



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TELECOMUNICACIONES**

TRABAJO DE TITULACIÓN

Trabajo complejo, previo a la obtención del título

INGENIERIA EN TELECOMUNICACIONES

TEMA:

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.

AUTOR:

Lima Pozo Edwin Steven

TUTOR SUGERIDO:

Ing. Manuel Asdrual Montaña B.



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-Pariño, Mgtr.

DOCENTE ESPECIALISTA - GUIA UIC II

Ing. Manuel Asdrual Montaña B, MSc

DOCENTE TUTOR

Ing. Corina Gonzabay De La A, Mgtr.

SECRETARIA



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

DECLARACIÓN DE DÒCENTE TUTOR

En mi calidad de docente tutor del componente práctico de examen complejo denominado: **“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”**, elaborado por **Lima Pozo Edwin Steven**, estudiante de la Carrera de Telecomunicaciones, Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniería en Telecomunicaciones, me permito declarar que, tras supervisar el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos. En consecuencia, lo considero apto en todos sus aspectos y listo para ser evaluado por el docente especialista.

Atentamente

A handwritten signature in blue ink, appearing to read "M. Asdrual", is written over a horizontal line.

Ing. Manuel Asdrual M, MSC

DOCENTE TUTOR

DECLARACIÓN DE DOCENTE ESPECIALISTA

En mi calidad de docente especialista del componente práctico de examen complejo denominado, **“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”**, elaborado por **Lima Pozo Edwin Steven**, estudiantes de la carrera de Telecomunicaciones, Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniería en Telecomunicaciones, me permito declarar que, tras supervisar el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos. En consecuencia, lo considero apto en todos sus aspectos y listo para la sustentación del trabajo.

Atentamente



Ing. Luis Amaya Fariño, Mgtr

DOCENTE ESPECIALISTA

DECLARACIÓN AUTORÍA DE LAS ESTUDIANTES

El presente trabajo del componente practico de examen complejo denominado:
“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”,
declaramos que la concepción análisis y resultados son originales a la actividad educativa en el área de Telecomunicaciones.

Atentamente




Lima Pozo Edwin Steven

C.I. 2450523507

DECLARACIÓN DE RESPONSABILIDAD

Quienes suscriben, Lima Pozo Edwin Steven con C.I. 2450523507, estudiantes de la carrera de Telecomunicaciones, declaramos que el trabajo de titulación denominada **“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”** pertenece y es exclusiva responsabilidad de las autoras y pertenece al patrimonio intelectual de la Universidad Estatal Península de Santa Elena.

Atentamente



Lima Pozo Edwin Steven

C.I. 2450523507

AGRADECIMIENTO

Este proyecto realizado, tengo el honor en agradecer profundamente a mi familia que con su apoyo moral fueron la energía que me impulso en este camino sin su apoyo este logro no sería posible.

A mis docentes que por su compromiso con la formación de los estudiantes lograron transmitir sus conocimientos y poder motivarme a alcanzar nuevas alturas académicas generando interés en la carrera y saber que existen muchas cosas de gran importancia.

A mi tutor de proyecto, ya que por su tiempo y paciencia guio su experiencia y consejos que fueron esenciales para este proyecto.

Finalmente, agradezco a todas las personas que de alguna manera contribuyeron, a que este proyecto se implementara y decir que siempre serán recordados.

DEDICATORIA

Dedico este logro a mi familia por ser el pilar fundamental de mi vida por su amor incondicional y a su apoyo constante por dame esa motivación de que los sueños se alcanzan con esfuerzos y perseverancia este trabajo realizado por mi persona es un hecho de esfuerzo, pero logrado ahora es mi turno de afrontar desafíos.

ÍNDICE DE CONTENIDO

AGRADECIMIENTO	7
DEDICATORIA	8
RESUMEN	13
ABSTRACT	13
CAPÍTULO I	14
1.1. Introducción	14
1.2. Objetivo general	16
1.3. Objetivo específico	16
1.4. Justificación	16
1.5. Metodología	17
CAPÍTULO II	19
2.1 Fundamentos en administración en redes	19
2.1.1 Definición de administración de redes	19
2.1.2 Importancia de administración de redes empresariales	19
2.2 Cloud Router Switch Mikrotik	20
2.2.1 Características y funcionalidades de los equipos Mikrotik	20
2.2.2 Comparativas con otros dispositivos de red	22
2.2.3 Especificaciones y aplicaciones	23
2.3 Balance de carga	26
2.3.1 Concepto de balance de carga	26
2.3.2 Métodos de balanceo de carga	26
2.3.3 Balanceo entre la fibra óptica y LTE	27
2.3.4 Conmutación automática(failover)	28
2.4 Segmentación de VLANs	28
2.4.1 Concepto de segmentación de VLANs	28
2.4.2 Ventajas de las VLAN	28
2.4.3 Seguridad en las VLAN	29
2.5 Gestión del ancho de banda	30
2.5.1 Importancia de la gestión de ancho de banda	30
2.5.2 Calidad de servicio (QOS)	30
2.5.2.1 Principios de QOS	31
2.5.2.3 Ventajas y desventajas	32
2.5.3 Herramientas para el monitoreo y optimización del tráfico de red	33

2.6	Acceso móvil y fibra óptica	35
2.6.1	Ventajas de acceso móvil en redes	35
2.6.2	Causas y procedimiento en el uso de acceso móvil	35
2.6.3	Ventajas de acceso de la fibra en redes	36
2.6.4	Desafíos y soluciones de la fibra	36
CAPÍTULO III		38
3.1	Diseño de la arquitectura de la red	38
3.1.1	Esquema lógico de la red	38
3.1.2	Esquema físico de la red	39
3.2	Configuración del balance de carga y failover	39
3.2.1	Detalles de conexiones WAN primaria (fibra óptica)	39
3.2.2	Configurar las interfaces WAN (ether1 y sfp1)	41
3.2.3	Configurar rutas con prioridad con failover	44
3.3.1	Establecer configuración NAT	48
3.4	Establecer configuraciones de VLANs	50
3.4.1	Establecer IP a las VLANs	53
3.4.2	Establecer VLANs en modo TRUNK	56
3.5	Implementación de calidad de servicio QoS	58
3.5.1	Reglas de Firewall para el tráfico de VLANs	58
3.5.2	Reglas para limitar las VLANs	61
3.5.3	Establecer configuración QoS	62
3.5.4	Establecer PCQ para granularla	64
CAPITULO IV		66
4.1	Resultados	66
4.1.1	Evaluación del Desempeño de Balanceo de Carga y Failover	66
4.1.2	Análisis de Tráfico y Eficiencia en Redes VLAN Integradas con QoS	67
4.1.4	Monitoreo y Validación de Configuraciones WAN y VLAN	71
4.1.5	Priorización, Failover y Limitación de Ancho de Banda	73
4.1.6	Coud router switch CRS112.8P-4S-IN	75
CONCLUSIONES		77
RECOMENDACIONES		78
REFERENCIAS		79

ÍNDICE DE FIGURAS

Figura 1 Cloud router switch	21
Figura 2 Imagen de simulación	38
Figura 3 Conexiones entre equipos	39
Figura 4 Modulo sfp	40
Figura 5 Software winbox	40
Figura 6 Conexiones de proveedor a los puertos	41
Figura 7 Renombrar las interfases sfp1 y ether1	42
Figura 8 Configuración wan1	43
Figura 9 Configuración wan 2	43
Figura 10 Ruta principal para wan 1	44
Figura 11 Ruta respaldo wan2	45
Figura 12 Marcado de paquetes 1	46
Figura 13 Marcado de paquetes 2	47
Figura 14 Marcado de paquetes 3	47
Figura 15 Marcado de paquetes 4	48
Figura 16 Configuración nat para wan 1	49
Figura 17 Configuración nat para wan2	50
Figura 18 Configurar vlan administración	51
Figura 19 Configurar vlans laboratorio	52
Figura 20 Configurar vlans red invitados	52
Figura 21 Configurar vlans para cámaras	53
Figura 22 Configuración de ip vlans administración	54
Figura 23 Configuración de ip vlans laboratorio	55
Figura 24 Configuración de ip vlans invitados	55
Figura 25 Configuración de ip vlans cámaras	56
Figura 26 Configuración bridge modo trunk	57
Figura 27 Asignación sfp2 con bridge trunk	58
Figura 28 Trafico proveniente vlan administración	59
Figura 29 Trafico proveniente vlan laboratorio a internet	59
Figura 30 Trafico proveniente vlan invitados a internet	60
figura 31 Trafico de vlans cámaras	60
Figura 32 Limitamos el tráfico entre vlans	61
Figura 33 Bloqueo vlans invitado hacia laboratorio	62

Figura 34 Priorizar el tráfico vlan cámaras	63
Figura 35 Priorizar el tráfico vlans administración	63
Figura 36 Priorizar vlans laboratorio	64
Figura 37 Priorizar el tráfico vlan invitados	64
Figura 38 Configuración del ancho de banda de forma granular	65
Figura 39 Rutas específicas de acceso a internet	66
Figura 40 Trafico activos de internet1 y intenet2	67
Figura 41 Distribución de balance de carga entre wans	67
Figura 42 Interfaces vlan por consola	68
Figura 43 Simulación tráfico de vlans	68
Figura 44 Validación de ancho de banda	69
Figura 45 Reglas del firewall par vlans	70
Figura 46 Validación de qos por colas	71
Figura 47 Conmutación por error	72
Figura 48 Restricciones de tráfico entere vlans	72
Figura 49 Prueba de failover	73
Figura 50 Prioridades de ancho de banda	74
Figura 51 Lista de los tipos de colas configuradas	75
Figura 52 Switch modo puente	76

ÍNDICE DE TABLAS

Tabla 1 Comparativa de equipos de diferentes marcas	23
Tabla 2 Especificaciones y aplicaciones mikrotik	24
Tabla 3 Estudio y complemento de uso	25
Tabla 4 Técnicas de balanceo de carga	27
Tabla 5 Ventajas y descripciones vlans	29
Tabla 6 Características y descripción de qos	32
Tabla 7 Ventajas y desventajas de qos	33
Tabla 8 Causas y procedimientos en redes móviles	36
Tabla 9 Desafío y soluciones de la fibra óptica	37

RESUMEN

El proyecto realizado se implementó en una red de disponibilidad continua de Internet utilizando un equipo Mikrotik modelo CRS310-1G.5G-4S+IN como equipo principal conectando a dos proveedores de Internet con diferentes direcciones IP, la primera para disponibilidad continua y la segunda como respaldo, la arquitectura también incluye segmentación de VLANs para distintos departamentos como administración, laboratorio, invitados y cámaras, con distintos rangos de IP así mismo implementando políticas de comunicación entre ellas, otras configuraciones realizadas es el balance de carga y conmutación por errores failover, que garantiza la disponibilidad del Internet, también se configuraron límites de ancho de banda mediante QoS para una gestión eficiente de los recursos, priorizando respuestas a posibles fallos de la red interna y finalmente implementar herramientas nativas de Mikrotik para la supervisión continua de tráfico.

Palabras clave: balanceo de carga, calidad de servicio QoS, segmentación de red, continuidad de servicio.

ABSTRACT

The project carried out consists of implementing a continuous Internet availability network, using a Mikrotik equipment model CRS310-1G.5G-4S+IN as the main equipment connecting two Internet providers with different IP addresses, one for continuous availability and the other as a backup, the architecture also includes segmentation of VLANs for different departments such as administration, laboratory, guests and cameras. with different IP ranges as well as implementing communication policies between them, other configurations made is load balancing and failover, which guarantees the availability of the Internet, bandwidth limits were also configured through QoS for efficient management of resources, prioritizing responses to possible failures of the internal network and finally implementing native Mikrotik tools for continuous traffic monitoring.

Keywords: load balancing, QoS quality of service, network segmentation, service continuity

CAPÍTULO I

1.1. Introducción

En la actualidad el acceso a Internet y la administración eficaz de redes son primordiales para poder garantizar una conectividad y rendimiento óptimo en entornos o áreas empresariales, las existencias tecnológicas han avanzado significativamente hacia las necesidades que las arquitecturas de redes ofrezcan segmentación y disponibilidad de servicio constante, la gestión avanzada del ancho de banda también es prioridad para aplicaciones críticas con respecto a los equipos MikroTik que se han posicionado como herramientas versátiles y rentables para implementar soluciones de conectividad avanzadas en diversas organizaciones.

En este tema de proyecto, **“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”** que busca cumplir necesidades que surgen mediante algún diseño en la configuración e implementación de una red empresarial con disponibilidad constante de acceso a Internet, La propuesta se centra en garantizar una conectividad confiable y estable, utilizando balance de carga con dos proveedores que brindan acceso, por medio de fibra óptica, como conexión principal y una conexión móvil como respaldo, también segmentando la red mediante VLANs con el fin de individualizar y proteger el tráfico de diferentes áreas funcionales como administración, cámaras, sala de cómputo y red de invitados.

las sistematizaciones de redes están en disponibilidad en base al rendimiento y seguridad de las infraestructuras red, es decir la conectividad a Internet y la permanecía de los servicios de red, que son importantes para la capacidad de cualquier organización, las comunicaciones internas y los servicios al cliente, pueden ser interrumpidos por la falta de conectividad, causando daños críticos a la economía y la productividad. Por lo tanto, la mayoría de las organizaciones invierten en redes de alta disponibilidad, incluyendo la redundancia y la creación de un balanceo de carga de servicio de red activo, incluso cuando los principales proveedores de servicios de red no están funcionando.

El balanceo de carga y el failover en varias conexiones se dan hacia Internet porque se han transformado en destrezas fundamentales para poder reducir la dependencia en una sola conexión, esto admite que, si una conexión falla, otra pueda asumir automáticamente la carga, garantizando la continuidad del servicio, al mismo tiempo, los procesos y formas de segmentación de red, es decir configuración virtual local área Network (VLAN) que se ha creado como estrategia principal al organizar y separar varias formas de tráfico de red, permitiendo una gestión más controlada y segura del flujo de datos [1].

La gestión correcta y eficiente del ancho de banda se incluyen en las técnicas QoS (calidad de servicio) estas configuraciones de administración han generado interés ya que son prácticas, que aseguran mejorar el rendimiento de las aplicaciones con más demanda de tráfico de datos, que tengan prioridad según las áreas, y así las redes configuradas no existan congestiones, logrando garantizar una disponibilidad óptima y eficaz, optimizando los recursos de nuestros accesos al Internet.

Los equipos de MikroTik son una solución robustas y versátiles para una gestión y control de redes eficiente, porque, no solo son para segmentar VLANS también permiten el monitoreo y las limitaciones de tráfico de datos, a través de sus técnicas de configuración, de control de anchos de banda ofreciendo nuevas alternativas para el acceso a Internet permitiendo compartir las conexiones de datos móviles con otros dispositivos utilizando opciones como tethering, wifi o USB [2].

Esta propuesta también resulta eficiente en ambientes donde el acceso a Internet es limitado ya que resulta priorizar ciertos servicios o dispositivos en una oficina, entornos académicos o también en redes domésticas avanzadas, facilitando el dispositivo móvil como proveedor de Internet dando una flexibilidad temporal de acceso emergente al Internet sin depender de infraestructura física.

Finalmente, se adquiere la oportunidad de implementar una solución de red utilizando un dispositivo Mikrotik CRS310-1G-GS-4S+IN permitiendo configuraciones avanzadas de balanceo de carga, segmentación de VLANs y gestión de ancho de banda para QoS, con este equipo podemos dar una solución garantizada a los posibles fallos de Internet dando una continuidad de servicio, también configurando conexiones primaria y secundaria, optimizando el tipo de gestión de los recursos de la red y organizando el tráfico[3].

1.2. Objetivo general

Implementar una red de distribución de Internet usando un equipo MIKROTIK, segmentando la red mediante VLANs y gestión del ancho de banda en cada segmento para la optimización de recursos.

1.3. Objetivo específico

- Configurar balance de carga entre una conexión de fibra óptica y un enlace móvil de respaldo, basado en la compartición móvil para asegurar la continuidad del servicio en caso de falla mediante conmutación automática (failover).
- Establecer las VLANs en distintos entornos en una línea troncal para garantizar la comunicación controlada y un acceso seguro de recurso internos.
- Implementar QoS en aplicaciones críticas y departamentos prioritarios para un mejor rendimiento de la red.
- Validar el tráfico de la red mediante herramientas integras en el equipo para garantizar que las configuraciones cumplan con los requisitos.

1.4. Justificación

El crecimiento de las redes informáticas, también depende en distintos ambientes empresariales el cual se requiere soluciones vigorosas que demuestren la disponibilidad continua del Internet, con esto se requiere la seguridad de los datos con una gestión eficiente del tráfico de las interfaces o áreas planteadas, para el proyecto planteado se justifica por la necesidad de abordar problemáticas comunes como la gestión de redes empresariales, como interrupciones en el servicio de Internet congestión de ancho de banda y falta de segmentación adecuada en el tráfico.

Uno de las principales explicaciones que sustentan este proyecto es la importancia de contar con una infraestructura de red capaz de garantizar la continuidad del servicio, por medio de la implementación de un balance de carga que sea receptado por fibra óptica como enlace primordial y móvil como un enlace de respaldo, y así se asegura la disponibilidad del Internet, incluso en caso de fallas del enlace principal, este método incluye una conmutación automática de failover que es crítico para minimizar interrupciones que puedan afectar las operaciones de una organización [4].

La segmentación de la red mediante VLANs, que representa una parte esencial para mejorar la seguridad y eficiencia, en la gestión de tráfico de la red, al dividir la red en áreas lógicas el cual nos proporciona el control del acceso a los recursos internos y minimizar riesgos asociados a vulnerabilidades de seguridad que se dan en las redes internas, entre estos enlaces esta la segmentación que facilita la gestión de cada grupo al configurarse y así mismo monitorearlas de manera independiente [5].

Consiguiente la ejecución de políticas de QOS, es fundamental para optimizar el uso del ancho de banda ya que este proyecto prioriza aplicaciones críticas, utilizadas en departamentos esenciales garantizando que las tareas más importantes cuenten con la capacidad necesaria para un funcionamiento óptimo, el cual esta característica es particularmente relevante en entornos empresariales donde múltiples usuarios y dispositivos compiten por recursos limitados [6].

En el último procedimiento se realizó la utilización de herramientas de monitoreo y análisis del tráfico de la red el cual no solo permitirá validar las configuraciones, sino que también, proporcionar datos para futuras optimizaciones a beneficio de red, con ello se busca reforzar el enfoque preventivo y proactivo del proyecto para asegurar un desempeño estable y eficiente de la red

Finalmente, este proyecto no solo responde a una necesidad técnica porque también busca contribuir beneficios tangibles tales como una mayor continuidad operativa, y mejorar la gestión de recursos tecnológicos y un incremento en la seguridad de la red ya que por estas razones se considera, una propuesta viable, escalable y alineada con las necesidades en redes empresariales.

1.5. Metodología

Investigación Exploratoria

En la primera fase se realizará una revisión profunda de las técnicas de la literatura técnica y científica relacionada con el balance de carga, la segmentación de VLAN y la distribución del ancho de banda en distintas áreas en redes empresariales, cuyo análisis estará inmerso en el estudio de las funcionalidades y configuraciones realizadas de los equipos Mikrotik de esa manera, las mejores prácticas en la implementación de políticas de calidad de servicio y failover se podrá

mejorar el acceso a Internet mediante fibra óptica y móvil, que están inmersa en la arquitectura, con investigación exploratoria nos ayudara a entender los fundamentos teóricos y técnicos necesarios para desarrollar el proyecto práctico así como identificar los beneficios y desafíos asociados a cada tecnología involucrada.

Diseño Experimental

Se configurará un entorno controlado para replicar la arquitectura de red planteada en el proyecto, en este apartado se integrara configuración de un equipo CRS310-1G-5S-4S+IN y será como un equipo principal en la arquitectura, el balanceo de carga entre un enlace de fibra óptica y un enlace móvil, son el acceso a Internet, se implementará la segmentación de la red VLANs como, administración, cámaras, sala de cómputo y red de invitados agregando los rangos de IP y políticas específicas para cada segmento, configurado se diseñarán y probarán reglas de QoS para priorizar aplicaciones críticas y garantizar un uso eficiente del ancho de banda.

Pruebas de Configuración

En este proceso se empleará las pruebas prácticas para verificar el correcto funcionamiento de las configuraciones realizadas el cual se evaluara el balance de carga y la conmutación automática failover en que se realizara varias pruebas de falla del enlace principal y se analizará la correcta comunicación y seguridad entre las VLANs, mediante herramientas de monitoreo y diagnóstico del equipo, la evaluación realizadas incluirán simulaciones de saturación de ancho de banda para validar las reglas de QoS y el rendimiento de la red.

Monitoreo y Validación

finalmente se emplearán tecinas para monitorear el tráfico de la red utilizando herramientas integradas en MikroTik con esto se busca analizar el tráfico de la red y evaluar la efectividad de las configuraciones implementadas en esta arquitectura, la evaluaciones nos llevaran a notar posibles cuellos de botella que pueden surgir en tráfico de datos, el ajustes necesarios en las políticas de QoS y optimizaciones en la segmentación de las VLANs, los procesos recopilados de las evaluaciones serán documentados y servirán como base para la optimización final de la red.

CAPÍTULO II

2.1 Fundamentos en administración en redes

2.1.1 Definición de administración de redes

La administración de redes se conforma en un conglomerado de desarrollos, que requiere la arquitectura mediante la gestión de herramientas y técnicas empleadas para administrar y mejorar los recursos de la red en un ambiente empresarial, con esto buscamos englobar la configuración y mantenimiento de dispositivos de red, tales como equipos routers, puntos de acceso y switch con el propósito de gestionar las redes y garantizar una ejecución efectiva y al mismo tiempo que sea segura y confiable para minimizar interrupciones que involucren la comunicación fluida entre los usuarios y las aplicaciones [7].

