budi Prasetio, "Load balancing analysis on MikroTik routers using PCC and NTH methods," 2025. [Online]. https://journal.itts.ac.id/index.php/cyfors/en/article/view/11/10

[10] Firmansah y Hadi, "Komparasi load balancing metode PCC dan NTH pada MikroTik implementasi di Al Irsyad Tengaran 7 Batu," 2023. [Online]. https://jurnal.stkippgritulungagung.ac.id/index.php/jipi/article/view/3261/1465

[11] Carlos Andrés Flores Ortiz, "Implementación de un balanaceador de carga de salida a internet basado en un servidor linux," May 2024. [Online]. https://bibdigital.epn.edu.ec/handle/15000/25498?utm_source

[12] Mariuxi Tatiana Vasquez Figueroa, "Análisis comparativo de los algoritmos de balanceo de cargas Round Robin y Least Connection de HAProxy en los sistemas de gestión de

base de datos," 2023. [Online]. https://dspace.utb.edu.ec/bitstream/handle/49000/15076/E-UTB-FAFI-SIST.INF-000203.pdf?sequence=1&isAllowed=y

[13] Mikrotik. (2025) Ráfagas de velocidad (Burst). [Online]. https://manual.mikrotik.com/docs/firewall-and-quality-of-service/queues/queue-burst/?utm_source

[14] Peplink. (2023) Load Balancing Algorithms. [Online]. https://www.peplink.com/technology/load-balancing-algorithms/#:~:text=Prioridad,si%20falla%20la%20conexi%C3%B3n%20actual.

[15] José Luis Oña Riera, "Diseño e implementación de una red WISP para interconectar tres sectores rurales en la provincia de Bolívar.," 2025. [Online]. https://www.dspace.espol.edu.ec/bitstream/123456789/65822/1/T-115117%20POSTG119%20O%c3%91A%20RIERA%20JOSE.pdf

[16] Edgar Antonio Quinga Tupiza, "WISP: qué es y por qué tiene tanta importancia en las conexiones," agosto 2024. [Online]. https://dspace.ups.edu.ec/handle/123456789/28418?utm_source

[17] Nicole Abigail Belduma Rentería, "Diseño e implementación de un banco de pruebas WISP (Wireless Internet Service Provider) utilizando tecnología inalámbrica de Cambium Networks," 2021. [Online]. https://dspace.ups.edu.ec/handle/123456789/21755

[18] Ubiquiti Inc., "airFiber 5XHD," Ubiquiti, Especificaciones técnicas 2023. [Online]. https://dl.ui.com/datasheets/airfiber/airFiber_5XHD_DS.pdf?utm_source

[19] Christian Javier Amaguaña Aguilar, "Herramientas de seguridad defensiva y ofensiva para redes LoRaWAN: desarrollo de un prototipo de módulo de análisis de tráfico basado en Wireshark para detección de ataques de denegación usando inspección de tramas LoRaWAN que provea una capa de integraci," 2022. [Online]. https://bibdigital.epn.edu.ec/handle/15000/23416

[20] Edison Alexis Candela Forero, "Implementación sistema de monitoreo de red utilizando la herramienta PRTG Network Monitor," 2021. [Online]. https://digitk.areandina.edu.co/server/api/core/bitstreams/526a66e2-37a8-4860-a9f0-61de9cf152e1/content

[21] Verónica Aleksei Viloria Ramírez, "Mejoramiento de la calidad de servicios (QoS)," Universidad de Cuenca, 2023. [Online]. https://dspace-test.ucuenca.edu.ec/bitstream/123456789/42849/1/Trabjo-de-Titulaci%C3%B3n.pdf?utm_source

[22] Johanny Andres Peña Florez, Pedro Jose Davila Rincón Jayson David Gonzalez Avellaneda, "Diseño y optimización de la red wi-fi para la empresa laboratorios farmapar sas," septiembre 2020. [Online]. https://repository.ucc.edu.co/server/api/core/bitstreams/60456438-e5da-46e8-93a9-4609c53ce8f6/content

[23] Andika Yudhistira, "Analisa Performa Algoritmo de equilibrio de carga HTTP Round Robin, menor conexión y menor tiempo de respuesta en NodeJS," 2024. [Online]. https://etd.repository.ugm.ac.id/penelitian/detail/246099

