Universidad Católica de Santa María

Facultad de Ciencias e Ingenierías Físicas y Formales

Escuela Profesional de Ingeniería Electrónica

DISEÑO DE UN PUNTO DE INTERCAMBIO DE TRÁFICO PARA LA MEJORA EN EL SISTEMA DE COMUNICACIÓN PRIVADA ENTRE UNA MUNICIPALIDAD Y SUS COMISARÍAS PARA LA CIUDAD DE AREQUIPA

Tesis presentada por el Bachiller:

Siú Velarde, Ferdy Arturo

para optar el Título Profesional de:

Ingeniero Electrónico

Con Especialidad en:

Telecomunicaciones

Asesor:

Dr. Ing. Sulla Torres, Raúl Ricardo

Arequipa-Perú

2021

DICTAMEN

UCSM-ERP

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

INGENIERIA ELECTRONICA

TITULACIÓN CON TESIS

DICTAMEN APROBACIÓN DE BORRADOR

Arequipa, 26 de Julio del 2021

Dictamen: 001938-C-EPIE-2021

Visto el borrador del expediente 001938, presentado por:

2010240231 - SIU VELARDE FERDY ARTURO

Titulado:

DISEñO DE UN PUNTO DE INTERCAMBIO DE TRáFICO PARA LA MEJORA EN EL SISTEMA DE COMUNICACIóN PRIVADA ENTRE UNA MUNICIPALIDAD Y SUS COMISARíAS PARA LA CIUDAD DE AREQUIPA

Nuestro dictamen es:

APROBADO

1567 - COAGUILA GOMEZ RONALD PERCING
DICTAMINADOR

1691 - QUISPE YAUYO JUAN MEDARDO
DICTAMINADOR

1692 - VALDIVIESO HERRERA DIANA ISABEL
DICTAMINADOR

DEDICATORIA

A mi madre por su apoyo infinito.

AGRADECIMIENTOS

A las personas que me apoyaron en este proyecto.

RESUMEN

El presente estudio propone el diseño de un punto de intercambio de tráfico en un distrito de la ciudad de Arequipa entre la municipalidad y las comisarías de su jurisdicción. A través de la obtención de los datos y calculando el promedio del ancho de banda requerido, considerando los servicios de mayor utilización en redes de comunicaciones como: VoIP, video y datos para determinar las capacidades de enlaces siendo la base del diseño.

El diseño de la topología del punto de intercambio de tráfico es apto para cualquier marca. Pero basa la configuración del diseño en la marca Mikrotik, por poseer una imagen de sistema operativo de licencia libre y por no tener la necesidad de poseer diferentes licencias para las funcionalidades requeridas, además por ser equipos robustos que soportan el tráfico y topología, realizando la simulación en un entorno virtual de licencia libre.

El diseño de la red de telecomunicaciones propuesta para el punto de intercambio de tráfico consta: del manejo, análisis y funcionamiento de las cuatro primeras capas del modelo OSI, con herramientas para medir latencias, tiempos de redundancia, pérdidas de paquetes y un analizador de protocolos para optimizar el diseño.

Finalmente, se logró desarrollar el diseño de la topología del punto de intercambio, de tráfico en base a los cálculos realizados para las capacidades de enlace, realizando las pruebas de funcionamiento y medición de las diferentes propuestas presentadas con las variables del punto de intercambio de tráfico, obteniendo así un enfoque de uso privado con servicios propios y compartidos.

Se espera que este diseño, pueda servir como modelo para la implementación de futuros puntos de intercambio en la ciudad, como en el país.

Palabras Claves: *Análisis, Diseño, Ancho de Banda, Punto de Intercambio de Tráfico, Protocolos, Mikrotik*

ABSTRACT

This study proposes the design of a traffic exchange point in a district of the city of Arequipa between the municipality and the police stations in its jurisdiction. Through obtaining the data and calculating the average of the required bandwidth, considering the most widely used services in communications networks such as: VoIP, video and data to determine the link capacities, being the basis of the design.

The design of the peering point topology is suitable for any brand. But it bases the design configuration on the Mikrotik brand, for having a free license operating system image and for not having the need to have different licenses for the required functionalities, in addition to being robust equipment that supports traffic and topology, performing the simulation in a virtual environment of free license.

The design of the telecommunications network proposed for the traffic exchange point consists of: the management, analysis and operation of the first four layers of the OSI model, with tools to measure latencies, redundancy times, packet losses and a protocol analyzer to optimize the design.

Finally, it was possible to develop the design of the traffic exchange point topology based on the calculations made for the link capacities, carrying out the performance tests and measurement of the different proposals presented with the variables of the traffic exchange point. , thus obtaining a private use approach with its own and shared services.

It is expected that this design can serve as a model for the implementation of future exchange points in the city, as well as in the country.

Keywords: *Analysis, Design, Bandwidth, Traffic Exchange Point, Protocols, Mikrotik*

INTRODUCCIÓN

Un punto de intercambio de tráfico es el intercambio de redes de datos entre tres o más participantes que se interconectan a una infraestructura física, en la cual por medio de protocolos de enrutamiento hacen emparejamientos y publican sus redes de forma directa, sin necesidad de usar sus enlaces de internet.

En el Perú existe en funcionamiento dos puntos de intercambio de tráfico, uno funciona solo en Lima y otro que está en actual formación y crecimiento; mientras que en otros países de Latinoamérica se posee un punto de intercambio por ciudad.

Esto en consecuencia genera que muchas entidades gubernamentales posean conexiones de internet en diferentes proveedores locales, con capacidades insuficientes. Lo cual limita su conexión externa hacia diferentes servicios internacionales como nacionales y en algunos casos locales.

Por ello y en base a la necesidad de la creación de nuevos puntos de intercambio de tráfico que apoyen el desarrollo de las redes y el internet en el Perú; se desarrolló el diseño de una topología de red de un punto de intercambio de tráfico en un entorno virtual con equipos de la marca Mikrotik. Buscando incentivar su creación, así como dar un acercamiento al funcionamiento, diseño y desempeño.

Para el desarrollo de esta topología se seleccionó un emulador de licencia libre y de fácil manejo que ayude a modelar el sistema para poder realizar las pruebas de funcionamiento, así como imágenes del sistema operativo de los dispositivos utilizados de libre adquisición, con la finalidad de encontrar puntos a favor y en contra frente a una posible implementación.

Finalmente, en la presente tesis se incluye el manejo del emulador propuesto, la topología presentada junto a su implementación en el entorno virtual, mostrando propuestas de diseño y evaluando la mejor alternativa para una futura implementación.

Los resultados obtenidos de las pruebas de funcionamiento del punto de intercambio se desarrollaron en base a los diferentes protocolos utilizados y presentando una propuesta de equipos seleccionados para una implementación física del proyecto.

La tesis está conformada por 8 capítulos distribuidos de la siguiente manera:

En el Capítulo I; se plantea el problema de investigación, se brinda una introducción al problema dando a conocer su identificación, descripción del problema, objetivos, estado de arte y los aportes de la tesis.

En el Capítulo II; se aborda el marco teórico, presentando los conceptos que engloban al punto de intercambio de tráfico, su funcionamiento, tipos y una vista a la evolución en América latina, centrándose en el enfoque de Perú.

En el Capítulo III; se desarrolla una evaluación y análisis de las necesidades de diseño del punto de intercambio de tráfico realizando el cálculo de los principales servicios para determinar anchos de banda.

En el Capítulo IV; se determina la metodología de medición presentando las variables a medir en la tesis propuesta, así como los instrumentos utilizados para poder realizar dichas mediciones.

En el Capítulo V; se determina las herramientas de implementación, software y hardware que se utilizara en la tesis como modelo.

En el Capítulo VI; se desarrolla los diseños y propuestas de topologías que se aplicaran para el desarrollo del punto de intercambio de tráfico y realizando comparaciones de funcionamiento entre ellas para determinar la mejor alternativa de diseño.

En el Capítulo VII; se aplicará una propuesta practica desarrollando la simulación de la topología final y presentando la topología según sus diferentes etapas. Asimismo, se obtiene los resultados de la simulación y el análisis de esos resultados por medio de los instrumentos de medición presentados.

En el Capítulo VIII; se determina el equipamiento necesario para la implementación del punto de intercambio de tráfico determinando su utilidad y presupuesto.

Finalmente se plantea las conclusiones en función de los objetivos planteados y las recomendaciones ante futuras aplicaciones o mejoras en el diseño propuesto.

ÍNDICE

CAPITULO VI: DISEÑOS Y PROPUESTAS 0126

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ACRÓNIMOS

ACELP: Predicción Lineal Excitada por Código Algebraico (Algebraic Code Excited Linear Prediction)

ADPCM: Modulación de Código de Pulso Diferencial Adaptativo (Adaptative Differential Pulse-Code Modulation)

AFRINIC: Registro regional de Internet para África (African Network Information Center)

AOC: Cable Óptico Activo (Active Optical Cable)

APNIC: Registro Regional para Asia y Pácifico (Asia-Pacific Network Information Center)

ARP: Protocolo de Resolución de Direcciones (Address Resolution Protocol)

AS: Sistema Autónomo (Autonomous System)

ASN: Número de Sistema Autónomo (Number of Autonomous System)

BGP- MP: Protocolo de puerta de enlace de frontera (Border Gateway Protocol - MultIProtocol)

BGP: Protocolo de puerta de enlace de frontera (Border Gateway Protocol)

BTU: Unidad Térmica Británica (British Thermal Unit)

CDN: Red de Distribución de Contenido (Content Delivery Network)

CIDR: Enrutamiento entre Dominios sin Clases (Classless Inter-Domain Routing)

CPU: Unidad Central de Procesamiento (Central Processing Unit)

CS-ACELP: Estructura Conjugada ACELP (Conjugate Structure ACELP)

DHCP: Protocolo de Configuración Dinámica de Host (Dynamic Host Configuration Protocol)

DNS: Servidores de Nombre de Dominio (Domain Name Server)

ESP: Carga de Seguridad de Encapsulación (Encapsulation Security Payload)

FIFO: Primero en Entrar Primero en Salir (First In First Out)

GB: Gigabyte

GNS: Simulación Gráfica de Redes (Graphic Network Simulation)

GPS: Gigabit por Segundo (Gigabit per second)

GUI: Interfaz gráfica de Usuario (Graphical User interface)

ICMP: Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol)

ICREA: Asociación Internacional de Expertos en Data centers (International Computer Room Experts Association)

ID: Identificador (Identifier)

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers)

IGMP: Protocolo de Mensajes de Control de Internet (Internet Group Managment Protocol)

IOS: Sistema Operativo Internetwork (Internetwork Operating System)

IP: Protocolo de Internet (Internet Protocol)

IPng: IP Siguiente generación (IP Next Generation)

IPP: Punto de intercambio de tráfico (Internet Peering Point)

ISP: Proveedor de Servicios de Internet (Internet Service Provider)

ITU: Unión Internacional de Telecomunicaciones (The International Telecommunication Union)

IX-F: Federación de Intercambio de Internet (Internet eXchange Federation)

IXP: Punto de intercambio de tráfico (Internet Exchange Point)

L2TP: Protocolo de túnel de capa (2Layer 2 Tunneling Protocol)

LAC-IX: Puntos de intercambio de América y el Caribe (Latin America and Caribean IXPS)

LACNIC: Registro de Direcciones de Internet de América Latina y Caribe (Latin American and Caribbean Internet Address Registry)

LACP: Protocolo de Agregación de enlaces (Link Agregation Control Protocol)

LLC: Control de Enlace Lógico (Logical Link Control)

LSA: Anuncio de Estado de Enlace (Link State Advertisement)

MAC: Control de Acceso a Medios (Media Access Control)

Mbps: Megabits por Segundo (Megabits per Second)

MPLS: Conmutación de Etiquetas MultIProtocolo (MultIProtocol Label Switching)

Ms: Milisegundos

MUM: Reunión de Usuarios Mikrotik (Mikrotik User Meeting)

NAP: Punto de Acceso a la Red (Network Access Point)

NIR: Registros Nacionales de Internet (Nacional Internet Registry)

NSP: Proveedores de Servicios de Red (Network Service Provider)

OSI: Interconexión de sistemas abiertos (Open System Interconnection)

OSPF: Abrir el Camino más Corto **(**Open Shortest Path First)

P2P: Red de Pares (Peer Two Peer)

PCM: Modulación de Código de Pulso (Pulse Mode Modulation)

Ping: Buscador de paquetes en redes (Packet Internet Groper)

PIT: Punto de Intercambio de tráfico

PNETLab: Laboratorio de Herramientas de Emulador de Redes (Packet Network Emulator Tool Lab)

PPS: Paquete Por Segundo (Paquet Per Second)

PPTP: Protocolo de túnel Punto a punto (Point to Point Tunneling Protocol)

QoS: Calidad de Servicio (Quality of Service)

RA: Arbitro de Enrutamiento (Routing Arbitrator)

RIP: Protocolo de información de encaminamiento (Routing Information Protocol)

RIR: Registro Regional de Internet (Regional Internet Registry)

RPKI: Infraestructura de Clave Pública de Recursos (Resource Public Key Infrastructure)

RSTP: Protocolo de árbol de expansión Rápido (Rapid Spanning Tree Protocol)

SSH: Cápsula Segura **(**Secure Shell)

STP: Protocolo de árbol de expansión (Spanning Tree Protocol)

TTL: Tiempo de vida (Time to Live)

VoIP: Voz sobre protocolo de Internet (Voice Over IP)

VPLS: Servicio de Lan Privada Virtual (Virtual Private Lan Service)

VRRP: Protocolo de redundancia de Router Virtual (Virtual Router Redundancy Protocol)

WISP: Proveedor de Servicios de Internet Inalámbrico (Wireless Internet Service Provider)

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1. Problema de Investigación

1.1 Identificación del problema

Los sistemas de comunicación de redes de datos entre municipalidades y comisarías de la ciudad de Arequipa trabajan de forma independiente, perdiendo recursos que pueden ser aprovechados si se cuenta con un sistema de comunicación privado conectado entre ellos. Cada municipalidad, así como las comisarías, cuentan con conexiones de internet independientes y con servicios de red independientes, lo cual genera que las consultas que pueda haber entre ellos sean lentas y estén limitadas por el ancho de banda contratado por cada una.

Problemas como un corte de servicio de internet en alguna de estas entidades provocaría que los servicios prestados en la red dejen de ser publicados, provocando caídas de servicio y pudiendo generar problemas en la seguridad de la ciudadanía.

1.2 Descripción del problema

En la actualidad, un punto de intercambio de tráfico está diseñado para interconectar los diferentes proveedores de servicio de internet (ISP) de una localidad con proveedores de contenido (CDN) y algunos organismos de gobierno; para mejorar la conectividad entre ellos y reducir los costos de interconexión a nivel internacional, mejorando de esta manera niveles de latencia, aumento en tasas de transferencia y performance en el servicio prestado a sus usuarios. La comunicación entre los distintos miembros del punto de intercambio de tráfico se hace directamente por protocolos de enrutamiento, con sus respectivos recursos IP.

Es importante mencionar que, para la interconexión en el punto de intercambio de tráfico, cada miembro debe poseer sus propios recursos IPS brindados por el RIR de su

localidad, para el caso de Latinoamérica y el Caribe el RIR encargado de brindar la asignación de recursos es LACNIC.

De esta manera, los miembros del punto de intercambio de tráfico se comunican de forma directa sin tener que utilizar recursos de conexión internacional. Siendo limitados por la capacidad del enlace físico que los interconecta al punto de intercambio de tráfico.

En base a los beneficios brindados por el punto de intercambio de tráfico y por el poco desarrollo que tienen en Perú en comparación a países como Chile, Argentina, Brasil.

Se propone el diseño de un punto de intercambio de tráfico, para poder interconectar una municipalidad y sus comisarías para la ciudad de Arequipa con el fin de mejorar la conexión entre estas y puedan prestar mayores servicios IP en favor de la seguridad de la población.

Esto también con la finalidad de crear una red redundante y convergente ante problemas de conexión externa a su red, es decir, un corte de servicio de internet que provoque la caída de servicios prestados por la entidad y podrá ser solucionados por medio de este sistema garantizando una conexión a un nivel requerido.

Finalmente, implementando el punto de intercambio de tráfico, permite escalar el sistema de forma rápida integrando nuevos miembros bajo el mismo concepto y mejorando sus prestaciones.

1.3 Objetivos

1.3.1 General

Diseñar y simular un punto de intercambio de tráfico, que conecte una municipalidad con sus Comisarías en la ciudad de Arequipa, por medio de un emulador de red utilizando equipos Mikrotik.

1.3.2 Especifico

- Evaluar las principales variables dentro del funcionamiento de un punto de intercambio de tráfico.
- Emplear herramientas licencia libre para la simulación, tanto en software de dispositivos como el entorno de emulación.
- Manejo del protocolo de internet en sus dos versiones IPv4 e IPv6 para los equipos simulados.
- Simular el funcionamiento de un punto de intercambio de tráfico con equipos Mikrotik.
- Evaluar el desempeño del diseño de forma cuantitativa y cualitativa del diseño propuesto.

1.4 Alcance

El alcance de la tesis busca presentar el diseño de un punto de intercambio de tráfico disponible para cualquier marca, pero basado en la configuración de equipos de la marca Mikrotik.

La implementación del diseño se realizará por medio del emulador PNETLab con el fin de poder medir el desenvolvimiento del punto de intercambio con la marca propuesta y verificar su funcionamiento.

Finalmente busca proponer el desarrollo en los servicios de redes e internet de Arequipa como:

- Conocimiento en el funcionamiento de un punto de intercambio de tráfico.
- Manejo local de servicios internos.
- Incentivo a la creación de puntos de intercambio de tráfico.
- Expansión del uso de recursos y creación de nuevos servicios.
- Desarrollo en las redes de los participantes.

1.5 Limitación

Las limitaciones presentadas en la siguiente tesis son las siguientes:

- La versión gratuita de la imagen del sistema operativo de Mikrotik brinda solo 1 Mbps de tráfico, imposibilitando pruebas reales de throughput entre los enlaces.
- La versión gratuita de la imagen del sistema operativo de Cisco proporciona una sola interfaz de red para poder realizar la topología.
- El gran número de dispositivos utilizados para la topología limita el uso de recursos del computador donde se corra la simulación.
- Algunos protocolos no funcionan de la misma manera en un entorno virtual como en el real.

1.6 Estado del arte

El acceso a internet se ha convertido en una de las necesidades primordiales por los países del mundo. Con la evolución de las tecnologías de información y con servicios que disponen de internet para poder intercomunicarse, hace que la demanda del uso de internet presente niveles de crecimiento a través de los años.

Esto a su vez, genera un problema del uso de recursos físicos de interconexión para poder comunicar todos los destinos que componen internet.

Como parte de la solución ante este problema, nace la necesidad de crear puntos estratégicos de intercambio de tráfico que eviten el sobre uso de esos recursos y a su vez generen ventajas en su implementación.

A estos puntos de intercambio de tráfico se les denomina IXP por sus siglas en ingles Internet Exchange Point o Puntos de Intercambio de Tráfico.

Los IXP hoy en día están ubicados en gran parte del mundo mejorando la interconectividad y evolucionando la infraestructura de internet.

Estos puntos de intercambio de tráfico generan grandes ventajas, como la reducción en tiempos de respuesta, mejor manejo de la infraestructura internacional, mayores capacidades, entre otros.

El enfoque de un punto de intercambio de tráfico fue establecido para poder interconectar proveedores de internet y proveedores de contenido y de esa forma facilitar el intercambio de tráfico entre ellos, pero como parte de la evolución de los puntos de intercambio de tráfico este enfoque fue cambiando y se empezaron a establecer puntos de intercambio de tráfico más específicos, en los que los participantes pueden ser de un ámbito educacional, gubernamental, religioso, entre otros. Buscando el mismo fin, mejorar su interconectividad y dar un paso más en el desarrollo de sus redes.

América latina no es ajena al desarrollo de los puntos de intercambio de tráfico, teniendo como claro ejemplo Brasil, Chile y Argentina, países con gran desarrollo en la creación de IXP en su territorio.

En la actualidad, Perú no cuenta con un desarrollo evolutivo en la creación de puntos de intercambio de tráfico de ningún tipo, ya que a la fecha cuenta con punto de intercambio de tráfico denominado Nap Perú ubicado en la capital y un punto de intercambio recién en proceso de expansión denominado Pit Perú.

1.7 Antecedentes

A continuación, se presentan trabajos enfocados en el desarrollo e impacto de los puntos de intercambio de tráfico.

Título: Promoción del uso de puntos de intercambio de tráfico: una guía de políticas, gestión y problemas técnicos.

Autor: Jensen Mike

Año:2012

Tipo: Articulo presentado por la Internet Society

En este artículo el autor desarrolla el aspecto técnico en la implementación de un punto de intercambio de tráfico, presenta ejemplos de puntos de intercambio de tráfico, así como los modelos operacionales y una perspectiva de los puntos importantes a tener en cuenta en la implementación del punto de intercambio de tráfico.

Título: La Conectividad en América Latina y el Caribe: El rol de los Puntos de Intercambio.

Autor: Galperín Herman

Año:2013

Tipo: Informe presentado por la Internet Society.

El informe presenta el desarrollo de puntos de intercambio de tráfico de 4 países de Latinoamérica y el Caribe. Recopilando mejores prácticas, y su evolución con el fin

de incentivar la creación de un mayor número de puntos de intercambio de tráfico en la región y poder brindar un alza en la mejora de los servicios prestados.

Título: Tomografía de la red: Medición de parámetros De un Internet eXchange Point.

Autor: Carisimo Esteban

Año: 2014

Tipo: Tesis licenciatura Ingeniería Electrónica.

Título: Modelos e impactos de los puntos de intercambio de tráfico (IXP) en América Latina y Caribe.

Autores: Jolías Lucas, Prince Alejandro.

Esta tesis describe el impacto en la creación de un punto de intercambio de tráfico en Bolivia, basado en la medición de parámetros por medio de una plataforma creada por el autor.

Tipo: Artículo publicado en el simposio argentino sobre tecnología y Sociedad.

En este artículo se desarrolla el impacto que tuvieron 9 países de Latinoamérica y el Caribe en el desarrollo de sus puntos de intercambio de tráfico, realizando comparativas sobre la evolución del tráfico tratado, ventajas en la implementación, tipos de modelos organizacionales y los impactos que tuvo la creación de estos puntos de intercambio de tráfico.

Título: Diseño de Puntos de Intercambio de Internet en entornos virtuales con tecnología Cisco, implementando servicios multimedia.

Autores: Padilla Estrada Néstor Jose, Rojos Lorío Aliana mercedes, Ramírez Santana Ulises Andrés

Año: 2018

Tipo: Tesis licenciatura en ingeniería en telemática.

Esta tesis de grado, se presenta el diseño de un punto de intercambio de tráfico, en diferentes etapas, implementando en cada una de estas etapas un servicio adicional o servicios comúnmente utilizados en un punto de intercambio de tráfico, todo en un entorno virtual.

1.8 Aportes

Como aportes del siguiente trabajo se tiene:

- Análisis del ancho de banda requerido de una municipalidad con las comisarías de un distrito y el diseño de red de telecomunicaciones de un punto de intercambio de tráfico basado en la marca Mikrotik desde la perspectiva de 3 capas del modelo OSI, capa de enlace de datos, capa de red y capa de transporte.
- Manejo de un emulador de redes y su forma de funcionamiento con diferentes marcas de dispositivos.
- Un análisis de los resultados obtenidos y un enfoque del funcionamiento de los protocolos en la marca propuesta.
- Comparaciones de trabajo en la versión virtual de la marca y simulando un entorno de trabajo real.

CAPÍTULO II: MARCO TEÓRICO

2. Fundamentos Teóricos

2.1 Recursos IP

2.1.1 IPv4

El formato del protocolo de internet versión 4 está formado por 32 bits, distribuidos en 4 octetos y separados por puntos. Haciendo un total de 4 294 967 296 direcciones únicas. Estas direcciones pueden ser presentadas en formato binario o decimal.

A continuación, se muestran las dos notaciones más comunes para representar direcciones IPv4, ambas equivalentes entre sí:

Decimal: 172.65.86.2

Binario: 10101100. 01000001. 01010110. 00000010

En la tabla 1 se desarrolla el análisis la dirección 172.65.86.2/24 detallando los parámetros de red que involucran a la IP mencionada.

Tabla 2.Análisis de dirección IPv4

Dirección	IPv4
Notación completa	172.65.86.2 /24
Red	172.65.86.0
Host	172.65.86.2
Broadcast	172.65.86.1
Prefijo de red	/24

Fuente: Elaboración propia.

2.1.1.1 Cabecera IPv4

Según Information Sciences Institute (1981), el datagrama IP está formado por 2 campos, los cuales son: el campo de la cabecera IP y el campo de contenido que alberga información sobre servicios de protocolos de nivel superior.

Según Information Sciences Institute (1981), la parte de la cabecera IP contiene datos como las direcciones origen y destino, el tipo de protocolo e información relevante para que se pueda efectuar la comunicación de las partes.

Figura 2.Encabezado del protocolo IPv4.
Fuente: *Mejía (2011)*

Según Information Sciences Institute (1981), en la figura 1 se muestra el esquema del encabezado del protocolo IPv4.

- Versión: comprendida por 4 bits, indica la versión del formato de la cabecera IP.
- Longitud de cabecera: conformada por los 4 bits siguientes, indica el comienzo de los datos.
- Tipo de servicio: comprendida por 8 bits, brinda una visión de los parámetros de la calidad de servicio y también determina los tipos servicios que se pueden brindar, como datos, voz, etc.
- Longitud total: comprendida por 16 bits, es la longitud del datagrama por completo. Medible en octetos o bytes incluidos el encabezado y los datos, tiene como límite máximo 65 536 bytes.
- Identificación: comprendido por 16 bits, es un valor añadido por el emisor, para que del lado del receptor pueda recibir los fragmentos de datagrama y puedan ser ensamblados de su lado.
- Banderas: comprendido por 3 bits, indica si existe fragmentación.

  - Bit 0: reservado, con valor predeterminado de cero.
  - Bit 1: Con un valor de 0 indica que es divisible, con un valor de 1 indica que no es divisible.
  - Bit 2: Si el valor es 0 es la última parte del fragmento, si el valor es 1 indica que existen más fragmentos del datagrama.

- Desplazamiento de fragmento: comprendido por 13 bits, este campo muestra la parte del datagrama que pertenece al fragmento. Con un valor de 0 se reconoce la primera parte de varios fragmentos.
- Tiempo de vida (TTL): comprendido por 8 bits, indica la cantidad de veces que el paquete puede cursar por la red antes de ser desechado. El valor máximo es de 255 y el conteo es de forma descendente hasta llegar a un valor de 0, cuando llegue a este valor el paquete será descartado por el router.
- Protocolo: comprendido por 8 bits, indica el tipo de protocolo utilizado por el datagrama de internet.
- Suma de comprobación de encabezado: comprendido por 16 bits, verifica que los datos no hayan sido modificados, la comprobación se hace por medio de un algoritmo, el cual suma los componentes de los 16 bits del encabezado.
- Dirección IP Origen: comprendida por 32 bits, muestra la dirección del dispositivo correspondiente al origen del datagrama
- Dirección IP Destino: comprendida por 32 bits, muestra la dirección del dispositivo al cual se le enviará el paquete.

2.1.1.2 Clases de direcciones

Clase A

Según Information Sciences Institute (1981), la clase A, designa 7 bits de mayor peso para definir la dirección de red correspondiente a su clase y los 24 bits restantes servirán para definir las direcciones locales.

Clase B

Según Information Sciences Institute (1981), la clase B, utiliza los primeros 14 bits de mayor peso para poder separar la dirección de red y los 16 sobrantes son para definir las direcciones locales.

Clase C

Según Information Sciences Institute (1981), la clase C, maneja los 21 bits de mayor peso para poder definir las direcciones de red, los 8 restantes son para las direcciones locales.

Clase D

Según Information Sciences Institute (1981), la clase D es el rango de direcciones definidos por la red 224.0.0.0/4, utilizado para asignaciones IPv4 Multicast.

Clase E

Según Cotton y Vegoda (2010), definen la clase E como el bloque de direcciones reservado para aplicaciones en el futuro.

2.1.1.3 Tipos de direcciones

Públicas

En la versión IPv4 existe un tipo de direcciones únicas entre sí, es decir, no se repiten en ninguna parte del mundo y son a través de estas IPs que los servicios públicos de internet funcionan en el mundo.

Según el Registro de direcciones de Internet para America Latina y Caribe (2020), las direcciones de uso único y global son denominas direcciones públicas ya que cuentan con un propósito único dentro de internet, el cual es comunicar servicios que corran en la red, comunicados a través de estas IPs.

Privadas

Según el Registro de direcciones de Internet para America Latina y Caribe (2020), este tipo de espacio de direcciones no deben ser alcanzables desde el exterior de una red local, es decir, no deben ser visibles desde internet.

Según el Registro de direcciones de Internet para America Latina y Caribe (2020), este rango de direcciones fue seleccionado para operar dentro de las redes privadas de las organizaciones, por lo que no se debe solicitar ningún permiso a ningún registro de internet para poder utilizarlas.

Estas direcciones IPv4 privadas se muestran en la tabla 2.

Tabla 3. Clases de direcciones IPv4

Clase	Rango de direcciones IP	CIDR	Número de redes
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8	1
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12	16
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16	254
Uso especial	169.254.0.0 – 169.254.255.255	169.254.0.0/16	1

Fuente: Elaboración propia.

Direcciones Especiales y reservadas

Según el Registro de direcciones de Internet para America Latina y Caribe (2020), se definen a este tipo de direcciones IPv4 como las conceptualizadas en el RFC 1112[1] que son utilizadas para aplicaciones del tipo multidifusión.

2.1.2 IPv6

Como parte del cambio, expansión y evolución de internet. El aumento exponencial de aplicaciones ligadas a esté, el aumento de dispositivos requeridos, la seguridad, entre otros factores hizo que la versión 4 del protocolo de internet no supla las nuevas necesidades, por tanto, la creación de un nuevo protocolo que pudiera sostener esta evolución se hizo necesaria.

Según el Registro de direcciones de Internet para America Latina y Caribe (2020), a raíz de la necesidad de la creación de un protocolo que preceda al de la versión 4, se creó la versión 6 del protocolo de internet, la cual empezó a mediados de 1991, año en el cual, la IETF crea un grupo de trabajo para fomentar el desarrollo, investigación y estudio para resolver los problemas del crecimiento de internet, en el año 1993 IETF denomino a este grupo de trabajo como IPng (IP next generation).

Según Gerometta (2011), el proceso empieza en el año 1993 cuando se realiza la publicación de un RFC dando a conocer los nuevos requerimientos solicitados para la creación del nuevo protocolo, denominado en ese momento como IPng.

Según Gerometta (2011), en el año 1995, se le denomina oficialmente a esta nueva versión del protocolo como protocolo de internet versión 6 (IPv6), en 1996 las primeras

[1] RFC: 1112: https://tools.ietf.org/html/rfc1112

pruebas se corren sobre una infraestructura de internet denominada 6bone en la cual Cisco daba soporte a un número reducido de sus dispositivos.

Según Gerometta (2011), para el año 1999 se da inicio a la concesión de prefijos IPv6 a los proveedores de internet (ISP), año 2000 los principales fabricantes empiezan a dar soporte en sus equipos al nuevo protocolo de internet, en el año 2006 finalizan los periodos de prueba sobre el protocolo.

2.1.2.1 Cambios frente al protocolo de internet versión 4

Según Deering y Hinden (1998), las variaciones del protocolo versión 4 de internet y la versión 6 están definidos por las siguientes características.

- Aumento en las capacidades de direcciones: permite un mayor número de direcciones a partir del aumento de la cantidad de bits en la dirección IP, de 32 a 128 bits. Aumentando un campo alcance (Scope), mejora la escalabilidad en el enrutamiento de multidifusión. Finalmente, para enviar paquetes a un conjunto o grupo de nodos, se utiliza una nueva dirección denominada dirección Anycast.
- Reducción en el formato del encabezado: con el fin de optimizar el procesamiento de los router y el costo de ancho de banda ocupado por el encabezado, se utilizaron algunos campos de forma opcional y se eliminaron otros campos del encabezado de IPv4 en el nuevo formato del encabezado IPv6.
- Optimización en el soporte para extensión y opciones: la forma en que los encabezados IP son codificados en la nueva versión, permite la posibilidad de agregar nuevas opciones en el futuro, un reenvió más eficaz y facilitan el manejo de la longitud de las opciones.

- Capacidad de etiquetado de flujo: tiene la capacidad de poder seleccionar flujos de tipos de tráfico solicitados por él remitente, lo que va permitir seleccionar tipos de servicios, dando la posibilidad a un manejo del servicio en tiempo real para un manejo de calidad de servicio.
- Capacidad de privacidad y autenticación: la autenticación, privacidad y la confidencialidad son extensiones existentes en los encabezados de la versión 6 del protocolo de internet.

2.1.2.2 Cabecera IPv6

La característica general del protocolo de internet versión 6 es la cantidad de bits disponibles en la dirección IP, cuenta con 128 bits lo cual posibilita la cantidad de 2^{128} direcciones, equivalente a 340 sextillones de direcciones versión 6.

Según Mejía (2011), la versión 6 del protocolo de internet trae consigo diferencias en su cabecera respecto a su par de la versión 4. Estas diferencias buscan tener un proceso más eficiente al momento de procesar la lectura de las cabeceras, reduciendo tiempos y nivel de procesamiento en los router. Para lograr esto, muchos de los campos de la cabecera del protocolo de internet versión 4 fueron eliminados o puestos como optativos para la nueva versión 6 del protocolo.

Según Mejía (2011), se reducen los campos de la cabecera, de 12 de la versión 4 a 8 en la versión 6, renombrando algunos campos de la versión anterior.

Figura 3.Encabezado IPv6.
Fuente: *Mejía (2011)*

Según Mejía (2011), en la figura 2 mostramos el esquema del encabezado del protocolo IPv6.

- Longitud de carga útil: denominado en la anterior versión como longitud total, contiene la longitud total de los datos, consta de 16 bits de la cabecera.
- Siguiente cabecera: denominado en la versión anterior como protocolo, está compuesto por 8 bits y maneja cadenas consecutivas, con el fin de evitar las cabeceras de tamaño variable, de esta forma se logra eliminar el campo opciones.
- Tiempo de saltos: denominado en la anterior versión como tiempo de vida, está compuesto por 8 bits e indica el tiempo de vida que tendrá el datagrama, representado por el número de numero de saltos.

Según Mejía (2011), como campos novedosos frente a la antigua versión se tienen:

- Clase de tráfico: compuesto por 8 bits, con similares características en la cabecera de la versión 4 denominado tipo de servicio, con la diferencia que para la nueva versión este campo esta siempre habilitado para su revisión.

- Etiqueta de flujo: compuesto por 20 bits, utilizado para servicios que tengan como necesidad un mayor enfoque en las características de tiempo real.
- Versión: Indica la versión del protocolo, para este caso 6.
- Los campos de origen y destino cuentan con 128 bits cada uno.

2.1.2.3 Direccionamiento en el protocolo de internet versión 6

La versión 6 del protocolo de internet, define 5 tipos de direcciones.

Según Hinden y Deering (2006), las direcciones son especificadas según su peso ordenado por los bits de orden superior, como lo muestra la tabla 3.

Tabla 4. Tipos de direcciones IPv6

Tipo de dirección	Prefijo Binario	Notación IPv6	Sección
Sin especificar	00...0 (128 bits)	::/128	2.5.2
Loopback	00...1 (128 bits)	::1/128	2.5.3
Multicast	11111111	FF00::/8	2.7
Link-Local Unicast	1111111010	FE80::/10	2.5.6
Global Unicast	(Todo lo demás)		

Fuente: Hinden & Deering, (2006).

2.1.2.3.1 Dirección sin especificar

Según Deering y Hinden (1998), la dirección 00:00:00:00:00:00:00:00, indica que no existe la dirección como tal y por tanto no debe ser colocada en ninguna parte de la red.

Según Deering y Hinden (1998), la dirección no debe ser indicada en el campo destino del encabezado, de esta forma el enrutador no debe recibir esa dirección para ser procesada.

2.1.2.3.2 Dirección Unicast

Según Hinden & Deering (2006), las direcciones Unicast son compuestas por las direcciones global Unicast, site-to-site Unicast y link-local Unicast, entre otras.

Según Deering y Hinden (1998), este grupo de direcciones están las utilizadas por un propósito en específico, como por ejemplo las direcciones IPv6 que se componen con la integración de las direcciones IPv4.

Según Deering y Hinden (1998), estas direcciones pueden ser utilizadas para temas de variabilidad en sus mascarás, similar a CIDR (Classless Inter-Domain Routing) para IPv4.

2.1.2.3.3 Direcciones Loopback

Según Hinden y Deering (2006), la dirección 00:00:00:00:00:00:00:01 es denominada como dirección Unicast Loopback, es una dirección que puede ser vinculada con una interfaz virtual, mas no con una interfaz física. Tiene la característica de poder reenviarse paquetes así misma. Y es denomina interfaz de bucle interno.

Si el enrutador recibe está red, no la agregará en su tabla de rutas y procederá a eliminarla; por eso debe utilizarse solo como una interfaz de nombramiento o identificación.

2.1.2.3.4 Dirección Global Unicast

La figura 3 muestra el esquema del formato de la dirección global Unicast IPv6.

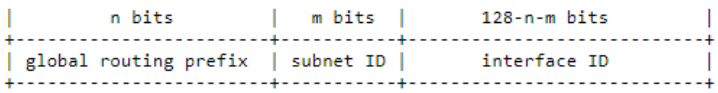


Figura 4. Formato de dirección IPv6 gobal Unicast
Fuente: *Deering & Hinden, (1998)*

Según Hinden y Deering (2006), este tipo de direcciones, se componen por tres campos para su identificación, el primer campo denominado prefijo de enrutamiento global está definido para un sitio que puede contener un grupo de subredes y/o enlaces. El campo de ID de subred actúa como el identificador del enlace dentro de la organización. Finalmente, el ID de interfaz es utilizada para nombrar la interfaz del enlace.

Su equivalente en la red, serían las IPv4 publicas ya que son las enrutables en todo internet.

2.1.2.3.5 Dirección Multicast

Las direcciones Multicast IPv6 tienen el formato como se muestra en la figura 4.

Figura 5. Formato de dirección IPv6 Multicast.
Fuente: *Hinden & Deering, (2006)*

Según Hinden y Deering (2006), esta dirección cuenta con 4 campos que componen los 128 bits de toda la dirección.

Según Hinden y Deering (2006), los 8 primeros bits en 1, definen a la dirección como una dirección Multicast. Es utilizada para distinguir a un grupo de interfaces dentro de los diferentes nodos que componen la red.

Según Hinden y Deering (2006), de esta forma, cuando se recibe un paquete que fue enviado con una dirección Multicast, ese paquete será recibido por las interfaces que sean identificadas con esa dirección.

2.1.2.3.6 Dirección Anycast

Según Deering y Hinden (1998), en este tipo de direcciones se identifican a un conjunto de interfaces que son parte de diferentes nodos, pero pertenecientes a una misma organización.

Según Deering y Hinden (1998), estas direcciones obtienen la dirección Anycast de tal forma que cuando el paquete tiene que ser enviado, utilizará como salida la interfaz más cercana basándose en parámetros de protocolos de enrutamiento. También indica que, al recibir la dirección de unidifusión en más de una interfaz, se convierte automáticamente en una dirección Anycast.

Según Deering y Hinden (1998), como uso común de este tipo de direcciones, está la distinción dentro de un proveedor de servicios de internet o cualquier organización ya que los router serán identificados con esa dirección para poder ser diferenciados entre sí.

2.1.3 Protocolos de enrutamiento IPv4 e IPv6

Los protocolos de enrutamiento presentes para IPv4 están disponibles para IPv6.

A continuación, mostramos la tabla 4, la cual muestra los protocolos de enrutamiento disponibles para cada versión:

Tabla 5. Protocolos de enrutamiento IPv4 e IPv6

Protocolos de enrutamiento		
Protocolo de Internet	**Interno**	**Externo**
IPv4	RIPv1 RIPv2 IGRP EIGRP IS-IS OSPF	BGP
IPv6	RIPng EIGRP IPv6 IS-IS IPv6 OSPFv3	BGP-4 MultIProtocol Extensions (BGP - MP)

Fuente: Elaboración Propia.

2.2 Protocolos de Enrutamiento

2.2.1 Protocolos de enrutamiento internos

2.2.1.1 OSPF

2.2.1.1.1 Definición

Según Malik, Srinivasan, Khan, y Wang (2012), el protocolo abierto de enlaces por sus siglas en ingles OSPF, es un protocolo de enrutamiento que se caracteriza por compartir la información de sus tablas de enrutamiento entre los router pertenecientes a un mismo sistema autónomo. OSPF divide toda la red en áreas interconectadas entre sí y tiene como característica principal ser un protocolo de enrutamiento complaciente ante eventualidades.

Una ilustración general del protocolo OSPF se muestra en la figura 5.

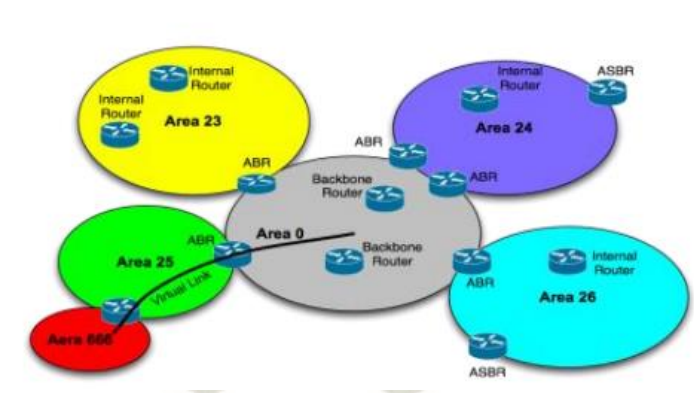


Figura 6. Áreas y routers de OSPF.
Fuente: *Malik, Srinivasan, Khan, & Wang (2012)*

Según Malik, Srinivasan, Khan, y Wang (2012), las áreas que son parte del protocolo de enrutamiento OSPF, están constituidas por un número determinado de segmentos, los cuales representan los router que se conectan con otros por medio de un medio o canal de comunicación.

Según Moy (1998), a este protocolo de enrutamiento, se le conoce como un protocolo de enrutamiento interno, por tener la capacidad de responder ante cambios de topología suscitados, sin que en esto exista un consumo considerable en el tráfico de enrutamiento. Basando su funcionamiento en el estado de enlace entre los router conectados; enviando tablas de rutas entre los router correspondientes a un mismo sistema autónomo. Soporta CIDR, así como el etiquetado de información que será enviada de forma externa, cuenta con autenticación para su implementación entre los enlaces y mensajes de multidifusión que permiten estar al tanto de los estados de los enlaces de todo el sistema que compone la red con OSPF, enviando y recibiendo la información de la misma.

Según Moy (1998), el protocolo de enrutamiento denominado OSPF, es un protocolo de enrutamiento utilizado dentro del dominio de un sistema autónomo, es decir, es un protocolo de enrutamiento interno, por no compartir rutas ni información con otros sistemas autónomos. Se basa en la administración de rutas por medio de diferentes áreas que componen todo el diseño de la red OSPF y actúa frente a cambios originados en la red, permaneciendo de esta forma la fluidez del tráfico dentro de la red, sin que esto signifique que el funcionamiento de este protocolo utilice muchos recursos para poder enviar la información actualizada de sus rutas y los estados de enlace que los componen.

2.2.1.1.2 Estado de Enlace

Según CISCO (2005), en el protocolo de enrutamiento OSPF la interconexión existente entre los router es conocida como enlace. Los router tendrán la cantidad de enlaces, como enrutadores conectados a sus interfaces. De esa forma, envían información sobre los enlaces como la dirección IP, la máscara, el tipo de red, entre otros. Toda esa información es conocida como estado del enlace y la información recopilada por los

router formara una base de datos de los estados de enlace, por ello al protocolo OSPF se le conoce como un protocolo de estado de enlace.

El protocolo de enrutamiento OSPF trabaja con la información enviada por los router sobre los enlaces contiguos que tiene cada uno. La información enviada posee datos como la dirección IP, el tipo de red conectada, el estado del enlace para verificar si está activo o no, entre otros. Con esta información recopilada los router son capaces de poder tomar decisiones sobre la red.

2.2.1.1.3 Costo

Según CISCO (2005), el costo en el protocolo de enrutamiento OSPF es el valor indicativo de la capacidad de enlace que se posee, siendo este valor inversamente proporcional a la capacidad del enlace presentada. Al costo de la interfaz, se le conoce como métrica.

Para determinar el costo de una interfaz se utiliza la siguiente formula:

$$costo = \frac{100000000}{Ancho\ de\ banda\ (bps)}$$

El costo trabaja como un valor de cada interfaz, dependiendo la capacidad de la misma, esto con el fin de poder determinar mejores caminos para el tráfico que pasa sobre la red que utiliza OSPF como protocolo de enrutamiento.

2.2.1.1.4 Enlaces Virtuales

Según CISCO (2005), los enlaces virtuales existentes dentro del protocolo de enrutamiento OSPF, cumplen dos funciones principales. Unir virtualmente un área separada físicamente del área principal o backbone, para conseguir que todas las áreas estén interconectadas al área backbone.

Según CISCO (2005), de ocurrir alguna incidencia en el área principal, este enlace virtual pueda actuar como interconexión para unir las áreas al área principal de respaldo. Ya que, en el protocolo de enrutamiento OSPF todas las áreas deben estar interconectadas al área principal o área backbone, existe la posibilidad de tener un área alejada físicamente al área principal, por lo que se recurre a un enlace virtual para poder realizar la interconexión.

2.2.1.1.5 Características

Según Moy (1998), las principales características del protocolo de enrutamiento OSPF son:

- Alto nivel de redundancia a partir de tiempos mínimos de respuesta ante sucesos imprevistos en la red.
- Soporte de redes CIDR.
- Posibilidad de habilitar autenticación entre los vecinos brindando un nivel más de seguridad
- Con el manejo de áreas dentro del protocolo, se reduce el procesamiento en los dispositivos y no utiliza grandes recursos de ancho de banda para sus actualizaciones, manteniendo las actualizaciones de rutas por áreas.

Según Moy (1998), para poder mantener una interoperabilidad con protocolos de enrutamiento externo, permite la importación de rutas aprendidas por BGP para poder publicarlas sobre sus áreas o según convenga.

2.2.1.1.6 Áreas

Según Moy (1998), para tener un mejor manejo sobre la red y mejorar los niveles de procesamiento al utilizar este protocolo, OSPF trabaja por medio de áreas, permitiendo

dividir el procesamiento y las tablas de rutas por medio de áreas definidas. OSPF define sus áreas de la siguiente manera.

2.2.1.1.7 Backbone

Según Moy (1998), el área principal conocida como área backbone, es el área de la red en la cual se recibe toda la información de las áreas colindantes y se encarga de repartir esta información de ruteo a las otras áreas que no son backbone. Se caracteriza por tener como número de ID el valor 0.0.0.0 del área y por tener los ruteadores de las otras áreas conectados directamente como se muestra en la figura 6.

Según Moy (1998), estos ruteadores pueden estar conectados de forma física o por medio de un enlace virtual, el caso del enlace virtual se da cuando la conexión al área backbone no se puede hacer de forma directa y se utiliza un área que si este conectada directamente al área backbone como medio para poder realizar el enlace virtual. Este enlace virtual dentro del protocolo de enrutamiento es tomado como si fuese un enlace directo punto a punto.

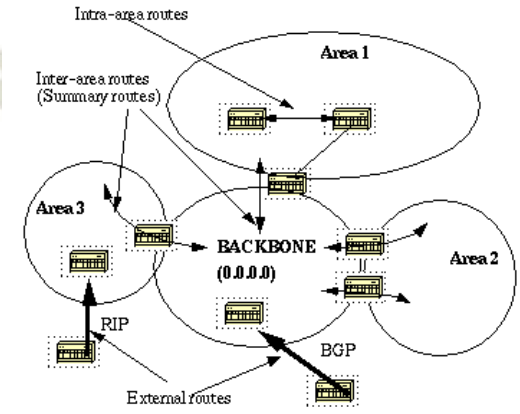


Figura 7. Áreas de OSPF.
Fuente: *CISCO,(2005)*

2.2.1.1.8 Inter-Área

Según Moy (1998), cuando la comunicación se va dar entre dos áreas no troncales el router del área da la información de rutas para poder llegar a su destino, normalmente

utiliza el camino más próximo para mandar el paquete al área backbone y esta área lo redirecciona al destino, ya que el área backbone posee la información de todas las rutas. Cuando un área no está conectada directamente al área backbone se utilizan los enlaces virtuales para poder hacer la conexión virtual y siga el mismo proceso.

Según Moy (1998), los router de las inter-área reciben rutas sumarias de los ruteadores de borde para simplificar procesos y no generar carga en todos los enrutadores, la ubicación de esta área puede visualizarse en la figura 6 mostrada anteriormente.

Las inter-área, son áreas interconectadas al área troncal y se caracterizan por recibir suma acumulada de rutas del router de área backbone para reducir la tabla de rutas y el procesamiento en todos los router.

2.2.1.1.9 Tipos de Router

2.2.1.1.9.1 Router interno

Según Moy (1998), son los router dentro de un área y que sirven como punto limítrofe entre áreas, a estos router se les denomina router internos.

2.2.1.1.9.2 Router de borde de área

Según Moy (1998), los router que están conectados a más de un área, se les denomina router de borde de área. Estos router recopilan información de sus áreas y las envían al área backbone para que el área backbone pueda distribuir toda la información a las otras áreas. Poseen varias copias en su memoria sobre la base de estado de enlace definidas para cada área.

Según Moy (1998), los router conectados a más de un área poseen información sobre sus áreas conectadas y son enviadas al router de backbone para que pueda ser distribuida, estos son los que conectan normalmente a los router internos y les permiten la salida a otras áreas.

2.2.1.1.9.3 Router Backbone

Según Moy (1998), son los router que colindan con varias áreas, pero además poseen una interfaz directa al área backbone.

2.2.1.1.9.4 Router de límite de sistema autónomo

Según Moy (1998), los router de límite de sistema autónomo, son ajenos a un lineamiento mencionado anteriormente, estos router pueden estar en cualquier posición dentro de las diferentes áreas de la red OSPF, pueden estar como router de área, internos y pueden o no participar del área backbone de la red, su principal característica es que comparte rutas con los router de otros sistemas autónomos, intercambiando información de rutas entre sí, de esta forma los router de borde de sistema autónomo intercambian rutas con sus pares.

Los router de límite de sistema autónomo, son los que tienen como punto extremo el router de otro sistema autónomo, comparten sus rutas con los sus vecinos de otros sistemas autónomos y normalmente corren más de un protocolo de enrutamiento, como por ejemplo BGP y la información aprendida de esos router, son enviadas a los router de backbone para compartir esa información con los otros dispositivos que componen la red OSPF.

2.2.1.1.10 OSPv3

Con la llegada de IPv6 se hizo necesaria la evolución de los protocolos de enrutamiento que trabajan sobre IPv4.

Para el caso del protocolo de enrutamiento OSPF, su versión disponible para IPv6 fue denominado OSPFv3 y esta descrito en el RFC 5340[2].

[2] RFC 5340: datatracker.ietf.org/doc/html/rfc5340

Según Jian y Fang (2011), la forma de trabajo de OSPFv3 varia levemente con la forma de trabajo de OSPFv2 de IPv4. Ya que en esta nueva versión tiene que tratar IPs de mayor longitud y cabeceras diferentes. Por ello la lógica de funcionamiento es la misma exceptuando algunas características específicas de OSPFv3 explicadas a continuación.

Según Jian y Fang (2011), los cambios establecidos en OSPFv3 con respecto a OSPFv2 son los siguientes:

- El manejo del protocolo no se realiza sobre la subred de los router como sucede con OSPFv2, la interfaz de interconexión es la encargada de establecer las adyacencias entre vecinos.
- Tiene la posibilidad de implementar sobre un solo enlace múltiples instancias lo cual no ocurre directamente con OSPFv2.
- Para poder identificar a los vecinos OSPFv3 utiliza las direcciones link-local de cada router sobre la interfaz y en los mensajes LSA se incorpora la información de esa dirección link-local para enviarla a los vecinos y no se produce él envió de esa información entre los otros enrutadores.
- Los paquetes de LSA no contienen información de IPv6.
- Los router designados y los router de respaldo designados ya no son elegidos en base a la asignación de IPs, sino que la selección se basa solo en los valores del router ID.
- Como comparativa los encabezados de los paquetes IPv6 presentan una longitud de 16 bits frente a los 32 bits que representan los encabezados de IPv4 en OSPFv2.

- La autenticación presentada en OSPFv2 ha sido reemplazada por mecanismos de autenticación de cabecera y encapsulado de carga útil más conocido como ESP.

Los paquetes utilizados para establecer las sesiones en IPv6 son los mismos que en OSPFv2: Hello, Data base Description, Link State Request, Link State Update, Link State Acknowledgement.

2.2.2 Protocolos de enrutamiento externo

2.2.2.1 BGP

2.2.2.1.1 Definición

Según Rekhter, Li y Hares (2006), dentro de los protocolos de enrutamiento externo, se encuentra el protocolo de puerta de enlace de frontera (BGP), este protocolo se caracteriza por el intercambio de información existente con otras redes que comparten información a través de BGP. Como resultado se obtiene la información de rutas existentes de cada sistema autónomo (AS), que comparten sus rutas con BGP.

Según Rekhter, Li y Hares (2006), haciendo uso de la información obtenida de BGP es posible plasmar un diagrama de conectividad de los diferentes AS con el objetivo de realizar políticas de ruteo con los AS y hace posible la eliminación de bucles a nivel de enrutamiento que puedan existir.

Según Rekhter, Li y Hares (2006), este protocolo de enrutamiento maneja información de ruteo de los AS que intercambien información con BGP, validando información obtenida en la dirección destino del encabezado IP. De esa forma, si se desea llegar a un destino por un AS diferente al que figura en la tabla de ruteo obtenida por BGP, no podrá realizarse ya que solo se tiene control sobre el primer salto en la tabla de rutas.

Según Rekhter, Li y Hares (2006), BGP permite publicar redes eliminando el concepto de clases, ya que tolera mecanismos como el enrutamiento entre dominios sin clases (CIDR), la sumarización de redes y agregación de rutas de AS.

La figura 7 muestra los caminos que tienen los diferentes AS para llegar a su destino, ilustrando de esa manera el funcionamiento del vector distancia de BGP

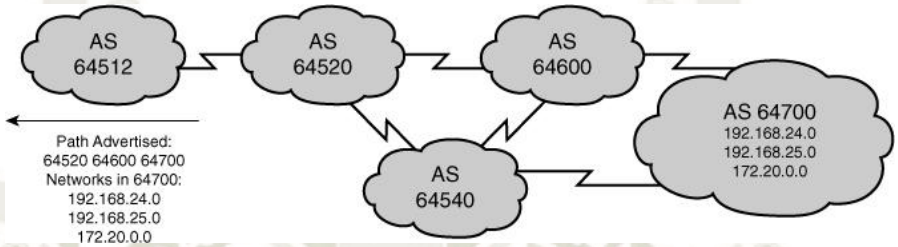


Figura 8. Vector distancia BGP.
Fuente: *Long (2007)*

Según Long (2007), a diferencia de los protocolos de enrutamiento interno donde la información anunciada a sus pares son métricas y redes publicadas, en BGP como protocolo de enrutamiento externo intercambia información de accesibilidad de red, denominada vector distancia. El vector distancia lleva información de los AS necesarios para poder llegar a un destino determinado.

Según Long (2007), en la figura 7 se observa el AS origen con número 64512 y el AS destino 64700 con las redes destino:

- 192.168.24.0
- 192.168.25.0
- 172.20.0.0

El vector distancia indica los siguientes caminos para llegar al AS 6470:

- 64512-64520-64600-64700
- 64512-64520-64600-64540-64700
- 64512-64520-64540-64600-64700

- 64512-64530-64540-64550-64700

Según Long (2007), siendo estas, solo algunas de las posibilidades existentes para poder llegar al AS destino, existiendo otras opciones basadas en la gráfica. Como protocolo de enrutamiento externo, BGP se encarga de compartir información de los diferentes AS que componen la red de internet. Este es el protocolo de enrutamiento utilizado por los proveedores de internet, así como de los proveedores de contenido para poder compartir su información de rutas.

Según Long (2007), con la finalidad de facilitar la tabla de rutas recibida en los enrutadores, realizan un diagrama de los diferentes AS para poder llegar a un destino determinado.

Con ayuda de los parámetros obtenidos de los vectores distancia de BGP pueden aplicarse políticas de ruteo dentro del AS mediante el uso de atributos dirigidos a los AS subyacentes, para poder influenciar en él tráfico y de esta forma permite evitar bucles de ruteo.

2.2.2.1.2 Características de BGP

Según Long (2007), las características del protocolo de puerta de enlace de frontera (BGP) son:

- Utiliza una conexión de protocolo TCP con el puerto 179, aprovechando la característica de TCP al ser un protocolo orientado a la conexión, así BGP no requiere un sistema independiente de retransmisión de datos ante eventualidades.
- Los enrutadores de borde dentro de un AS son los encargados de establecer la sesión BGP, 2 enrutadores de AS diferentes son denominados pares BGP o vecino BGP.

- Con la sesión BGP establecida entre los enrutadores, permite el intercambio de rutas entre ambos pares, una vez compartidas sus rutas, las actualizaciones de las rutas se hacen por medio del envió de cambios en las rutas de cada AS, sin la necesidad de reenviar la tabla en su totalidad. Utiliza mensajes de keepalive para confirmar que la sesión entre los pares siga activa.
- BGP envía los paquetes a su destino sin detenerse por cada octeto de datos enviado, como sucede con otros protocolos como OSPF. Esto se da gracias a que el protocolo TCP envía desde el receptor el acuse de recibo en la mitad de los octetos enviados, sin tener que esperar a que se reciban todos los octetos.

2.2.2.1.3 Características del vector distancia de BGP

Según Long (2007), algunas de las características del vector distancia BGP son:

- La información adquirida de las rutas de los sistemas autónomos sirve para hacer una visualización de la topología de los AS, garantizando que las rutas hacia los destinos estén libres de bucles y poder aplicar políticas de ruteo en base a esa información.
- Pensado en grandes redes como internet, BGP cumple con las especificaciones para ser desplegado a gran escala.
- Las políticas de ruteo aplicadas en BGP se aplican directamente sobre el AS, de esta forma permite influir en el tráfico pasante por esas redes afectadas por el AS. Estas políticas pueden ser aplicadas para un bloque CIDR o para redes independientes publicadas por BGP, para que puedan ser tratadas independientemente entre los AS vecinos.

- El manejo de atributos para influir en el tráfico hacia los AS vecinos solo tendrá influencia en este primer salto, ya que no se tiene control sobre el manejo de las rutas en el siguiente AS, BGP incluye políticas de ruteo de salto a salto entre los vecinos adyacentes.
- BGP admite políticas basadas en paradigma de ruteo de salto a salto y ya que las redes de internet se mueven bajo este concepto, lo hace aplicable y escalable en el desarrollo de este.

2.2.2.2 Tipos

Según Long (2007), el protocolo de puerta de enlace (BGP) puede ser usado para enrutar redes de sistemas autónomos diferentes (eBGP) y como enrutamiento dentro de un mismo sistema autónomo (iBGP)

2.2.2.2.1 eBGP

Según Long (2007), el protocolo eBGP intercambia información de redes entre diferentes AS. Tiene un valor de 20 como distancia de ruta predefinido.

Según Long (2007), dentro del AS, el intercambio de información de ruteo se da mediante un protocolo de enrutamiento interno (IGP).

La figura 8 ilustra el concepto de eBGP.

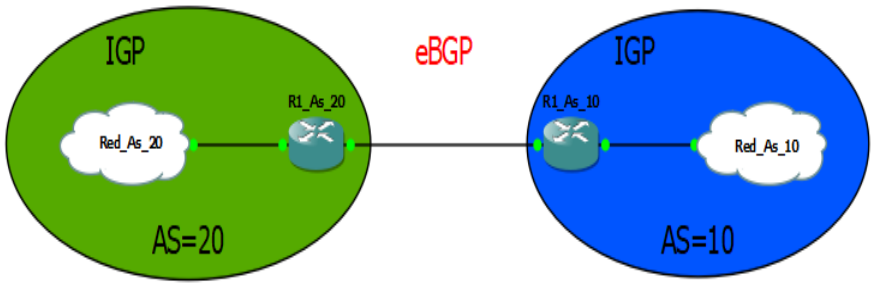


Figura 9. Topología eBGP.
Fuente: Elaboración propia.

2.2.2.2.1.1 Requerimientos para establecer la sesión eBGP

Según Long (2007), existen varios requisitos para establecer la sesión eBGP entre sus pares. Se mencionan a continuación algunos:

- Para que la sesión eBGP pueda establecerse, es necesario que los vecinos o pares pertenezcan a un AS diferente, es decir, que tengan un número diferente de sistema autónomo.
- Previo a establecerse la sesión eBGP, el protocolo TCP debe establecer una sesión con su vecino, para que después la sesión eBGP sea establecida. Mientas no esté establecida la sesión TCP entre los equipos, eBGP no compartirá información de rutas.
- Los enrutadores a nivel de IP deben ser alcanzables entre sí para que se pueda establecer la sesión entre los pares.

2.2.2.2.2 iBGP

Según Long (2007), el enrutamiento realizado dentro de enrutadores de un AS con el protocolo BGP, se denomina iBGP. Tiene como distancia de ruta 200.

En la figura 9 se presenta una topología básica de implementación con iBGP.

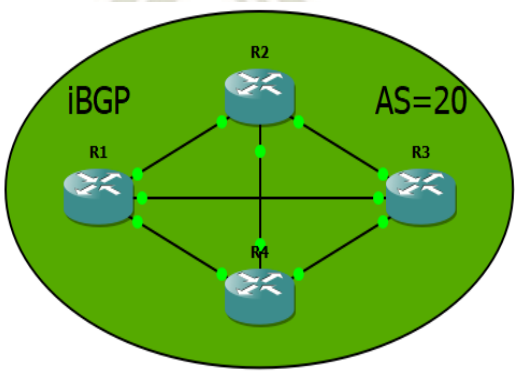


Figura 10. Topología iBGP.
Fuente: Elaboración propia.

2.2.2.2.2.1 Requerimientos para establecer la sesión iBGP

Según Long (2007), existen varios requisitos para establecer la sesión iBGP entre sus pares. Se mencionan a continuación algunas:

- La sesión iBGP deberá establecerse entre enrutadores pertenecientes a un mismo AS.
- Previo a establecerse la sesión iBGP, el protocolo TCP debe establecer una sesión con su vecino, para que después la sesión iBGP sea establecida. Mientras no esté establecida la sesión TCP entre los equipos, iBGP no compartirá información de rutas.
- Dentro del AS los enrutadores que establezcan la sesión deben ser alcanzables entre sí a nivel de IP.

2.2.2.3 Detector de Colisiones

Según Long (2007), el protocolo de puerta de enlace de frontera (BGP), presenta como una de sus características principales un camino de rutas entre sistemas autónomos de origen a destino libre de bucles en todo el trayecto. Una vez que los enrutadores reciben la información de las rutas de sus vecinos, no reciben nueva información de rutas que contengan su mismo sistema autónomo en la actualización de la tabla de rutas existente.

Según Long (2007), con la información recopilada se crea un diagrama de los AS la cual no contiene bucles y ayuda a crear políticas de ruteo basadas en las rutas destino y el vector distancia del AS.

El protocolo BGP bosqueja una idea de la topología de saltos de ruta para poder llegar a su red destino, es decir, indica a través de que AS es posible llegar a esa red destino. Gracias a esto, BGP permite mantener la información de enrutamiento libre de bucles que puedan ocasionar problemas de enrutamiento y permite el manejo de atributos

para influenciar el tráfico de la red del AS origen, pero este manejo solo se mantiene en el primer salto de BGP entre el AS origen y los AS vecinos, en los demás AS no tendrá el manejo de rutas destino.

2.2.2.4 BGP -MP

Según Bates, Chandra, Katz, y Rekhter (2007), a diferencia de otros protocolos de enrutamientos, como OSPF tratado con anterioridad, en el que se crea una nueva versión para poder manejar enrutamiento con IPv6. En BGP no sucede lo mismo, ya que es sobre el mismo protocolo existente donde se utiliza la nueva versión de IP.

Según Bates, Chandra, Katz, y Rekhter (2007), BGP para manejar el enrutamiento de IPv6 se basa en la extensión de BGP denominada BGP-4 MultiProtocol Extensión (BGP – MP).

Según Bates, Chandra, Katz, y Rekhter (2007), esta versión no fue pensada solo para la utilización en IPv6 ya que su uso se basa en diferentes familias de direcciones como Multicast, Unicast, vpn4, etc.

Según Bates, Chandra, Katz, y Rekhter (2007), el manejo y selección del protocolo para poder utilizar los diferentes tipos de familia se basa en el manejo de los parámetros AFI (Address Family Indicator) y SAFI (Subsequent Address Family). Con estos parámetros podemos definir si se realizara con direcciones IPv4 o IPv6, del tipo Unicast o Multicast.

Según Cicileo (2017), la extensión del protocolo BGP admite la utilización de diferentes familias de direcciones IP utilizando los identificadores AFI y SAFI de la siguiente manera:

AFI= 1 para IPv4

AFI= 2 para IPv6

SAFI= 1 para Unicast

SAFI= 2 para Multicast

Según Cicileo (2017), la asignación del router ID viene dada a través de la dirección loopback con una longitud de 32 bits. El uso de transporte del tráfico IPv4 o IPv6 puede realizarse a través de las sesiones TCP tanto de IPv4 como para IPv6.

Según Cicileo (2017), indica que se recomienda el uso separado de sesiones para cada tipo de AFI utilizado en el enrutador y de esa forma mantener los tráficos separados. Finalmente recomienda no establecer sesiones BGP con vecinos sobre direcciones Link-local.

Según Cicileo (2017), para un uso del protocolo en su versión multiprotocolo, indica que la necesidad de levantar sesiones independientes de IPv4 e IPv6 no es necesaria ya que el siguiente salto es inalterado, pero ante una eventual caída de esa sesión ambos tráficos se verán perjudicados, por lo que es recomendado también levantar sesiones independientes, tanto en iBGP como eBGP.

2.2.2.5 Seguridad y validadores de rutas

2.2.2.5.1 RPKI

Según Lepinski y Kent (2012), como parte de la implementación de sistemas de seguridad que acompañen a la publicación de prefijos por medio de BGP. Se crearon los RPKI (An Infrastructure to Support Secure Internet Routing)

Según Vega, Rocha y Cicileo (2021), los RPKI son una base de datos que contienen los prefijos disponibles por cada ASN, validados por un ROA y los RIR brindan la autenticación de estos prefijos por medio de esos certificados.

Según Vega, Rocha y Cicileo (2021), esta base de datos se incluirá en las tablas de rutas de los router, para poder establecer la tabla de rutas final en base a la comparativa de los datos del RPKI con los prefijos recibidos a través de BGP. La mayoría de las marcas cuentan con la posibilidad de agregar en sus router el acceso a esta base de datos para definir las tablas de rutas publicadas por BGP.

Según Vega, Rocha y Cicileo (2021), para hacer uso de este validador, los enrutadores deben permitir en sus versiones la conexión con estas bases de datos, para finalmente realizar una tabla de rutas en función a una comparativa de los prefijos recibidos por BGP y la base de datos obtenida por medio de RPKI.

2.2.2.5.2 ROA

Según Vega, Rocha y Cicileo (2021), como parte inicial del proceso de implementación de RPKI, los titulares de recursos IP y de ASN deben registrar en sus respectivos RIR un certificado en el cual confirmen el uso y manejo de los recursos estipulados con su número de AS.

Según Vega, Rocha y Cicileo (2021), estos certificados digitales son denominados ROA (Route Origination Authorization). Los ROA son un apoyo de verificación por medio de una firma digital que tienen las siguientes características.

- Tiene similitud con los route o route6 entregado por los IRR.
- La autorización puede ser de forma selectiva para los dueños de los recursos, seleccionando los prefijos que anunciaran.
- Validan un ASN por cada prefijo publicado en internet.
- La información recolectada es publicada en base de datos públicas.
- Contienen certificados digitales por medio de sus firmas.

2.3 Recursos Públicos

Internet es conocido como la interconexión de redes a nivel mundial, por ello cada integrante debe poseer recursos únicos que garanticen la interconexión entre las demás redes. Estos recursos son entregados por los RIR de cada localidad a cada participante, en esta sección se desarrollará el concepto y tipo de recursos entregados.

2.3.1 Registros Regionales de Internet

Según Lacnic (2020), una de las prioridades relacionadas al avance tecnológico que tienen los países, es realizar una adecuada distribución de los recursos de internet, la distribución de recursos está a cargo de los registros regionales de internet (RIRs), estos últimos se crean y son habilitados para su funcionamiento por cada comunidad regional, pero los RIRs deben cumplir con ciertas exigencias dadas por el IANA, quien le va a dar dicho reconocimiento para que represente de manera oficial a cada región.

Según Lacnic (2020), el IANA estableció la creación de 5 RIRs, los que se encargaran del manejo y distribución de los recursos de internet.

- American Registry for Internet Numbers (ARIN) para Estados Unidos y Canadá.
- RIPE Network Coordination Centre (RIPE) para Europa, Oriente medio y Asia Central.
- Asia-Pacific Network Information Centre (APCNIC) para Asía y Región Pacífica.
- Latin American and Caribbean Internet Address Registry (LACNIC) para América Latina y el Caribe.

- African Network Information Center (AfriNIC) para África.

Cada RIR está encargado de hacer la distribución, manejo y control de recursos IP, así como los números de sistemas autónomos dentro de sus regiones.

2.3.2 Sistema Autónomo

Según Lacnic (2020), al sistema autónomo (AS) se le conoce como el conjunto de dispositivos que componen una red IP en particular, estructurada con políticas de ruteo únicas manejadas por uno o más operadores de red. Cada una de estas es identificada con un número individual, el cual tiene como objetivo servir como identificador en el cambio de rutas a nivel exterior con otros AS.

Según Lacnic (2020), indica que un conjunto de redes que basan sus políticas de ruteo de forma diferente, son necesarias las implementaciones de más de un sistema autónomo, y si dentro de varios conjuntos de redes la política es la misma, deberá contar con solo un AS para todas las redes, esto se definió ya que se suele considerar que un grupo de redes que comparte una misma gestión y no políticas debe ser considerada como un solo sistema autónomo.

La interconexión de los diferentes AS hace posible la comunicación global y genera el concepto de Internet, de esta forma internet es conocido como una gran interconexión de redes. Toda entidad que desee participar en este proceso, debe contar con los recursos adecuados de IP y ASN.

Según Lacnic (2020), la asignación de números para cada sistema autónomo está establecida en los RFC 1930[3] y RFC 4893[4] para la asignación de 16 bits y 32 bits respectivamente. Para el primer caso de 16 bits, el sistema autónomo tendrá la asignación

[3] RFC 1930: datatracker.ietf.org/doc/html/rfc1930
[4] RFC 4893: datatracker.ietf.org/doc/html/rfc4893

de un número decimal en el rango entre el 0 y 65535 y para el caso de 32 bits tendrá la asignación del número decimal del rango entre 0 y 4294967295. Tanto para los números de sistemas autónomos de 32 y 16 bits, deben estar representados con la notación decimal entera conocida como “asplain” definida en el RFC 5396[5].

2.3.2.1 Requisitos para la asignación de ASN

Según Lacnic (2020), la entrega de recursos públicos por parte de Lacnic estará disponible para las organizaciones que cumplan con:

- Un plan de conexión no mayor a seis meses con otras organizaciones que también posean recursos públicos, de sobrepasar este tiempo establecido, Lacnic procederá con la designación de esos recursos a otra organización que si cumpla con lo establecido.
- La organización solicitante del recurso deberá presentar a Lacnic el desarrollo de su plan de ejecución de enrutamiento para la interconexión del ASN entregado e indicar los prefijos que publicará bajo el dominio de ese ASN.
- La actualización de la información estará a cargo del solicitante en los sistemas de información de Lacnic como WHOIS.