En el contexto institucional nos conlleva, no solo asegurar el funcionamiento de red, sino también organizar y preparar próximas necesidades para gestionar el tráfico y utilizar reglas de protección que mantengan segura la información sensible. Además de eso el manejo de redes para favorecer en protocolos estándares como SNMP (Simple Network Management Protocol) y herramientas propias para la monitorización y configuración para acceder a un control centralizado y efectivo.

2.1.2 Importancia de administración de redes empresariales

La importancia de las red en entornos empresariales tanto la administración de redes tiene un fin estratégico y beneficioso porque podemos garantizar la continuidad del acceso a Internet sin interrupciones, para asegurar servicios intangibles de una empresa tales como aplicaciones de negocio, sistemas de comunicación y plataformas en la nube, que suelen ser utilizadas por los mismos, esto quiere decir que es una necesidad que el acceso a Internet estén disponibles en todo momento, y así brindar una red bien administrada que permite identificar y resolver problemas de manera proactiva antes de que afecten a los usuarios finales.

La protección es otro fundamento importante en la administración de redes empresariales, en un ambiente donde los ataques cibernéticos son cada vez más comunes para una administración efectiva se permite implementar procesos de prevención y defensa como segmentación de VLANs y políticas de acceso, para proteger datos sensibles y mantener la integridad del sistema [8].

También optimizar los recursos del acceso brindando es primordial que mantenga una adecuada administración dentro de la red, con esto se hace posible que las aplicaciones y servicios esenciales, no tengan un congestionamiento de tráfico de datos y así mismo expandiendo el desempeño general de la red, con esto también conlleva a una gestión más eficaz del ancho de banda y una correcta asignación de direcciones IP, especialmente en redes empresariales.

Finalmente, la gestión de redes es fundamental, para la capacidad de expansión y evolución de las infraestructuras empresariales, no obstante, a medida que las empresas crecen o adoptan nuevas tecnologías tales como, Internet de las cosas o la inteligencia artificial por eso es fundamental crear una red bien gestionada que permite añadir estos avances de una manera más dinámica y eficiente para poder garantizar su compatibilidad y funcionalidad.

Asimismo, la administración de redes no solo es un constituyente técnico, es decir también un fundamento estratégico, en los ambientes empresariales actuales que lleva a cabo su promulgación efectiva que permite que las organizaciones operen de manera más eficiente, segura y preparada para enfrentar los retos tecnológicos del futuro.

2.2 Cloud Router Switch Mikrotik

2.2.1 Características y funcionalidades de los equipos Mikrotik

El equipo Cloud Router Switch modelo CRS310-1G-5S-4S+IN como se ve en la figura 1 es un dispositivo robusto para el diseño para ambientes empresariales incluso en implementaciones de proveedores de servicio de Internet, ya que exige un alto rendimiento y confianza, asimismo nos brinda una funcionalidad avanzada que destacan sus características y funcionalidades principales como, Puertos y conectividad avanzada, el desempeño mejorado con tecnología moderna, y el diseño optimizado para entornos interiores, la versatilidad en la implementación y adaptabilidad en entornos difíciles [9].



*Figura 1 Cloud router switch
Fuente: Elaborado por autor*

Puertos y conectividad avanzada

- Constan con cinco puertos SFP de 1G también cuentan con puertos SFP+ de 10G que son perfectos para la integración de la fibra óptica el cual se demandan conexiones de alta velocidad con bajas latencias.
- También tiene puerto Gigabit Ethernet añadida ya que con esa conexión directa al equipo (switch) está garantizando la máxima velocidad y compatibilidad con PoE-in que al mismo tiempo tiene ingreso de energía para flexibilidad en la alimentación.
- El dispositivo también cuenta con un Soporte para conexiones de fibra óptica confiables que pueden ampliar hasta 100 metros o más, convirtiéndolo en una de las opciones mejores que el cobre, que es utilizado en ambientes donde las interferencias electromagnéticas o la seguridad son una preocupación.

Desempeño mejorado con tecnología moderna

Cuenta con un rendimiento optimizado gracias a una tecnología de vanguardia por el motivo que este equipo integra una CPU ARM v7 98DX226S y 256 MB de RAM que garantiza la robustez para realizar tareas avanzadas como es la administración de redes con nuevo chips de conmutación Marvell, que afirman un beneficio superior con un soporte para procesamiento de paquetes a nivel hardware así mismo otras de las opciones tienen el filtrado de VLAN y el enrutamiento de capa 3 descargados por hardware maximizan la eficiencia al liberar recursos del sistema es un equipo con bastantes capacidades para entornos exigentes, es decir que este equipo combina potencia y modernidad en cada operación.

Diseño optimizado para entornos interiores

En áreas interiores para este equipo muestra, una planificación compacta y firme para montaje en el rack en estándar de 1U que es ideal para mantener instalaciones organizadas y a su vez profesionales, el equipo internamente cuenta con su sistema de refrigeración mejorado garantiza y estabilidad operativa incluso en condiciones prolongadas e exigentes, con estas características se busca la combinación de funcionalidad profesional y estética en una solución perfecta para ambientes con alto rendimiento y orden sin complicar la eficacia.

Versatilidad en la implementación

Este equipo fue diseñado para ofrecer versatilidad en la implantación e instalación, porque el cual es perfecto para ISP pequeños o medianos, que buscan soluciones con respecto a la fibra óptica, específicamente para enlaces de 10 Gigabits, es por eso que su tecnología asegura bajas latencias y una mínima pérdida de datos por eso que incluso en redes que superan los 100 metros de distancias, con esas características lo convierte en una herramienta esencial para extender la estabilidad y el rendimiento en ambientes exigentes y su vez garantizando una conectividad.

Adaptabilidad en entornos difíciles

Este equipo cuenta con una excelente adaptabilidad en entornos difíciles porque brinda un soporte para PoE-in que facilita su instalación e implementación en lugares complicados, al facilitar las exigencias de alimentación eléctrica ya que ingresa por el puerto ether1, y el equipo está diseñado particularmente hacia lugares internos el cual combina acople rápido para la instalación con un robusto entorno de funciones, es más son ideales para redes empresariales y proyectos especializados, por eso se convierte en el procedimiento perfecto para plantarse desafíos técnicos sin comprometer el rendimiento ni la eficiencia en instalaciones complejas.

2.2.2 Comparativas con otros dispositivos de red

En los equipos MikroTik son fuertemente competitivo ante otras marcas comunes en telecomunicaciones, existen marcas líderes en el mercados nacionales e internacionales como lo son Cisco y Ubiquiti por eso existe una perspectiva que se presenta en una tabla comparativa que selecciona beneficios claves en los diferentes equipos.

Distintivo	MikroTik	Cisco	Ubiquiti
Precio	Bajo	Alto	Medio
Disposición de configuración	Media	Compleja	Alta
Capacidad VLAN y QoS	Alta	Alta	Media
Herramientas internas	Amplias	Limitadas	Limitadas
Escalabilidad	Alta	Muy alta	Media
Soporte técnico	Existe grupos activos con costo adicional para dar soportes profesionales.	Soporte premium incluido (alto costo)	Existe grupos activos con costo adicional para dar soportes profesionales.
Manejo y flexibilidad	Muy alta	Alta	Media
Consumo energético	Bajo	Variable	Bajo

*Tabla 1. Comparativa de equipos de diferentes marcas
Fuente: Elaborado por autor*

En esta tabla 1 podemos observar que MikroTik es una opción recomendable para proyectos el cual se buscan un balance entre costos y una flexibilidad de instalación, lo cual hace especialmente atractivo para pequeñas y medianas empresas, ya que son para las partes operativas de la red con presupuesto limitado.

2.2.3 Especificaciones y aplicaciones

Especificaciones

Las especificaciones de este equipo CRS310-1G-5S-4S+IN ofrecen un rendimiento confiable ya que integra el sistema operativo RouterOS con licencia nivel 5, el cual proporciona herramientas evolucionadas para la gestión de redes, es decir las descripciones técnicas por parte del equipo.

Descripción	Complemento
Modelo	CRS310-1G-5S-4S+IN
Puertos Ethernet 10/100/1000	1
Puertos SFP	5
Puertos SFP+	4
Puerto de consola	RJ45
Arquitectura	ARM de 32 bits
CPU	98DX226S
Número de núcleos de CPU	1
Frecuencia nominal de CPU	800 MHz
Dimensiones	200 x 166 x 45 mm
Licencia del sistema operativo	Nivel 5
Sistema operativo	RouterOS
Tamaño de RAM	256 MB
Tamaño de almacenamiento	16 MB
Tipo de almacenamiento	Flash
Temperatura ambiente probada	-40°C a 70°C
Número de entradas de CC	2 (toma de CC, PoE-IN)
Voltaje de entrada del conector CC	18-57 V
Consumo máximo de energía	20 W
Consumo máximo de energía sin accesorios	8 W
Tipo de refrigeración	1 ventilador
PoE in	802.3af/at
Voltaje de entrada PoE	18-57 V

*Tabla 2 Especificaciones y aplicaciones Mikrotik
Fuente: Elaborado por autor*

En esta tabla 2 podemos ver ciertas especificaciones que se pueden dar y tener conocimientos del equipo para poder ser manipulados con eficiencia.

Aplicaciones

El equipo CRS310-1G-5S-4S+IN de MikroTik es un switch enrutador robusto y potente que está diseñado para satisfacer diversas aplicaciones en redes empresariales y proyectos con ISP los cuales también son en ciertos entornos educativos y soluciones de red en interiores.

Estudio	Complemento
Redes empresariales	Segmentación de tráfico mediante VLAN para gestionar muchos departamentos o áreas.
	Para poder garantizar la disponibilidad continua de acceso a Internet es necesario un equilibrio y conmutación de error
Proyectos ISP pequeños y medianos	Conexiones de fibra óptica con velocidades de hasta a 10 Gbps para distribución 10 Gbps y servicios para la distribución.
	equipos en ubicaciones remotas o con acceso limitado a la electricidad.
Entornos de laboratorio y educativos	Las pruebas de segmentación y monitoreo de tráfico escuchasen realizan utilizando herramientas avanzadas de RouterOS las pruebas se realizan utilizando herramientas avanzadas de RouterOS.
	En entornos educativos las configuraciones, se utiliza para crear redes sólidas Fuerte y eficiente.
Soluciones de red en interiores	Diseño para compacto estándar instalaciones de rack 1U en centros de datos pequeños e Instalaciones de rack en pequeños centros de datos.
	El funcionamiento es fiable incluso a temperaturas extremas es una temperatura que oscilan entre -40 °C y 70 °C.-40°C a 70°C.

*Tabla 3 Estudio y complemento de uso
Fuente: Elaborado por autor*

En esta tabla 3 podemos ver ciertas aplicaciones que se pueden dar y tener conocimientos en que áreas podemos implementarlos.

2.3 Balance de carga

2.3.1 Concepto de balance de carga

Las unidades MikroTik se pueden hacer configuraciones significativas tal como el balance de carga, que radica en direccionar el tráfico de la red tanto el acceso que ingresa y el tráfico que sale, entre ellos están las conexiones red de área amplia también llamado WAN, utilizando para desarrollar reglas de tráfico de la red, Con esta función nos aprueba desarrollar el ancho de banda disponible y así poder reducir la latencia para garantizar un servicio sin interrupciones, ya que el equipo MikroTik utiliza metodologías como PCC (Per Connection Classifier), ECMP (Equal-Cost Multi-Path Routing) y failover para proporcionar herramientas eficaces hacia para administración de múltiples conexiones simultáneamente y mejorar el rendimiento general de la red [10].

2.3.2 Métodos de balanceo de carga

Para el balance de carga en equipos Mikrotik existen varios tipos de balanceo y están adaptados a distintos escenarios el cual se puede utilizar, con estos métodos podemos incluir diferentes tipos de balance tales como **Per Connection Classifier (PCC)** que consiste en clasificar los enlaces según parámetros establecidos o necesidad incluyente, **NTH** es un tipo de balance que direcciona el tráfico de forma uniforme en intervalos determinado y el balanceo **Equal-Cost Multi-Path Routing (ECMP)** que se utiliza rutas de semejante coste para balancear el tráfico, el cual se presenta en una tabla con una representación breve de cada técnica de balanceo.

Técnica	Representación	Ventajas	Limitaciones
PCC	Clasifica las conexiones en función de parámetros como IP y puertos para garantizar la coherencia.	Flexible y eficiente para flujos continuos.	Requiere configuración avanzada.
ECMP	Utiliza rutas de igual costo para equilibrar automáticamente el flujo de tráfico.	Configuración sencilla que es compatible con rutas estáticas.	Control reducido sobre ciertos flujos.
NTH	Divide los paquetes en intervalos específicos y distribuye el tráfico de manera uniforme.	Se pueden implementar redes simples y fáciles.	No se garantiza la coherencia para conexiones persistentes.

*Tabla 4 Técnicas de balanceo de carga
Fuente: Elaborado por autor*

En esta tabla 4 podemos ver ciertas técnicas de balanceo de carga que se pueden dar y tener conocimientos en que áreas podemos implementarlos.

2.3.3 Balanceo entre la fibra óptica y LTE

Para conformar tipos de balance entre fibra óptica y móvil permite mezclar la alta velocidad y estabilidad de la fibra, con la flexibilidad de LTE como respaldo, ya que los equipos MikroTik administra los dos enlaces como tipo WAN utilizando reglas personalizadas acorde a la necesidad, el cual se asignan tráfico según parámetros como prioridad o carga con esto se asegura que las aplicaciones críticas usen la conexión de fibra, mientras que el móvil actúa como un enlace adicional para la redundancia o para manejar picos de tráfico, maximizando la capacidad disponible de la red.

2.3.4 Conmutación automática(failover)

El failover en equipos MikroTik responde la continuación del servicio al momento de pasar de un extremo a otro automáticamente entre enlaces de acceso es decir que cuando alguno de los accesos tiene algún fallo, esto se crea mediante la supervisión continua de las conexiones WAN ya que con las herramientas como **Netwatch** o rutas estáticas, son con localización de disponibilidad (check-gateway) ya que en situaciones de enlace primario como fibra óptica deje de estar activo, el tráfico se direcciona al enlace secundario como lo es el móvil sin interrupciones perceptibles para los usuarios, asegurando alta disponibilidad en la red.

2.4 Segmentación de VLANs

2.4.1 Concepto de segmentación de VLANs

La segmentación de Redes de Área Local Virtual (VLANs) es una configuración y a su vez una práctica primordial ya que es ocupada en diseño de redes, esta práctica es esencial en arquitecturas en el diseño de redes modernas, es este proceso se especificará conceptos relevantes básicos pero importantes.

Una **VLAN** es una red lógica que integra un conjunto de dispositivo en conexiones físicas en infraestructuras agrupadas, pero el cual se realizan la segmentación de manera virtual, con este detalle nos dice que los equipos o dispositivos que estén conectados a diferentes VLAN y no sean identificados entre ellos y no puedan comunicarse entre sí, al menos que la configuración se lo requiera.

Las VLAN suelen ser configuradas en switches y routers para:

- Individualizar el tráfico entre áreas o departamentos dependiendo el propósito.
- Optimizar y administrar el ancho de banda.
- Mejorar y monitorear la gestión y administración de la red.

2.4.2 Ventajas de las VLAN

En este apartado se detallarán aspectos esenciales que debemos conocer ya que se considera ventajas para la instalación e implementación de las VLANs tanto en la parte de seguridad, administración, reducción de tráfico, optimización, flexibilidad y compatibilidad de QoS.

Ventaja	Descripción
Seguridad	Limita riesgo de ataques internos acceso entre áreas.
Mejor administración	es más fácil asignar y gestionar recursos para cada departamento o área. y gestionar recursos en función de las necesidades de cada departamento o área.
Reducción de tráfico de difusión	Al mantener la difusión de paquetes dentro de la misma VLAN, se mejora el rendimiento de la red.
Optimización del ancho de banda	Reduce la congestión de la red al dividir los grupos que producen mucho tráfico. dividiendo los grupos que producen mucho.
Flexibilidad	La red se debe reconfigurar lógicamente sin realizar cambios físicos en la infraestructura.
Compatibilidad con QoS	permite priorizar más fácil o priorizar tráfico crítico, como aplicaciones comerciales o videoconferencias.

Tabla 5 Ventajas y descripciones VLANS

Fuente: Elaborado por autor

En esta tabla 5 podemos ver ciertas ventajas que nos brinda al configurar VLANS el cual se puede tener conocimientos para su implementación y monitorización.

2.4.3 Seguridad en las VLAN

La segmentación por VLAN no es solo materne y guiar en tráfico de la red, porque a su vez refuerza la seguridad al implementar barreras lógicas entre dispositivos y áreas porque con esto conlleva a la separación de enlaces, los primordiales aspectos de seguridad que aporta la configuración de VLANs son aislamiento del tráfico, mitigación de ataques internos, acceso controlado mediante ACL y reducción de amenazas externas.

Aislamiento del tráfico

La mayor ventaja es que las VLAN permiten segmentar el tráfico de la red, de modo que los dispositivos dentro de una VLAN puedan comunicarse entre sí a la velocidad nativa de la red, el tráfico direccionado algún equipo o dispositivo deber direccionarse por un enrutador firewall o dispositivo similar, en otras palabras, esto permite configurar políticas capaces de bloquear algunos protocolos o cualquier parte de la red.

Mitigación de ataques internos

En redes no segmentadas, una red local permite a un atacante iniciar libremente casi cualquier ataque MITM, rastreo de paquetes o ataques de inundación, por ejemplo, suplantación de ARP. Por lo tanto, el uso de VLAN reducirá la visibilidad en los diferentes segmentos.

Acceso controlando con ACL

Esta opción nos garantiza que solo fluya tráfico en las comunicaciones necesarias entre las VLANs permitidas de manera que se pueda controlar el acceso con listas configuradas para permitir y denegar el tráfico entre las mismas.

Reducción de amenazas externas

En algunas redes conectadas a Internet, la exposición de algunos dispositivos al exterior es normal, por ejemplo, es necesaria para servidores web o cámaras IP, las VLAN pueden utilizarse para separar esos dispositivos del resto de la red de modo que, en la remota eventualidad de que un dispositivo se vea de algún modo comprometido por un atacante, éste no tenga acceso a otros segmentos, posiblemente ya que muchos son más sensibles.

2.5 Gestión del ancho de banda

2.5.1 Importancia de la gestión de ancho de banda

Gestión de ancho de banda sería un aspecto fundamental de la gestión de los recursos de una red. Esto es especialmente importante en entornos empresariales o en situaciones donde haya una alta densidad de usuarios. Para ello la solución es dar prioridad al tráfico crítico (videoconferencias, permitir el acceso a bases de datos, ...) pues, al final, estas tareas son por norma general de sobras más importantes que las que en su mayoría no son urgentes, pudiendo de esta manera garantizar que el sistema de red vaya bien y que los usuarios obtengan la mejor experiencia posible. Además de esto, cabe añadir que esto ayudará a prevenir problemas de congestión y colisiones en la red fortaleciendo así su estabilidad y rendimiento. Las herramientas avanzadas en los dispositivos MikroTik nos permiten establecer límites, sin asignar distintos niveles de prioridades y observar el uso del ancho de banda para que la red no solamente esté operativa, sino que, además, podrá ser ampliada sin ningún tipo de problemas.

2.5.2 Calidad de servicio (QOS)

La Calidad de Servicio, o QoS, hace referencia a un conjunto de prácticas que sirven para manejar el tráfico en una red, priorizando ciertas clases de tráfico frente a otras. Con el objetivo de que las aplicaciones adecuadas mantengan niveles sólidos de rendimiento, sin tener en cuenta que MikroTik QoS permite reservar ancho de banda, limitar latencias y prevenir la pérdida de paquetes, aspectos fundamentales para servicios como VoIP, streaming y sistemas financieros; MikroTik utiliza reglas que garantizan que el tráfico de las aplicaciones que necesitan prioridad se ofrezca con nivel de alta prioridad, mientras que el tráfico menos crítico se hace con un nivel de baja prioridad.

2.5.2.1 Principios de QoS

Algunos principios fundamentales de QoS son entre otros el tráfico de tráfico, la priorización y la asignación efectiva de recursos y los principios de QoS y sí, los principios se han establecido para que el tráfico crítico tenga mayor nivel de prioridad frente al tráfico que se considera innecesario en MikroTik, QoS se ha aplicado clasificando el tráfico con la ayuda de reglas definidas por el usuario y aplicándolas en las colas, que tienen algunos parámetros definidos, para incluir el ancho de banda garantizado la capacidad máxima, este enfoque para gestionar los flujos de datos entre las redes, de hecho aumenta la eficiencia general de la red al mismo tiempo que los regula, reduciendo las latencias en la mayoría de los servicios sensibles al tiempo y, por lo tanto, mejorando la experiencia del cliente.

2.5.2.2 Características y descripción de calidad de servicios

Existen características que nos ayudan a completar un análisis de configuración para QoS para gestionar de manera adecuada y segura en una red establecida en los equipos Mikrotik.

Características	Descripción
Clasificación de tráfico	La clasificación de tráfico permite identificar y separar paquetes por dirección IP, puerto o tipo de servicio.
Colas simples y jerárquicas	Configura límites y prioridades de ancho de banda, desde nodos individuales hasta segmentos.
Priorización de tráfico	Prioriza aplicaciones y servicios en función de su criticidad.
Limitación de ancho de banda	Establece límites para evitar la saturación y asegurar una utilización óptima de los recursos.
Soporte para múltiples colas	Compatible con códigos FIFO, SFQ y HTB para una gestión eficiente del tráfico.
Monitorización en tiempo real	Herramientas integradas para monitorear el uso del ancho de banda y la efectividad de las reglas.

*Tabla 6 Características y descripción de QoS
Fuente: Elaborado por autor*

En esta tabla 6 podemos ver ciertas características con sus respectivas descripciones que nos brinda QoS el conocimiento de instrucciones para su implementación y mejorar conectividad y optimizar recursos al usuario.

2.5.2.3 Ventajas y desventajas

Consigo mismo también se presentan algunas ventajas y desventajas que ocurren en la parte de implementación y configuración, tal com podemos observar en la siguiente tabla.