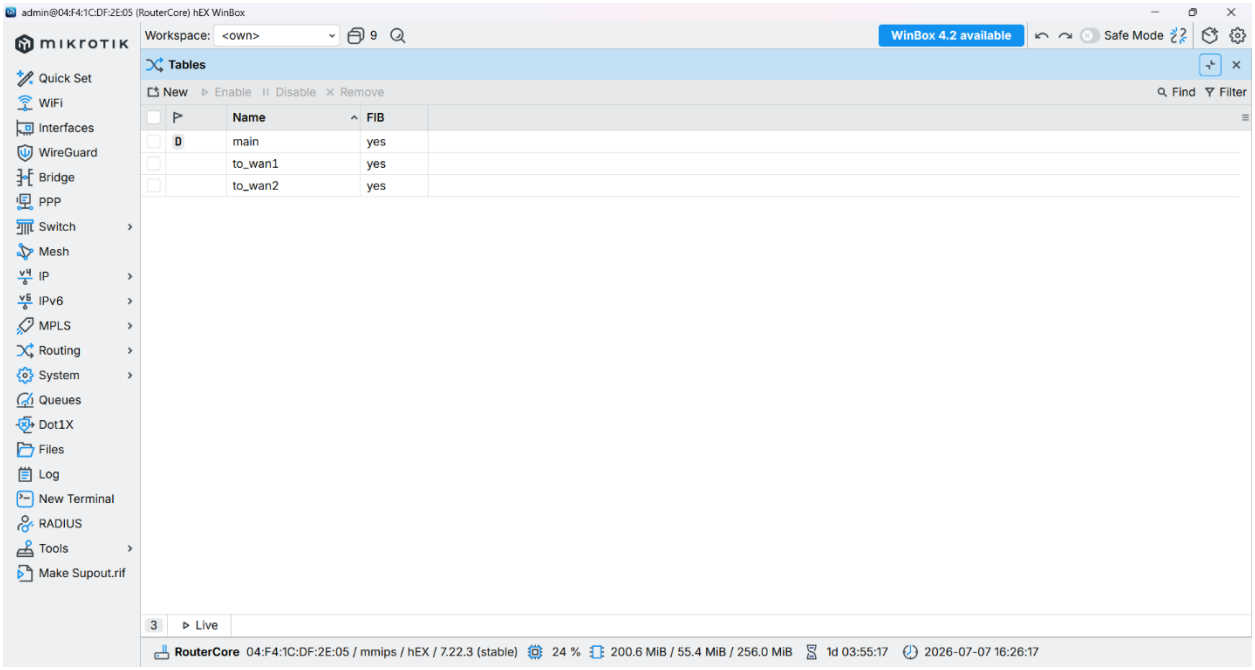
[24] Nejer Haro Diego Fernando, "Desarrollo de un algoritmo de balanceo de carga dinámico de múltiples rutas para la redistribución de flujos en una red SDN," 2023. [Online]. https://repositorio.utn.edu.ec/bitstream/123456789/13801/2/04%20RED%20329%20TRABAJO%20GRADO.pdf?utm_source

[25] Simon Arnold Kassing, "Performance Evaluation of Networked Systems," 2022. [Online]. https://www.research-collection.ethz.ch/server/api/core/bitstreams/09606e1b-69c6-4417-8800-6bbd6dde9579/content

[26] Carlos William Suárez González, "Estudio para la implementación de redes comunitarias WISP para la comuna Bellavista del Cerro," 2022. [Online]. https://repositorio.upse.edu.ec/items/b44da169-5f1a-41c9-832e-eb1e7629f2ff