2.4 Proveedores de Servicio de Internet

Según Texeira y Rexford (2006), el internet está compuesto por un gran número de miembros poseedores de sus propios recursos públicos tales como ASN y direcciones IP interconectados entre sí, muchos de estos miembros son los proveedores de servicio de internet (ISP).

[5] RFC:5396: datatracker.ietf.org/doc/html/rfc5396

Según Texeira y Rexford (2006), la conexión de un cliente a un servicio, va depender de la interconexión que tenga el ISP con otros ISP para poder interconectarse al servicio y del nivel de los ISP al que se conecten para proveer mejoras en el servicio. Esta conexión muchas veces es entre dos localidades diferentes, pasando por un sin número de enlaces pertenecientes a diferentes proveedores, lo que genera un aumento en la tabla de rutas de los equipos y por tanto un aumento en el procesamiento. Se estima un promedio de más de150 000 prefijos de red que contiene un enrutador para poder llegar a cualquier destino de internet, esta cifra contenida en cada enrutador que compromete la interconexión y funcionamiento de la red.

Según Texeira y Rexford (2006), el internet, está constituido por un gran número de redes independientes entre sí que manejan sus propias reglas y políticas de ruteo, intercomunicadas con otras redes.

Según Texeira y Rexford (2006), la masividad de internet genera que los diferentes dueños de las redes obtengan volúmenes de datos de diferentes tamaños, generando una jerarquía según el volumen de tráfico que mueven a nivel mundial, de esta forma se empiezan a catalogar según sus características.

Según Texeira y Rexford (2006), las diferentes redes de internet se comunican a través del protocolo de enrutamiento BGP. Y manejan políticas y reglas independientes entre sí, separadas cada uno por la autonomía de su sistema autónomo. Existe una selección y jerarquización de las redes según como se interconecten con otras redes.

Según Winther (2006), una ilustración común de como confluye el tráfico a través de los grandes proveedores se muestra en la figura 10.

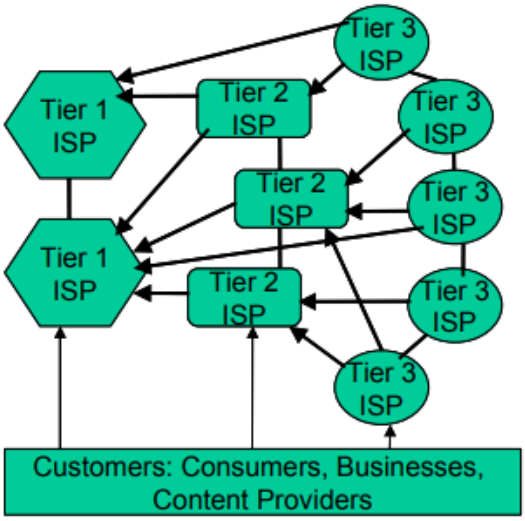


Figura 11. Jerarquia global de internet.
Fuente *Winther (2006)*

Según Winther (2006), los proveedores tier1 o nivel 1 poseen grandes infraestructuras a nivel mundial, de tal forma que otros proveedores de menor tamaño se interconectan a sus redes para poder confluir con las otras redes que conforman internet. Por su tamaño, este tipo de proveedores realiza políticas de emparejamiento gratuito con proveedores de igual tamaño y conexiones de tipo privadas o de tránsito ante proveedores de menores recursos. Esto debido a la gran cantidad del tráfico de internet que mueve en potestad de sus redes.

Según Winther (2006), de esta forma, los proveedores de nivel 2 interconectan las redes de los proveedores de nivel 3 con las del nivel 1. Pero los proveedores de nivel 2 no tienen la magnitud de los de un nivel superior y su punto central no se basa en la distribución de servicio a clientes finales, como sucede con los proveedores de nivel 3.

A continuación, nombramos algunos proveedores de nivel 1:

- AT&T
- Verizon
- NTT
- Level 3

- Turkish Telecom
- Telekom South África
- France Telecom

Y de nivel 2:

- Reach y Singapore Telecom
- STIX
- Internexa

Según Lacnic (2020), los proveedores de servicio de internet son los capacitados para poder brindar a sus usuarios finales recursos de protocolo de internet. Un proveedor de servicio de internet no está limitado por un espacio geográfico, caso contrario a lo que sucede con los registros regionales de internet (RIRs).

2.5 Punto de Intercambio de tráfico

La forma más directa de intercambiar redes entre tres o más participantes es por medio de un punto de intercambio de tráfico.

Según Kioti, Ager, Kotronis, Nomikos y Dimitropoulos (2006), cada participante comparte las redes que desee publicar y recibe las redes de los otros participantes sin tener que pasar por enlaces externos ni alquilar enlaces de terceros para poder hacerlo, con su interconexión al punto de intercambio bastará para poder realizarlo.

En la siguiente sección se revisará todo lo concerniente a los puntos de intercambio de tráfico.

2.5.1 Concepto de Punto de intercambio de tráfico

Según Kioti, Ager, Kotronis, Nomikos y Dimitropoulos (2006), los puntos de intercambio de tráfico (IXP), representan la parte central del esqueleto que compone

internet, ya que es ahí donde los proveedores de servicio y proveedores de contenido comparten información entre sí.

Según Cavalcanti (2010), los IXP son componentes físicos donde los proveedores de servicio y los operadores de redes intercambian información entre sí, cada uno de estos agentes identificados con un número de sistemas autónomo (AS), interconectados a un conmutador y enrutadores los cuales son de libre interconexión y de políticas neutrales, estas políticas se remontan desde la época de 1990.

Según Cavalcanti (2010), de esta forma, el tráfico de los miembros es intercambiado entre sí y no requieren de conexiones externas para su interconexión, manteniendo el tráfico de forma local en el IXP.

Según Cavalcanti (2010), los puntos de intercambio de tráfico (IXP), conocidos también por las siglas NAP (Punto de Acceso de Red), son una infraestructura física donde diferentes entidades que componen el ecosistema de internet se interconectan entre sí, para poder intercambiar información de redes. Todos los integrantes deben poseer un ASN e intercambiarán información con los otros integrantes por medio del protocolo de enrutamiento BGP. Esto con el fin de poder reducir costos, latencias y mejorar la performance de sus servicios propuestos a usuarios finales.

2.5.1.1 Reseña

Según Bucke (2016), el nacimiento del punto de intercambio de tráfico (IXP), se remonta entre los años 1987 y 1994 cuando la red de la fundación nacional para la ciencia (NSFNET) tenía el control del núcleo de la red y decide ceder el control y manejo del núcleo de internet al sector privado en el año 1992. Fecha desde la cual y bajo el nuevo manejo del núcleo de internet, dio una nueva perspectiva del cambio que se suscitaba con

esta nuevo manejo económico y comercial, dando origen a tres agentes importantes dentro del nuevo funcionamiento, los cuales fueron:

- Proveedores de servicios de Red (NSP)
- Puntos de acceso a la red (NAP)
- Arbitro de enrutamiento (RA)

Según Bucke (2016), NSP tenía a su cargo las operaciones de red, NAP se encargaba de las interconexiones entre los diferentes puntos geográficos de Estados Unidos, donde se ubicaban las cabeceras de los NSP y el RA actúa como una base de datos del enrutamiento de los NSP la cual es compartida en los NAP, asemejándose al funcionamiento actual que tienen los servidores de rutas.

Según Bucke (2016), el mantenimiento, control y supervisión de los NAP estaban a cargo de las operadoras dominantes en el país, lo que conllevo a un desacuerdo general entre las otras operadoras provocando que estas se salieran de la conexión del NAP, además por el interés de las grandes operadoras de solo conectarse con operadoras de su mismo nivel hizo que las operadoras de niveles inferiores sean rezagadas de este sistema de interconexión, provocando que los NAP ya no sean útiles para su uso y desequilibrando el funcionamiento que se tenía hasta el momento.

Según Bucke (2016), la idea de la interconexión de los grandes operadores no se vio beneficiada por los grandes montos económicos que significaban su implementación, de esa forma la idea de una interconexión libre en un lugar físico neutral se consideró la mejor opción para que, las que operadoras de todo nivel puedan interconectarse y realizar cambio de tráfico entre ellas, de esta forma surgió el concepto actual de punto de intercambio de tráfico con reglas neutrales y beneficiosas para sus miembros.

Según Bucke (2016), los puntos de intercambio de tráfico nacen a raíz de la necesidad de la interconexión de proveedores de servicios de red existentes en la NSFET, el lugar físico donde se interconectaban los diferentes proveedores de servicio se llamó NAP, fueron 4 los NAP existentes en un inicio, los cuales hacían posible la interconexión de la red de internet manejada por NSFET.

Según Bucke (2016), con mayor número de proveedores de servicio y la adopción de un nuevo control del núcleo de internet entregada por la NSFET a entidades privadas, surgió una nueva necesidad del manejo de la interconexión basada en un punto libre, donde los grandes proveedores no implantarán normas y reglas de interconexión, lo cual en un principio provoco un declive en el sistema.

Según Jensen (2012), los puntos de intercambio de tráfico son conocidos por las siglas IXP-IX (Internet Exchange Point), IPP (Internet Peering Point), NAP (Network Access Point) entre otras, la forma en cómo se les nombre a esos puntos de intercambio va variar ya que no existe una regla de nombramiento para este sistema de interconexión.

Según Jensen (2012), la sigla más antigua adaptada fue la de NAP, con la cual fue la forma de interconexión que tuvo la NSFET con sus 4 puntos de intercambio.

Así surge la noción de un punto de intercambio de tráfico neutral, rápido y con prestaciones que beneficiaban a todos los miembros que se conecten a este.

2.5.1.2 Funcionamiento

Por medio del protocolo de enrutamiento BGP, los diferentes miembros que componen el punto de intercambio de tráfico crean políticas de enrutamiento para el intercambio de redes, por medio de infraestructuras de capa 2 o capa 3 con políticas de emparejamiento definidas por el punto de intercambio de tráfico, con el fin de mejorar la performance y obtener beneficios a partir de esos emparejamientos.

2.5.1.3 Modos de Interconexión

Los puntos de intercambio permiten dos políticas de emparejamiento entre sus miembros.

La conexión bilateral y la conexión multilateral. La decisión de que política usar, va ir de acuerdo al enfoque de cada punto de intercambio, basándose en las ventajas que cada una de estas formas de interconexión propongan para el desarrollo del punto de intercambio de tráfico.

2.5.1.3.1 Peering Bilateral

Según Giotsas, Zhou y Luckie (2013), los acuerdos bilaterales son sesiones BGP que se establecen con entre cada uno de los miembros, entre más miembros existan, la cantidad de sesiones aumentará. Dentro de los modelos de intercambio este tipo de acuerdo no es favorecido ya que, el fin de interconectarse a un punto de intercambio de tráfico es poder obtener sesiones con políticas abiertas y con la mayor la cantidad de miembros que fuera posible, sin que esto signifique tener que manejar gran cantidad de sesiones BGP a la par por dispositivo interconectado al IXP.

La interconectividad en una arquitectura de peering bilateral se muestra en la figura 11.

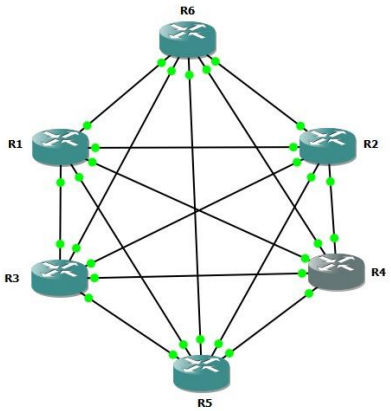


Figura 12. Arquitectura de peering bilateral.
Fuente: Elaboración propia.

Según Giotsas, Zhou y Luckie (2013), el acuerdo de peering bilateral es el establecimiento de sesiones BGP de forma independiente con los múltiples participantes, entre más participantes tenga el IXP, la cantidad de sesiones aumentará. Estas sesiones se realizarán con los equipos de cada participante, no dependen de ningún equipo de otro miembro para poder entablar la sesión.

2.5.1.3.2 Peering Multilateral

Según Giotsas, Zhou y Luckie (2013), el acuerdo de emparejamiento multilateral es la opción escalable de emparejamiento frente a su par bilateral, las sesiones se entablan a través de servidores de rutas que interconectan a todos los miembros y de esa forma los miembros reciben las rutas de todos los demás miembros.

Según Giotsas, Zhou y Luckie (2013), la arquitectura de un emparejamiento multilateral es presentada por la figura 12.

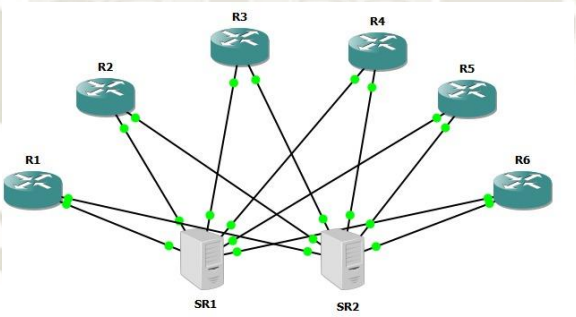


Figura 13. Arquitectura de peering multilateral.
Fuente: Elaboración propia.

Según Schlinker, Zarifis, Cunha, Feamster y Katz-Bassett (2014), la propuesta de un acuerdo multilateral por medio de servidores de rutas son alternativas presentadas por los IXP para facilitar el emparejamiento entre sus miembros.

Según Schlinker, Zarifis, Cunha, Feamster y Katz-Bassett (2014), el emparejamiento multilateral es la forma de realizar sesiones con pares BGP de forma escalable por medio de un servidor de rutas que sirve como concentrador de rutas de todos

los miembros. De esta forma con una sesión es posible recibir las rutas de todos los miembros y manejar las políticas de ruteo desde el enrutador de cada miembro.

2.5.2 Modelos de los Punto de intercambio de tráfico

Según Jensen (2012), existen 2 modelos principales de puntos de intercambio de tráfico.

Según Jensen (2012), el modelo de capa 3 en el cual los miembros del punto de intercambio de tráfico se interconectan a través de un router el cual es brindado por la entidad que maneje el punto de intercambio de tráfico. Este modelo de tráfico no permite un manejo o control de las políticas a los miembros conectados ya que la administración, manejo y control es realizado por la organización que maneja el punto de intercambio de tráfico, es un modelo en el cual los miembros son totalmente dependientes de un tercero.

Según Jensen (2012), el segundo es un modelo de capa 2, donde miembros se interconectan entre sí a través de un conmutador que se encuentra en el espacio físico que compone al punto de intercambio de tráfico y cada miembro posee un propio enrutador para poder establecer las políticas de ruteo que prefieran y teniendo un mayor control sobre estas.

Según Jensen (2012), los IXP modelos de capa 3 normalmente terminan siendo modificados a un IXP de modelo capa 2 ya que a gran escala no pueden ser manejables.

Existe un tercer tipo de punto de intercambio de tráfico de capa 2 y capa 3, existe un tipo de punto de intercambio de tráfico híbrido. Que nace a raíz de la necesidad de manejar un punto de intercambio de tráfico de capa 3 y capa 2 a la vez, esto por elegir el tipo de IXP de forma errada, normalmente los modelos de capa 3 al ser poco manejables a gran escala, tienen que cambiar a un tipo hibrido agregando dispositivos de capa 2 para su interconexión y finalmente migrando por completo al modelo de capa 2.

2.5.2.1 Modelo Capa 2

Según Jensen (2012), en este modelo los miembros pertenecientes al punto de intercambio de tráfico realizan la interconexión por BGP entre cada uno. Dando la posibilidad de poder interconectarse entre los miembros sin la necesidad de usar el IXP o utilizando la infraestructura del IXP.

La arquitectura de un punto de intercambio básico de capa 2 se muestra en la figura 13.

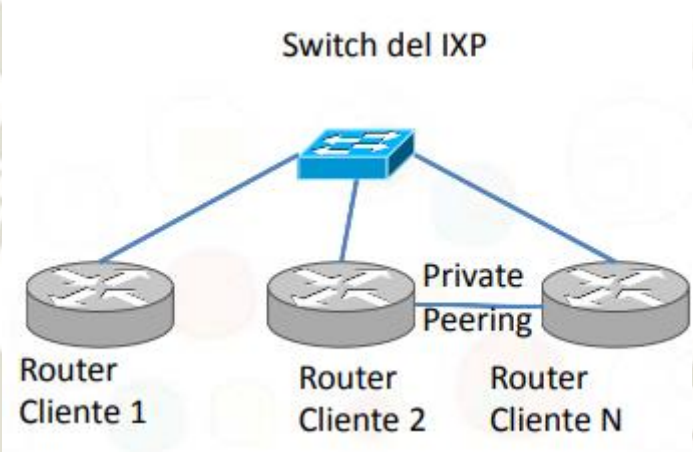


Figura 14. Arquitectura Punto de intercambio de tráfico modelo capa 2.
Fuente: *Cicileo (2016)*

Según el Banco de desarrollo de América Latina (2014), el modo de capa 2 presenta una arquitectura de peering abierto, es caracterizado por presentar una interconexión entre miembros de forma directa, sin tener la necesidad de conectarse a un equipo brindado por el administrador, para poder entablar las sesiones BGP entre los miembros, de esta forma el administrador limita su trabajo a monitoreo de anuncios y a la confirmación de conexión entre los miembros.

Según el Banco de desarrollo de América Latina (2014), los miembros cuentan con un equipo propio para poder realizar los emparejamientos de BGP, así controlan con quienes quieren emparejarse y manejan el control de tráfico entre otros atributos.

Según el Banco de desarrollo de América Latina (2014), este tipo de modelo presenta menos fallas, basado la experiencia de los diferentes IXP implementados bajo este modelo. Los IXP de capa 2 son los que presentan una arquitectura más básica entre los diferentes modelos y a su vez la que presenta menos opción de falla, ya que cuentan con un conmutador que se encarga de interconectar a los miembros, por su parte cada miembro cuenta con un enrutador para poder establecer las sesiones BGP con los otros miembros, dando autonomía de conexión y control de atributos sobre las sesiones con los demás miembros.

2.5.2.2 Modelo Capa 2 más servidor de rutas

Según Cicileo (2016), el servidor de rutas es un servidor físico el cual corre un aplicativo de enrutamiento. Este aplicativo permite a los miembros establecer sesiones BGP entre los miembros del IXP para poder intercambiar información de ruteo entre ellos. Los servidores de rutas tienen el papel de solo manejar lógica de ruteo y no trabaja con los paquetes enviados entre los miembros que entablaron la sesión.

Según Cicileo (2016), como característica principal, reduce la necesidad de implementar sesiones BGP entre todos los miembros del IXP, de esta forma con una sola sesión por miembro pueden entablarse comunicación e intercambio de rutas con todos los demás miembros.

El número de sesiones está representado por:

$$Número\ de\ sesiones = n(n-1)$$

La descripción del punto de intercambio de tráfico de capa 2 con servidor de rutas se muestra en la figura 14.

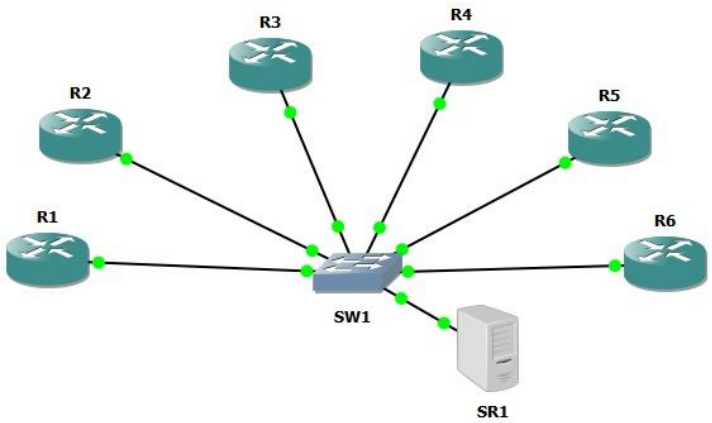


Figura 15. Arquitectura Punto de intercambio de tráfico modelo capa 2 con servidor de rutas.
Fuente: Elaboración propia.

Según Cicileo (2016), en base a las desventajas presentadas por el modelo de capa 2 en función a la cantidad de participantes, el emparejamiento de un gran número de miembros requiere un trabajo extenso a la larga, siendo inmanejable y de difícil control para los demás miembros. Agregando un servidor de rutas al modelo de capa 2 este problema es solucionado, ya que los miembros realizarán las sesiones directas con los otros miembros que lo deseen y además tendrán la opción de interconectarse con todos los demás miembros a través de una sola sesión de BGP con el servidor de rutas, este se encargada de publicar las redes de los otros miembros.

El uso de un servidor de rutas presenta las siguientes ventajas

- Oportunidad de enrutamiento escalable.
- Simplificación en la configuración y administración de ruteo en los ISP.
- Separación de ruteo y envió de tráfico.
- Práctica adecuada para el ruteo entre ISP.

2.5.2.3 Modelo Capa 3

Según Cicileo (2016), en los IXP de modelo capa 3, el administrador del IXP realiza las interconexiones de BGP entre los miembros a través de un router manejado y

controlado por ellos. De esta forma los miembros entablan sus sesiones BGP a través del router del administrador. De requerir una interconexión con algún miembro, esta sesión deberá hacerse de forma directa con el equipo del otro miembro y no pasar por medio del enrutador del administrador del IXP.

Los puntos de intercambio de tráfico de capa 3 presentan una arquitectura similar a la mostrada en la figura 15.

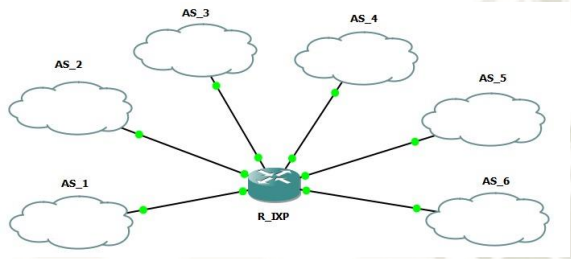


Figura 16. Arquitectura Punto de intercambio de tráfico modelo capa 3.
Fuente: Elaboración propia.

Los modelos de capa 3 basan su interconexión de forma centralizada en un enrutador que es de propiedad del punto de intercambio de tráfico. Este enrutador maneja todas las rutas y sesiones de los diferentes miembros y los miembros son dependientes del enrutador del IXP para poder manejar políticas de ruteo y de tráfico sobre los otros miembros.

2.5.3 Impacto del establecimiento de un Punto de intercambio de tráfico.

La tabla 5 muestra los resultados obtenidos de una evaluación sobre el impacto de la creación de puntos de intercambio de tráfico en Kenia y Nigeria, obteniendo los beneficios mostrados a continuación.

Tabla 6. Resumen de los beneficios clave

Beneficios	KIXP	IXPN	Resumen
Latencia	Reducción de 200-600 ms a 2-10 ms	Reducción de 200- 600 ms a 2-10 ms	Aumento notable en el rendimiento para los usuarios finales

Intercambio de tráfico local	Picos de 1 Gbit/s	Picos de 300 Mbit/s	Ahorros anuales de más de 1 millón de dólares en tráfico internacional de en ambos países
Contenido	Presencia local de la red de Google, además de repatriación del contenido nacional	Igual que en Kenia	Aumento del tráfico de datos en redes móviles e ingresos correspondientes
Gobierno electrónico	La autoridad fiscal de Kenia cobra los impuestos en línea	Uso por parte de redes educativas y de investigación	Beneficios sociales gracias al acceso del gobierno electrónico al IXP
Otros Beneficios	Mayor cantidad de tráfico regional intercambiado en KIXP	Plataformas financieras alojadas localmente	Los IXP traen beneficios económicos

Fuente: Kende y Hurpy (2012)

2.5.4 Ventajas y Desventajas de un Punto de intercambio de tráfico

A continuación, se muestran mediante la tabla 6 las ventajas y desventajas de la implementación de un punto de intercambio de tráfico.

Tabla 7. Ventajas y desventajas de un punto de intercambio de tráfico

Ventajas	Desventajas
✓ Tráfico local se enruta localmente ✓ Menor latencia para las aplicaciones ✓ Menores costos ✓ Posibilidad de CDNs ✓ El tráfico de una región/país/zona no es visto desde otras regiones/países ✓ Introducción de nuevas tecnologías (IPv6, RPKI, etc.)	x Cuando hay una legislación Proveedor monopolista de tránsito. x Con todos los demás operadores de red que están legislados con clientes de este proveedor monopolista. x Cuando la economía local es tan pequeña que no puede sostener más de un operador de red.

✓ Acciones coordinadas ante incidentes de seguridad, problemas técnicos, etc. ✓ Sentido de "comunidad"	x Naciones muy pequeñas (¿quizás menos de 10000 habitantes?) x Costosa conectividad doméstica x Conectividad internacional costosa x Ofertas de servicios restringidas y deficiente x No hay economía doméstica en Internet

Fuente: Estrada, Padilla, Lorío, Rojas, y Ramírez (2018)

Según Yong (2013), las mejores prácticas están enfocadas por los lados que componen el punto de intercambio de tráfico, los miembros y el operador del IXP, cada uno de ellos debe ser cuidadoso en temas de publicación, filtrado, seguridad entre otros.

Según Yong (2013), por el lado del operador del Punto de intercambio de tráfico se tiene que considerar:

- Seguridad y filtrado en los puertos que interconectan a los miembros.
- Establecer aprovisionamientos automáticos, que eviten errores comunes realizados por las personas y minimizar riesgos.
- Los emparejamientos realizados por el route server deberán ser transparentes, es decir, no debe ser un punto intermedio de publicación entre los miembros, sino solo un punto de transporte y no reflejarse los AS del route server en rutas compartidas.
- Tener sumo cuidado en temas de tormenta de broadcast y poseer equipos que puedan lidiar con un problema de ese tipo.

Según Yong (2013), por el lado de los miembros se debe considerar:

- El tipo de tráfico innecesario para IXP debe ser bloqueado.

- No tener bucles de red conectados al IXP, con el fin de evitar tormentas de broadcast.
- Dentro de las reglas de filtrado, no publicar las redes dispuestas por el IXP.
- Establecer conexión de emparejamiento con los route servers del IXP para facilitar la gestión y ordenamiento.

Según Amsix (2021), como parte de las recomendaciones brindadas a la hora de interconectarse con el IXP tenemos:

Tipo de tráfico permitido:

- IPv4
- ARP
- IPv6

Según Amsix (2021), solo permite tráfico del tipo IEEE 802.3, (IEEE, 2018), basado en ethernet, el IEEE 802.2, (IEEE, 1989), no está permitido por lo ello el tráfico del tipo LLC encapsulado no es aceptado.

Según Amsix (2021), prevenir el ingreso de tráfico indebido evitando:

- Múltiples Direcciones Mac: los puertos del enrutador solo aceptarán una dirección MAC, al ver otra no podrá reconocerse en el puerto y por tanto perderá la conectividad.
- Spanning Tree Protocol (STP): el puerto interconectado al IXP no deben estar incluido en una configuración de STP o algún otro protocolo que implique lo mismo.
- Protocolos de Enrutamiento: solo debe admitirse tráfico intercambiable del protocolo BGP, cualquier otro protocolo de enrutamiento debe ser bloqueado.

- Protocolos de descubrimiento: este tipo de protocolos debe estar deshabilitado en la interfaz que interconecte con el IXP.
- Protocolos de unidifusión: el único protocolo permitido será el ARP, cualquier otro tipo como IGMP, DHCP no serán admitidos.
- Para el caso de IPv6 la propiedad de anuncio permitida en IPv6 deberá ser deshabilitada, por provocar tráfico innecesario que no será recibido por los miembros.

Según Amsix (2021), dentro de las mejores prácticas vistas para la implementación de un IXP, el punto más importante es la seguridad y evitar tráfico innecesario proveniente de ciertos protocolos.

La mayoría de los enrutadores al trabajar en modelos de capa 2 deben evitar los problemas que conlleva el conectarse por medio de esta capa, como la tormenta de broadcast, lectura innecesaria de ARP, protocolos de descubrimiento, bucles, entre otros.

2.5.4.1 Requerimientos de implementación de un IXP

Según Singh (2020), como parte de la implementación del IXP, deben considerarse los siguientes aspectos:

- Espacio físico y espacio por miembro
- Control y supervisión de temperatura
- Seguridad
- Energía
- Accesos
- Cableado
- Soporte técnico

Según la Internet Society (2020), los requisitos para la implementación física de un punto de intercambio de tráfico se nombran a continuación:

1. Disponer de un espacio físico para la colocación de racks de comunicaciones los cuales contendrán equipamiento del IXP, equipamiento de los miembros, servicios y equipos de transmisión.
2. La infraestructura de IXP debe poseer equipamiento de redundancia con switch de 48 puertos e interfaces SPF.
3. El control de la temperatura debe realizarse según el tamaño, la carga de equipos, entre otros factores.

   Basando este cálculo en la formula mostrada a continuación:

   Carga de calor total = BTU del área de la habitación + BTU de ventana+ BTU del equipo + BTU de iluminación

   Ejemplificando el cálculo realizado en IXP toolkit (Internet Society, 2020) en base a un punto de intercambio de tráfico de 15 m², con una carga de equipos de 10000w y carga luminosa de 100w, se presenta una carga total de 48310 BTU recomendando 2 sistemas de aire acondicionado de 36 000 BTU cada uno teniendo uno como redundancia.
4. Se debe asegurar como mínimo un servicio de redundancia de energía ininterrumpido de 12 a 24 horas en base a inversores de 10KVA y tableros de distribución energético independientes por cada rack de comunicaciones.
5. Realizar un cableado acorde a él data center bajo estándares.

Por los requerimientos físicos en su implementación, debe considerarse la implementación de un data center que aloje el IXP certificado que garantice los principales servicios sin interrupción. Certificaciones como TIER creada por el Uptime

Institute o la certificación ICREA, cada una de ellas tienen diferentes niveles o jerarquías que garantizan la disponibilidad en los data center.

2.5.5 Puntos de Intercambio de tráfico en Latino América y el Caribe

Según Galperin (2013), la situación de los puntos de intercambio de tráfico en América Latina y el Caribe se describe a continuación:

- Existen en 16 países con un promedio de 46 IXP en todo latino América y el caribe, entendiéndose así que un tercio de los países que son parte del territorio de América Latina y el Caribe cuentan con un IXP.
- Los IXP a lo largo del territorio en mención se distribuyen de la siguiente manera: América central cuenta con un IXP ubicado en Panamá, el Caribe cuenta con 6 IXP ubicados en Cuba, República Dominicana, Granada, Haití, Curacao y Sint Maarten, el resto está distribuido en Sudamérica.
- En su mayoría los IXP tienen políticas de manejo implantadas por los miembros que los conforman, volviéndose así puntos no comerciales, existen también IXP que poseen un manejo público como es el caso de Brasil y también existen modelos de IXP privados como en Chile.
- Los diferentes miembros de un IXP manejan un costo dentro de los IXP basado en su capacidad y número de puertos utilizados, existen casos donde el costo es implantado según el consumo originado del miembro para los casos de servicios adicionales.
- La interconexión que prevalece dentro de estos IXP es de forma multilateral, todos los miembros deben establecer conexiones con todos los otros miembros, habiendo la posibilidad de poder realizar emparejamientos bilaterales dentro del mismo IXP.

- Los IXP van a variar la cantidad de tráfico que muevan, según la cantidad de miembros y la participación de ISP grandes del país.
- Los proveedores de internet no son los únicos miembros interconectados a un IXP, existes desde entidades gubernamentales hasta redes científicas. Comparado con IXP de otros continentes como Europa o Asía, se ve la presencia de proveedores de diferentes países dentro de un IXP.
- Salvo excepciones, los IXP como en Chile y Bolivia, donde el gobierno por medio de leyes obliga a mantener el tráfico local por medio de los IXP, en otros casos los gobiernos no influyen en las políticas de los IXP.

El desarrollo de los IXP en Latinoamérica y el Caribe siguen una curva evolutiva favorable para la región, no se cuenta con el desarrollo que pueda tener Asia o Europa, pero el incremento que se va dando, significa que la importancia de los IXP va siendo entendida por más países dentro de la región. Para comprender el desarrollo del internet en la región son necesarios los IXP y la creación de nuevas políticas que ayuden a su evolución.

2.5.5.1 LAC-IX

Según Bertón (2016), la Asociación de puntos de intercambio de Internet de Latinoamérica y el Caribe (Latin American and Caribean Internet Exchange Asociation, LAC-IX) nace con la visión de promover el desarrollo de IXP en la región de Sudamérica y el Caribe, para así fomentar el desarrollo del internet en base a manejos y parámetros que garanticen un intercambio de tráfico eficaz entre los integrantes. Forma parte de la Internet eXchange Federation (IX-F).

Según Nimpuno (2019), la Asociación de puntos de intercambio de Internet de Latino América y el Caribe conglomera alrededor de 90 IXP dentro de toda la región,

albergando IXP de todo tamaño. Representa gran cantidad de la demanda del consumo de internet en la región y por ello la presencia de varios proveedores de contenido ha ido en aumento, mejorando el desarrollo de los IXP. Como asociación LAC-IX fomenta el desarrollo del internet en América Latina y el Caribe, promoviendo el desarrollo de puntos de intercambio en toda la región y de esa forma realizar en mayores cantidades el intercambio de tráfico local reduciendo el uso de enlaces internacionales de todos los miembros que conforman los IXP. Actualmente LAC-IX posee como socios a la Internet Society y a Lacnic.

Según Lacix (2020), en la actualidad existen 80 puntos de intercambio de tráfico entre los 17 asociados que actualmente conforman LAC-IX.

Según Lacix (2020), a continuación, se muestra la tabla 7 donde se muestran los socios existentes dentro de LAC-IX.

Tabla 8. Socios de LAC-IX

Número	Tipo de Socio	Nombre del Asociado	País
1	Socio Activo	Cabase	Argentina
2	Socio Activo	ix.br	Brasil
3	Socio Activo	Amsix	Caribe
4	Socio Activo	inteRed	Panamá
5	Socio Activo	CITI	México
6	Socio Activo	Ahtic	Haití
7	Socio Activo	ETECSA	Cuba
8	Socio Activo	cr!X	Costa Rica
9	Socio Activo	IXPy	Paraguay

10	Socio Activo	IXPECUADOR	Ecuador
11	Socio Activo	Ix.DO	Dominicana
12	Socio Activo	IXP.GT	Guatemala
13	Socio Activo	PIT PERU IX	Perú
14	Socio Activo	PIT BOLIVIA	Bolivia
15	Socios Adherente	Konnecta	México
16	Socios Adherente	Aprosva	Ecuador
17	Socios Adherente	Internet Service Yucatan	México
18	Socios Adherente	IXSAL	El Salvador

Fuente: Lacix (2020)

Según ITU (2020), la tabla 8 nos muestra los indicadores obtenidos por los países miembros de la comunidad andina.

Tabla 9. Indicadores Perfiles Comunidad Andina

Indicador	Estado Plurinacional de Bolivia	Colombia	Ecuador	Perú
Población (Millones)	11.4	45.5	16.9	31.2
Tráfico PIT in/out (Gbps)	2/1.2	35	32	22/31
Banda ancha bajada/subida (Mbps)	2/0.512	25/550/20 (ultra)	1	4/1 básica 10/2.5 intermedia 20/10 avanzada
Conexiones a Internet (Millones)	9.8	32.1	10.7	26.45

Conexiones a Internet Móvil (Millones)	9.28	25.7	9.1	24
Conexiones a Internet fijo (Millones)	0.50	6.4	1.6	2.48
Conexiones a servicio móvil celular (Millones)	11.44	62.8	15.6	41
Conexiones a telefonía Fija (Millones)	0.72	6.95	1.9	2.84

Fuente: ITU (2020)

2.5.5.2 Actualidad Perú

Según el Banco de desarrollo de América Latina (2014), la capacidad de tráfico que mueve el Perú se encuentra distribuida de la siguiente manera: Lima y Callao manejan un 68% de banda ancha[6], 12% se distribuye entre las ciudades de Cuzco, la Libertad y Arequipa, el 20% restante se distribuye entre los departamentos restantes.

Según el Banco de desarrollo de América Latina (2014), también indica que la posición geográfica de Perú lo pone en un papel de interconexión de doble comunidad, con la parte sur del continente Argentina, Chile, Brasil, Uruguay, Paraguay con la parte restante del continente compuesta por las regiones de Andina / Centroamérica / Norteamérica, la cual componen México, Guatemala, Honduras, El Salvador, Nicaragua, Colombia, Venezuela, Bolivia y Ecuador.

Según el Banco de desarrollo de América Latina (2014), un aspecto importante que se menciona, es que el Perú provee interconexión con la parte sur del continente y tiene el rol de poder dar un punto de interconexión al exterior a Bolivia. Su par en importancia sería Panamá, la cual se encarga de las regiones Centrales y las regiones restantes.

[6] Banda ancha: transmisión de datos existente en un canal de comunicaciones

El Perú cuenta con una posición privilegiada geográficamente que le permitiría poder explotar todo el potencial de redes, tráfico y servicios que pudiera implementarse dentro de un IXP al interconectar las regiones adyacentes a él.

El Perú en la actualidad cuenta con 3 IXP implementados en la región los cuales son:

- NAP Perú
- PIT Perú
- NAP Inca

2.5.5.2.1 Nap Perú

Según el Banco de desarrollo de América Latina (2014), el NAP Perú es un punto de intercambio de tráfico en el cual se encuentran conectados los principales ISP del país, es decir, los proveedores con mayor nivel de tráfico en el país, tiene una administración privada y como característica, su consejo directivo está compuesto por cargos que rigen los miembros conectados al NAP Perú. Tienen políticas de acuerdos multilaterales entre los miembros y funciona como un punto de tráfico neutro.

En la arquitectura del NAP Perú se puede apreciar, una infraestructura con redundancia y doble conexión por proveedor, un manejo de servicios por Vlan. Como se muestra en la figura 16.

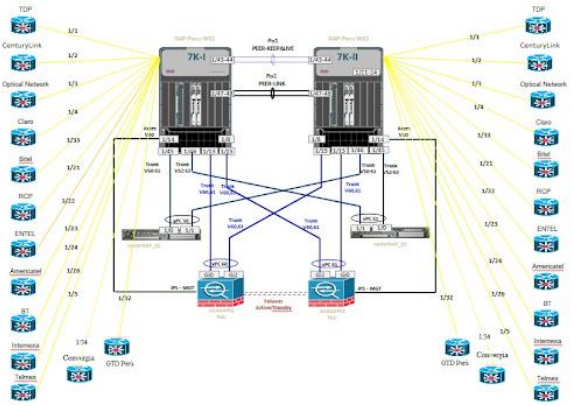


Figura 17. Arquitectura IXP modelo capa 2.
Fuente: *Asociación Nacional de Proveedores de Internet (2021)*

2.5.5.2.1.1 Normativas

Según la ODN (2007), parte de las normativas para poder ser miembro del Nap Perú es pertenecer al RIR de la región, para este caso LACNIC y recursos públicos como IPs públicas propias y número de sistema autónomo. También debe contar con enlaces de transporte externos, es decir, internacionales.

Según la ODN (2007), para el tema de la interconexión física de un nuevo miembro en el IXP, esté podrá utilizar enlaces su propia arquitectura de despliegue para llegar hasta el lugar o también podrá usar la fibra de otro proveedor para que le pueda brindar transporte y de esa manera interconectarse.

Según la ODN (2007), aparte de los requerimientos mencionados con anterioridad, el (Comité Técnico NAP – PERU, 2006), indica que los enlaces en uso de los miembros dentro del NAP Perú tendrá como límite de uso el 80% de su capacidad total, teniendo que aumentar su capacidad una vez superado esté límite, los miembros cuentan con puertos de al menos de 100Mbps de interconexión y al momento de interconectarse, deben de hacerlo de forma redundante, es decir, cada miembro debe poseer dos conexiones dentro del NAP Perú.

2.5.5.2.1.2 Tráfico

El tráfico con el cuál el Nap Perú trabaja se muestra en la figura 17.

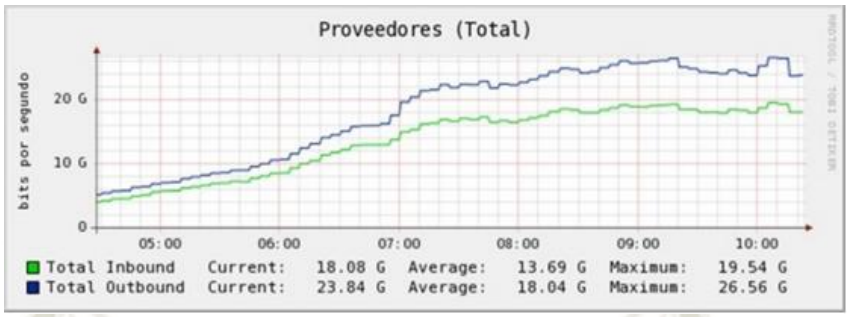


Figura 18. Cantidad de tráfico en Nap Perú.
Fuente: *ITU (2020)*

2.5.5.2.2 Pit Perú

Según Lacix (2020), el Pit Perú es un punto de intercambio de tráfico un con mentalidad de interconexión neutral entre sus miembros. Dentro de los cuales se pueden observar ISP, CDN, universidades entre otros. Adoptan políticas de emparejamiento multilateral y bilateral a criterio dependiente de los miembros. Promueven el protocolo de enrutamiento BGP y una visión de autonomía en las redes del Perú.

Según Lacix (2020), el Pit Perú es un punto de intercambio de tráfico moderno, fundado en el 2018, es el punto de intercambio con menos tiempo de operación en el Perú. Y es un punto de intercambio con políticas neutrales para sus miembros, buscando conectar no solo a proveedores de servicio o contenido, sino a cualquier entidad que pueda sacar un provecho de la interconexión.

2.5.5.2.2.1 Normativas

Según PIT Perú (2020), parte de las normativas para la interconexión en el Pit Perú son:

1. Los participantes deben contar con recursos propios otorgados por un RIR, no específicamente el RIR de Latinoamérica, permiten la opción de asesoría para obtener dichos recursos.

2. Como protocolo de enrutamiento utiliza BGP para realizar los emparejamientos.
3. Pit Perú cuenta con puertos de interconexión de 1, 10, 40 y 100 Gbps, a su vez permite el incremento de capacidad de enlace mediando protocolos como LACP o bonding[7].
4. La interconexión al Pit Perú es manejada por políticas puestas por cada miembro, no hay limitantes que especifiquen el cómo.
5. Los puertos que utilicen los miembros como capacidad no deben tener menos del 20% de capacidad restante, tendrán que realizar ampliaciones de canal luego de suscitado esto.
6. Los acuerdos permitidos entre los participantes pueden ser tanto bilaterales como multilaterales.

2.5.5.2.2.2 Especificaciones sobre módulos ópticos

Según PIT Perú (2020), Pit Perú cuenta con diferentes centros de datos alrededor de Lima, donde es posible realizar la interconexión.

Como parte de las especificaciones de interconexión con sus dispositivos y el uso de sus módulos ópticos presentan la tabla 9.

[7] Bonding: agregación de enlaces físicos en un enlace virtual con el fin de duplicar capacidad y aplicar niveles de redundancia.

Tabla 10. Módulos ópticos para interconexión

Estándar	Distancia Máxima
1000Base-LX	10 km
10GBase-LR	10 km
10GBase-ER	40 km
40GBase-LR4	10 km
40GBase-ER4	40 km
100GBase-LR4	10 km
100GBase-ER4	40 km

Fuente: PIT Perú (2020)

2.5.5.2.2.3 Especificaciones sobre Direcciones MAC y tipos de tráfico

Según PIT Perú (2020), con el fin de mantener las prácticas, reglamentaciones y estatutos, solo se admitirán en los puertos de Pit Perú los siguientes EtherTypes:

- Ox0800 – IPv4
- 0x0806 – ARP
- 0x86dd – IPv6

Según PIT Perú (2020), los puertos estarán configurados para solo aceptar una dirección MAC, ante la presencia de otra MAC no será reconocida por el puerto. Se permite el uso de protocolos de expansión como LACP previendo futuras expansiones.

Según PIT Perú (2020), el trafico proveniente de los miembros solo deberá ser el tipo Unicast, cualquier otro tipo como Anycast o Multicast no serán permitidos. Los protocolos de descubrimientos deberán ser deshabilitados.

2.5.5.2.3 Nap Inca

Según León (2012), este punto de intercambio de tráfico se encuentra a cargo de Internexa S.A, indican que cada miembro es responsable de la interconexión con el IXP, sin importar el medio por el cual se vaya a interconectar, sea por un medio alámbrico, inalámbrico o óptico. Posee dos switch para una interconexión con redundancia, por ello los miembros tienen la posibilidad de conectarse a ambos switch. Dentro de las políticas Internexa permite y promueve la unión de IXP regionales con Nap Inca para su expansión.

Según León (2012), a pesar de poseer precios inferiores a los presentados por Nap Perú, Nap Inca no presenta miembros afiliados en la actualidad. El Nap Inca se encuentra registrado en la página de IXPdb.euro-ix[8], pero no presenta mayor información de su composición o administración.

2.6 Redes de distribución de Contenido

Según Krishnamurthy, Wills y Zhang (2001), el aumento de servicios en la red, las conexiones por usuario y la resolución de solicitudes por usuario a un mismo destino provocaba grandes cuellos de botella de información, traducidos en aumento de latencia, bajas tasas de transferencia y sobre todo de vista al usuario una degradación del servicio de red.

Según Krishnamurthy, Wills y Zhang (2001), a partir de ese problema nace la necesidad de crear nuevos puntos de destino que sean capaces de satisfacer las necesidades de los usuarios, para ello se crean diferentes sistemas de respuesta a búsquedas como por ejemplo el cache web locales o de implementación en la nube, estructuras P2P, CDN, entre otros.

[8] Nap Inca en IXPdb.euro-ix: IXPdb.euro-ix.net/en/IXPdb/organization/411/

Según Krishnamurthy, Wills y Zhang (2001), las redes de distribución de contenido (CDN), son un número de servidores con la característica de poder ser localizados en diferentes sitios geográficamente o en el mismo sitio de los servidores de origen de consulta, teniendo la facultad de poder resolver peticiones de usuarios a nombre de los servidores de servicios consultados.

Según Krishnamurthy, Wills y Zhang (2001), al recibir estos servidores que componen la CDN la consulta por parte del usuario, están en la capacidad de resolver la petición para que sea respondida por cualquier servidor que contenga la información solicitada, de esta forma mejoran el rendimiento de la red ya que pueden mandar a resolver peticiones a servidores de otras localidades basándose en tiempos de latencia, disponibilidad de canal entre otros.

Según Molina, Palau, Esteve, Alonso y Ruiz (2006), el proceso de funcionamiento de una CDN se basa en 2 características principales, la división de contenido en subprocesos y él envió de solicitudes a servidores diferentes, de esta forma existe una mejora en la disponibilidad y tiempos de respuesta para los servicios solicitados.

Según Molina, Palau, Esteve, Alonso y Ruiz (2006), también indica que el punto de mayor desarrollo y ventaja de una CDN son el proceso de envío de solicitudes a diferentes destinos ya que con su correcto uso, se realizan mejoras en independencia de servidores, proveedores, flexibilidad y da un enfoque de crecimiento ya no jerarquizado en forma vertical, promoviendo el uso de recursos de forma horizontal. Como resultado de este proceso se obtiene una reducción en tiempos de latencia y descongestión de enlaces de proveedor de contenidos dando una mejor experiencia al usuario final.

Según Molina, Palau, Esteve, Alonso y Ruiz (2006), la forma en que una CDN resuelve las consultas de sus orígenes es determinada por dos factores, resolución en base

a la localización de recursos uniforme (URL) y en base a la resolución del nombre de dominio (DNS), en la cual los servidores de DNS reciben las peticiones y por medio del manejo de nombres de dominio permite alterar los lugares de consulta y respuesta que tendrán para el usuario.

CAPÍTULO III: EVALUACIÓN Y ANÁLISIS DE NECESIDADES

3. Desarrollo de requerimientos

En el presente capítulo, evaluaremos las necesidades y requerimientos del diseño del punto de intercambio de tráfico en la jurisdicción de un distrito entre la municipalidad con sus comisarías.

3.1 Descripción del escenario

El proyecto, busca diseñar un punto de intercambio de tráfico o IXP, en un distrito entre la municipalidad con sus comisarías en la ciudad de Arequipa.

3.1.1 Departamento de Arequipa

En la actualidad, Arequipa como departamento está conformada por 8 provincias las cuales están conformadas por un total de 109 distritos distribuidos como muestra la figura 18.

Demarcación Política de la región Arequipa

N°	PROVINCIAS	CAPITAL	N° DE DISTRITOS
1	Arequipa	Arequipa	29
2	Camaná	Camaná	8
3	Caravelí	Caravelí	13
4	Castilla	Aplao	14
5	Caylloma	Chivay	20
6	Condesuyos	Chuquibamba	8
7	Islay	Mollendo	6
8	La Unión	Cotahuasi	11

FUENTE: INEI: resultados definitivos - Arequipa

Figura 19. Distribución de número de distritos por cada provincia de Arequipa. Fuente:www.regionArequipa.gob.pe/Cms_Data/Contents/GobRegionalArequipaInv/Media/CORESEC/PLANES/PLAN-REGIONAL-DE-SEGURIDAD-CIUDADANA-2019-AREQUIPA.pdf

Teniendo un mayor número de comisarías la provincia de Arequipa con respecto a las otras provincias del departamento.

3.1.1.1 Provincia de Arequipa

Según el plan regional de seguridad ciudadana del 2019 emitido por el gobierno regional de Arequipa[9], la provincia de Arequipa está compuesta por 59 comisarías en 27 distritos.

Los distritos de Quequeña y San Juan de Siguas no cuentan con comisarías en sus distritos, por ello solo se tomarán en cuenta la información sobre los 27 distritos restantes de la provincia en los cuales si se cuenta con comisarías por distrito.

Según Informática (2018), de los datos del INEI del año 2018 entre los distritos más poblados se encuentran el distrito de Cerro Colorado con un total de 197 954 habitantes, el distrito de Paucarpata con 131 346 habitantes, el distrito de Cayma con 91935 habitantes, el distrito de Alto Selva Alegre con 85 870 habitantes, el distrito José Luis Bustamante y Rivero con 81 829 habitantes entre otros.

Los distritos que cuentan con más comisarías en su territorio son el distrito de Paucarpata con 6 comisarías, Cerro Colorado y la Joya con 5 comisarías, Cayma y Miraflores con 4 comisarías y José Luis Bustamante y Rivero con 3 comisarías.

3.2 Requerimientos

En base a la información adquirida sobre los números de comisarías y según la población de cada distrito de la provincia de Arequipa, se tomará como punto de referencia el distrito de José Luis Bustamante y Rivero para hallar un cálculo promedio en cuanto al ancho de banda requerido por municipalidad y Comisaría.

[9] Plan Regional de Seguridad Ciudadana del 2019: www.regionarequIPa.gob.pe/Cms_Data/Contents/GobRegionalArequIPaInv/Media/CORESEC/PLANES/PLAN-REGIONAL-DE-SEGURIDAD-CIUDADANA-2019-AREQUIPA.pdf

3.2.1 Municipalidad

Cada distrito cuenta con una municipalidad y con un número determinado de comisarías. El distrito de José Luis Bustamante y Rivero, pertenece a uno de los distritos con mayor densidad poblacional de Arequipa y mayor número de comisarías.

En la actualidad cuenta con un total de 67 cámaras[10] distribuidas en todo el distrito buscando garantizar un mayor nivel de seguridad y reducción del delito.

Según la Municipalidad Distrital de José Luis Bustamante y Rivero (2019), los servicios brindados por el serenazgo se presentan en la tabla 10.

Tabla 11. Servicios de Serenazgo

Servicio	Cantidad
Supervisor	3
Encargado de grupo	3
Técnicos en seguridad. (Serenos)	54
Personal de Call Center	3
Personal de Central de Monitoreo	2
Radios Handy	25
Teléfonos Celulares RPC	6
Camionetas	8
Autos	3
Chaleco antibalas	25
Camillas	8

Fuente: Elaboración propia.

[10] Número de cámaras en la actualidad: https://www.munibustamante.gob.pe/noticia/2281-nueva-red-de-camaras-de-videovigilancia-disminuira-indice-de-inseguridad-en-bustamante-y-rivero

3.2.2 Comisarías

Según la Municipalidad Distrital de José Luis Bustamante y Rivero (2019), el distrito de José Luis Bustamante y Rivero cuenta con 3 comisarías en su jurisprudencia.

- José Luis Bustamante y Rivero
- Simón Bolívar
- Ciudad mi Trabajo

Según la Municipalidad Distrital de José Luis Bustamante y Rivero (2019), se divide su territorio en 8 zonas administrativas las cuales se muestran en la figura 19.

Figura 20. División administrativa del distrito de José Luis Bustamante y Rivero.
Fuente: *Municipalidad Distrital de José Luis Bustamante y Rivero (2019)*

Según la Municipalidad Distrital de José Luis Bustamante y Rivero (2019), los datos obtenidos se presenta la tabla 11, en la cual se mencionan las jurisdicciones de comisarías y la ubicación de cámaras de vigilancia distribuidas en las zonas administrativas del distrito.

Tabla 12. Distribución de zonas por comisarías y Cámaras de vigilancia

Zona Administrativa	Jurisdicción Policial	Ubicación de Cámaras de Vigilancia
Zona 1	Comisaría Ciudad mi Trabajo	Av. EEUU con Tupac Amaru, Av. Dolores con EEUU, Óvalo de la paz
Zona 2	Comisaría Simón Bolívar	Av. Avelino Cáceres Farmacia
Zona 3		----------
Zona 4		Av. Dolores Saunas, Av. Dolores con EEUU, Ovalo de la Estrella
Zona 5		----------
Zona 6	Comisaría José Luis Bustamante y Rivero	Av. Dolores Saunas
Zona 7		----------
Zona 8		Av. EEUU con Tupac Amaru, Av. Avelino Cáceres Farmacia y Tiendas EFE, Av. Dolores Grifo Primax, Av. Vidaurrazaga, Av. Dolores con EEUU, Óvalo de la paz

Fuente: Elaboración propia.

La distribución del personal por cada Comisaría se muestra en la figura 20.

1. Comisaría de José Luis Bustamante y Rivero:

Comisario	: Cmdte. PNP Jesús Martin Alzamora Green
Oficiales	: 03
Sub Oficiales	: 132
Vehículos	: 05
Motocicletas	: 02
Ubicación	: Urb. Quinta Tristán Nº V-02
Teléfono	: 054-427290/ 348608
Correo electrónico	: cpnpbustamanteyrivero@hotmail.com

1. Comisaría de Ciudad Mi Trabajo

Comisario	: Cmdte. PNP Eduardo Santiago Del Campo Pérez
Oficiales	: 02
Sub oficiales	: 66
Especialistas	: 04 (01 inoperativo).
Vehículos	: 01
Ubicación	: Av. Independencia s/n Ciudad mi trabajo.
Teléfono	: 054-435060
Correo Electrónico	: ciaciudadmitrabajo@hotmail.com

2. Comisaría de Simón Bolívar

Comisario	: MY. PNP José Antonio Apestegui Pinto
Oficiales	01
Sub oficiales	: 47
Vehículos patrulleros	: 03, (01 inoperativo).
Ubicación	: Av. Caracas Nº 629.
Teléfono	: 054-431382/427653
Correo Electrónico	: ciapnpsimonbolivar@hotmail.com

Figura 21. Distribución de personal por Comisaría en el distrito de José Luis Bustamante y Rivero.
Fuente: *Municipalidad Distrital de José Luis Bustamante y Rivero (2019)*

3.2.3 Bases del Diseño

El diseño se basa en la data obtenida sobre el distrito de José Luis Bustamante y Rivero, la municipalidad y sus comisarías.

3.2.3.1 Servicios

A continuación, se describen los servicios prestados y la cantidad de dispositivos involucrados por cada entidad.

3.2.3.2 Municipalidad

De la información obtenida en el apartado superior, se tiene que para la municipalidad deben considerarse los puntos para el diseño presentados en la tabla 12.

Tabla 13. Servicios disponibles y cantidad de dispositivos para la municipalidad.

Función	Número de dispositivos	Servicio
Call center	3	VoIP
Central de monitoreo	2	Video, texto y datos
Cámaras de seguridad	67	Video, audio
Monitoreo servicios del punto de intercambio de tráfico IXP	1	Internet, texto, datos

Fuente: Elaboración propia.

3.2.3.2.1 Comisaría

En la figura 21 se obtuvieron los valores aproximados de la cantidad de personal con el que cuenta cada Comisaría.

En la tabla 13 se muestran las funciones y dispositivos que compartirá la Comisaría de José Luis Bustamante y Rivero.

Tabla 14. Servicios disponibles y cantidad de dispositivos para las comisarías.

Comisaría	**Función**	**Número de dispositivos**	**Servicio**
Comisaría José Luis Bustamante y Rivero	Call center	3	VoIP
	Central de monitoreo	2	Video, audio
	Monitoreo servicios del punto de intercambio de tráfico IXP	1	Internet, texto, datos
Comisaría Ciudad mi Trabajo	Call center	2	VoIP
	Central de monitoreo	1	Video, audio
	Monitoreo servicios del punto de intercambio de tráfico IXP	1	Internet, texto, datos
Comisaría Simón Bolívar	Call center	2	VoIP
	Central de monitoreo	1	Video, audio
	Monitoreo servicios del punto de intercambio de tráfico IXP	1	Internet, texto, datos

Fuente: Elaboración propia.

3.3 Cálculos de capacidad de enlace

3.3.1 Servicios

En la siguiente sección mostraremos el cálculo de los servicios que compartirán en el punto de intercambio de tráfico cada miembro.

3.3.1.1 VoIP

Según Frans (2011), el servicio de VoIP se basa en él envió de tramas de datos provenientes de la voz los cuales por medio de un códec son enviados a través de las líneas con diferentes valores de compresión dependiendo el tipo de códec que se utilice.

En la tabla 14 se muestra una tabla resumen de los códec para entender su comportamiento.

Tabla 15. Relación de códec de voz elegible para telefonía IP

Códec	**Algoritmo**	**Frecuencia de Muestreo (KHz)**	**Retardo (ms)**	**Tasa de bits por segundo (Kbps)**	**Tasa de bits por segundo para IP**	**Factor de compresión**
G.711	PCM	8	1	64	87.2	2
G.723.1	ACELP	8	1	5.3	21.9	24.15
				6.4	20.8	20
G.726	ADPCM	8	0.125	32	55.2	3.2
G.729	CS-ACELP	8	15	8	31.2	16

Fuente: Frans (2011)

3.3.1.1.1 Cálculo de ancho de banda para VoIP

Para nuestro caso las líneas implementadas estarán diseñadas para un único uso en el punto de intercambio de tráfico, es decir, este ancho de banda siempre tiene que estar disponible para VoIP.

Para hallar el ancho de banda requerido de VoIP es necesario conocer los valores de las variables del tamaño total del paquete y los paquetes por segundo (PPS) los cuales vienen representados en la ecuación 1 y ecuación 2 obtenidas de:

Ecuación 1.- Ancho de Banda= Tamaño total del paquete x PPS

$$Ecuación\ 2. - PPS = \frac{Tasa\ de\ bits\ del\ \text{códec}}{Tamaño\ de\ carga\ útil\ de\ voz}$$

Se realizarán los cálculos en base al códec G.711 para garantizar la mejor calidad en llamada.

Tamaño total del paquete:

- Encabezado Capa 2: 18bytes
- IP: 20 bytes
- UDP: 8 bytes
- RTP: 12 bytes
- Tamaño de carga útil de voz (G.711): 160 bytes

Tasa de bits del códec G.711= 64Kbps

Reemplazando los valores en las ecuaciones 1 y 2 se obtiene:

Tamaño total del Paquete=18+20+8+12+160

Tamaño total del Paquete=218 bytes

$$PPS=\frac{64000}{(160*8)}$$

PPS=50

Ancho de Banda= 218 x 50 x 8

Ancho de Banda= 87.2Kbps

De esta forma, determinamos que el ancho de banda requerido por línea es de 87.2Kbps.

3.3.1.2 Video

El servicio de video viene dado por la cantidad de cámaras disponibles en total en todo el distrito. Su cálculo estará basado en el tipo de compresión que se utilice en las cámaras, así como el número de cámaras disponibles.

Para entender este cálculo es necesario detallar datos de la trama ethernet con el fin de ilustrar los siguientes pasos.

En la figura 21 mostramos la composición de bytes de la trama ethernet conocida por el estándar IEEE 802.3

IEEE 802.3

7	1	6	6	2	46 a 1500	4
Preámbulo	Delimitador de inicio de trama	Dirección de destino	Dirección de origen	Longitud	Encabezado y datos de 802.2	Secuencia de verificación de trama

Figura 22. Cantidad de Bytes en la trama Ethernet.
Fuente: *Cisco (2005)*

De esta figura podemos determinar que el apartado diseñado para el encabezado y datos está compuesto por un máximo de 1500 bytes.

Distribuidos de la siguiente forma:

- 20 bytes destinados a la Cabecera IP
- 20 bytes destinados para la cabecera TCP
- 1460 bytes destinados para datos

De igual forma, a partir de la figura 21 podemos determinar que la trama ethernet consta de un máximo de 1526 bytes, de esos 1526 bytes, descontamos los 1500 destinados a encabezado y datos restando 66 bytes denominados bytes de sobrecarga.

3.3.1.2.1 Cálculo de ancho de banda para Video

A partir, de los datos obtenidos en la sección anterior, procedemos a realizar el cálculo de ancho de banda para la transmisión de video.

Para hallar el ancho de banda requerido deben tomarse en consideración las ecuaciones 3,4,5 y 6.

Ecuación 3.- $\text{Número de tramas} = \frac{\text{Tamaño de fotograma [Kbyte]}}{\text{Datos útiles de trama [bytes]}}$

Ecuación 4.- Sobrecarga total=Número de Tramas x Sobrecarga total por encapsulamiento [bytes]

Ecuación 5.- Total de bytes transmitidos=Tamaño de fotograma + Sobrecarga total

Ecuación 6.- Ancho de Banda por cámara=Total de bytes transmitidos x PPS [bps]

Y los datos:

Datos útiles de trama = 1460 bytes

Sobrecarga total por encapsulamiento = 66 bytes

Para nuestro caso consideraremos cámaras de 2592 x 1944 de resolución o su equivalente 5 MP y con un envió de fotogramas por segundo (FPS) de 30, el cual es un valor promedio estimado para visualización en tiempo real con una compresión promedio del tipo H.265.

De los datos descritos, tenemos que la cámara de 5 MP posee un tamaño de fotograma de 24.3Kbytes.

Reemplazando las ecuaciones 3 obtenemos:

$$\text{Número de tramas} = \frac{24.3K}{1460}$$

Número de tramas=17

Dado que las tramas no pueden presentarse en forma decimal al momento de enviarse se redondeará para fines de cálculo, obteniendo 17 tramas, ahora reemplazando en la ecuación 4, 5 y 6.

Sobrecarga total=17x 66

Sobrecarga total=1122 bytes

Total de bytes transmitidos=24.3k + 1122

Total de bytes transmitidos=25.322Kbytes

$$\text{Total de bytes transmitidos} = 25.322Kbytes \times \frac{8\ bit}{1byte}$$

Total de bytes transmitidos=202.576Kbits

Ancho de Banda por cámara=2.02Mb x 30 [bps]

Ancho de Banda por cámara=6Mbps

Según la información que se tiene, la municipalidad cuenta con 67 cámaras, lo cual nos da un total de 402 Mbps como ancho de banda requerido para las 67 cámaras.

3.3.1.3 Texto, Datos

Dentro de esta sección se involucran documentos comunes como PDF, Word, Excel entre otros utilizados por un usuario, y se utilizará la ecuación 7 y 8.

Ecuación 7.- $\text{Tamaño del archivo} = \text{Peso} \times \frac{8 \text{ bits}}{1 \text{ byte}}$

Ecuación 8.- Ancho de Banda=Tamaño de Archivo x PPS

Considerando un peso promedio de 4Mbytes por documento y un envió de 7 documentos cada 20 minutos, haciendo los reemplazos en las ecuaciones 7 y 8 se obtiene.

$$\text{Tamaño del archivo} = 4\text{Mbyte} \times \frac{8 \text{ bits}}{1 \text{ byte}}$$

$$\text{Tamaño del Archivo} = 32\text{Mbits}$$

$$\text{Ancho de Banda} = 32\text{M} \times \frac{7}{20 \text{ min}} \times \frac{1 \text{ min}}{60 \text{ segundos}}$$

$$\text{Ancho de Banda} = 186.67 \text{ Kbps}$$

En base al resultado obtenido, cada miembro del punto de intercambio de tráfico deberá contar con 186.67Kps disponibles en sus enlaces.

3.3.1.4 Internet

Si alguno de los miembros desea pasar por el punto de intercambio de tráfico, se separa un ancho de banda de 15Mbps para usos de internet, siendo este un valor promedio de consumo entre las empresas.

3.4 Evaluación de ancho de banda requerido

De los datos obtenidos de la anterior sección, obtenemos la tabla 15 presentando el resumen de recursos de ancho de banda necesarios.

Tabla 16. Resumen de Ancho de banda requerido por miembro

Sede	Servicio	Ancho de Banda(bps)	Número	Ancho de Banda Total
Municipalidad José Luis Bustamante y Rivero	VoIP	87.2K	3	261.6K
	Video	402M	1	402M
	Texto, Datos	186.67K	2	373.4K
	Internet	15M	1	15M
Total				417.23M
Comisaría José Luis Bustamante y Rivero	VoIP	87.2K	3	261.6K
	Video	402M	1	402M
	Texto, Datos	186.67K	2	373.4K
	Internet	15M	1	15
Total				417.23M
Comisaría Ciudad mi Trabajo	VoIP	87.2K	2	174.4K
	Video	402M	1	402M
	Texto, Datos	186.67K	1	186.67K
	Internet	15M	1	15M
Total				417.16M
Comisaría Simón Bolívar	VoIP	87.2K	2	174.4K
	Video	402M	1	402M

	Texto, Datos	186.67K	1	186.67K
	Internet	15M	1	15M
Total				417.16M

Fuente: Elaboración propia.

3.5 Proyecciones

Según los datos obtenidos en la tabla 15 se estima que por cada miembro perteneciente al punto de intercambio de tráfico se requiere un promedio de 417.2Mbps de ancho de banda para satisfacer sus necesidades y a un crecimiento a corto plazo del 25% de su capacidad actual se tiene que por miembro se requerirán 522Mbps de capacidad.

Los enlaces habilitados para el tipo de infraestructura que componen al punto de intercambio de tráfico son de no menor a 1Gbps satisfaciendo de esta forma su necesidad mínima y brindando un margen de expansión de crecimiento o uso inmediato.

En base a estos datos, el punto de intercambio de tráfico estará diseñado para satisfacer las necesidades cualquier jurisdicción de la ciudad de Arequipa entre la municipalidad y sus comisarías.

CAPÍTULO IV: METODOLOGÍA DE MEDICIÓN

4. Variables e instrumentos de medición

4.1 Latencia

Según Bradner (1991), se define como latencia en dispositivos de redes, al tiempo que transcurre desde que el primer bit de una trama sale en dirección a su destino hasta que el destino recibe ese primer bit de la trama.

Es un valor de tiempo medible originado del envió de un paquete desde un dispositivo hacia otro. Muchas aplicaciones dependen del tiempo de latencia para poder asegurar su funcionamiento y rendimiento.

4.2 Throughput

Según Bradner (1991), es la velocidad máxima que puede ofrecer un dispositivo, asegurando que durante su uso no se produzca ninguna clase de pérdidas en el enlace ni degradación de servicio. Es útil conocer el valor real de la velocidad que permite el dispositivo para poder comparar con los valores de pérdidas de tramas que se produzcan en el enlace.

Según Poretsky, Erramili, Perser y Khurana (2006), el throughput es el valor que asegura, que no exista un reenvió de paquetes a causa de una limitación de enlace generando pérdidas y sobre uso.

El throughput es la velocidad real que tiene un enlace, es decir, la capacidad real que se presenta al momento de transferir datos, asegurando que entre origen y destino no existan pérdida de paquetes que puedan originar problemas de recepción o reenvió de paquetes a partir de esta pérdida.

4.3 Pérdida de paquetes

Según Poretsky, Erramili, Perser y Khurana (2006), para que se produzca el desborde del buffer, el dispositivo tiene que sobrepasar su capacidad, un método determinista usado para determinar el momento antes de que se produzca este desborde es denominado congestión incipiente.

Según Poretsky, Erramili, Perser y Khurana (2006), cuando el buffer se encuentra saturado se produce un fenómeno denominado colapso de congestión, donde los paquetes que ingresen al buffer serán eliminados por no tener más espacio de almacenamiento, finalmente el fenómeno denominado congestión de reenvió, el cual es el factor de pérdida dentro del buffer saturado y se utiliza la pérdida de paquetes como como métrica para medir este factor.

Según Kurose y Ross (2017), la pérdida de paquetes se da cuando en una red, la interfaz física de un dispositivo recibe paquetes provenientes de un destino y al llegar a la interfaz de salida el buffer, se encuentra con paquetes en cola y además de eso, su espacio de buffer ya fue sobrepasado, dado esto, cualquier paquete que ingrese en el buffer será eliminado, hasta que el buffer se libere y pueda recibir más paquetes. Existen también otros tipos de retardo que pueden afectar una red, como los retardos de reenvió o transmisión.

Según Kurose y Ross (2017), clarifican el hecho, de que la performance con la que un dispositivo trabaje, es decir, la capacidad de almacenamiento de buffer va depender de factores como costo, diseño e implementación. Ya que un dispositivo con una capacidad más amplia de almacenamiento, no va asegurar una red libre de desbordamiento de paquetes, ya que existen temas como cantidad de tráfico que influyen directamente en esta pérdida de paquetes, por tanto, es un factor que se usa para medir el desenvolvimiento de una red.

Según Kurose y Ross (2017), en una topología de red, los dispositivos que originan paquetes hacia dispositivos que los van a recibir, pasan por dispositivos intermediarios que serán los encargados de determinar el camino correcto de los paquetes. Entre mayor sea la cantidad de paquetes que se vayan para procesar, los equipos tendrán una mayor carga de procesamiento para poder efectuar su tarea y a su vez sus interfaces se verán saturadas, los buffers de cada interfaz de dispositivo poseen un límite de almacenamiento de paquetes, al ser estos valores sobrepasados, se ocasionarán la pérdida de paquetes al no poder ser procesados por los equipos y provocando que el dispositivo de origen tenga que realizar reenvió de paquetes. Todo esto se refleja en un porcentaje de pérdida de paquetes que va indicar una variable que ayudara a definir el desempeño de la red.

En la figura 22 se muestran los tipos de retardo a los que están sujetos los paquetes al pasar de un origen a un destino.

Según Kurose y Ross (2017), el retardo de procesamiento estará ligado a los procesos que esté realizando el dispositivo al momento de recibir el paquete para su transmisión, el paquete es leído por el dispositivo y determina en el campo de la cabecera del protocolo de internet su dirección origen y destino. Este proceso puede tardar microsegundos dependiendo del dispositivo.

Según Kurose y Ross (2017), indica que el retardo de cola, está ligado a la pérdida de paquetes, ya que depende del almacenamiento del buffer al momento de transmitir un paquete, es decir, mientras más lleno se encuentre el buffer se tendrá un mayor retardo de procesamiento ya que el paquete tendrá que esperar a que los paquetes en fila ya existentes del buffer puedan ser enviados, para que este pueda ser por fin ser procesado por el dispositivo, el proceso toma tiempos de milisegundos.

Según Kurose y Ross (2017), el retardo de transmisión es el proceso de envió del paquete a través el dispositivo, con un manejo de envío de paquetes de tipo FIFO (First In First Out), es decir, el primero que entra es el primero que sale, el último paquete entrante tendrá que esperar su turno para ser enviado, esté posee tiempos de procesamiento entre los micro y milisegundos.