Ventajas	Desventajas
Configuración flexible y adaptable.	Requiere conocimientos avanzados para su uso.
Mejora la experiencia en aplicaciones críticas.	Puede ser complejo en redes grandes.
Integración nativa con herramientas MikroTik.	La configuración inadecuada puede causar problemas de rendimiento.
Monitoreo efectivo para ajustes dinámicos.	Limitaciones en redes con enlaces altamente saturados.

*Tabla 7 Ventajas y desventajas de QoS
Fuente: Elaborado por autor*

En esta tabla 7 podemos ver ciertas ventajas y desventajas que pueden surgir en la calidad de servicio (QoS) el cual se puede tener instrucciones y prevenciones.

2.5.3 Herramientas para el monitoreo y optimización del tráfico de red

Monitorear y optimizar el tráfico de red son de la mayor importancia para preservar y asegurar un rendimiento óptimo de la infraestructura de red ya que sus equipos MikroTik, cuenta con una serie de herramientas para manejar el tráfico de manera efectiva, y para poder detectar algunas falencias y garantizar que el ancho de banda sea utilizado de una manera óptima, las cuales Son:

- Traffic Flow (NetFlow)

Por qué se dice que esta herramienta toma la máxima información sobre el tráfico del lado de la red para realizar clasificación y descubrimiento de tráfico en tiempo real y clasificar patrones en el tráfico para tomar decisiones de asignación de recursos.

- Torch

Esencialmente magnifica lo que ves, en tiempo real, con las IP de origen y destino, así como los puertos utilizados junto con el tipo de tráfico Túnel Torch es ideal para cuellos de botella y información sobre tráfico no deseado.

- Queue Tree

Se utiliza para agrupar y priorizar el tráfico en su red para que pueda pagar todas las facturas a la vez con la programación suficiente, esto mantiene todas las aplicaciones críticas en su ancho de banda completo en todo momento, mientras que categoriza el resto como tráfico.

- Bandwidth Test

Las Prueba de ancho de banda para medir el potencial de ancho de banda REAL de su red y averiguar si está siendo obstaculizado en la infraestructura/implementar soluciones para solucionar los cuellos de botella.

- Graphs

Proporciona una instantánea de la utilización del ancho de banda y la carga de la red durante diferentes zonas horarias, esto le permite ver qué hacer y avanzar en caso de alguna optimización de la red

- Netwatch

Es ideal para vigilar la disponibilidad de dispositivos o servicios en su red esto puede configurar reglas de monitoreo para vigilar interrupciones en el servicio y el equipo, y hacer que alcance automáticamente cosas como reinicios de dispositivos o cambios de conexión.

- Tracerouter, Ping

Esas opciones de configuración se utilizan para analizar y verificar conexiones con otras direcciones o servidores para ver si existe una conexión y establecer PING que se considera como una herramienta que diagnostica las conexiones entre IP o servidores, el cual funciona enviando paquetes de solicitud al Internet Control Message Protocol (ICMP) la dirección gestionada el cual nos mide un tiempo de latencia de conexión tanto de ida y de regreso, así mismo detecta la pérdida de paquetes y el TRANCEROUTE es conocido como una herramienta que rastrea los paquetes desde la parte de donde se originan hasta la parte de destino, esta herramienta de análisis envió paquetes a los protocolos ICMP Y UDP y los resultado nos enlista los dispositivos intermediarios en los tiempos.

- **NAT LOGS Y FIREWALL**

Estas herramientas son beneficiosas para la gestión de redes en su mayoría se consideran herramientas para monitorear, analizar la seguridad y monitorear tráfico generado en la red, NAT LOGS mantiene el propósito de registrar las traducciones de IP privada a IP pública manteniendo un nivel de operación con la gestión de las direcciones IP direccionando conexiones internas hacia el Internet, y FIREWALL LOGS es una herramienta que son registros que documentan el tráfico en la red el cual muestra las conexiones bloqueadas y permitidas.

2.6 Acceso móvil y fibra óptica

2.6.1 Ventajas de acceso móvil en redes

El acceso móvil en redes suministra en flexibilidad y conveniencia al poseer una conexión desde cualquier lugar con cobertura el cual es una cobertura inalámbrica, es perfecto donde la instalación sea para entornos donde la movilidad es necesaria por su fácil implementación también ofrece una disposición rápida y adaptándose ligeramente a cambios en la infraestructura, como sabemos también cuenta con las tecnologías móviles que se puede alcanzar un rendimiento elevado en técnicas de velocidad y latencia, por esto se facilita las aplicaciones que requieren conexiones rápidas para dar el acceso a datos es útil en áreas rurales donde la conectividad de fibra óptica aún no está disponible.

2.6.2 Causas y procedimiento en el uso de acceso móvil

En este apartado notamos problemas y opciones que podemos encontrar en coberturas de redes inalámbricas, direccionada al uso de dispositivos móviles tal como se ve en la tabla de causas y procedimiento.

causas	Procedimiento
Cobertura limitada	Implementación de redes inalámbricas LTE o Wi-Fi híbrido.
Interrupciones de señal	Disponibilidad de dispositivos de repetición o tecnología de optimización de señal.
Seguridad y encriptación	Instalaciones de VPNs y protocolos de encriptación con ello proteger los datos.
Consumo de ancho de banda	Implementación de políticas de QoS para priorizar aplicaciones críticas y limitar el consumo en tareas menos sensibles.
Costo de datos móviles	Optar por planes de datos corporativos o híbridos, que combinen acceso móvil con conexiones fijas.

*Tabla 8 causas y procedimientos en redes móviles
Fuente: Elaborado por autor*

En esta tabla 8 podemos observar ciertas causas y procedimientos que se dan en el uso de coberturas inalámbricas.

2.6.3 Ventajas de acceso de la fibra en redes

El acceso de fibra óptica se está convirtiendo rápidamente en la próxima conexión a Internet de alta velocidad y baja latencia, así que la fibra en aplicaciones requieren un ancho de banda masivo, como videoconferencias o transferencia de datos en tiempo real, la Fibra, al ser menos susceptible a las interferencias electromagnéticas y no perder señal, ofrece rendimiento a un nivel constante en largos tramos de distancia, Por último, al ser una tecnología fiable está lejos de estar congestionada, lo que le confiere más fiabilidad que una conexión tradicional. Del mismo modo, la fibra óptica también es ajustable, lo que permite la escalabilidad que admite requisitos de ancho de banda más altos si es necesario.

2.6.4 Desafíos y soluciones de la fibra

Es este apartado notamos de desafíos y soluciones que podemos encontrar en coberturas de fibra óptica, direccionada al uso de dispositivos móvil tal como se ve en la tabla.

Desafío	Solución
Costo de implementación inicial	Utilización de opciones de financiamiento o asociaciones con proveedores de telecomunicaciones.
Falta de infraestructura en áreas remotas	Expansión gradual de la infraestructura mediante redes de fibra óptica o híbridas.
Interrupciones por daños físicos	Uso de cables de fibra óptica blindados y reforzados, y realización de mantenimientos preventivos.
Instalación compleja	Capacitación de personal especializado y uso de tecnologías de instalación más eficientes.
Limitación en la cobertura	Implementación de enlaces de fibra óptica y tecnologías inalámbricas complementarias para alcanzar zonas de difícil acceso.

Tabla 9 Desafío y soluciones de la fibra óptica

Fuente: Elaborado por autor

En esta tabla 9 podemos observar ciertos desafíos y soluciones que se dan en el uso de coberturas de fibra óptica.

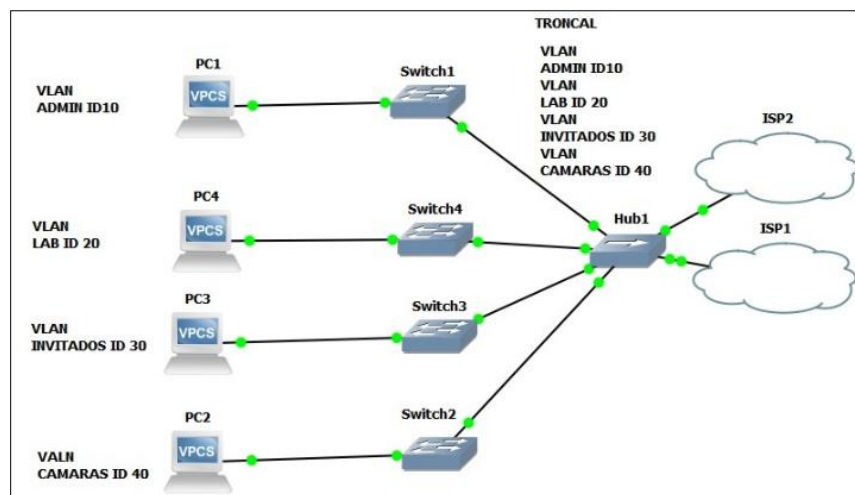
CAPÍTULO III

3.1 Diseño de la arquitectura de la red

3.1.1 Esquema lógico de la red

El diseño presentado en la figura 2 esta simulado en software que representa una topología de red para probar configuraciones esenciales para el proyecto, utilizando VLAN y dispositivos conectados a la red, asignados VLANs específicas, para ir organizando los grupos de dispositivos, que son las siguientes, VLAN para administración, VLAN para laboratorio, VLAN para cámaras y VLAN para invitados, con esto grupos se distribuyen a las conexiones locales mediante líneas troncales y mientras que el ISP1 y ISP2 actúa como punto de agregación conectados al switch principal, con estos dos proveedores de Internet permite redundancia y pruebas de conectividad externa para la red.

Con este diseño es ideal para simular entornos corporativos y así mismo evaluar el aislamiento entre VLAN ya que podemos probar configuraciones de seguridad como listas de control de acceso (ACL) y validar el comportamiento del enrutamiento entre VLAN.



*Figura 2 Imagen de Simulación
Fuente: Elaborado por autor*

3.1.2 Esquema físico de la red

El diseño utiliza switch MikroTik modelo CRS112-8G-4S-IN y modelo CRS310-1G-5S-4S+IN que se muestra en la figura 3 están conectados mediante módulos SFP MikroTik S-31DLC20D con cables de fibra multimodos y conectores LC tanto el switch CRS112 se asignan a áreas específicas, que están interconectados con el CRS310 que actúa como switch central y es gestionado por los dos vía SFP1 con IP 172.1.88.1 y ISP2 vía Ether1 IP 192.168.5.1 el cual la fibra óptica garantiza alta velocidad y estabilidad mientras que la segmentación permite una red segura y eficiente.

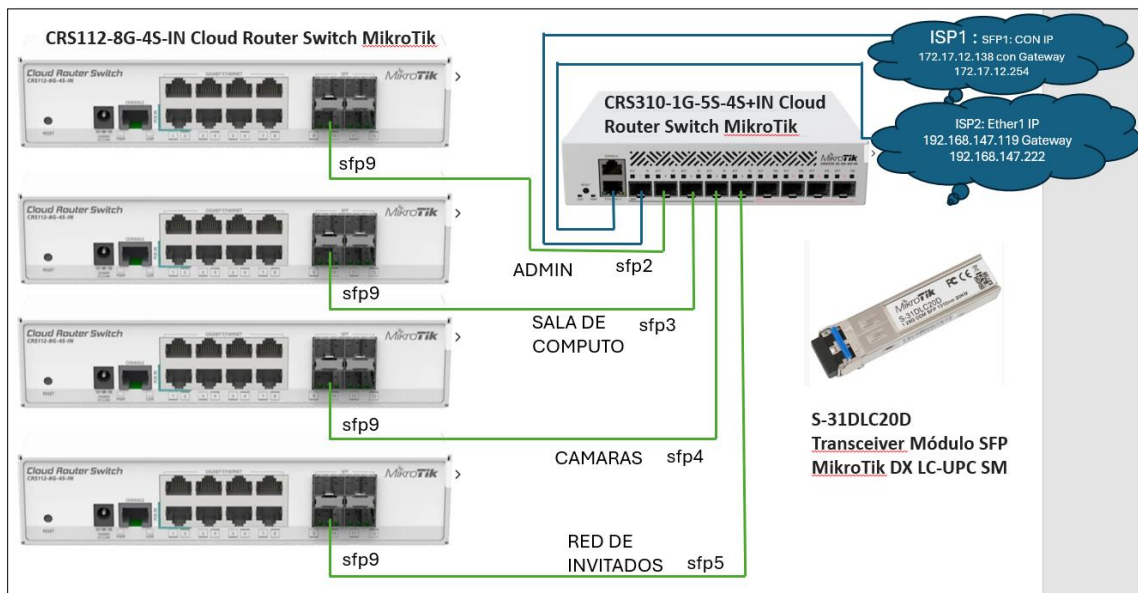


Figura 3 Conexiones entre equipos
Fuente: Elaborado por autor

3.2 Configuración del balance de carga y failover

3.2.1 Detalles de conexiones WAN primaria (fibra óptica)

Para la conexión de fibra óptica fue asignada al puerto SFP1 del MikroTik, primero se fijó el puerto SFP1 en el dispositivo MikroTik CRS310-1G-5S-4S+IN y se insertó el módulo SFP en el puerto, y cuidando que encaje firmemente.



Figura 4 Modulo SFP
Fuente: Elaborado por autor

El módulo SFP como se ve en figura 4 tiene dos ranuras para los conectores de fibra TX y RX así que se conectó correctamente el transmisor de fibra del proveedor en el receptor (RX) del módulo y el receptor del proveedor en el transmisor. (TX) del módulo, utilizando un cable de fibra óptica full dúplex con conectores LC, detallando el módulo utilizado es de marca Mikrotik modelo s-31DLC20D, que es un transceptor óptico diseñado para transmitir datos por medio de la fibra óptica con velocidades de 1.25 Gbps con una longitud de onda 1310 nm con un alcance de hasta 20 km.

Para establecer las configuraciones e implementar la red se realizaron en software winbox y conexión por consola para una configuración rápida y eficaz.

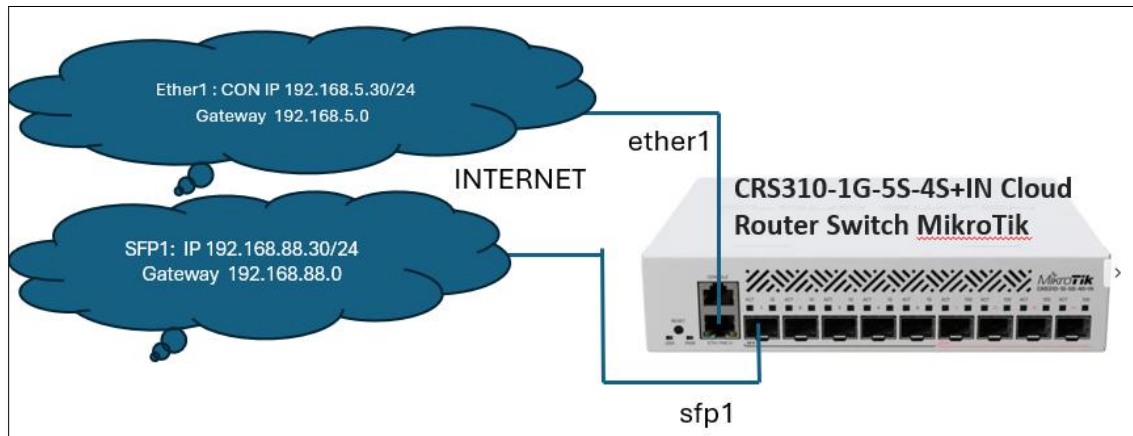


Figura 5 software winbox
Fuente: Elaborado por autor

La figura 5 muestra la aplicación utilizada para las configuraciones, dentro de la interfaz de administración Mikrotik.

3.2.2 Configurar las interfaces WAN (ether1 y sfp1)

Dentro de este apartado asignaremos la IP 192.168.5.30/24 con Gateway 192.168.5.0 en la interfaz Ether1 y 192.168.88.30/24 con Gateway 192.168.88.0 en SFP1 directamente en equipo, añadiremos rutas estáticas con igual distancia hacia ambos Gateway, estableciendo conectividad redundante, esto se puede realizar desde el menú IP > Routes en MikroTik. Para garantizar conectividad óptima, activaremos el monitoreo de rutas (check-gateway) en cada enlace.



*Figura 6 Conexiones de proveedor a los puertos
Fuente: Elaborado por autor*

En esta figura 6 se muestra las conexiones con los puertos y las IP para su implementación.

3.2.2.1 Nombrar las interfaces de acceso

Para generar cambio de nombres a la interfaz ether1 y sfp1 se configura en el apartado INTERFACE en winbox, luego seleccionando ether1 uno se abre una ventana de configuraciones generales el cual se cambiaron por Internet1 y el mismo procedimiento para la interfaz sfp1 se realizó el cambio a Internet2 llevando a cabo la configuración de manera efectiva tal como se muestra el procedimiento en la figura 7.

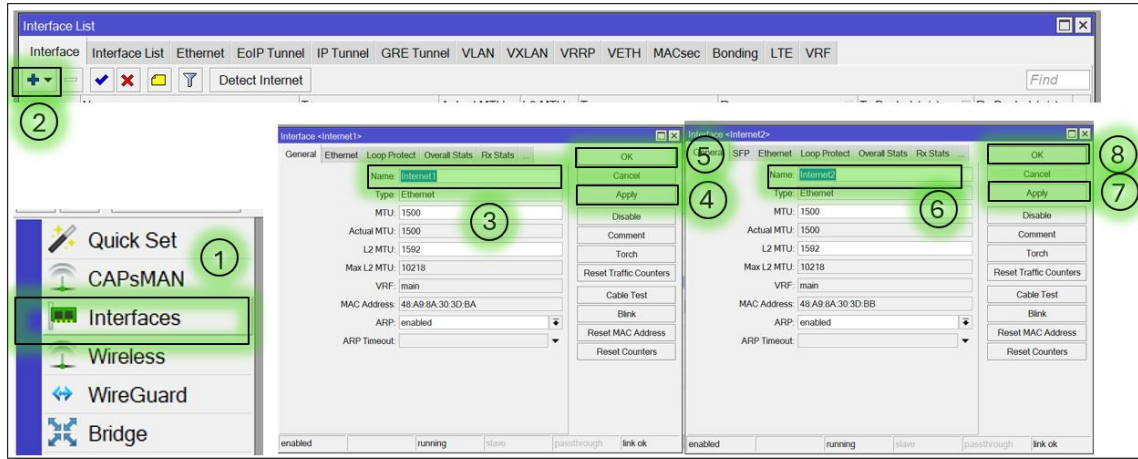


Figura 7 Renombrar las interfaces sfp1 y ether1
Fuente: Elaborado por autor

Esta configuración realizada para renombrar las interfaces de acceso nos facilita el manejo de gestión ya que podemos identificar las interfaces según los ISP de manera que se refleja el propósito que se tiene para aquellas.

3.2.2.2 Asignación de direcciones IP estáticas

Para las asignaciones de IP a cada interfaz se le asignó una dirección IP estática perteneciente a las redes de los ISP, esto establece la conexión entre el dispositivo Mikrotik y los routers de los proveedores de Internet.

Las opciones utilizadas en la figura 8 son **Add** que añade una nueva dirección IP a una interfaz específica **address 192.168.5.30/24** se define la dirección IP asignada a la interfaz **Internet1** de esta dirección, debe estar dentro del rango de la red asignada por el ISP1, en este caso **192.168.5.0/24**, y también **/24** indica una máscara de red de 24 bits, equivalente a **255.255.255.0**, que define el tamaño de la subred, **interface=Internet1** especifica la interfaz donde se aplicará esta dirección IP y por último usamos el comando **comment="WAN 1"**: Añade un comentario para identificar que esta configuración pertenece a la primera conexión WAN.

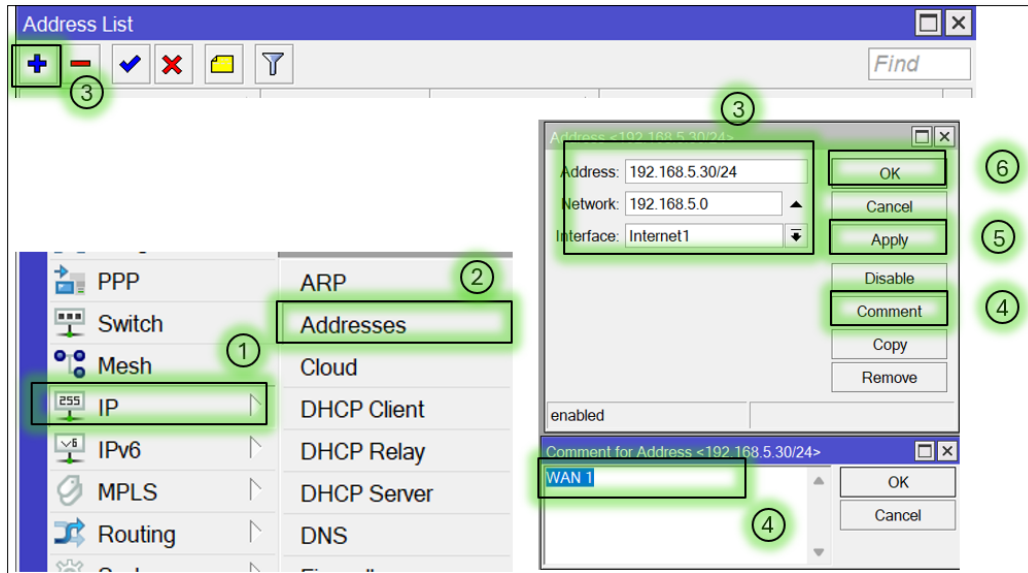


Figura 8 configuración WAN1
Fuente: Elaborado por autor

En la figura 9 de la misma mera para la interfaz ether1 configuramos **address=192.168.88.30/24** se Define la dirección IP asignada a la interfaz **Internet2**, correspondiente a la red de ISP2 en comando **interface=Internet2** que especifica que la dirección IP que debe ser aplicada a la interfaz **Internet2** y por último ocupamos **comment=WAN 2** para marca esta configuración como perteneciente a la segunda conexión WAN.