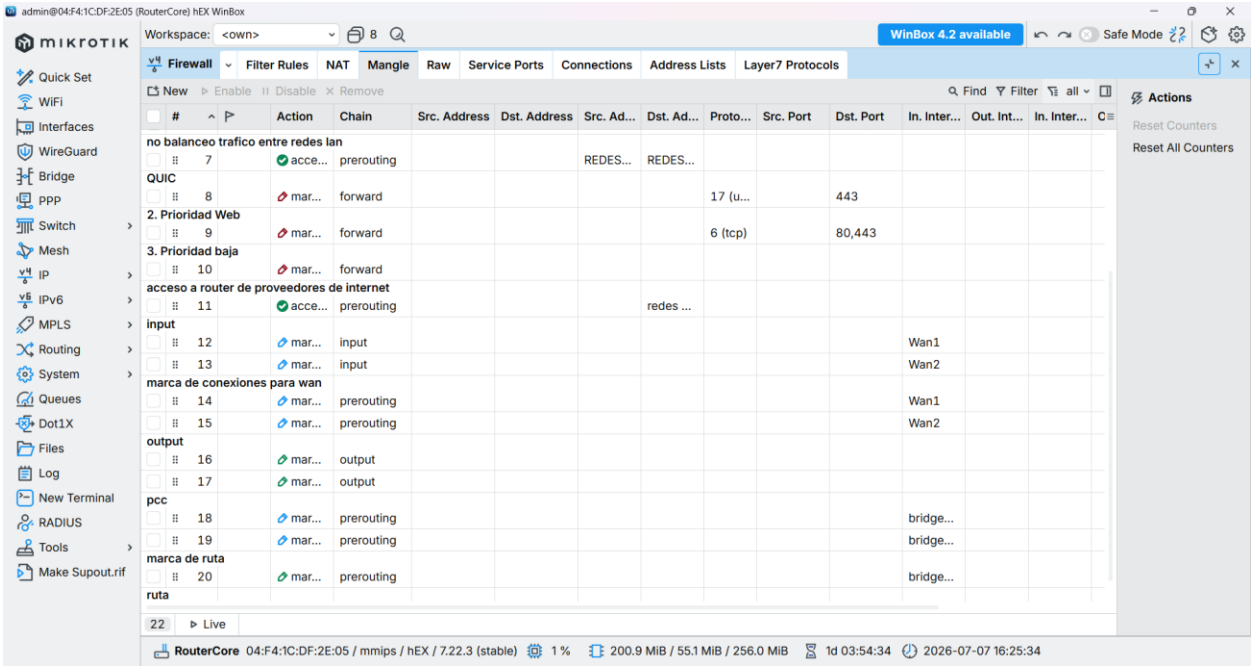
# ANEXOS

***Figura 102.*** *Marcas de rutas en Routing Table.*



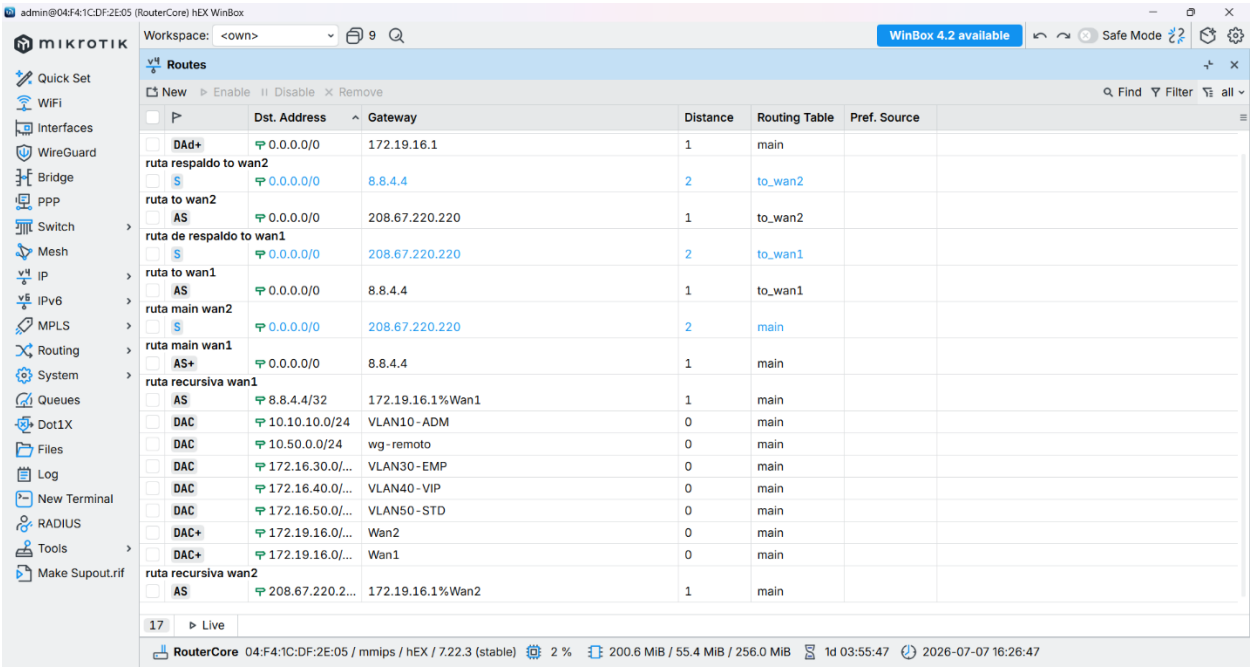

*Nota.* Elaboración propia.

***Figura 103.*** *Reglas Mangle.*




*Nota.* Elaboración propia.

***Figura 104.*** *IP/Routes: reglas para el failover.*




*Nota.* Elaboración propia.

***Figura 105.*** *Equipos instalados en el* rack *4.*


*Nota.* Elaboración propia.

***Figura 106.*** *Colocación del cable Ethernet para la antena sectorial.*

*Nota.* Elaboración propia.

***Figura 107.*** *Colocación de la antena CPE y del router para habilitar la conexión del usuario estándar.*

*Nota.* Elaboración propia.