Según Kurose y Ross (2017), el retardo de propagación, este ligado al espacio físico por el cual se comunican los dispositivos, es el tiempo en el que un paquete se demora en llegar desde su origen a su destino. En medios cableados los tiempos serán menores, que en medios inalámbricos. La velocidad de propagación está en el rango de:

$$2 * 10^8\ m/s\ o\ 3 * 10^8\ \text{m/s}$$

Y finalmente el tiempo de propagación será la distancia entre los dispositivos origen y destino entre su velocidad de transmisión.

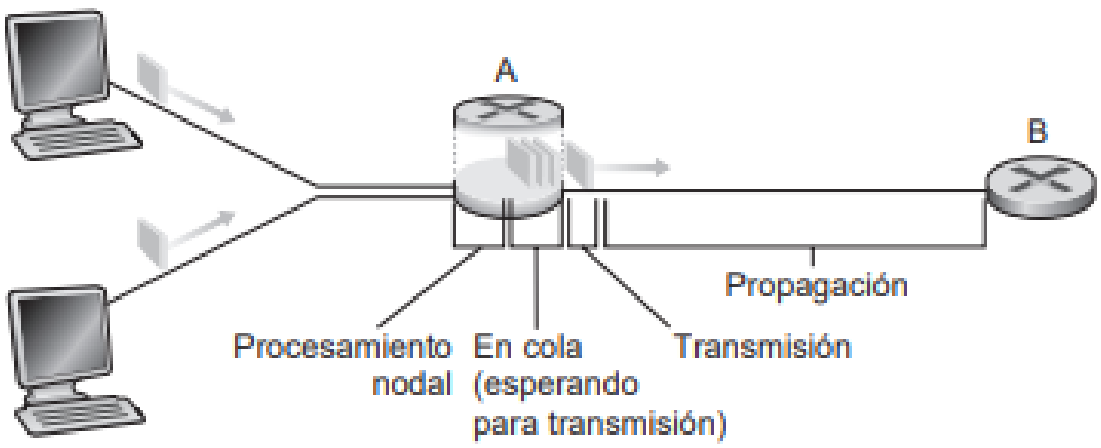


Figura 23. Tipos de Retardo.
Fuente: *Kurose y Ross (2017)*

4.4 Ping

Es una herramienta de troubleshooting que utiliza el protocolo ICMP para determinar discontinuidad en la red por medio de mensajes enviados entre origen y destino.

Una respuesta fructífera se da cuando el emisor envía un mensaje a su receptor y la respuesta del receptor llega sin problemas al emisor, de esta forma se confirma la conectividad entre ambos puntos.

Con la ayuda del protocolo ICMP, los dispositivos envían mensajes de Eco Request y Eco Reply, tanto de emisor como receptor respectivamente para confirmar la conectividad entre ellos.

Con esta herramienta, es posible medir el tiempo de redundancia de la red, pérdida de paquetes, porcentaje de pérdida de paquetes y latencias.

4.5 Wireshark

Según Wang, Xu y Yan (2010), Wireshark es una potente herramienta de acceso libre y código abierto la cual permite la resolución de problemas, análisis y desarrollo de protocolos dentro de una red por medio de análisis de paquetes.

Según Wang, Xu y Yan (2010), siendo una de las herramientas con mayor alcance y desarrollo, permitiendo tener opciones ventajosas sobre otras alternativas de similar uso.

Según Wang, Xu y Yan (2010), esta herramienta está disponible para sistemas operativos Linux y Windows. Al ser de código abierto, permite un alcance mayor entre los mejores desarrolladores de la comunidad permitiendo su constante evolución.

Según Wang, Xu y Yan (2010), como parte de la historia, el analizador de paquetes Wireshark inicia su desarrollo bajo el nombre de Ethereal, el cual es cambiado en el 2006 por Wireshark. Esta herramienta es de gran difusión entre los profesionales de redes por la versatilidad y manejo que brinda al usuario y por los alcances que permite en el análisis de paquetes TCP/UDP, pudiendo ser utilizada desde un aspecto educacional hasta profesional.

CAPÍTULO V: HERRAMIENTAS DE IMPLEMENTACIÓN

5. Hardware y Software

5.1 Mikrotik

5.1.1 Perfil

Según SIA Mikrotīkls (2021), Mikrotik es una empresa desarrolladora de software y hardware desempeñada en el rubro de las redes y telecomunicaciones, ofreciendo equipos de administración de redes y enrutamiento, bajo el concepto de fácil manejo y administración de equipos con soluciones aptas para el desarrollo de proyectos desde usuarios finales hasta proveedores de servicio de internet (ISP) teniendo un alcance a nivel mundial para la compra y venta de productos.

Mikrotik es una empresa conocida por los router y switch ofrecidos dentro de su catálogo, estos productos no solo cuentan con la parte hardware, sino que trabajan su propia versión software para el desarrollo de su equipamiento. De gran reconocimiento a nivel mundial, Mikrotik compite con otros grandes proveedores de similar mercado para el desarrollo de proyectos de redes, como por ejemplo empresas, domicilios hasta proveedores de servicio de internet.

5.1.2 Historia

Según SIA Mikrotīkls (2021), Mikrotik fue fundada en la capital de Latvia, Riga en el año 1995 con la visión de brindar proyectos de desarrollo para soluciones de proveedores de servicio de internet inalámbrico (WISP). Como primera etapa tuvo el desarrollo de software propietario dirigido a soluciones de enrutamiento basadas en Intel en el año 1997, en el año 2002 lanza su propio hardware con el software embebido denomino RouterBoard. Actualmente se distribuye en 145 países alrededor del mundo tal como se ve en la figura 23.

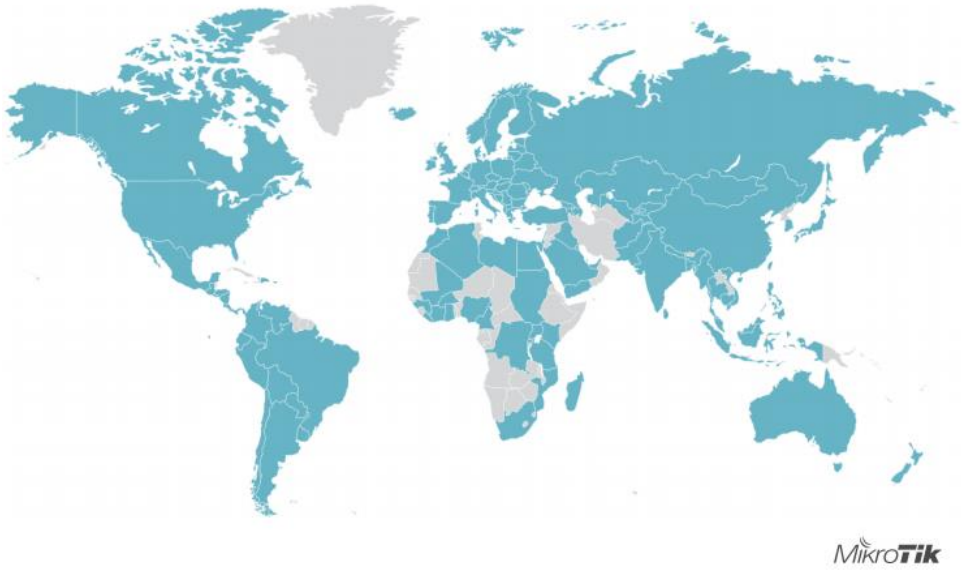


Figura 24. Disponibilidad de equipos Mikrotik en el mundo.
Fuente: *SIA Mikrotīkls (2021)*

5.1.3 Mum

Según SIA Mikrotīkls (2021), el Mikrotik User Meeting (MUM), es un evento organizado por la compañía Mikrotik, sobre temas del sistema operativo RouterOS y el hardware RouterBoard. Realizado en diferentes partes del mundo contando con más de 150 reuniones en su haber, tuvo como mayor cantidad de asistentes la presencia de 3000 personas en un evento. También conto con más de 145 representantes de empresas los cuales tuvieron a su cargo presentaciones y participaciones en el evento.

Según SIA Mikrotīkls (2021), la empresa tiene como finalidad presentar temas de interés desarrollados por especialistas sobre la tecnología y proyectos que involucren los productos Mikrotik, sobre temas actuales y de interés para los diferentes asistentes y usuarios de la marca.

Según SIA Mikrotīkls (2021), Mikrotik desarrolla eventos con el fin de incentivar la investigación y aplicaciones de temas de redes enfocadas a routing y switching. Estos eventos son llamados Mum (Mikrotik User Meetings), se dan en diferentes países y

buscan crear lazos y conocimiento entre los distintos usuarios de esta tecnología compartiendo conocimiento y desarrollando el interés por la marca y las nuevas tecnologías.

5.1.3.1 Mum Perú

Como parte de los eventos organizados por la empresa Mikrotik, Latinoamérica cuenta con eventos desarrollados durante el año en diferentes países. En Perú, hasta la fecha se han organizado 2 Mum, en el año 2016 y en el año 2019.

5.1.4 Mikrotik RouterOs y SwitchOs

Según SIA Mikrotīkls (2021), Mikrotik desarrollo un software propietario denominad RouterOS, el cual puede funcionar en un entorno de PC común o en el hardware desarrollado por Mikrotik denominado RouterBoard.

Este software cuenta con soporte en diferentes protocolos utilizados en redes. A continuación, se nombran algunos de los protocolos soportados por RouterOS.

- Soporte 802.11a/b/g/n/ac
- Calidad de Servicio (QoS)
- Túneles y firewall
- Hotspot
- Protocolos de enrutamiento: RIP, OSPF, BGP, MPLS
- Acceso remoto con WinBox, GUI e interfaz Web
- Alta disponibilidad con VRRP
- Interfaces Bonding
- Telnet, mac-telnet, ssh, consola
- Configuración y monitoreo en tiempo real

- Soporte OpenFlow

El software RouterOS está enfocado en una configuración de equipos enrutadores y existe un software diseñado para la configuración de switch denominado SwitchOS, este varia en su forma de configuración ya que presenta una interfaz netamente gráfica en un entorno web.

Los Switch de la marca Mikrotik, permiten ser configurados desde cualquiera de estos dos softwares, basta con cambiar dentro de su configuración el software con el que se quiera trabajar.

A continuación, se muestran las figuras 24 y 25 con los entornos de configuración de RouterOS y SwitchOS.

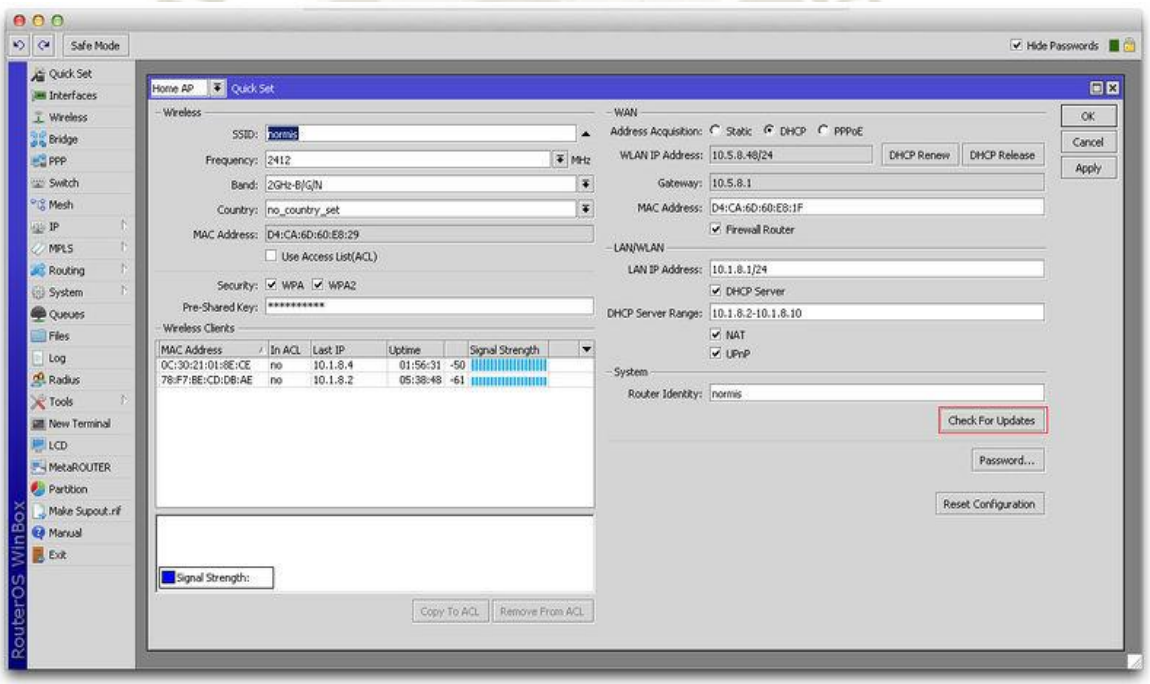


Figura 25. Interfaz WinBox RouterOS.
Fuente: SIA Mikrotīkls (2020)

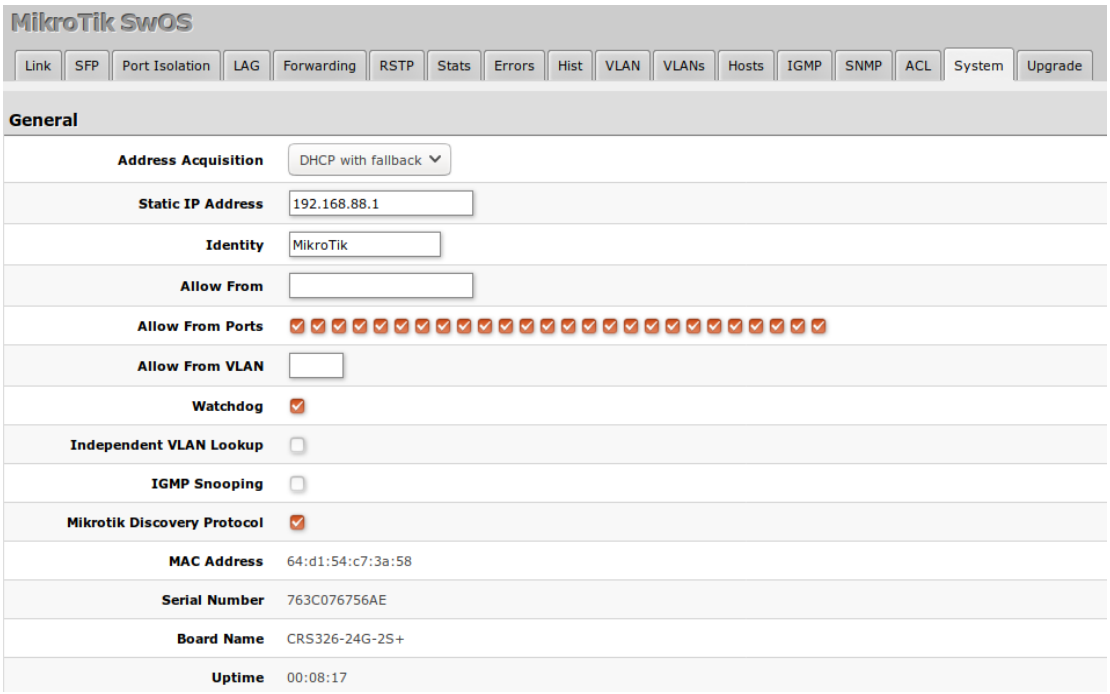


Figura 26. Interfaz Web SwitchOS.
Fuente: *SIA Mikrotīkls (2020)*

5.1.4.1 Niveles de Licenciamiento

Según SIA Mikrotīkls (2021), el software propietario de Mikrotik RouterOS, cuenta con diferentes niveles de licenciamiento, estos niveles van a depender de las características que se tengan, como por ejemplo la cantidad de Vlans, VPN del tipo PPTP, L2TP, etc. Entre mayor sea su nivel de licenciamiento mayor será su costo de adquisición. Pero se cuentan con demos de prueba de las licencias para que puedan ser probadas por los usuarios.

A continuación, se presenta mayor detalle de las licencias en la figura 26.

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	do not sell	$45	$95	$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Figura 27. Cuadro de Niveles de Licencia.
Fuente: *SIA Mikrotīkls (2020)*

5.1.5 Herramientas de gestión y configuración

Mikrotik cuenta con un gran número de interfaces de configuración para sus equipos, desde un terminal de conexión común de ingreso por SSH o telnet, hasta herramientas propietarias como se presentan a continuación.

5.1.5.1 WinBox

Según SIA Mikrotīkls (2019), WinBox es una interfaz gráfica de usuario (GUI), la cual permite configurar y monitorear equipos con RouterOS, de simple y perceptible manejo, permite funciones generales para el manejo del equipo, existiendo ciertas configuraciones no habilitadas por la interfaz GUI, pero si desde una interfaz de consola. Diseñada para trabajar sobre sistemas operativos Windows, también presenta la aplicación para sistemas operativos MacOS y Linux.

En la figura 27 se muestra la interfaz WinBox de un equipo Mikrotik.

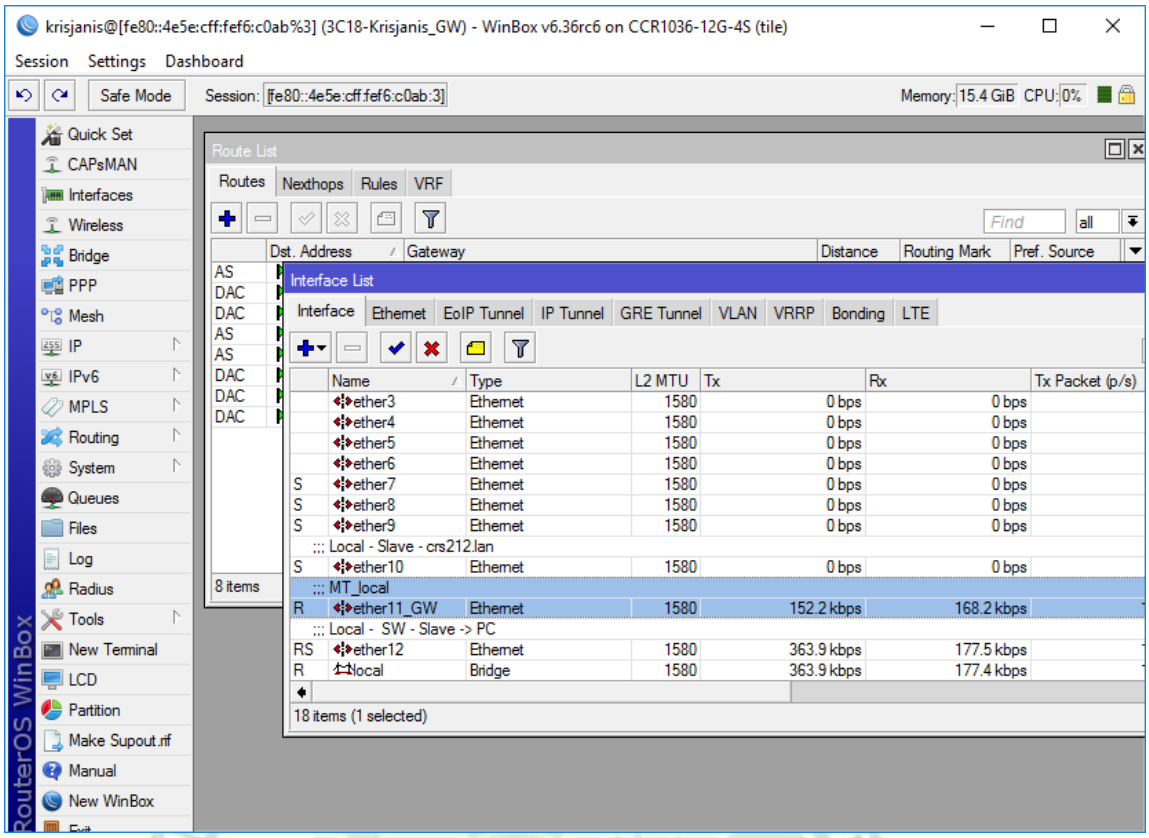


Figura 28. WinBox Mikrotik.
Fuente: *SIA Mikrotīkls (2019)*

5.1.5.2 Configuración por Web

Según SIA Mikrotīkls (2019), la interfaz WebFig es una interfaz Web que brinda Mikrotik con las características de configuración presentadas en WinBox, esta interfaz tiene el mismo nivel de configuración de WinBox, lo que le permite realizar configuración, monitoreo y resolución de problemas en un equipo.

En la figura 28 se muestra la interfaz WebFig de Mikrotik para la configuración y monitoreo de equipos.

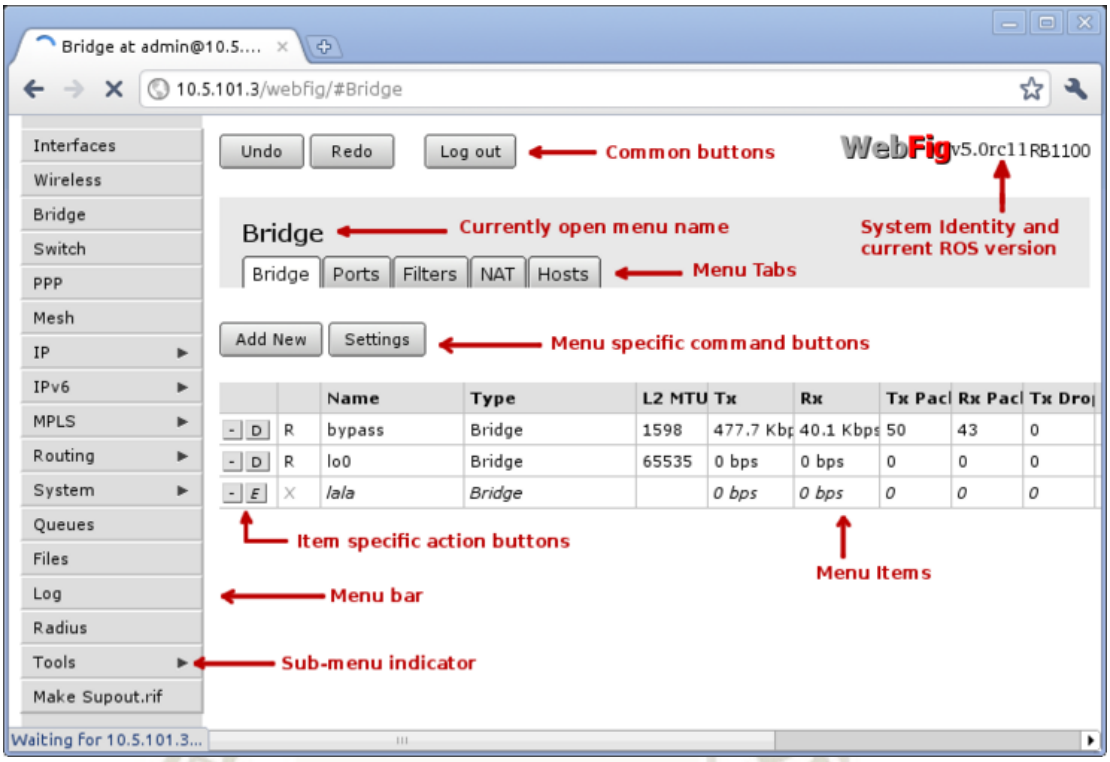


Figura 29. WebFig Mikrotik.
Fuente: *SIA Mikrotīkls (2019)*

La interfaz Web permite personalizar la pantalla para que puedan utilizarla diferentes usuarios según el nivel de administración del equipo.

5.1.5.3 Aplicación Móvil

Según SIA Mikrotīkls (2021), la aplicación móvil creada por Mikrotik para los teléfonos inteligentes está presente en versiones tanto para Android como para iOS, permite al usuario configurar de forma básica principales características del dispositivo y permite también realizar configuraciones más avanzadas para usuarios con un mayor nivel de experiencia. La aplicación permite realizar trabajos de monitoreo de campo para determinar estado de equipos entre otras funciones.

En la figura 29 se muestra la interfaz de la aplicación móvil de Mikrotik para sus dispositivos.

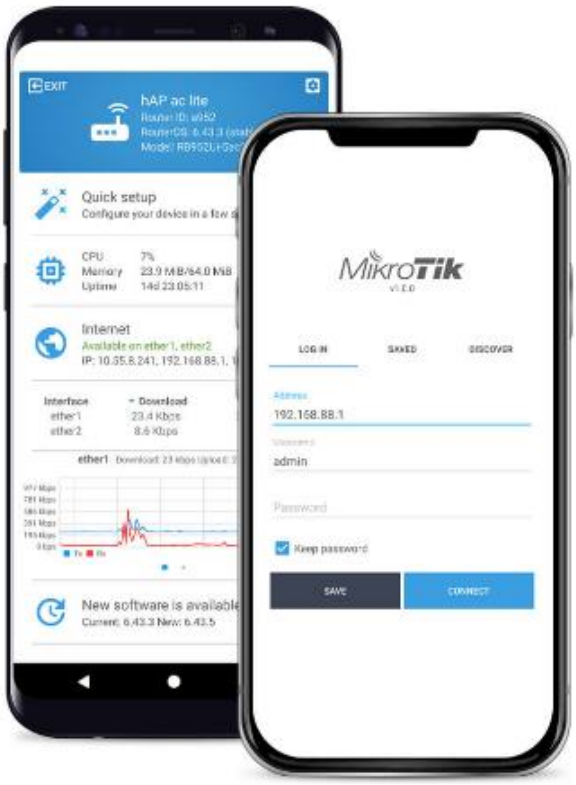


Figura 30. Aplicación Móvil.
Fuente: *SIA Mikrotīkls (2021)*

5.1.5.4 Dude

Según SIA Mikrotīkls (2017), The Dude es un aplicativo sin costo presentado por Mikrotik como una alternativa de monitoreo y configuración masivo de red. Tiene la posibilidad de realizar escaneos de red basado en búsquedas por redes y realizar gráficas tentativas de la interconexión existente entre los dispositivos.

En la figura 30 se muestra como The Dude grafica de forma tentativa la red del usuario mostrando enlaces y otros parámetros de red.

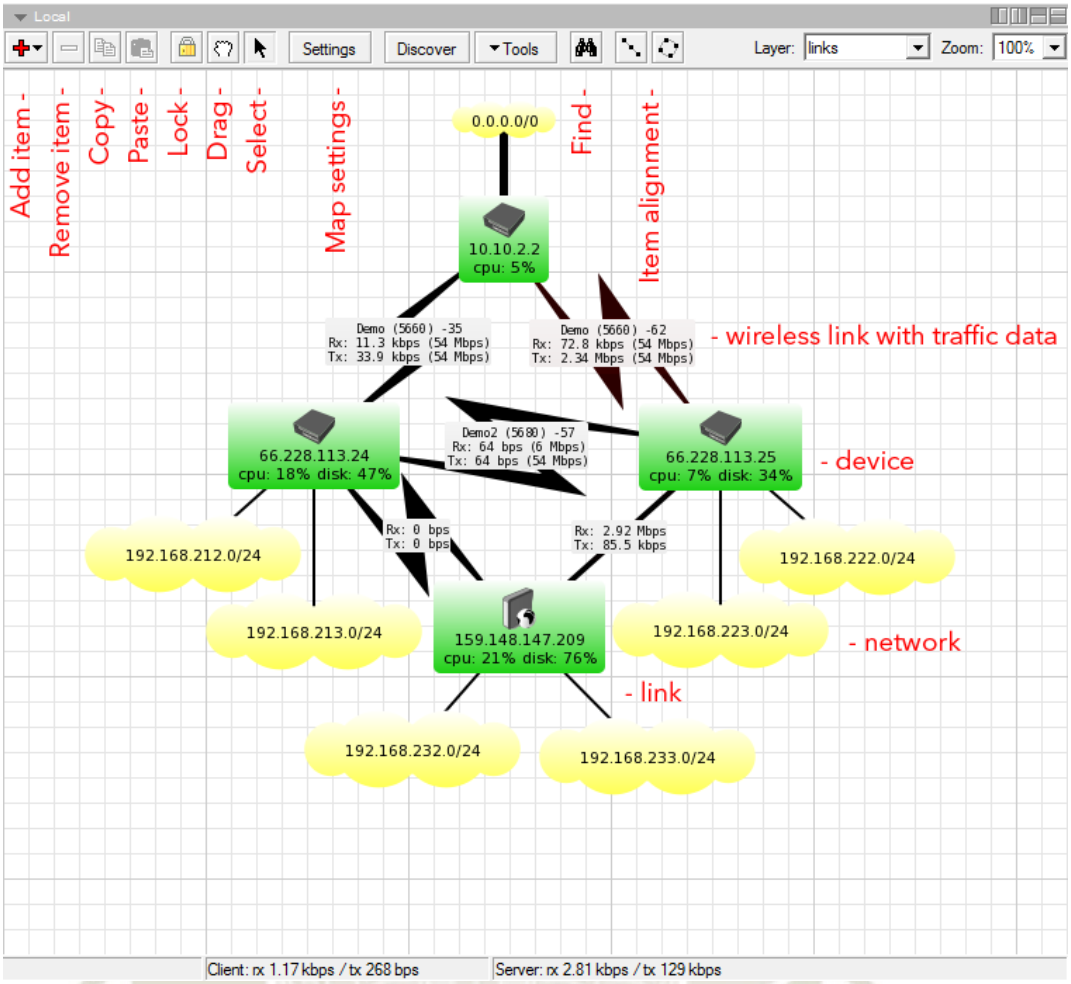


Figura 31. Dude Mikrotik.
Fuente: *SIA Mikrotīkls (2017)*

The Dude, permite realizar una estación de monitoreo en tiempo real de la red, basado en protocolo snmp lo cual permite visualizar el tráfico entre las interfaces, niveles de CPU, memoria, entre otros parámetros para garantizar la buena performance del sistema.

The dude cuenta con un aplicativo el cual se conecta al servidor y obtiene toda la información de los dispositivos. El servidor puede ser configurado en una PC descargando el software de Mikrotik o puede ser utilizado desde un RouterBoard, Mikrotik cuenta con equipos específicos para este tipo de aplicativo como por ejemplo el RB110AHx4 DUDE Edition.

5.2 VMware Workstation

Como entorno de virtualización usaremos VMware Workstation 16 Player, el cual nos permite bajo el uso no comercial, poder agregar maquinas virtual sin necesidad de licencia o costo.

Pero sin la posibilidad de poder manipular los parámetros por defecto con los que trabajan las máquinas virtuales a importar.

Primero deberemos descargar el instalador de VMware Workstation 16 Player en la página oficial la cual es https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html.

Una vez descargada la versión 16.1.1 obtendremos un ejecutable .exe que contiene el programa a instalar.

En la figura 27 vemos el ejecutable que se descarga de la página principal.

Figura 32. Instalador VMware-player 16.1.1
Fuente: Elaboración propia.

Debemos ejecutar ese programa para empezar con la instalación de VMware.

En la figura 32, se muestra la preparación para la instalación del software en nuestra PC.

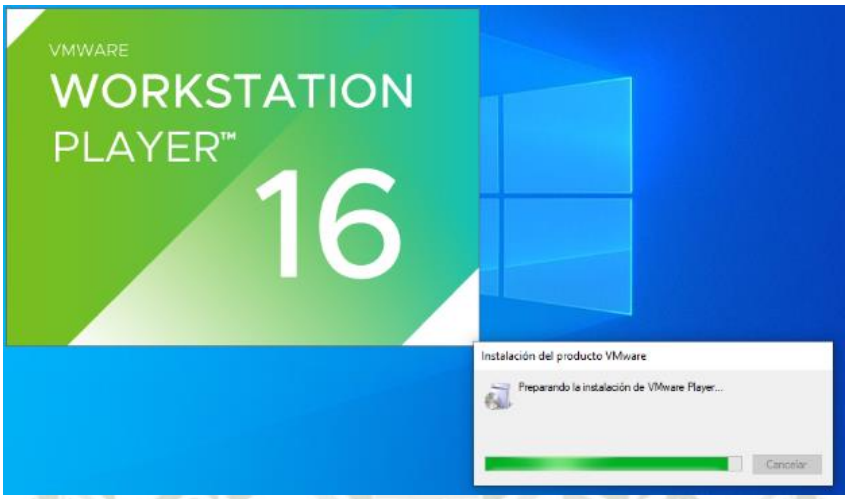


Figura 33. Preparación para la instalación de VMware Workstation Player 16.
Fuente: Elaboración propia.

Los pasos siguientes son de carácter intuitivo, ya que solo requieren seguir las instrucciones consecutivas sin ningún proceso que requiera mayor análisis.

En las Figuras 33, 34 y 35 se muestra el proceso de instalación de VMware Workstation Player.

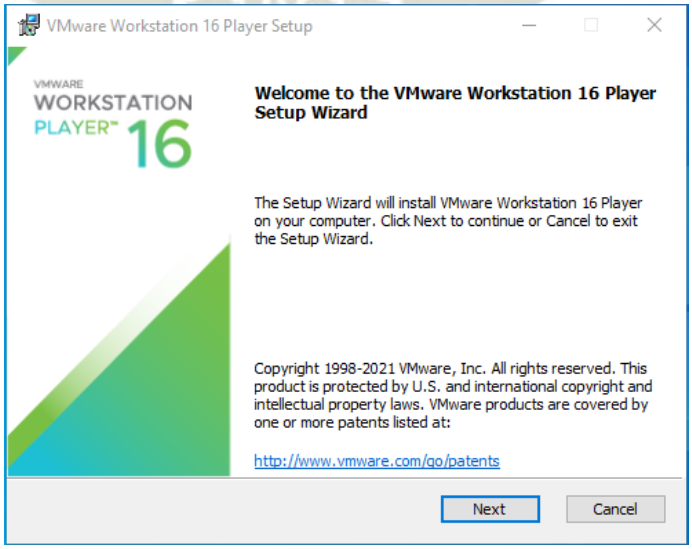


Figura 34. Instalación de VMware Workstation.
Fuente: Elaboración propia.

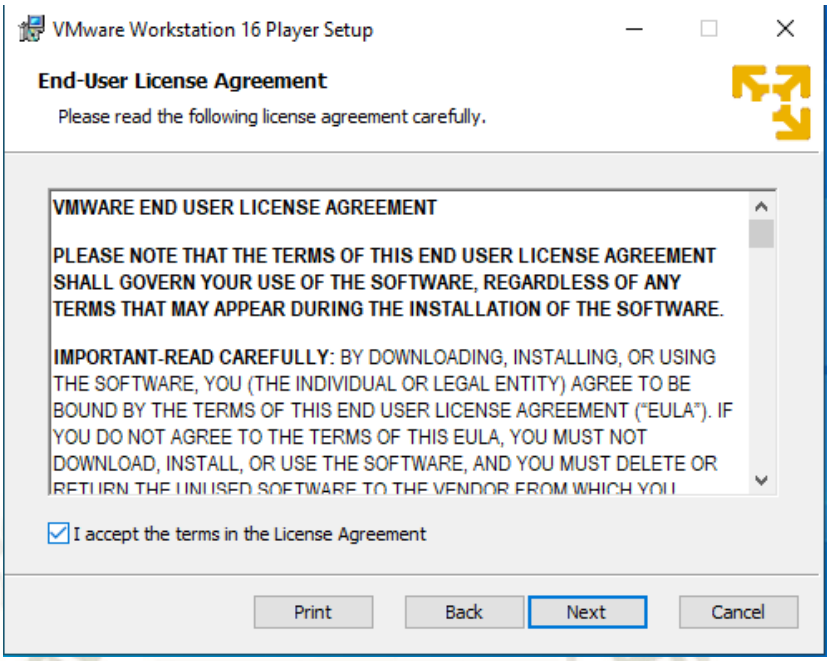


Figura 35. Términos y condiciones de la instalación.
Fuente: Elaboración propia.

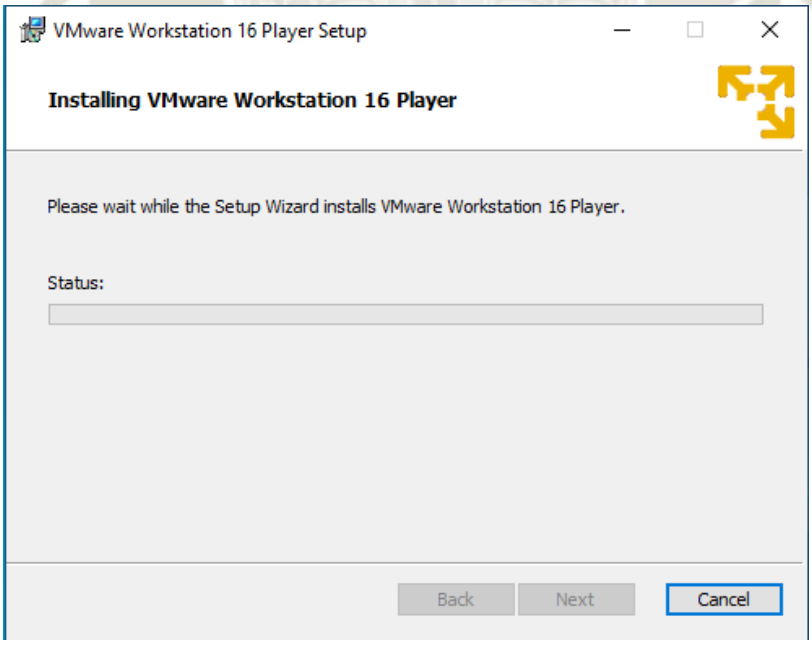


Figura 36. Proceso de instalación de VMware Workstation 16 Player.
Fuente: Elaboración propia.

Terminado todo este proceso, la instalación está concluida y como resultado, obtenemos la figura 36.

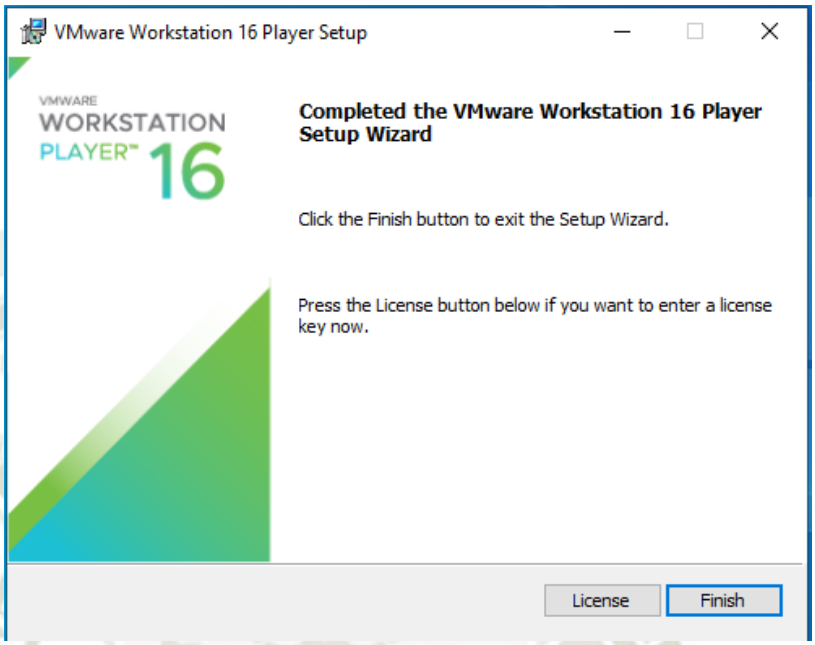


Figura 37. Instalación finalizada.
Fuente: Elaboración propia.

5.3 PNETLab

5.3.1 Perfil

De siglas Packet Network Emulator Tool Lab, PNETLAB es una alternativa para el diseño y emulación de dispositivos de red con el fin de analizar distintos modelos de red y ejecutar alternativas de modelamiento para una posible implementación en dispositivos reales.

Junto a otros softwares que presentan la posibilidad de simular o emular redes de comunicaciones como, Packet Tracer, Kiva, Netsim, GNS3, entre otros, PNETLab permite la interoperabilidad entre dispositivos de diferentes marcas basado en el IOS de cada dispositivo en una misma plataforma.

Según PNET (2021), PNETLab es un entorno de emulación que forma una comunidad entre los miembros que desarrollan proyectos dentro de este emulador.

Posee dos formas de trabajo denominados “PNETLab Box”, así como una tienda denominada “PNETLab Store” para poder adquirir diferentes laboratorios, herramientas de análisis, Dockers, base de datos, entre otros. Con material realizado o subido por otros miembros; estos productos pueden ser de forma gratuita o de pago.

Dentro de las formas de trabajo, existe un modelo Online el cual permite la interacción y adquisición de los laboratorios colgados en la plataforma de PNETLab. Esa es la única opción para poder acceder al PNETLab Store.

Y una opción Offline, la cual no interconecta con la plataforma de PNETLab Store.

Estas dos opciones de trabajo vienen embebidas dentro de la máquina virtual que contiene PNETLab.

Con la configuración e instalación de PNETLab se crea un usuario en el modo Online y un usuario por defecto para el modo Offline.

A continuación, en la figura 37 se muestra la pantalla principal de PNETLab en la cual se aprecian los laboratorios disponibles, opciones de cuenta, sistema, entre otros.

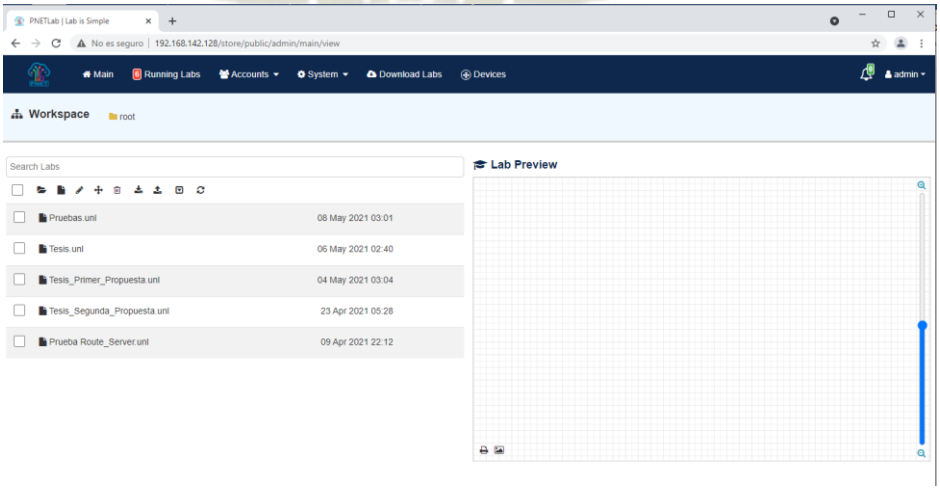


Figura 38. Pantalla principal PNETLab.
Fuente: Elaboración propia.

5.3.2 Características

Según PNET (2021), el emulador PNETLab presenta las siguientes características:

- Software de adquisición libre.
- Versión Offline.
- Tienda de dispositivos y laboratorios.
- Dockers integrados.
- Imágenes de sistemas operativos de diferentes marcas.
- Administración de usuarios por cuenta.
- Wireshark.
- Telnet, entre otros.

5.3.3 Requerimientos del sistema

Los requerimientos del sistema para poder garantizar el correcto funcionamiento del servidor son:

- Memoria Ram: 2 GB - 8 GB
- Procesadores: 4
- Disco Duro: 100GB
- Adoptador de Red: Nat
- Adaptador 2 de red: Bridge

Estos parámetros son resumidos en la figura 38 mostrada a continuación.

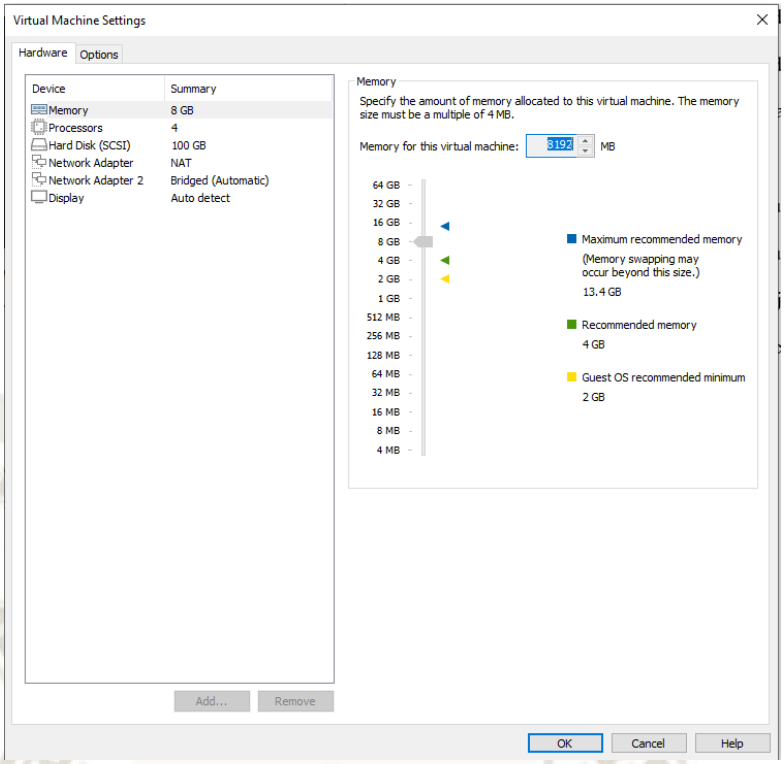


Figura 39. Requerimientos de la máquina virtual para PNETLab.
Fuente: Elaboración propia.

Al trabajar con una versión gratuita de VMware no se permite realizar cambios en los valores de los parámetros dados por defecto en la máquina virtual.

De tal forma, que los parámetros visualizados en la figura anterior son los parámetros que vienen por defecto en la máquina virtual descargada de PNETLab.

5.3.4 Instalación y configuración del emulador PNETLab

5.3.4.1 Proceso de Instalación

En la siguiente sección se procederá a enlistar los pasos requeridos para la instalación y configuración del emulador PNETLab en el sistema operativo Windows 10.

Los pasos para su instalación son de forma simple y sin mayor dificultad ya que cuenta con menús de instalación de fácil percepción.

Al ser un software libre, no requiere un costo, solo deberá ingresar a la web oficial de PNETLab e ir a la sección descargas para poder adquirir la máquina virtual que

contiene el software. La página oficial para la descarga del software es pnetlab.com/pages/download.

Seleccionar la fuente de descarga la cual puede ser Google Drive o Mega según convenga.

En la figura 39 se muestra las diferentes opciones existentes para la descarga de la máquina virtual que contiene el software PNETLab.

Link Download	MD5 Checksum	Size
Link Download PNET 4.2.10 Google Drive		2G
Link Download PNET 4.2.10 Google Drive (Backup 1)		2G
Link Download PNET 4.2.10 Mega (Backup 2)		2G

Figura 40. Descarga de la máquina virtual de PNETLab.
Fuente: https://pnetlab.com/pages/download

Se descargará una máquina virtual denominada PNET_X.Y.ova en la cual X y representan la versión descargada y ". OVA" la extensión de la máquina virtual, la cual podrá ser importada a un entorno de virtualización.

En la figura 40, se muestra la máquina virtual descargada desde la web principal.

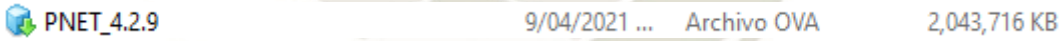


Figura 41. Máquina virtual de extensión ". OVA", descargada desde la web de PNETLab.
Fuente: Elaboración propia.

5.3.4.1.1 Instalación de PNETLab

La instalación de PNETLab se basa en la importación de la máquina virtual descargada anteriormente en un entorno de virtualización para poder ejecutarlo.

Para nuestro caso, el software VMware Workstation Player 16.1.1 en el cual realizaremos la importación de la máquina virtual.

Nos pedirá nombrar la nueva máquina virtual a importar y el directorio de ejecución.

Se ejecutará como se muestra en la figura 41.

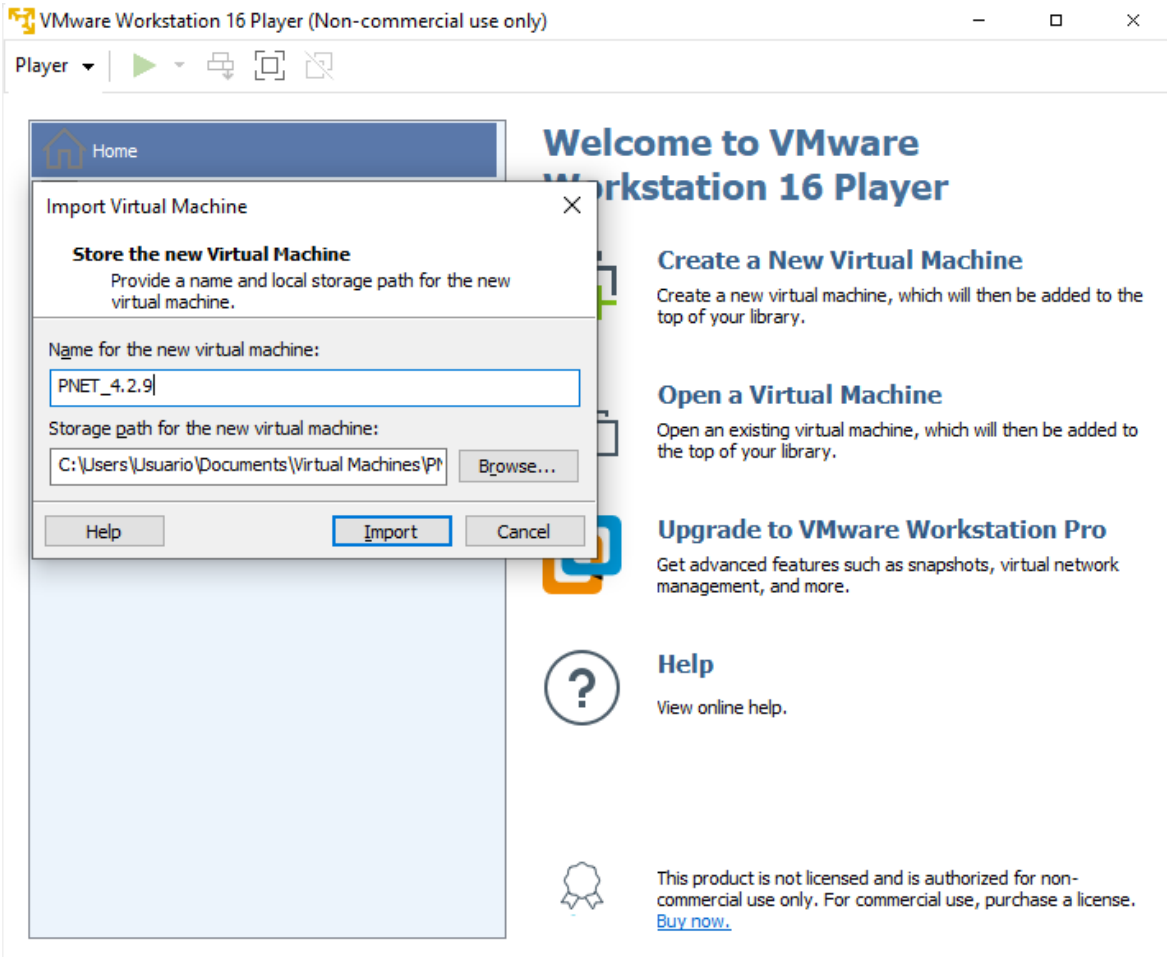


Figura 42. Importar la máquina virtual a VMware Workstation Player.
Fuente: Elaboración propia.

Una vez seleccionada y nombrada la máquina virtual deberá seleccionarse la opción “import” y se procederá a importar los datos de la máquina virtual al directorio seleccionado.

Una vez finalizado el proceso de importación de la máquina virtual obtendremos la figura 42.

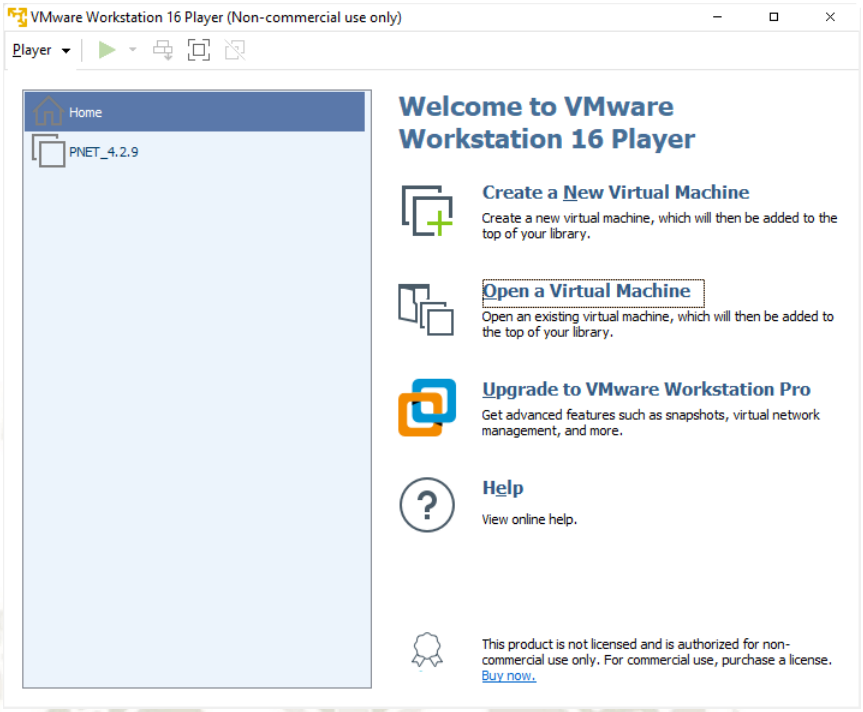


Figura 43. Máquina Virtual importada en el entorno de VMware.
Fuente: Elaboración propia.

Es importante verificar que este activada la opción de virtualización en la máquina virtual, tal como la muestra la figura 43.

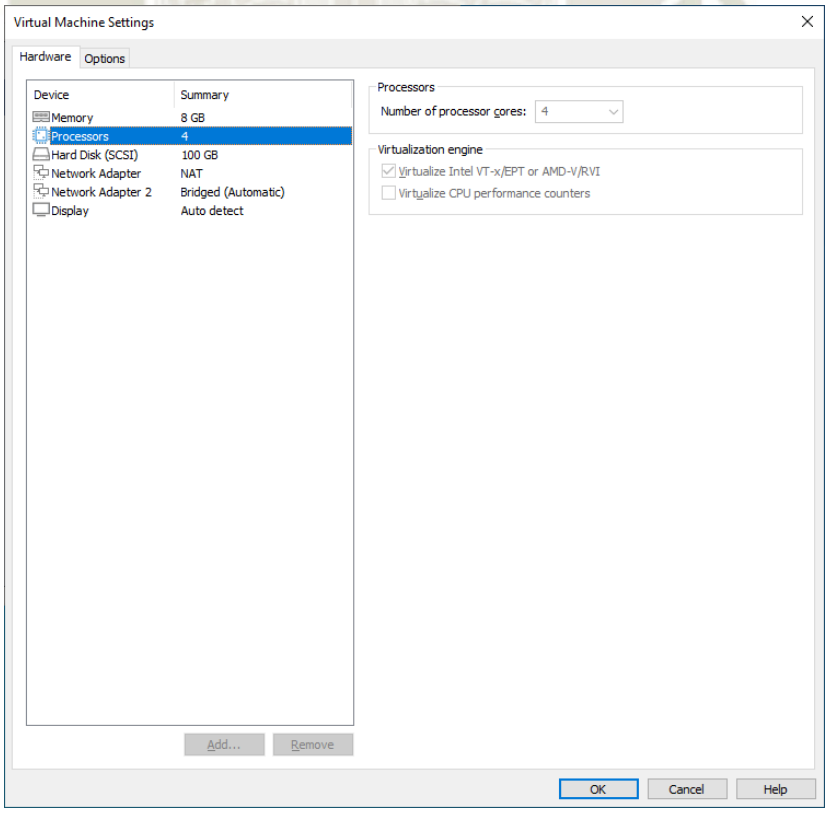


Figura 44. Opción de Virtualización habilitada.
Fuente: Elaboración propia.

Se procederá a encender la máquina virtual, una vez encendida la máquina virtual mostrará una pantalla negra con la información de acceso al emulador PNETLab, el proceso de ejecución no requiere ningún paso adicional ya que consta solo de prender la máquina virtual.

En la figura 44, mostramos la pantalla de acceso, los usuarios propuestos para poder ingresar a la configuración de la máquina virtual y la IP para poder acceder al emulador desde la web.

Figura 45. Pantalla de acceso e IP de ingreso al software.
Fuente: Elaboración propia

En la figura 45 se muestra la pantalla de inicio luego de ingresar a la máquina virtual de PNETLab.

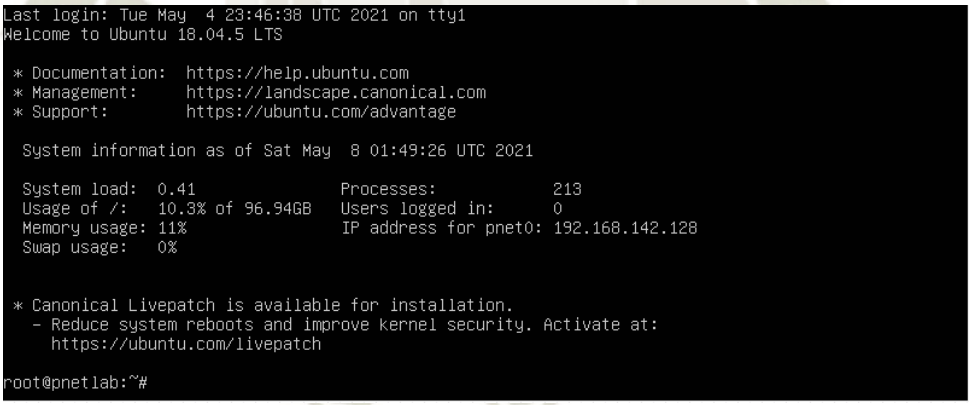


Figura 46. Pantalla de inicio máquina virtual PNETLAB.
Fuente: Elaboración propia.

En la figura 46 se muestra la pantalla inicial de PNETLab al ingresar por web con la IP 192.168.142.128, la cual es mostrada en la figura anterior.

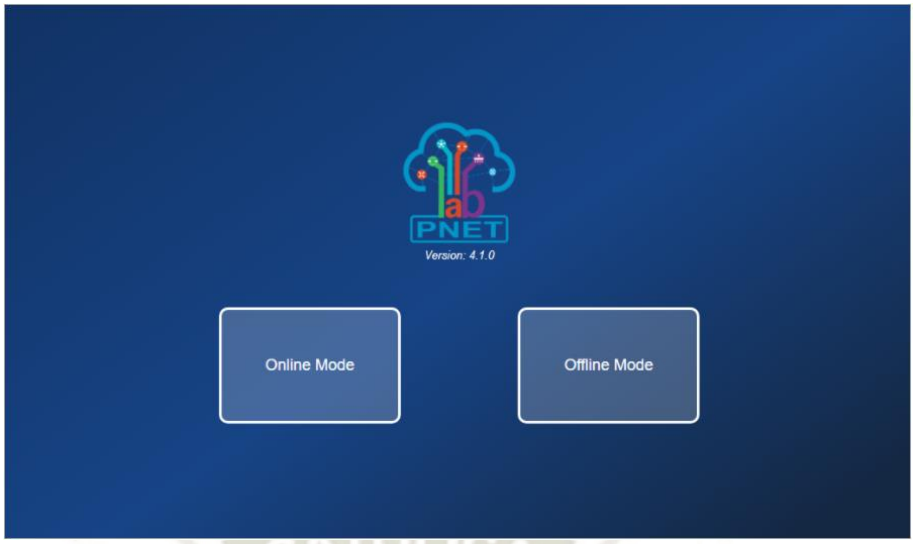


Figura 47. Pantalla de inicio máquina virtual PNETLAB.
Fuente: https://pnetlab.com/pages/download

5.3.4.1.2 Instalación de la Imagen del Sistema Operativo de Mikrotik

Para poder trabajar con Mikrotik en el entorno de PNETLab, debemos utilizar el QEMU disponible en la web oficial de Mikrotik, para cargar ahí la imagen del sistema operativo de Mikrotik.

Como primera etapa, se deberá ingresar a la zona de descargas de la página oficial de Mikrotik, www.mikrotik.com/download y buscar el área “Cloud Hosted Router”, en esa sección buscar el archivo descargable de nombre “Raw disk image” en la versión long-term.

La versión Long-term que es la versión libre de errores de Mikrotik o denominada a largo plazo, la versión Stable es una versión actual de Mikrotik donde es posible que aún se presenten errores, también existen versiones beta de testeo utilizadas para desarrolladores que deseen experimentar con nuevas herramientas que pudiera habilitar Mikrotik, pero esta versión contiene errores y no es recomendable usarla para equipos en redes en funcionamiento.

En la figura 47 se muestra la zona de descarga de la imagen de Mikrotik, para este caso se utilizará la versión Long-Term, al ser la versión de Mikrotik que no presenta errores.

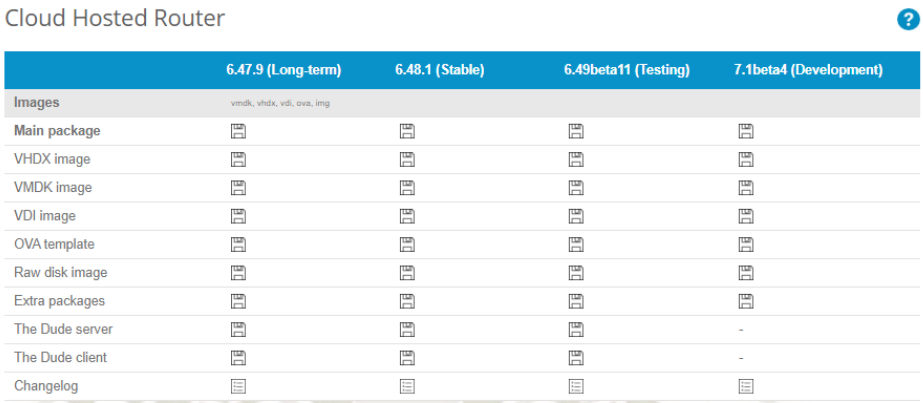


Figura 48. Web Mikrotik para la descarga de Imagen de RouterOs.
Fuente: https://mikrotik.com/download

En la figura 48, se muestra la descarga del archivo que estará en formato comprimido desde la página web mencionada anteriormente, corresponderá a la versión 6.47.9 y tendrá por nombre chr-6.47.9.img.zIP.

Este archivo deberá ser descomprimido para su uso.

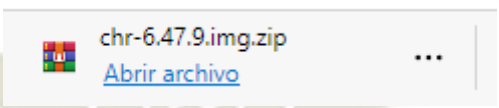


Figura 49. Descarga de Imagen Mikrotik.
Fuente: Elaboración propia.

El proceso para cargar esta imagen en el PNETLab se describe en las siguientes figuras.

Deberá ingresar por SSH a la máquina virtual con la IP mostrada en figuras anteriores.

Se ingresó por la consola a la máquina virtual, tal como lo muestra la Figura 49.

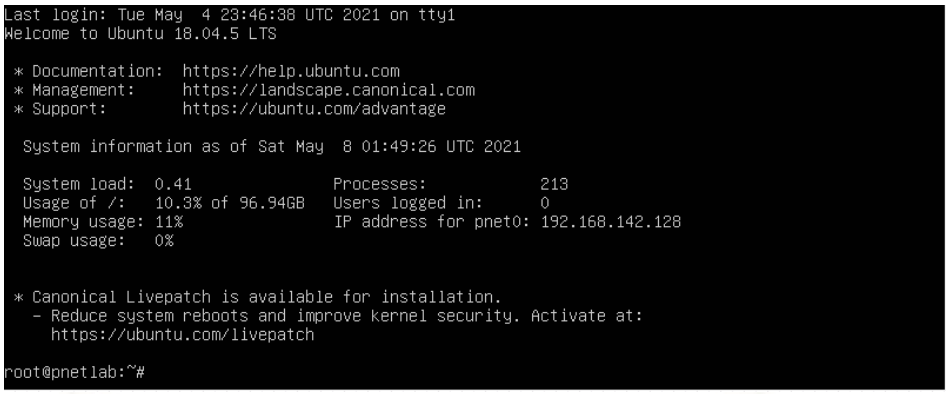


Figura 50. Pantalla de inicio de máquina virtual PNETLAB, desde consola.
Fuente: Elaboración propia.

Dentro de la consola de la máquina virtual deberá crearse una carpeta para la imagen del Mikrotik dentro de la carpeta de los Qemu.

La creación de la carpeta esta presentada en la figura 50.

```
root@pnetlab:~# cd /opt/unetlab/addons/qemu/mikrotik-6.47.9/
```

Figura 51. Creación de carpeta para Mikrotik en la máquina virtual.
Fuente: Elaboración propia.

Con ayuda del software WinSCP ingresamos a carpeta creada y dentro de esa carpeta subimos la imagen del Mikrotik descargada con anterioridad.

En la venta de WinSCP bastará con arrastrar la imagen a la carpeta deseada.

En la figura 51 se muestra la carpeta creada en la máquina virtual a la derecha y la imagen de Mikrotik a la izquierda.

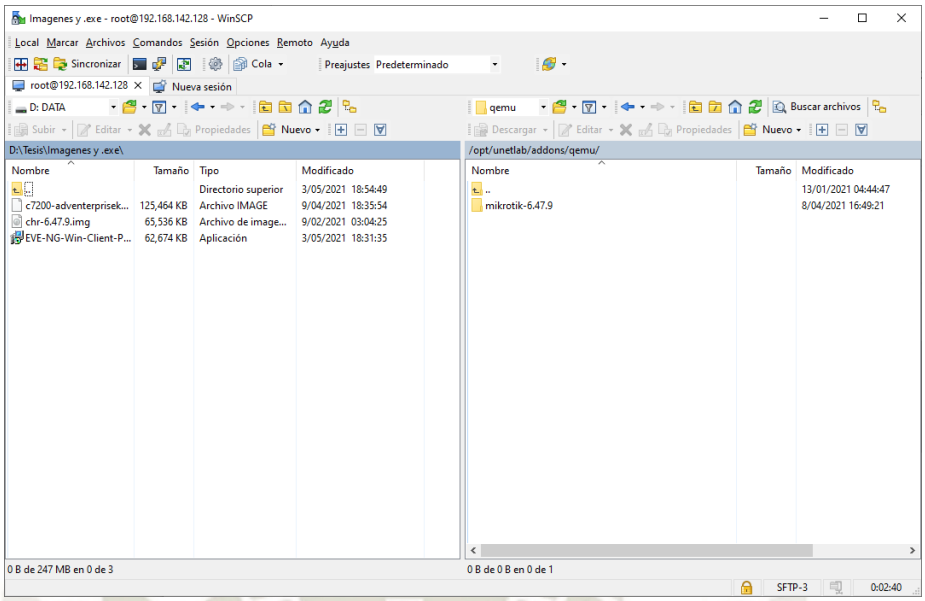


Figura 52. Creación de carpeta para Mikrotik en la máquina virtual y visualización de imagen a subir.
Fuente: Elaboración propia.

Una vez que se ha subido la imagen a la carpeta creada, deberá cambiarse el tipo de extensión y nombre para que pueda ser reconocida por PNETLab.

El cambio de nombre y extensión se muestra en la figura 52.

```
root@pnetlab:~# mv chr-6.47.9.img hda.qcow2_
```

Figura 53. Cambio de nombre y extensión de la imagen subida a la carpeta creada en la máquina virtual.
Fuente: Elaboración propia.

Finalmente deben actualizarse los permisos para que puedan usarse las imágenes subidas sin ningún problema. Los comandos para esto están presentados en la figura 53.

```
root@pnetlab:~# /opt/unetlab/wrappers/unl_wrapper -a fixpermissions
```

Figura 54. Actualización de permisos en la máquina virtual.
Fuente: Elaboración propia.

Ingresando a la carpeta creada en los primeros pasos, visualizaremos la imagen del Mikrotik con el nombre que cambiamos.

En la figura 54, se muestra el resultado de esto.

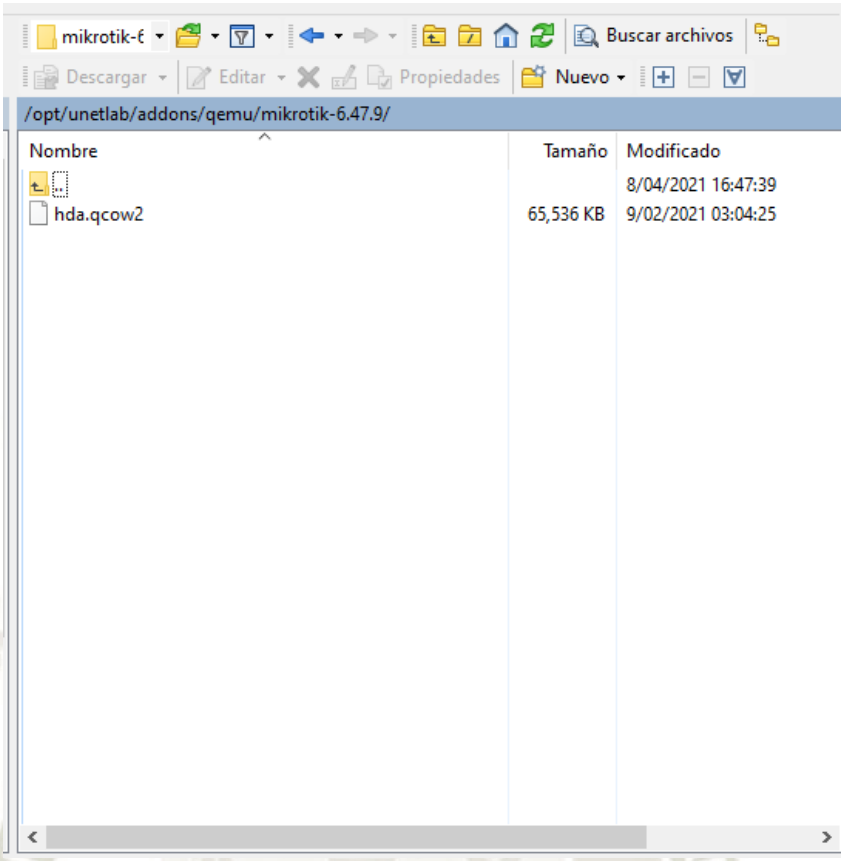


Figura 55. Visualización de la imagen de Mikrotik configurada y editada para su uso. Fuente: Elaboración propia.

5.3.4.1.3 Instalación IOS Cisco

Para poder trabajar con dispositivos Cisco dentro del entorno PNETLab, al igual que con Mikrotik es necesario incluir la imagen del dispositivo Cisco en el entorno de PNETLab.

Como primer paso, debemos seleccionar el tipo de dispositivo y su imagen correspondiente.

Para nuestro caso, usaremos la imagen del router cisco c7200.

Realizamos la descarga de la imagen desde la web: www.telectronika.com/descargas/cisco-imagenes-ios-para-gns3-dynamIPs-y-vm/.

Y buscaremos el sistema operativo del router cisco C7200.

El archivo descargado mostrado es un tipo .bin, el cual se muestra en la figura 55, y es necesario modificarlo a una extensión “. image” para poder hacer uso de él dentro del emulador PNETLab.

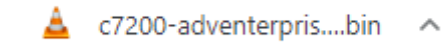


Figura 56. Imagen del sistema operativo del router cisco C7200 con la extensión .bin
Fuente: Elaboración propia.

Una vez modificado el iOS de cisco a la extensión “. image” obtendremos el resultado de la figura 56.

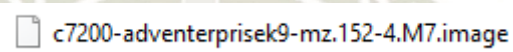


Figura 57. Imagen del sistema operativo del router cisco C7200 con la extensión “. image”.
Fuente: Elaboración propia.

Finalmente, procedemos a subir la imagen al directorio “/opt/unetlab/addons/dynamIPs/” en la máquina virtual de PNETLab por medio del software WinSCP, como se muestra en la figura 57.