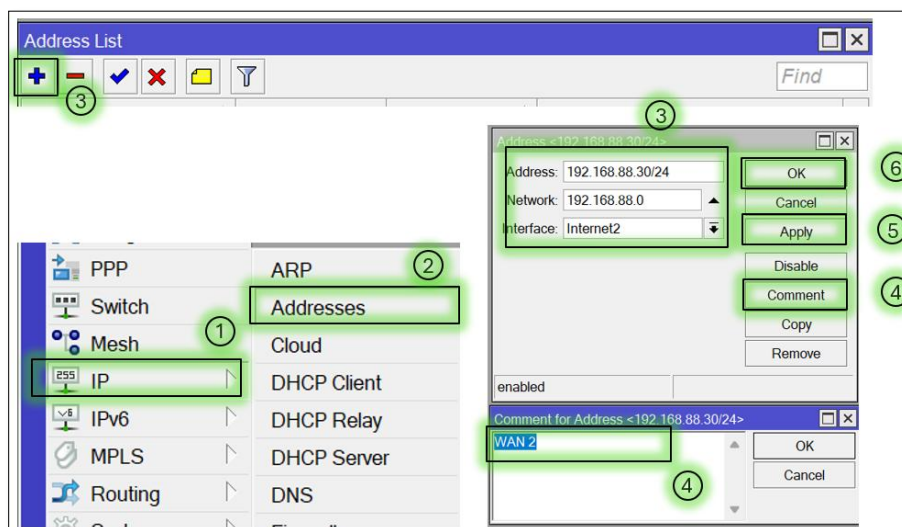


Figura 9 configuración WAN 2
Fuente: Elaborado por autor

3.2.3 Configurar rutas con prioridad con failover

Este enfoque asegura que WAN1 y WAN2 tenga una continuidad de servicio ante fallos existente por esa razón se establecen rutas estáticas para definir el comportamiento del tráfico de red el cual se le da prioridad a la fibra óptica que es una red más estable con prioridad alta y la ruta que es por compartición móvil se le da una prioridad más baja con esto establecemos el direccionamiento como principal y como respaldo.

En la figura 10 configuramos **IP router** se accede al menú de configuración de rutas estáticas en el dispositivo MikroTik luego **add** marcamos **Gateway=192.168.5.1** que define la dirección IP del Gateway de la conexión principal (WAN1) con una **distance=1** que Asigna prioridad más alta también usamos comentarios con **comment="Ruta principal - WAN1"** que proporciona una descripción para identificar esta ruta fácilmente.

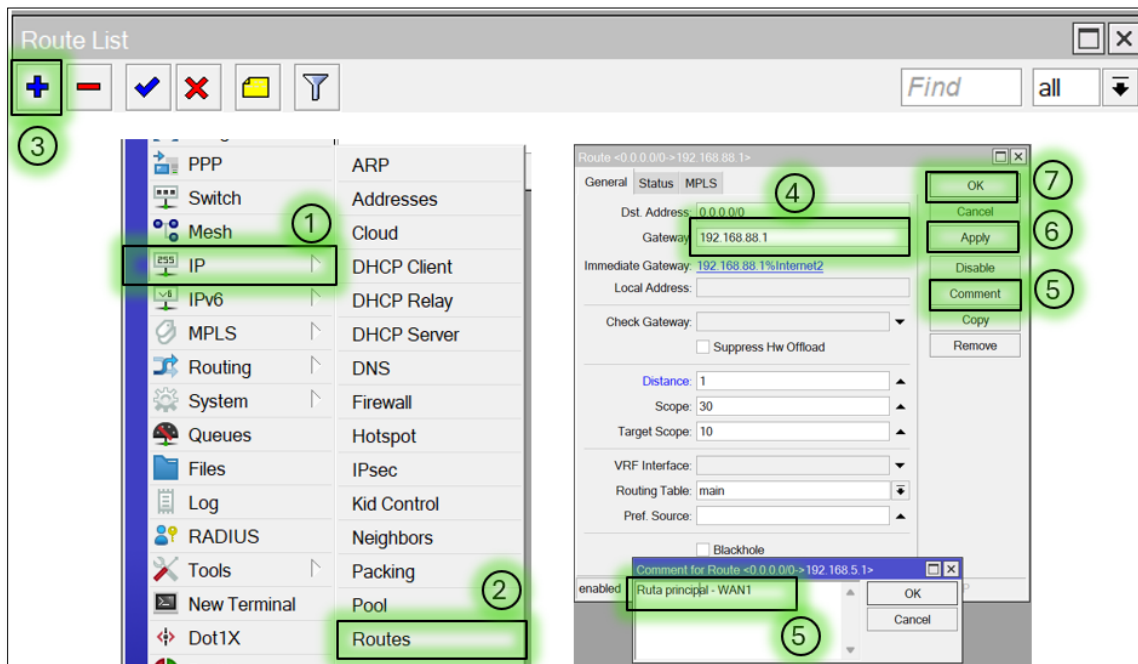


Figura 10 ruta principal para WAN 1

Fuente: Elaborado por autor

En la figura 11 ocupamos **add** luego configuramos **gateway=192.168.88.1** que define la dirección IP del Gateway de la conexión de respaldo (WAN2) utilizamos **distance=2** que nos asigna prioridad más baja y por último usamos **comment=Ruta de respaldo - WAN2**: Agrega una etiqueta descriptiva.

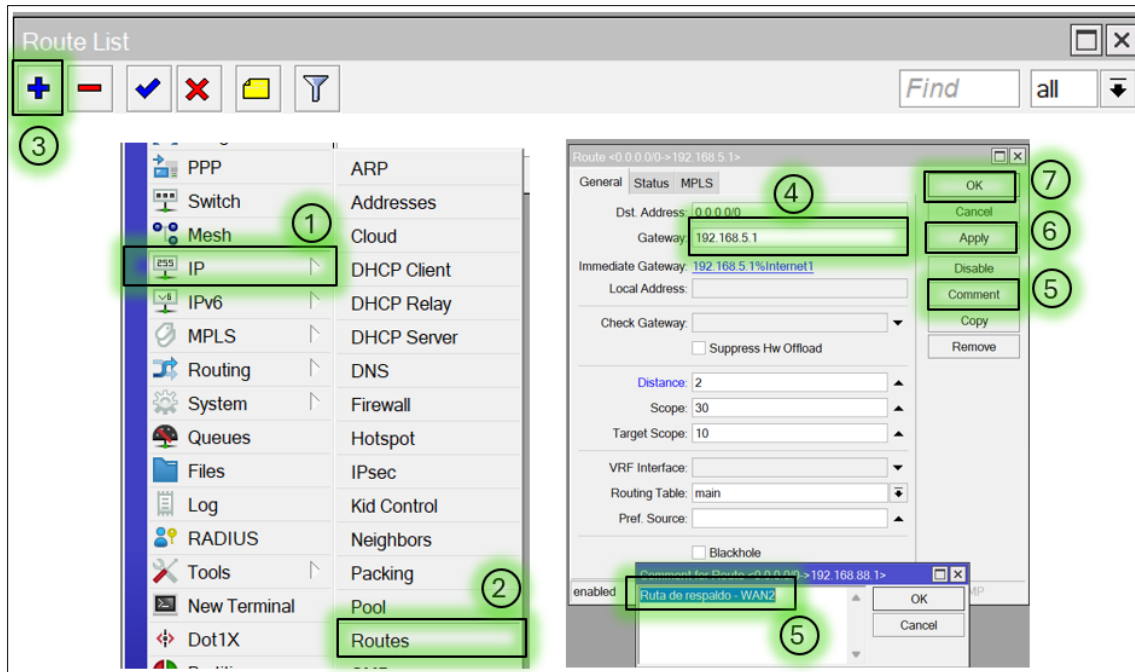


Figura 11 ruta respaldo WAN2
Fuente: Elaborado por autor

Las opciones configuradas son instrucciones dadas para definir configuraciones de enrutamientos en un dispositivo de red con respecto a capa 3 ya que habilita protocolos de enrutamiento como el protocolo RIP, OSPF o EIGRP que son protocolos claves para gestionar el tráfico fluyente dentro y fuera de una red ya sea estática o dinámica.

3.3 Establecer configuraciones de balanceo de carga

Para las configuraciones de balanceo de carga son necesarias las reglas de Mangle que se utilizan para clasificar y marcar el tráfico entrante de la red, es decir WAN1 Y WAN2 que son los proveedores, esto permite gestionar de manera eficiente el balanceo de carga optimizando el uso de los enlaces y distribuyendo la carga de manera eficiente.

Se utilizará un balanceo de carga PCC ya que es un método generalmente utilizado en equipos Mikrotik RouterOS ya que asegura la distribución entre múltiples enlaces de Internet de forma eficiente logrando un uso optimizado, las configuraciones utilizadas son **IP > Firewall > Mangle** que es primordial para marcar paquetes o rutas que permiten la personalización del manejo de tráfico.

En la figura 12 mostramos la configuración del primer marcado de tráfico el cual se debe acceder al menú de configuración de reglas Mangle para modificar o marcar el tráfico en función de criterios específicos luego ocupar **add** para crear, luego vamos a la opción **chain=prerouting** que aplica la regla antes de que el paquete sea procesado por el enrutamiento luego configuramos en la opción **in-interface=Internet1** que especifica la interfaz de entrada WAN1 nos vamos al apartado **action=mark-connection** que marca las conexiones entrantes y configuramos **new-connection-mark=WAN1_conn** que se asigna la marca de conexión WAN1_conn luego se activa la opción **passthrough=yes** que permite que el paquete siga siendo evaluado por reglas adicionales.

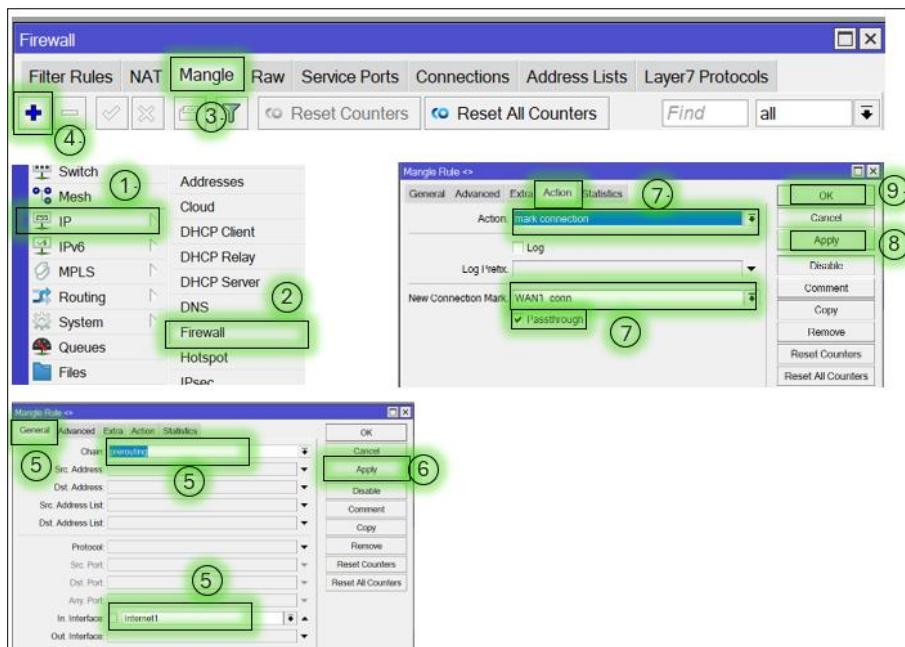


Figura 12 marcado de paquetes 1

Fuente: Elaborado por autor

En la segunda configuración como se muestra en la figura 13 es similar a la regla anterior, el cual es nuestra tercera regla, pero para la interfaz de entrada WAN2 para configurar correctamente se puede seguir en los pasos generados por los numero.

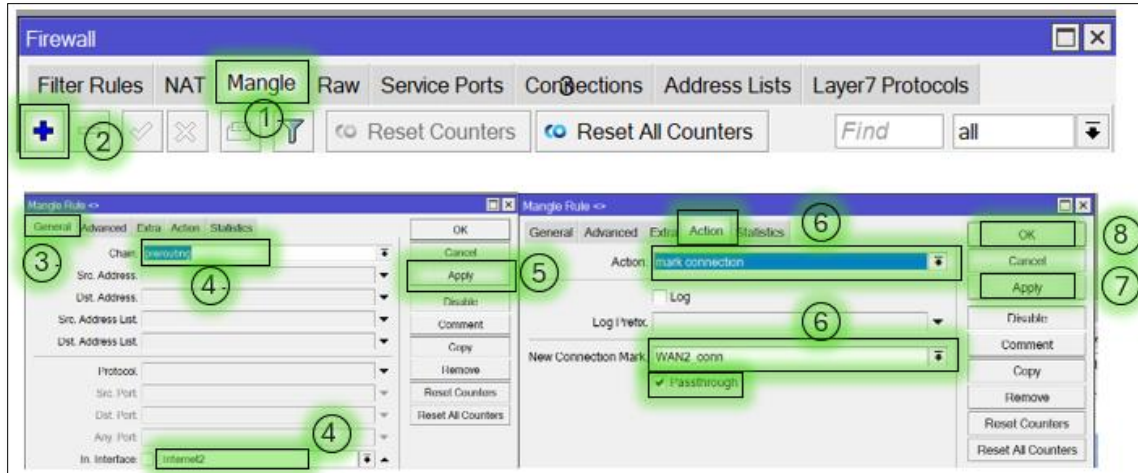


Figura 13 marcado de paquetes 2
Fuente: Elaborado por autor

En la figura 14 se muestra nuestra la tercera regla que se debe crear con la opción **add** luego pasamos a la opción **connection-mark=WAN1_conn** que aplica la regla solo a conexiones marcadas como WAN1_conn después en el apartado **action=mark-routing** el cual nos marca el enrutamiento del tráfico luego **new-routing-mark=WAN1** que nos signa la marca de enrutamiento WAN1 también utilizamos **passthrough=yes** que nos permite procesar reglas adicionales y por ultimo **comment="Enrutar conexiones por WAN1"** que nos añade un comentario para identificar la regla.

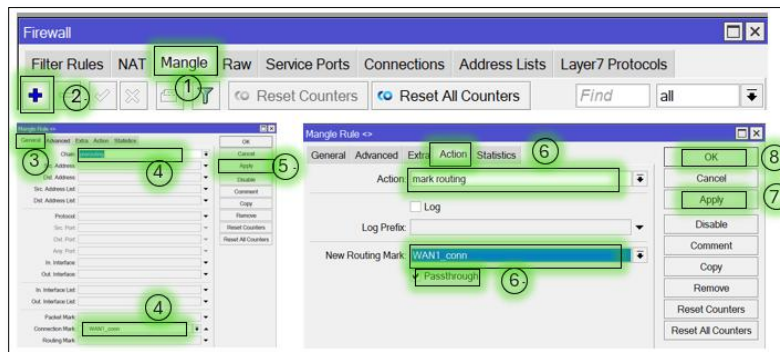


Figura 14 marcado de paquetes 3
Fuente: Elaborado por autor

La cuarta configuración dada en la figura 15 es similar a la regla anterior, pero nuestra para las conexiones marcadas como WAN2_conn.

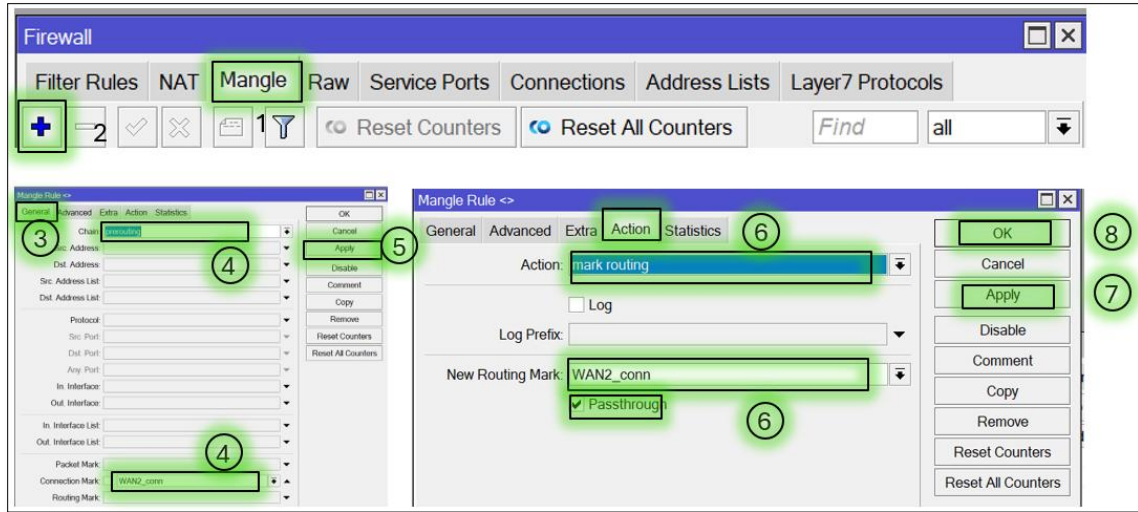


Figura 15 marcado de paquetes 4
Fuente: Elaborado por autor

Como vemos en las imágenes la configuración como parte primordial se hace la descripción de las opciones utilizadas, estas reglas aseguran que el tráfico entrante de cada interfaz se proceda enrutar de forma controlada, mejorando la eficiencia del balanceo de carga.

3.3.1 Establecer configuración NAT

Las configuraciones NAT es esencial para la conectividad y seguridad en redes porque son configuraciones que se emplean en donde direcciones IP públicas son escasas ya que realiza una conmutación en redes públicas y privadas esto es para garantizar que los dispositivos de las VLANs puedan acceder a Internet así sean con direcciones privadas en esta acción **Masquerade** en ambas interfaces WAN podrá traducir automáticamente las direcciones privadas para que puedan acceder a Internet desde redes internas y manejar el tráfico adecuadamente.

En las configuraciones realizadas esta una las opciones integradas en el software RouterOS que es **IP>firewall>NAT** en esta opción configuramos una regla de masquerade para cada interfaz WAN asegurando que todas las **VLANs** tengan acceso a **Internet** el cual están asociadas al marcado de rutas configuradas anterior mente en **MANGLE** con esto buscamos priorizar que el tráfico salga por las rutas balanceadas y que los usuarios conectados a la **VLANs** puedan navegar a **Internet** sin inconvenientes.

En el apartado **IP firewall NAT** se accede al menú de configuración como se ve en la figura 16 de reglas de NAT, en donde se definen las traducciones de direcciones para el tráfico, luego nos vamos a la opción **chain=srcnat** que aplica la regla en el tráfico saliente que será modificado antes de enviarse al exterior después configuramos **out-interface=Internet1** que especifica que la regla se aplica al tráfico saliente por la interfaz WAN1 subimos al apartado **action=masquerade** que traduce las direcciones IP privadas a la dirección IP pública asignada dinámicamente a WAN1 y por ultimo ocupamos la opción **comment="NAT para WAN1"** que nos añade un comentario descriptivo para identificar la regla.

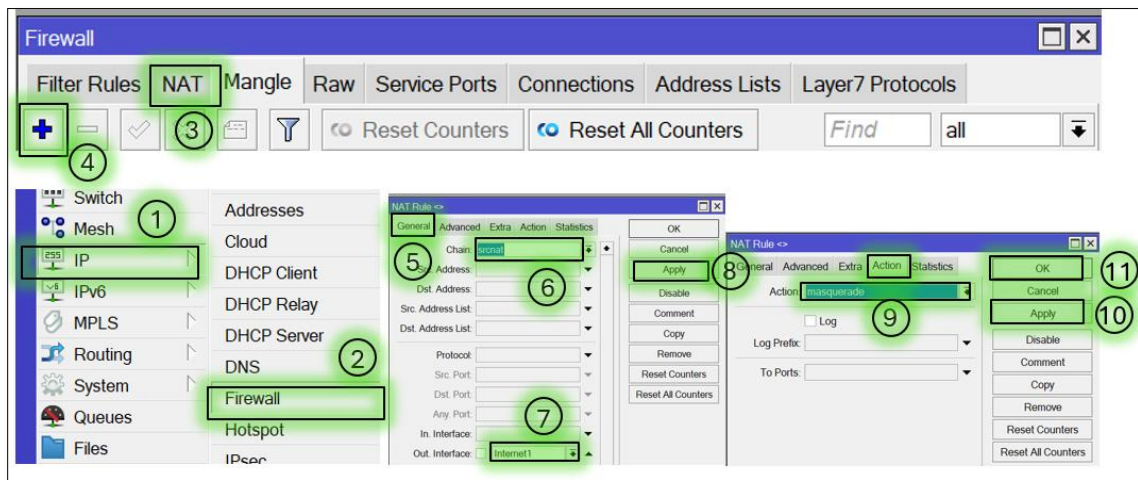


Figura 16 configuración NAT para WAN 1
Fuente: Elaborado por autor

La figura 17 es similar a la regla anterior, pero aplicada a la interfaz WAN2, permitiendo la salida de tráfico por esta conexión.

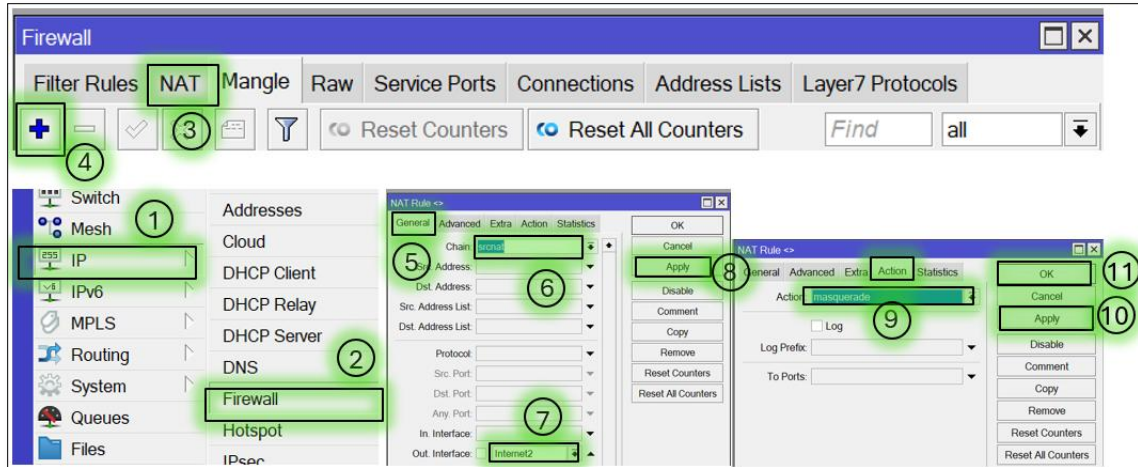


Figura 17 configuración NAT para WAN2
Fuente: Elaborado por autor

Para la configuración integradas es primordial permitir la conectividad a Internet des redes privadas el cual la principal función de esta configuración es convertir las IP privadas de los dispositivos internos en una dirección publica reconocida en Internet ya que nos facilita tipos de acceso en línea asegurando respuesta de servidores.

3.4 Establecer configuraciones de VLANs

Es importante asegurar que los dispositivos dentro de un VLANs puedan comunicarse directamente salvo que se creen reglas adicionales para comunicarse directamente con otras, las configuraciones VLANs serán direccionadas en modo troncal aislando el tráfico según áreas y funciones necesarias para el uso de las mismas, con una segmentación de esta magnitud mejora la seguridad y facilita la administración de la red en cual se va a emplear cuatro VLANs con ID 10, 20, 30 y 40 que serán destinadas en distintas áreas como administración, laboratorio, invitados y cámaras.

Para definir las VLANs de las distintas áreas se configuraron en un solo puerto el cual es el puerto sfp2 para todas las VLANs y poder enviar distintos tipos de tráfico a un solo puerto el cuales son ideales para interconectar switches y de ahí a otros dispositivos el cual el switch utilizado como puente es CRS112 que nos dará conexiones hacia los dispositivos manteniendo la segmentación lógica.

Para esta configuración VLANs como se ve la figura 18 se va al apartado **interface vlan** para acceder al menú de configuración de las mismas, donde se definen las interfaces virtuales vinculadas a un puerto físico luego seleccionamos la opción **add** luego en el apartado **name=VLAN_Admin** el cual Definimos un nombre descriptivo para identificar la VLAN destinada al área de administración luego nos vamos a **vlan-id=10** que asigna el ID único para esta VLAN, utilizado para etiquetar los paquetes pertenecientes a esta configuración.

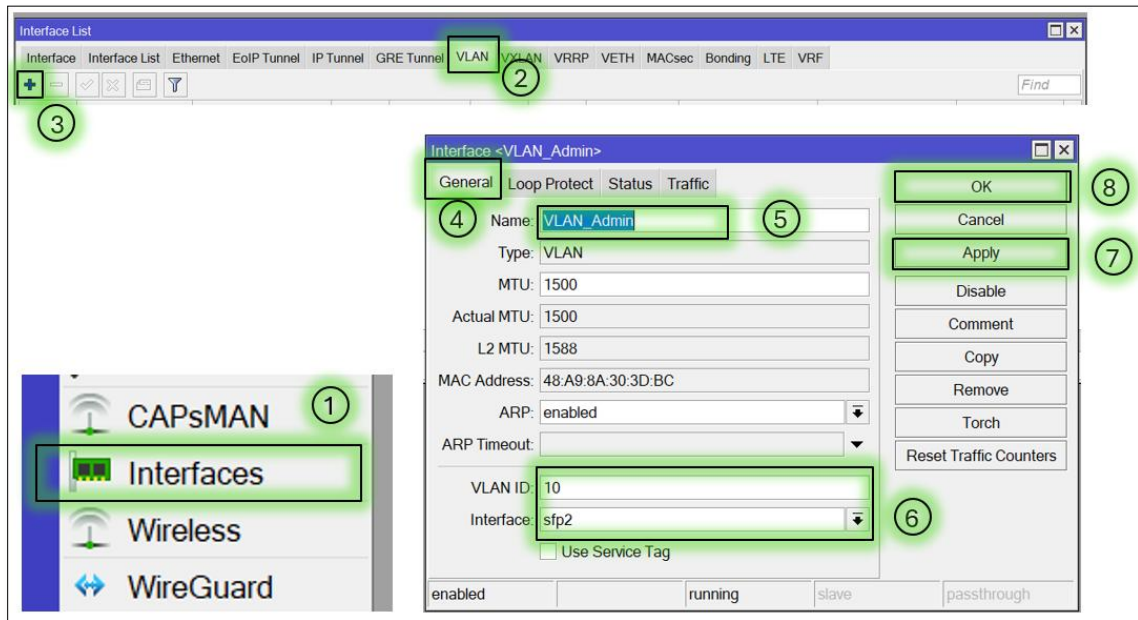


Figura 18 Configurar vlan administración
Fuente: Elaborado por autor

En la figura 19 son para la configuración de la siguiente VLANs se define una VLAN para los Laboratorio con el ID 20, aislando su tráfico del resto de la red sfp2.

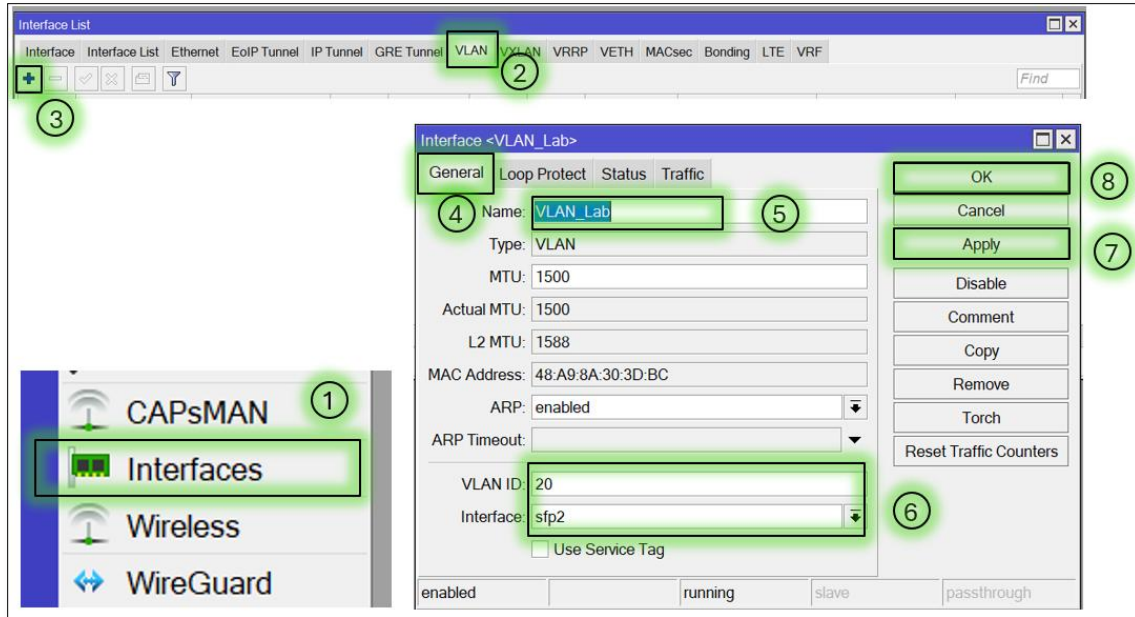


Figura 19 Configurar VLANs laboratorio
Fuente: Elaborado por autor

En la figura 20 para la configuración de la siguiente VLANs se define una VLAN para los invitados con el ID 30, aislando su tráfico del resto de la red sfp2.

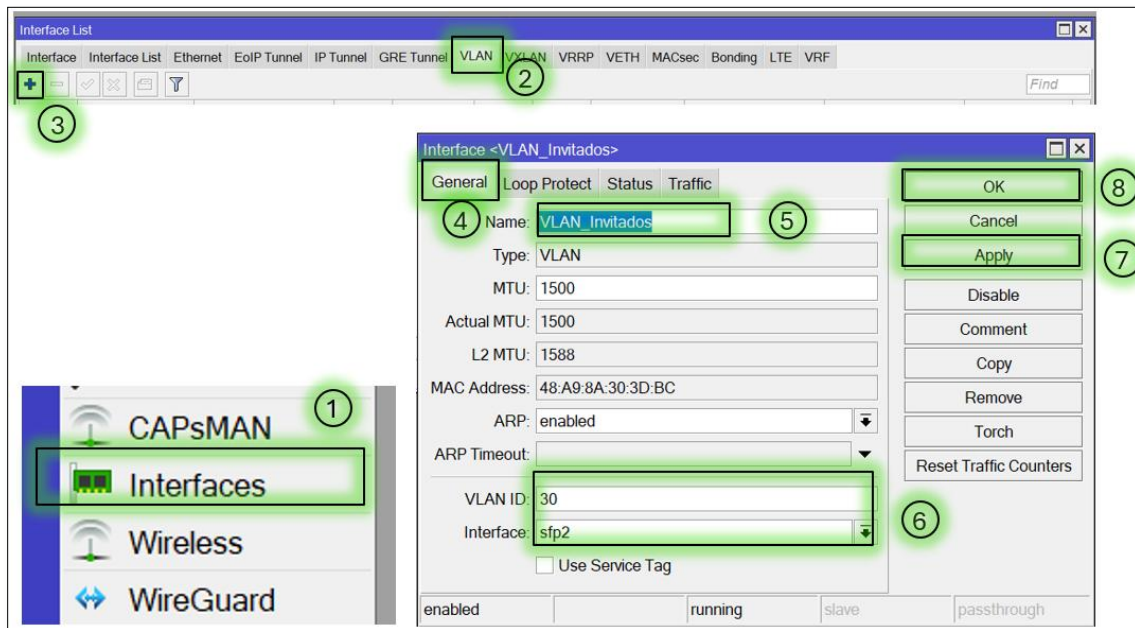


Figura 20 Configurar VLANs red invitados
Fuente: Elaborado por autor

En la figura 21 creamos la configuración de la siguiente VLANs se define una VLAN para Cámaras con el ID 40, conectado al puerto sfp2.

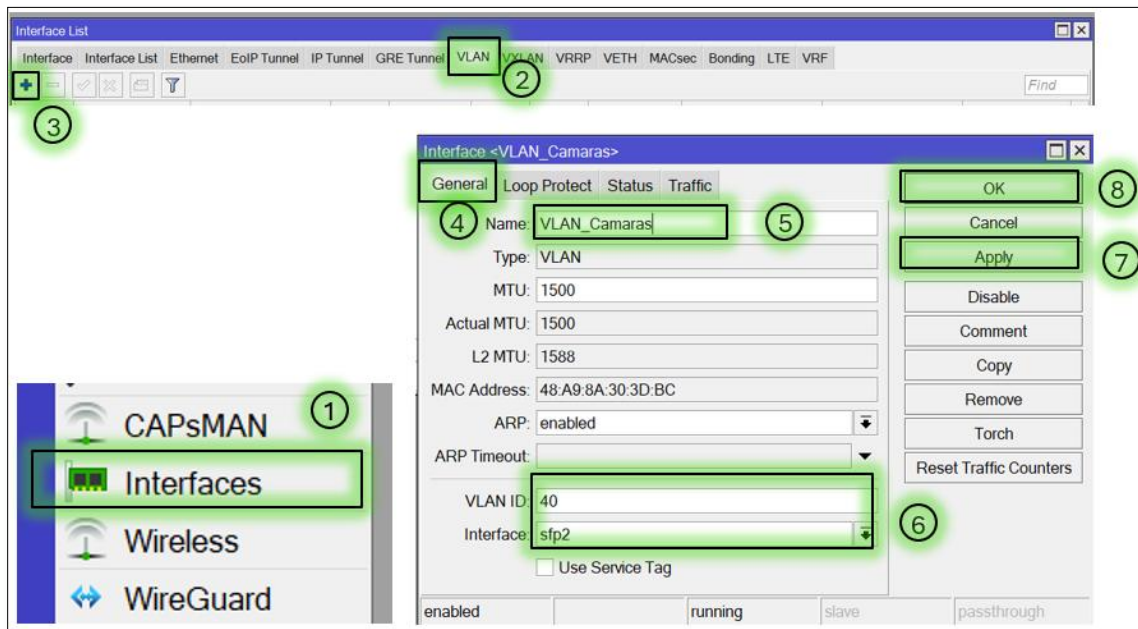


Figura 21 configurar VLANs para cámaras
Fuente: Elaborado por autor

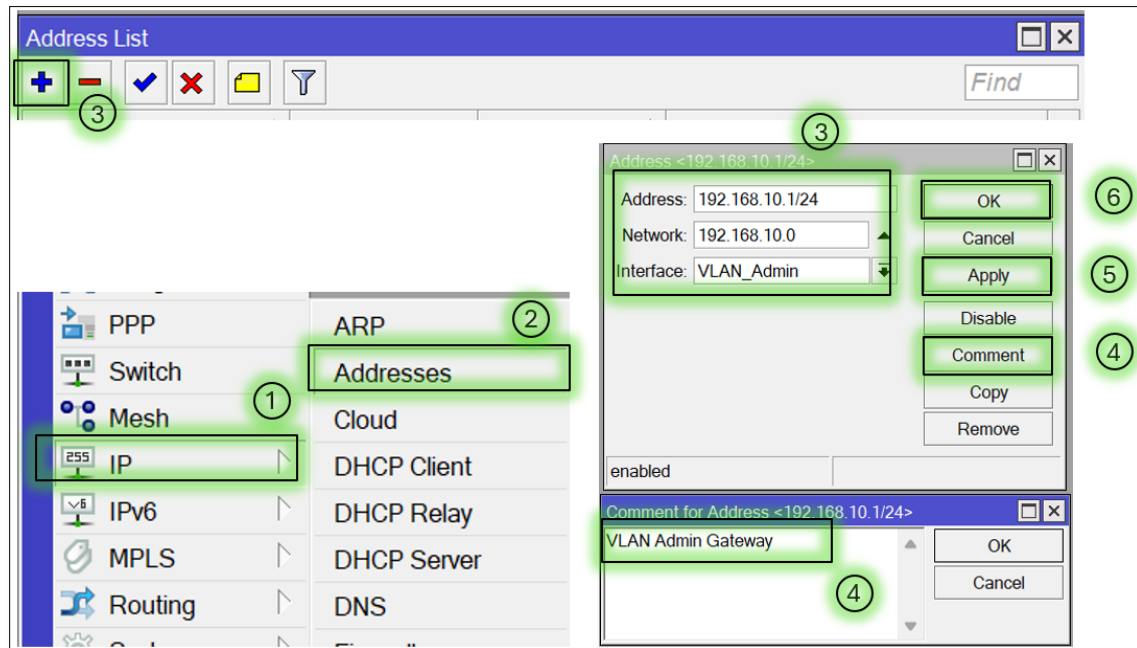
La segmentación realizada facilita la gestión de red de cada segmento de tal manera que se comporta como una red aislada de las demás, limitando la propagación de tráfico innecesario para mejorar el rendimiento más seguro y eficiente, esencial para mantener una seguridad más estable, con este diseño se logran asignar recursos dinámicamente para la optimización del uso del ancho de banda.

3.4.1 Establecer IP a las VLANs

Es este punto se genera la configuración a cada VLANs para que puedan comunicarse dentro del segmento y poder acceder a servicios externos, ya que están configurados a varias asignaciones de IP según sus VLANs, es importante ya que habilitamos en enrutamiento para otros dispositivos.

Para la configuración que se muestra en la figura 22 entramos en el apartado **ip address** que nos permite acceder al menú de configuración de direcciones IP en el router ya que aquí se asignan direcciones a interfaces, incluyendo las de las VLAN nos vamos a la opción **address=192.168.10.1/24** y asignamos la dirección IP 192.168.10.1 con una máscara de red de 24 bits (255.255.255.0) el cual esta dirección será el Gateway después nos vamos a la opción

interface=VLAN_Admin que nos especifica que esta dirección está vinculada a la interfaz virtual de la VLAN VLAN_Admin y por últimos ocupamos **comment="VLAN Admin Gateway"** que nos añade un comentario descriptivo para identificar la función de esta dirección.



*Figura 22 configuración de IP VLANs administración
Fuente: Elaborado por autor*

En la figura 23 creamos la configuración en la entramos en el apartado **ip address** que nos permite acceder al menú de configuración de direcciones IP en el router el cual se configura el Gateway 192.168.20.1 para la VLAN del laboratorio, con las mismas características que el anterior.

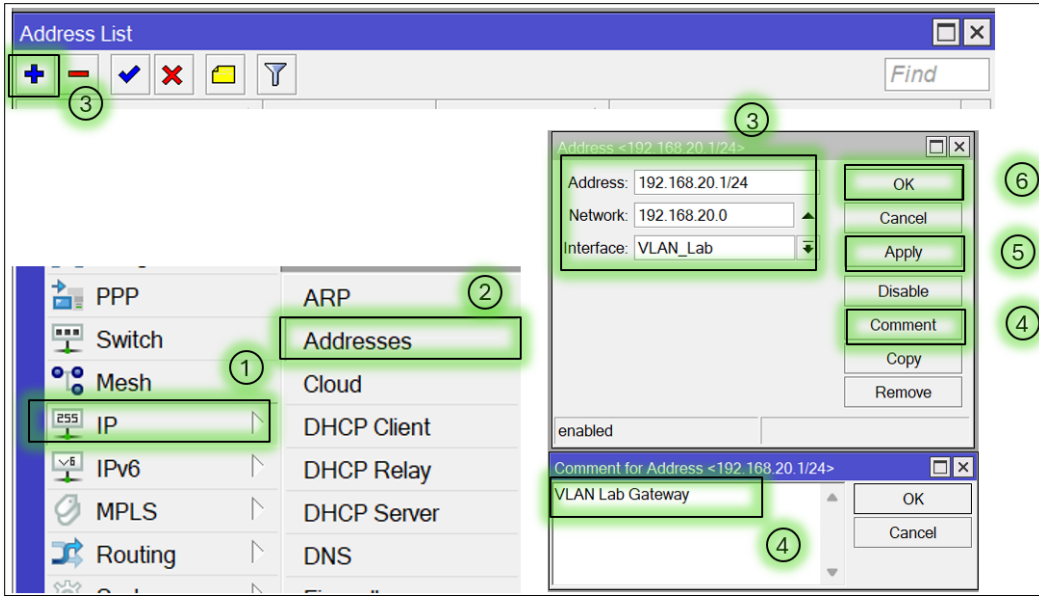


Figura 23 configuración de IP VLANs laboratorio
Fuente: Elaborado por autor

Para la configuración que se presenta en la figura 24 entramos en el apartado **ip address** que nos permite acceder al menú de configuración de direcciones IP en el router el cual añade el Gateway 192.168.30.1 a la VLAN destinada a los invitados, con las mismas características que el anterior.

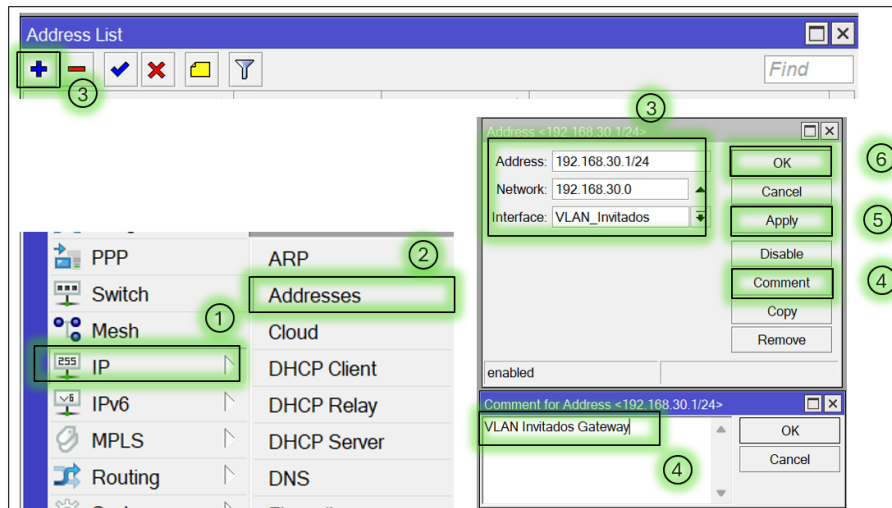


Figura 24 configuración de IP VLANs invitados
Fuente: Elaborado por autor

Para la configuración en la entramos en el apartado **ip address** que nos permite acceder al menú de configuración de direcciones IP en el router el cual se ingresa el Gateway 192.168.40.1 para la

VLAN dedicada al tráfico de cámaras de seguridad, con las mismas características que el anterior tal como se aprecia en la figura 25.