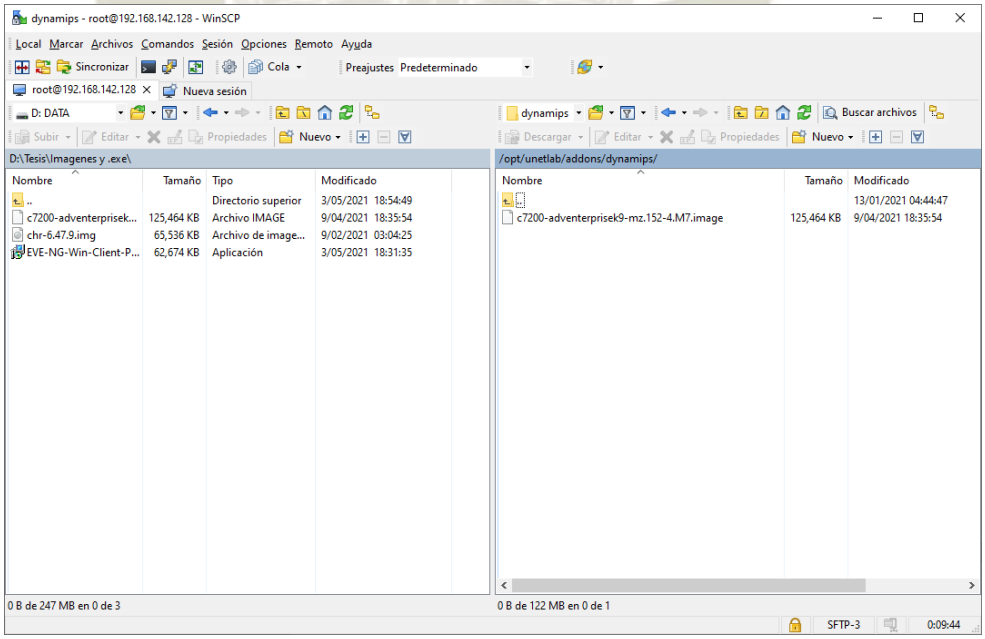


Figura 58. Directorio de PNETLab con la imagen del router cisco.
Fuente: Elaboración propia.

5.3.4.2 Creación de laboratorios en PNETLab

Con las imágenes de los dispositivos que usaremos ya establecidos dentro del emulador podemos proceder a realizar las topologías diseñadas.

Como primer paso accederemos al emulador por medio de la IP 192.168.142.128 brindada anteriormente, tal como muestra la figura 58.

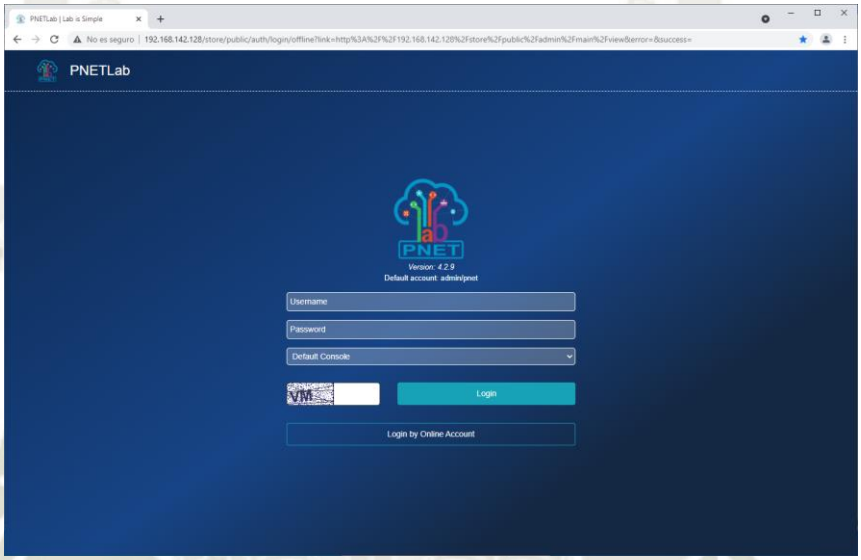


Figura 59. Página de acceso emulador PNETLab cuenta offline.
Fuente: Elaboración propia.

Luego de ingresar al emulador con las credenciales de acceso, nos mostrará una pantalla principal, como muestra la figura 59.

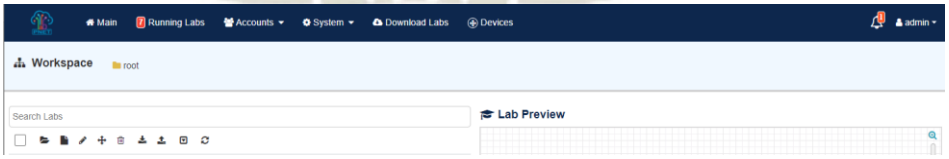


Figura 60. Pantalla principal PNETLab.
Fuente: Elaboración propia.

Dentro de esta pantalla procedemos a crear un nuevo laboratorio para probar los dispositivos cargados al emulador en pasos anteriores.

Los pasos son mostrados en las figuras 60 y 61 a continuación.

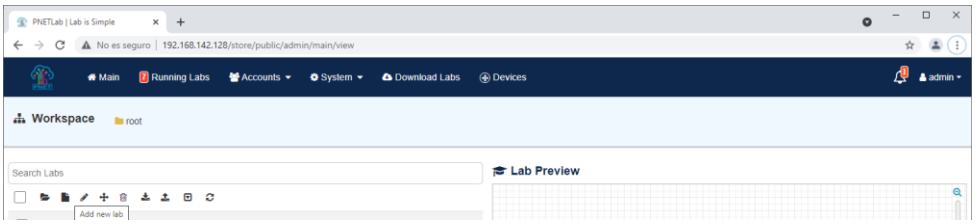


Figura 61. Creación del laboratorio en el entorno de PNETLab.
Fuente: Elaboración propia.

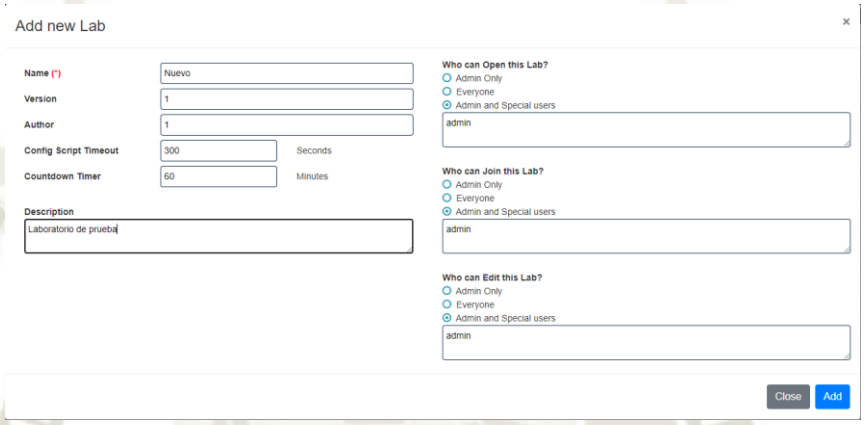


Figura 62. Datos para la creación de un nuevo laboratorio.
Fuente: Elaboración propia.

Una vez creado el laboratorio, nos mostrará una pantalla similar a la figura 62.

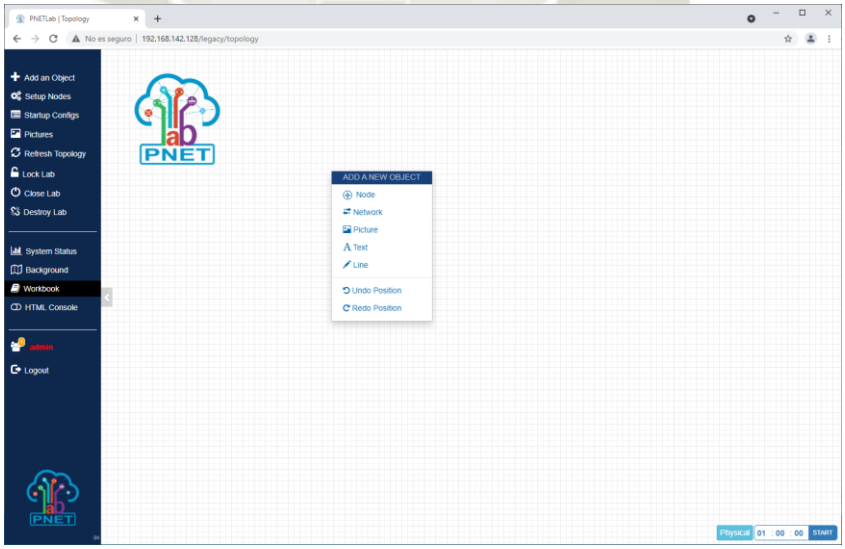


Figura 63. Pantalla Principal del nuevo laboratorio creado.
Fuente: Elaboración propia.

Para agregar nodos y verificar los dispositivos subidos anteriormente se hace clic en la opción nodo y de esta forma muestra los dispositivos habilitados en PNETLab.

Para nuestro caso visualizamos el equipo Mikrotik y Cisco respectivamente en la figura 63.

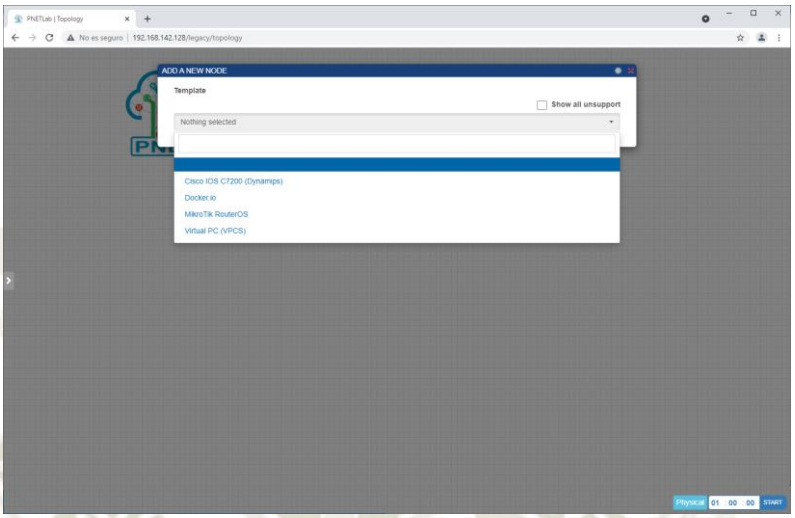


Figura 64. Visualización de nodos con los dispositivos agregados anteriormente.
Fuente: Elaboración propia.

CAPÍTULO VI: DISEÑOS Y PROPUESTAS

6. Diseño de Topología

El fundamento básico de un punto de intercambio de tráfico es la interconectividad entre varios miembros, con el fin de mejorar sus latencias, tasas de transferencia, anchos de banda, etc.

Ahora procederemos a la etapa de diseño del punto de intercambio de tráfico a partir de las herramientas mencionadas con anterioridad.

Para el diseño propuesto en la tesis, se identifican cuatro puntos importantes a considerar.

- Los equipos deben trabajar tanto con IPv4 como IPv6.
- Presentar redundancia automática entre los dispositivos.
- Enrutamiento dinámico para los participantes y servicios.
- Enlaces independientes entre sí.

6.1.1 Generalidades

La visión general del punto de intercambio de tráfico debe compartir el esquema mostrado en la figura 64.

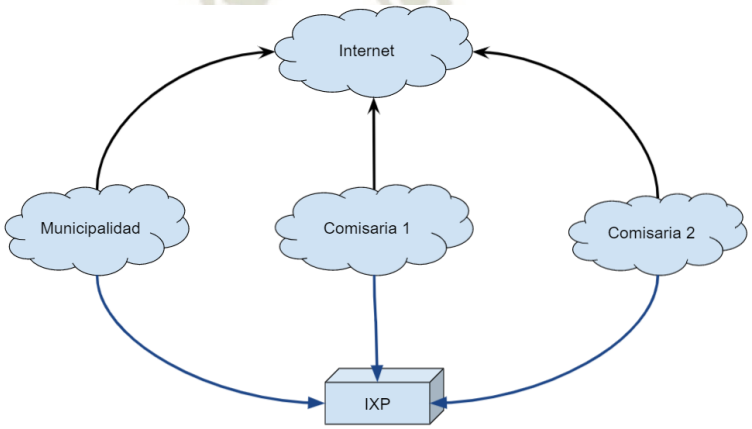


Figura 65. Esquema general del punto de intercambio de tráfico entre la municipalidad con sus comisarías.
Fuente: Elaboración propia.

En la cual, se aprecia a los miembros pertenecientes de este punto de intercambio de tráfico, las conexiones a internet y sus conexiones hacia el punto de intercambio de tráfico, ambos enlaces independientes entre sí.

El flujo del tráfico de datos dentro del punto de intercambio de tráfico entre los miembros esta mostrado en la figura 65.

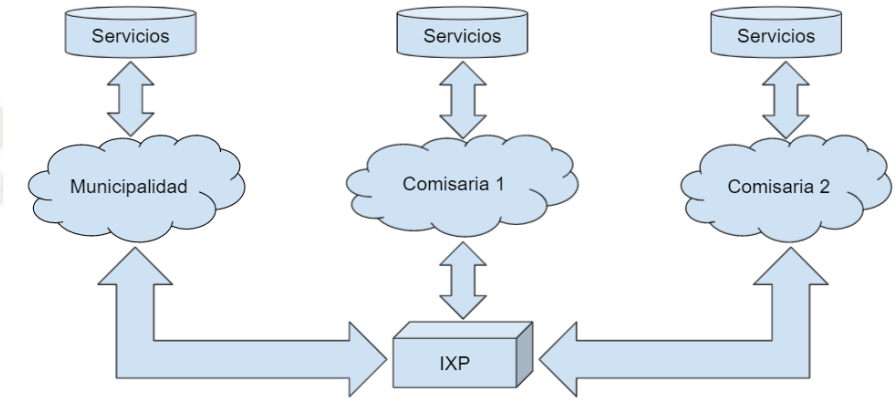


Figura 66. Esquema del flujo de datos entre los miembros del IXP.
Fuente: Elaboración propia.

Partiendo del esquema anterior se procede a realizar el diseño del IXP, empezando por el desarrollo de las redes independientes de cada miembro y los servicios que puedan ofrecer dentro del punto de intercambio de tráfico.

Luego, el diseño de la confluencia del tráfico entre ellos, garantizando la comunicación y mostrando los valores de conectividad entre los miembros.

6.2 Primera Propuesta

En base al objetivo propuesto, se realizó el diseño de la primera propuesta de la topología red para el cumplimiento de los requisitos en el diseño de la red del punto de intercambio de tráfico.

La primera propuesta es presentada en la figura 66.

Las redes de los participantes son presentadas como nubes, en las cuales se encuentran configuradas las IPs de los diferentes servicios que puedan prestar.

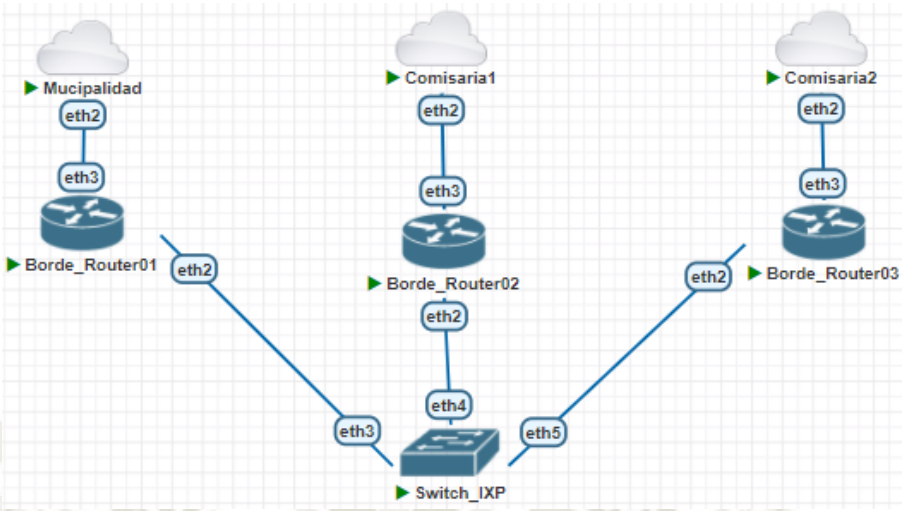


Figura 67. Topología de la primera propuesta.
Fuente: Elaboración propia.

La primera propuesta, garantiza la interconectividad entre los router de borde de cada uno de los participantes.

Con dicha interconectividad, por medio de protocolos de enrutamiento (internos y externos), se garantiza el alcance a nivel de redes entre los tres participantes.

El número de dispositivos requeridos para la implementación de esta primera propuesta se muestran a continuación en la tabla 16.

Tabla 17. Distribución de dispositivos propuesta 1

Dispositivos	Participantes				Función
	IXP	**Municipalidad**	**Comisaría 1**	**Comisaría 2**	
Router de borde	-----	1	1	1	Router de borde para levantar sesiones BGP con los demás participantes
Switch	1	-----	-----	-----	Conectividad capa 2 entre los router de borde

Fuente: Elaboración propia.

La distribución de redes se realizó como se describe la tabla 17.

Tabla 18. Distribución de redes propuesta 1

Participantes	IPV4		IPV6		Vlan	ASN
	Loopback	**Enlaces**	**Servicios**	**Enlaces**	**Servicios**		
Municipalidad	10.1.0.0/24	10.1.1.0/24	10.1.2.0/24	2001:db8:1000::/48	2001:db8:1001::1/48	------	20
Comisaría 1	10.2.0.0/24	10.2.1.0/24	10.2.2.0/24	2001:cafe::/48	2001:cafe:1::/48	------	30
Comisaría 2	10.3.0.0/24	10.3.1.0/24	10.3.2.0/24	2001:cafe:1000::/48	2001:cafe:1001::/48	------	40
IXP	10.10.9.0/24	10.10.10.0 /24	------	2001:db8::/48	-----	100	50

Fuente: Elaboración propia.

6.2.1 Configuración de dispositivos

Creación de Vlan:

[tesis@Borde_Router01] > interface vlan print

Flags: X - disabled, R - running

NAME MTU ARP VLAN-ID INTERFACE

0 R vlan100 1500 enabled 100 Trunk

[tesis@Borde_Router02] > interface vlan print

Flags: X - disabled, R - running

```
 #   NAME                                                MTU ARP          VLAN-ID
INTERFACE
 0 R vlan100                                          1500 enabled          100 Trunk
[tesis@Borde_Router03] > interface vlan print
Flags: X - disabled, R - running
 #   NAME              MTU ARP          VLAN-ID INTERFACE
 0 R vlan100           1500 enabled          100 Trunk
```

Direccionamientos:

```
[tesis@Municipalidad] > IP address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS          NETWORK       INTERFACE
 0   10.1.0.1/32      10.1.0.3      Loopback
 1   10.1.1.1/30      10.1.1.0      ether2
 2   10.1.2.1/24      10.1.2.0      Municipalidad
[tesis@Municipalidad] > IPv6 address print
Flags: X - disabled, I - invalid, D - dynamic, G - global, L - link-local
 #    ADDRESS                          FROM-POOL INTERFACE          ADVERTISE
 0  G 2001:db8:1000::1/64                       ether2              no
 1  G 2001:db8:1001::1/64                       Municipalidad       no
 2 DL fe80::10df:23ff:fe27:6005/64               Municipalidad       no
```

```
 3 DL fe80::388b:51ff:fe2a:5efd/64                Loopback          no

 4 DL fe80::5285:dff:fe00:2d01/64                 ether2            no

 5 DL fe80::5285:dff:fe00:2d00/64                 ether1            no

[tesis@Borde_Router01] > IP address print

Flags: X - disabled, I - invalid, D - dynamic

 #   ADDRESS          NETWORK        INTERFACE

 0   10.10.10.6/24    10.10.10.0     vlan100

 1   10.1.0.2/32      10.1.0.1       Loopback

 2   10.1.1.2/30      10.1.1.0       ether3

[tesis@Borde_Router01] > IPv6 address print

Flags: X - disabled, I - invalid, D - dynamic, G - global, L - link-local

 #    ADDRESS                              FROM-POOL INTERFACE   ADVERTISE

 0  G 2001:db8::2:1/64                              vlan100     no

 1  G 2001:db8:1000::2/64                           ether3      no

 2 DL fe80::d48e:a0ff:fee6:6e6b/64                   Loopback    no

 3 DL fe80::5246:a4ff:fe00:2001/64                   Trunk       no

 4 DL fe80::5246:a4ff:fe00:2001/64                   vlan100     no

 5 DL fe80::5246:a4ff:fe00:2002/64                   ether3      no

 6 DL fe80::5246:a4ff:fe00:2000/64                   ether1      no

[tesis@Comisaría01] > IP address print
```

Flags: X - disabled, I - invalid, D - dynamic

#	ADDRESS	NETWORK	INTERFACE
0	10.2.0.1/32	10.2.0.3	Loopback
1	10.2.1.1/30	10.2.1.0	ether2
2	10.2.2.1/24	10.2.2.0	Comisaría

[tesis@Comisaría01] > IPv6 address print

Flags: X - disabled, I - invalid, D - dynamic, G - global, L - link-local

#	ADDRESS	FROM-POOL	INTERFACE	ADVERTISE
0	G 2001:cafe::1/64		ether2	no
1	G 2001:cafe:1::1/64		Comisaría	no
2	DL fe80::e45f:8ff:fecc:487c/64		Loopback	no
3	DL fe80::583b:ebff:feff:b416/64		Comisaría	no
4	DL fe80::5267:3cff:fe00:2e01/64		ether2	no
5	DL fe80::5267:3cff:fe00:2e00/64		ether1	no

[tesis@Borde_Router02] > IP address print

Flags: X - disabled, I - invalid, D - dynamic

#	ADDRESS	NETWORK	INTERFACE
0	10.10.10.7/24	10.10.10.0	vlan100
1	10.2.0.2/32	10.2.0.1	LoopBack
2	10.2.1.2/30	10.2.1.0	ether3

```
[tesis@Comisaría02] > IP address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS          NETWORK        INTERFACE
 0   10.3.0.1/32      10.3.0.3       Loopback
 1   10.3.2.1/24      10.3.2.0       Comisaría02
 2   10.3.1.1/30      10.3.1.0       ether2
 3   192.168.1.2/24   192.168.1.0    ether2
[tesis@Comisaría02] > IPv6 address print
Flags: X - disabled, I - invalid, D - dynamic, G - global, L - link-local
 #    ADDRESS                          FROM-POOL INTERFACE   ADVERTISE
 0  G 2001:cafe:1000::1/64                       ether2      no
 1  G 2001:cafe:1001::1/64                       Comisaría02 no
 2 DL fe80::ac:17ff:fe1c:9af7/64                 Loopback    no
 3 DL fe80::dc8d:f8ff:fe62:7a51/64               Comisaría02 no
 4 DL fe80::52b3:9fff:fe00:2f01/64               ether2      no
 5 DL fe80::52b3:9fff:fe00:2f00/64               ether1      no
[tesis@Borde_Router03] > IP address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS          NETWORK        INTERFACE
 0   10.10.10.8/24    10.10.10.0     vlan100
```

```
1   10.3.0.2/32       10.3.0.1       Loopback

2   10.3.1.2/30       10.3.1.0       ether3

[tesis@Borde_Router03] > IPv6 address print

Flags: X - disabled, I - invalid, D - dynamic, G - global, L - link-local

#    ADDRESS                              FROM-POOL INTERFACE   ADVERTISE

0  G 2001:db8::4:1/64                                vlan100     no

1  G 2001:cafe:1000::2/64                            ether3      no

2 DL fe80::c4db:2bff:fe02:61ea/64                    Loopback    no

3 DL fe80::523f:1ff:fe00:2301/64                     Trunk       no

4 DL fe80::523f:1ff:fe00:2301/64                     vlan100     no

5 DL fe80::523f:1ff:fe00:2302/64                     ether3      no

6 DL fe80::523f:1ff:fe00:2300/64                     ether1      no
```

Configuración del Switch

```
/interface bridge

add name=Trunk

/interface wireless security-profiles

set [ find default=yes ] supplicant-identity=MikroTik

/interface bridge port

add bridge=Trunk interface=ether2

add bridge=Trunk interface=ether3
```

add bridge=Trunk interface=ether4

add bridge=Trunk interface=ether5

A continuación, en las figuras 67, 68 y 69 se muestran las rutas de los tres dispositivos correspondientes a la Municipalidad, Comisaría 1 y Comisaría 2 en las cuales se verifica que por medio de enrutamiento dinámicos las redes de sus pares son alcanzables, gracias a la topología propuesta.

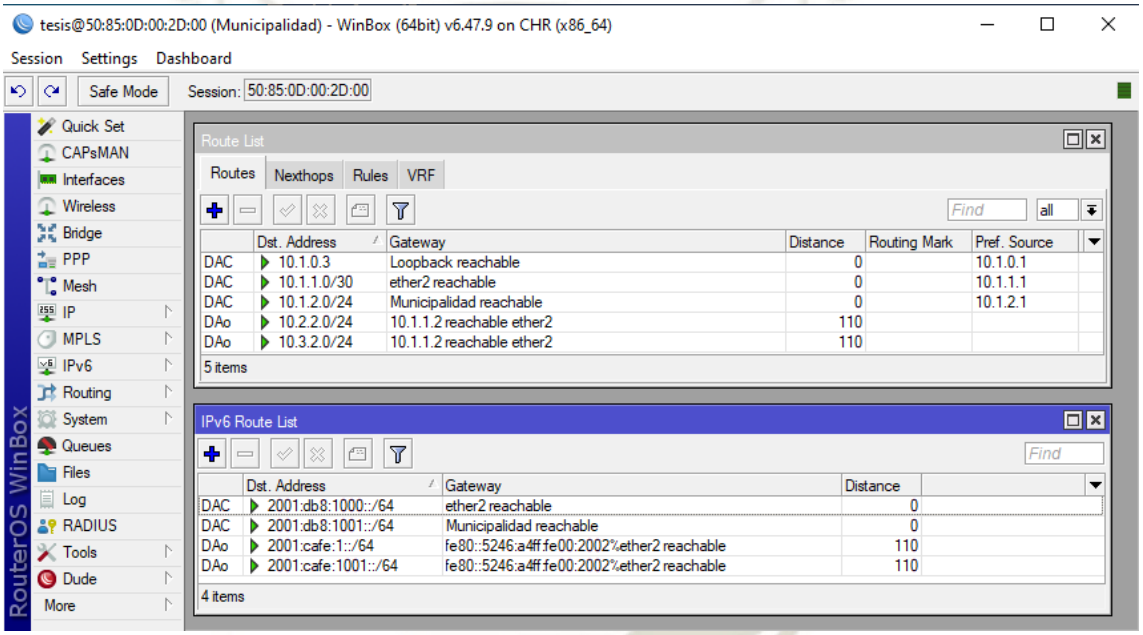


Figura 68. Visualización de rutas IPv4 e IPv6 desde el enrutador denominado Municipalidad.
Fuente: Elaboración propia.

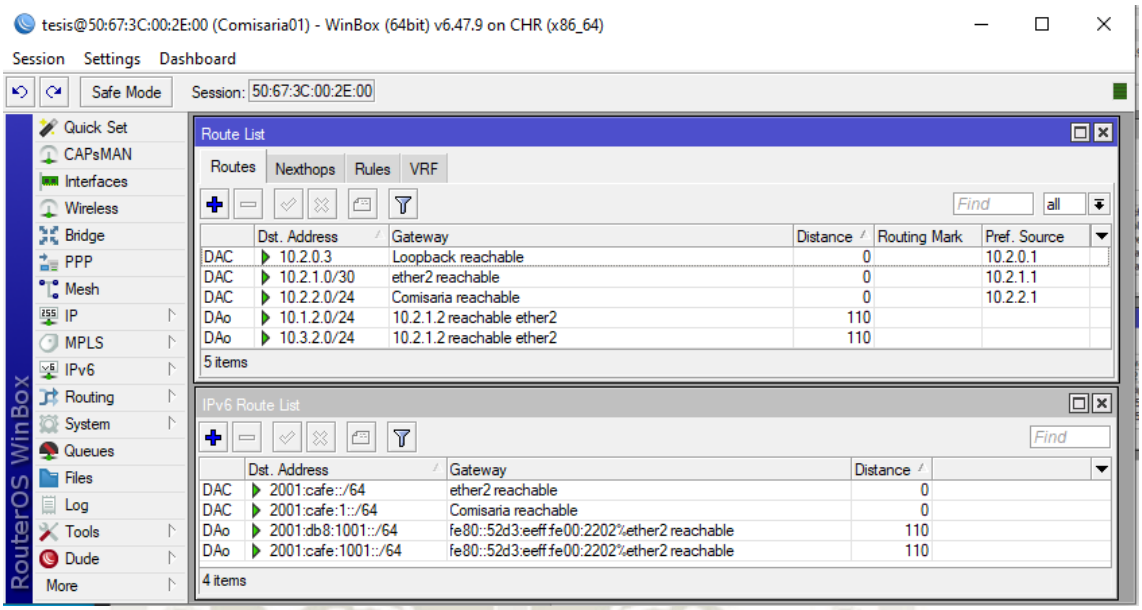


Figura 69.Visualización de rutas IPv4 e IPv6 desde el enrutador denominado Comisaría 1.
Fuente: Elaboración propia.

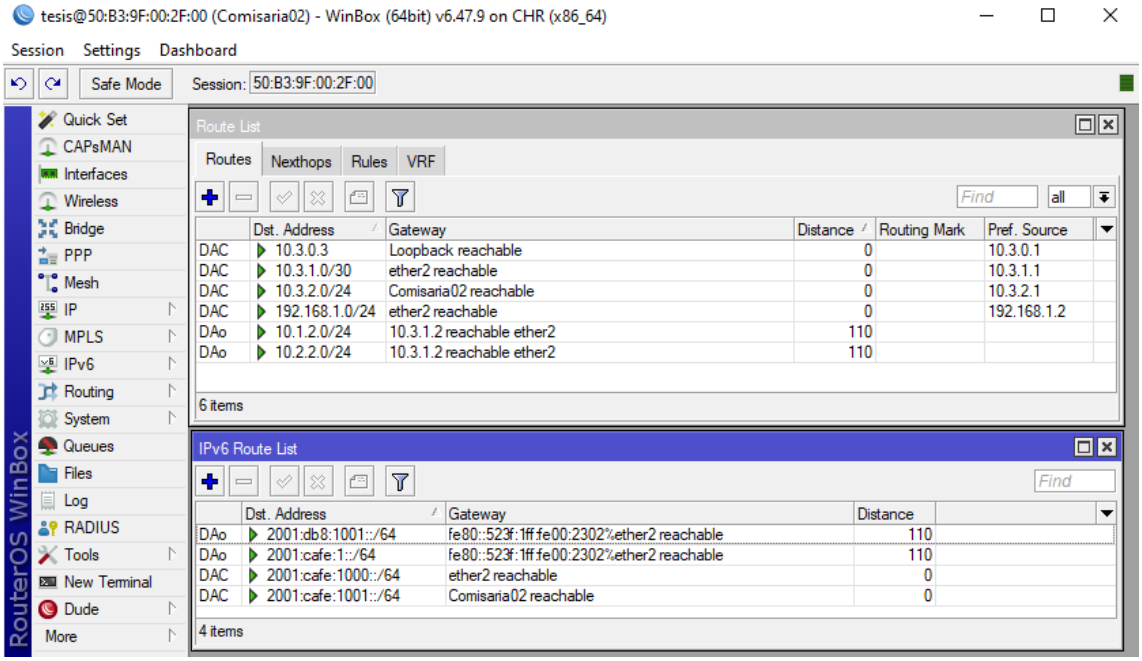


Figura 70. Visualización de rutas IPv4 e IPv6 desde el enrutador denominado Comisaría 2.
Fuente: Elaboración propia.

6.2.2 Pruebas de funcionalidad

6.2.2.1 Funcionalidad con todos los dispositivos

En esta etapa, se realizaron las pruebas de conectividad entre las redes de la municipalidad, la Comisaría 1 y la Comisaría 2 para comprobar el funcionamiento de la red propuesta.

6.2.2.1.1 Municipalidad - Comisaría1

96 10.2.2.1 56 62 2ms

97 10.2.2.1 56 62 2ms

98 10.2.2.1 56 62 2ms

99 10.2.2.1 56 62 2ms

sent=100 received=100 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=3ms

6.2.2.1.2 Municipalidad – Comisaría 2

96 10.3.2.1 56 62 2ms

97 10.3.2.1 56 62 2ms

98 10.3.2.1 56 62 2ms

99 10.3.2.1 56 62 2ms

sent=100 received=100 packet-loss=0% min-rtt=1ms avg-rtt=2ms max-rtt=3ms

6.2.2.2 Funcionamiento con el Switch IXP desconectado

Como segundo paso, se pasará a simular una desconexión del switch IXP intermedio para verificar el comportamiento de la topología.

6.2.2.2.1 Municipalidad – Comisaría 1

96 10.2.2.1 timeout

97 10.2.2.1 timeout

98 10.2.2.1 timeout

99 10.2.2.1 timeout

sent=100 received=79 packet-loss=21% min-rtt=1ms avg-rtt=2ms max-rtt=4ms

6.2.2.2.2 Municipalidad – Comisaría 2

96 10.3.2.1 timeout

97 10.3.2.1 timeout

98 10.3.2.1 timeout

99 10.3.2.1 timeout

sent=100 received=77 packet-loss=23% min-rtt=2ms avg-rtt=2ms max-rtt=6ms

6.2.2.3 Funcionamiento con el Router de Borde de la Comisaría 1 desconectado

Se procede a la desconexión del router de borde de la Comisaría 1, para analizar el comportamiento de la topología propuesta.

6.2.2.3.1 Municipalidad - Comisaría 1

101 10.2.2.1 timeout

102 10.2.2.1 timeout

103 10.2.2.1 timeout

sent=104 received=46 packet-loss=55% min-rtt=2ms avg-rtt=2ms max-rtt=4ms

6.2.2.3.2 Municipalidad – Comisaría 2

96 10.3.2.1 56 62 2ms

97 10.3.2.1 56 62 2ms

98 10.3.2.1 56 62 2ms

99 10.3.2.1 56 62 2ms

sent=100 received=100 packet-loss=0% min-rtt=1ms avg-rtt=2ms max-rtt=4ms

6.2.2.4 Resultados

Como parte de las simulaciones de la primera propuesta, se logró el funcionamiento del punto de intercambio de tráfico, comprobando la conectividad entre la municipalidad y ambas Comisarías, tal como se muestra en la tabla 18.

Tabla 19. Conectividad entre la Municipalidad, Comisaría 1 y Comisaría 2

Conectividad Municipalidad y Comisarías				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo promedio (ms)**
Municipalidad – Comisaría 1	100	100	0	2
Municipalidad – Comisaría 2	100	100	0	6

Fuente: Elaboración propia.

De la tabla 18, se comprueba que todos los miembros lograron el nivel de conectividad esperado para la topología, teniendo comunicación entre todos.

La siguiente prueba consistió en la desconexión del switch que comparte la conexión de los router de borde de cada miembro.

Los resultados obtenidos se muestran en la tabla 19.

Tabla 20. Conectividad entre la Municipalidad, Comisaría 1 y Comisaría 2 con el Switch desconectado

Conectividad Municipalidad y Comisarías con Switch Desconectado				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad – Comisaría 1	100	79	21	Sin redundancia
Municipalidad – Comisaría 2	100	77	23	Sin redundancia

Fuente: Elaboración propia.

Con los resultados de esta prueba, se comprueba que el único punto de interconexión entre los miembros es el switch IXP, por tanto, al ser desconectado los miembros del IXP perdieron comunicación entre sí.

Como última prueba, se procedió a simular la desconexión del router de borde de la Comisaría 1 y los resultados obtenidos se muestran en la tabla 20.

Tabla 21. Conectividad entre la Municipalidad, Comisaría 1 y Comisaría 2 con el Router de Borde de la Comisaría 1 desconectado

Conectividad Municipalidad y Comisarías con router de borde de la Comisaría 1 desconectado				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad – Comisaría 1	104	46	58	Sin redundancia
Municipalidad – Comisaría 2	103	103	0	No requiere

Fuente: Elaboración propia.

De la tabla 20 obtenemos que, de la prueba de desconexión del router de borde de la Comisaría 1, la comunicación no se pierde entre la Municipalidad y la Comisaría 2 pero si se ve afectada en la comunicación entre la Municipalidad y la Comisaría 1, dado que el único enlace existente entre la Comisaría 1 y el punto de intercambio de tráfico se ve afectado.

Sin obtener ningún nivel de redundancia en la red y carecer de dispositivos de respaldo, es necesario el cambio en la topología propuesta, la cual nos permita poder tener una red sostenible con redundancia y a prueba de fallo de dispositivos.

6.3 Segunda Propuesta

Luego de realizar el análisis de la primera propuesta, se obtiene una interconexión entre los participantes, pero esta interconexión no presenta ningún tipo de redundancia, por lo que la integración de dispositivos que garanticen la interconectividad con un nivel de redundancia y el aprovechamiento de la topología para presentar nuevos servicios comunitarios, se desarrollan la segunda propuesta presentada en la figura 70.

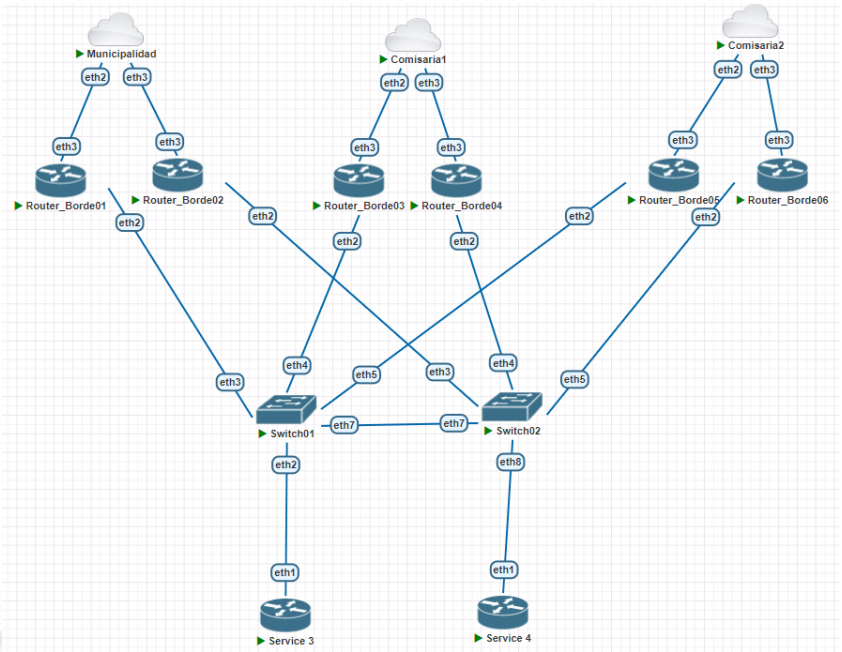


Figura 71. Topología de la segunda propuesta.
Fuente: Elaboración propia.

En esta segunda propuesta, se disponen dos router de borde para la interconexión del punto de intercambio de tráfico, dos switch para la interconexión de capa 2 entre los router de borde de cada participante y la adición de dos enrutadores de servicios comunitarios entre los participantes, de esta forma los puntos críticos de redundancia encontrados en la primera propuesta son suplidos.

Teniendo router de borde con redundancia, se requiere la adición de sistemas de elección de rutas para la elección de dispositivos principales y secundarios entre los otros router de borde; esto se hace a partir del manejo de los atributos de BGP en cada router de borde, por medio ellos los enrutadores son capaces de decidir qué dispositivos vecinos serán los principales o secundarios.

Y hace posible la agregación de servicios adicionales al de los miembros dentro del punto de intercambio de tráfico.

Los dispositivos que componen la topología de la segunda propuesta son mostrados en la tabla 21.

Tabla 22. Distribución de dispositivos de la segunda propuesta

Dispositivos	Participantes				Función
	IXP	**Municipalidad**	**Comisaría 1**	**Comisaría 2**	
Router	-----	2	2	2	Router de borde para levantar sesiones BGP con los demás participantes, con su par para temas de redundancia.
Switch	2	------	------	------	Conectividad capa 2 entre los router de borde, con su par para temas de redundancia.

Fuente: Elaboración propia.

La distribución de redes para esta segunda propuesta esta mostrada en la tabla 22.

Tabla 23. Distribución de redes para la segunda propuesta

Participantes	IPV4			IPV6		VLAN	ASN
	Loopback	**Enlaces**	**Servicios**	**Enlaces**	**Servicios**		
Municipalidad	10.1.0.0/24	10.1.1.0/24	10.1.2.0/24	2001:db8:1000::/48	2001:db8:1001::/48	------	20
Comisaría 1	10.2.0.0/24	10.2.1.0/24	10.2.2.0/24	2001:cafe::/48	2001:cafe:1::/48	------	30
Comisaría 2	10.3.0.0/24	10.3.1.0/24	10.3.2.0/24	2001:cafe:1000::/48	2001:cafe:1001::/48	------	40
IXP	------	10.10.10.0/24	------	2001:db8::/48	------	100	50
Servicio 3	10.10.9.0/24	192.168.1.0/24	192.168.50.0/24	------	------	3	50
Servicio 4	10.10.9.0/24	----------	----------	2001:db8:1:1::/48	2001:db8:1:1::/48	4	50

Fuente: Elaboración propia.

6.3.1 Configuración de Dispositivos

Creación de Vlans

[tesis@Borde_Router01] > interface vlan print

Flags: X - disabled, R - running

```
#   NAME              MTU ARP          VLAN-ID INTERFACE
0 R vlan3             1500 enabled       3 Trunk
1 R vlan4             1500 enabled       4 Trunk
2 R vlan100           1500 enabled       100 Trunk
[tesis@Borde_Router02] > interface vlan print
Flags: X - disabled, R - running
#   NAME              MTU ARP          VLAN-ID INTERFACE
0 R vlan3             1500 enabled       3 Trunk
1 R vlan4             1500 enabled       4 Trunk
2 R vlan100           1500 enabled       100 Trunk
[tesis@Borde_Router03] > interface vlan print
Flags: X - disabled, R - running
#   NAME              MTU ARP          VLAN-ID INTERFACE
0 R vlan3             1500 enabled       3 Trunk
1 R vlan4             1500 enabled       4 Trunk
2 R vlan100           1500 enabled       100 Trunk
[tesis@Borde_Router04] > interface vlan print
Flags: X - disabled, R - running
#   NAME              MTU ARP          VLAN-ID INTERFACE
0 R vlan3             1500 enabled       3 Trunk
```

1 R vlan4 1500 enabled 4 Trunk

2 R vlan100 1500 enabled 100 Trunk

[tesis@Borde_Router05] > interface vlan print

Flags: X - disabled, R - running

NAME MTU ARP VLAN-ID INTERFACE

0 R vlan3 1500 enabled 3 Trunk

1 R vlan4 1500 enabled 4 Trunk

2 R vlan100 1500 enabled 100 Trunk

[admin@Borde_Router06] > interface vlan print

Flags: X - disabled, R - running

NAME MTU ARP VLAN-ID INTERFACE

0 R vlan3 1500 enabled 3 Trunk

1 R vlan4 1500 enabled 4 Trunk

2 R vlan100 1500 enabled 100 Trunk

Direccionamientos

El direccionamiento realizado para la municipalidad y sus router de borde 01, 02 se muestran en las figuras 71, 72 y 73 respectivamente.

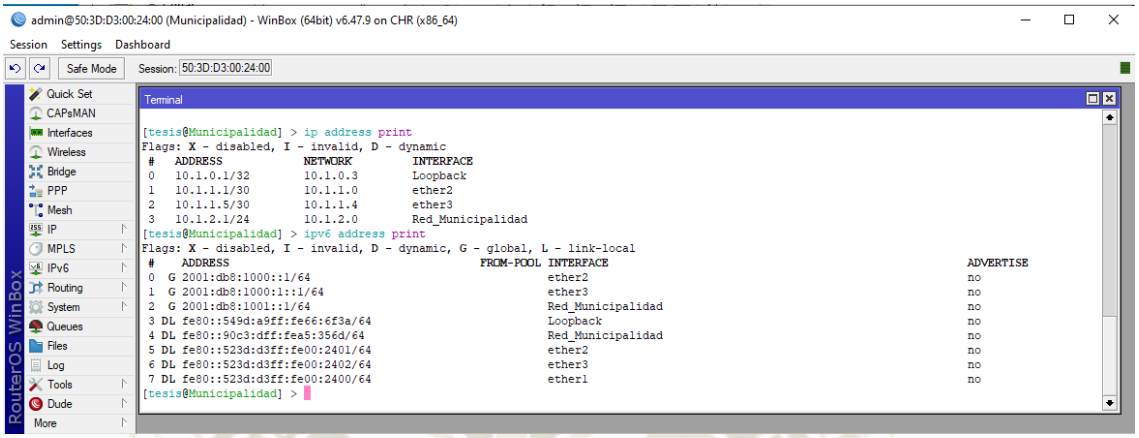


Figura 72. Direccionamiento Router Municipalidad.
Fuente: Elaboración propia.

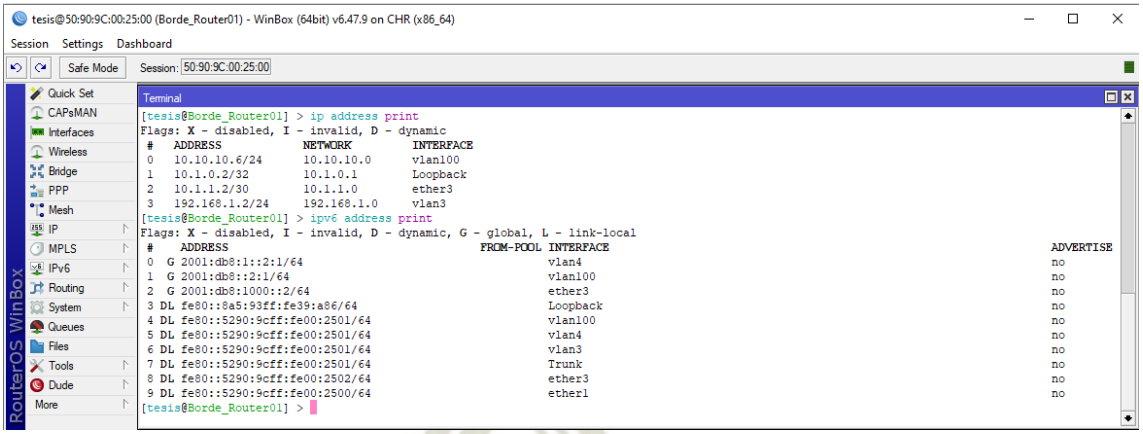


Figura 73. Direccionamiento Borde Router 01.
Fuente: Elaboración propia.

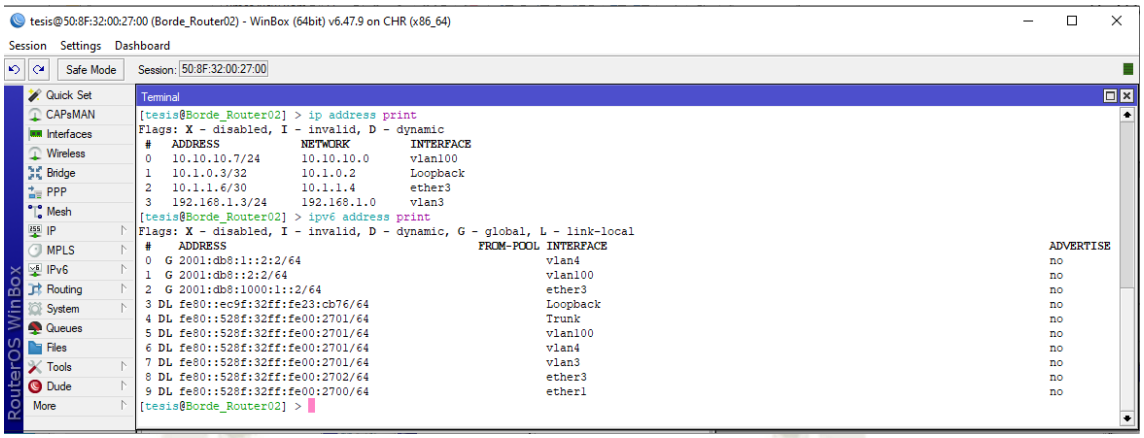


Figura 74. Direccionamiento Borde Router 02.
Fuente: Elaboración Propia.

El direccionamiento realizado para la Comisaría 1 y los router de borde 03 y 04 se muestran en las figuras 74, 75 y 76 respectivamente.

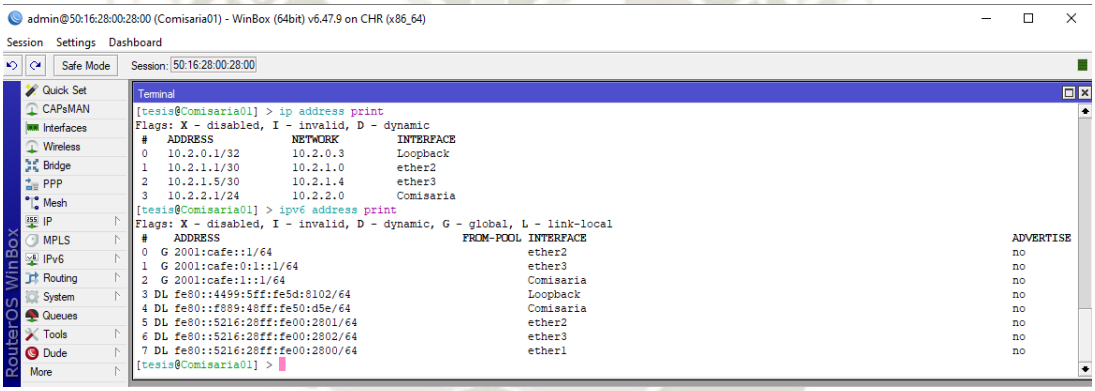


Figura 75. Direccionamiento Router Comisaría 1.
Fuente: Elaboración propia.

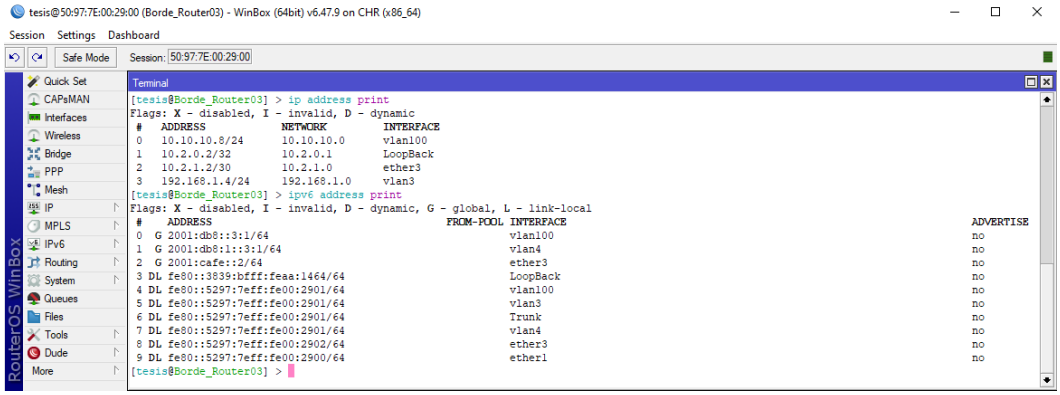


Figura 76. Direccionamiento Borde Router 03.
Fuente: Elaboración propia.

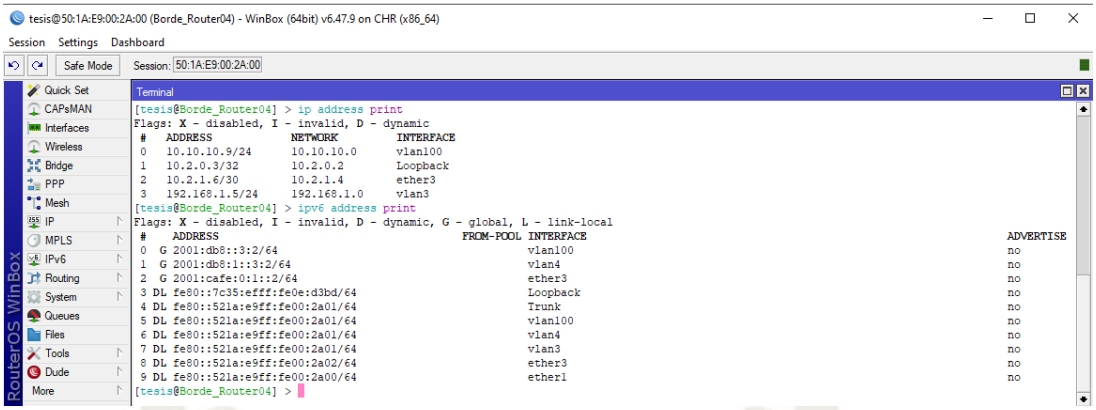


Figura 77. Direccionamiento Borde Router 04.
Fuente: Elaboración propia.

El direccionamiento realizado para la Comisaría 2 y los router de borde 05, 06 se muestran en las figuras 77, 78 y 79 respectivamente.

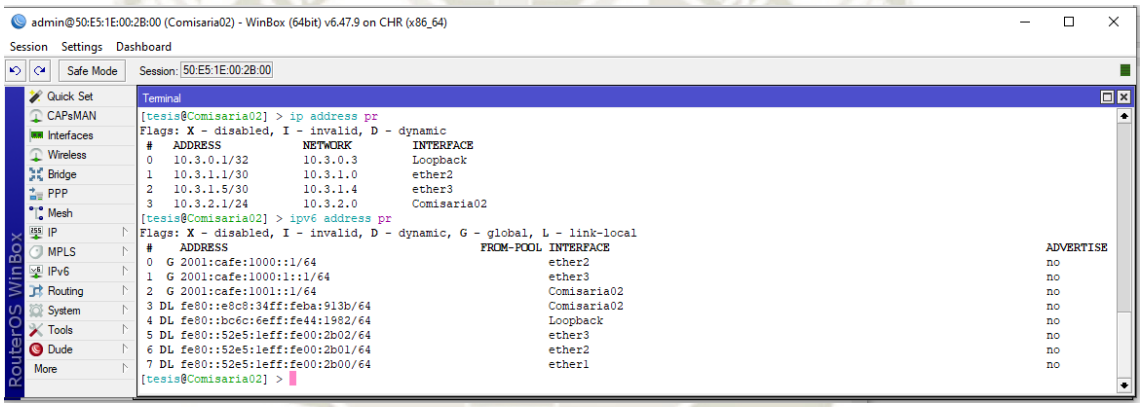


Figura 78. Direccionamiento Router Comisaría 2.
Fuente: Elaboración propia.

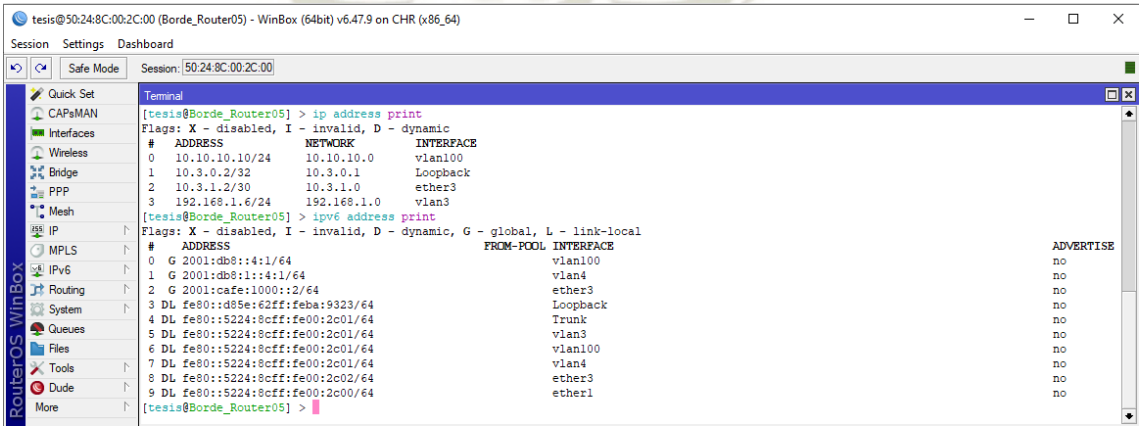


Figura 79. Direccionamiento Borde Router 05.
Fuente: Elaboración propia.

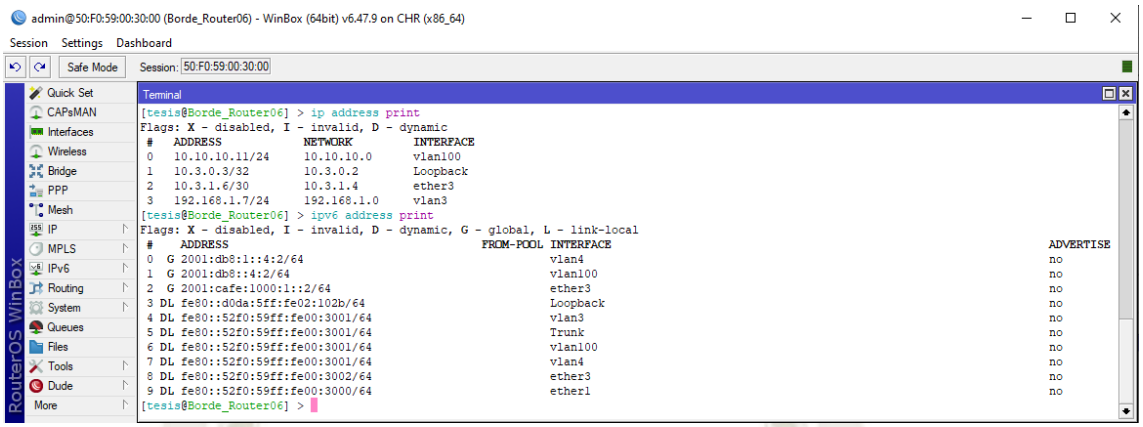


Figura 80. Direccionamiento Borde Router 06.
Fuente: Elaboración propia.

Vecinos BGP

El establecimiento de sesiones BGP así como los enlaces activos de OSPF en version 2 y 3 se muestran en la figura 80.

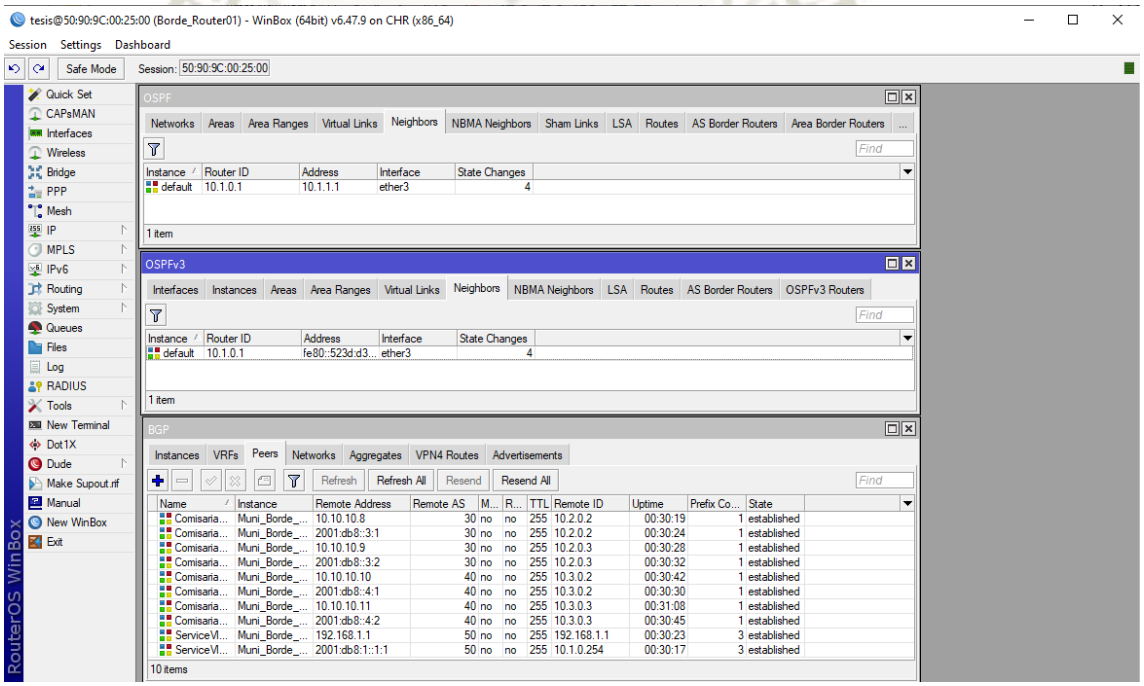


Figura 81. Tabla de vecinos establecidos por medio de protocolos de enrutamiento OSPF y BGP en el Borde Router 01.
Fuente: Elaboración propia.

El manejo de atributos en BGP hace posible poder determinar rutas principales o secundarias, en la figura 81 se visualiza el manjeo del atributo BGP Local Preference para determinar la ruta secundaria.

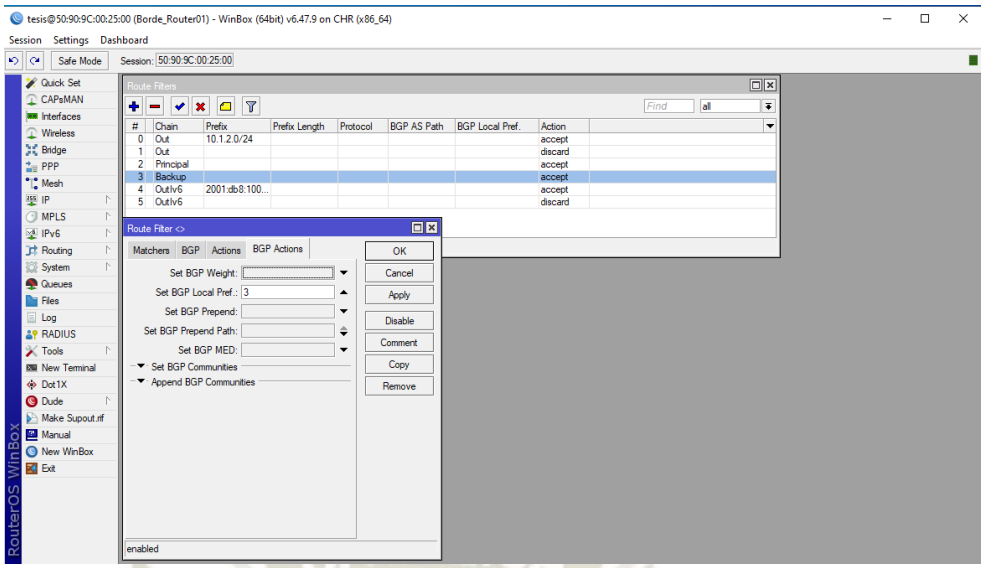


Figura 82. Manejo de atributos BGP para determinar router vecino secundario del router de borde 01.
Fuente: Elaboración propia.

Luego de establecer todas las sesiones BGP y el protocolo OSPF en funcionamiento, la tabla de rutas visualizada en la figura 82 nos muestra las rutas alcanzables por el router de borde 01 y muestra como se manejan los atributos en cada sesión configurada en el router.

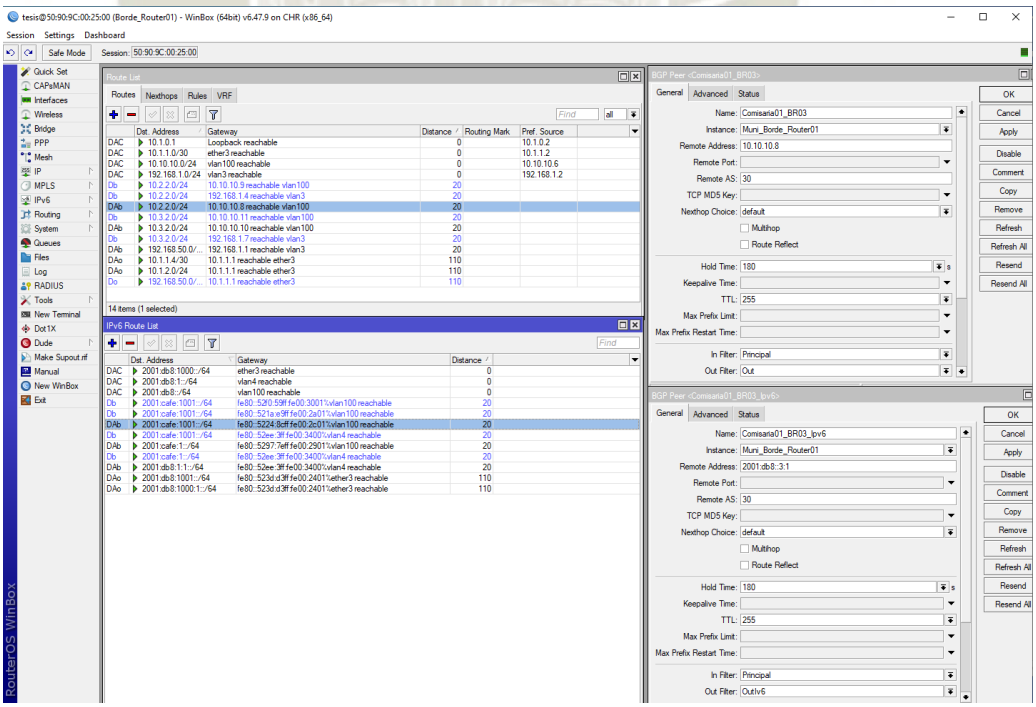


Figura 83. Tabla de rutas mostrando las redes alcanzables por el router principal establecido con atributos en el borde router 01.
Fuente: Elaboración propia.

La tabla de rutas del router de la Municipalidad es mostrada en la figura 83 en la que se pueden ver las redes de los otros miembros y servicios.

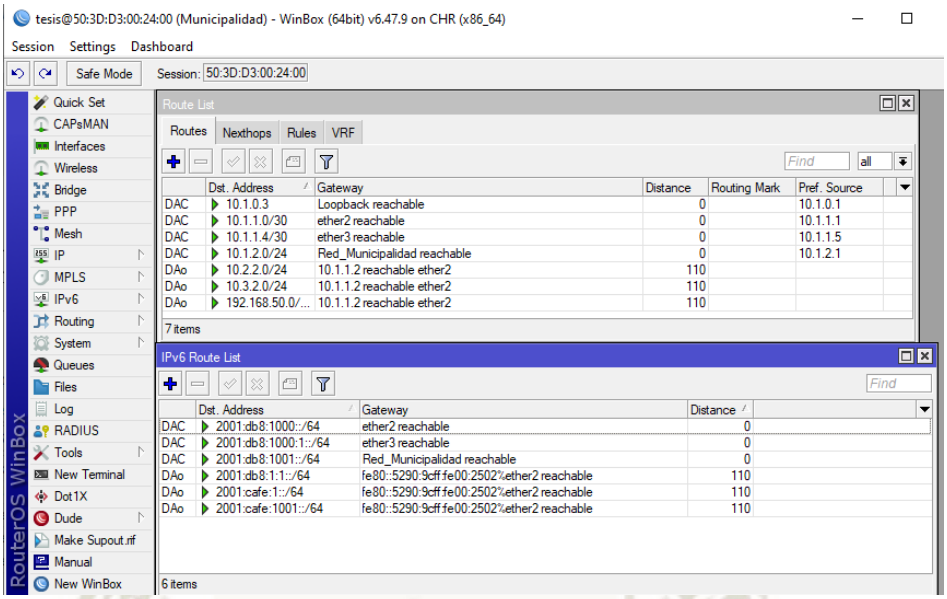


Figura 84. Tabla de rutas mostrando rutas alcanzables de los otros participantes por medio de enrutamiento dinámico en el router municipalidad.
Fuente: Elaboración propia.

En las figuras 84 y 85 se muestra la tabla de rutas del router de la Comisaría 1 y Comisaría 2 respectivamente, en la que se aprecian las redes de los demás miembros y servicios.

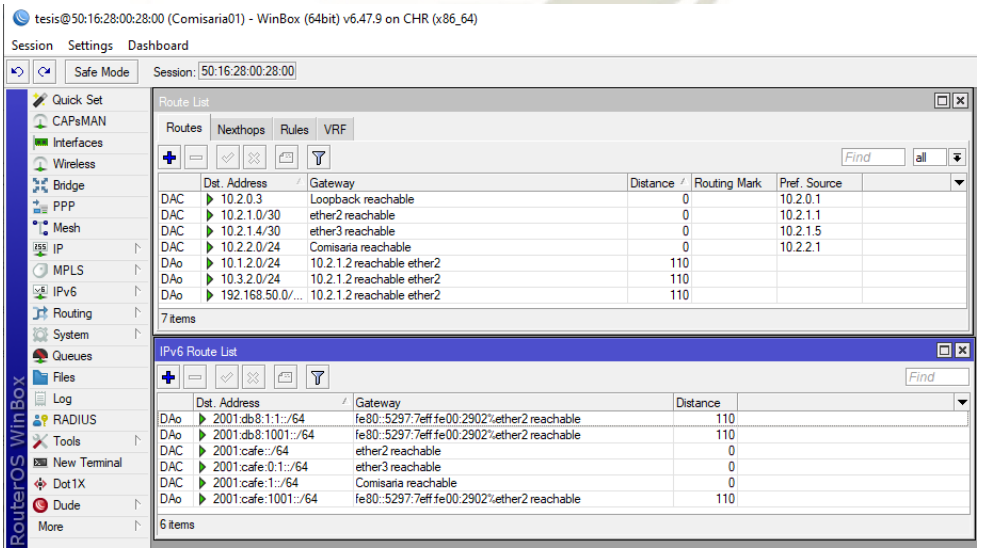


Figura 85. Tabla de rutas mostrando rutas alcanzables de los otros participantes por medio de enrutamiento dinámico en el router Comisaría 1.
Fuente: Elaboración propia.

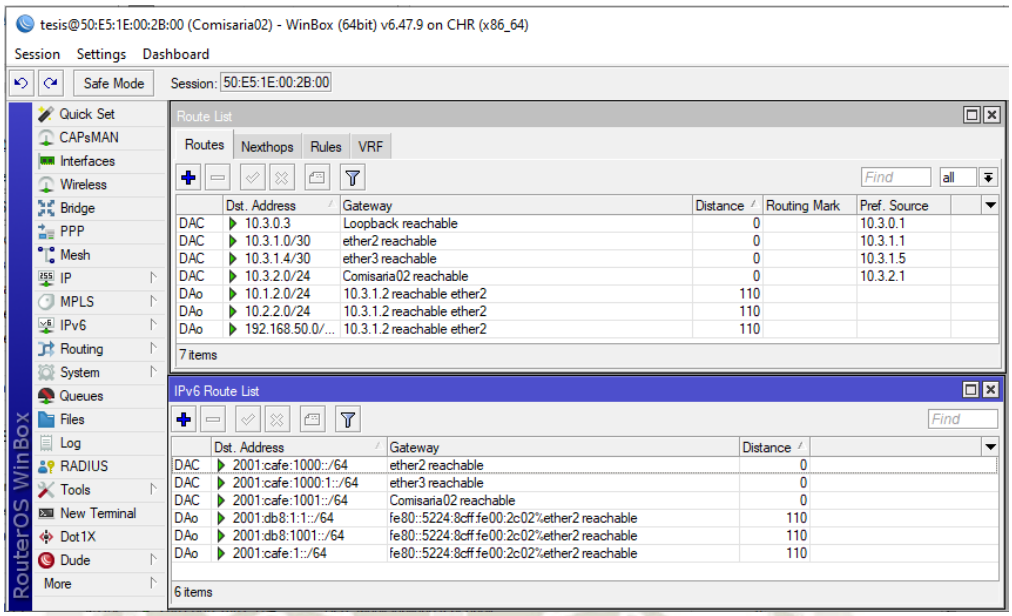


Figura 86. Tabla de rutas mostrando rutas alcanzables de los otros participantes por medio de enrutamiento dinámico en el router Comisaría 2.
Fuente: Elaboración propia.