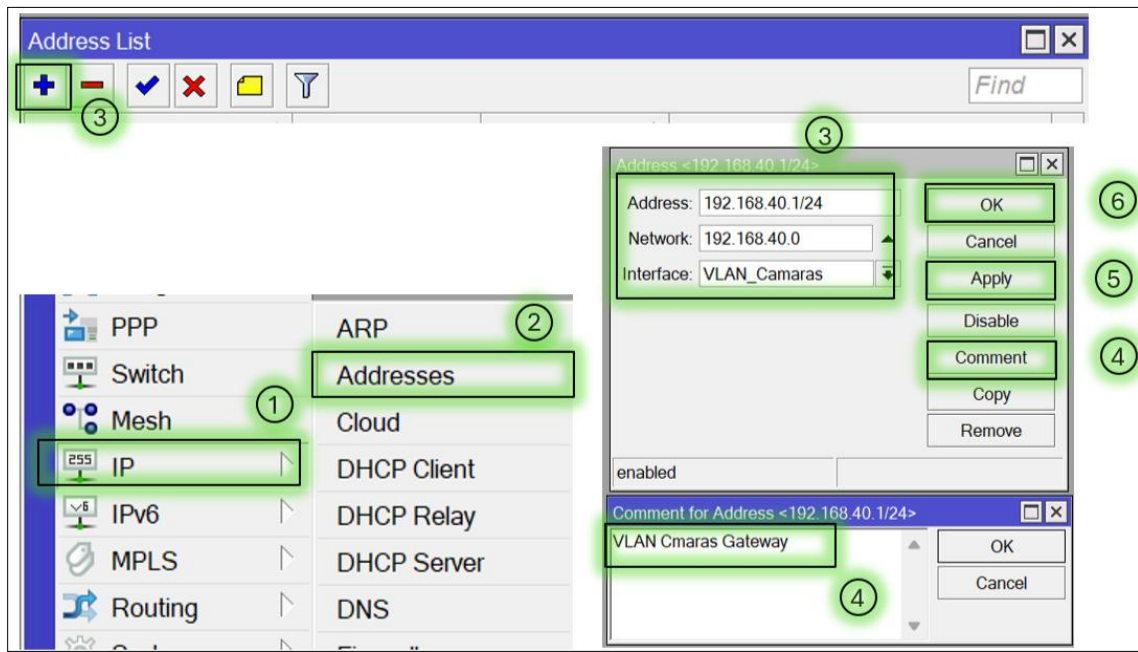


Figura 25 configuración de IP VLANs Cámaras
Fuente: Elaborado por autor

En esta parte de las ilustraciones se asignaron Gateway para cada VLAN, permitiendo a los dispositivos dentro de cada segmento comunicarse con su red correspondiente y descripción de las opciones utilizadas.

También, es crucial garantizar un correcto funcionamiento es por aquello que cada dirección IP asignada actúa como puerta de enlace predeterminada, con esto permitimos que los dispositivos se comuniquen a una red local conforme cada rango único de direcciones IP y su puerta de enlaces, evitando conflictos entre VLANs ya que también se habilita el enrutamiento con redes externas, algunas configuraciones importantes adicionales son configurar el protocolo DHCP, utilizado en direcciones de cada segmento.

3.4.2 Establecer VLANs en modo TRUNK

Para establecer una configuración en un puerto trunk es esencial gestionar varias VLANs por que estas opciones se utilizan para centralizar y gestionas el tráfico de cada segmento al utilizar modo trocal dentro de un bridge conectado al puerto sfp2 esta nos ayuda a transportar el tráfico etiquetado

de múltiples VLANs esta opción se etiqueta en el estándar IEE 8201.Q el cual permite mantener la separación lógica de la segmentación que asegura la interoperabilidad con los otros equipos.

En la figura 26 hacemos la configuración con el apartado **interface bridge** para acceder al menú de configuración de bridges, donde se crean y administran estas interfaces virtuales vamos a la opción de **add** crea un apartado adicional para la configuración luego seleccionamos la opción **name=Bridge_Trunk** que nos crea un bridge con el nombre Bridge_Trunk, que servirá como punto central para gestionar el tráfico de las VLANs por ultimo en la opción **comment=Bridge para VLAN Trunk** que se añade un comentario para identificar su función como bridge para el trunk de las VLANs.

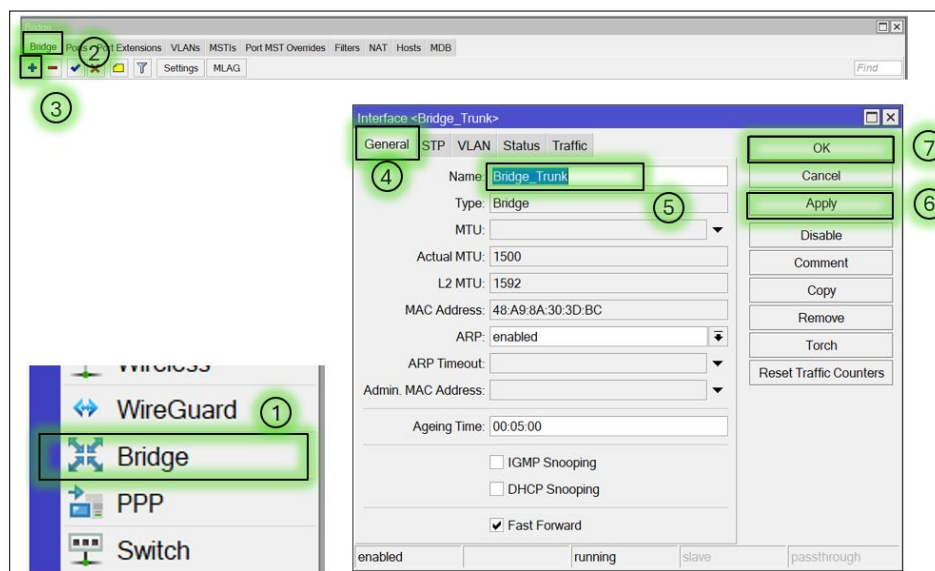


Figura 26 configuración bridge modo trunk
Fuente: Elaborado por autor

En la figura 27 configuramos **interface bridge port** se accede al menú para añadir puertos físicos o virtuales al bridge creado luego se selecciona en **add** en la parte de **bridge=Bridge_Trunk** el cual nos especifica que el puerto será parte del bridge Bridge_Trunk luego se configura **interface=sfp2** que asigna el puerto físico sfp2 como miembro del bridge, que será utilizado como puerto trunk para transportar el tráfico de las VLANs y final mente **comment=Trunk para las VLANs** que añade un comentario descriptivo para identificar su propósito.

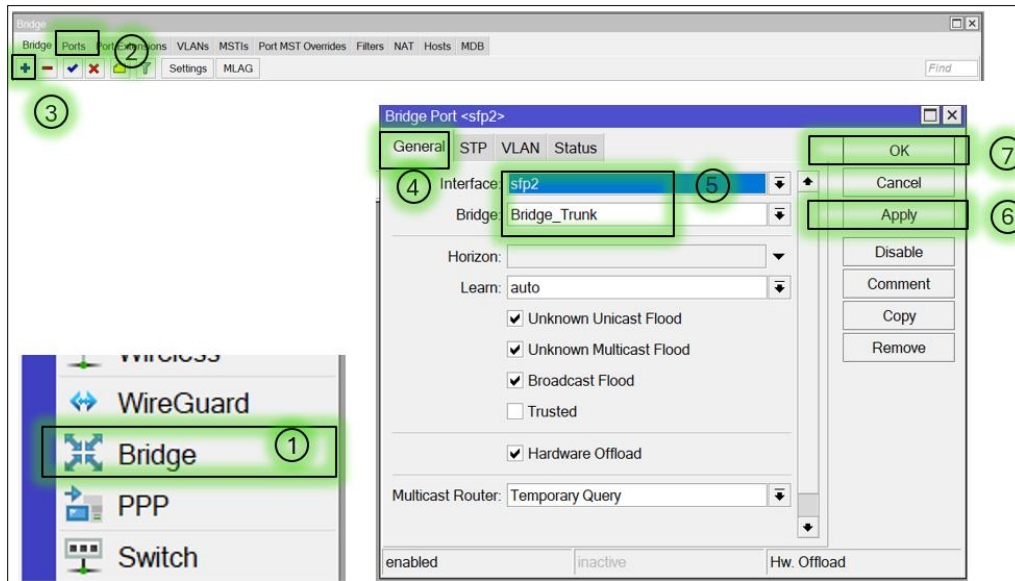


Figura 27 asignación sfp2 con bridge trunk
Fuente: Elaborado por autor

Como se presenta las imágenes se creó un bridge para centralizar las VLANs en un puerto trunk y el puerto **sfp2** se designa como puerto trunk para transportar todas las VLANs. Al momento de configurar el puerto sfp2 con una conexión troncal se puede transportar datos hacia otros switches mejorando el transporte de tráfico.

3.5 Implementación de calidad de servicio QoS

3.5.1 Reglas de Firewall para el tráfico de VLANs

La implementación de todas estas configuraciones en la calidad de servicio se refiere a la gestión de tráfico de las VLANs hacia el Internet a través de la interfaz WAN1 que permite el tráfico solo legítimo, las reglas diseñadas para aceptar tráficos provenientes de otras interfaces son comprometiendo una gestión eficiente del flujo de datos.

Para esta configuración presentada en la figura 28 entramos en **ip firewall filter** ya que permite acceder al menú de configuración de las reglas de filtrado del firewall, donde se gestionan las reglas que controlan el tráfico de red luego se va en **add** donde abre otro apartado se configura en **chain=forward** que nos dice que la regla se aplica al tráfico que está siendo reenviado entre interfaces es decir, entre la interfaz de origen y destino luego en la opción **action=accept** ya que esta opción es permitir el tráfico que cumpla con los criterios establecidos en la regla luego a **in-interface=VLAN_Admin** que nos especifica que el tráfico entrante proviene de la interfaz de la

VLAN de administración “VLAN_Admin” luego a **out-interface=Internet1** que indica que el tráfico será enviado a través de la interfaz Internet1 hacia Internet y por ultimo usamos **comment="Permitir tráfico Admin a Internet"** que añade un comentario explicativo para identificar el propósito de la regla.

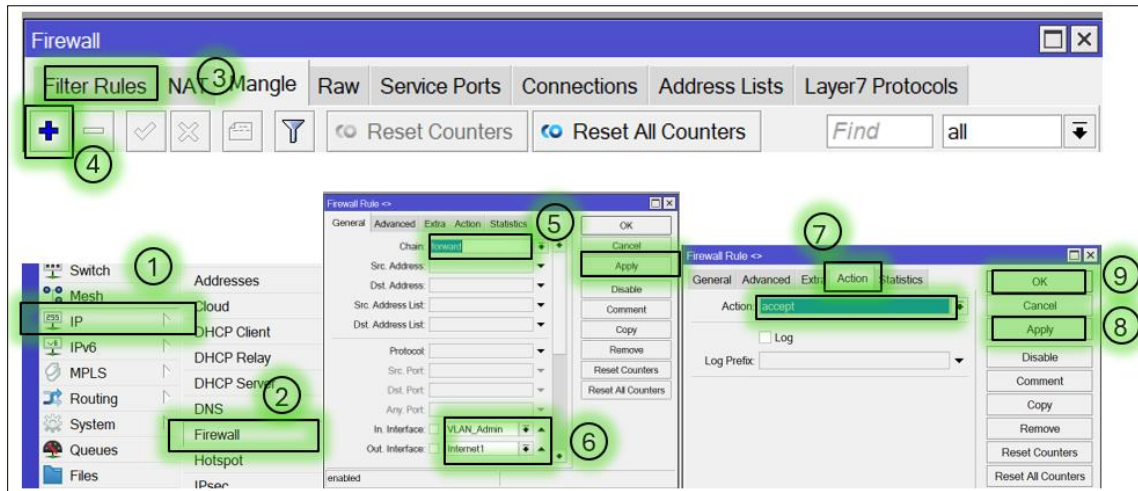


Figura 28 trafico proveniente Vlan administración
Fuente: Elaborado por autor

En la figura 29 se Configura una regla similar para permitir que el tráfico de la VLAN de laboratorio (VLAN_Lab) acceda a Internet a través de la misma interfaz Internet1

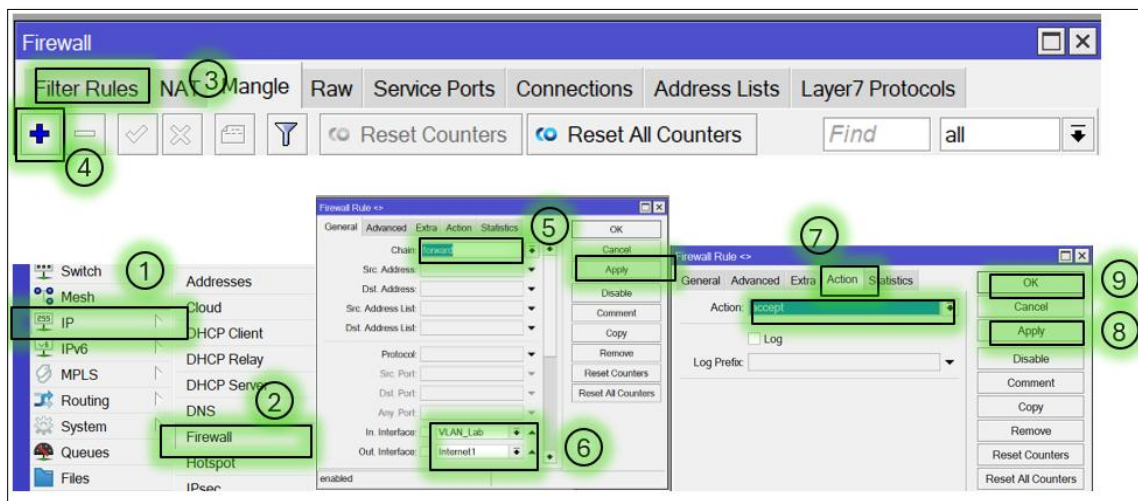


Figura 29 trafico proveniente Vlan laboratorio a Internet
Fuente: Elaborado por autor

En la figura 30 permite el tráfico proveniente de la VLAN de invitados para salir hacia Internet

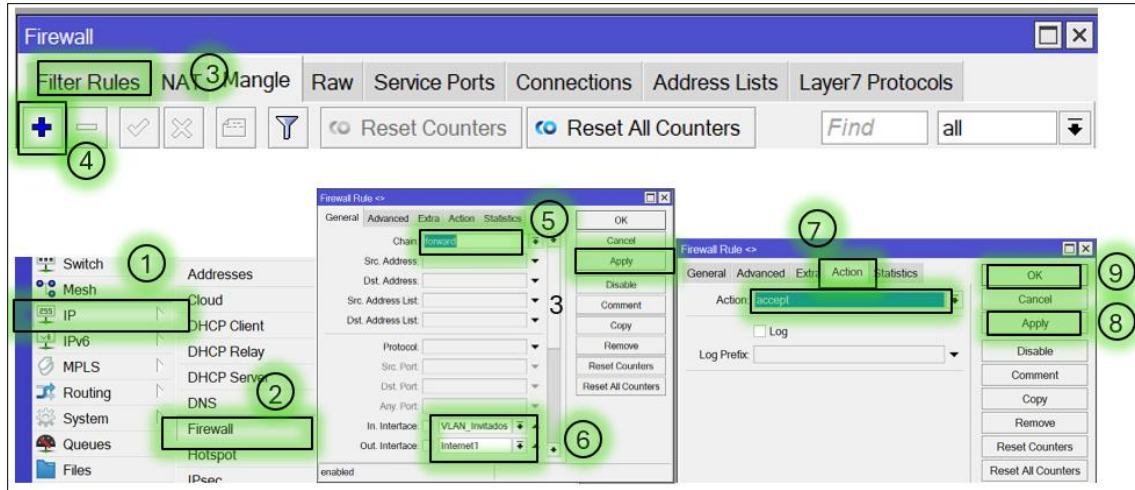


Figura 30 tráfico proveniente Vlan invitados a Internet
Fuente: Elaborado por autor

En la figura 31 configuramos el tráfico de la VLAN de cámaras de seguridad (VLAN_Camaras) hacia Internet.

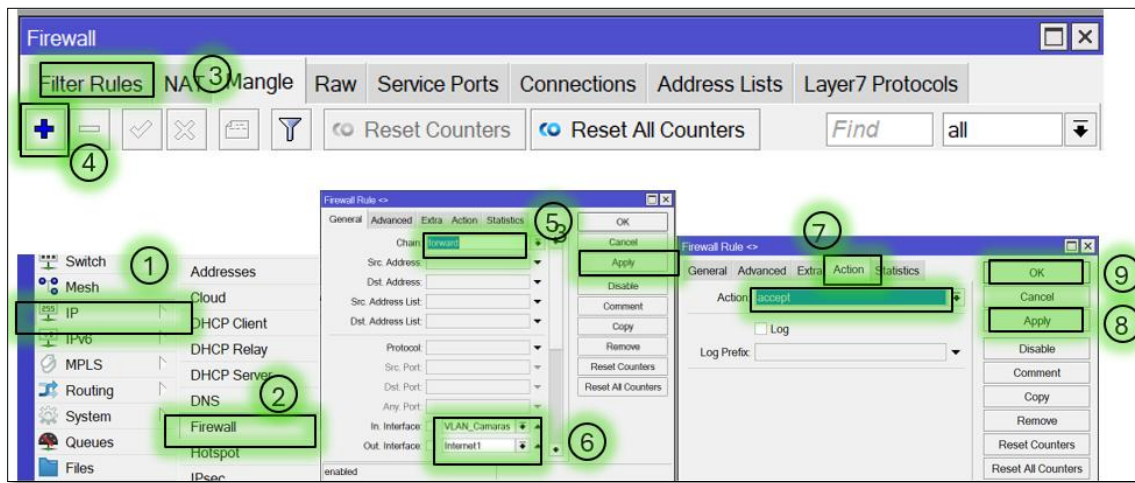


Figura 31 trafico de VLANs cámaras
Fuente: Elaborado por autor

Estas configuraciones pretenden construir reglas de direccionamiento para permitir el tráfico entre la VLANs hacia las WAN nos van a permitir el acceso a Internet es esencial para poder garantizar conectividad y seguridad del mismas.

3.5.2 Reglas para limitar las VLANs

En este punto se configurarán reglas en las configuraciones de firewall que son implementadas para aislar las VLANs entre sí en este caso bloquearemos en acceso de la VLANs invitados hacia las otras VLANs ya que con esto permitimos que la red de invitados tenga un acceso de recursos críticos asegurando que los dispositivos no autorizados puedan ingresar a la infraestructura.

Se accede al menú para configurar las reglas de filtrado del firewall como se ve en la figura 32 **ip firewall filter** donde se gestionan las reglas que determinan qué tráfico es permitido o bloqueado en la red en la opción **add** luego que abra el apartado seleccionar **chain=forward** que es la regla se aplica al tráfico que circula entre interfaces que se está reenviando de una VLAN a otra la opción **action=drop** que es la acción desbloquear el tráfico que cumpla con los criterios definidos en la regla y después a **in-interface=VLAN_Invitados** que nos especifica que el tráfico de la VLAN de invitados es el que se va a filtrar y en la parte de **out-interface=VLAN_Admin** el cual la regla bloquea el tráfico que intenta salir de la VLAN de invitados hacia la VLAN de administración y por últimos **comment=Bloquear Invitados hacia Admin** que proporciona un comentario para describir la función de la regla.

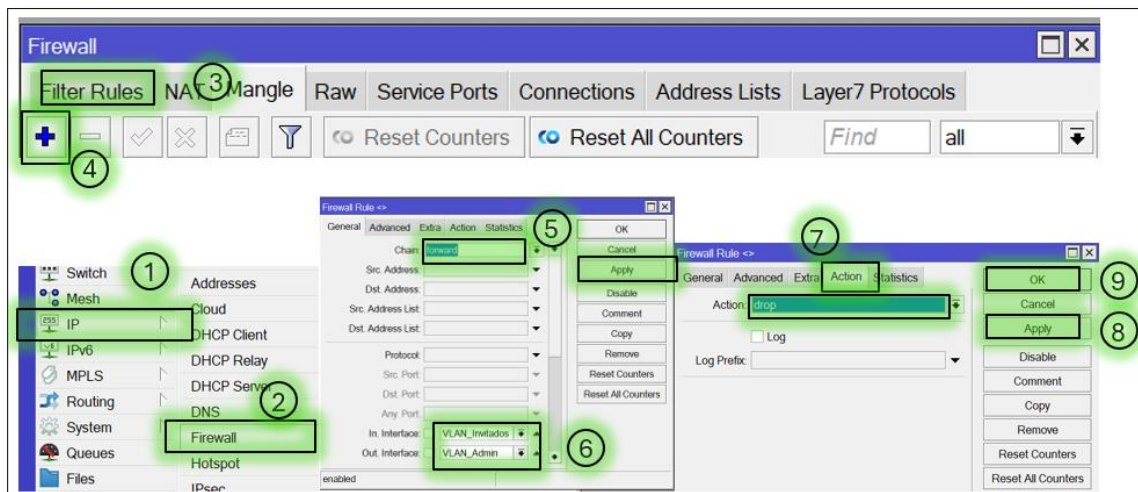


Figura 32 limitamos el tráfico entre VLANs
Fuente: Elaborado por autor

En la figura 33 es similar a la regla anterior, esta regla bloquea el tráfico de la **VLAN de invitados** hacia la **VLAN de laboratorio**.



Figura 33 bloqueo VLANs Invitado hacia laboratorio
Fuente: Elaborado por autor

Se observaron en las configuraciones de las ilustraciones en general se implementaron políticas de aislamiento de red, el cual se bloquearon el acceso a la red de invitados que prohíben la intervención a las demás y nos da un aislamiento esto es crucial en la seguridad de la red al impedir que dispositivos externos de la VLANs tengan algún tipo de comunicación con las demás con esto mejoramos la protección de los segmentos de la red más sensibles.

3.5.3 Establecer configuración QoS

El fin principal para establecer la configuración de QoS es asegurar que ciertos tipos de VLANs tengan prioridad al manejo de ancho de banda las políticas de calidad de servicio creadas, la cámaras serán prioridad uno ya que son por seguridad, red de laboratorios con nombre de VoIP asignado será prioridad tres y la red de administración nombrada como streaming de video con prioridad 2 y por ultimo esta la red de invitado que se le da una prioridad 8 ya que las necesidades son con más exigencias en el ámbito de la red externa con esto evitamos congestión en la red.

En la configuración que se muestra la figura 34 se va a la opción **queue simple** se accede al menú para configurar colas simples, una técnica de QoS en MikroTik que permite asignar prioridades y límites de ancho de banda a direcciones específicas, rangos de IP o subredes para configurar le damos a la opción **name=Prioridad-Camaras** que es el nombre de la cola que identifica la prioridad asignada al tráfico de cámaras luego a la configuración **target=192.168.40.0/24** que especifica que esta cola aplica a todo el tráfico en la subred de la VLAN de cámaras (192.168.40.0/24) le damos **max-limit=20M/20M** que establece un límite máximo de ancho de

banda de 20 Mbps para descarga y subida y le damos a la opción **priority=1/1** el cual no asigna la prioridad más alta 1 es la máxima prioridad y por último usamos **comment= Priorizar VLAN Cámaras** que es comentario descriptivo sobre la función de la cola.

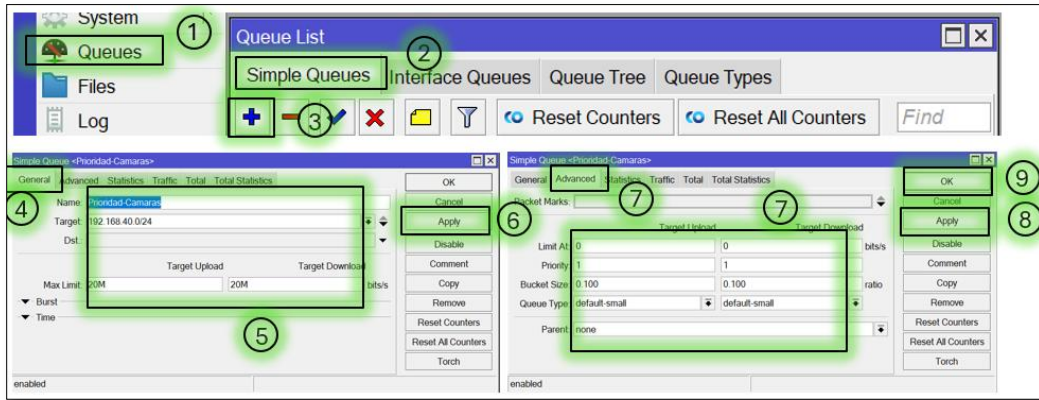


Figura 34 priorizar el tráfico VLAN Cámaras
Fuente: Elaborado por autor

En la figura 35 se configura la cola para el tráfico VoIP en la VLAN de administración (192.168.10.0/24) con alta prioridad (2).

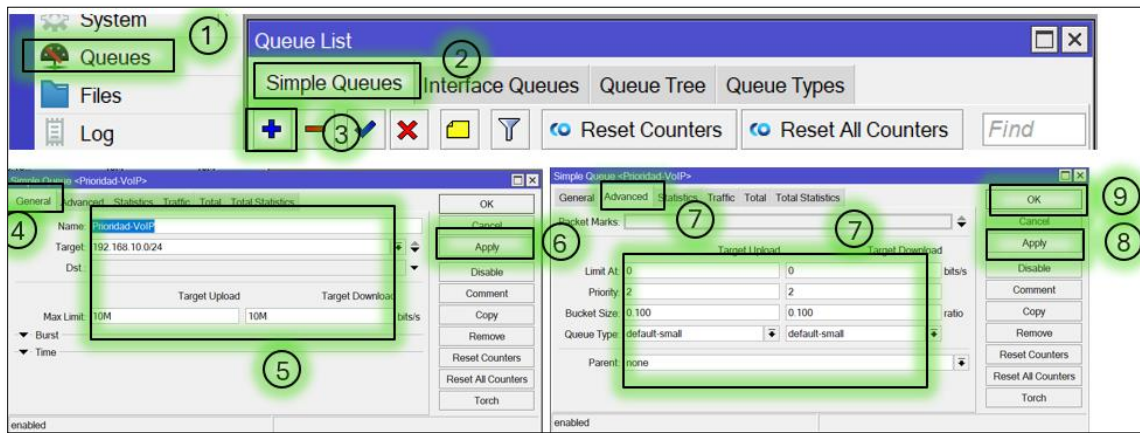


Figura 35 priorizar el tráfico VLANs administración
Fuente: Elaborado por autor

En la figura 36 se crea una cola para priorizar el tráfico de streaming de video desde la VLAN de laboratorio (192.168.20.0/24) con prioridad moderada (3).

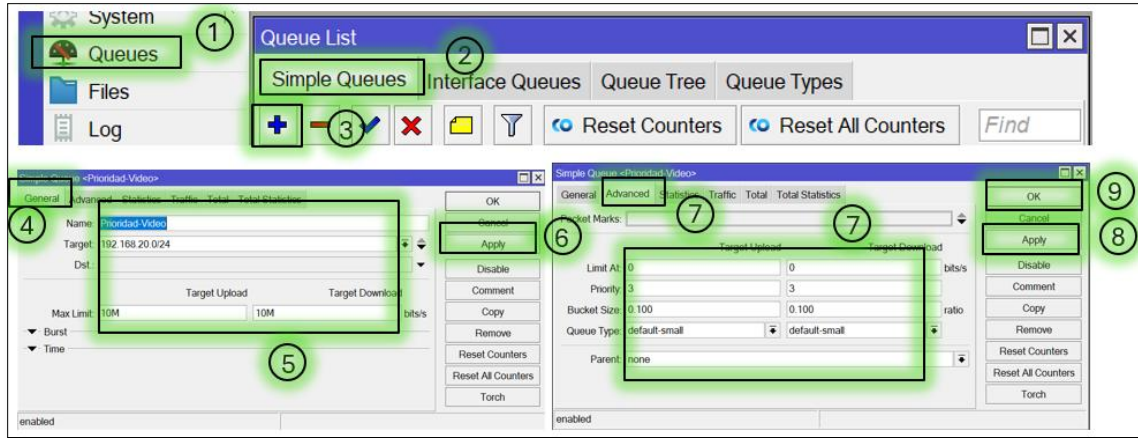


Figura 36 priorizar VLANs laboratorio
Fuente: Elaborado por autor

Las configuraciones realizadas en la figura 37 nos hace saber que las asignaciones realizadas con prioridad 8 a la red de invitados limita el ancho de banda a 5 Mbps para la VLANs de invitados asegurando que el tráfico no crítico no afecte el rendimiento de la demás aplicación más utilizadas dentro de la red.

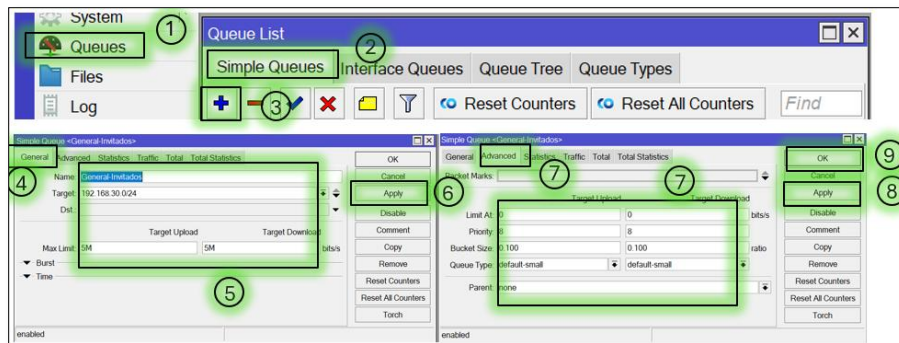


Figura 37 priorizar el tráfico VLAN invitados
Fuente: Elaborado por autor

Con esta configuración realizadas en te proceso se regula el tráfico de datos para asegurar los dispositivos utilizados en cada VLANs tengan un flujo controlado, ya que nos facilita un control de gestión del ancho de banda total para las VLANs lo que simplifica la congestión del tráfico.

3.5.4 Establecer PCQ para granularla

Este método de granular establece que es utilizado para la gestión del ancho de banda ya que nos permite asignar un ancho de banda a múltiples conexiones de manera equitativa es decir esta

opción divide el ancho de banda según las unidades que tengamos en esa VLANs el cual al dividirse el ancho de banda para cada conexión se hace más pequeña.

En la figura 38 se muestra como configurar el ancho de banda de manera granular de la VLANs invitados.

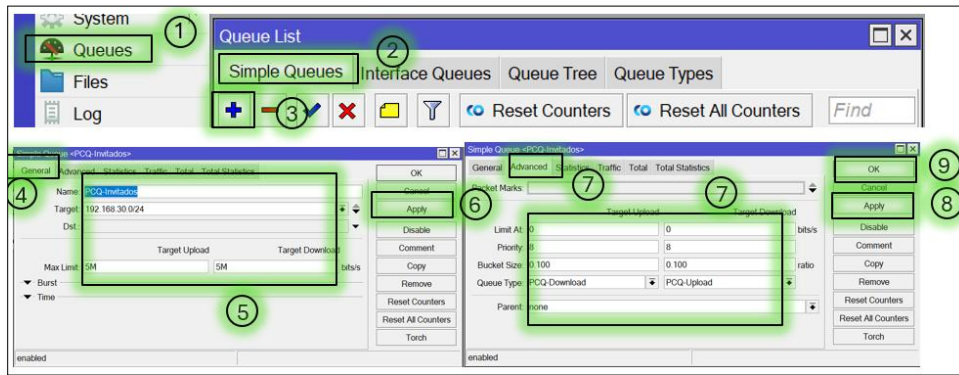


Figura 38 configuración del ancho de banda de forma granular
Fuente: Elaborado por autor

CAPITULO IV

4.1 Resultados

4.1.1 Evaluación del Desempeño de Balanceo de Carga y Failover

En este proyecto se verifico la evaluación del desempeño de una red configurada con dos conexiones WAN utilizando un equipo Mikrotik con una configuración de balance de carga y un mecanismo de conmutación por error, para disponer del servicio en todo momento ante posibles fallos que se puedan generar en la conexión principal con esto se implementaron reglas de Mangle para marcar conexiones, rutas estáticas con prioridades y NAT para enmascarar el tráfico saliente.

4.1.1.1 Verificación de rutas y conmutación por error del failover

En esta figura 39 se muestra rutas activas el cual se realizaron configuraciones del acceso al Internet, para ver lo realizado se utilizó comando en consola utilizando IP router print para poder ver las interfaces nombradas para el acceso nombradas como WAN1 Y WAN2.

```
[admin@MikroTik] /interface/vlan> /ip route print
Flags: D - DYNAMIC; I, A - ACTIVE; C, S, Y - COPY; H - HW-OFFLOADED
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#   DST-ADDRESS   GATEWAY      DISTANCE
;;; Ruta de respaldo - WAN2
0 As 0.0.0.0/0     192.168.88.1 2
;;; Ruta principal - WAN1
1 IsH 0.0.0.0/0    192.168.5.1  1
DIcH 192.168.5.0/24  Internet1    0
DAc 192.168.10.0/24  VLAN_Admin   0
DAc 192.168.20.0/24  VLAN_Lab     0
DAc 192.168.30.0/24  VLAN_Invitados 0
DAc 192.168.40.0/24  VLAN_Camaras 0
DAc 192.168.88.0/24  Internet2    0
[admin@MikroTik] /interface/vlan> █
```

Figura 39 rutas específicas de acceso a Internet
Fuente: Elaborado por autor

Luego verificamos las conexiones y el tráfico generado por estas interfaces Internet1 y Internet2 que están conectadas en sfp1 y ether1 para validar una conmutación el cual presentamos el monitoreo de ambas, con la opción monitor-traffic para el comportamiento del mismo, ya que son las interfaces de acceso tal como se muestra en la figura 40.

```
[admin@MikroTik] > /interface monitor-traffic Internet1,Internet2
      name:  Internet1  Internet2
rx-packets-per-second:      655      3
rx-bits-per-second:         5.9Mbps  1536bps
fp-rx-packets-per-second:   670      3
fp-rx-bits-per-second:      6.0Mbps  1440bps
tx-packets-per-second:      288      0
tx-bits-per-second:         690.7kbps  0bps
fp-tx-packets-per-second:   0        0
fp-tx-bits-per-second:      0bps     0bps
tx-queue-drops-per-second:  0        0
-- [Q quit|D dump|C-z pause]
```

Figura 40 tráfico activos de Internet1 y intenet2
Fuente: Elaborado por autor

4.1.1.2 Estadísticas de tráfico balanceado (Mangle)

Para estas configuraciones de trafico de balance de carga se gestionaron en las dos líneas de acceso WAN1 y WAN2 con marcando en las tablas de enrutamientos en el dispositivo separando el tráfico en distintos criterios, se generó tráfico en ambas interfaces dando conexión a varios dispositivos que confirmaron la distribución entre ambas WAN tal como se observa en la figura 41.

```
[admin@MikroTik] > /ip firewall mangle print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN      ACTION          BYTES  PACKETS
;;; Marcar conexiones WAN1
0 prerouting mark-connection  320 231  1 016
;;; Marcar conexiones WAN2
1 prerouting mark-connection  21 302 043  73 228
;;; Enrutar conexiones por WAN1
2 prerouting mark-routing     456 878  1 444
;;; Enrutar conexiones por WAN2
3 prerouting mark-routing     26 721 778  85 753
[admin@MikroTik] >
```

Figura 41 Distribución de balance de carga entre WANs
Fuente: Elaborado por autor

En estos resultados se observó el flujo de conexión primaria y secundaria manteniendo la conectividad de los dispositivos en las redes locales podemos observar que el balanceo distribuyó las conexiones de manera eficiente.

4.1.2 Análisis de Tráfico y Eficiencia en Redes VLAN Integradas con QoS

Para la configuración se creó la segmentación de red mediante VLANs y la priorización de tráfico con QoS en un entorno Mikrotik donde se visualizan las configuraron para separar diferentes tipos

de tráfico direccionados para varias Áreas el cual se implementaron colas simples y basadas en PCQ para garantizar un ancho de banda adecuado para cada VLAN.

4.1.2.1 Monitoreo del tráfico por VLAN

Para poder validar las opciones configuradas impuesta en la red se usó la opción del terminal de consola dentro del software Winbox con la figura podemos demostrar la perfecta configuración de las VLANs configuradas con sus ID asignadas tal como se ve en la figura 42.

```
[admin@MikroTik] > /interface vlan print
Flags: R - RUNNING
Columns: NAME, MTU, ARP, VLAN-ID, INTERFACE
#  NAME      MTU  ARP  VLAN-ID  INTERFACE
;; VLAN Admin
0 R VLAN_Admin 1500 enabled 10 sfp2
;; VLAN Camaras
1 R VLAN_Camaras 1500 enabled 40 sfp2
;; VLAN Invitados
2 R VLAN_Invitados 1500 enabled 30 sfp2
;; VLAN Lab
3 R VLAN_Lab 1500 enabled 20 sfp2
[admin@MikroTik] >
```

Figura 42 interfaces Vlan por consola
Fuente: Elaborado por autor

Para poder verificar el tráfico entre las VLANs se generó una conexión a cada ruta de la VLANs para que puedan generar tráfico tal como se ve en la figura 43 con esto compruebo que el tráfico se está direccionando de manera adecuada.

```
[admin@MikroTik] > /interface monitor-traffic VLAN_Admin,VLAN_Lab,VLAN_Invitados,VLAN_Camaras
name: VLAN_Admin VLAN_Lab VLAN_Invitados VLAN_Camaras
rx-packets-per-second: 74 1 53 8
rx-bits-per-second: 67.0kbps 448bps 81.7kbps 4.6kbps
fp-rx-packets-per-second: 74 1 53 8
fp-rx-bits-per-second: 67.0kbps 448bps 81.7kbps 4.6kbps
rx-drops-per-second: 0 0 0 0
rx-errors-per-second: 0 0 0 0
tx-packets-per-second: 189 0 105 2
tx-bits-per-second: 1865.7... 0bps 904.7kbps 960bps
fp-tx-packets-per-second: 0 0 0 0
fp-tx-bits-per-second: 0bps 0bps 0bps 0bps
tx-drops-per-second: 0 0 0 0
tx-queue-drops-per-second: 0 0 0 0
tx-errors-per-second: 0 0 0 0
[Q quit|D dump|C-z pause]
```

Figura 43 simulación tráfico de VLANs
Fuente: Elaborado por autor

4.1.2.2 Validación de ancho de banda por colas

En la verificación también se verifico la visualización configuras del ancho de banda por colas para poder confirmar que el tráfico de la VLANs invitados está limitado y que cámara tiene prioridad alta tal como se ve en la figura 44.

```
[admin@MikroTik] > /queue simple print stats
Flags: X - disabled, I - invalid; D - dynamic
0   ;;; Priorizar VLAN Cmaras
    name="Prioridad-Camaras" target=192.168.40.0/24 rate=0bps/0bps total-rate=0bps
    packet-rate=0/0 total-packet-rate=0 queued-bytes=0/0 total-queued-bytes=0
    queued-packets=0/0 total-queued-packets=0 bytes=0/0 total-bytes=0 packets=0/0
    total-packets=0 dropped=0/0 total-dropped=0

1   ;;; Priorizar VLAN Admin para VoIP
    name="Prioridad-VoIP" target=192.168.10.0/24 rate=12.0kbps/376bps total-rate=0bps
    packet-rate=21/0 total-packet-rate=0 queued-bytes=0/0 total-queued-bytes=0
    queued-packets=0/0 total-queued-packets=0 bytes=4059595/1483382 total-bytes=0
    packets=27035/5050 total-packets=0 dropped=175/0 total-dropped=0

2   ;;; Priorizar VLAN Lab para Video Streaming
    name="Prioridad-Video" target=192.168.20.0/24 rate=0bps/0bps total-rate=0bps
    packet-rate=0/0 total-packet-rate=0 queued-bytes=0/0 total-queued-bytes=0
    queued-packets=0/0 total-queued-packets=0 bytes=0/0 total-bytes=0 packets=0/0
    total-packets=0 dropped=0/0 total-dropped=0

3   ;;; Trfico general VLAN Invitados
    name="General-Invitados" target=192.168.30.0/24 rate=0bps/0bps total-rate=0bps
    packet-rate=0/0 total-packet-rate=0 queued-bytes=0/0 total-queued-bytes=0
    queued-packets=0/0 total-queued-packets=0 bytes=0/0 total-bytes=0 packets=0/0
    total-packets=0 dropped=0/0 total-dropped=0
    total-packets=0 dropped=0/0 total-dropped=0 pcq-queues=0/0
```

Figura 44 validación de ancho de banda
Fuente: Elaborado por autor

El en las figuras expuestas se obtuvo el análisis de tráfico que demostró que la segmentación mejoró la gestión de datos y evitó congestiones en la red principal que con la priorización de tráfico se pudo asegurar que servicios críticos como cámaras y VoIP recibieran mayor ancho de banda, mientras que el tráfico de invitados era limitado.

4.1.3 Validación de Balanceo y priorización de tráfico

Para validad el balanceo correcto y la priorización de tráfico generados en las VLANs se concluyeron asignamos reglas de firewall para las cada VLANs y creando reglas de QoS permitiendo el tráfico controlado y con colas simples para asegurar un rendimiento más estable en cada segmento.

4.1.3.1 Reglas del firewall para VLAN

Con las reglas implementadas en firewall para vlans nos muestra el trafico permitido y no permitido entre las interfaces para seguridad entre las mismas el cual se muestra el trafico permitiendo seguir reglas especificas como se muestran en la figura 45.

```
[admin@MikroTik] > /ip firewall filter print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN      ACTION      BYTES  PACKETS
;;; Permitir trfco Admin a Internet
0 forward  accept      831 646  10 086
;;; Permitir trfco Admin a Internet
1 forward  accept      7 543 766  19 868
;;; Permitir trfco Lab a Internet
2 forward  accept           0      0
;;; Permitir trfco Lab a Internet
3 forward  accept      3 862 708  23 777
;;; Permitir trfco Invitados a Internet
4 forward  accept           0      0
;;; Permitir trfco Invitados a Internet
5 forward  accept          304      4
;;; Permitir trfco Cmaras a Internet
6 forward  accept           0      0
;;; Permitir trfco Cmaras a Internet
7 forward  accept      1 259 223   5 094
;;; Bloquear Invitados hacia Admin
8 forward  drop           0      0
;;; Bloquear Invitados hacia Lab
9 forward  drop           0      0
[admin@MikroTik] >
```

Figura 45 Reglas del firewall por VLANs
Fuente: Elaborado por autor

4.1.3.2 Validación de colas QoS

En el contexto las configuraciones realizaadas en QoS confirma la prioridad y asignacion que se les dio al ancho de banda a las VLANs criticas para limitar un congestionamiento de trafico tal como se ve en la figura 46

```
Flags: X - disabled, I - invalid; D - dynamic
0   ;;; Priorizar VLAN Cmaras
    name="Prioridad-Camaras" target=192.168.40.0/24 parent=none packet-marks="" priority=1/1
    queue=default-small/default-small limit-at=0/0 max-limit=20M/20M burst-limit=0/0
    burst-threshold=0/0 burst-time=0s/0s bucket-size=0.1/0.1

1   ;;; Priorizar VLAN Admin para VoIP
    name="Prioridad-VoIP" target=192.168.10.0/24 parent=none packet-marks="" priority=2/2
    queue=default-small/default-small limit-at=0/0 max-limit=10M/10M burst-limit=0/0

4   ;;; Limitar ancho de banda en VLAN Invitados
    name="PCQ-Invitados" target=192.168.30.0/24 parent=none packet-marks="" priority=8/8
    queue=PCQ-Download/PCQ-Upload limit-at=0/0 max-limit=5M/5M burst-limit=0/0
    burst-threshold=0/0 burst-time=0s/0s bucket-size=0.1/0.1

[admin@MikroTik] >
```

Figura 46 validación de QoS por colas
Fuente: Elaborado por autor

También podemos decir que se observaron mejoras significativas en la estabilidad y rendimiento de la red específicamente en las áreas donde el tráfico es intensivo, como cámaras y laboratorio las herramientas de monitoreo del Mikrotik confirmaron una administración eficiente del ancho de banda.

4.1.4 Monitoreo y Validación de Configuraciones WAN y VLAN

En este estudio se realizaron a cabo pruebas para monitorear y validar las configuraciones de dos interfaces WAN y Múltiples VLAN, integradas en un enrutador Mikrotik. Se verificaron la conectividad, el equilibrio de carga, el failover y las restricciones de tráfico entre VLAN mediante reglas de firewall.