6.3.2 Pruebas de Funcionalidad

6.3.2.1 Funcionamiento entre todos los dispositivos

6.3.2.1.1 Municipalidad – Comisaría 1

96 10.2.2.1 56 62 2ms

97 10.2.2.1 56 62 2ms

98 10.2.2.1 56 62 2ms

99 10.2.2.1 56 62 2ms

sent=100 received=100 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=4ms

6.3.2.1.2 Municipalidad – Comisaría 2

96 10.3.2.1 56 62 2ms

97 10.3.2.1 56 62 2ms

98 10.3.2.1 56 62 2ms

99 10.3.2.1 56 62 2ms

sent=100 received=100 packet-loss=0% min-rtt=1ms avg-rtt=2ms max-rtt=4ms

6.3.2.1.3 Comisaría 1 – Comisaría 2

96 2001:cafe:1001::1 56 62 2ms echo reply

97 2001:cafe:1001::1 56 62 2ms echo reply

98 2001:cafe:1001::1 56 62 2ms echo reply

99 2001:cafe:1001::1 56 62 2ms echo reply

sent=100 received=100 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=3ms

6.3.2.1.4 Comisaría 2 – Service 4

96 2001:db8:1:1::1 56 63 2ms echo reply

97 2001:db8:1:1::1 56 63 2ms echo reply

98 2001:db8:1:1::1 56 63 2ms echo reply

99 2001:db8:1:1::1 56 63 2ms echo reply

sent=100 received=100 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=3ms

6.3.2.2 Funcionamiento con Router de Borde desconectado

Las siguientes pruebas se realizaron simulando el comportamiento real de los router, es decir, se forzó la desconexión del router de borde por medio de sus interfaces para medir tiempos reales de redundancia en un entorno real.

6.3.2.2.1 Desconexión router de Borde 01

6.3.2.2.1.1 Municipalidad – Comisaría 1

57 10.2.2.1 56 62 4ms

58 10.2.2.1 56 62 5ms

59 10.2.2.1 56 62 3ms

sent=60 received=57 packet-loss=5% min-rtt=1ms avg-rtt=2ms max-rtt=5ms

En la figura 86, se muestra el comportamiento de la prueba de conectividad realizada desconectando el router de borde 01, teniendo una caída del enlace de 3 segundos, a partir del segundo 13 hasta el segundo 16.

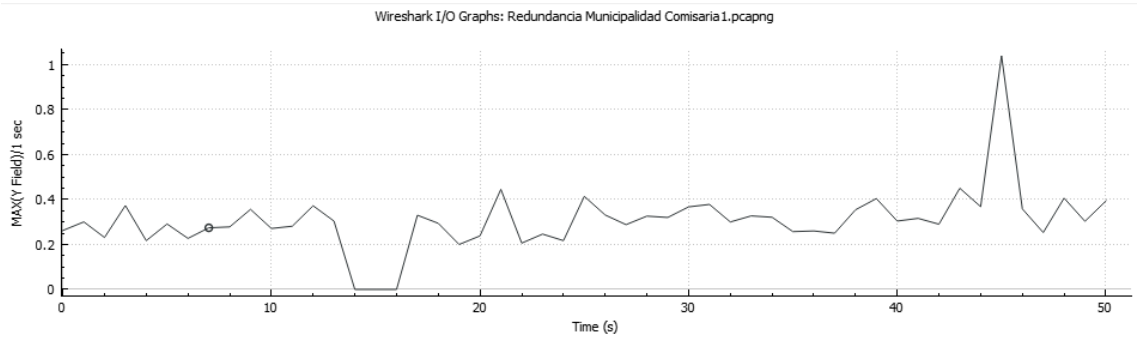


Figura 87. Tiempo de redundancia en las pruebas de conectividad entre la municipalidad y la Comisaría 1, con router de borde 01 desconectado.
Fuente: Elaboración propia.

6.3.2.2.1.2 Municipalidad – Comisaría 2

35 10.3.2.1 56 62 2ms

36 10.3.2.1 56 62 3ms

37 10.3.2.1 56 62 3ms

sent=38 received=36 packet-loss=5% min-rtt=1ms avg-rtt=2ms max-rtt=4ms

En la figura 87, se muestra el comportamiento de la prueba de conectividad realizada desconectando el router de borde 01, teniendo una caída del enlace de 2 segundos, a partir del segundo 16 hasta el segundo 18.

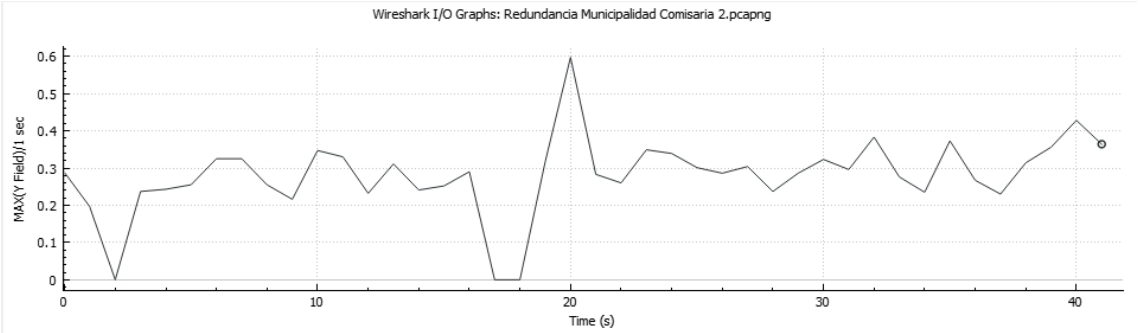


Figura 88. Tiempo de redundancia en las pruebas de conectividad entre la municipalidad y la Comisaría 2, con router de borde 01 desconectado.
Fuente: Elaboración propia.

6.3.2.2.2 Desconexión router de Borde 05

6.3.2.2.2.1 Comisaría 2 – Municipalidad

76 2001:db8:1001::1 56 61 5ms echo reply

77 2001:db8:1001::1 56 61 5ms echo reply

78 2001:db8:1001::1 56 61 3ms echo reply

79 2001:db8:1001::1 56 61 3ms echo reply

sent=80 received=77 packet-loss=3% min-rtt=2ms avg-rtt=2ms max-rtt=6ms

En la figura 88, se muestra el comportamiento de la prueba de conectividad realizada desconectando el router de borde 05, teniendo una caída del enlace de 3 segundos, a partir del segundo 33 hasta el segundo 36.

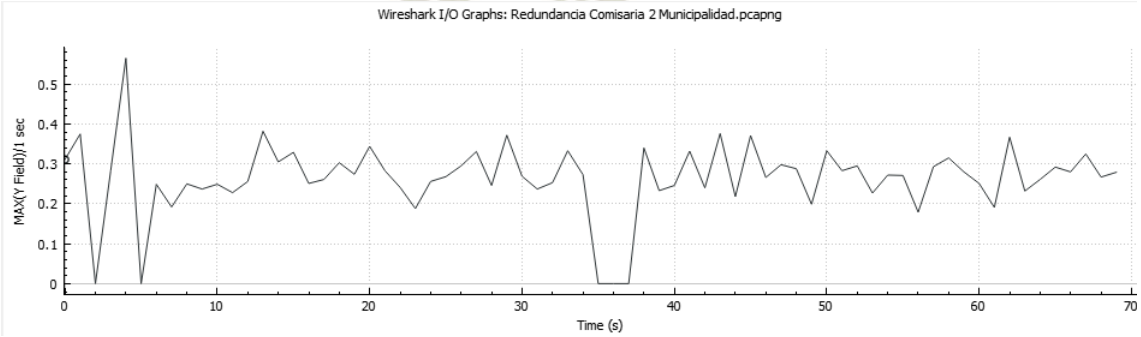


Figura 89. Tiempo de redundancia en las pruebas de conectividad entre la Comisaría 2 y la municipalidad, con router de borde 05 desconectado.
Fuente: Elaboración propia.

6.3.2.2.2.2 Comisaría 2 – Service 3

74 192.168.50.1 56 63 3ms

75 192.168.50.1 56 63 2ms

76 192.168.50.1 56 63 2ms

77 192.168.50.1 56 63 2ms

sent=78 received=75 packet-loss=3% min-rtt=1ms avg-rtt=2ms max-rtt=5ms

En la figura 89, se muestra el comportamiento de la prueba de conectividad realizada desconectando el router de borde 05, teniendo una caída del enlace de 3 segundos, a partir del segundo 27 hasta el segundo 30.

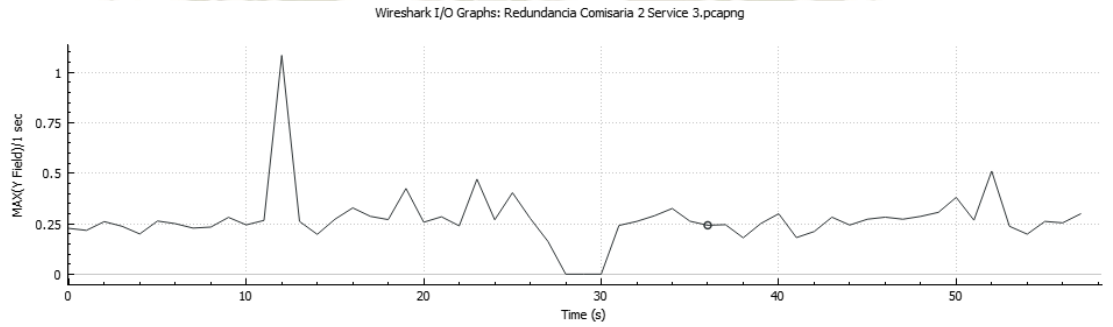


Figura 90. Tiempo de redundancia en las pruebas de conectividad entre la Comisaría 2 y service 3, con router de borde 05 desconectado.
Fuente: Elaboración propia.

6.3.2.3 Funcionamiento con Switch IXP 01 desconectado

6.3.2.3.1.1 Municipalidad – Service 3

32 192.168.50.1 56 63 2ms

33 192.168.50.1 timeout

34 10.1.1.2 84 64 0ms net unreachable

35 10.1.1.2 84 64 0ms net unreachable

36 no route to host

37 no route to host

38 no route to host

39 no route to host

sent=40 received=33 packet-loss=17% min-rtt=1ms avg-rtt=1ms max-rtt=4ms

En la figura 90, se muestra el comportamiento de la prueba de conectividad realizada desconectando el switch IXP 01, se observa que el enlace no vuelve a levantar luego del segundo 32, perdiendo comunicación total con el service 3.

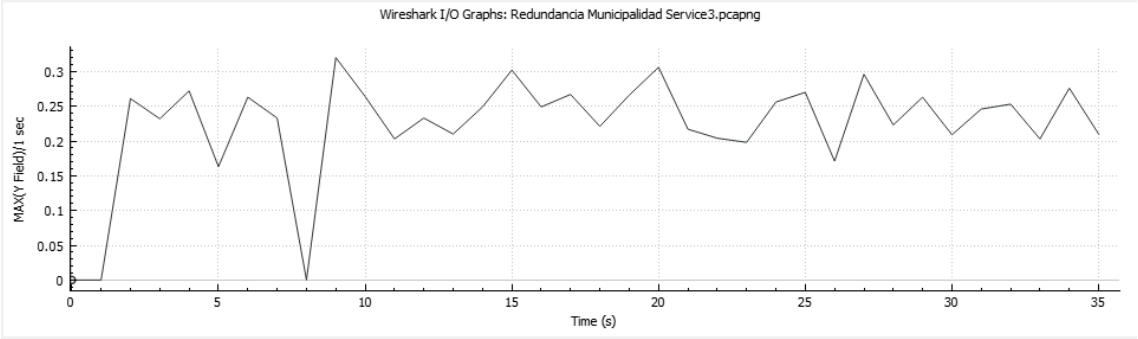


Figura 91. Tiempo de redundancia en las pruebas de conectividad entre la municipalidad y service 3, con el switch IXP 01 desconectado.
Fuente: Elaboración propia.

6.3.2.4 Funcionamiento con Switch IXP 02 desconectado

6.3.2.4.1.1 Municipalidad – Comisaría 1

42 10.2.2.1 56 62 2ms

43 10.2.2.1 56 62 2ms

44 10.2.2.1 56 62 2ms

45 10.2.2.1 56 62 2ms

sent=46 received=46 packet-loss=0% min-rtt=1ms avg-rtt=2ms max-rtt=7ms

En la figura 91, se muestra el comportamiento de la prueba de conectividad realizada desconectando el switch IXP 02, sin presentar caídas en el enlace.

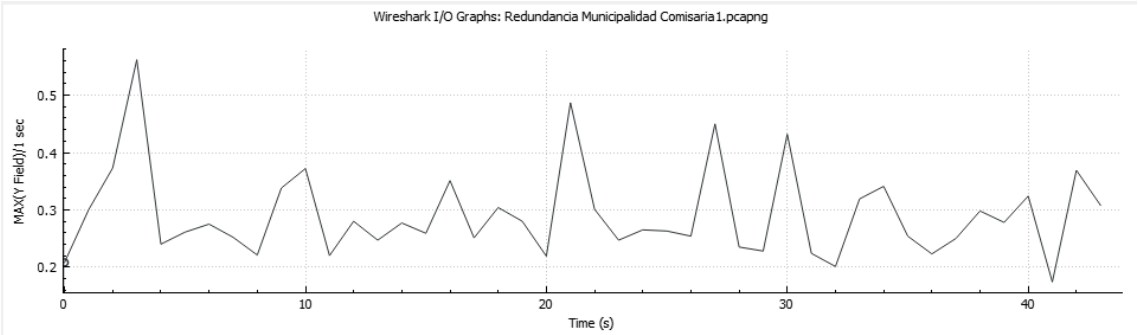


Figura 92. Tiempo de redundancia en las pruebas de conectividad entre la municipalidad y la Comisaría 1, con el switch IXP 02 desconectado.
Fuente: Elaboración propia.

6.3.2.4.1.2 Comisaría 2 – Service 4

36 2001:db8:1000::2 104 64 0ms net unreachable

37 2001:db8:1000::2 104 64 1ms net unreachable

38 no route to host

39 no route to host

sent=40 received=34 packet-loss=15% min-rtt=2ms avg-rtt=2ms max-rtt=13ms

En la figura 92, se muestra el comportamiento de la prueba de conectividad realizada desconectando el switch IXP 02, cayendo el enlace hacia el service 4 luego del segundo 30.

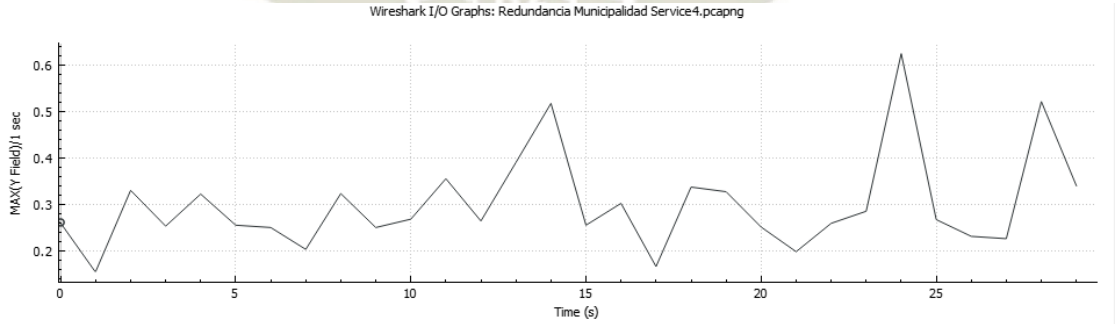


Figura 93. Tiempo de redundancia en las pruebas de conectividad entre la municipalidad y el service 4, con el switch IXP 02 desconectado.
Fuente: Elaboración propia.

6.3.2.5 Resultados

De acuerdo a las pruebas realizadas en esta sección, se logró la conectividad entre los diferentes miembros del punto de intercambio de tráfico.

Para las pruebas de redundancia de la topología se pusieron diferentes escenarios, luego de las simulaciones realizadas y de las figuras obtenidas de esas simulaciones se presentan las tablas resumen de cada una de ellas.

Como primera prueba se desconectó el router de borde 01 y se realizaron las pruebas de conectividad entre la municipalidad y las Comisarías para ambos casos, los tiempos de redundancia fueron de 3 segundos, tal como lo muestra la tabla 23 y 24 respectivamente.

Tabla 24. Conectividad entre la Municipalidad y la Comisarías 1 con el Router de Borde 01 desconectado

Conectividad Municipalidad y Comisaría 1				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad – Comisaría 1	60	57	3	3

Fuente: Elaboración propia.

Tabla 25. Conectividad entre la Municipalidad y la Comisarías 2 con el Router de Borde 01 desconectado

Conectividad Municipalidad y Comisaría 2				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad – Comisaría 2	38	36	2	2

Fuente: Elaboración propia.

Como segunda prueba se realizó la desconexión del router de borde 05 y se realizaron pruebas de conectividad entre la Comisaría 2 y la municipalidad, los resultados son mostrados en la tabla 25, obteniendo un tiempo de redundancia de 3 segundos.

Tabla 26. Conectividad entre la Comisaría 2 y la Municipalidad con el Router de Borde 05 desconectado

Conectividad Comisaría 2 y Municipalidad				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Comisaría 2 – Municipalidad	80	77	3	3

Fuente: Elaboración propia.

Y las pruebas de conectividad entre la Comisaría 2 y el router service 3, son mostrados en la tabla 26, obteniendo un tiempo de redundancia de 3 segundos.

Tabla 27. Conectividad entre la Comisaría 2 y el Service 3con el Router de Borde 05 desconectado

Conectividad Comisaría 2 y Service 3				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Comisaría 2 – Service 3	78	75	3	3

Fuente: Elaboración propia.

Como tercera prueba, se realizó con la desconexión del switch IXP 1, de esta forma se realizaron pruebas de conectividad entre la municipalidad y el service 3, con resultados mostrados en la tabla 27.

De esta prueba, podemos determinar que el enlace hacia el router service 3 no es redundante, por no contar con una doble conexión hacia los switch IXP 01 y 02 respectivamente.

Tabla 28. Conectividad entre la Municipalidad y el Service 3 con el Switch IXP 1 desconectado

Conectividad Municipalidad y Service 3				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad – Service 3	40	33	7	Sin redundancia

Fuente: Elaboración propia.

Finalmente, se realizó la prueba con la desconexión del switch IXP 02, probando la conectividad entre la Municipalidad y la Comisaría 1, con los resultados mostrados en la tabla 28.

De esta prueba podemos determinar que el enlace no se ve afectado, ya que el tráfico pasa solo por el Switch IXP 01.

Tabla 29. Conectividad entre la Municipalidad y la Comisaría 1 con el Switch IXP 02 desconectado

Conectividad Municipalidad y Comisaría 1				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad – Comisaría 1	46	46	46	Enlace no pierde conectividad

Fuente: Elaboración propia.

En la tabla 29 se muestran las pruebas de conectividad entre la municipalidad y el service 4, de lo cual podemos decir que el router de service 4 no es redundante en la topología por solo contar con un enlace hacia el switch IXP 02.

Tabla 30. Conectividad entre la Municipalidad y el Service 4 con el Switch IXP 02 desconectado

Conectividad Municipalidad y Service 4				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad – Service 4	40	34	6	No es redundante

Fuente: Elaboración propia.

Como conclusión del diseño de esta segunda propuesta, se verifica que la topología cumple con el nivel de redundancia requerido, pero no es lo suficientemente sostenible para poder soportar una arquitectura de red actual, por ello se presenta una tercera topología, diseñada sobre las ventajas obtenidas de esta topología pasando a un nivel mayor de redundancia y jerarquía.

Buscando el máximo enfoque en el aprovechamiento de los recursos y dando una visión de crecimiento conforme a la evolución actual de las redes de datos.

6.4 Tercera Propuesta

Como parte de la evolución de las redes, la necesidad de la creación de una propuesta sostenible, escalable y con un enfoque de crecimiento basado en una jerarquía de red, hace posible una diferenciación en el diseño de las redes propuestas anteriormente.

Con el aumento de tráfico que se va evidenciando con el pasar del tiempo, los requerimientos de las redes actuales basan su topología en enlaces de capacidad aumentable y sostenible con diferentes niveles de redundancia y modelos jerárquicos. En base a eso la topología de la propuesta dos, anteriormente mostrada, solo cumple con un nivel de redundancia y sin una visión hacia un crecimiento a futuro.

Es por ello, que esta tercera propuesta, propone una topología basada en jerarquización de tres niveles los cuales son denominados:

- Borde
- Core
- Acceso

Este diseño, presenta redundancia en los tres niveles, una topología escalable en crecimiento y configuración, ante el aumento de más participantes, con el aumento de posibles nodos y sosteniendo una capacidad de tráfico distribuida entre las tres partes, permitiendo así también el ingreso de futuros sistemas a la topología actual presentada.

En la figura 93 presentamos la topología propuesta, en la cual se implementan protocolos de enrutamiento dinámico tanto externos como internos, basado en el manejo de atributos para la selección de enlaces principales como secundarios.

Una topología libre de bucles, utilizando el protocolo de capa 2, RSTP (Rapid Spanning Tree Protocol), garantizando de esta forma la redundancia de la red ante una eventual caída de dispositivos.

Finalmente cuenta con la agregación de un servidor de rutas, para facilitar el emparejamiento entre los router de borde de los diferentes participantes y router de servicio en IPv4 e IPv6 only.

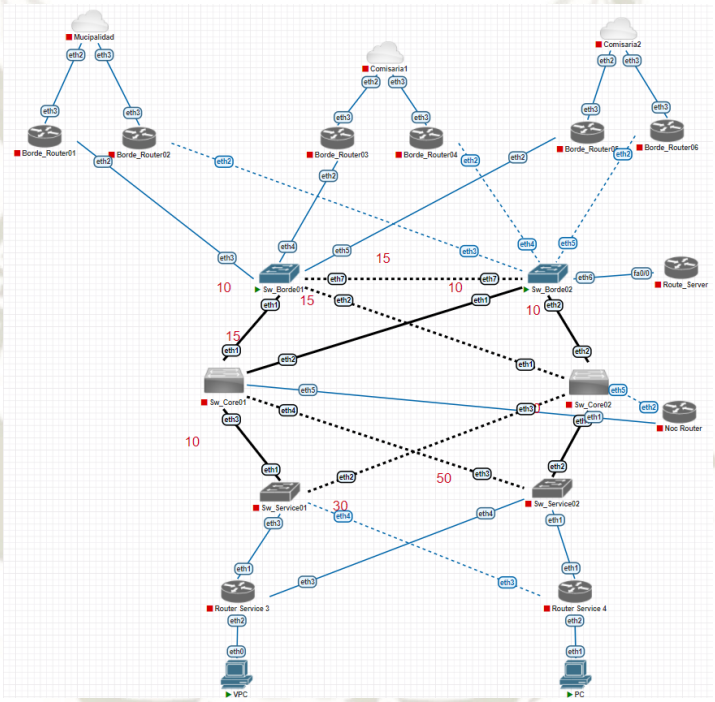


Figura 94. Topología de la tercera propuesta.
Fuente: Elaboración propia.

En la tabla 30, se enlistan los dispositivos implementados para la topología propuesta, la cantidad de enlaces y capacidades utilizada por cada participante.

Tabla 31. Distribución de dispositivos y enlaces de la tercera propuesta

Participante	**Router**	**Switch**	**Route Server**	**Enlaces Capacidad 1G**	**Enlaces Capacidad 10G**
Municipalidad	3	0	-----	2	0
Comisaría 1	3	0	-----	2	0
Comisaría 2	3	0	-----	2	0
IXP	3	6	1	7	9

Fuente: Elaboración propia.

En la tabla 31 se presenta un esquema generalizado de las redes de cada participante.

Tabla 32. Distribución de redes IPv4 e IPv6 y vlan propuesta 3

Participantes	IPV4				IPV6		Vlan	ASN
	Loopback	**Enlaces**	**Servicios**	**Noc**	**Enlaces**	**Servicios**		
Municipalidad	10.1.0.0/24	10.1.1.0/24	10.1.2.0/24	------	2001:db8:1000::/48	2001:db8:1001::/48	-----	20
Comisaría 1	10.2.0.0/24	10.2.1.0/24	10.2.2.0/24	------	2001:cafe::/48	2001:cafe:1::/48	-----	30
Comisaría 2	10.3.0.0/24	10.3.1.0/24	10.3.2.0/24	------	2001:cafe:1000::/48	2001:cafe:1001::/48	-----	40
IXP	10.10.9.0/24	10.10.10.0 /24	------	11.11.11.0/24	2001:db8::/48	------	100	50
Servicio 3	10.10.9.0/24	192.168.1.0/24	192.168.50.0/24	------	------	------		
		192.168.2.0/24					6	
Servicio 4	10.10.9.0/24	------	------	------	2001:db8:1:2::/64	2001:db8:1:1::/64	6	
					2001:db8:1::/64		4	

Fuente: Elaboración propia.

CAPÍTULO VII: APLICACIÓN PRÁCTICA TERCERA PROPUESTA

7. Simulación y análisis de resultados

7.1 Configuración y simulación de la topología

7.1.1 Distribución de IPs y Vlan por dispositivos.

En este apartado, mostraremos la distribución de Vlans e IPs configuradas en los dispositivos de la tercera propuesta.

La tabla 32 esquematiza las Vlan existentes, su función y los dispositivos en las que están configurados dentro de la topología.

Tabla 33. Vlans existentes en el punto de intercambio de tráfico

Vlan	Función	Dispositivos
3	Vlan de comunicación entre los router de borde, para el intercambio de redes con el service 3	Router de Borde, Switch Borde, Switch Core, Switch Acceso, Router Service 3
4	Vlan de comunicación entre los router de borde, para el intercambio de redes con el service 4	Router de Borde, Switch Borde, Switch Core, Switch Acceso, Router Service 4
5	Vlan de administración del Noc	Switch Borde, Switch Core, Switch Acceso, Router Service 3 y 4, Router Noc
6	Vlan de comunicación entre los router de borde, para el intercambio de	Router de Borde, Switch Borde, Switch Core, Switch Acceso, Router Service 3 y 4

	redes con los servicios 3 y 4	
100	Vlan de comunicación entre los router de borde, para el intercambio de redes de los miembros	Router de Borde, Switch Borde, Switch Core, Switch Acceso, Route server

Fuente: Elaboración propia.

Y la tabla 33 muestra la distribución de IPs por dispositivo planteado en la topología.

Tabla 34. Distribución de direcciones IP por dispositivo

Dispositivos	IPv4	Interface	IPv6	Interface
Municipalidad	10.1.0.1/32		Loopback	
	10.1.1.1/30	Ether 2		Ether 2
			2001:db8:1000::1/6	
	10.1.1.5/30	Ether 3	2001:db8:1000:1::1/64	Ether 3
	10.1.2.1/24	Red_Municipalidad	2001:db8:1001::1/64	Red_Municipalidad
Router de Borde 01	10.1.0.2/32		Loopback	
	10.1.1.2/30	Ether 3	2001:db8:1000::2/64	Ether 3
	192.168.1.2/24	Vlan 3	2001:db8:1::2:1/64	Vlan 4
	192.168.2.2/24	Vlan 6	2001:db8:1:2::2/64	Vlan 6
	10.10.10.6/24	Vlan 100	2001:db8::2:1/64	Vlan 100
Router de Borde 02	10.1.0.3/32		Loopback	
	10.1.1.6/30	Ether 3	2001:db8:1000:1::2/64	Ether 3
	192.168.1.3/24	Vlan 3	2001:db8:1::2:2/64	Vlan 4
	192.168.2.3/24	Vlan 6	2001:db8:1:2::3/64	Vlan 6
	10.10.10.7/24	Vlan 100	2001:db8::2:2/64	Vlan 100

Comisaría 1	10.2.0.1/32		Loopback	
	10.2.1.1/30	Ether 2	2001:cafe::1/64	Ether 2
	10.2.1.5/30	Ether 3	2001:cafe:0:1::1/64	Ether 3
	10.2.2.1/24	Red_Comisaría 1	2001:cafe:1::1/64	Red_Comisaría 1
Router de Borde 03	10.2.0.2/32		Loopback	
	10.2.1.2/30	Ether 3	2001:cafe::2/64	Ether 3
	192.168.1.4/24	Vlan 3	2001:db8:1::3:1/64	Vlan 4
	192.168.2.4/24	Vlan 6	2001:db8:1:2::4/64	Vlan 6
	10.10.10.8/24	Vlan 100	2001:db8::3:1/64	Vlan 100
Router de Borde 04	10.2.0.3/32		Loopback	
	10.2.1.6/30	Ether 3	2001:db8::3:2/64	Ether 3
	192.168.1.5/24	Vlan 3	2001:db8:1::3:2/64	Vlan 4
	192.168.2.5/24	Vlan 6	2001:cafe:0:1::2/64	Vlan 6
	10.10.10.9/24	Vlan 100	2001:db8:1:2::5/64	Vlan 100
Comisaría 2	10.3.0.1/32		Loopback	
	10.3.1.1/30	Ether 2	2001:cafe:1000::1/64	Ether 2
	10.3.1.5/30	Ether 3	2001:cafe:1000:1::1/64	Ether 3
	10.3.2.1/24	Red_Comisaría 2	2001:cafe:1001::1/64	Red_Comisaría 2
Router de Borde 05	10.3.0.2/32		Loopback	
	10.3.1.2/30	Ether 3	2001:cafe:1000::2/64	Ether 3
	192.168.1.6/24	Vlan 3	2001:db8:1::4:1/64	Vlan 4
	192.168.2.6/24	Vlan 6	2001:db8:1:2::6/64	Vlan 6
	10.10.10.10/24	Vlan 100	2001:db8::4:1/64	Vlan 100
Router de Borde 06	10.3.0.3/32		Loopback	
	10.3.1.6/30	Ether 3	2001:cafe:1000:1::2/64	Ether 3
	192.168.1.7/24	Vlan 3	2001:db8:1::4:2/64	Vlan 4

	192.168.2.7/24	Vlan 6	2001:db8:1:2::7/64	Vlan 6
	10.10.10.11/2	Vlan 100	2001:db8::4:2/64	Vlan 100
Route Server	10.10.10.2/2	Vlan 100	2001:DB8::1:2/64	Vlan 100
Switch de Borde 01	11.11.11.4/2	Vlan 5	----------	
Switch de Borde 02	11.11.11.5/2	Vlan 5		
Switch Core 01	11.11.11.2/3	Vlan 5		
Switch Core 02	11.11.11.3/4	Vlan 5		
Switch Service 01	11.11.11.6/5	Vlan 5		
Switch Service 02	11.11.11.7/6	Vlan 5		
Router Service 3	10.10.9.2/32	Loopback	----------	
	192.168.50.1/24	Ether 2		
	192.168.1.1/24	Vlan 3		
	11.11.11.8/24	Vlan 5		
	192.168.2.1/24	Vlan 6		
Router Service 4	10.1.0.254/32	Loopback		
	11.11.11.9/24	Vlan 5	2001:db8:1:1::1/64	Ether 2
	----------		2001:db8:1::1:1/64	Vlan 4
			2001:db8:1:2::1/64	Vlan 6

Fuente: Elaboración propia.

7.1.2 Configuración de Interfaces, IP y Vlan

Municipalidad

[tesis@Municipalidad]>

/interface bridge

add name=Loopback

add name=Red_Municipalidad

/IP address

add address=10.1.0.1 interface=Loopback network=10.1.0.3

add address=10.1.1.1/30 interface=ether2 network=10.1.1.0

add address=10.1.1.5/30 interface=ether3 network=10.1.1.4

add address=10.1.2.1/24 interface=Red_Municipalidad network=10.1.2.0

/IPv6 address

add address=2001:db8:1000::1 advertise=no interface=ether2

add address=2001:db8:1000:1::1 advertise=no interface=ether3

add address=2001:db8:1001::1 advertise=no interface=Red_Municipalidad

[tesis@Borde_Router01] >

/interface bridge

add name=Loopback

/interface vlan

add interface=ether2 name=vlan3 vlan-id=3

add interface=ether2 name=vlan4 vlan-id=4

add interface=ether2 name=vlan4 vlan-id=6

add interface=ether2 name=vlan100 vlan-id=100

/IP address

add address=10.10.10.6/24 interface=vlan100 network=10.10.10.0

add address=10.1.0.2 interface=Loopback network=10.1.0.1

add address=10.1.1.2/30 interface=ether3 network=10.1.1.0

add address=192.168.1.2/24 interface=vlan3 network=192.168.1.0

add address=192.168.2.2/24 interface=vlan6 network=192.168.2.0

/IPv6 address

add address=2001:db8:1::2:1 advertise=no interface=vlan4

add address=2001:db8::2:1 advertise=no interface=vlan100

add address=2001:db8:1000::2 advertise=no interface=ether3

add address=2001:db8:1:2::2 advertise=no interface=vlan6 **[tesis@Borde_Router02]** >

/interface bridge

add name=Loopback

add name=Trunk

/interface bridge port

add bridge=Trunk interface=ether2

/interface vlan

add interface=Trunk name=vlan3 vlan-id=3

add interface=Trunk name=vlan4 vlan-id=4

add interface=Trunk name=vlan4 vlan-id=6

add interface=Trunk name=vlan100 vlan-id=100

/IP address

/IP address

add address=10.10.10.7/24 interface=vlan100 network=10.10.10.0

add address=10.1.0.3 interface=Loopback network=10.1.0.2

add address=10.1.1.6/30 interface=ether3 network=10.1.1.4

add address=192.168.1.3/24 interface=vlan3 network=192.168.1.0

add address=192.168.2.3/24 interface=vlan6 network=192.168.2.0

/IPv6 address

add address=2001:db8:1::2:2 advertise=no interface=vlan4

add address=2001:db8::2:2 advertise=no interface=vlan100

add address=2001:db8:1000:1::2 advertise=no interface=ether3

add address=2001:db8:1:2::3 advertise=no interface=vlan6

Comisaría 1

[tesis@Comisaría01] >

/interface bridge

add name=Comisaría

add name=Loopback

/IP address

add address=10.2.0.1 interface=Loopback network=10.2.0.3

add address=10.2.1.1/30 interface=ether2 network=10.2.1.0

add address=10.2.1.5/30 interface=ether3 network=10.2.1.4

add address=10.2.2.1/24 interface=Comisaría network=10.2.2.0

/IPv6 address

add address=2001:cafe::1 advertise=no interface=ether2

add address=2001:cafe:0:1::1 advertise=no interface=ether3

add address=2001:cafe:1::1 advertise=no interface=Comisaría

[tesis@Borde_Router03] >

/interface bridge

add name=LoopBack

add name=Trunk

/interface vlan

add interface=Trunk name=vlan3 vlan-id=3

add interface=Trunk name=vlan4 vlan-id=4

add interface=Trunk name=vlan4 vlan-id=6

add interface=Trunk name=vlan100 vlan-id=100

/interface bridge port

add bridge=Trunk interface=ether2

/IP address

add address=10.10.10.8/24 interface=vlan100 network=10.10.10.0

add address=10.2.0.2 interface=LoopBack network=10.2.0.1

add address=10.2.1.2/30 interface=ether3 network=10.2.1.0

add address=192.168.1.4/24 interface=vlan3 network=192.168.1.0

add address=192.168.2.4/24 interface=vlan6 network=192.168.2.0

/IPv6 address

/IPv6 address

add address=2001:db8::3:1 advertise=no interface=vlan100

add address=2001:db8:1::3:1 advertise=no interface=vlan4

add address=2001:cafe::2 advertise=no interface=ether3

add address=2001:db8:1:2::4 advertise=no interface=vlan6 [tesis@Borde_Router04] >

/interface bridge

add name=Loopback

add name=Trunk

/interface vlan

add interface=Trunk name=vlan3 vlan-id=3

add interface=Trunk name=vlan4 vlan-id=4

add interface=Trunk name=vlan4 vlan-id=6

add interface=Trunk name=vlan100 vlan-id=100

/interface bridge port

add bridge=Trunk interface=ether2

/IP address

add address=10.10.10.9/24 interface=vlan100 network=10.10.10.0

add address=10.2.0.3 interface=Loopback network=10.2.0.2

add address=10.2.1.6/30 interface=ether3 network=10.2.1.4

add address=192.168.1.5/24 interface=vlan3 network=192.168.1.0

add address=192.168.2.5/24 interface=vlan6 network=192.168.2.0

/IPv6 address

add address=2001:db8::3:2 advertise=no interface=vlan100

add address=2001:db8:1::3:2 advertise=no interface=vlan4

add address=2001:cafe:0:1::2 advertise=no interface=ether3

add address=2001:db8:1:2::5 advertise=no interface=vlan6

Comisaría 2

[tesis@Comisaría02] >

/interface bridge

add name=Comisaría02

add name=Loopback

/IP address

add address=10.3.0.1 interface=Loopback network=10.3.0.3

add address=10.3.1.1/30 interface=ether2 network=10.3.1.0

add address=10.3.1.5/30 interface=ether3 network=10.3.1.4

add address=10.3.2.1/24 interface=Comisaría02 network=10.3.2.0

/IPv6 address

add address=2001:cafe:1000::1 advertise=no interface=ether2

add address=2001:cafe:1000:1::1 advertise=no interface=ether3

add address=2001:cafe:1001::1 advertise=no interface=Comisaría02

[tesis@Borde_Router05] >

/interface bridge

add name=Loopback

add name=Trunk

/interface vlan

add interface=Trunk name=vlan3 vlan-id=3

add interface=Trunk name=vlan4 vlan-id=4

add interface=Trunk name=vlan4 vlan-id=6

add interface=Trunk name=vlan100 vlan-id=100

/interface bridge port

add bridge=Trunk interface=ether2

/IP address

add address=10.10.10.10/24 interface=vlan100 network=10.10.10.0

add address=10.3.0.2 interface=Loopback network=10.3.0.1

add address=10.3.1.2/30 interface=ether3 network=10.3.1.0

add address=192.168.1.6/24 interface=vlan3 network=192.168.1.0

add address=192.168.2.6/24 interface=vlan6 network=192.168.2.0

/IPv6 address

add address=2001:db8::4:1 advertise=no interface=vlan100

add address=2001:db8:1::4:1 advertise=no interface=vlan4

add address=2001:cafe:1000::2 advertise=no interface=ether3

add address=2001:db8:1:2::6 advertise=no interface=vlan6

[tesis@Borde_Router06] >

/interface bridge

add name=Loopback

add name=Trunk

/interface vlan

add interface=Trunk name=vlan3 vlan-id=3

add interface=Trunk name=vlan4 vlan-id=4

add interface=Trunk name=vlan4 vlan-id=6

add interface=Trunk name=vlan100 vlan-id=100

/interface bridge port

add bridge=Trunk interface=ether2

/IP address

add address=10.10.10.11/24 interface=vlan100 network=10.10.10.0

add address=10.3.0.3 interface=Loopback network=10.3.0.2

add address=10.3.1.6/30 interface=ether3 network=10.3.1.4

add address=192.168.1.7/24 interface=vlan3 network=192.168.1.0

add address=192.168.2.7/24 interface=vlan6 network=192.168.2.0

/IPv6 address

add address=2001:db8:1::4:2 advertise=no interface=vlan4

add address=2001:db8::4:2 advertise=no interface=vlan100

add address=2001:cafe:1000:1::2 advertise=no interface=ether3

add address=2001:db8:1:2::7 advertise=no interface=vlan6

IXP

[tesis@Sw_Borde01] >

/interface bridge

add name=Trunk priority=0x4000

/interface vlan

add interface=Trunk name=vlan5 vlan-id=5

/interface bridge port

add bridge=Trunk interface=ether3

add bridge=Trunk interface=ether4

add bridge=Trunk interface=ether5

add bridge=Trunk interface=ether6 pvid=100

add bridge=Trunk interface=ether7 path-cost=15

add bridge=Trunk interface=ether1

add bridge=Trunk interface=ether2 path-cost=15

/IP address

add address=11.11.11.4/24 interface=vlan5 network=11.11.11.0

[tesis@Sw_Borde02] >

/interface bridge

add name=Trunk priority=0x5000

/interface vlan

add interface=Trunk name=vlan5 vlan-id=5

/interface bridge port

add bridge=Trunk interface=ether3

add bridge=Trunk interface=ether4

add bridge=Trunk interface=ether5

add bridge=Trunk interface=ether6 pvid=100

add bridge=Trunk interface=ether7 path-cost=15

add bridge=Trunk interface=ether1

add bridge=Trunk interface=ether2

/IP address

add address=11.11.11.5/24 interface=vlan5 network=11.11.11.0

[tesis@Sw_Core01] >

/interface bridge

add name=Trunk priority=0x1000

/interface vlan

add interface=Trunk name=vlan5 vlan-id=5

/interface bridge port

add bridge=Trunk interface=ether3

add bridge=Trunk interface=ether4

add bridge=Trunk interface=ether2

add bridge=Trunk interface=ether1

add bridge=Trunk interface=ether5

/IP address

add address=11.11.11.2/24 interface=vlan5 network=11.11.11.0

[tesis@Sw_Core02] >

/interface bridge

add name=Trunk priority=0x2000

/interface vlan

add interface=Trunk name=vlan5 vlan-id=5

/interface bridge port

add bridge=Trunk interface=ether3 path-cost=30

add bridge=Trunk interface=ether4

add bridge=Trunk interface=ether1 path-cost=15

add bridge=Trunk interface=ether2

add bridge=Trunk interface=ether5

/IP address

add address=11.11.11.3/24 interface=vlan5 network=11.11.11.0

[tesis@Sw_Service01] >

/interface bridge

add name=Trunk priority=0x6000

/interface vlan

add interface=Trunk name=vlan5 vlan-id=5

/interface bridge port

add bridge=Trunk interface=ether1

add bridge=Trunk interface=ether3

add bridge=Trunk interface=ether4

add bridge=Trunk interface=ether2 path-cost=30

/IP address

add address=11.11.11.6/24 interface=vlan5 network=11.11.11.0

[tesis@Sw_Service02] >

/interface bridge

add name=Trunk priority=0x7000

/interface vlan

add interface=Trunk name=vlan5 vlan-id=5

/interface bridge port

add bridge=Trunk interface=ether1

add bridge=Trunk interface=ether2

add bridge=Trunk interface=ether3 path-cost=50

add bridge=Trunk interface=ether4

/IP address

add address=11.11.11.7/24 interface=vlan5 network=11.11.11.0

[tesis@Service 3] >

/interface bridge

add name=Loopback

add name=Trunk

/interface vlan

add interface=Trunk name=vlan3 vlan-id=3

add interface=Trunk name=vlan5 vlan-id=5

add interface=ether3 name=vlan6 vlan-id=6

/interface bridge port

add bridge=Trunk interface=ether1 path-cost=1

/IP address

add address=192.168.1.1/24 interface=vlan3 network=192.168.1.0

add address=192.168.50.1/24 interface=ether2 network=192.168.50.0

add address=10.10.9.2 interface=Loopback network=10.10.9.2

add address=11.11.11.8/24 interface=vlan5 network=11.11.11.0

add address=192.168.2.1/24 interface=vlan6 network=192.168.2.0

[tesis@Service 4] >

/interface bridge

add name=Loopback

add name=Service

/interface vlan

add interface=ether3 name=vlan4 vlan-id=4

add interface=ether1 name=vlan5 vlan-id=5

add interface=ether1 name=vlan6 vlan-id=6

/IP address

add address=10.1.0.254 interface=Loopback network=10.1.0.254

add address=11.11.11.9/24 interface=vlan5 network=11.11.11.0

/IPv6 address

add address=2001:db8:1::1:1 advertise=no interface=vlan4

add address=2001:db8:1:1::1 interface=ether2

add address=2001:db8:1:2::1 advertise=no interface=vlan6

[tesis@NOC] >

/interface bridge

add name=Trunk

/interface vlan

add interface=Trunk name=vlan5 vlan-id=5

add interface=Trunk name=vlan100 vlan-id=100

/interface bonding

add mode=active-backup name=bonding1 primary=ether1 slaves=ether1,ether2

/interface bridge port

add bridge=Trunk interface=bonding1

/IP address

add address=11.11.11.1/24 interface=vlan5 network=11.11.11.0

add address=10.10.10.1/24 interface=vlan100 network=10.10.10.0

7.1.3 Configuración de OSPF

La conexión de los router de borde 01 y 02 con respecto al router de la municipalidad se muestran en la figura 94.

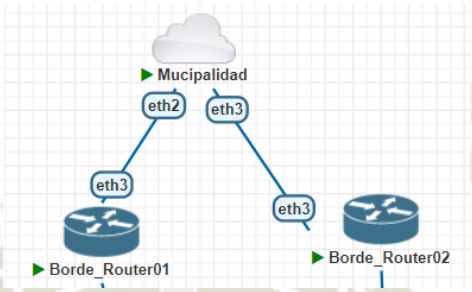


Figura 95. Enlaces entre la red de la municipalidad y los router borde.
Fuente: Elaboración propia.

[tesis@Municipalidad] >

/routing ospf instance

set [find default=yes] router-id=10.1.0.1

/routing ospf interface

add interface=ether3 network-type=point-to-point

add cost=9 interface=ether2 network-type=point-to-point

add interface=Red_Municipalidad network-type=point-to-point

/routing ospf network

add area=backbone network=10.1.1.4/30

add area=backbone network=10.1.1.0/30

add area=backbone network=10.1.2.0/24

/routing ospf-v3 instance

set [find default=yes] router-id=10.1.0.1

/routing ospf-v3 interface

add area=backbone interface=ether3 network-type=point-to-point

add area=backbone cost=9 interface=ether2 network-type=point-to-point

add area=backbone interface=Red_Municipalidad

[tesis@Borde_Router01] >

routing ospf instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.1.0.2

/routing ospf interface

add interface=ether3 network-type=point-to-point

/routing ospf network

add area=backbone network=10.1.1.0/30

/routing ospf-v3 instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.1.0.3

/routing ospf-v3 interface

add area=backbone interface=ether3 network-type=point-to-point

[tesis@Borde_Router02] >

/routing ospf instance

set [find default=yes] redistribute-bgp=as-type-2 router-id=10.1.0.3

/routing ospf interface

add interface=ether3 network-type=point-to-point

/routing ospf network

add area=backbone network=10.1.1.4/30

/routing ospf-v3 instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.1.0.3

/routing ospf-v3 interface

add area=backbone interface=ether3 network-type=point-to-point

La conexión de los router de borde 03 y 04 con respecto al router de la Comisaría 1 se muestran en la figura 95.

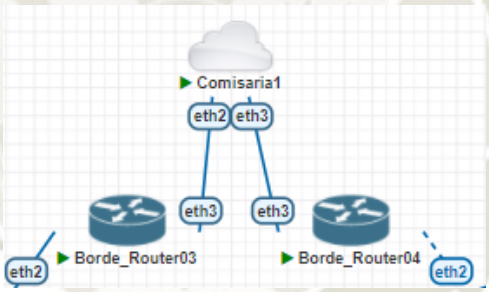


Figura 96. Enlaces entre la red de la Comisaría1 y los router borde.
Fuente: Elaboración propia.

[tesis@Comisaría01] >

/routing ospf instance

set [find default=yes] router-id=10.2.0.1

/routing ospf interface

add cost=9 interface=ether2 network-type=point-to-point

add interface=ether3 network-type=point-to-point

/routing ospf network

add area=backbone network=10.2.1.0/30

add area=backbone network=10.2.1.4/30

add area=backbone network=10.2.2.0/24

/routing ospf-v3 interface

add area=backbone cost=9 interface=ether2 network-type=point-to-point

add area=backbone interface=ether3 network-type=point-to-point

add area=backbone interface=Comisaría

[tesis@Borde_Router03] >

/routing ospf instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.2.0.2

/routing ospf interface

add interface=ether3 network-type=point-to-point

/routing ospf network

add area=backbone network=10.2.1.0/30

/routing ospf-v3 instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.2.0.2

/routing ospf-v3 interface

add area=backbone interface=ether3 network-type=point-to-point

[tesis@Borde_Router04] >

/routing ospf instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.2.0.3

/routing ospf interface

add interface=ether3 network-type=point-to-point

/routing ospf network

add area=backbone network=10.2.1.4/30

/routing ospf-v3 instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.2.0.3

/routing ospf-v3 interface

add area=backbone interface=ether3 network-type=point-to-point

La conexión de los router de borde 05 y 06 con respecto al router de la Comisaría 2 se muestran en la figura 96.

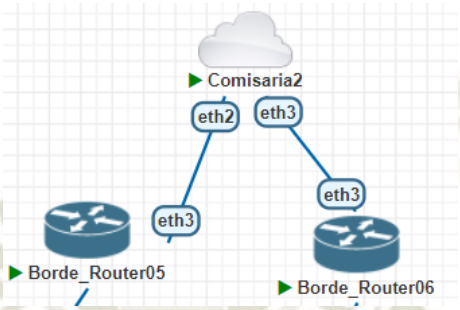


Figura 97. Enlaces entre la red de la Comisaría 2 y los router borde.
Fuente: Elaboración propia.

[tesis@Comisaría02] >

/routing ospf instance

set [find default=yes] router-id=10.3.0.1

/routing ospf interface

add cost=9 interface=ether2 network-type=point-to-point

add interface=ether3 network-type=point-to-point

/routing ospf network

add area=backbone network=10.3.1.0/30

add area=backbone network=10.3.1.4/30

add area=backbone network=10.3.2.0/24

/routing ospf-v3 instance

set [find default=yes] router-id=10.3.0.1

/routing ospf-v3 interface

add area=backbone cost=9 interface=ether2 network-type=point-to-point

add area=backbone interface=ether3 network-type=point-to-point

add area=backbone interface=Comisaría02

[tesis@Borde_Router05] >

/routing ospf instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.3.0.2

/routing ospf interface

add interface=ether3 network-type=point-to-point

/routing ospf network

add area=backbone network=10.3.1.0/30

/routing ospf-v3 instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.3.0.2

/routing ospf-v3 interface

add area=backbone interface=ether3 network-type=point-to-point

[tesis@Borde_Router06] >

/routing ospf instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.3.1.3

/routing ospf interface

add interface=ether3 network-type=point-to-point

/routing ospf network

add area=backbone network=10.3.1.4/30

/routing ospf-v3 instance

set [find default=yes] redistribute-bgp=as-type-1 router-id=10.3.1.3

/routing ospf-v3 interface

add area=backbone interface=ether3 network-type=point-to-point

7.1.4 Configuración de RSTP en los switch del IXP

Como parte de la configuración para obtener la redundancia en capa 2 dentro de la topología, el manejo del protocolo RSTP se hace indispensable.

En la figura 97 se aprecia la distribución de switch como sus costos de interfaz para poder implementar correctamente el protocolo RSTP.

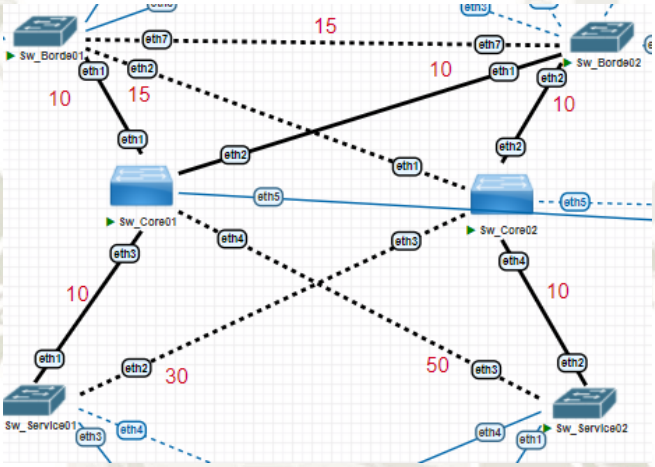


Figura 98. Distribución de costos en las interfaces en la topología del Punto de intercambio de tráfico.
Fuente: Elaboración propia.

El principio de RSTP consta en elegir un switch el cual tendrá el "root bridge" en sus interfaces, los switch adyacentes tendrán que hacer caminos que lleguen al Switch que contiene el root bridge, basado en los costos de cada interfaz, garantizando de esta manera que la topología de capa 2 no presente bucles, ya que las interfaces innecesarias por el momento se desactivarán lógicamente.

En el esquemático, para poder cumplir con los requerimientos dados, se eligió como switch principal al Sw_Core01, este switch es elegido como el switch principal ya que cuenta con el valor de prioridad menor entre todos los de la topología. Como segundo switch se eligió al Sw_Core02.

Para garantizar la topología sin bucles, así como las rutas que nosotros diseñamos para que puedan funcionar como alternas, se tuvo que configurar los valores de prioridad

de los enlaces según nuestro requerimiento y de esa forma adecuar el protocolo a nuestra necesidad.

En la tabla 34 se muestran los valores de prioridad de los switch, así como el costo por interfaz y el número de orden que tendría cada switch para convertirse en el principal.

Tabla 35. Valores de costos y prioridades de switch

			Costo de Interfaz					
Prioridad	**Valor de prioridad (HEX)**	**Dispositivos**	**Sw_Borde 01**	**Sw_Borde 02**	**Sw_Core 01**	**Sw_Core 02**	**Sw_Service 01**	**Sw_Service 02**
3°	4000	Switch_Borde 01	-----	15	10	15	-----	-----
4°	5000	Switch_Borde 02	15	-----	10	10	-----	-----
1°	1000	Switch_Core 01	10	10	-----	-----	10	50
2°	2000	Switch_Core 02	15	10	-----	-----	30	10
5°	6000	Switch_Service 01	-----	-----	10	30	-----	-----
6°	7000	Switch_Service 02	-----	-----	50	10	-----	-----

Fuente: Elaboración propia.

7.1.5 Configuración de BGP y filtros de enrutamiento en los router de borde Municipalidad

[tesis@Borde_Router01] >

/routing bgp instance

set default disabled=yes

add as=20 client-to-client-reflection=no name=Muni_Borde_Router01 redistribute-ospf=yes router-id=10.1.0.2

/routing bgp peer

add in-filter=Principal instance=Muni_Borde_Router01 name=Comisaría01_BR03 out-filter=Out remote-address=10.10.10.8 remote-as=30 use-bfd=yes

add in-filter=Principal instance=Muni_Borde_Router01 name=Comisaría02_BR05 out-filter=Out remote-address=10.10.10.10 remote-as=40 use-bfd=yes

add in-filter=Backup instance=Muni_Borde_Router01 name=Comisaría01_BR04 out-filter=Out remote-address=10.10.10.9 remote-as=30 use-bfd=yes

add in-filter=Backup instance=Muni_Borde_Router01 name=Comisaría02_BR06 out-filter=Out remote-address=10.10.10.11 remote-as=40 use-bfd=yes

add in-filter=Service3 instance=Muni_Borde_Router01 name=Service3 out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Muni_Borde_Router01 name=Comisaría01_BR03_IPv6 out-filter=OutIv6 remote-address=2001:db8::3:1 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Muni_Borde_Router01 name=Comisaría02_BR05_IPv6 out-filter=OutIv6 remote-address=2001:db8::4:1 remote-as=40 use-bfd=yes

add address-families=IPv6 in-filter=Backup instance=Muni_Borde_Router01 name=Comisaría01_BR04_IPv6 out-filter=OutIv6 remote-address=2001:db8::3:2 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Backup instance=Muni_Borde_Router01 name=Comisaría02_BR06_IPv6 out-filter=OutIv6 remote-address=2001:db8::4:2 remote-as=40 use-bfd=yes

add address-families=IPv6 in-filter=Service4 instance=Muni_Borde_Router01 name=Service4 out-filter=OutIv6 remote-address=2001:db8:1::1:1 remote-as=50 use-bfd=yes

add in-filter=Service3_Bckp instance=Muni_Borde_Router01 name=Service3_Bckp out-filter=Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Service4_Bckp instance=Muni_Borde_Router01 name=Service4_Bckp out-filter=OutIv6 remote-address=2001:db8:1:2::1 remote-as=50 use-bfd=yes

/routing filter

add action=accept chain=Out prefix=10.1.2.0/24

add action=discard chain=Out

add action=accept chain=Principal prefix=10.2.2.0/24

add action=accept chain=Principal prefix=10.3.2.0/24

add action=accept chain=Principal prefix=192.168.50.0/24

add action=accept chain=Principal prefix=2001:db8:1:1::/64

add action=accept chain=Principal prefix=2001:cafe:1::/64

add action=accept chain=Principal prefix=2001:cafe:1001::/64

add action=discard chain=Principal

add action=accept chain=Backup prefix=10.2.2.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=10.3.2.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:cafe:1::/64 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:cafe:1001::/64 set-bgp-local-pref=3

add action=discard chain=Backup set-bgp-local-pref=3

add action=accept chain=OutIv6 prefix=2001:db8:1001::/64

add action=discard chain=OutIv6

add action=accept chain=Service3 prefix=192.168.50.0/24

add action=discard chain=Service3

add action=accept chain=Service4 prefix=2001:db8:1:1::/64

add action=discard chain=Service4

add action=accept chain=Service3_Bckp prefix=192.168.50.0/24 set-bgp-local-pref=3

add action=discard chain=Service3_Bckp set-bgp-local-pref=3

add action=accept chain=Service4_Bckp prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=discard chain=Service4_Bckp set-bgp-local-pref=3

[tesis@Borde_Router02] >

/routing bgp instance

set default disabled=yes

add as=20 client-to-client-reflection=no name=Municipalidad_Backup redistribute-ospf=yes router-id=10.1.0.3

/routing bgp peer

add in-filter=Backup instance=Municipalidad_Backup name=Route_Server out-filter=Out remote-address=10.10.10.2 remote-as=50 tcp-md5-key=@qp-IXP use-bfd=yes

add in-filter=Principal instance=Municipalidad_Backup name=Comisaría1_BR03 out-filter=Out remote-address=10.10.10.8 remote-as=30 use-bfd=yes

add in-filter=Principal instance=Municipalidad_Backup name=Comisaría2_BR05 out-filter=Out remote-address=10.10.10.10 remote-as=40 use-bfd=yes

add address-families=IPv6 in-filter=Backup instance=Municipalidad_Backup name=Route_Server_IPv6 out-filter=OutIv6 remote-address=2001:db8::1:2 remote-as=50 tcp-md5-key=@qp-IXP use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Municipalidad_Backup name=Comisaría1_BR03_IPv6 out-filter=OutIv6 remote-address=2001:db8::3:1 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Municipalidad_Backup name=Comisaría2_BR05_IPv6 out-filter=OutIv6 remote-address=2001:db8::4:1 remote-as=40 use-bfd=yes

add in-filter=Service3 instance=Municipalidad_Backup name=Service3 out-filter=Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Service4 instance=Municipalidad_Backup name=Service4 out-filter=OutIv6 remote-address=2001:db8:1:2::1 remote-as=50 use-bfd=yes

add in-filter=Service3_Bkp instance=Municipalidad_Backup name=Service3_Bckp out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Service4_Bkp instance=Municipalidad_Backup name=Service4_Bckp out-filter=OutIv6 remote-address=2001:db8:1::1:1 remote-as=50 use-bfd=yes

/routing filter

add action=accept chain=Out prefix=10.1.2.0/24

add action=discard chain=Out

add action=accept chain=Principal prefix=10.2.2.0/24

add action=accept chain=Principal prefix=10.3.2.0/24

add action=accept chain=Principal prefix=192.168.50.0/24

add action=accept chain=Principal prefix=2001:db8:1:1::/64

add action=accept chain=Principal prefix=2001:cafe:1::/64

add action=accept chain=Principal prefix=2001:cafe:1001::/64

add action=discard chain=Principal

add action=accept chain=Backup prefix=10.2.2.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=10.3.2.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:cafe:1::/64 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:cafe:1001::/64 set-bgp-local-pref=3

add action=discard chain=Backup set-bgp-local-pref=3

add action=accept chain=OutIv6 prefix=2001:db8:1001::/64

add action=discard chain=OutIv6

add action=accept chain=Service3 prefix=192.168.50.0/24

add action=discard chain=Service3

add action=accept chain=Service4 prefix=2001:db8:1:1::/64

add action=discard chain=Service4

add action=accept chain=Service3_Bkp prefix=192.168.50.0/24 set-bgp-local-pref=3

add action=discard chain=Service3_Bkp set-bgp-local-pref=3

add action=accept chain=Service4_Bkp prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=discard chain=Service4_Bkp set-bgp-local-pref=3

Comisaría 1

[tesis@Borde_Router03] >

/routing bgp instance

set default disabled=yes

add as=30 client-to-client-reflection=no name=Comi_Borde_Router03 redistribute-ospf=yes router-id=10.2.0.2

/routing bgp peer

add in-filter=Principal instance=Comi_Borde_Router03 name=Municipalidad_BR01 out-filter=Out remote-address=10.10.10.6 remote-as=20 use-bfd=yes

add in-filter=Backup instance=Comi_Borde_Router03 name=MunicIPlaidad_BR02 out-filter=Out remote-address=10.10.10.7 remote-as=20 use-bfd=yes

add in-filter=Principal instance=Comi_Borde_Router03 name=Comisaría2_BR05 out-filter=Out remote-address=10.10.10.10 remote-as=40 use-bfd=yes

add in-filter=Backup instance=Comi_Borde_Router03 name=Comisaría2_BR06 out-filter=Out remote-address=10.10.10.11 remote-as=40 use-bfd=yes

add in-filter=Service3 instance=Comi_Borde_Router03 name=Service3 out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Comi_Borde_Router03 name=Municipalidad_BR01_IPv6 out-filter=OutIPv6 remote-address=2001:db8::2:1 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Backup instance=Comi_Borde_Router03 name=MunicIPlaidad_BR02_IPv6 out-filter=OutIPv6 remote-address=2001:db8::2:2 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Comi_Borde_Router03 name=Comisaría2_BR05_IPv6 out-filter=OutIPv6 remote-address=2001:db8::4:1 remote-as=40 use-bfd=yes

add address-families=IPv6 in-filter=Backup instance=Comi_Borde_Router03 name=Comisaría2_BR06_IPv6 out-filter=OutIPv6 remote-address=2001:db8::4:2 remote-as=40 use-bfd=yes

add address-families=IPv6 in-filter=Service4 instance=Comi_Borde_Router03 name=Service4 out-filter=OutIPv6 remote-address=2001:db8:1::1:1 remote-as=50 use-bfd=yes

add in-filter=Service3_Bckp instance=Comi_Borde_Router03 name=Service3_Bckp out-filter=Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Service4 instance=Comi_Borde_Router03 name=Service4_Bckp out-filter=OutIPv6 remote-address=2001:db8:1:2::1 remote-as=50 use-bfd=yes

/routing filter

add action=accept chain=Principal prefix=10.1.2.0/24

add action=accept chain=Principal prefix=10.3.2.0/24

add action=accept chain=Principal prefix=192.168.50.0/24

add action=accept chain=Principal prefix=2001:db8:1:1::/64

add action=accept chain=Principal prefix=2001:db8:1001::/64

add action=accept chain=Principal prefix=2001:cafe:1001::/64

add action=discard chain=Principal

add action=accept chain=Backup prefix=10.1.2.0/24 set-bgp-prepend=3

add action=accept chain=Backup prefix=10.3.2.0/24 set-bgp-prepend=3

add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-prepend=3

add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-prepend=3

add action=accept chain=Backup prefix=2001:db8:1001::/64 set-bgp-prepend=3

add action=accept chain=Backup prefix=2001:cafe:1001::/64 set-bgp-prepend=3

add action=discard chain=Backup set-bgp-prepend=3

add action=accept chain=Out prefix=10.2.2.0/24

add action=discard chain=Out

add action=accept chain=OutIPv6 prefix=2001:cafe:1::/64

add action=discard chain=OutIPv6

add action=accept chain=Service3 prefix=192.168.50.0/24

add action=discard chain=Service3

add action=accept chain=Service4 prefix=2001:db8:1:1::/64

add action=discard chain=Service4

add action=accept chain=Service3_Bckp prefix=192.168.50.0/24 set-bgp-local-pref=3

add action=discard chain=Service3_Bckp set-bgp-local-pref=3

add action=accept chain=Service4_Bckp prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=discard chain=Service4_Bckp set-bgp-local-pref=3

[tesis@Borde_Router04] >

/routing bgp instance

set default disabled=yes

add as=30 client-to-client-reflection=no name=Comisaría01_Backup redistribute-ospf=yes router-id=10.2.0.3

/routing bgp peer

add in-filter=Backup instance=Comisaría01_Backup name=Router_Server02 out-filter=Out remote-address=10.10.10.2 remote-as=50 tcp-md5-key=@qp-IXP use-bfd=yes

add in-filter=Principal instance=Comisaría01_Backup name=Municipalidad_BR01 out-filter=Out remote-address=10.10.10.6 remote-as=20 use-bfd=yes

add in-filter=Principal instance=Comisaría01_Backup name=Comisaría2_BR05 out-filter=Out remote-address=10.10.10.10 remote-as=40 use-bfd=yes

add in-filter=Service3_Bkp instance=Comisaría01_Backup name=Service3_Bckp out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Backup instance=Comisaría01_Backup name=Route_Server02_IPv6 out-filter=OutIPv6 remote-address=2001:db8::1:2 remote-as=50 tcp-md5-key=@qp-IXP use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Comisaría01_Backup name=Municipalidad_BR01_IPv6 out-filter=OutIPv6 remote-address=2001:db8::2:1 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Comisaría01_Backup name=Comisaría2_BR05_IPv6 out-filter=OutIPv6 remote-address=2001:db8::4:1 remote-as=40 use-bfd=yes

add address-families=IPv6 in-filter=Service4_Bkp instance=Comisaría01_Backup name=Service4_Bckp out-filter=OutIPv6 remote-address=2001:db8:1::1:1 remote-as=50 use-bfd=yes

add in-filter=Service3 instance=Comisaría01_Backup name=Service3 out-filter=Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Service4 instance=Comisaría01_Backup name=Service4 out-filter=OutIPv6 remote-address=2001:db8:1:2::1 remote-as=50 use-bfd=yes

/routing filter

add action=accept chain=Principal prefix=10.1.2.0/24

add action=accept chain=Principal prefix=10.3.2.0/24

add action=accept chain=Principal prefix=192.168.50.0/24

add action=accept chain=Principal prefix=2001:db8:1:1::/64

add action=accept chain=Principal prefix=2001:db8:1001::/64

add action=accept chain=Principal prefix=2001:cafe:1001::/64

add action=discard chain=Principal

add action=accept chain=Backup prefix=10.1.2.0/24 set-bgp-prepend=3

add action=accept chain=Backup prefix=10.3.2.0/24 set-bgp-prepend=3

add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-prepend=3

add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-prepend=3

add action=accept chain=Backup prefix=2001:db8:1001::/64 set-bgp-prepend=3

add action=accept chain=Backup prefix=2001:cafe:1001::/64 set-bgp-prepend=3

add action=discard chain=Backup set-bgp-prepend=3

add action=accept chain=Out prefix=10.2.2.0/24

add action=discard chain=Out

add action=accept chain=OutIPv6 prefix=2001:cafe:1::/64

add action=discard chain=OutIPv6

add action=accept chain=Service3 prefix=192.168.50.0/24

add action=discard chain=Service3

add action=accept chain=Service4 prefix=2001:db8:1:1::/64

add action=discard chain=Service4

add action=accept chain=Service3_Bkp prefix=192.168.50.0/24 set-bgp-local-pref=3

add action=discard chain=Service3_Bkp set-bgp-local-pref=3

add action=accept chain=Service4_Bkp prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=discard chain=Service4_Bkp set-bgp-local-pref=3

Comisaría 2

[tesis@Borde_Router05] >

/routing bgp instance

set default disabled=yes

add as=40 client-to-client-reflection=no name=Comisaría_Borde_Router05 redistribute-ospf=yes router-id=10.3.0.2

/routing bgp peer

add in-filter=Principal instance=Comisaría_Borde_Router05 name=Municipalidad_BR01 out-filter=Out remote-address=10.10.10.6 remote-as=20 use-bfd=yes

add in-filter=Principal instance=Comisaría_Borde_Router05 name=Comisaría1_BR03 out-filter=Out remote-address=10.10.10.8 remote-as=30 use-bfd=yes

add in-filter=Backup instance=Comisaría_Borde_Router05 name=Municipalidad_BR02 out-filter=Out remote-address=10.10.10.7 remote-as=20 use-bfd=yes

add in-filter=Backup instance=Comisaría_Borde_Router05 name=Comisaría1_BR04 out-filter=Out remote-address=10.10.10.9 remote-as=30 use-bfd=yes

add in-filter=Service3 instance=Comisaría_Borde_Router05 name=Service3 out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Comisaría_Borde_Router05 name=Municipalidad_BR01_IPv6 out-filter=OutIPv6 remote-address=2001:db8::2:1 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Comisaría_Borde_Router05 name=Comisaría1_BR03_Iv6 out-filter=OutIPv6 remote-address=2001:db8::3:1 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Comisaría_Borde_Router05 name=Comisaría1_BR04_IPv6 out-filter=OutIPv6 remote-address=2001:db8::3:2 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Backup instance=Comisaría_Borde_Router05 name=Municipalidad_BR02_IPv6 out-filter=OutIPv6 remote-address=2001:db8::2:2 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Service4 instance=Comisaría_Borde_Router05 name=Service4 out-filter=OutIPv6 remote-address=2001:db8:1::1:1 remote-as=50 use-bfd=yes

add in-filter=Service3_Bckp instance=Comisaría_Borde_Router05 name=Service3_Bckp out-filter=Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Service4_Bckp instance=Comisaría_Borde_Router05 name=Service4_Bckp out-filter=OutIPv6 remote-address=2001:db8:1:2::1 remote-as=50 use-bfd=yes

/routing filter

add action=accept chain=Principal prefix=10.1.2.0/24

add action=accept chain=Principal prefix=10.2.2.0/24

add action=accept chain=Principal prefix=192.168.50.0/24

add action=accept chain=Principal prefix=2001:db8:1:1::/64

add action=accept chain=Principal prefix=2001:db8:1001::/64

add action=accept chain=Principal prefix=2001:cafe:1::/64

add action=accept chain=Backup prefix=10.1.2.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=10.2.2.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:db8:1001::/64 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:cafe:1::/64 set-bgp-local-pref=3

add action=accept chain=Out prefix=10.3.2.0/24

add action=discard chain=Out

add action=accept chain=OutIPv6 prefix=2001:cafe:1001::/64

add action=discard chain=OutIPv6

add action=accept chain=Service3 prefix=192.168.50.0/24

add action=discard chain=Service3

add action=accept chain=Service4 prefix=2001:db8:1:1::/64

add action=discard chain=Service4

add action=accept chain=Service3_Bckp prefix=192.168.50.0/24 set-bgp-local-pref=3

add action=discard chain=Service3_Bckp set-bgp-local-pref=3

add action=accept chain=Service4_Bckp prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=discard chain=Service4_Bckp set-bgp-local-pref=3

[tesis@Borde_Router06] >

/routing bgp instance

set default disabled=yes

add as=40 client-to-client-reflection=no name=Comisaría02_Backup redistribute-ospf=yes router-id=10.3.0.3

/routing bgp peer

add in-filter=Backup instance=Comisaría02_Backup name=Route_Server02 out-filter=Out remote-address=10.10.10.2 remote-as=50 tcp-md5-key=@qp-IXP use-bfd=yes

add in-filter=Principal instance=Comisaría02_Backup name=Municipalidad_BR01 out-filter=Out remote-address=10.10.10.6 remote-as=20 use-bfd=yes

add in-filter=Principal instance=Comisaría02_Backup name=Comisaría1_BR03 out-filter=Out remote-address=10.10.10.8 remote-as=30 use-bfd=yes

add in-filter=Service3_Bkp instance=Comisaría02_Backup name=Service3_Bckp out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Backup instance=Comisaría02_Backup name=Route_Server_IPv6 out-filter=OutIPv6 remote-address=2001:db8::1:2 remote-as=50 tcp-md5-key=@qp-IXP use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Comisaría02_Backup name=Municipalidad_BR01_IPv6 out-filter=OutIPv6 remote-address=2001:db8::2:1 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Principal instance=Comisaría02_Backup name=Comisaría1_BR03_IPv6 out-filter=OutIPv6 remote-address=2001:db8::3:1 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Service4_Bkp instance=Comisaría02_Backup name=Service4_Bckp out-filter=OutIPv6 remote-address=2001:db8:1::1:1 remote-as=50 use-bfd=yes

add in-filter=Service3 instance=Comisaría02_Backup name=Service3 out-filter=Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes

add address-families=IPv6 in-filter=Service4 instance=Comisaría02_Backup name=Service4 out-filter=OutIPv6 remote-address=2001:db8:1:2::1 remote-as=50 use-bfd=yes

/routing filter

add action=accept chain=Principal prefix=10.1.2.0/24

```
add action=accept chain=Principal prefix=10.2.2.0/24

add action=accept chain=Principal prefix=192.168.50.0/24

add action=accept chain=Principal prefix=2001:db8:1:1::/64

add action=accept chain=Principal prefix=2001:db8:1001::/64

add action=accept chain=Principal prefix=2001:cafe:1::/64

add action=accept chain=Backup prefix=10.1.2.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=10.2.2.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:db8:1001::/64 set-bgp-local-pref=3

add action=accept chain=Backup prefix=2001:cafe:1::/64 set-bgp-local-pref=3

add action=accept chain=Out prefix=10.3.2.0/24

add action=discard chain=Out

add action=accept chain=OutIPv6 prefix=2001:cafe:1001::/64

add action=discard chain=OutIPv6

add action=accept chain=Service3 prefix=192.168.50.0/24

add action=discard chain=Service3

add action=accept chain=Service4 prefix=2001:db8:1:1::/64

add action=discard chain=Service4

add action=accept chain=Service3_Bkp prefix=192.168.50.0/24 set-bgp-local-pref=3
```

add action=discard chain=Service3_Bkp set-bgp-local-pref=3

add action=accept chain=Service4_Bkp prefix=2001:db8:1:1::/64 set-bgp-local-pref=3

add action=discard chain=Service4_Bkp set-bgp-local-pref=3

7.1.6 Configuración de Route Server

Se utilizo como route server, la imagen de un dispositivo cisco, el cual nos permite realizar las configuraciones y tener el comportamiento de un route server.

La conexión del route server se hace por medio de los switch de borde, para este caso se interconecta al switch de borde 02 como se muestra en la figura 98.

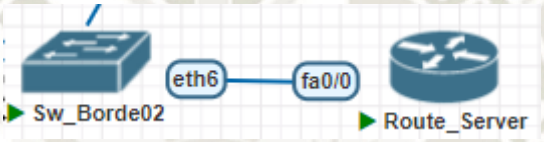


Figura 99. Topología de interconexión del route server.
Fuente: Elaboración propia.

Route_Server#

enable

configure terminal

interface FastEthernet0/0.100

encapsulation dot1q 100

IP address 10.10.10.2 255.255.255.0

IPv6 address 2001:db8::1:2/64

no shutdown

exit

interface FastEthernet0/0

no shutdown

exit

IPv6 Unicast-routing

router bgp 50

bgp log-neighbor-changes

neighbor IXP peer-group

neighbor IXP password @qp-IXP

neighbor 10.10.10.7 remote-as 20

neighbor 10.10.10.7 peer-group IXP

neighbor 10.10.10.9 remote-as 30

neighbor 10.10.10.9 peer-group IXP

neighbor 10.10.10.11 remote-as 40

neighbor 10.10.10.11 peer-group IXP

exit

router bgp 50

bgp log-neighbor-changes

neighbor 1xp peer-group

neighbor 1xp password @qp-IXP

neighbor 2001:db8::2:2 remote-as 20

neighbor 2001:db8::2:2 peer-group 1xp

neighbor 2001:db8::3:2 remote-as 30

neighbor 2001:db8::3:2 peer-group 1xp

neighbor 2001:db8::4:2 remote-as 40

neighbor 2001:db8::4:2 peer-group 1xp

address-family IPv6

neighbor 2001:db8::2:2 activate

neighbor 2001:db8::3:2 activate

neighbor 2001:db8::4:2 activate

exit

7.1.7 Configuración BGP Router Service 3 y Router Service 4

La interconexión de los router de servicio 3 y 4 se ilustran en la figura 99.

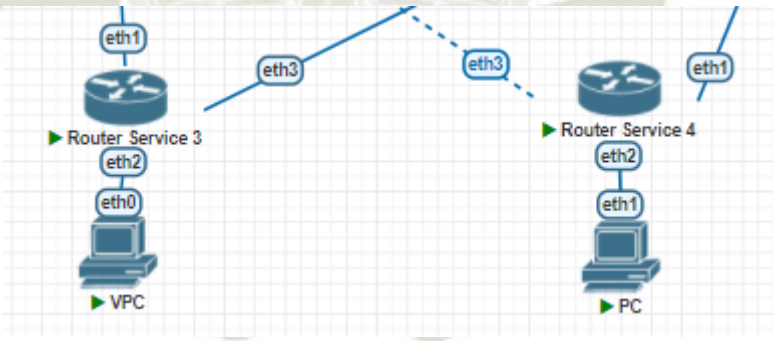


Figura 100. Topología de interconexión de los router de servicio 3 y 4.
Fuente: Elaboración propia.

Service 3

[tesis@Service 3] >

/routing bgp instance

set default disabled=yes

add as=50 client-to-client-reflection=no name=Service3 router-id=10.10.9.2

/routing bgp network

add network=192.168.50.0/24 synchronize=no

/routing bgp peer

add in-filter=Muni_Principal instance=Service3 name=Municipalidad_BR01 out-filter=Out remote-address=192.168.1.2 remote-as=20 use-bfd=yes

add in-filter=Comisaría1_Principal instance=Service3 name=Comisaría1_BR03 out-filter=Out remote-address=192.168.1.4 remote-as=30 use-bfd=yes

add in-filter=Comisaría1_Bckp instance=Service3 name=Comisaría1_BR04_Bckp out-filter=Out remote-address=192.168.1.5 remote-as=30 use-bfd=yes

add in-filter=Comisaría2_Principal instance=Service3 name=Comisaría2_BR05 out-filter=Out remote-address=192.168.1.6 remote-as=40 use-bfd=yes

add in-filter=Comisaría2_Bckp instance=Service3 name=Comisaría2_BR06_Bckp out-filter=Out remote-address=192.168.1.7 remote-as=40 use-bfd=yes

add hold-time=5s in-filter=Muni_Backup instance=Service3 name=Municipalidad_BR02 out-filter=Out remote-address=192.168.2.3 remote-as=20 use-bfd=yes

add in-filter=Muni_Principal instance=Service3 name=Municipalidad_BR01_Bckp out-filter=Out remote-address=192.168.2.2 remote-as=20 use-bfd=yes

add hold-time=5s in-filter=Muni_Backup instance=Service3 name=Municipalidad_BR02_Bckp out-filter=Out remote-address=192.168.1.3 remote-as=20 use-bfd=yes

add in-filter=Comisaría1_Bckp instance=Service3 name=Comisaría1_BR03_Bckp out-filter=Out remote-address=192.168.2.4 remote-as=30 use-bfd=yes

add in-filter=Comisaría1_Principal instance=Service3 name=Comisaría1_BR04 out-filter=Out remote-address=192.168.2.5 remote-as=30 use-bfd=yes

add in-filter=Comisaría2_Bckp instance=Service3 name=Comisaría2_BR05_Bckp out-filter=Out remote-address=192.168.2.6 remote-as=40 use-bfd=yes

add in-filter=Comisaría2_Principal instance=Service3 name=Comisaría2_BR06 out-filter=Out remote-address=192.168.2.7 remote-as=40 use-bfd=yes

/routing filter

add action=accept chain=Muni_Principal prefix=10.1.2.0/24

add action=discard chain=Muni_Principal

add action=accept chain=Muni_Backup prefix=10.1.2.0/24 set-bgp-local-pref=3

add action=accept chain=Muni_Backup set-bgp-local-pref=3

add action=accept chain=Out prefix=192.168.50.0/24

add action=discard chain=Out

add action=accept chain=Comisaría1_Principal prefix=10.2.2.0/24

add action=accept chain=Comisaría1_Bckp prefix=10.2.2.0/24 set-bgp-local-pref=3

add action=discard chain=Comisaría1_Principal

add action=discard chain=Comisaría1_Bckp set-bgp-local-pref=3

add action=accept chain=Comisaría2_Principal prefix=10.3.2.0/24

add action=discard chain=Comisaría2_Principal

add action=accept chain=Comisaría2_Bckp prefix=10.3.2.0/24 set-bgp-local-pref=3

add action=discard chain=Comisaría2_Bckp set-bgp-local-pref=3

Service 4

[tesis@Service4] >

/routing bgp instance

set default disabled=yes

add as=50 client-to-client-reflection=no name=Service4 router-id=10.1.0.254

/routing bgp network

add network=2001:db8:1:1::/64 synchronize=no

/routing bgp peer

add address-families=IPv6 in-filter=Muni_Principal instance=Service4 name=Municipalidad_BR01 out-filter=Out remote-address=2001:db8:1::2:1 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Comisaría1_Principal instance=Service4 name=Comisaría1_BR03 out-filter=Out remote-address=2001:db8:1::3:1 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Comisaría1_Bckp instance=Service4 name=Comisaría1_BB04_Bckp out-filter=Out remote-address=2001:db8:1::3:2 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Comisaría2_Principal instance=Service4 name=Comisaría2_BR05 out-filter=Out remote-address=2001:db8:1::4:1 remote-as=40 use-bfd=yes

add address-families=IPv6 in-filter=Comisaría2_Principal instance=Service4 name=Comisaría2_BR06 out-filter=Out remote-address=2001:db8:1::4:2 remote-as=40 use-bfd=yes

add address-families=IPv6 in-filter=Muni_Backup instance=Service4 name=Municipalidad_BR02_Bckp out-filter=Out remote-address=2001:db8:1:2::3 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Muni_Principal instance=Service4 name=Municipalidad_BR02 out-filter=Out remote-address=2001:db8:1::2:2 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Muni_Backup instance=Service4 name=Municipalidad_BR01_Bckp out-filter=Out remote-address=2001:db8:1:2::2 remote-as=20 use-bfd=yes

add address-families=IPv6 in-filter=Comisaría1_Bckp instance=Service4 name=Comisaría1_BR03_Backup out-filter=Out remote-address=2001:db8:1:2::4 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Comisaría1_Principal instance=Service4 name=Comisaría1_BB04 out-filter=Out remote-address=2001:db8:1:2::5 remote-as=30 use-bfd=yes

add address-families=IPv6 in-filter=Comisaría2_Bckp instance=Service4 name=Comisaría2_BR05_Bckp out-filter=Out remote-address=2001:db8:1:2::6 remote-as=40 use-bfd=yes

add address-families=IPv6 in-filter=Comisaría2_Bckp instance=Service4 name=Comisaría2_BR06_Bckp out-filter=Out remote-address=2001:db8:1:2::7 remote-as=40 use-bfd=yes

/routing filter

add action=accept chain=Muni_Principal prefix=2001:db8:1001::/64

add action=discard chain=Muni_Principal

add action=accept chain=Muni_Backup prefix=2001:db8:1001::/64 set-bgp-local-pref=3

add action=discard chain=Muni_Backup set-bgp-local-pref=3

add action=accept chain=Out prefix=2001:db8:1:1::/64

add action=discard chain=Out prefix=2001:db8:1:1::/64

add action=accept chain=Comisaría1_Principal prefix=2001:cafe:1::/64

add action=accept chain=Comisaría1_Bckp prefix=2001:cafe:1::/64 set-bgp-local-pref=3

add action=discard chain=Comisaría1_Principal

add action=discard chain=Comisaría1_Bckp set-bgp-local-pref=3

add action=accept chain=Comisaría2_Principal prefix=2001:cafe:1001::/64

add action=discard chain=Comisaría2_Principal

add action=accept chain=Comisaría2_Bckp prefix=2001:cafe:1001::/64 set-bgp-local-pref=3

add action=discard chain=Comisaría2_Bckp set-bgp-local-pref=3

7.1.8 Noc Router

El router denominado Noc Router, es el encargado de controlar el punto de intercambio de tráfico desde la infraestructura interna, su conexión con la topología lo podemos ver en la figura 100.

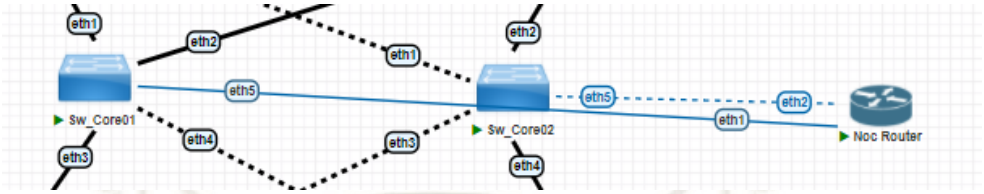


Figura 101. Topología de conexión del noc router.
Fuente: Elaboración propia.

Tiene dos conexiones simultaneas a los Switch Core, con la finalidad de dar redundancia de enlaces con un protocolo denominado Bonding “Active Backup” que deshabilita lógicamente la interfaz denominada secundaria. La comunicación con los dispositivos del punto de intercambio de tráfico y el Noc router, es por medio de vlan.

El Noc router, cuenta con dos vlan, la primera denominada vlan 5, que es la vlan de administración independiente de los dispositivos del punto de intercambio de tráfico, y la vlan 100, que es del rango del route server para poder acceder a su configuración.

7.1.9 Managment Máquina Virtual

El acceso a cada equipo para su configuración y verificación se hace por medio de una interfaz bridge entregada por el emulador.

Dicha interfaz es denominada managment cloud y permite unir la interfaz física de la computadora, con la interfaz de la máquina virtual.

La interfaz managment es presentada en la figura 101.

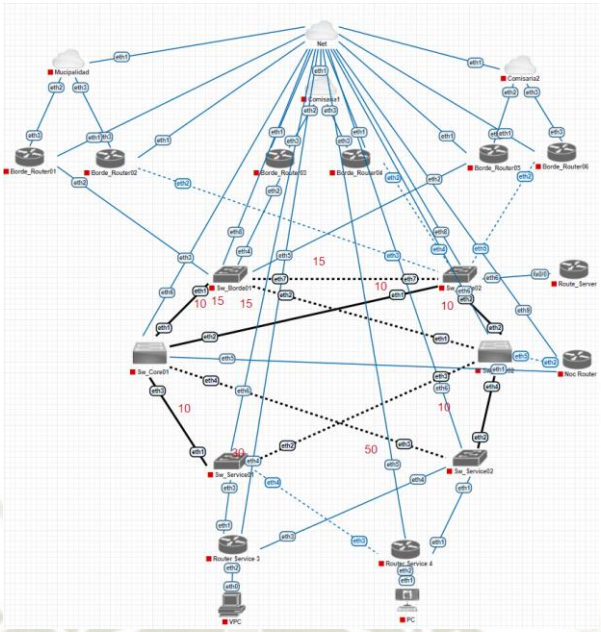


Figura 102. Interfaz Managmente cloud para la administración y verificación de dispositivos.
Fuente: Elaboración propia.

Con ayuda de esta interfaz virtual, nos permite acceder a los equipos por medio de WinBox, como lo muestra la figura 102.

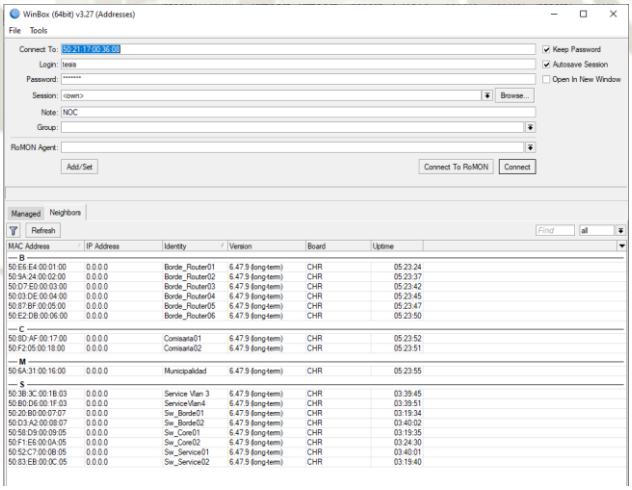


Figura 103. Interfaz WinBox con el listado de dispositivos que contempla la topología del punto de intercambio de tráfico de la tercera propuesta.
Fuente: Elaboración propia.

7.2 Análisis de resultados

En la siguiente sección se mostrarán los resultados obtenidos de la simulación de la tercera topología propuesta, mostrando el análisis de las etapas que conllevaron el diseño de esta propuesta.

7.2.1 Establecimiento de enrutamiento OSPF

Según el diseño propuesto, la primera etapa de interconexión entre los miembros del punto de intercambio de tráfico con sus router de borde será por medio del protocolo de enrutamiento dinámico OSPF.

Se realizará el análisis previo al establecimiento de adyacencias del protocolo OSPF por medio del software de análisis de red Wireshark

En la figura 103, se muestra el proceso llevado por el router de la municipalidad con el router de borde 01 para poder establecer el enrutamiento entre ambos dispositivos.

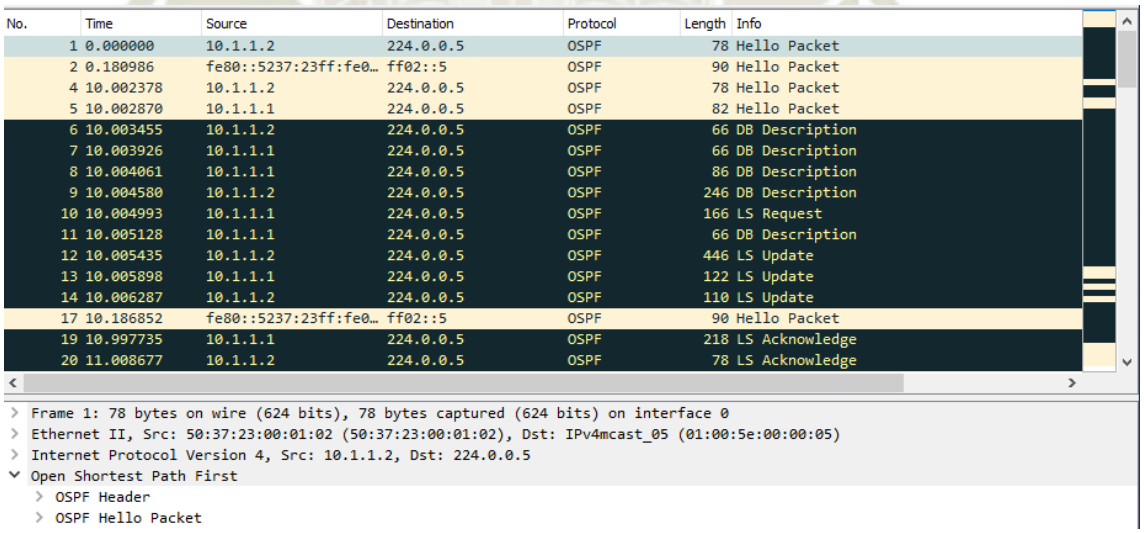


Figura 104. Captura de Wireshark en el establecimiento de sesiones OSPF del router de la municipalidad.
Fuente: Elaboración propia.

La IP 224.0.0.5 es una dirección Multicast utilizada por OSPF para poder establecer la comunicación con sus vecinos.

Para poder establecer la adyacencia entre dispositivos, estos tuvieron que compartir los cinco mensajes de OSPF, estableciendo estos mensajes desde la IP 10.1.1.1 correspondiente al router de la municipalidad hacia la IP Multicast 224.0.0.5 para comunicarse con su vecino directo, el router de borde 01.

Como respuesta, el router de borde 01 con IP 10.1.1.2 envía los datos correspondientes en el mensaje hacia la IP 224.0.0.5 para que de dicha forma el router de la municipalidad reciba esta información.

Este proceso de comunicación se cumple para todos los mensajes que OSPF requiere para poder establecer la adyacencia.

7.2.2 Selección de interfaces por medio de costos OSPF

La selección de interfaces por medio de OSPF, se maneja en base al valor del costo que posee cada interfaz, la interfaz que tenga el menor valor, será la seleccionada como interfaz principal.

Para nuestro caso, ejemplificando la red de la municipalidad, el router de borde 01 está conectado a la ether2 y el router de borde 02 a la ether3.

En base a esa elección de costos se elige la interfaz ether2 tanto del OSPF v2 como OSPF v3 con el valor de 9.

En la figura 104 se muestra la configuración de OSPF en el router de la Municipalidad, para manejar los costos de las interfaces.

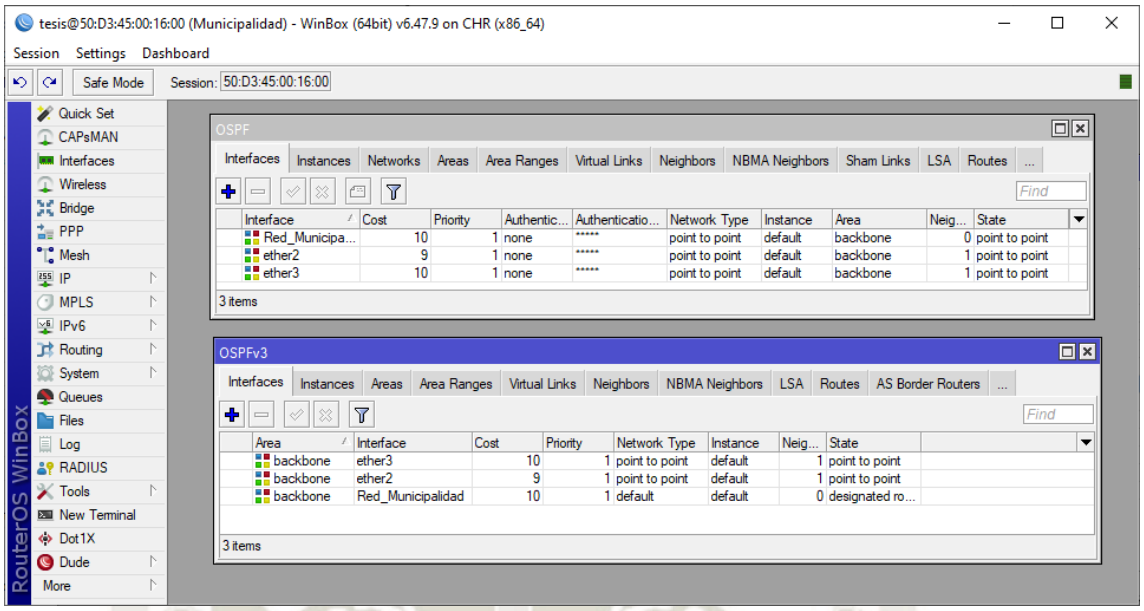


Figura 105. Interfaz WinBox manejo de costos por interfaz para determinar enlaces principales y secundarios.
Fuente: Elaboración propia.

La selectividad de interfaces, se ve reflejada en la tabla de rutas, tal como se muestra en la figura 105.

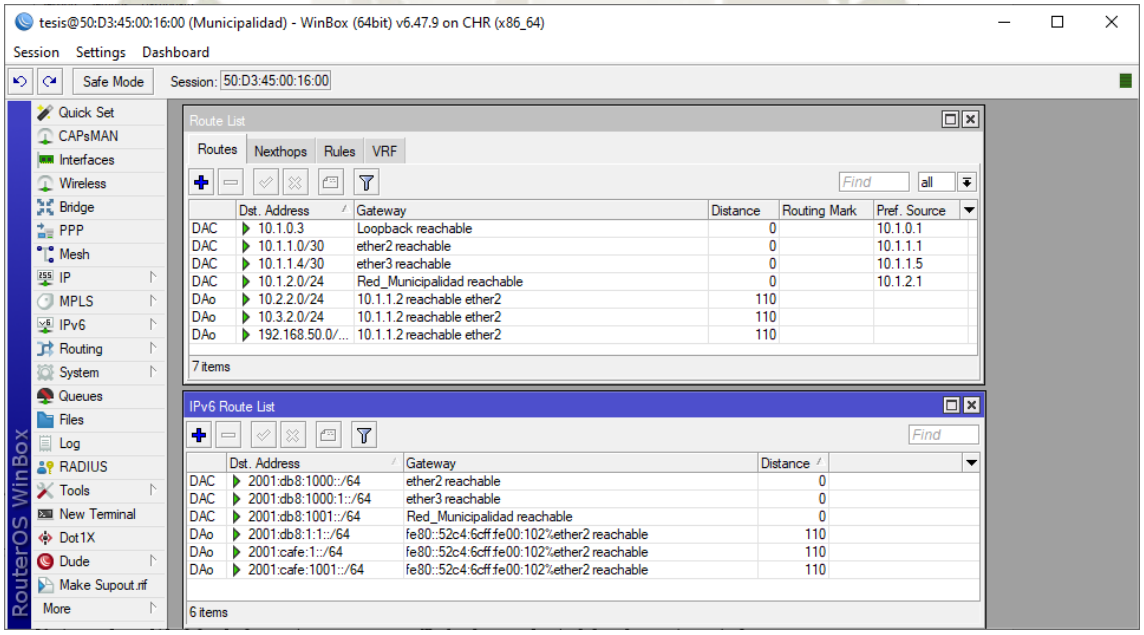


Figura 106. Interfaz WinBox tabla de ruta correspondiente al router de la municipalidad.
Fuente: Elaboración propia.

Todas las redes destino son alcanzables a través de la IP correspondiente al router de borde 01, es decir, por la ether2.

7.2.3 Establecimiento de sesiones BGP

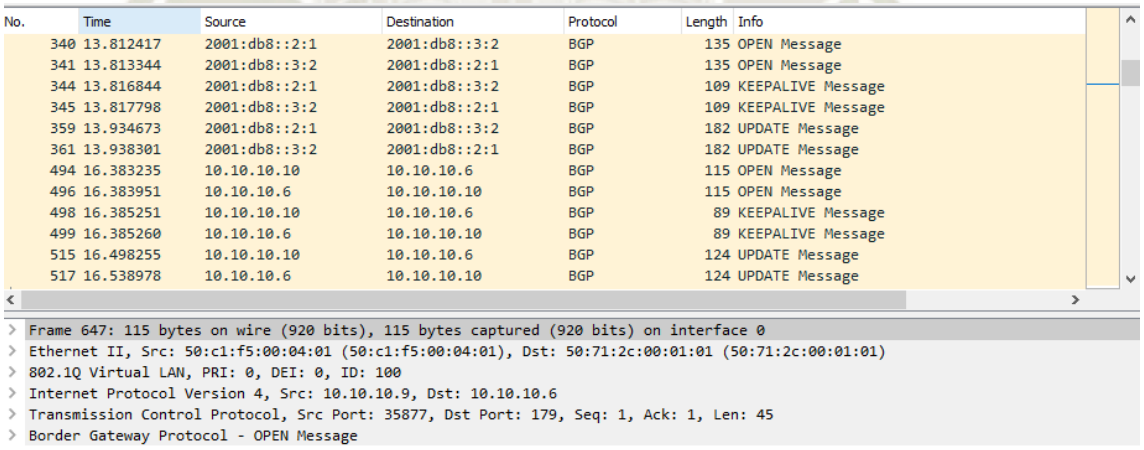
Se realizará el análisis previo al establecimiento de sesión BGP por medio del software de análisis de red Wireshark.

Y se mostrará el resultado obtenido de cada router de borde luego de establecer las sesiones con todos los vecinos configurados tanto en IPv4 como IPv6.

7.2.3.1 Análisis del establecimiento de Sesión BGP

Como se mencionó, el protocolo BGP es un protocolo de enrutamiento el cual establece sesiones con sus pares intercambiando información en sesiones establecidas por medio del protocolo TCP y puerto 179.

En la figura 106 se visualiza el proceso del establecimiento de las sesiones BGP del router de borde 01 de IPv6 2001:db8::2:1 e IPv4 10.10.10.6 con el router de borde 04 de IP 2001:db8::3:2 y el router de borde 05 de IP 10.10.10.10.



No.	Time	Source	Destination	Protocol	Length	Info
340	13.812417	2001:db8::2:1	2001:db8::3:2	BGP	135	OPEN Message
341	13.813344	2001:db8::3:2	2001:db8::2:1	BGP	135	OPEN Message
344	13.816844	2001:db8::2:1	2001:db8::3:2	BGP	109	KEEPALIVE Message
345	13.817798	2001:db8::3:2	2001:db8::2:1	BGP	109	KEEPALIVE Message
359	13.934673	2001:db8::2:1	2001:db8::3:2	BGP	182	UPDATE Message
361	13.938301	2001:db8::3:2	2001:db8::2:1	BGP	182	UPDATE Message
494	16.383235	10.10.10.10	10.10.10.6	BGP	115	OPEN Message
496	16.383951	10.10.10.6	10.10.10.10	BGP	115	OPEN Message
498	16.385251	10.10.10.10	10.10.10.6	BGP	89	KEEPALIVE Message
499	16.385260	10.10.10.6	10.10.10.10	BGP	89	KEEPALIVE Message
515	16.498255	10.10.10.10	10.10.10.6	BGP	124	UPDATE Message
517	16.538978	10.10.10.6	10.10.10.10	BGP	124	UPDATE Message

```
> Frame 647: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface 0
> Ethernet II, Src: 50:c1:f5:00:04:01 (50:c1:f5:00:04:01), Dst: 50:71:2c:00:01:01 (50:71:2c:00:01:01)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: 10.10.10.9, Dst: 10.10.10.6
> Transmission Control Protocol, Src Port: 35877, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
> Border Gateway Protocol - OPEN Message
```

Figura 107. Captura de Wireshark del establecimiento de sesiones BGP del router de borde 01.
Fuente: Elaboración propia.

Previo al establecimiento la sesión BGP, los router deben establecer tres tipos de mensajes, los cuales son Open, Keepalive y Update.

En la figura 106 el mensaje Open, intercambia información del tipo de versión de la sesión, el número de sistema autónomo, el identificador y otros datos opcionales primarios.

Luego de recibidos esos mensajes por ambas partes, existe un mensaje de reconocimiento y confirmación de conectividad con el vecino, este es el mensaje Keepalive.

Finalmente, los mensajes de Update actualizan la información entre vecinos, enviando nuevos destinos o eliminando los destinos que ya no existan.

7.2.3.2 Router de Borde de la Municipalidad

La figura 107 y 108 muestran la tabla de sesiones BGP establecidas por los router de borde 01 y 02 respectivamente.

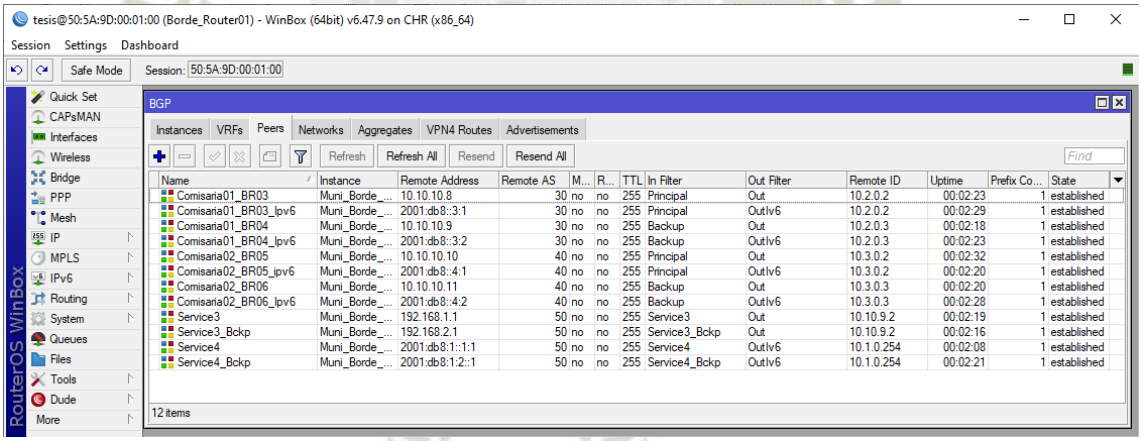


Figura 108. Interfaz WinBox con el listado de sesiones BGP activas en el router de borde 01.
Fuente: Elaboración propia.

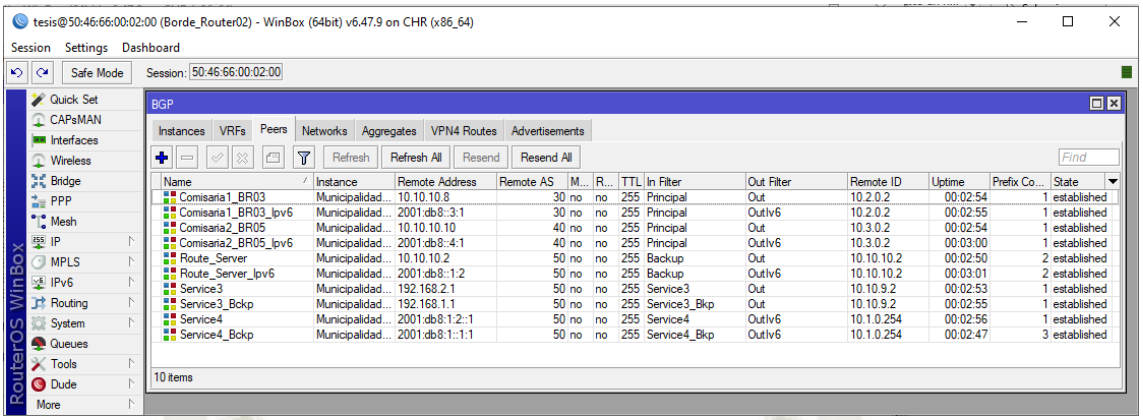


Figura 109. Interfaz WinBox con el listado de sesiones BGP activas en el router de borde 02.
Fuente: Elaboración propia.

El router de borde 02 cuenta con menos sesiones BGP, ya que establece sesión con el route server el cual tiene la IP 10.10.10.2 y 2001:db8::1:2 a través de la sesión multilateral.

De esa forma las sesiones con los router de borde 04 y 06 se ve resumida en una sola sesión.

7.2.3.3 Router de Borde de la Comisaría 1

Las figuras 109 y 110 se muestra la tabla de sesiones BGP establecidas del router de borde 03 y 04 respectivamente.

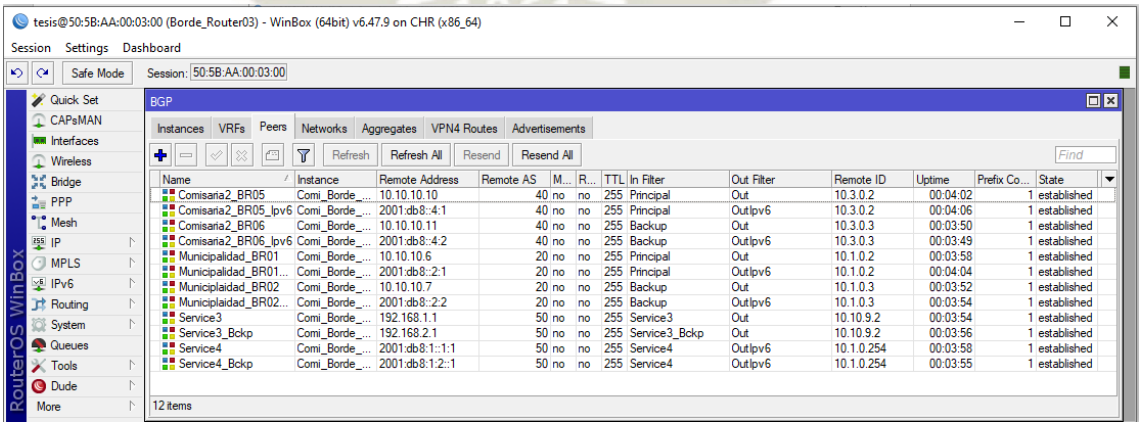


Figura 110. Interfaz WinBox con el listado de sesiones BGP activas en el router de borde 03.
Fuente: Elaboración propia.

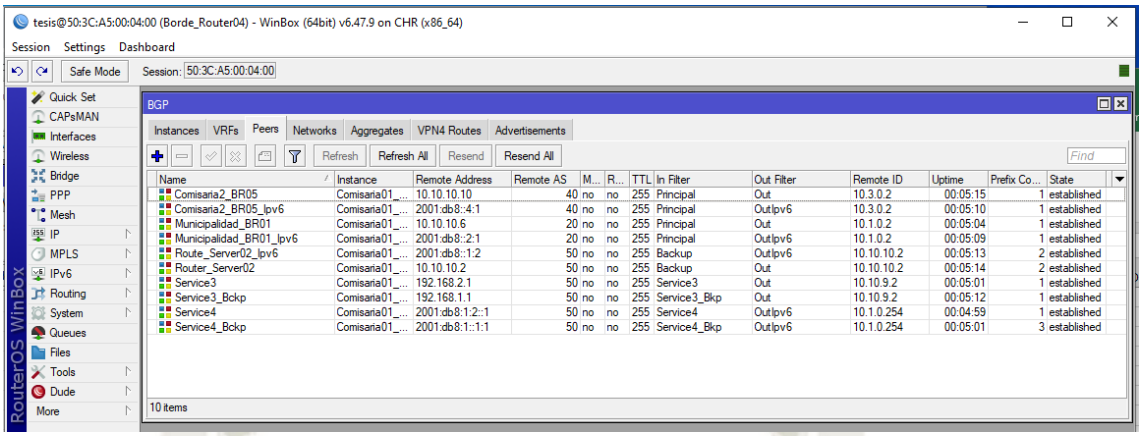


Figura 111. Interfaz WinBox con el listado de sesiones BGP activas en el router de borde 04.
Fuente: Elaboración propia.

Al igual que el router de borde 02, el router de borde 04 establece una sesión BGP con el route server y de esa forma reduce el número de sesiones necesarias para establecer con todos sus pares.

7.2.3.4 Router de Borde de la Comisaría 2

Las figuras 111 y 112 muestran la tabla de sesiones BGP establecidas en los router de borde 05 y 06 respectivamente.

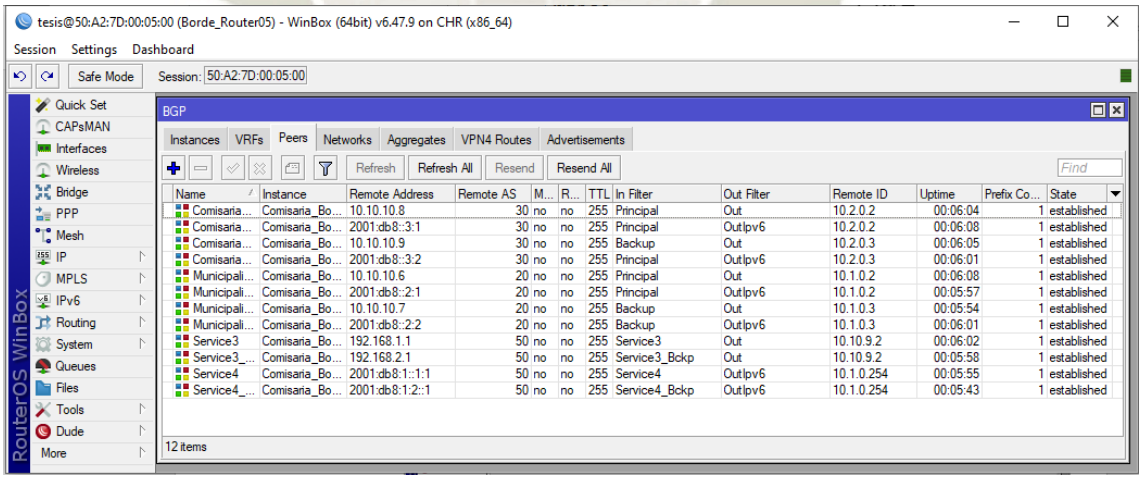


Figura 112. Interfaz WinBox con el listado de sesiones BGP activas en el router de borde 05.
Fuente: Elaboración propia.

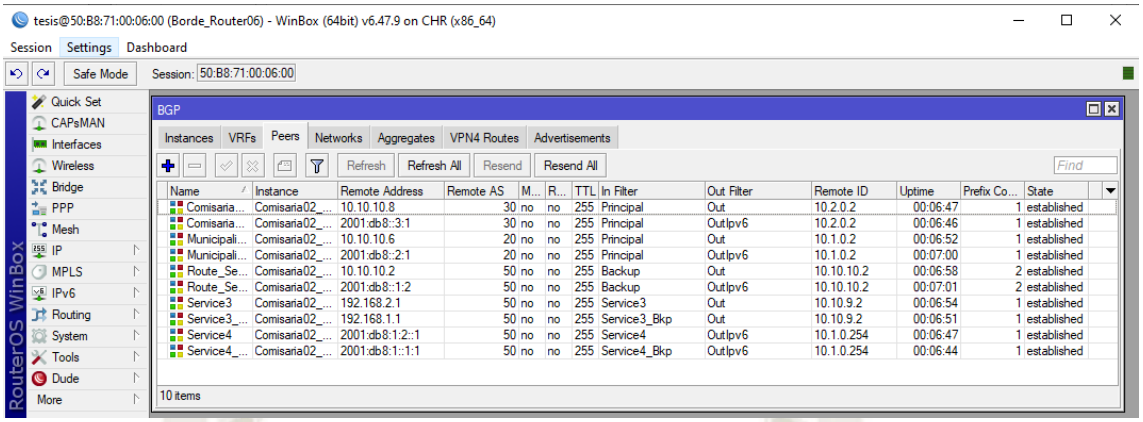


Figura 113. Interfaz WinBox con el listado de sesiones BGP activas en el router de borde 06.
Fuente: Elaboración propia.

El router de borde 06 al igual que el 02 y 04 establece una sesión con el route server en una sesión multilateral.

Los router de borde 02, 04 y 06 establecen la parte backup de la topología propuesta en la parte de borde.

7.2.3.5 Router de Servicios

Las figuras 113 y 114 muestran las sesiones BGP establecidas para los router de servicio 3 y 4.

Ninguno de ellos cuenta con una sesión hacia el router server, por ello poseen sesiones independientes con cada miembro y sus router de borde.

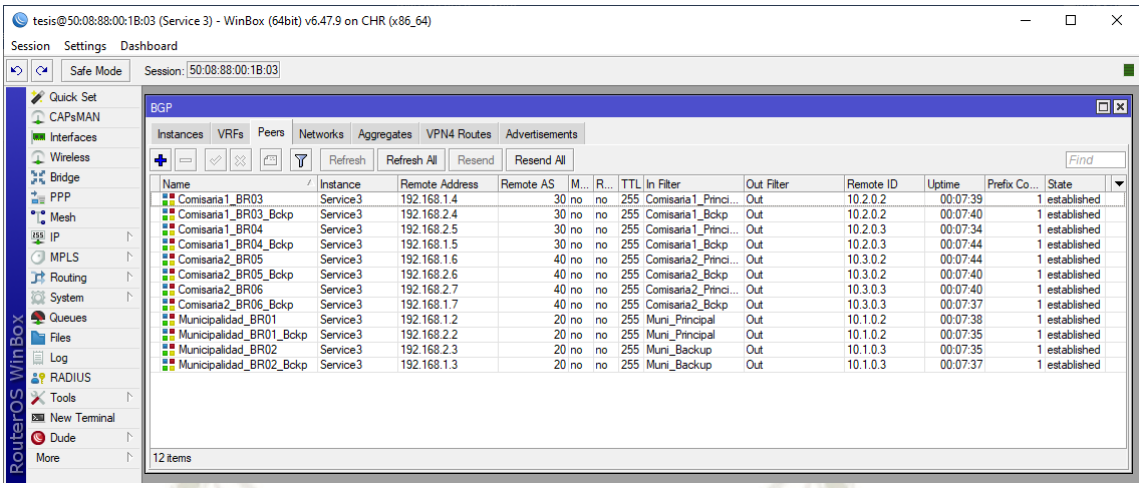


Figura 114. Interfaz WinBox con el listado de sesiones BGP activas en el router service 3. Fuente: Elaboración propia.

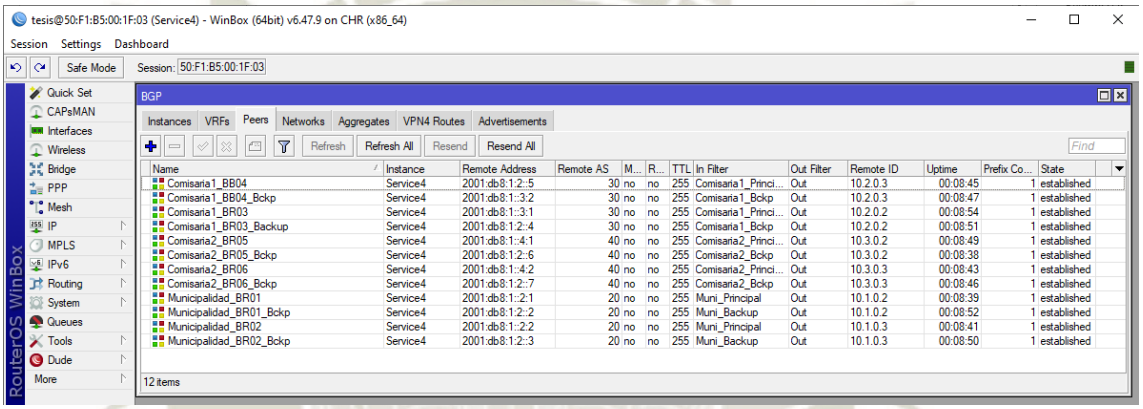


Figura 115. Interfaz WinBox con el listado de sesiones BGP activas en el router service 4. Fuente: Elaboración propia.

7.2.4 Visualización de rutas alcanzables por medio del Route Server

Las rutas de los vecinos que proporciona el route server poseen dos saltos de ASN por no ser un emparejamiento directo.

De esa forma cuando un router de borde quiere alcanzar una red vecina por medio del route server, este deberá pasar por dos ASN, el del IXP y del vecino que posee la red.

Es por esto, que esas rutas poseen dos valores en la columna “BGP AS Path” de la tabla de rutas, esto se verifica en la figura 115 mostrada a continuación.

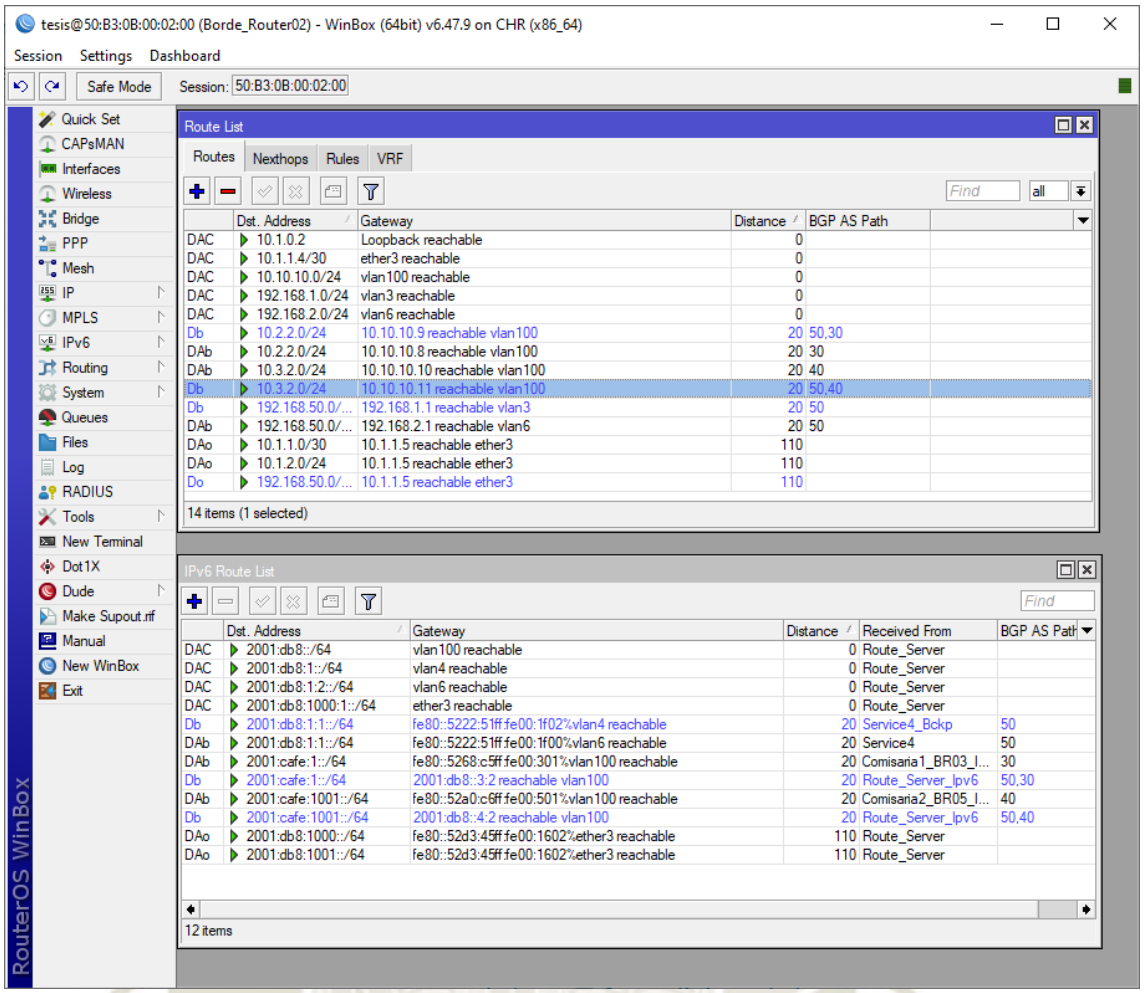


Figura 116. Interfaz WinBox de las tablas de rutas del router de borde 02, mostrando los valores de BGP AS Path para determinar que rutas provienen del route server.
Fuente: Elaboración propia.

7.2.5 Selectividad de rutas por medio de atributos BGP y filtros de enrutamiento

Para un manejo más selectivo en BGP, se utilizan tanto filtros de entrada como de salida que van a indicar parámetros que el router va ser capaz de enviar a sus vecinos.

Cada vecino debe contar con reglas específicas de entrada y salida para asegurar el diseño establecido.

Para el manejo de rutas en el protocolo BGP, deben manipularse los valores de los atributos que posee BGP. En este caso, manipulamos el valor de “Local Preference” para poder determinar la ruta secundaria. La ruta secundaria será seleccionada por el valor menor de “Local Preference” que posean los vecinos configurados en BGP, el valor por

defecto es de 100, de esta forma usando un valor de 3 definimos las rutas secundarias para los vecinos.

Estas reglas en las que se modifica el “Local-Preference” deben ingresarse en los filtros de entrada de cada vecino configurado.

Para definir las redes que serán publicadas a cada vecino, se debe agregar un filtro definiendo las redes que se deseen publicar y eliminar cualquier otra red. Este filtro deberá agregarse por cada vecino en la sección de filtros de salida.

En la figura 116 se visualiza la tabla de vecinos configurados con sus respectivos filtros de entrada y salida y los vecinos configurados para el router de borde 01.

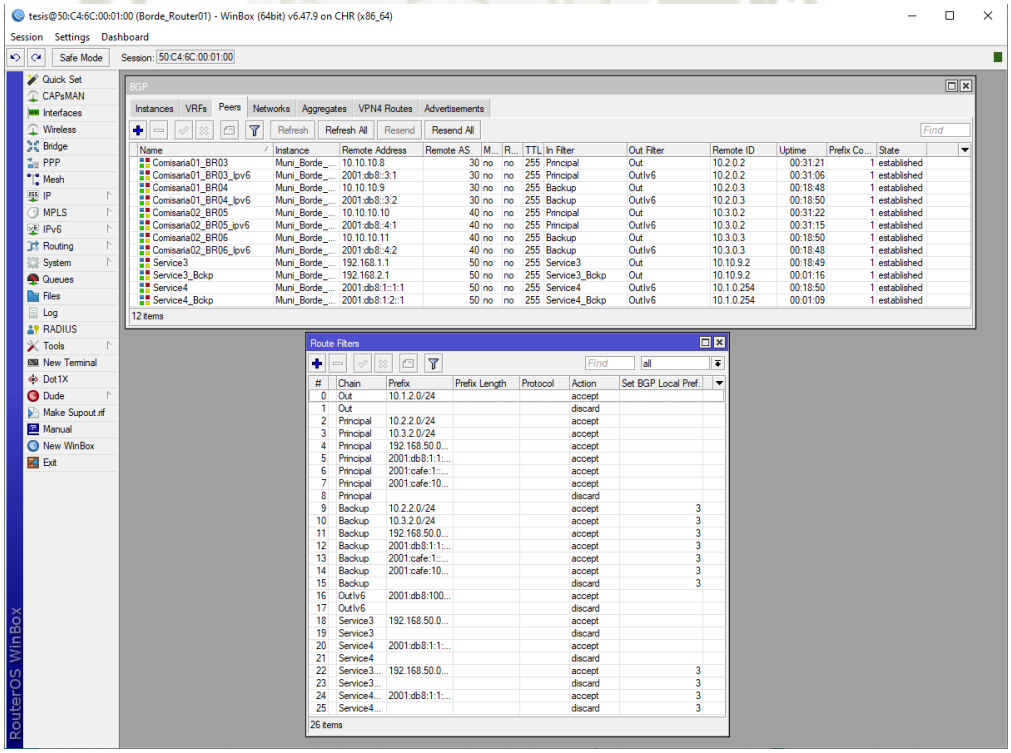


Figura 117. Interfaz WinBox del router de borde 01 con los filtros configurados para la selección de rutas, selección de redes a publicar y la adhesión de esos filtros a cada vecino. Fuente: Elaboración propia.

7.2.6 Rutas visibles por miembro

En esta sección se mostrarán las rutas alcanzables por cada miembro del punto de intercambio de tráfico.

7.2.6.1 Municipalidad

La figura 117, muestra las rutas alcanzables por el router que representa la red de la municipalidad.

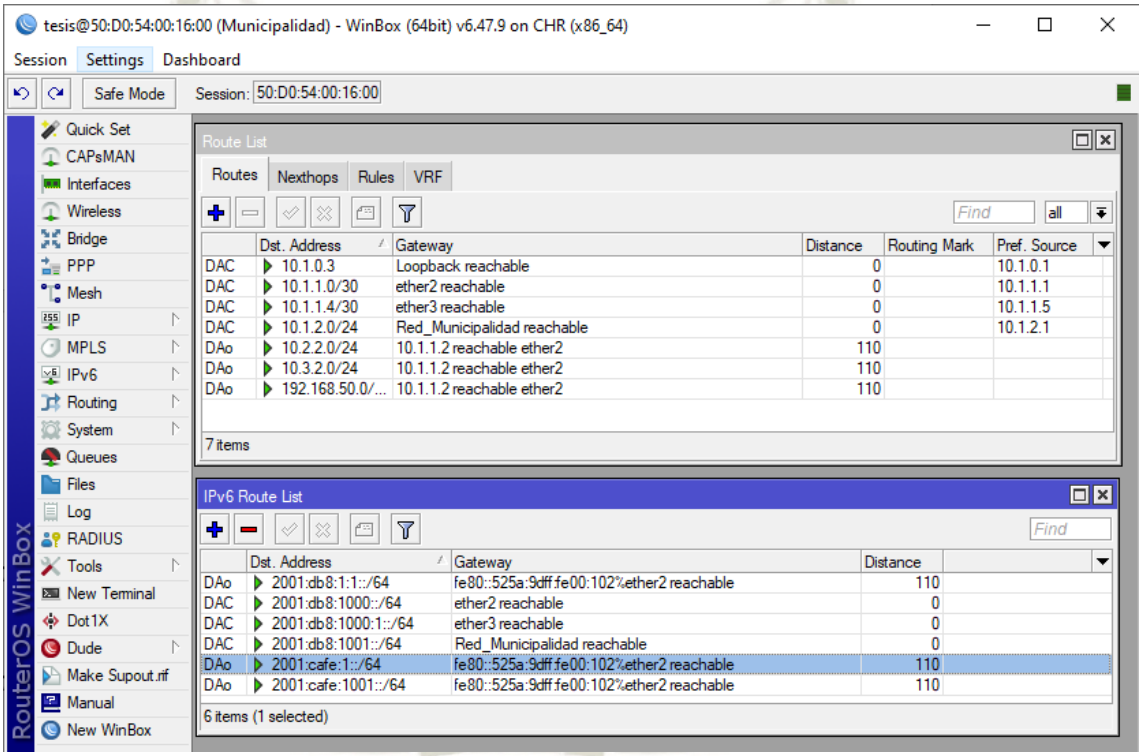


Figura 118. Interfaz WinBox lista de rutas alcanzables desde la red de la municipalidad. Fuente: Elaboración propia.

Según lo planificado, este router debe visualizar las redes tanto de IPv4 como IPv6 de la Comisaría 1 y Comisaría 2 así como la red IPv4 del router de servicio 3 y la red IPv6 del router de servicio 4.

7.2.6.2 Comisaría 1

La figura 118, muestra las redes alcanzables por el router que representa la red de la Comisaría 1.

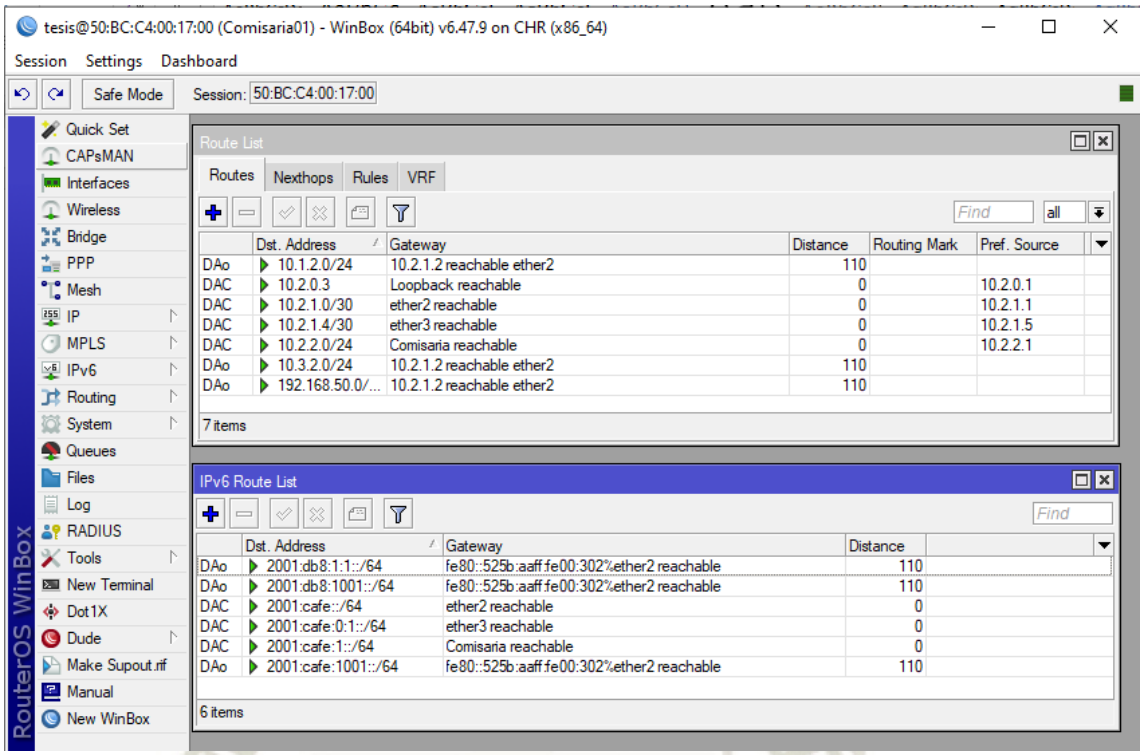


Figura 119. Interfaz WinBox lista de rutas alcanzables desde la red de la Comisaría 1.
Fuente: Elaboración propia.

Según lo planificado, este router debe visualizar las redes de todos sus vecinos, municipalidad, Comisaría 2, service 3 y service 4.

7.2.6.3 Comisaría 2

La figura 119, muestra las redes alcanzables por medio del router que representa la red de la Comisaría 2.

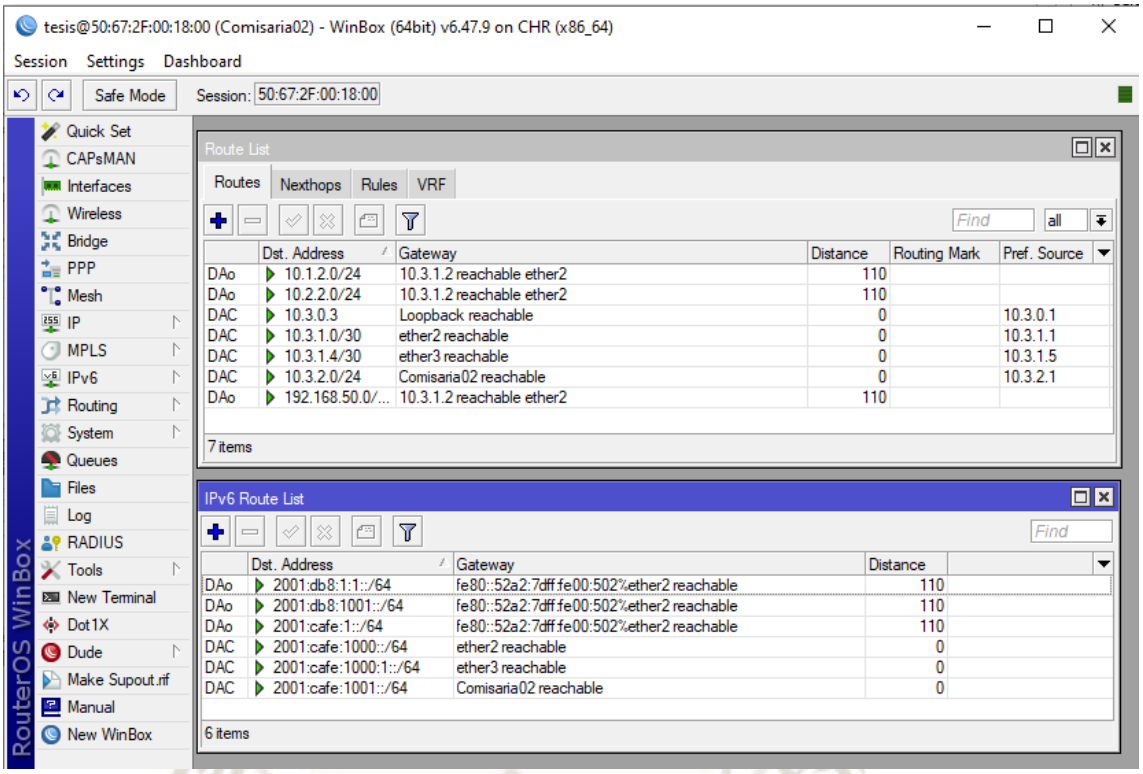


Figura 120. Interfaz WinBox lista de rutas alcanzables desde la red de la Comisaría 2. Fuente: Elaboración Propia.

Según el diseño, este route debe visualizar las redes de la municipalidad, Comisaría 1, service 3 y service 4 en la tabla de rutas.

7.2.7 Conectividad entre miembros y servicios

7.2.7.1 Municipalidad – Comisaría 1

[tesis@Municipalidad] > ping 10.2.2.1 src-address=10.1.2.1

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	10.2.2.1	56	62	5ms	
1	10.2.2.1	56	62	3ms	
2	10.2.2.1	56	62	2ms	
3	10.2.2.1	56	62	2ms	

sent=4 received=4 packet-loss=0% min-rtt=2ms avg-rtt=3ms max-rtt=5ms

[tesis@Municipalidad] > ping 2001:cafe:1::1 src-address=2001:db8:1001::1

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	2001:cafe:1::1	56	62	5ms	echo reply
1	2001:cafe:1::1	56	62	3ms	echo reply
2	2001:cafe:1::1	56	62	2ms	echo reply
3	2001:cafe:1::1	56	62	3ms	echo reply
4	2001:cafe:1::1	56	62	3ms	echo reply

sent=5 received=5 packet-loss=0% min-rtt=2ms avg-rtt=3ms max-rtt=5ms

7.2.7.2 Municipalidad – Comisaría 2

[tesis@Municipalidad] > ping 10.3.2.1 src-address=10.1.2.1

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	10.3.2.1	56	62	5ms	
1	10.3.2.1	56	62	3ms	
2	10.3.2.1	56	62	2ms	
3	10.3.2.1	56	62	2ms	

sent=4 received=4 packet-loss=0% min-rtt=2ms avg-rtt=3ms max-rtt=5ms

[tesis@Municipalidad] > ping 2001:cafe:1001::1 src-address=2001:db8:1001::1

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	2001:cafe:1001::1	56	62	5ms	echo reply

1 2001:cafe:1001::1 56 62 2ms echo reply

2 2001:cafe:1001::1 56 62 5ms echo reply

3 2001:cafe:1001::1 56 62 2ms echo reply

sent=4 received=4 packet-loss=0% min-rtt=2ms avg-rtt=3ms max-rtt=5ms

7.2.7.3 Municipalidad – Service 3

[tesis@Municipalidad] > ping 192.168.50.1 src-address=10.1.2.1

SEQ HOST SIZE TTL TIME STATUS

0 192.168.50.1 56 63 5ms

1 192.168.50.1 56 63 3ms

2 192.168.50.1 56 63 3ms

3 192.168.50.1 56 63 11ms

sent=4 received=4 packet-loss=0% min-rtt=3ms avg-rtt=5ms max-rtt=11ms

7.2.7.4 Municipalidad - Service 4

[tesis@Municipalidad] > ping 2001:db8:1:1::1 src-address=2001:db8:1001::1

SEQ HOST SIZE TTL TIME STATUS

0 2001:db8:1:1::1 56 63 9ms echo reply

1 2001:db8:1:1::1 56 63 3ms echo reply

2 2001:db8:1:1::1 56 63 4ms echo reply

3 2001:db8:1:1::1 56 63 4ms echo reply

4 2001:db8:1:1::1 56 63 4ms echo reply

sent=5 received=5 packet-loss=0% min-rtt=3ms avg-rtt=4ms max-rtt=9ms

7.2.7.5 Comisaría 1 – Comisaría 2

[tesis@Comisaría01] > ping 2001:cafe:1001::1 src-address=2001:cafe:1::1

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	2001:cafe:1001::1	56	62	3ms	echo reply
1	2001:cafe:1001::1	56	62	2ms	echo reply
2	2001:cafe:1001::1	56	62	2ms	echo reply
3	2001:cafe:1001::1	56	62	4ms	echo reply

sent=4 received=4 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=4ms

7.2.7.6 Comisaría 1 – Service 3

[tesis@Comisaría01] > ping 192.168.50.1 src-address=10.2.2.1

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	192.168.50.1	56	63	11ms	
1	192.168.50.1	56	63	6ms	
2	192.168.50.1	56	63	3ms	
3	192.168.50.1	56	63	4ms	

sent=4 received=4 packet-loss=0% min-rtt=3ms avg-rtt=6ms max-rtt=11ms

7.2.7.7 Comisaría 01 – Service 4

[tesis@Comisaría01] > ping 2001:db8:1:1::1 src-address=2001:cafe:1::1

SEQ	HOST	SIZE	TTL	TIME	STATUS

0 2001:db8:1:1::1 56 63 6ms echo reply

1 2001:db8:1:1::1 56 63 3ms echo reply

2 2001:db8:1:1::1 56 63 3ms echo reply

3 2001:db8:1:1::1 56 63 3ms echo reply

sent=4 received=4 packet-loss=0% min-rtt=3ms avg-rtt=3ms max-rtt=6ms

7.2.7.8 Comisaría 02 – Service 3

[tesis@Comisaría02] > ping 192.168.50.1 src-address=10.3.2.1

SEQ HOST SIZE TTL TIME STATUS

0 192.168.50.1 56 63 4ms

1 192.168.50.1 56 63 3ms

2 192.168.50.1 56 63 2ms

3 192.168.50.1 56 63 2ms

sent=4 received=4 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=4ms

7.2.7.9 Comisaría 02 – Service 4

[tesis@Comisaría02] > ping 2001:db8:1:1::1 src-address=2001:cafe:1001::1

SEQ HOST SIZE TTL TIME STATUS

0 2001:db8:1:1::1 56 63 6ms echo reply

1 2001:db8:1:1::1 56 63 4ms echo reply

2 2001:db8:1:1::1 56 63 10ms echo reply

3 2001:db8:1:1::1 56 63 3ms echo reply

sent=4 received=4 packet-loss=0% min-rtt=3ms avg-rtt=5ms max-rtt=10ms

7.2.8 Redundancia de la red manipulando el router de borde 01 para que este inactivo y verificar la conectividad entre municipalidad con todos los miembros, considerando parámetros de comportamiento del CHR de Mikrotik.

En las siguientes pruebas se muestra el tiempo de redundancia tanto de IPv4 como IPv6 desde la red de la municipalidad.

Para esta prueba, se considera que al apagar el router en el software no deshabilita la interfaz del router que colinda, esto por temas de la imagen CHR del Mikrotik en el emulador, por ello la redundancia del router demora el tiempo en el que el mensaje LSA indique que no hay rutas del lado de esa interfaz y recién se deshabiliten esas rutas.

7.2.8.1 Municipalidad - Comisaría 01

55 10.2.2.1 56 62 11ms

56 10.2.2.1 56 62 4ms

57 10.2.2.1 56 62 7ms

58 10.2.2.1 56 62 3ms

59 10.2.2.1 56 62 3ms

sent=60 received=25 packet-loss=58% min-rtt=2ms avg-rtt=5ms max-rtt=24ms

53 2001:cafe:1::1 56 62 5ms echo reply

54 2001:cafe:1::1 56 62 5ms echo reply

55 2001:cafe:1::1 56 62 3ms echo reply

56 2001:cafe:1::1 56 62 4ms echo reply

57 2001:cafe:1::1 56 62 5ms echo reply

58 2001:cafe:1::1 56 62 4ms echo reply

59 2001:cafe:1::1 56 62 6ms echo reply

sent=60 received=25 packet-loss=58% min-rtt=2ms avg-rtt=4ms max-rtt=8ms

7.2.8.2 Municipalidad – Comisaría 2

52 10.3.2.1 56 62 3ms

53 10.3.2.1 56 62 4ms

54 10.3.2.1 56 62 5ms

55 10.3.2.1 56 62 5ms

56 10.3.2.1 56 62 7ms

57 10.3.2.1 56 62 6ms

58 10.3.2.1 56 62 3ms

59 10.3.2.1 56 62 4ms

sent=60 received=25 packet-loss=58% min-rtt=2ms avg-rtt=3ms max-rtt=7ms

51 2001:cafe:1001::1 56 61 12ms echo reply

52 2001:cafe:1001::1 56 61 10ms echo reply

53 2001:cafe:1001::1 56 61 13ms echo reply

54 2001:cafe:1001::1 56 61 12ms echo reply

55 2001:cafe:1001::1 56 61 9ms echo reply

56 2001:cafe:1001::1 56 61 10ms echo reply

57 2001:cafe:1001::1 56 61 9ms echo reply

58 2001:cafe:1001::1 56 61 7ms echo reply

59 2001:cafe:1001::1 56 61 10ms echo reply

sent=60 received=25 packet-loss=58% min-rtt=2ms avg-rtt=7ms max-rtt=17ms

7.2.8.3 Municipalidad – Service 3

53 192.168.50.1 56 63 3ms

54 192.168.50.1 56 63 3ms

55 192.168.50.1 56 63 3ms

56 192.168.50.1 56 63 2ms

57 192.168.50.1 56 63 2ms

58 192.168.50.1 56 63 2ms

59 192.168.50.1 56 63 3ms

sent=60 received=26 packet-loss=56% min-rtt=2ms avg-rtt=3ms max-rtt=11ms

7.2.8.4 Municipalidad – Service 4

52 2001:db8:1:1::1 56 63 3ms echo reply

53 2001:db8:1:1::1 56 63 2ms echo reply

54 2001:db8:1:1::1 56 63 3ms echo reply

55 2001:db8:1:1::1 56 63 4ms echo reply

56 2001:db8:1:1::1 56 63 2ms echo reply

57 2001:db8:1:1::1 56 63 3ms echo reply

58 2001:db8:1:1::1 56 63 3ms echo reply

59 2001:db8:1:1::1 56 63 4ms echo reply

sent=60 received=25 packet-loss=58% min-rtt=2ms avg-rtt=4ms max-rtt=13ms

7.2.8.5 Tablas Resumen

En base a los resultados obtenidos en el apartado anterior se realizaron tablas resumen de los resultados obtenidos.

La tabla 35 muestra el comportamiento entre la red de la municipalidad y la red de la Comisaría 1.

Tabla 36. Comportamiento CHR Mikrotik Municipalidad - Comisaría 1

Comportamiento del CHR de Mikrotik					
Dispositivos	**IP**	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad - Comisaría 1	IP v4	60	25	35	35
	IP v6	60	25	35	35

Fuente: Elaboración propia.