4.1.4.1 Validación de conmutación por error Failover

En esta figura 47 se muestra en tiempo real todas las interfaces y al desconectar una de ellas como actúa y existe el cambio en tiempo real obteniendo Internet en todo momento.

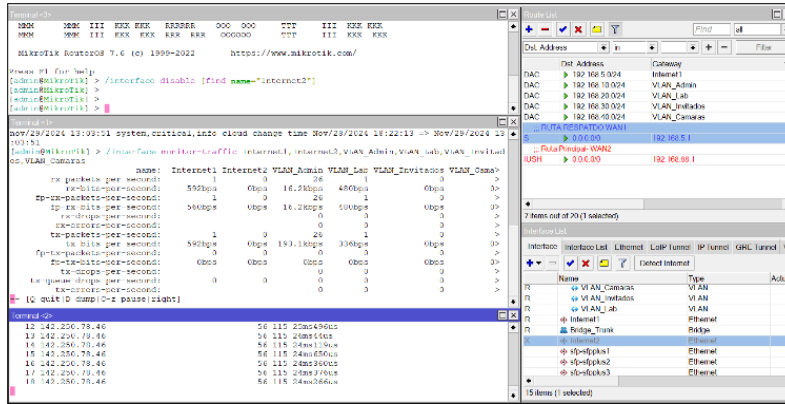


Figura 47 conmutación por error
Fuente: Elaborado por autor

4.1.4.2 Restricciones de tráfico entre VLANs

Luego validamos las restricciones entre las VLANs que se configuraron en IP firewall filter en cual nos verifica las configuraciones generadas tal como se muestra en la figura 48.

```
[admin@MikroTik] > /ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0   ;;; Permitir trafico Admin a Internet
    chain=forward action=accept in-interface=VLAN_Admin out-interface=Internet1 log=no log-prefix=""

1   ;;; Permitir trafico Admin a Internet
    chain=forward action=accept in-interface=VLAN_Admin out-interface=Internet2 log=no log-prefix=""

2   ;;; Permitir trafico Lab a Internet
    chain=forward action=accept in-interface=VLAN_Lab out-interface=Internet1

3   ;;; Permitir trafico Lab a Internet
    chain=forward action=accept in-interface=VLAN_Lab out-interface=Internet2 log=no log-prefix=""

4   ;;; Permitir trafico Invitados a Internet
    chain=forward action=accept in-interface=VLAN_Invitados out-interface=Internet1 log=no log-prefix=""

5   ;;; Permitir trafico Invitados a Internet
    chain=forward action=accept in-interface=VLAN_Invitados out-interface=Internet2 log=no log-prefix=""

6   ;;; Permitir trafico Cmaras a Internet
    chain=forward action=accept in-interface=VLAN_Camaras out-interface=Internet1

7   ;;; Permitir trafico Cmaras a Internet
    chain=forward action=accept in-interface=VLAN_Camaras out-interface=Internet2 log=no log-prefix=""

8   ;;; Bloquear Invitados hacia Admin
    chain=forward action=drop in-interface=VLAN_Invitados out-interface=VLAN_Admin

9   ;;; Bloquear Invitados hacia Lab
    chain=forward action=drop in-interface=VLAN_Invitados out-interface=VLAN_Lab
[admin@MikroTik] >
```

Figura 48 restricciones de tráfico entere VLANs
Fuente: Elaborado por autor

En estas ilustraciones se mostros la intervención de fallo simulado lo que mostró que las configuraciones respondieron correctamente bajo escenarios de balance carga ya que al

desconectar el enlace WAN y tráfico cruzado entre VLAN el cual los resultados respaldan la viabilidad de esta arquitectura para redes empresariales.

4.1.5 Priorización, Failover y Limitación de Ancho de Banda

Este proyecto se elaboró con el fin de optimizar redes integradas por WAN1 Y WAN2 y varias VLANS de salida para validar su funcionamiento ponemos a prueba el failover generado automáticamente el cual se asegura la continuidad del servicio ante casos de fallos y mejorar la distribución de los recursos logando tiempo mínimos de conmutación entre WANs concluyendo con una estabilidad y seguridad de la red mejorada.

4.1.5.1 Validación de conmutación por error (Failover)

Se demuestra un proceso de failover exitoso ya que podemos que al deshabilitar y habilitar repentinamente Internet 2 que es la conexión de fibra con prioridad 1 se crea la simulación de pérdida de conectividad en unas de las principales rutas tal como lo indica el monitoreo el cual se muestra pérdida de conectividad con **host unreachable** lo que confirma que no tenía valides para el Internet entrando en **tieme out** lo cual se observa que después de unos 21 milisegundos se obtiene respuesta los cual demuestra un failover exitoso de reconexión tal como se muestra en la figura 49.

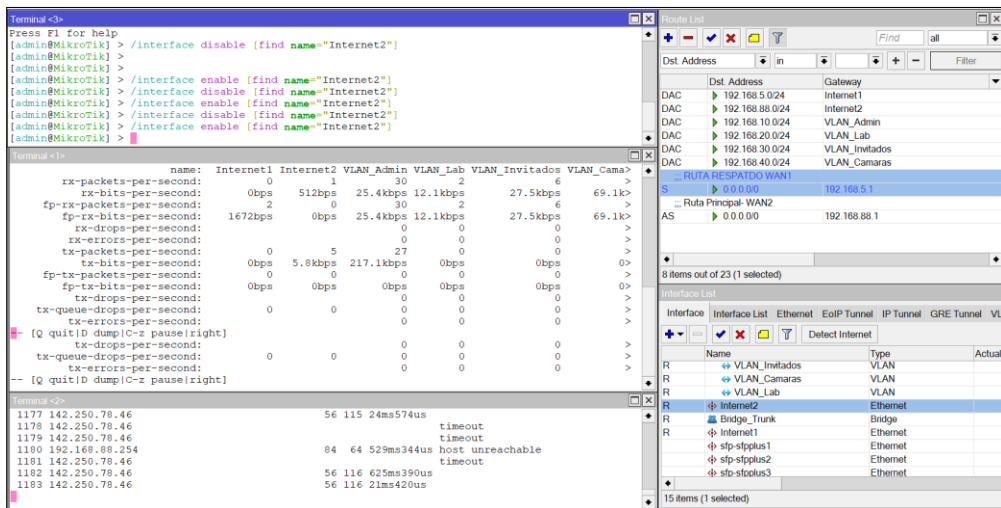


Figura 49 Prueba de failover
Fuente: Elaborado por autor

4.1.5.2 Restricciones de tráfico de ancho de banda entre VLANs

En el apartado nos muestra las prioridades según la necesidad que nuestra practica requiera en cual demostramos la configuración, que damos prioridad de tráfico a colas como cámaras VoIP que está conectada ala VLAN ID 40, como se puede demostrar tiene una tasa de tráfico más elevada con un total de datos procesados, que nos demuestra el uso constante y prioritario, así mismo la cola Prioridad VoIP generada en la VILAN 10 demostrando, el procesamiento de tráfico como prioridad dos, ya que es adecuado para llamadas de voz reduciendo posibles retardos, la cola Prioridad video conectada ala VLAN ID 20 tiene prioridad 3 reflejando menos tráfico pro con una prioridad adecuada, la cola General de Invitados en VLAN ID 30 tiene una prioridad 8 ya que muestra la actividad moderada y no prioritaria para la ocasión, y final mente las limitaciones que se dan en la red de invitados es cola se generó para limitar el ancho de banda pero no existen tráficos activos con estas pruebas se demuestra en tiempo real los valores de paquete por segundo y la calidad de gestión de los servicios prioritarios que reciban suficiente ancho de banda aunque las tasas de trafico de red están configuradas para mantener un equilibrio efectivo entre servicios críticos y no prioritarios tan como se muestra en la figura 50.

```
[admin@MikroTik] > /queue simple print stats
Flags: X - disabled, I - invalid; D - dynamic
0   ;;; Priorizar VLAN Cmaras
    name="Prioridad-Camaras" target=192.168.40.0/24 rate=91.7kbps/4.3Mbps total-rate=0bps
    packet-rate=155/433 total-packet-rate=0 queued-bytes=0/0 total-queued-bytes=0
    queued-packets=0/0 total-queued-packets=0 bytes=5359376/129956156 total-bytes=0
    packets=45992/108184 total-packets=0 dropped=0/20875 total-dropped=0

1   ;;; Priorizar VLAN Admin para VoIP
    name="Prioridad-VoIP" target=192.168.10.0/24 rate=36.9kbps/656.8kbps total-rate=0bps
    packet-rate=39/67 total-packet-rate=0 queued-bytes=0/0 total-queued-bytes=0
    queued-packets=0/0 total-queued-packets=0 bytes=28986364/463456165 total-bytes=0
    packets=203674/391745 total-packets=0 dropped=478/131019 total-dropped=0

2   ;;; Priorizar VLAN Lab para Video Streaming
    name="Prioridad-Video" target=192.168.20.0/24 rate=12.6kbps/4.6kbps total-rate=0bps
    packet-rate=2/3 total-packet-rate=0 queued-bytes=0/11616 total-queued-bytes=0
    queued-packets=0/8 total-queued-packets=0 bytes=16454235/644120737 total-bytes=0
    packets=267425/463522 total-packets=0 dropped=0/44305 total-dropped=0

3   ;;; Trfico general VLAN Invitados
    name="General-Invitados" target=192.168.30.0/24 rate=28.1kbps/961.7kbps total-rate=0bps
    packet-rate=31/95 total-packet-rate=0 queued-bytes=0/0 total-queued-bytes=0
    queued-packets=0/0 total-queued-packets=0 bytes=1901526/21916650 total-bytes=0
    packets=9215/20188 total-packets=0 dropped=47/3811 total-dropped=0

4   ;;; Limitar ancho de banda en VLAN Invitados
    name="PCQ-Invitados" target=192.168.30.0/24 rate=0bps/0bps total-rate=0bps
    packet-rate=0/0 total-packet-rate=0 queued-bytes=0/0 total-queued-bytes=0
    queued-packets=0/0 total-queued-packets=0 bytes=0/0 total-bytes=0 packets=0/0
    total-packets=0 dropped=0/0 total-dropped=0 pcq-queues=0/0
[admin@MikroTik] >
```

Figura 50 prioridades de ancho de banda
Fuente: Elaborado por autor

En el apartado **queue type print** se demuestra las configuraciones realizadas por diferentes tipos de cola en el equipo Mikrotik el cual es gestionada y al mismo tiempo prioriza el tráfico de la red

como se observa las colas están divididas en **PCQ (Per Connection Queuing)** que se dieron configuraciones como **PCQ Download** y **PCQ Upload** que distribuyen equitativamente el ancho de banda asignado entre diferentes accesos, el cual se clasifica el tráfico por direcciones fuentes o destino como **src address** y **dst address** y con colas **FIFO** y **SFQ** se ocupan colas **ethernet default** y **hospot default** que son mecanismos para manejar el tráfico de forma equitativa sin granular tal como está en la figura 51.

```
[admin@MikroTik] > /queue type print
Flags: * - default
0 * name="default" kind=pfifo pfifo-limit=50

1 * name="ethernet-default" kind=pfifo pfifo-limit=50

2 * name="wireless-default" kind=sfq sfq-perturb=5 sfq-allot=1514

3 * name="synchronous-default" kind=red red-limit=60 red-min-threshold=10 red-max-threshold=50
red-burst=20 red-avg-packet=1000

4 * name="hotspot-default" kind=sfq sfq-perturb=5 sfq-allot=1514

5 name="PCQ-Download" kind=pcq pcq-rate=2M pcq-limit=50KiB pcq-classifier=dst-address
pcq-total-limit=2000KiB pcq-burst-rate=0 pcq-burst-threshold=0 pcq-burst-time=10s
pcq-src-address-mask=32 pcq-dst-address-mask=32 pcq-src-address6-mask=128
pcq-dst-address6-mask=128

6 name="PCQ-Upload" kind=pcq pcq-rate=2M pcq-limit=50KiB pcq-classifier=src-address
pcq-total-limit=2000KiB pcq-burst-rate=0 pcq-burst-threshold=0 pcq-burst-time=10s
pcq-src-address-mask=32 pcq-dst-address-mask=32 pcq-src-address6-mask=128
pcq-dst-address6-mask=128

7 * name="pcq-upload-default" kind=pcq pcq-rate=0 pcq-limit=50KiB pcq-classifier=src-address
pcq-total-limit=2000KiB pcq-burst-rate=0 pcq-burst-threshold=0 pcq-burst-time=10s
pcq-src-address-mask=32 pcq-dst-address-mask=32 pcq-src-address6-mask=128
pcq-dst-address6-mask=128

8 * name="pcq-download-default" kind=pcq pcq-rate=0 pcq-limit=50KiB pcq-classifier=dst-address
pcq-total-limit=2000KiB pcq-burst-rate=0 pcq-burst-threshold=0 pcq-burst-time=10s
pcq-src-address-mask=32 pcq-dst-address-mask=32 pcq-src-address6-mask=128
pcq-dst-address6-mask=128

10 * name="multi-queue-ethernet-default" kind=mq-pfifo mq-pfifo-limit=50

11 * name="default-small" kind=pfifo pfifo-limit=10

[admin@MikroTik] > █
```

*Figura 51 lista de los tipos de colas configuradas
Fuente: Elaborado por autor*

Estas configuraciones realizadas nos aseguran una distribución eficiente del tráfico, aunque si disminuye el ancho de banda de nuestro acceso a Internet se asegura que para la distribución va a seguir funcionando, pero causa latencia más alta, pérdida de calidad de las aplicaciones utilizadas y caída de rendimiento.

4.1.6 Cloud router switch CRS112.8P-4S-IN

El cloud router switch es complementado con el router principal este es utilizado como modo puente las configuraciones impuestas de las misma que el router principal como las

configuraciones de las VLANs, pero a diferencia del router principal se cambia todas las VLANs a modo bridge para crear el puente y poder conectar nuestros dispositivos tal como se muestra en la figura 52.

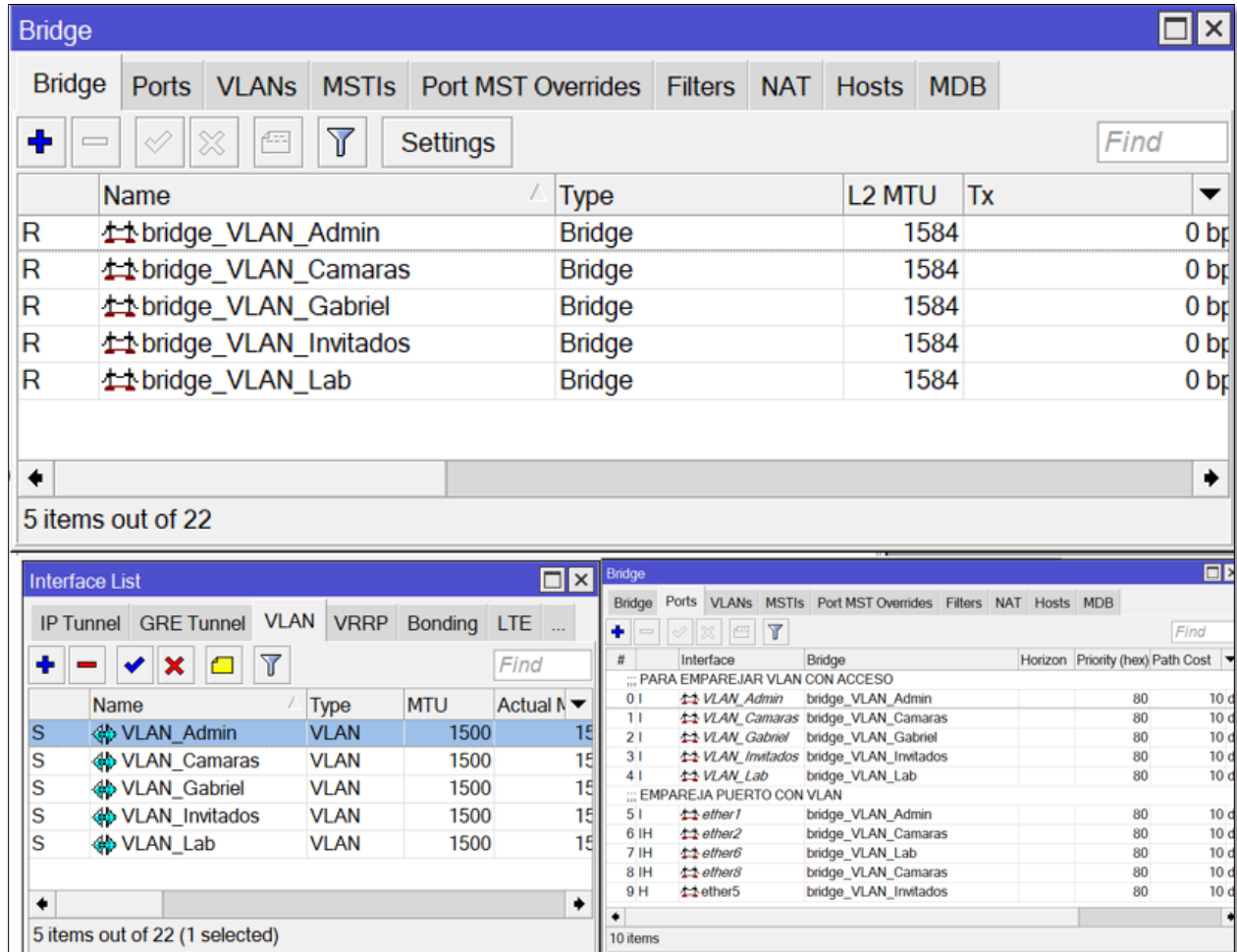


Figura 52 switch modo puente
Fuente: Elaborado por autor

CONCLUSIONES

- La configuración de balanceo de carga y failover entre las conexiones WAN demostró ser efectiva para asegurar la continuidad del proyecto al minimizar los tiempos inactividad del Internet en algunos escenarios de fallos.
- La segmentación de tráfico mediante las VLANs logró un flujo de datos más eficiente con la configuración realizada, y permitió el uso de recursos adecuado para cada segmento.
- La implementación de colas simples también permitió una adecuada distribución del ancho de banda, garantizando prioridades que se generó a los segmentos mientras limitaba el tráfico no esencial.
- La implementación con los equipos reales se identificaron problemas de conexión y la falta de visibilidad de tráfico entre los equipos lo que da la importancia a las pruebas en tiempo real de las interfaces.

RECOMENDACIONES

- Implementar herramientas de monitoreo como torch, ping o traffic-monitor al configurar nos permite visualizar en tiempo real la inactividad de las interfaces o anomalías antes que afecten a los usuarios.
- Inspeccionar el quipo al implementar pruebas para ver si el dispositivo soporta configuraciones como VLANs o bance de carga.
- Documentar las configuraciones realizadas backup que guarda las configuraciones y documentar todos los cambios hechos para facilitar el mantenimiento.
- Diseñar un plan de contingencia ante fallos inesperados incluyendo simulaciones como perdida de conexión y la capacidad de conmutación del sistema al recuperar trafico

REFERENCIAS

- [1] M. Syafrizal and O. Pahlevi, “Load Balancing dengan Metode HSRP Untuk Meningkatkan Akses Layanan Server PT. Telekomunikasi Indonesia Tbk. LOAD BALANCING DENGAN METODE HSRP UNTUK MENINGKATKAN AKSES LAYANAN SERVER PT. TELEKOMUNIKASI INDONESIA TBK”.
- [2] M. Syafrizal and O. Pahlevi, “Load Balancing dengan Metode HSRP Untuk Meningkatkan Akses Layanan Server PT. Telekomunikasi Indonesia Tbk. LOAD BALANCING DENGAN METODE HSRP UNTUK MENINGKATKAN AKSES LAYANAN SERVER PT. TELEKOMUNIKASI INDONESIA TBK”.
- [3] D. Mustofa, A. Wirasto, A. Muttakin, D. N. Astrida, D. Intan, and S. Saputra, “Implementation of Load Balancing Per Connection Classifier on Mikrotik for Internet Services at Private Vocational Schools”, doi: 10.58905/SAGA.vol1i3.169.
- [4] D. M. Kesa, “Corresponding author: Derick Musundi Kesa Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations,” *World Journal of Advanced Research and Reviews*, vol. 2023, no. 03, pp. 970–992, 2023, doi: 10.30574/wjarr.2023.18.3.1166.
- [5] U. Naseer, L. Niccolini, U. Pant, A. Frindell, R. Dasineni, and T. A. Benson, “Zero Downtime Release: Disruption-free Load Balancing of a Multi-Billion User Website,” 2020, doi: 10.1145/3387514.3405885.
- [6] A. Seufert, S. Schröder, and Michael Seufert, “Delivering User Experience over Networks: Towards a Quality of Experience Centered Design Cycle for Improved Design of Networked Applications,” vol. 2, p. 463, 2021, doi: 10.1007/s42979-021-00851-x.
- [7] O. V Lemeshko, O. S. Yeremenko, M. O. Yevdokymenko, and B. Sleiman, “OPTIMIZING HARD QOS AND SECURITY WITH DISJOINT PATH ROUTING”.
- [8] A. Ghaffari and V. A. Takanloo, “QoS-Based Routing Protocol with Load Balancing for Wireless Multimedia Sensor Networks Using Genetic Algorithm,” *World Appl Sci J*, vol. 15, no. 12, pp. 1659–1666, 2011.
- [9] “Enrutadores y dispositivos inalámbricos MikroTik - Productos: CRS310-1G-5S-4S+IN.” Accessed: Nov. 30, 2024. [Online]. Available: https://mikrotik.com/product/crs310_1g_5s_4s_in
- [10] “¿Qué tipo de balanceo recomiendas en MikroTik RouterOS? - abcXperts.” Accessed: Nov. 30, 2024. [Online]. Available: <https://abcxperts.com/docs/que-tipo-de-balanceo-recomiendas/?srsltid=AfmBOooMnpzN34ajrnn3j9fc8AEQ-kachF0kj542rnRms7VY4hOZKYN7>