La tabla 36 muestra el comportamiento entre la red de la municipalidad y la red de la Comisaría 2.

Tabla 37. Comportamiento CHR Mikrotik Municipalidad - Comisaría 2

Comportamiento del CHR de Mikrotik					
Dispositivos	**IP**	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad - Comisaría 2	IP v4	60	25	35	35
	IP v6	60	25	35	35

Fuente: Elaboración propia.

La tabla 37 muestra el comportamiento entre la red de la municipalidad, la red del service 3 y la red del service 4.

Tabla 38. Comportamiento CHR Mikrotik Municipalidad, Service 3 y Service 4

Comportamiento del CHR de Mikrotik					
Dispositivos	**Service**	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad – Service	3	60	26	34	35
	4	60	25	35	35

Fuente: Elaboración propia.

7.2.8.6 Figuras de las pruebas realizadas

7.2.8.6.1 Figura del comportamiento de la redundancia en la conectividad entre la Municipalidad y la Comisaría 1

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de desconexión es de aproximadamente 35 segundos entre el router de la municipalidad y el router de la Comisaría 1.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 120.

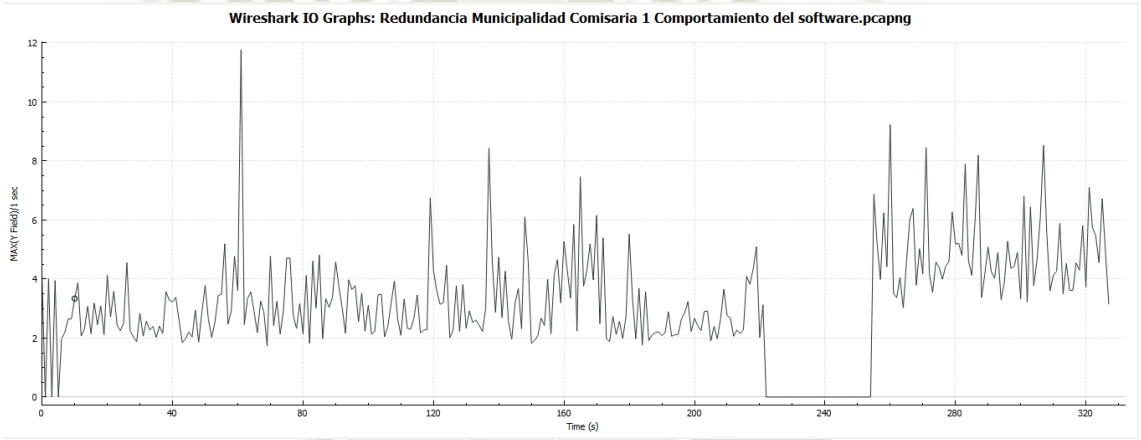


Figura 121. Tiempo de redundancia entre router de la municipalidad y el router de la Comisaría 1 con el comportamiento del CHR de Mikrotik.
Fuente: Elaboración propia.

En la figura 120 se observa que la muestra fue con más de 250 paquetes y el enlace sufre una abrupta caída cerca del paquete 220, retomando la continuidad del enlace a partir del paquete 255.

De esa forma, estableciendo un tiempo de 1 segundo. entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 35 segundos.

7.2.8.6.2 Figura del comportamiento redundante en la conectividad entre la Municipalidad y la Comisaría 2

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de desconexión es de aproximadamente 35 segundos entre el router de la municipalidad y el router de la Comisaría 2.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 121.

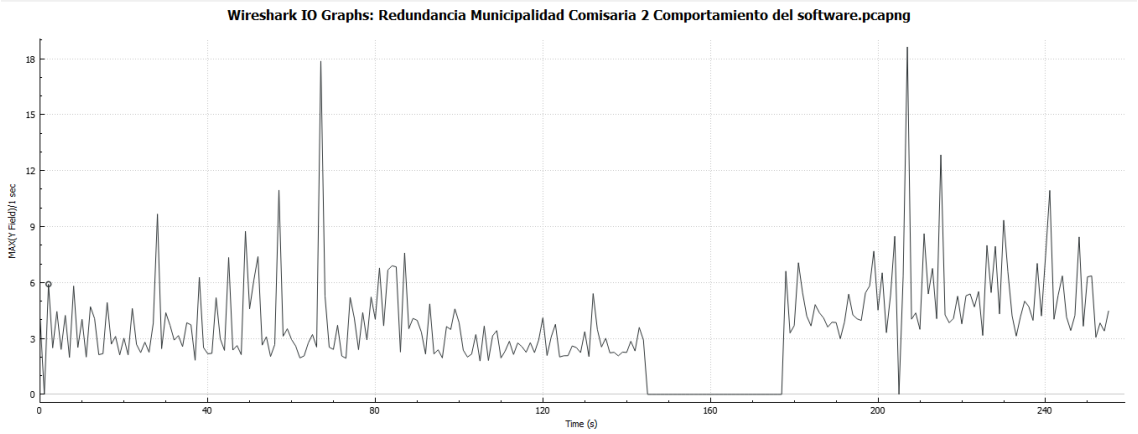


Figura 122. Tiempo de redundancia entre router de la municipalidad y el router de la Comisaría 2 con el comportamiento del software.
Fuente: Elaboración propia.

En la figura 121 se observa que la muestra fue con más de 250 paquetes y el enlace sufre una abrupta caída cerca del paquete 145, retomando la continuidad del enlace a partir del paquete 180

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 35 segundos.

7.2.8.6.3 Figura del comportamiento redundante en la conectividad entre la Municipalidad y el Service 3

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de desconexión es de aproximadamente 35 segundos entre el router de la municipalidad y el router service 3.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 122.

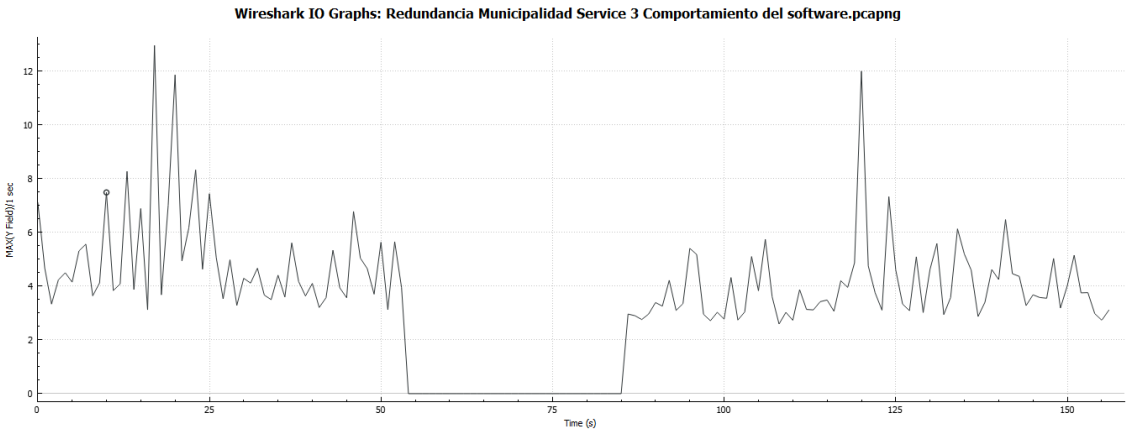


Figura 123. Tiempo de redundancia entre router de la municipalidad y el router service 3 con el comportamiento del software.
Fuente: Elaboración propia.

En la figura 122 se observa que la muestra fue con más de 160 paquetes y el enlace sufre una abrupta caída cerca del paquete 55, retomando la continuidad del enlace a partir del paquete 85.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 30 segundos.

7.2.8.6.4 Figura del comportamiento redundante en la conectividad entre la Municipalidad y el Service 4

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de desconexión es de aproximadamente 35 segundos entre el router de la municipalidad y el router service 4.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 123.

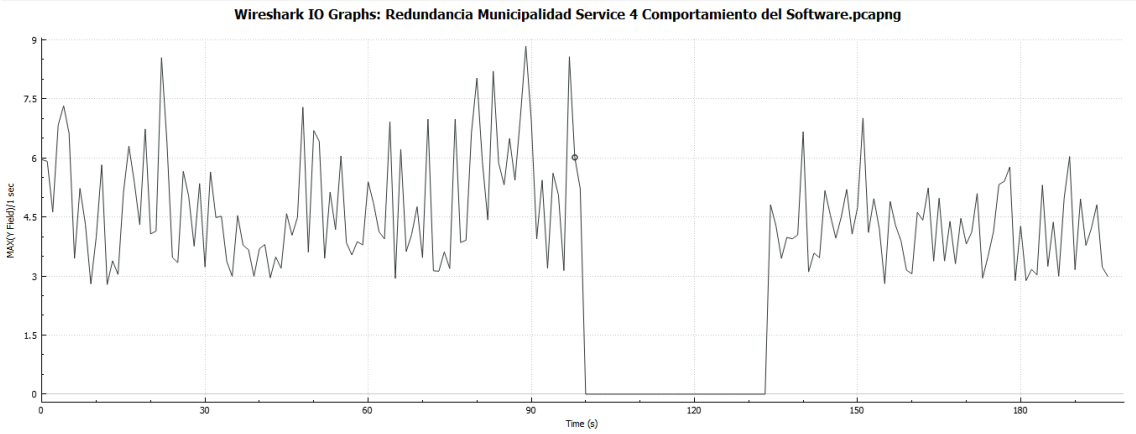


Figura 124. Tiempo de redundancia entre router de la municipalidad y el router service 4 con el comportamiento del software.
Fuente: Elaboración propia.

En la figura 123 se observa que la muestra fue con más de 180 paquetes y el enlace sufre una abrupta caída cerca del paquete 100, retomando la continuidad del enlace a partir del paquete 135

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 35 segundos.

7.2.9 Redundancia en la red manipulando el Router de Borde 01 para que este inactivo y verificar la conectividad entre Municipalidad con todos los miembros, simulando comportamiento real.

En la siguiente prueba, se deshabilitará el router de borde 01 y se deshabilitarán las interfaces de los equipos adyacentes al router de borde 01, para simular la caída física del equipo y poder determinar los tiempos de redundancia en ese caso.

Se muestran pruebas tanto de IPv4 como de IPv6.

7.2.9.1 Municipalidad - Comisaría 01

16 10.2.2.1 56 62 5ms

17 10.2.2.1 56 62 5ms

18 10.2.2.1 56 62 4ms

19 10.2.2.1 56 62 6ms

sent=20 received=17 packet-loss=15% min-rtt=2ms avg-rtt=3ms max-rtt=6ms

15 2001:cafe:1::1 56 61 10ms echo reply

16 2001:cafe:1::1 56 61 6ms echo reply

17 2001:cafe:1::1 56 61 11ms echo reply

18 2001:cafe:1::1 56 61 7ms echo reply

19 2001:cafe:1::1 56 61 13ms echo reply

sent=20 received=18 packet-loss=10% min-rtt=2ms avg-rtt=7ms max-rtt=17ms

7.2.9.2 Municipalidad – Comisaría 02

14 10.3.2.1 56 62 4ms

15 10.3.2.1 56 62 4ms

16 10.3.2.1 56 62 2ms

17 10.3.2.1 56 62 5ms

18 10.3.2.1 56 62 5ms

19 10.3.2.1 56 62 3ms

sent=20 received=17 packet-loss=15% min-rtt=2ms avg-rtt=4ms max-rtt=9ms

14 2001:cafe:1001::1 56 61 9ms echo reply

15 2001:cafe:1001::1 56 61 10ms echo reply

16 2001:cafe:1001::1 56 61 9ms echo reply

17 2001:cafe:1001::1 56 61 7ms echo reply

18 2001:cafe:1001::1 56 61 14ms echo reply

19 2001:cafe:1001::1 56 61 9ms echo reply

sent=20 received=17 packet-loss=15% min-rtt=2ms avg-rtt=6ms max-rtt=14ms

7.2.9.3 Municipalidad – Service 3

14 192.168.50.1 56 63 3ms

15 192.168.50.1 56 63 2ms

16 192.168.50.1 56 63 3ms

17 192.168.50.1 56 63 2ms

18 192.168.50.1 56 63 5ms

19 192.168.50.1 56 63 4ms

sent=20 received=17 packet-loss=15% min-rtt=2ms avg-rtt=4ms max-rtt=9ms

7.2.9.4 Municipalidad – Service 4

14 2001:db8:1:1::1 56 63 2ms echo reply

15 2001:db8:1:1::1 56 63 3ms echo reply

16 2001:db8:1:1::1 56 63 2ms echo reply

17 2001:db8:1:1::1 56 63 4ms echo reply

18 2001:db8:1:1::1 56 63 3ms echo reply

19 2001:db8:1:1::1 56 63 3ms echo reply

sent=20 received=17 packet-loss=15% min-rtt=2ms avg-rtt=3ms max-rtt=8ms

7.2.9.5 Tablas Resumen

En base a los resultados obtenidos en el apartado anterior se realizaron tablas resumen de los resultados obtenidos.

La tabla 38 muestra el comportamiento entre la red de la municipalidad y la red de la Comisaría 1.

Tabla 39. Comportamiento real Mikrotik Municipalidad - Comisaría 1

		Comportamiento Real			
Dispositivos	**IP**	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad - Comisaría 1	IP v4	20	17	3	3
	IP v6	20	18	2	2

Fuente: Elaboración propia.

La tabla 39 muestra el comportamiento entre la red de la municipalidad y la red de la Comisaría 2.

Tabla 40. Comportamiento real Mikrotik Municipalidad - Comisaría 2

		Comportamiento Real			
Dispositivos	**IP**	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad - Comisaría 2	IP v4	20	17	3	3
	IP v6	20	17	3	3

Fuente: Elaboración propia.

La tabla 40 muestra el comportamiento entre la red de la municipalidad con la red del service 3 y la red del service 4.

Tabla 41. Comportamiento real Mikrotik Municipalidad, Service 3 y Service 4

	Comportamiento Real				
Dispositivos	**Service**	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad – Service	3	20	17	3	2
	4	20	17	3	2

Fuente: Elaboración propia.

7.2.9.6 Figura de Comportamiento

7.2.9.6.1 Figura del comportamiento redundante en la conectividad entre la Municipalidad y la Comisaría 1

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de desconexión es de aproximadamente 3 segundos entre el router de la municipalidad y el router de la Comisaría 1.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 124.

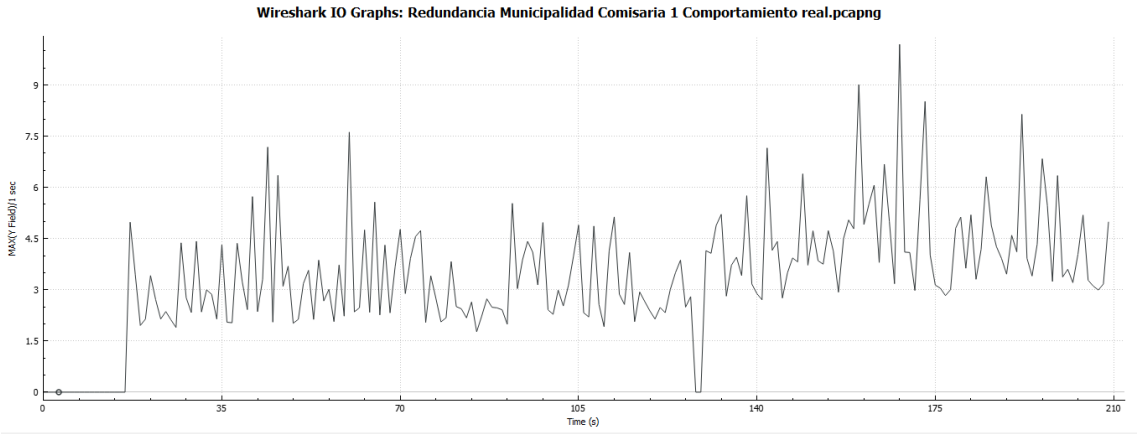


Figura 125. Tiempo de redundancia entre router de la municipalidad y el router de la Comisaría 1 con el comportamiento real.
Fuente: Elaboración propia.

En la figura 124 se observa que la muestra fue con más de 200 paquetes y sufre una caída abrupta cerca del paquete 126, retomando la continuidad del enlace a partir del paquete 128

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 2 segundos.

7.2.9.6.2 Figura del comportamiento redundante en la conectividad entre la Municipalidad y la Comisaría 2

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de desconexión es de aproximadamente 3 segundos entre el router de la municipalidad y el router de la Comisaría 2.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 125.

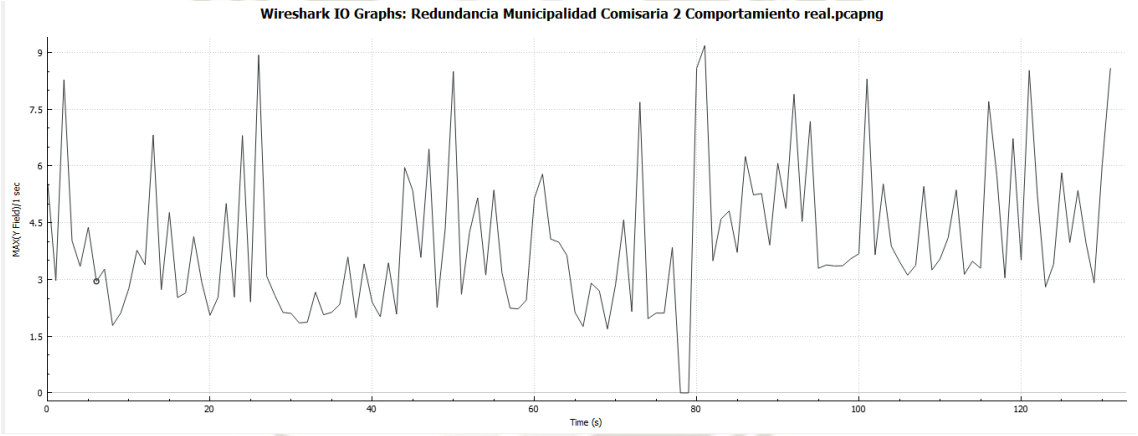


Figura 126. Tiempo de redundancia entre router de la municipalidad y el router de la Comisaría 2 con el comportamiento real.
Fuente: Elaboración propia.

En la figura 125 se observa que la muestra fue con más de 130 paquetes y sufre una abrupta caída cerca del paquete 77, retomando la continuidad del enlace a partir del paquete 79

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 2 segundos.

7.2.9.6.3 Figura del comportamiento redundante en la conectividad entre la Municipalidad y el Service 3

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de desconexión es de aproximadamente 2 segundos entre el router de la municipalidad y el router service 3.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 126.

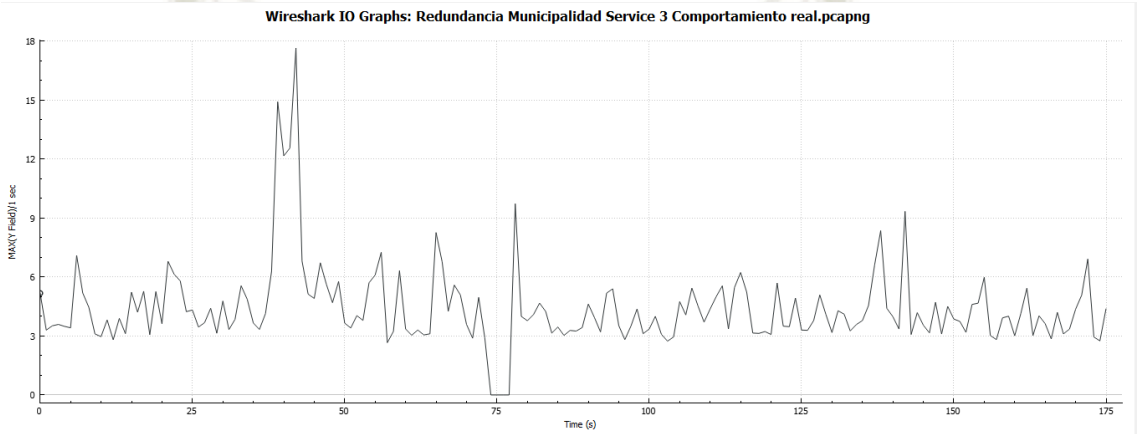


Figura 127. Tiempo de redundancia entre router de la municipalidad y el router service 3 con el comportamiento real.
Fuente: Elaboración propia.

En la figura 126 se observa que la muestra fue con más de 170 paquetes y sufre una abrupta caída cerca del paquete 75, retomando la continuidad del enlace a partir del paquete 77.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 2 segundos.

7.2.9.6.4 Figura del comportamiento redundante en la conectividad entre la Municipalidad y el Service 4

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de desconexión es de aproximadamente 2 segundos entre el router de la municipalidad y el router service 4.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 127.

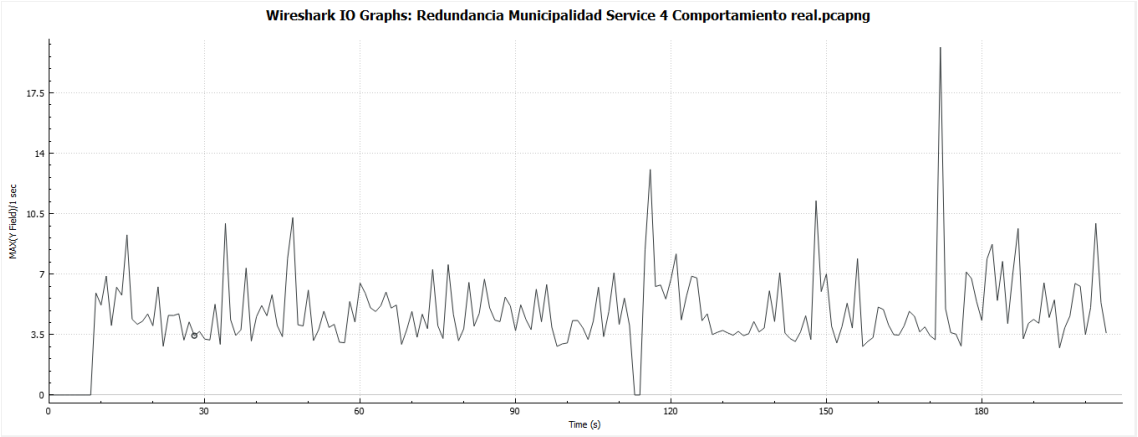


Figura 128. Tiempo de redundancia entre router de la municipalidad y el router service 4 con el comportamiento real.
Fuente: Elaboración propia.

En la figura 127 se observa que la muestra fue con más de 190 paquetes y sufre una abrupta caída cerca del paquete 115 retomando la continuidad del enlace a partir del paquete 117.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 2 segundos.

7.2.10 Funcionabilidad de RSTP

La funcionalidad de RSTP se hará mediante pruebas de conectividad desde el router de borde 01 y 02 hacia las IPs correspondientes de los router de servicio 3 y 4.

7.2.10.1 Captura del comportamiento de RSTP en Wireshark

En base al protocolo RSTP se diseñó la redundancia entre los switch que componen al punto de intercambio de tráfico.

Como ya se mencionó con anterioridad, el switch que actuara como punto principal será el switch core 01 ya que posee el menor valor hexadecimal de prioridad entre los switch que conforman la topología siendo este valor hexadecimal 1000 o decimal

4096, como segundo switch propuesto para que tome ese lugar se planteó al switch core 02 el cual posee el valor de prioridad hexadecimal 2000 o decimal 8192.

En la figura 128 y 129 se muestra el cambio de roles luego de dejar sin funcionamiento al switch core 01.

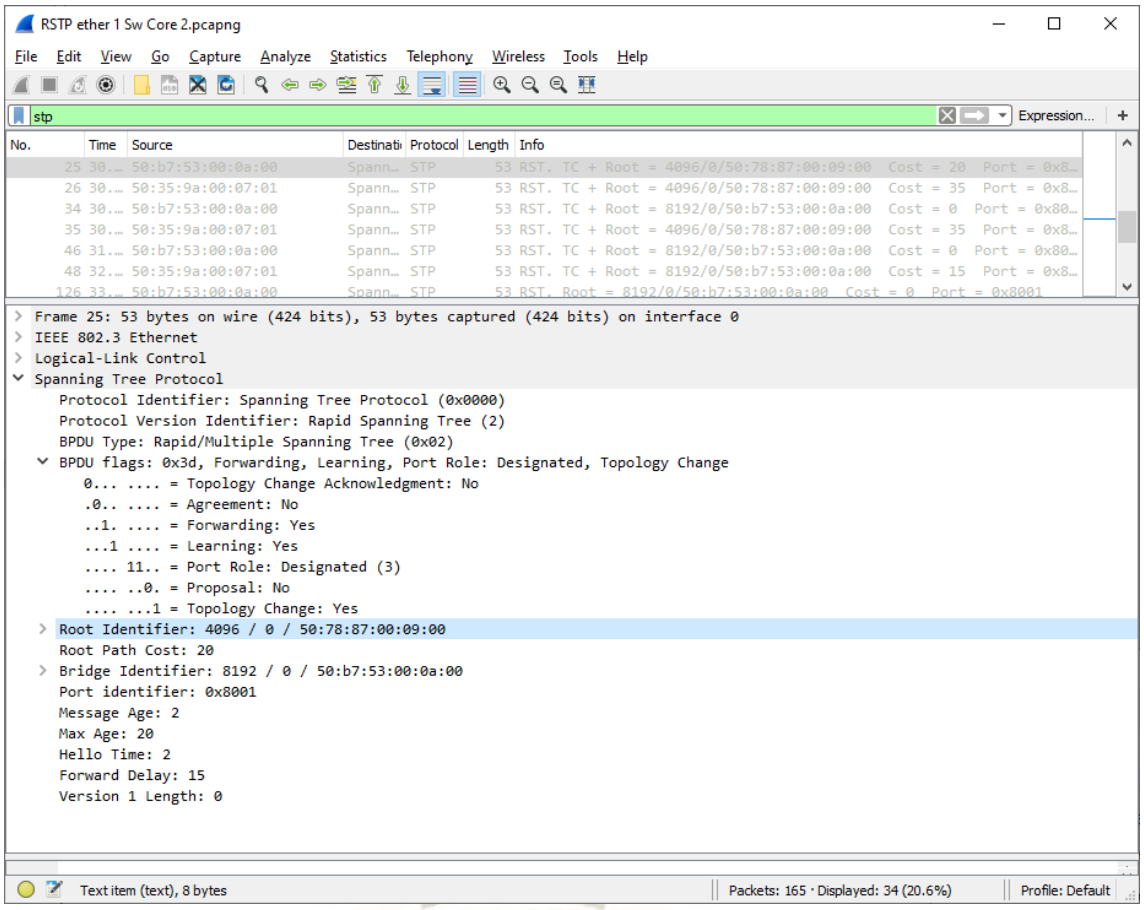


Figura 129. Interfaz Wireshark con el comportamiento RSTP del switch core 02 en la interface ether 1 previo a la designación como switch principal.
Fuente: Elaboración propia.

En la figura 128 se observa como el root bridge corresponde al switch que posee el valor de prioridad decimal 4096, el cual es el switch core 01.

La interfaz ether 1 tiene como rol ser puerto designado, de esta forma quien determina si el puerto estará activo lógicamente, es el dispositivo que se conecta a esa interfaz, en este caso sería el switch de borde 01.

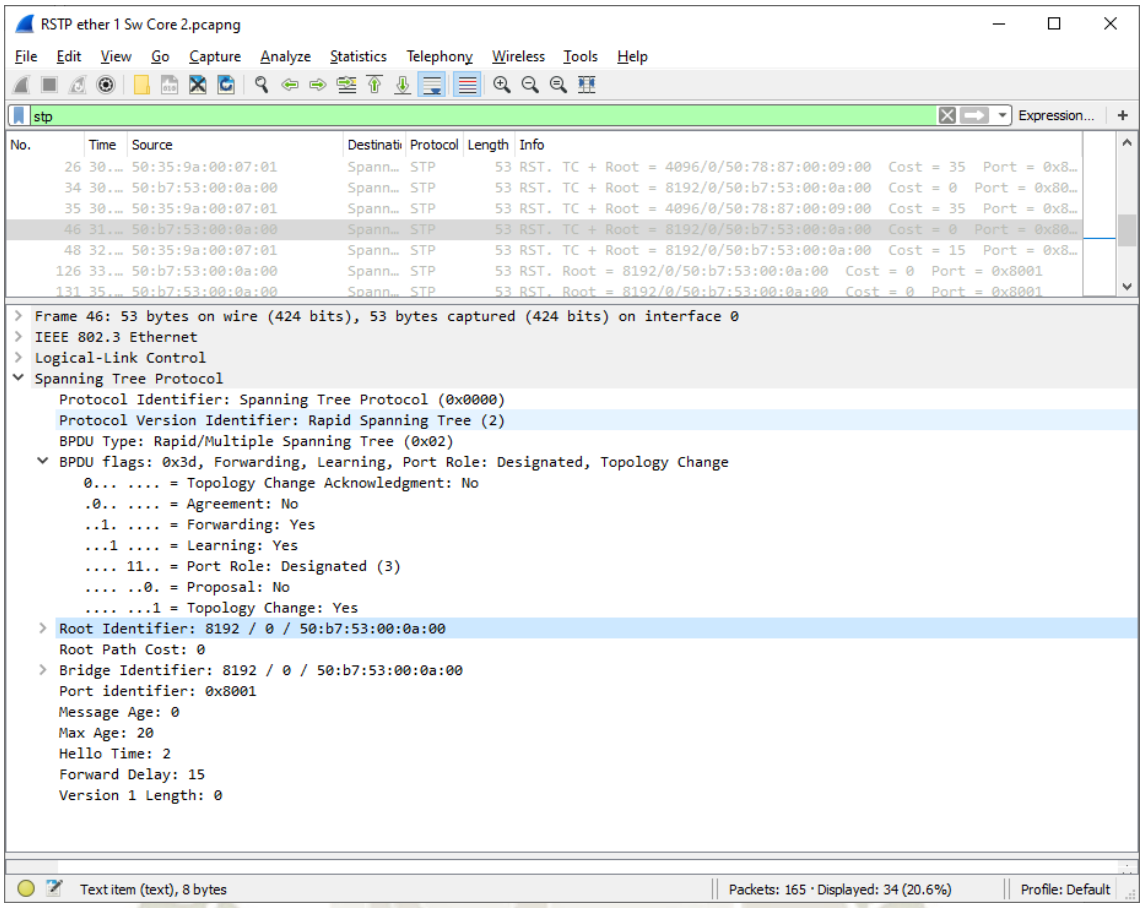


Figura 130. Interfaz Wireshark con el comportamiento RSTP del switch core 02 en la interface ether 1 luego de la designación como switch principal.
Fuente: Elaboración propia.

En la figura 129 se observa el cambio luego de la desconexión del switch core 01, dado que existe un cambio en el valor de la prioridad, se debe volver a elegir el switch principal bajo el mismo concepto, el valor de 8192 es el seleccionado como el principal correspondiente al switch core 02 por ser el menor valor de prioridad entre los otros switch.

En esta ocasión el puerto ether 1 es el puerto principal y señala como un puerto activo, de esta forma su vecino, el switch de borde 01 tendrá como rol ser el puerto designado.

7.2.10.2 Switch Borde 01 desconectado

Como parte de las pruebas de redundancia se procedió a apagar el switch borde 01.

De esta forma, la conexión del router de borde 01, router de borde 03 y router de borde 05 se verán afectadas.

En la figura 130 se muestra lo sucedido en el router de borde 01.

Mientras que el router de borde 02, router de borde 04 y router de borde 06 no tendrá efecto la desconexión de ese switch.

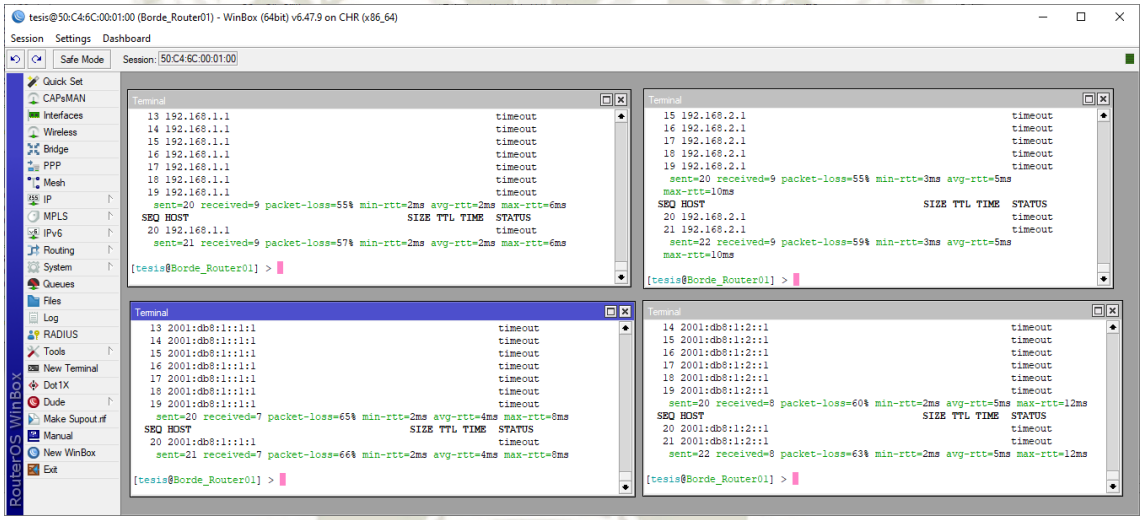


Figura 131. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 01 con el switch de borde 01 desconectado.
Fuente: Elaboración propia.

El efecto de la desconexión del switch borde 01 en el router de borde 02 se ilustra en la figura 131.

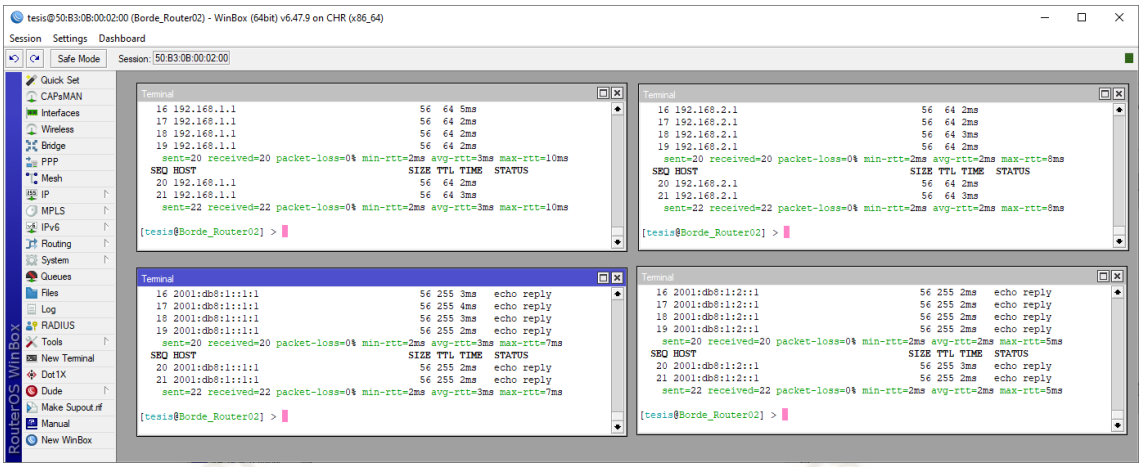


Figura 132. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 02 con el switch de borde 01 desconectado.
Fuente: Elaboración propia.

7.2.10.3 Switch Core 01 desconectado

Se procedió a apagar el switch core 01, como parte de las pruebas de redundancia.

Al ser este el switch principal, cualquier conexión de los router de borde se verán afectadas.

Las figuras 132 y 133 muestran la cantidad de paquetes perdidos que provoco esta caída en el router de borde 01 y router de borde 02 respectivamente.

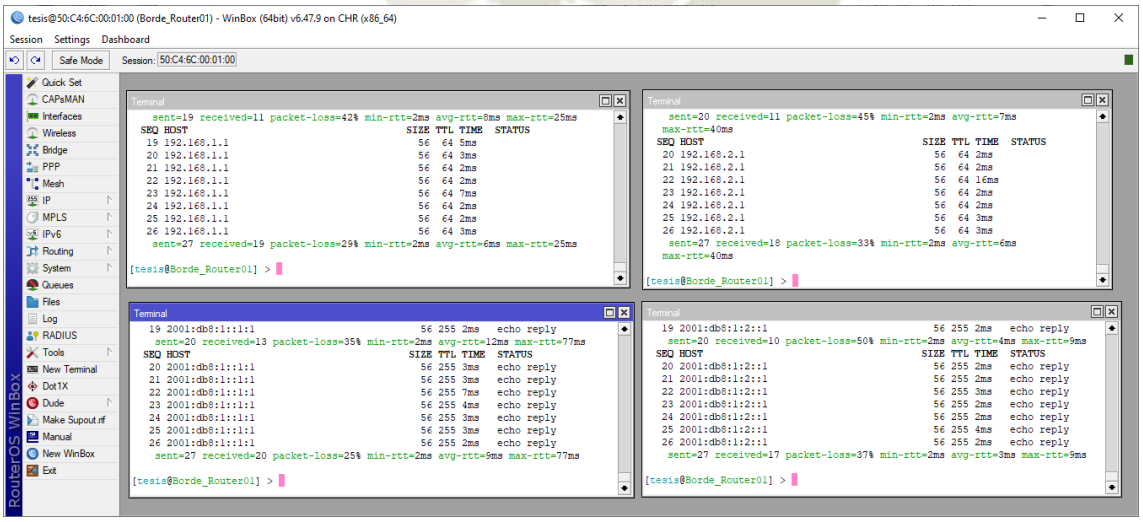


Figura 133. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 01 con el switch core 01 desconectado.
Fuente: Elaboración propia.

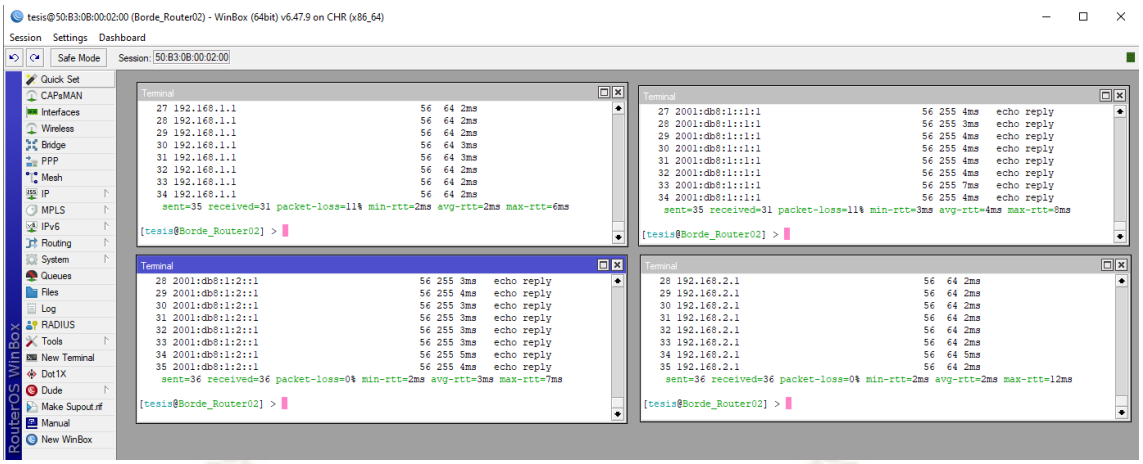


Figura 134. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 02 con el switch core 01 desconectado
Fuente: Elaboración propia.

7.2.10.4 Switch Core 02 desconectado

Como parte de las pruebas de redundancia se procedió a apagar el switch core 02.

El resultado de este suceso se muestra en las figuras 134 y 135 para el router de borde 01

y router de borde 02, respectivamente.

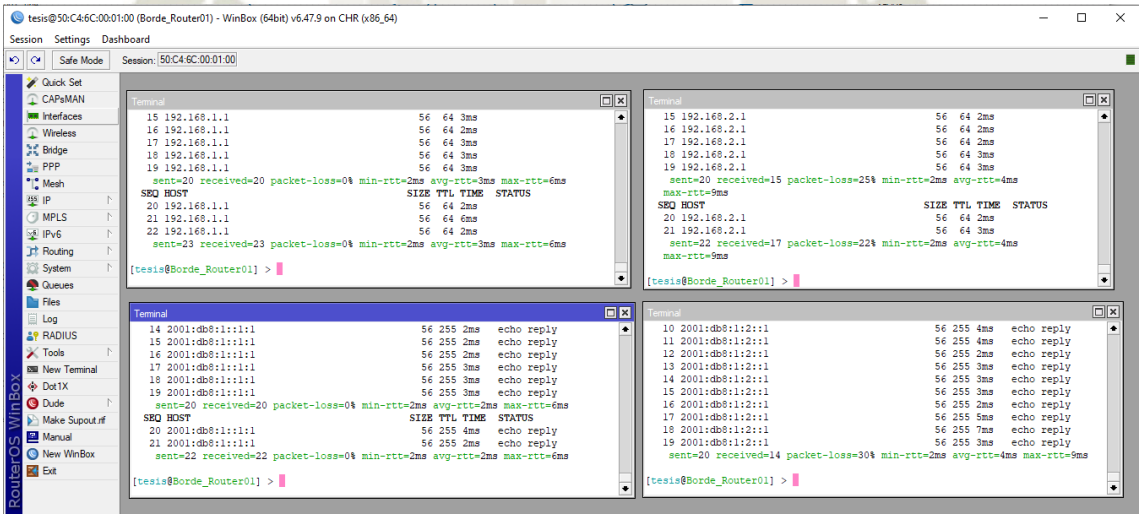


Figura 135. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 01 con el switch core 02 desconectado.
Fuente: Elaboración propia.

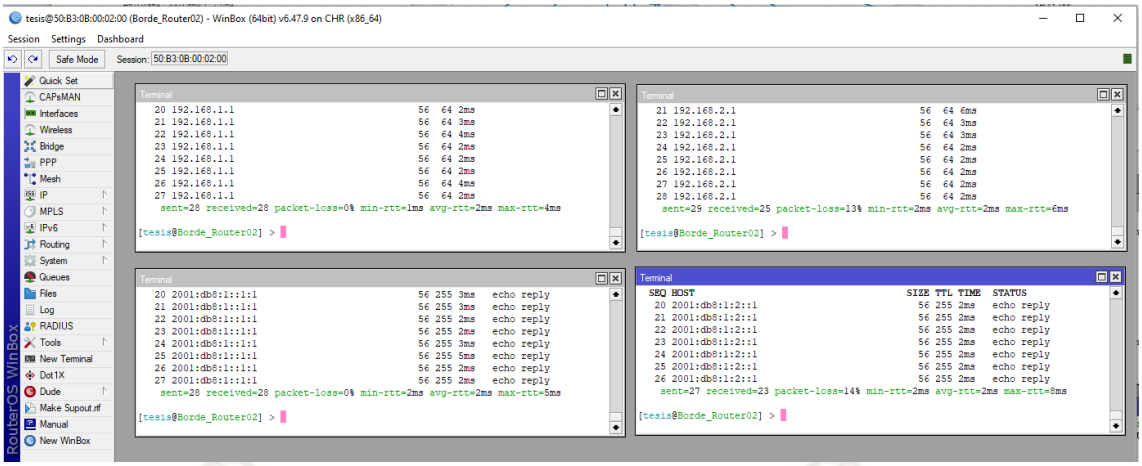


Figura 136. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 02 con el switch core 02 desconectado.
Fuente: Elaboración propia.

7.2.10.5 Switch Service 01 desconectado

Como parte de las pruebas de redundancia se procedió a apagar el switch service 01.

Por ello las vlan que pasaban por ese switch se vieron afectadas y como resultado no se tuvo conexión a la red 192.168.1.0/24 ni a la red 2001:db8:1::/64 pero no se perdió conexión hacia las redes 192.168.2.0/24 y a la 2001:db8:1:2::1/64 que pasan por el switch service 02.

El resultado de esto se muestra en las figuras 136 y 137 para los router de borde 01 y router de borde 02 respectivamente.

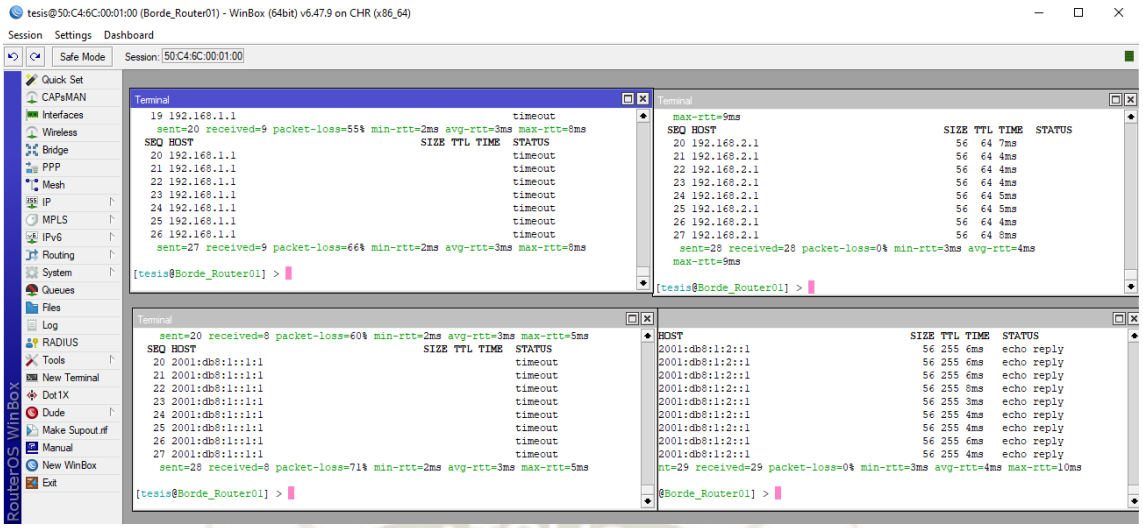


Figura 137. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 01 con el switch service 01 desconectado.
Fuente: Elaboración propia.

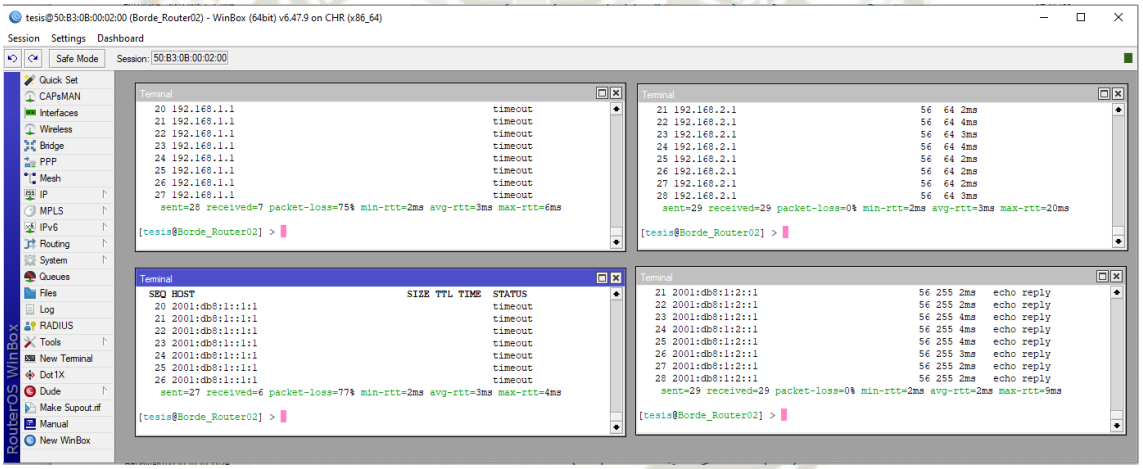


Figura 138. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 02 con el switch service 01 desconectado.
Fuente: Elaboración propia.

7.2.10.6 Switch Borde 01, Switch Core 02 y Switch Service 01 desconectado

Como parte de las pruebas de redundancia se procedió a apagar los switch borde 01, switch core 02 y switch service 01.

Como resultado de esto, los router de borde 01, router de borde 03 y router de borde 05 tendrán una desconexión total con la topología.

Mientras que el router de borde 02, router de borde 04 y router de borde 06 solo verán afectadas las redes que pasan por el switch service 01, explicadas anteriormente.

El resultado de esto se puede apreciar en la figura 138 para el router de borde 01 y la figura 139 para el router de borde 02.

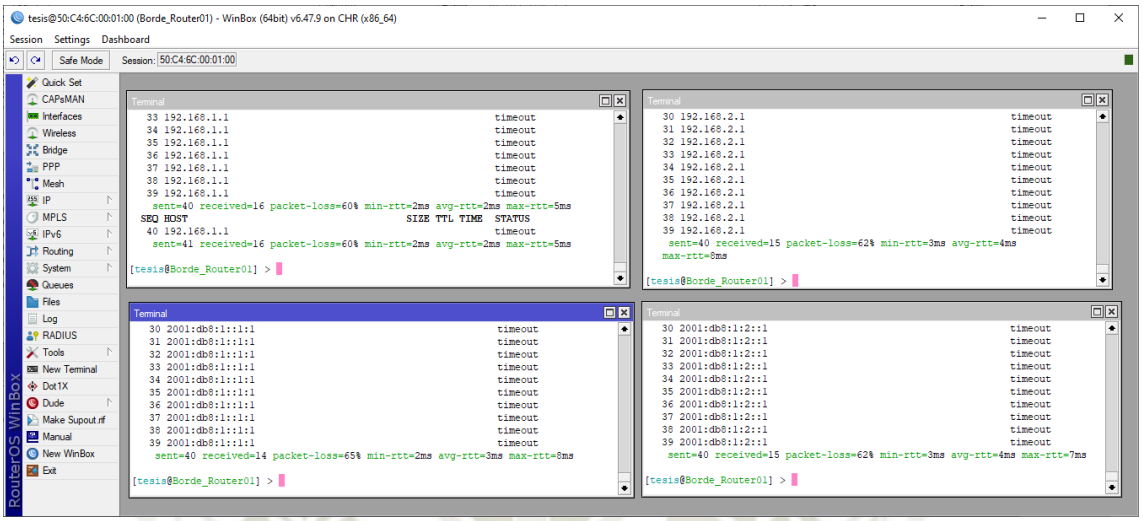


Figura 139. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 01 con el switch borde 01, switch core 02 y service 01 desconectado.
Fuente: Elaboración propia.

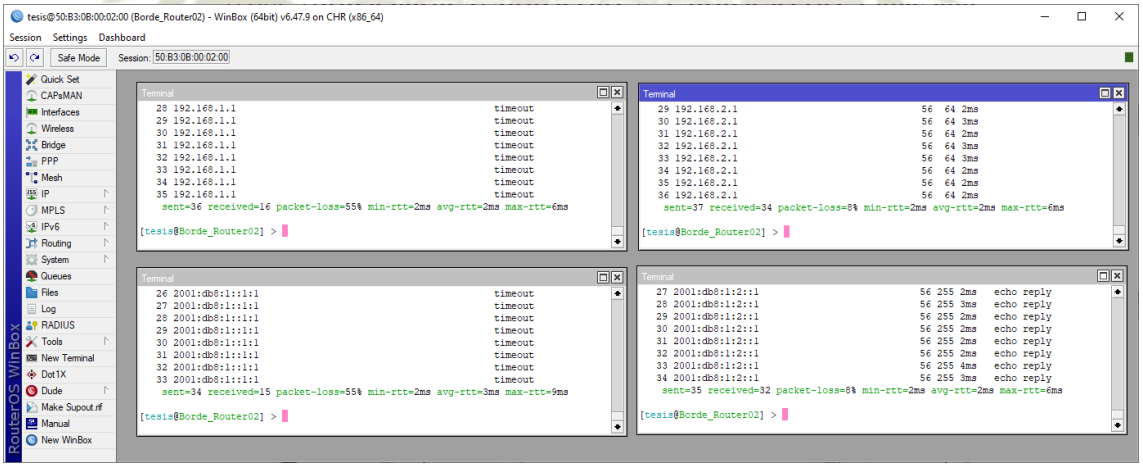


Figura 140. Interfaz WinBox pruebas de conectividad hacia las IPs del router service 3 y 4 desde el router de borde 02 con el switch borde 01, switch core 02 y service 1 desconectado.
Fuente: Elaboración propia.

7.2.10.7 Tablas resumen

En base a los resultados obtenidos en el apartado anterior se realizan tablas resumen de los resultados obtenidos.

La tabla 41 muestra el comportamiento entre el router de borde 01 y los router service 3 y router service 4 con la desconexión del switch borde 01.

Tabla 42. Desconexión Switch Borde 01, conectividad entre Router de Borde 01, Service 3 y Service 4

Switch borde 01 desconectado						
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**	**Estado**
Borde Router 01	3	192.168.1.1	20	9	11	Desconexión
		192.168.2.1	20	9	11	Desconexión
	4	2001:db8:1::1::1	20	7	13	Desconexión
		2001:db8:1:2::1:1	20	8	12	Desconexión

Fuente: Elaboración propia.

La tabla 42 muestra el comportamiento entre el router de borde 02 y los router service 3 y router service 4 con la desconexión del switch borde 01.

Tabla 43. Desconexión Switch Borde 01, conectividad entre Router de Borde 02, Service 3 y Service 4

Switch borde 01 desconectado					
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**
Borde Router 02	3	192.168.1.1	20	20	0
		192.168.2.1	20	20	0
	4	2001:db8:1::1:1	20	20	0
		2001:db8:1:2::1:1	20	20	0

Fuente: Elaboración propia.

La tabla 43 muestra el comportamiento entre el router de borde 01, el router service 3 y router service 4 con la desconexión del switch core 01.

Tabla 44. Desconexión Switch Core 01, conectividad entre Borde Router 01, Service 3 y Service 4

Switch Core 01 desconectado					
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**
Borde Router 01	3	192.168.1.1	27	19	8
		192.168.2.1	27	18	9
	4	2001:db8:1::1:1	27	20	7
		2001:db8:1:2::1:1	27	17	10

Fuente: Elaboración propia.

La tabla 44 muestra el comportamiento entre el router de borde 02, el router service 3 y router service 4 con la desconexión del switch core 01.

Tabla 45. Desconexión Switch Core 01, conectividad entre Router de Borde 02, Service 3 y Service 4

Switch Core 01 desconectado					
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**
Borde Router 02	3	192.168.1.1	35	31	4
		192.168.2.1	35	31	4
	4	2001:db8:1::1:1	36	36	0
		2001:db8:1:2::1:1	36	36	0

Fuente: Elaboración propia.

La tabla 45 muestra el comportamiento entre router de borde 01, el router service 3 y router service 4 con la desconexión del switch core 02.

Tabla 46. Desconexión Switch Core 02, conectividad entre Router de Borde 01, Service 3 y Service 4

Switch Core 02 desconectado					
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**
Borde Router 01	3	192.168.1.1	20	20	0
		192.168.2.1	20	15	5
	4	2001:db8:1::1:1	20	20	0
		2001:db8:1:2::1:1	20	14	6

Fuente: Elaboración propia.

La tabla 46 muestra el comportamiento entre el router de borde 02, el router service 3 y router service 4 con la desconexión del switch core 02.

Tabla 47. Desconexión Switch Core 02, conectividad entre Router de Borde 02, Service 3 y Service 4

Switch Core 02 desconectado					
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**
Borde Router 02	3	192.168.1.1	28	28	0
		192.168.2.1	29	25	4
	4	2001:db8:1::1:1	28	28	0
		2001:db8:1:2::1:1	27	23	4

Fuente: Elaboración propia.

La tabla 47 muestra el comportamiento entre router de borde 01, el router service 3 y router service 4 con la desconexión del switch service 01.

Tabla 48. Desconexión Switch Service 01, conectividad entre Router de Borde 01, Service 3 y Service 4

Switch Service 01 desconectado					
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**
Borde Router 01	3	192.168.1.1	27	9	18
		192.168.2.1	28	28	0
	4	2001:db8:1::1:1	28	8	20
		2001:db8:1::2::1:1	29	29	0

Fuente: Elaboración propia.

La tabla 48 muestra el comportamiento entre el router de borde 02, el router service 3 y el router 4 con la desconexión del switch service 01.

Tabla 49. Desconexión Switch Service 01, conectividad entre Router de Borde 02, Service 3 y Service 4

Switch Service 01 desconectado					
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**
Borde Router 02	3	192.168.1.1	27	8	19
		192.168.2.1	29	29	0
	4	2001:db8:1::1:1	27	6	21
		2001:db8:1::2::1:1	29	29	0

Fuente: Elaboración propia.

La tabla 49 muestra el comportamiento entre el router de borde 01, el router service 3 y router service 4 con la desconexión del switch borde 01, switch core 02 y switch service 01.

Tabla 50. Desconexión Switch Borde 01, Switch Core 02 y Switch Service 01, conectividad entre Borde Router 01 - Service 3 y Service 4

Switch Borde0 1, Core 02 y Service 01 desconectado						
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**	**Estado**
Borde Router 01	3	192.168.1.1	40	16	24	Desconexión
		192.168.2.1	40	15	25	Desconexión
	4	2001:db8:1::1:1	40	14	26	Desconexión
		2001:db8:1:2::1:1	40	15	25	Desconexión

Fuente: Elaboración propia.

La tabla 50 muestra el comportamiento entre el router de borde 02, el router service 3 y router service 4 con la desconexión del switch borde 01, switch core 02 y switch service 01.

Tabla 51. Desconexión Switch Borde 01, Switch Core 02 y Switch Service 01, conectividad entre Borde Router 02 - Service 3 y Service 4

Switch Borde 01, Core 02 y Service 01 desconectado						
Dispositivo	**Service**	**IP**	**Paquetes Enviados**	**Paquetes Recibidos**	**Paquetes Perdidos**	**Estado**
Borde Router 02	3	192.168.1.1	36	16	20	Desconexión
		192.168.2.1	37	34	3	Habilitado
	4	2001:db8:1::1:1	34	15	19	Desconexión
		2001:db8:1:2::1:1	35	32	3	Habilitado

Fuente: Elaboración propia.

7.2.11 Tiempos de redundancia

7.2.11.1 Desconexión Switch Core 01

7.2.11.1.1 Municipalidad – Service Vlan 03

73 192.168.50.1 56 63 4ms

74 192.168.50.1 56 63 2ms

75 192.168.50.1 56 63 3ms

76 192.168.50.1 56 63 6ms

77 192.168.50.1 56 63 6ms

78 192.168.50.1 56 63 6ms

79 192.168.50.1 56 63 9ms

sent=80 received=29 packet-loss=63% min-rtt=2ms avg-rtt=3ms max-rtt=9ms

7.2.11.1.2 Municipalidad – Service Vlan 04

154 no route to host

155 no route to host

156 2001:db8:1:1::1 56 63 8ms echo reply

157 2001:db8:1:1::1 56 63 15ms echo reply

158 2001:db8:1:1::1 56 63 4ms echo reply

159 2001:db8:1:1::1 56 63 5ms echo reply

sent=160 received=105 packet-loss=34% min-rtt=2ms avg-rtt=4ms max-rtt=16ms

7.2.11.2 Desconexión Switch Borde 01

7.2.11.2.1 Municipalidad – Service Vlan 3

20 192.168.50.1 56 63 3ms

21 192.168.50.1 56 63 3ms

22 192.168.50.1 56 63 2ms

23 192.168.50.1 56 63 3ms

24 192.168.50.1 56 63 3ms

sent=25 received=22 packet-loss=12% min-rtt=2ms avg-rtt=4ms max-rtt=13ms

7.2.11.2.2 Municipalidad – Service Vlan 4

SEQ HOST SIZE TTL TIME STATUS

20 2001:db8:1:1::1 56 63 3ms echo reply

21 2001:db8:1:1::1 56 63 4ms echo reply

22 2001:db8:1:1::1 56 63 4ms echo reply

23 2001:db8:1:1::1 56 63 3ms echo reply

24 2001:db8:1:1::1 56 63 4ms echo reply

sent=25 received=21 packet-loss=16% min-rtt=2ms avg-rtt=3ms max-rtt=6ms

7.2.11.3 Desconexión Switch Service 01

7.2.11.3.1 Municipalidad – Service Vlan 3

22 192.168.50.1 56 63 4ms

23 192.168.50.1 56 63 5ms

24 192.168.50.1 56 63 6ms

25 192.168.50.1 56 63 5ms

26 192.168.50.1 56 63 6ms

27 192.168.50.1 56 63 5ms

28 192.168.50.1 56 63 4ms

sent=29 received=28 packet-loss=3% min-rtt=3ms avg-rtt=5ms max-rtt=12ms

7.2.11.3.2 Municipalidad – Service Vlan 4

23 2001:db8:1:1::1 56 63 5ms echo reply

24 2001:db8:1:1::1 56 63 4ms echo reply

25 2001:db8:1:1::1 56 63 4ms echo reply

26 2001:db8:1:1::1 56 63 4ms echo reply

27 2001:db8:1:1::1 56 63 4ms echo reply

28 2001:db8:1:1::1 56 63 5ms echo reply

29 2001:db8:1:1::1 56 63 5ms echo reply

sent=30 received=29 packet-loss=3% min-rtt=2ms avg-rtt=4ms max-rtt=11ms

7.2.11.4 Desconexión Switch Core 02

7.2.11.4.1 Comisaría 1 – Service Vlan 3

14 192.168.50.1 56 63 3ms

15 192.168.50.1 56 63 3ms

16 192.168.50.1 56 63 3ms

17 192.168.50.1 56 63 2ms

18 192.168.50.1 56 63 3ms

19 192.168.50.1 56 63 4ms

sent=20 received=20 packet-loss=0% min-rtt=2ms avg-rtt=4ms max-rtt=9ms

7.2.11.4.2 Comisaría 1 – Service Vlan 4

13 2001:db8:1:1::1 56 63 4ms echo reply

14 2001:db8:1:1::1 56 63 4ms echo reply

15 2001:db8:1:1::1 56 63 2ms echo reply

16 2001:db8:1:1::1 56 63 3ms echo reply

17 2001:db8:1:1::1 56 63 3ms echo reply

18 2001:db8:1:1::1 56 63 3ms echo reply

19 2001:db8:1:1::1 56 63 4ms echo reply

sent=20 received=20 packet-loss=0% min-rtt=2ms avg-rtt=3ms max-rtt=7ms

7.2.11.5 Desconexión Switch Core 01, Switch Service 02

7.2.11.5.1 Comisaría 2 – Service Vlan 3

72 2001:db8:1:1::1 56 63 2ms echo reply

73 2001:db8:1:1::1 56 63 3ms echo reply

74 2001:db8:1:1::1 56 63 2ms echo reply

75 2001:db8:1:1::1 56 63 5ms echo reply

76 2001:db8:1:1::1 56 63 8ms echo reply

77 2001:db8:1:1::1 56 63 5ms echo reply

sent=78 received=24 packet-loss=69% min-rtt=2ms avg-rtt=3ms max-rtt=8ms

7.2.11.5.2 Comisaría 2 – Service Vlan 4

70 192.168.50.1 56 63 10ms

71 192.168.50.1 56 63 2ms

72 192.168.50.1 56 63 3ms

73 192.168.50.1 56 63 3ms

74 192.168.50.1 56 63 2ms

75 192.168.50.1 56 63 2ms

sent=76 received=23 packet-loss=69% min-rtt=2ms avg-rtt=3ms max-rtt=10ms

7.2.11.6 Tablas resumen

En base a los resultados obtenidos en el apartado anterior se realizan tablas resumen de los resultados obtenidos.

La tabla 51 muestra el comportamiento entre la red de la municipalidad, las redes del router service 3 y router service 4 con la desconexión del switch core 01.

Tabla 52. Desconexión Switch Core 01, conectividad entre Municipalidad, Service 3 y service 4

Desconexión Switch Core 01				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad - Service 3	80	29	51	54
Municipalidad - Service 4	160	105	55	55

Fuente: Elaboración propia.

La tabla 52 muestra el comportamiento entre la red de la municipalidad, las redes del router service 3 y router service 4 con la desconexión del switch borde 01.

Tabla 53. Desconexión Switch Borde 01, conectividad entre Municipalidad, Service 3 y Service 4

Desconexión Switch Borde 01				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad - Service 3	25	22	3	5
Municipalidad - Service 4	25	21	4	6

Fuente: Elaboración propia.

La tabla 53 muestra el comportamiento entre la red de la municipalidad, las redes del router service 3 y router service 4 con la desconexión del switch service 01.

Tabla 54. Desconexión Switch Service 01, conectividad entre Municipalidad, Service 3 y service 4

Desconexión Switch Service 01				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Municipalidad - Service 3	29	28	1	2
Municipalidad - Service 4	30	29	1	2

Fuente: Elaboración propia.

La tabla 54 muestra el comportamiento entre la red de la Comisaría 1, las redes del router service 3 y router service 4 con la desconexión del switch core 02.

Tabla 55. Desconexión Switch Core 02, conectividad entre Comisaría 1, Service 3 y Service 4

Desconexión Switch Core 02				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Comisaría 1 - Service 3	20	20	0	0
Comisaría 1 - Service 4	20	20	0	0

Fuente: Elaboración propia.

La tabla 55 muestra el comportamiento entre la red de la Comisaría 2, las redes del router service 3 y router service 4 con la desconexión del switch core 01 y switch service 02.

Tabla 56. Desconexión switch core 01 y switch service 02, conectividad entre Comisaría 2, Service 3 y Service 4

Desconexión Switch Core 01, Switch Service 02				
Dispositivos	**Paquetes enviados**	**Paquetes recibidos**	**Paquetes Perdidos**	**Tiempo de redundancia (seg)**
Comisaría 2 - Service 3	78	24	54	56
Comisaría 2 - Service 4	76	23	53	55

Fuente: Elaboración propia.

7.2.11.7 Figuras Obtenidas

7.2.11.7.1 Desconexión Switch Core 01

7.2.11.7.1.1 Figuras del comportamiento redundante en la conectividad entre la Municipalidad y el Service 3

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de redundancia es de aproximadamente 54 segundos entre el router de la municipalidad y el router service 3.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 140.

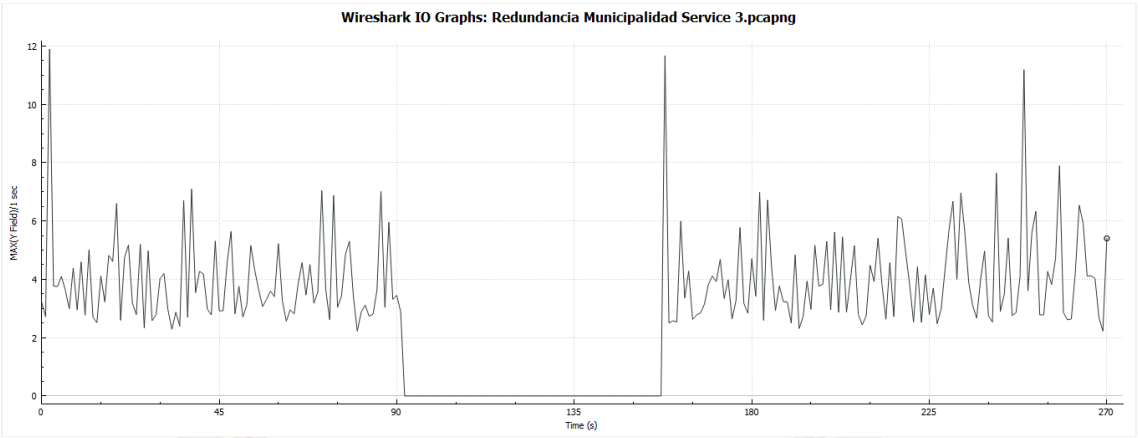


Figura 141. Tiempo de redundancia entre router de la municipalidad y el router service 3 con el switch core 01 sin funcionamiento.
Fuente: Elaboración propia.

En la figura 140 se observa que la muestra fue con más de 260 paquetes y que sufre una abrupta caída cerca del paquete 90, retomando la continuidad a partir del paquete 144.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 54 segundos.

7.2.11.7.1.2 Figuras del comportamiento redundante en la conectividad entre la Municipalidad y el Service 4

Según los datos obtenidos en las pruebas previas, se obtuvo que el tiempo de redundancia es de aproximadamente 54 segundos entre el router de la municipalidad y el router service 4.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 141.

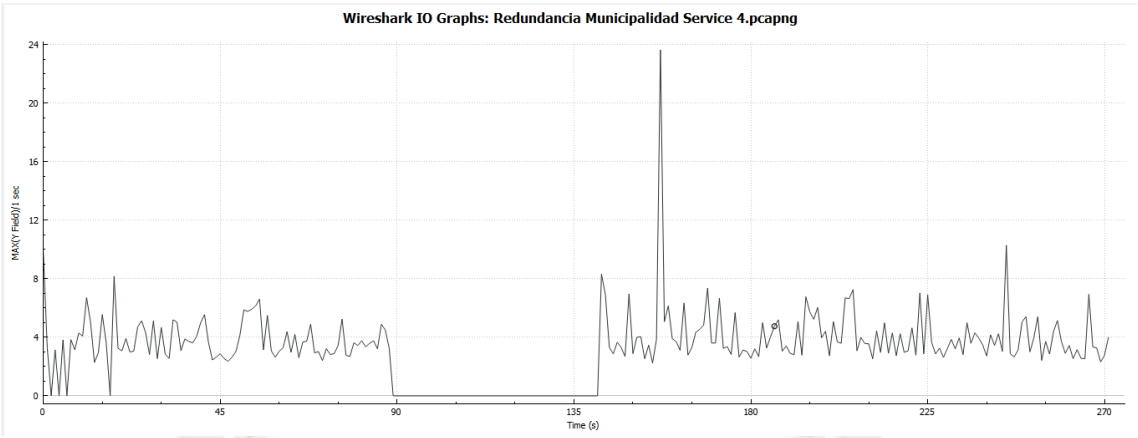


Figura 142. Tiempo de redundancia entre router de la municipalidad y el router service 4 con el switch core 01 sin funcionamiento.
Fuente: Elaboración propia.

En la figura 141 se observa que la muestra fue con más de 260 paquetes y que sufre una abrupta caída cerca del paquete 90, retomando la continuidad a partir del paquete 140.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 50 segundos.

7.2.11.7.2 Desconexión Switch Borde 01

7.2.11.7.2.1 Figuras del comportamiento redundante en la conectividad entre la Municipalidad y el Service 3

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de redundancia es de aproximadamente 5 segundos entre el router de la municipalidad y el router service 3.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 142.

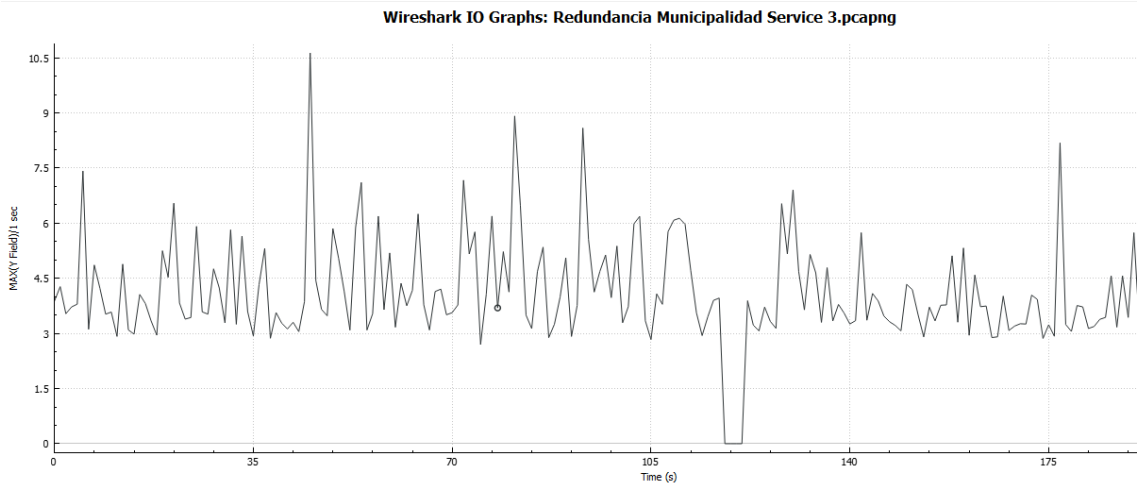


Figura 143. Tiempo de redundancia entre router de la municipalidad y el router service 3 con el switch borde 01 sin funcionamiento.
Fuente: Elaboración propia.

En la figura 142 se observa que la muestra fue con más de 180 paquetes y que sufre una abrupta caída cerca del paquete 119, retomando la continuidad a partir del paquete 125.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 6 segundos.

7.2.11.7.2.2 Figura del comportamiento redundante en la conectividad entre la Municipalidad y el Service 4

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de redundancia es de aproximadamente 6 segundos entre el router de la municipalidad y el router service 4.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 143.

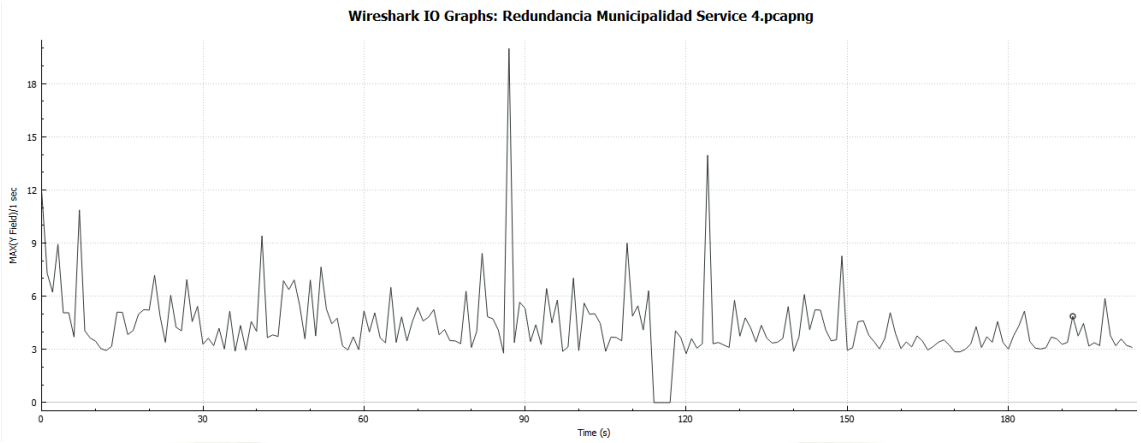


Figura 144. Tiempo de redundancia entre router de la municipalidad y el router service 4 con el switch borde 01 sin funcionamiento.
Fuente: Elaboración propia.

En la figura 143 se observa que la muestra fue con más de 190 paquetes y que sufre una abrupta caída cerca del paquete 112, retomando la continuidad a partir del paquete 118.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 6 segundos.

7.2.11.7.3 Desconexión Switch Service 01

7.2.11.7.3.1 Figura del comportamiento redundante en la conectividad entre la Municipalidad y el Service 3

Según los datos obtenidos en la prueba previas, se obtuvo que el tiempo de redundancia es de aproximadamente 2 segundos entre el router de la municipalidad y el router service 3.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 144.

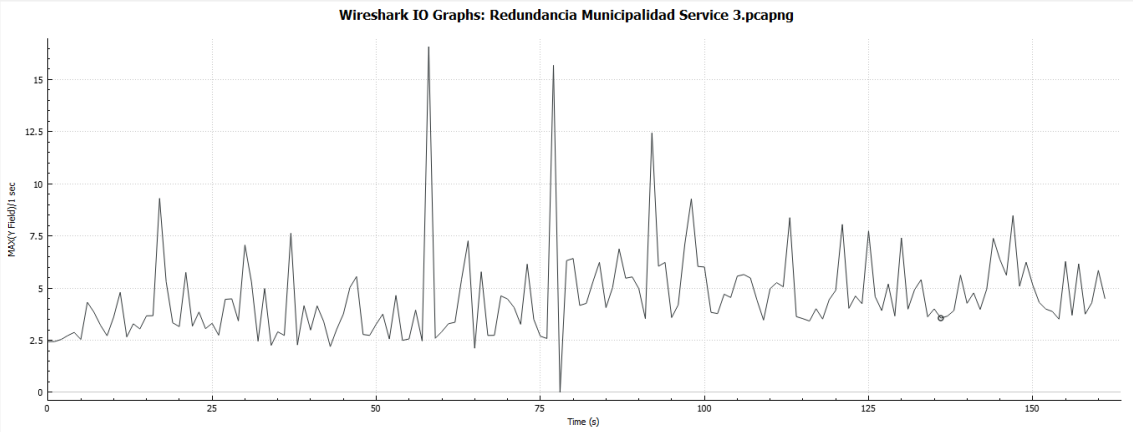


Figura 145. Tiempo de redundancia entre router de la municipalidad y el router service 3 con el switch service 01 sin funcionamiento.
Fuente: Elaboración propia.

En la figura 144 se observa que la muestra fue con más de 160 paquetes y que sufre una abrupta caída cerca del paquete 75, retomando la continuidad a partir del paquete 76.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 1 segundos.

7.2.11.7.3.2 Figura del comportamiento redundante en la conectividad entre la Municipalidad y el Service 4

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de redundancia es de aproximadamente 2 segundos entre el router de la municipalidad y el router service 4.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 145.

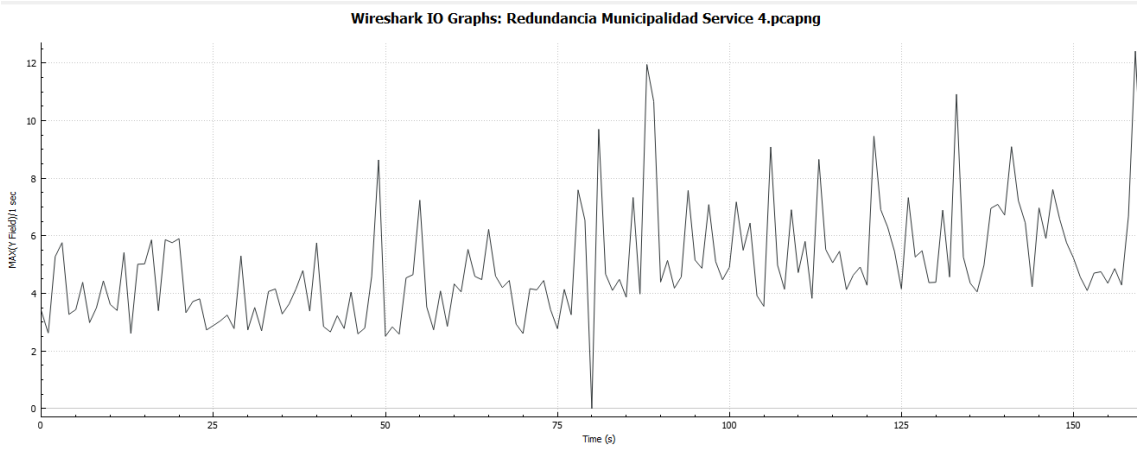


Figura 146. Tiempo de redundancia entre router de la municipalidad y el router service 4 con el switch borde 01 sin funcionamiento.
Fuente: Elaboración propia.

En la figura 145 se observa que la muestra fue con más de 160 paquetes y que sufre una abrupta caída cerca del paquete 78, retomando la continuidad a partir del paquete 79.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 2 segundos.

7.2.11.7.4 Desconexión Switch Core 02

7.2.11.7.4.1 Figura del comportamiento redundante en la conectividad entre la Comisaría 1 y el Service 3

Según los datos obtenidos en la prueba previa, se obtuvo que el enlace entre la Comisaría 1 y el router service 3 no sufrió una caída en el enlace.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 146.

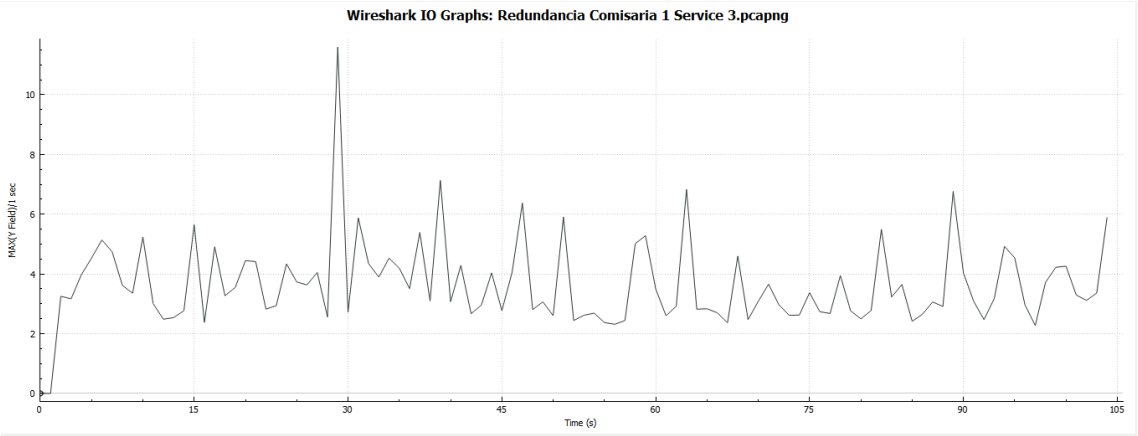


Figura 147. Tiempo de redundancia entre router de la Comisaría 1 y el router service 3 con el switch core 02 sin funcionamiento.
Fuente: Elaboración propia.

En la figura 146 se observa que la muestra fue con más de 100 paquetes.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el enlace no sufrió ninguna caída.

7.2.11.7.4.2 Gráfica del comportamiento redundante en la conectividad entre la Comisaría 01 y el Service 4

Según los datos obtenidos en la prueba previa, se obtuvo que el enlace entre la Comisaría 1 y el router service 4 no sufre ninguna afectación.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 147.

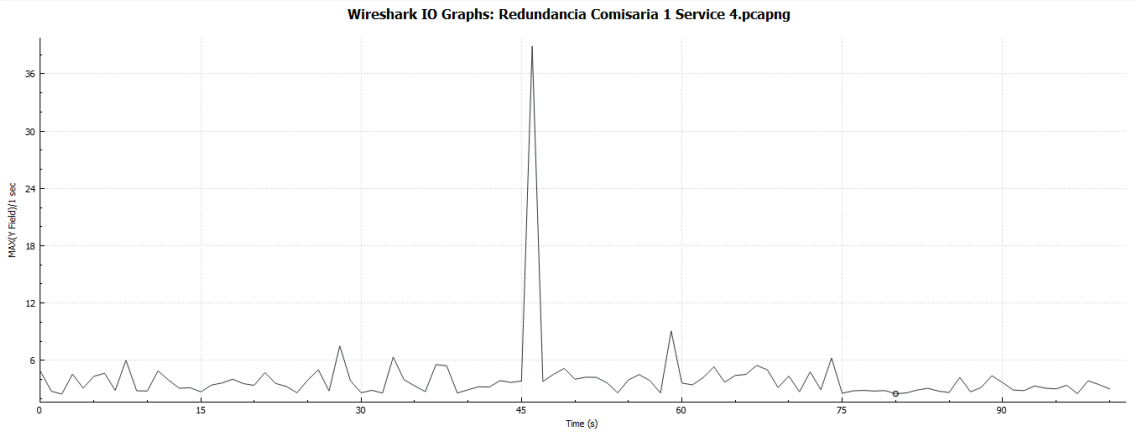


Figura 148. Tiempo de redundancia entre router de la Comisaría 1 y el router service 4 con el switch core 02 sin funcionamiento.
Fuente: Elaboración propia.

En la figura 147 se observa que la muestra fue con más de 100 paquetes.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el enlace no sufrió ninguna caída.

7.2.11.7.5 Desconexión Switch Core 01, Switch Service 02

7.2.11.7.5.1 Figura del comportamiento redundante en la conectividad entre la Comisaría 2 y el Service 3

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de redundancia es de aproximadamente 56 segundos entre el router de la Comisaría 2 y el router service 3.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 148.

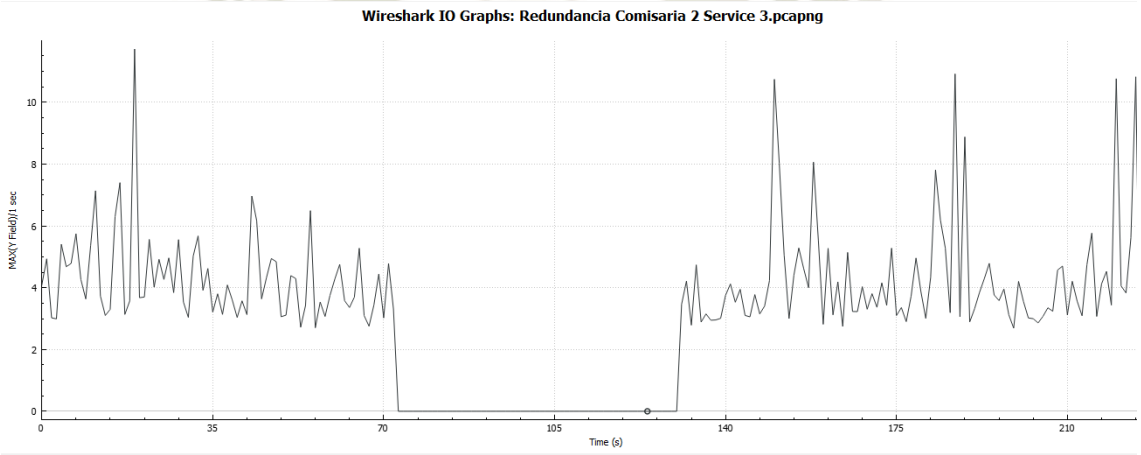


Figura 149. Tiempo de redundancia entre router de la Comisaría 2 y el router service 3 con el switch core 01 y switch service 02 sin funcionamiento.
Fuente: Elaboración propia.

En la figura 148 se observa que la muestra fue con más de 210 paquetes y que sufre una abrupta caída cerca del paquete 72, retomando la continuidad a partir del paquete 128. De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 56 segundos.

7.2.11.7.5.2 Figura del comportamiento redundante en la conectividad entre la Comisaría 2 y el Service 4

Según los datos obtenidos en la prueba previa, se obtuvo que el tiempo de redundancia es de aproximadamente 55 segundos entre el router de la Comisaría 2 y el router service 4.

Realizando el muestreo con una mayor cantidad de paquetes, se obtuvo la figura 149.

En la figura 149 se observa que la muestra fue con más de 210 paquetes y que sufre una abrupta caída cerca del paquete 69, retomando la continuidad a partir del paquete 125.

De esa forma, estableciendo un tiempo de 1 segundo entre cada paquete enviado y recibido se obtiene que el tiempo de redundancia fue de 56 segundos.

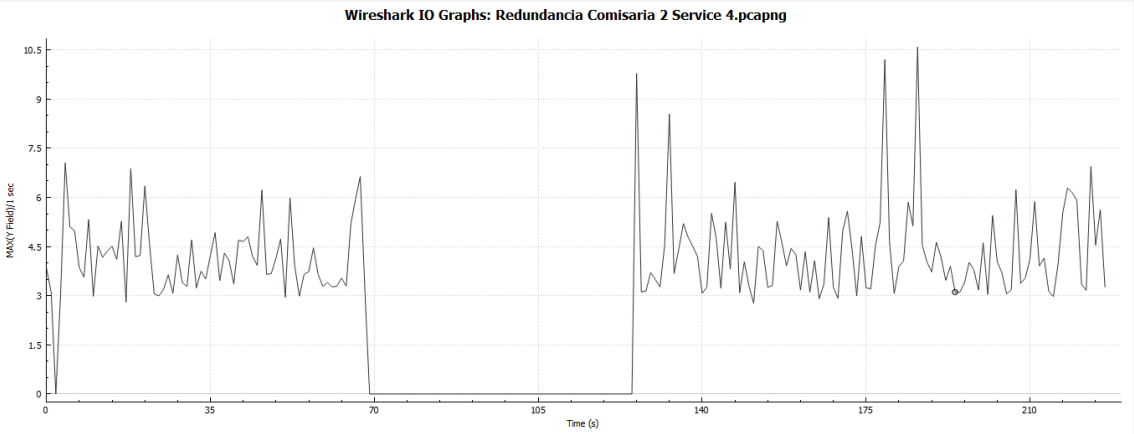


Figura 150. Tiempo de redundancia entre router de la Comisaría 2 y el router service 4 con el switch core 01 y switch service 02 sin funcionamiento.
Fuente: Elaboración propia.

De los datos obtenidos en las pruebas realizada, se concluye que el punto de intercambio de tráfico cumple con los objetivos de diseño, basando la experimentación en el análisis de la capa 2, capa 3 y capa 4 del modelo OSI.

Contando con enlaces redundantes entre los miembros, la jerarquización del punto de intercambio de tráfico, servicios adicionales prestados para los miembros y un control total de la topología de red.

Debido al cumplimiento del diseño del punto de intercambio de tráfico y la demostración del funcionamiento, a continuación, se presenta la propuesta de equipos para la implementación del punto de intercambio de tráfico.

CAPÍTULO VIII: EQUIPAMIENTO EN LA IMPLEMENTACIÓN DEL PUNTO DE INTERCAMBIO DE TRÁFICO

8. Hardware y Software propuesto para la implementación del punto de intercambio de tráfico

8.1 Equipamiento

En base al diseño y desarrollo de la topología realizada en el capítulo anterior, presentamos el hardware requerido para la implementación del punto de intercambio de tráfico y un manejo del costo aproximado.

Los precios estimados presentados en la tabla fueron obtenidos de la página de productos de Mikrotik[11] y el costo del servidor HP fue extraído de la página de Vralatech[12].

En la tabla 56 se presentan los dispositivos requeridos por parte de los miembros para su interconexión con el punto de intercambio de tráfico.

Tabla 57. Equipamiento por miembro del punto de intercambio de tráfico

Dispositivo	Función	Modelo	Descripción	Unidad	Costo Unitario ($)	Total ($)
Borde Router	Interconectar la red del participante con el IXP	CCR2004-1G-12S+2XS	Puerto de Fibra 10Gb: 12 Puerto de Fibra 25Gb: 2	2	595	1190

[11] Productos Mikrotik: https://mikrotik.com/products/

[12] Servidor Hp: https://vrlatech.com/product/hp-proliant-dl160-g9-server-1-x-e5-2660v3-16gb-ram-1-x-1-2tb-sas-2-5-hdd/

				Puerto ethernet 10/100/1000: 1 Ram: 4 GB CPU Core: 4			
SFP mono modo	kit	SFP para la interconexión de fibra entre dispositivos	S-3553LC-20D	SFP LC UPC Longitud de onda : 1310nm/1550 nm Distancia: 20 km	4	79	316
Total ($)		-------	-------	-------	-------	-------	1506

Fuente: Elaboración propia.

El costo aproximado por miembro para su interconexión es de 1 506 dólares americanos, cubriendo de esta manera los dos router de borde, los SFP para su interconexión externa; desde su sede hasta el punto de intercambio de tráfico y la interconexión entre los router de borde y los switch de borde dentro de la infraestructura del punto de intercambio de tráfico.

En la tabla 57 se presentan los dispositivos requeridos para la implementación del punto de intercambio de tráfico.

Tabla 58. Equipamiento del punto de intercambio de tráfico.

Dispositivo	Función	Modelo	Descripción	Unidad	Costo Unitario ($)	Total ($)
Service Router	Interconectar los servicios al IXP	RB3011UiAS-RM	Puerto de Fibra: 1 Puerto ethernet 10/100/1000: 10 Ram: 1GB CPU Core: 2	2	179	358
Noc Router	Administración y configuración del IXP	RB2011UiAS-RM	Puerto de Fibra: 1 Puerto ethernet 10/100: 5 Puerto ethernet 10/100/1000: 5 Ram: 128MB CPU Core: 1	1	119	119
Servidor	Servidor que brinde la máquina virtual para el route server y otros servicios	HP ProLiant DL160 G9 Server E5-2660v3	Procesador: 1 x Intel Xeon 10 Core E5-2660v3 2.30 GHz 25MB Intel Ram: 16GB DDR4 Memoria:11 x 1.2TB 12Gb/s	1	2655	2655

			10K RPM SAS 2.5" HDD			
Switch Borde	Interconexión entre borde router y switch core	CRS326-24S+2Q+RM	Puerto Ethernet 10/100/1000: 1 Puerto de Fibra 10Gb: 24 Puerto de fibra 40Gb: 2	2	499	998
Switch Core	Switch con mayor manejo de tráfico interconecta switch borde y switch service	CRS326-24S+2Q+RM	Puerto Ethernet 10/100/1000: 1 Puerto de Fibra 10Gb: 24 Puerto de fibra 40Gb: 2	2	499	998
Switch Service	Interconexión de servicios prestados del IXP hacia los miembros	CRS328-4C-20S-4S+RM	Puerto Ethernet combo: 4 Puerto de fibra 1 Gb: 20 Puerto de fibra 10Gb: 4 RAM: 512MB CPU Core: 1	2	379	758

Cable óptico de conexión directa activa AOC	Interconexión directa enlaces de 10Gbps	S+AO0005	Velocidad: 1Gbps/10Gbps Distancia: 5m	9	49	441
Cable óptico de conexión directa activa AOC	Interconexión directa enlaces de 1Gbps	S+AO0005	Velocidad: 1Gbps/10Gbps Distancia: 5m	10	49	490
Total ($)	-------	-------	-------	-------	-------	6817

Fuente: Elaboración propia.

El costo de adquisición del equipamiento para el punto de intercambio de tráfico tiene un valor estimado de 6817 dólares americanos.

Los precios a aquí presentados pueden variar según la marca de dispositivos que se desee utilizar, para nuestro caso, se hizo el cálculo en base a dispositivos Mikrotik y el servidor HP ProLiant DL 160 G9, los SFP de interconexión pueden variar según modelo, tipo y marca, para este caso, se pensó en la utilización de SFP activos de conexión directa, pensando en la maniobrabilidad y facilidad de uso entre los dispositivos y reducir la probabilidad de falla.

Los equipos Mikrotik propuestos se encuentran más detallados en los anexos del presente trabajo.

8.2 Capacidades de Enlace

Para el diseño propuesto, se consideraron las capacidades mínimas y máximas, con el fin de evitar cuellos de botella entre los dispositivos y garantizar que el punto de intercambio de tráfico no genere retardos a causa de saturación de enlaces, así mismo, permite un crecimiento en el tráfico de los router de borde, sin la necesidad de modificar enlaces en la parte Core del punto de intercambio de tráfico, hasta que excedan los 10Gpbs por interfaz, por lo que se tendría que pasar a interfaces de mayor capacidad, manteniendo el diseño pero con interfaces de mayor rendimiento.

Los miembros están equipados con dispositivos que cuentan con enlaces de 10Gbps, pero proyectados un inicio a trabajar con tasas de hasta 1Gbps por enlace, con opción de crecimiento inmediato a los 10Gbps disponibles por cada enlace físico y a futuro crecimiento en capacidad de enlaces por medio de protocolos de agregación como bonding, 802.3ad, entre otros.

El punto de intercambio de tráfico esta interconectado entre los switch con enlaces de 10Gbps con opción de crecimiento inmediato mediante protocolos de agregación de enlace o puertos de 40Gbps disponibles en los equipos.

Los servicios, están equipados con enrutadores con capacidad de 1 Gbps cada uno, con disponibilidad de crecimiento mediante protocolos de agregación de enlaces. Los switch de servicio cuentan con puertos de 10Gbps con proyección de crecimiento a futuro.

La tabla 58 las capacidades iniciales de los dispositivos del punto de intercambio de tráfico.

Tabla 59. Distribución de capacidades de enlace entre dispositivos

Interconexión entre dispositivos					
Dispositivo	**Interfaz**	**Dispositivo**	**Interfaz**	**Capacidad de Enlace**	**Importancia**
Municipalidad	Ether 2	Borde Router 01	Ether 3	1Gbps	Principal
Municipalidad	Ether 3	Borde Router 02	Ether 3	1Gbps	Secundario
Comisaría 1	Ether 2	Borde Router 03	Ether 3	1Gbps	Principal
Comisaría 1	Ether 3	Borde Router 04	Ether 3	1Gbps	Secundario
Comisaría 2	Ether 2	Borde Router 05	Ether 3	1Gbps	Principal
Comisaría 2	Ether 3	Borde Router 06	Ether 3	1Gbps	Secundario
Borde Router 01	Ether 2	Sw Borde 01	Ether 3	1Gbps	Principal
Borde Router 02	Ether 2	Sw Borde 02	Ether 3	1Gbps	Secundario
Borde Router 03	Ether 2	Sw Borde 01	Ether 4	1Gbps	Principal
Borde Router 04	Ether 2	Sw Borde 02	Ether 4	1Gbps	Secundario
Borde Router 05	Ether 2	Sw Borde 01	Ether 5	1Gbps	Principal
Borde Router 06	Ether 2	Sw Borde 02	Ether 5	1Gbps	Secundario
Sw Borde 01	Ether 7	Sw Borde 02	Ether 7	10Gpbs	Secundario
Sw Borde 01	Ether 1	Sw Core 01	Ether 1	10Gpbs	Principal
Sw Borde 01	Ether 2	Sw Core 02	Ether 1	10Gpbs	Secundario
Sw Borde 02	Ether 1	Sw Core 01	Ether 2	10Gpbs	Principal
Sw Borde 02	Ether 2	Sw Core 02	Ether 2	10Gpbs	Secundario
Sw Core 01	Ether 3	Sw Service 01	Ether 1	10Gpbs	Principal
Sw Core 01	Ether 4	Sw Service 02	Ether 3	10Gpbs	Secundario
Sw Core 01	Ether 5	Noc Router	Ether 1	1Gbps	Principal
Sw Core 02	Ether 3	Sw Service 01	Ether 2	10Gpbs	Secundario
Sw Core 02	Ether 4	Sw Service 02	Ether 2	10Gpbs	Principal
Sw Core 02	Ether 5	Noc Router	Ether 2	1Gbps	Secundario
Sw Service 01	Ether 3	Service Vlan 3	Ether 1	1Gbps	Principal
Sw Service 01	Ether 4	Service Vlan 4	Ether 3	1Gbps	Secundario
Sw Service 02	Ether 1	Service Vlan 4	Ether 1	1Gbps	Principal
Sw Service 02	Ether 4	Service Vlan 3	Ether3	1Gbps	Secundario

Fuente: Elaboración propia.

Según la descripción realizada en la tabla 58, los enlaces que conforman la topología propuesta son representados en la figura 150.

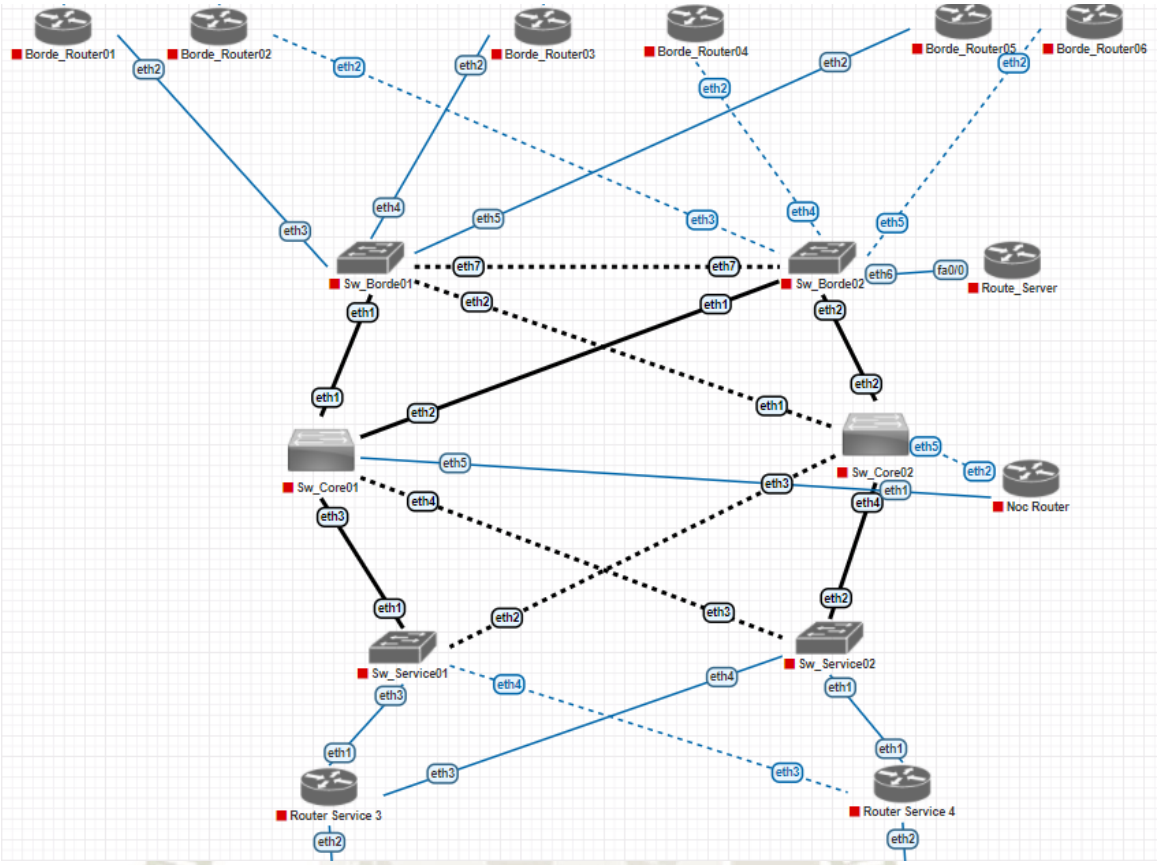


Figura 151.Capacidad de enlaces de la tercera topología.
Fuente: Elaboración Propia.

Los enlaces de color azul representan enlaces de 1Gbps, mientras que los enlaces de color negro representan enlaces de 10Gbps.

Los enlaces de líneas punteadas representan los enlaces redundantes de la topología.

8.3 Requerimientos del enlace físico entre miembros

La ubicación de los miembros del punto de intercambio de tráfico, así como la interconexión lógica se muestra en la figura 151.

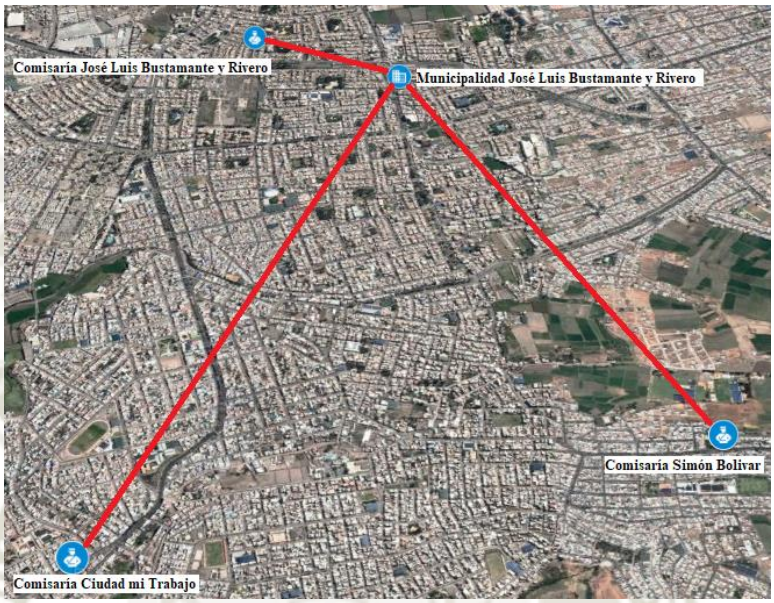


Figura 152. Ubicación de los miembros del punto de intercambio de tráfico
Fuente: Elaboración propia.

La interconexión de los miembros del punto de intercambio de tráfico se dará en el centro de datos ubicado en la municipalidad, esta será de forma cableada por el ancho de banda requerido y analizado en secciones anteriores.

Por los niveles de ancho de banda y por los requerimientos de crecimiento proyectados, una solución inalámbrica generaría problemas en la expansión del ancho de banda en el futuro, por lo que una conexión cableada por medio de fibra óptica seria la forma más eficiente para interconectar los miembros y no generar sobrecostos al momento de aumentar el ancho de banda por miembro.

Para la interconexión por medio de fibra óptica se debe considerar lo siguiente:

- Topología de conexión y el tipo de fibra óptica
    - Topología Punto a punto
    - Fibra monomodo

- Diseño del recorrido de las rutas de fibra para la interconexión
    - Ubicación de los puntos a interconectar
    - Determinar la ruta con menor distancia
    - Estudio técnico y cálculos de enlaces
    - Tipos de tendido a realizar: aéreo o subterráneo
- Desarrollo del tendido de fibra a realizar
    - Estudios de factibilidad y viabilidad
    - Certificaciones de cableado
- Módulos de fibra para la interconexión entre los equipos

8.4 Cálculo de Confiabilidad

El cálculo de la confiabilidad de los equipos propuestos lo realizaremos de acuerdo a los valores del tiempo medio entre fallas (MTBF) presentados por el fabricante según cada equipo.

En la tabla 59 mostramos los valores de MTBF según los equipos propuestos para la topología extraídos de la página oficial de Mikrotik.

Tabla 60. Tiempo medio entre fallas de dispositivos Mikrotik

Tiempo Medio entre fallas		
Dispositivo	**Modelo**	**MTBF**
Router	CCR 2004-1G-12S+-2XS	200000
Router	RB3011UiAS-RM	200000
Switch	RB2011UiAS-RM	200000
Switch	CRS326-24S+2Q+RM	200000
Switch	CRS328-4C-20S-4S+RM	200000

Fuente: Elaboración propia.

La confiabilidad está dada a partir de la ecuación de la distribución de Weibull:

$$C=e^{-(\frac{\tau}{MTBF})}$$

Donde:

τ= tiempo de funcionamiento (horas)

MTBF: tiempo medio entre fallas

Para 1 año:

$$C=e^{-(\frac{8760}{200000})}$$

C= 0.9571 → C= 95.7%

Para 5 años:

$$C=e^{-(\frac{43800}{200000})}$$

C=0.8033 → C= 80.3%

Para 10 años:

$$C=e^{-(\frac{87600}{200000})}$$

C= 0.6453 → C= 64.5%

Para 15 años:

$$C=e^{-(\frac{131400}{200000})}$$

C= 0.5184 → C=51.84%

En la tabla 60, mostramos el porcentaje de confiabilidad de los equipos propuestos, considerando un trabajo continuo de 24 horas por cada equipo.

Tabla 61. Porcentaje de Confiabilidad de los dispositivos

Confiabilidad			
Tiempo	**MTB**	**Horas por día**	**Confiabilidad (%)**
1 año	200000	24	95.7
5 años	200000	24	80.3
10 años	200000	24	64.5
15 años	200000	24	51.84

Fuente: Elaboración propia.

De los datos obtenidos en la tabla mostrada anteriormente, se obtiene que los equipos propuestos poseen un nivel de confiabilidad superior al 50% en un promedio de 10 años de funcionamiento continuo, a partir del año 15 el nivel de confiabilidad baja del 50%, por lo que el cambio de dispositivos a partir de la fecha es requerido para evitar futuras complicaciones.

8.5 Software

El acceso a los equipos debe realizarse desde cualquier herramienta que el gestor desee, desde herramientas proporcionadas por la misma marca, hasta herramientas externas desde el sistema operativo que el usuario elija, para garantizar la funcionalidad del sistema.

Para el manejo, configuración, análisis y troubleshooting de cada equipo, se utiliza software libre o propietario de la marca con licencia libre.

A continuación, se nombran las herramientas de mayor utilización para la gestión y manejo de los dispositivos de redes.

8.5.1 Dispositivos Mikrotik

La gestión de dispositivos Mikrotik puede realizarse de varias formas, la forma más común es mediante la utilización de herramientas propietarias de la marca con licencia libre, las cuales fueron profundizadas en capítulos anteriores.

Dentro de las herramientas propietarias tenemos:

- WinBox
- WebFig
- Aplicación móvil
- The Dude

Aparte del uso de esas herramientas, la administración de estos dispositivos puede ser desarrolladas por otros tipos de herramientas de conexión remota explicadas a continuación.

8.5.2 Putty

Los dispositivos acá presentados cuentan con acceso remoto habilitado por medio del protocolo SSH (Secure Shell), el cual es un protocolo con cifrado de 128 bits para la interconexión de los dispositivos, de esa forma la información transmitida entre ellos no podrá ser leída por un sniffer o alguna herramienta intermedia que intente leer comandos, usuarios, contraseñas o un analizador de protocolos.

Se propone la utilización del software denominado Putty, el cual tiene la opción de trabajar como cliente SSH, telnet, Rlogin, desarrollado en un inicio por Taha Simon.

Putty está disponible para plataformas de Windows, Linux, Mac OS y es un software de licencia libre. Entre sus características principales permite almacenar direcciones del host, permite conexión tanto de IPv4 como IPv6, el cambio de puerto de acceso, entre otros.

Putty es solo una herramienta de acceso, que va permitir entrar al terminal del dispositivo para poder realizar las configuraciones y su interfaz de acceso se muestra en la figura 152.

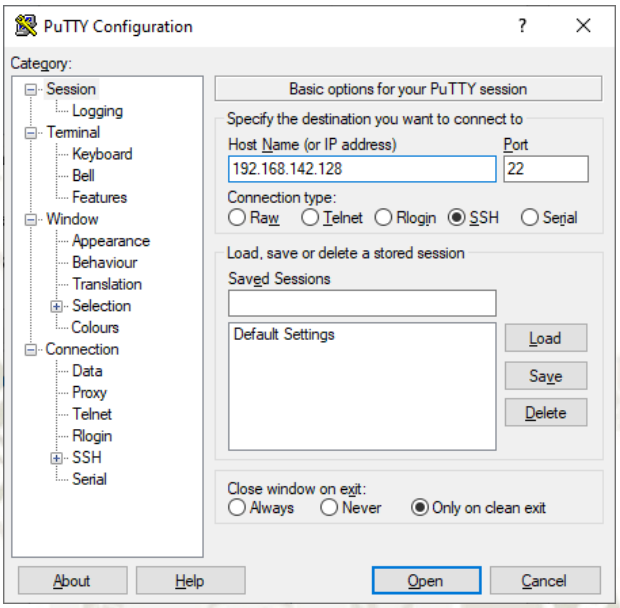


Figura 153. Interfaz de Putty.
Fuente: Elaboración propia.

8.5.3 Símbolo de Sistema Windows

El sistema operativo Windows cuenta con un terminal de comandos, denominado símbolo de sistema o “CMD”, es un espacio en el cual el usuario puede realizar tareas de administración, troubleshooting, puede habilitar SSH o telnet para el acceso a diferentes dispositivos.

Como parte de las herramientas disponibles de troubleshooting disponibles en Windows se tiene:

- Ping
- Tracert
- ARP
- Nslookup
- Netstats

- Route

Estas herramientas permiten al gestor de redes realizar pruebas de troubleshooting para determinar deficiencias en la topología, como caída de enlaces, malas configuraciones de red, tabla de rutas, tabla ARP entre otros.

En la figura 153 se muestra la pantalla del CMD de Windows.

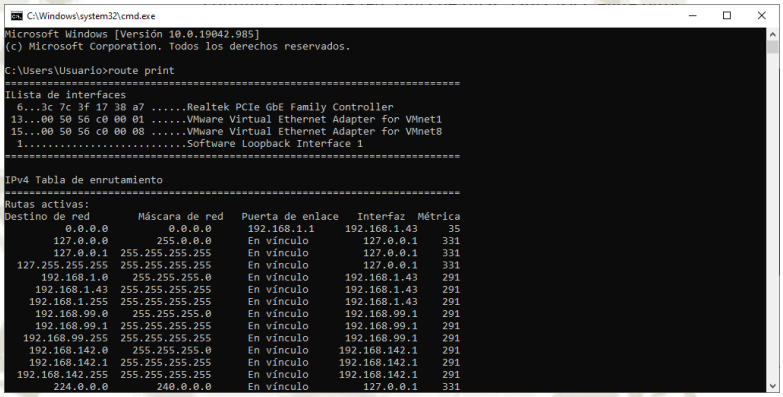


Figura 154. Interfaz CMD de Windows.
Fuente: Elaboración Propia.

8.5.4 Terminal Linux

Todos los sistemas operativos basados en Linux cuentan con un terminal o “Shell” de comandos, el cual tiene funciones similares al CMD de Windows.

Como parte de las herramientas de troubleshooting tenemos, por ejemplo:

- Netstat
- Tcpdump
- Ping
- Traceroute
- Tracepath
- Nmap
- Route

En la figura 154 se muestra la pantalla del Shell de comandos de Linux.

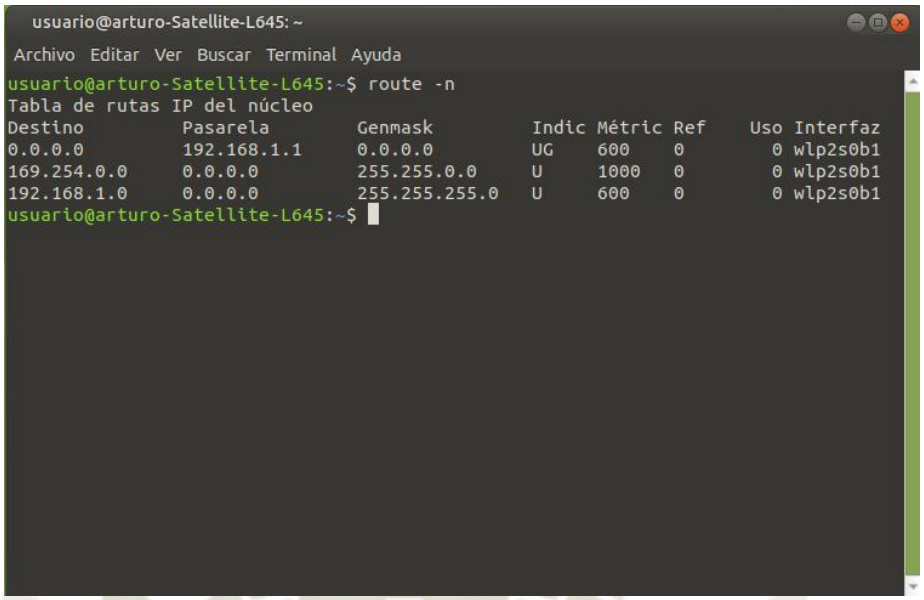


Figura 155. Shell de comando de Linux.
Fuente: Elaboración propia.

CONCLUSIONES

- Se realizó el cálculo de ancho de banda en base a las necesidades de los servicios por miembro del punto de intercambio de tráfico, obteniendo el ancho de banda total por sede, para realizar el diseño del punto de intercambio de tráfico de forma viable.

- Como parte del objetivo propuesto, se logró modelar el diseño de un punto de intercambio de tráfico con equipamiento de marca Mikrotik con ayuda de un emulador de redes, el cual está pensado para ser implementado con equipamiento de la marca en la actualidad. Mostrando la necesidad de agregar un dispositivo de otra marca que ayude a desarrollar la propuesta.

- Se logró entender el funcionamiento de un punto de intercambio de tráfico de capa 2 con un servidor de rutas que apoye el emparejamiento entre los diferentes miembros.

- Los comportamientos de las variables de medición fueron realizados según lo esperado con las herramientas disponibles por el mismo emulador y los dispositivos Mikrotik y el manejo de atributos disponibles por cada protocolo. Permitiendo de esta forma analizar el comportamiento de los diferentes protocolos utilizados frente a las diferentes pruebas realizadas.

- El manejo del protocolo RSTP ayudó a mantener una red redundante, pero dando tiempos de respuesta más altos de los esperados.

- Se utilizó la emulación de un dispositivo de la marca Cisco con el fin de poder recrear el comportamiento de un servidor de rutas y demostrar su forma de funcionamiento e integración con la topología basada en la marca Mikrotik

- La imagen del sistema operativo de los dispositivos Mikrotik no tienen limitación en funciones; lo que permitió un mayor desenvolvimiento en el desarrollo del proyecto y es una sola imagen para cualquier tipo de dispositivo, lo cual crea una gran ventaja frente a dispositivos de otras marcas. Teniendo como salvedad no poder realizar pruebas que involucren el ancho de banda ya que el sistema operativo gratuito de Mikrotik solo dispone de 1 Mbps de capacidad.

- Se analizó el comportamiento de los dispositivos Mikrotik en un entorno simulado y se realizó una comparación frente al modo de funcionamiento de un dispositivo simulando el comportamiento real, hallando que los tiempos de respuesta en un entorno real iban a mejorar frente a una propuesta netamente simulada.

- El manejo de routing de los dispositivos Mikrotik permiten un correcto desenvolvimiento en el proyecto, mientras que las funciones de switching de los dispositivos Mikrotik presentan ciertas desventajas frente a otras marcas; las cuales desarrollaron de mejor forma protocolos y manejo de dispositivos de capa 2.

RECOMENDACIONES

- Como parte del manejo de un software de emulación de redes, se recomienda analizar los parámetros mínimos de funcionamiento del software, así como los parámetros requeridos por los dispositivos a manejar y de esa forma utilizar el emulador que se preste mejor a las características que uno posea y desee implementar.
- Como parte de la etapa de diseño se recomienda tener las imágenes de los equipos propuestos, protocolos a utilizar y un plan de direccionamiento previo al armado e implementación de la simulación.
- Tener en claro el manejo y conocimiento de los protocolos utilizados en el diseño, ya que ayudaran a un mejor entendimiento del funcionamiento de la red, así como un soporte para la solución de problemas.
- Se recomienda tener en claro el entendimiento de redes jerárquicas, así como los modelos de redes en capa 2 para comprender el funcionamiento y evolución de los puntos de intercambio de tráfico.
- Se recomienda tener en cuenta que el bloqueo por dirección de MAC no puede realizarse en entorno virtualizado ya que los dispositivos al reiniciarse cambian de dirección MAC.
- Se recomienda realizar la implementación por etapas probando el funcionamiento independientemente, de esa forma al unir todas las etapas la solución de problemas se verá reducida a pequeñas partes específicas.

- El diseño propuesto tendrá un funcionamiento de igual manera si se consideran ASN del mismo valor, teniendo diferencias en los valores de rutas, pero no en la selectividad de las mismas por medio de comunidades BGP.

- La implementación del servidor de rutas no está desarrollada en el proyecto, solo se dio un enfoque de su funcionamiento, para una implementación con servidor de rutas; se recomienda la implementación de un servidor físico con software open source como BIRD, Quagga, Zebra, etc.

- Se recomienda usar el paquete "EVE-NG-Win-Client-Pack-2.0" para acceder a herramientas de administración como Putty o herramientas de análisis como Wireshark.

- Por último, se recomienda estar al tanto de las mejoras que la marca presentará en sus siguientes versiones para estar al tanto del desenvolvimiento, crecimiento y evolución que podrá tener el diseño propuesto a través del tiempo.

.

REFERENCIAS BIBLIOGRÁFICAS

Amsix. (2021). *Config Guide*. Obtenido de https://www.ams-ix.net/ams/documentation/config-guide

Asociación Nacional de Proveedores de Internet,. (2021). *Topología NAP*. Obtenido de http://www.nap.pe/acerca-del-nap-peru/topologia-nap/

Banco de desarrollo de América Latina. (2014). *Expansion de infraestructura regional para la interconexión de tráfico de internet en america latina*. CAF.

Bates, T., Chandra, R., Katz, D., & Rekhter, Y. (Enero 2007). *BGP-4, MultIProtocol Extensions for*. Internet Engineering Task Force (IETF).

Bradner, S. (Julio 1991). *Benchmarking Terminology for Network Interconnection Devices*. Internet Engineering Task Force (IETF).

Bucke, S., Silva, M., dos Reis, R., Lachos, D., Lourenco, H., & Rothenberg, C. (2016). An Analysis of the Largest National Ecosystem of Public Internet eXchange Points: The Case of Brazil. *JOURNAL OF COMMUNICATION AND INFORMATION SYSTEMS*, VOL. 31, NO. 1,.

Cavalcanti, D. B. (2010). The Role of Internet Exchange Points in Broadband Policy and Regulation. *Proceedings of the 4th ACORN-REDECOM Conference*.

Cicileo, G. (2016). IXP – Puntos de Intercambio. Lacnic.

Cicileo, G. (16 de Agosto de 2017). BGP en IPv6.

CISCO. (10 de Agosto de 2005). *OSPF Design Guide*. Obtenido de https://www.cisco.com/c/en/us/support/docs/IP/open-shortest-path-first-ospf/7039-1.html

Cisco. (13 de Abril de 2016). *Voice Over IP - Per Call Bandwidth Consumption.* Obtenido de https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html

Cisco Network Academy. (s.f.). *Ethernet.* Obtenido de https://www.itesa.edu.mx/netacad/introduccion/course/module5/#5.1.2.3

Coltun, R., Ferguson, D., Moy, J., & Lindem, A. (Julio 2008). *OSPF for IPv6.* internet Engineering Task Force (IETF).

Comité Técnico NAP – PERU. (2006). *Características técnicas de los Miembros del NAP - Peru.* NAP.

Cotton, M., & Vegoda, L. (2010). *Special Use IPv4 Addresses.* Internet Engineering Task Force (IETF).

de León, O. (2012). *Desarrollo de la conectividad nacional y regional en América Latina.*

Deering, S., & Hinden, R. (Diciembre 1998). *Internet Protocol, Version 6 (IPv6) Specification.* Internet Engineering Task Force (IETF).

Estrada Padilla.__, N. J., Lorío Rojas, A. M., & Ramírez Santana, U. A. (2018). *Diseño de Puntos de Intercambio de Internet en entornos virtuales con tecnología Cisco, implementando servicios multimedia.* León.

Frans Armando, G. C. (Diciembre de 2011). Diseño de una red de telemedicina para monitoreo de pacientes en el distrito de Sicaya perteneciente a la ciudad de Huancayo. Lima, Perú.

Galperin, H. (2013). *La Conectividad en América Latina y el Caribe El Rol de los Puntos de Intercambio de Tráfico.* Universidad de San Andrés.

Gerometta, O. (19 de Noviembre de 2011). *Mis Libros de Networking*. Obtenido de http://librosnetworking.blogspot.com/2011/11/IPv6-algo-de-historia.html

Giotsas, V., Zhou, S., & Luckie, M. (Diciembre 2013). Inferring multilateral peering. *CoNEXT '13: Proceedings of the ninth ACM conference on Emerging networking experiments and technologies*.

Hinden, R., & Deering, S. (Febrero 2006). *IP Version 6 Addressing Architecture*. Intenet Engineerig Task Force (IETF).

IEEE. (1989). EEE/ISO 802.2-1989 - ISO/IEEE International Standard - Information processing systems — Local area networks - Part 2: Logic Link Control. IEEE.

IEEE. (2018). IEEE 802.3-2018 - IEEE Standard for Ethernet. IEEE.

Informática, I. N. (octubre de 2018). *Arequipa Resultados Definitivos*. Obtenido de https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1551/04TOMO_01.pdf

Information Sciences Institute. (1981). *INTERNET PROTOCOL*. Marina del Rey: Defense Advanced Research Projects Agency.

Internet Society. (2020). *Physical Infrastructure*. Obtenido de https://www.IXPtoolkit.org/IXPs/physical-infrastructure/

ITU. (2020). *Estudio de Interconectividad y Reducción de Costos de Acceso a Internet en los Países de la Comunidad Andina.* ITU Publications.

Jackson Bertón, M. (2016). Una mirada dentro de La Casa de Internet.

Jensen, M. (Diciembre de 2012). *Promoting the Use of Internet Exchange Points: A Guide to Policy, Management, and Technical Issues.* Obtenido de Internet

Society: https://www.internetsociety.org/wp-content/uploads/2012/12/promote-IXP-guide.pdf

Jian, S., & Fang, Y. Y. (Julio 2011). *Research and implement of Ospfv3 in IPv6 network.*

Kende, M., & Hurpy, C. (2012). *Evaluación del impacto de los puntos de intercambio de tráfico. Estudio empírico de los casos de Kenia y Nigeria.* Internet Society.

Kioti, R., Ager, B., Kotronis, V., Nomikos, G., & Dimitropoulos, X. (Enero 2006). A Comparative Look into Public IXP Datasets. *ACM SIGCOMM Computer Communication Review*, Volumen 46, Numero 1, 22-29.

Krishnamurthy, B., Wills, C., & Zhang, Y. (2001). On the Use and Performance of Content. *Proceedings of the 1st ACM SIGCOMM Workshop on Internet measurement*.

Kurose, J. F., & Ross, K. W. (2017). *Redes de computadoras. Un enfoque descendente.* Pearson.

LACIX. (2020). *La comunidad de IXPs de la región continúa creciendo*. Obtenido de https://lac-ix.org/la-comunidad-de-IXPs-de-la-region-continua-creciendo-2/

LACIX. (2020). *PIT Perú se integra a LAC-IX*. Obtenido de https://lac-ix.org/pit-peru-se-integra-a-lac-ix/

Lacnic. (24 de 07 de 2020). *Lacnic*. Obtenido de Manual de políticas de internet: https://www.lacnic.net/innovaportal/file/543/1/manual-politicas-sp-2-14.pdf

Lacnic. (24 de Julio de 2020). *Lacnic Policy Manual.* Obtenido de https://www.lacnic.net/543/1/lacnic/manual-de-politicas-[v214---24_07_2020]

Lepinski, M., & Kent, S. (Febrero 2012). *An Infrastructure to Support Secure Internet Routing.* Internet Engineering Task Force (IETF) .

Long, H. P. (2007). *Cisco Documents Blog*. Obtenido de http://ciscodocuments.blogspot.com/2011/05/chapter-06-implementing-border-gateway.html

Malik, S. U. (Diciembre de 2014). Using formal methods to validate the usage, protocols, and feasibility in large scale computing systems. Fargo, North Dakota: Dakota State University of Agriculture and Applied Science.

Malik, S., Srinivasan, S. K., Khan, S. U., & Wang, L. (2012). A Methodology for OSPF Routing Protocol Verification. *12th Intlernational Conference on Scalable Computing and Communications.* Changzhou: IEEE.

Mejía, Ó. Á. (2011). Migración del protocolo IPv4 a IPv6. *Revista Contactos*, 55-60.

Molina, B., Palau, C. E., Esteve, M., Alonso, I., & Ruiz, V. (2006). On content delivery network implementation. *Computer Communications 29 (2006,* 2396–2412.

Moy, J. (Abril 1998). *OSPF Version 2.* Internet engineering Task Force (IETF).

Moy, J. (Abril 1998). *OSPF Standardization Report.* The Internet Society.

Moy, J. (Abril 1998). *OSPF Version 2.* Internet Engineering Task Force (IETF).

Nimpuno, N. (2019). IXP Development & Evolution – what have we learnt? *LACNIC 31*.

ODN consultores. (2007). *Análisis de la situación del NAP a nivel de EE.UU. y Latinoamérica.*

PIT Perú. (2020). *Normas Técnicas*. Obtenido de https://peruix.net/normas-tecnicas/

PIT Perú. (2020). *Normativas PIT Perú*. Obtenido de https://www.pitperu.net/normativas

PNET. (2021). *PNET Documentation*. Obtenido de https://pnetlab.com/pages/documentation

Poretsky, S., Erramili, S., Perser, J., & Khurana, S. (Octubre 2006). *Terminology for Benchmarking Network-layer Traffic Control Mechanisms.* Internet Engineering Task Force (IETF).

Registro de direcciones de Internet para America Latina y Caribe. (2020). *Manual de políticas de LACNIC.* Montevideo: LACNIC.

Rekhter, Y., Li, T., & Hares, S. (Enero 2006). *A Border Gateway Protocol 4 (BGP-4).* Internet Engineering Task Force (IETF).

Rivero, Municipalidad Distrital de José Luis Bustamante y. (2019). *Plan de Accion de Seguridad Ciudadana 2019*. Obtenido de https://www.munibustamante.gob.pe/archivos/1558638251.pdf

Schlinker, B., Zarifis, K., Cunha, I., Feamster, N., & Katz-Bassett, E. (Octubre 2014). PEERING: An AS for Us. *Proceedings of the 13th ACM Workshop on Hot Topics in Networks*.

SIA Mikrotīkls. (Abril de 2017). *Manual:The Dude*. Obtenido de https://wiki.mikrotik.com/wiki/Manual:The_Dude

SIA Mikrotīkls. (Febrero de 2019). *Manual:Webfig*. Obtenido de https://wiki.mikrotik.com/wiki/Manual:Webfig

SIA Mikrotīkls. (2019). *Manual:WinBox*. Obtenido de https://wiki.mikrotik.com/wiki/Manual:WinBox

SIA Mikrotīkls. (2020). Obtenido de https://wiki.mikrotik.com/wiki/Manual:Upgrading_RouterOS

SIA Mikrotīkls. (2021). Obtenido de https://mikrotik.com/

SIA Mikrotīkls. (Mayo de 2021). *Mikrotik Mobile App*. Obtenido de https://mikrotik.com/mobile_app

Singh, R. (Julio de 2020). Internet Exchange Points - Best Practices and Policy Considerations. Internet Society.

Texeira, R., & Rexford, J. (Marzo 2006). Managing Routing Disruptions in Internet Service Provider Networks. *IEEE Communications Magazine*.

Vega, E., Rocha, M., & Cicileo, G. (Mayo de 2021). Tutorial de enrutamiento seguro. LACNIC.

Wang, S., Xu, D., & Yan, S. (2010). Analysis and Application of Wireshark in TCP/IP Protocol Teaching. *201O International Conference on E-Health Networking, Digital Ecosystems and Technologies*.

Winther, M. (Mayo 2006). *Tier 1 ISP s : What They Are and Why They Are Important.* IDC.

Yong, T. C. (11 de Diciembre de 2013). IX Best Practices.

ANEXOS

Anexo Nro 1: Equipos Propuestos para implementación

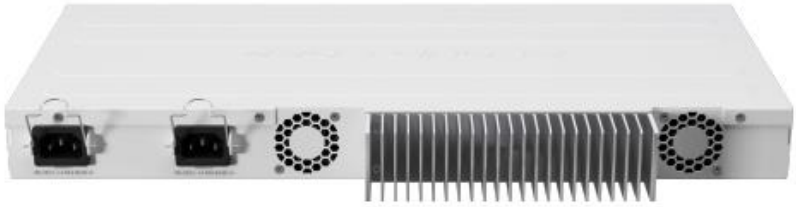
Router de Borde 01 -Borde 02 - Borde 03 - Borde 04 - Borde 05 - Borde 06

Mikrotik CCR2004-1G-12S+2XS

MikroTik CCR2004-1G-12S+2XS

The "Improvise. Adapt. Overcome." mindset can be very helpful, but sometimes you simply need a device that works and solves the problem without additional tinkering. The CCR2004-1G-12S+2XS does just that – forget about all connectivity troubles and expand your setup in any way you please.

Connectivity? You got it! This handy router features 12 x 10G SFP+ and 2 x 25G SFP28 ports.



This is our router with the most powerful single-core performance so far. It provides incredible results in single tunnel (up to 3.4 Gbps) and BGP feed processing.

Be prepared for anything: 10G, 40G and now 25G! Paired with such MikroTik multiport products as CRS317-1G-16S+RM, CRS312-4C+8XG-RM and CRS326-24S+2Q+RM, your networking setup will know no bounds. Performance-wise, CCR2004-1G-12S+2XS is on par with the renowned CCR1009/CCR1016 routers. And with dual redundant power supply you can forget about unexpected downtime! With its elaborate port configuration, the new CCR2004-1G-12S+2XS is the perfect addition to any professional networking arsenal – it will save you tons of time in some tricky situations!

MikroTik CCR2004-1G-12S+2XS

Specifications

Product code	CCR2004-1G-12S+2XS
CPU	AL32400 1700 MHz
CPU core count	4
Size of RAM	RouterOS v6 1792MB ECC / RouterOS v7 4GB ECC
RAM type	DDR4
Storage	128 MB, NAND
Number of 1G Ethernet ports	1
Number of 10G SFP+ ports	12
Number of 25G SFP28 ports	2
Operating system	RouterOS
Router license level	6
Supported input voltage	AC power supply 100 - 240 V
Number of AC inputs	2
Dimensions	443 x 224 x 44 mm
Operating temperature	-20°C to +60°C tested
Max power consumption	49 W

Included parts

2 IEC cords

Rackmount bracket white

Fastening set for rackmount case

IPsec test results

CCR2004-1G-12S+2XS		Hardware accelerated IPsec throughput test					
Mode	Configuration	1400 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Single tunnel	AES-128-CBC + SHA1	303.6	3400.3	353.6	1448.3	354.7	181.6
256 tunnels	AES-128-CBC + SHA1	302.0	3382.4	378.8	1551.6	376.4	192.7
256 tunnels	AES-128-CBC + SHA256	302.0	3382.4	378.8	1551.6	376.4	192.7
256 tunnels	AES-256-CBC + SHA1	300.3	3363.4	374.5	1534.0	374.5	191.7
256 tunnels	AES-256-CBC + SHA256	300.3	3363.4	374.5	1534.0	374.5	191.7

Router Service 3 – Router Service 4

MikrotikRB3011UiAS-RM

RB3011UiAS-RM

The RB3011 is a new multi port device, our first to be running an ARM architecture CPU for higher performance than ever before. The RB3011 has ten Gigabit ports divided in two switch groups, an SFP cage and for the first time a Superspeed full size USB 3.0 port, for adding storage or an external 3G/4G modem.

Unit comes with 1U rackmount enclosure, a touchscreen LCD panel, a serial console port and PoE output functionality on the last Ethernet port.

Specifications

Product code	RB3011UiAS-RM
CPU nominal frequency	1.4 GHz
CPU core count	2
Size of RAM	1 GB
10/100/1000 Ethernet ports	10
Switch chip model	QCA8337-AL3C-R
Power Jack	1
PoE in	Yes (passive only)
PoE out	Yes (port 10)
Supported input voltage	10 V - 30 V
Voltage Monitor	Yes
PCB temperature monitor	Yes
Dimensions	443x92x44mm
License level	5
Operating System	RouterOS
CPU	IPQ-8064
Max Power consumption	10 W

RB3011UiAS-RM 1

Specifications

SFP port	1
USB slot type	USB 3.0 type A
Number of USB ports	1
Serial port	RJ45
Suggested price	$179

Included

24V 1.2A Power adapter

K-19 fastening set

Rack ears

Performance test results

RB3011UiAS		All port test		RouterOS v6.30rc23			
Mode	Configuration	1518 byte		512 byte		64 byte	
		Mbps	kpps	Mbps	kpps	Mbps	kpps
Bridging	none (fast path)	3,946.8	325.0	3,849.4	939.8	783.5	1,530.2
Bridging	25 bridge filter rules	3,946.8	325.0	1,573.7	384.2	178.5	348.6
Routing	none (fast path)	3,946.8	325.0	3,849.4	939.8	736.1	1,437.6
Routing	25 simple queues	3,946.8	325.0	1,718.7	419.6	214.9	419.7
Routing	25 ip filter rules	2,453.1	202.0	836.0	204.1	96.5	188.4

1. All tests are done with Xena Networks specialized test equipment (XenaBay),and done according to RFC2544 (Xena2544)
2. Max throughput is determined with 30+ second attempts with 0.1% packet loss tolerance in 64, 512, 1518 byte packet sizes
3. Values in italic indicate that max throughput was reached without maxing out CPU, but because board interface configuration was maxed out
4. Test results show device maximum performance, and are reached using mentioned hardware and software configuration, different configurations most likely will result in lower results

Noc Router

Mikrotik 2001UiAS-RM

Model	RB2011iL	RB2011UiAS
CPU	Atheros AR9344 600MHz	
Memory	64MB DDR SDRAM onboard memory	128MB DDR SDRAM onboard memory
Ethernet	Five 10/100 Mbit Fast Ethernet ports with Auto-MDI/X Five 10/100/1000 Mbit Gigabit Ethernet ports with Auto-MDI/X	
Extras	Reset button, Reset jumper	
LEDs	Power, User, Ethernet activity	
Power input	Jack 8-28V DC; PoE in: 8-28V DC on Ether1 (Non 802.3af).	
Power output	500mA on Port 10	
Dimensions	Desktop:230x90x25mm Rackmount:443x92x44mm	
Power consumption	8W max	15W max
Operating System	MikroTik RouterOS, L4 license	MikroTik RouterOS, L5 license
Package includes	RB2011, power supply, screw set, rack ears	

Feature / Model	2011iL-IN	2011iL-RM	2011iLS-IN	2011UiAS-IN	2011UiAS-RM
Enclosure	Desktop	Rackmount	Desktop	Desktop	Rackmount
SFP port	-	-	Yes	Yes	Yes
Power output	on port 10	on port 10	on port 10	on port 10	on port 10
USB	-	-	-	Yes	Yes

Switch Borde 01 – Switch Borde 02 - Switch Core 01 – Switch Core 02

Mikrotik CRS326-24S+2Q+RM

MikroTik CRS326-24S+2Q+RM

CRS326-24S+2Q+RM

Our fastest switch for the most demanding setups

If you are working with substantial amount of data – like providing Internet access or maintaining a huge data center – this is the perfect upgrade for your setup. **CRS326-24S+2Q+RM** is our first product with 40 Gbps QSFP+ ports for remarkably fast and stable fiber connection.

Overall it has two 40 Gbps QSFP+ ports and twenty four 10 Gbps SFP+ ports, which provides total non-blocking throughput of 320 Gbps and switching capacity of 640 Gbps with forwarding rate of 252 Mpps with most common packets.

CRS326-24S+2Q+RM is easy to manage – it has a full size USB port for configuration and dual power supply for redundancy – no unexpected downtime, your clients and colleagues will be thankful!

You can choose between our legendary feature-packed RouterOS for booting or a simpler, but still powerful SwOS. If you would like the ability to use routing and other Layer 3 features in your CRS, use RouterOS.

This device is great for new or existing networks – we have developed an assortment of accessories that will help you unleash the full potential of this switch in any setup. **CRS326-24S+2Q+RM – a professional's choice!**

CRS326-24S-2Q+RM 1

Specifications

Product code	CRS326-24S+2Q+RM
CPU	QCA9531, 650 MHz
Size of RAM	64 MB
Storage	16 MB flash
10/100 Ethernet ports	1
10G SFP+ ports	24
40G QSFP+ ports	2
Supported input voltage	AC power supply 100 - 240 V
Redundant supply	Yes
USB port	USB type A
Serial port	RJ45
Dimensions	443 x 200 x 44 mm
Operating temperature	-20°C .. +60°C
Operating system	RouterOS or SwitchOS, License level 5
Max power consumption	69 W

Included parts

2 IEC cords

Screw and feet kit (K10)

Rack ears

Switching test results

QCA9531 CRS326-24S+2Q		RouterOS v6.45					
Mode	Configuration	1518 byte		512 byte		64 byte	
		kpps	Gbps	kpps	Gbps	kpps	Gbps
Switching	Non blocking Layer 2 throughput	26007,8	315,838	75187,5	307,968	240652	123,214
Switching	Non blocking Layer 2 capacity	26007,8	631,677	75187,5	615,936	240652	246,428
Switching	Non blocking Layer 1 throughput	26007,8	320	75187,5	320	240652	161,718
Switching	Non blocking Layer 1 capacity	26007,8	640	75187,5	640	240652	323,436

Like other CRS products, **CRS326-24S+2Q+RM** comes with a decent built-in CPU, that can utilize all RouterOS features, but with some performance restrictions (indicated in table below).

CPU Layer 3 performance results

QCA9531 CRS326-24S+2Q		RouterOS v6.45					
Mode	Configuration	1518 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Bridging	none (fast path)	37,3	453,0	82,2	336,7	184,3	94,4
Bridging	25 bridge filter rules	37,1	450,5	47,6	195,0	50,2	25,7
Routing	none (fast path)	37,6	456,6	69,0	282,6	94,1	48,2
Routing	25 simple queues	37,2	451,8	56,5	231,4	66,3	33,9
Routing	25 ip filter rules	26,7	324,2	29,4	120,4	30,9	15,8

Switch Service 01 – Switch Service 02

Mikrotik CRS328-4C-20S-4S+RM

MikroTik CRS328-4C-20S-4S+RM

CRS328-4C-20S-4S+RM

The CRS328-4C-20S-4S+RM is a 28 independent port switch with a combo group.

This device has twenty SFP ports, four SFP+ ports for 10G modules and four combo ports, where you can choose to use SFP or RJ45 ports from the combo group. These ports can also be software selected, so if you have plugged in all eight cables, you can use scripting, to decide which four combo ports will be active.

The device comes in a 1U rackmount case with two 100-240 V power supplies with failover functionality. A RJ45 console port is available for management and debugging, and a mode button can be customised to execute any RouterOS commands.

The device has a "Dual boot" feature that allows you to choose between two operating systems - RouterOS or SwOS.

If you prefer to have a simplified operating system with only switch specific features, use SwOS. If you would like the ability to use routing and other Layer 3 features in your CRS, use RouterOS. You can select the desired operating system from RouterOS, from SwOS or from the RouterBOOT loader settings. All the feature set comes with our disruptive price, providing best price/performance on the market.

Switching features

- Non-blocking Layer 2 switching capacity
- 16K host table
- IEEE 802.1Q VLAN
- Supports up to 4K simultaneous VLANs
- Port isolation
- Port security
- Broadcast storm control
- Port mirroring of ingress/egress traffic
- STP / RSTP / MSTP
- Access Control List
- MikroTik neighbor discovery
- SNMP
- 10218-byte jumbo frames support
- IGMP snooping
- IEEE 802.3ad and static link aggregation

Quick specifications

- 20 SFP ports
- 4 ETH/SFP combo ports
- 4 SFP+ ports
- Non-Blocking throughput: 64 Gbps
- Switching capacity: 128 Gbps
- Forwarding rate: 95.2 Mpps
- RJ45 serial console port
- Dual PSU
- Maximum power consumption: 43 W
- Temperature based fan control
- 1U rackmount

CRS328-4C-20S-4S+RM 1

MikroTik CRS328-4C-20S-4S+RM

Specifications

Product code	CRS328-4C-20S-4S+RM
CPU	98DX3236A1 800 MHz
RAM	512 MB
Storage type	Flash
Storage size	16 MB
Switch chip model	98DX3236A1
SFP cages	20
SFP+ cages	4
Ethernet/SFP Combo ports	4
Operating system	SwOS / RouterOS (Dual boot)
Supported input voltage	100 - 240 V
Dimensions	443 x 194 x 44 mm
Operating temperature	-20°C .. +60°C tested
Max power consumption	43 W
Serial port	RJ45
License level	5

Two IEC power cords

Rack ears

Anexo Nro 2: Configuración de equipos

Router Municipalidad

```
/interface bridge
add name=Loopback
add name=Red_Municipalidad
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=10.1.0.1
/routing ospf-v3 instance
set [ find default=yes ] router-id=10.1.0.1
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/IPv6 settings
set accept-router-advertisements=no
/interface list member
add interface=ether1 list=Admin
/IP address
add address=10.1.0.1 interface=Loopback network=10.1.0.3
add address=10.1.1.1/30 interface=ether2 network=10.1.1.0
add address=10.1.1.5/30 interface=ether3 network=10.1.1.4
add address=10.1.2.1/24 interface=Red_Municipalidad network=10.1.2.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/IPv6 address
add address=2001:db8:1000::1 advertise=no interface=ether2
add address=2001:db8:1000:1::1 advertise=no interface=ether3
add address=2001:db8:1001::1 advertise=no interface=Red_Municipalidad
/routing ospf interface
add interface=ether3 network-type=point-to-point
add cost=9 interface=ether2 network-type=point-to-point
add interface=Red_Municipalidad network-type=point-to-point
/routing ospf network
add area=backbone network=10.1.1.4/30
add area=backbone network=10.1.1.0/30
add area=backbone network=10.1.2.0/24
```

```
/routing ospf-v3 interface
add area=backbone interface=ether3 network-type=point-to-point
add area=backbone cost=9 interface=ether2 network-type=point-to-point
add area=backbone interface=Red_Municipalidad
/system identity
set name=Municipalidad
/tool mac-server
set allowed-interface-list=none
```

Router Comisaría 01

```
/interface bridge
add name=Comisaría
add name=Loopback
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=10.2.0.1
/routing ospf-v3 instance
set [ find default=yes ] router-id=10.2.0.1
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/IPv6 settings
set accept-router-advertisements=no
/interface list member
add interface=ether1 list=Admin
/IP address
add address=10.2.0.1 interface=Loopback network=10.2.0.3
add address=10.2.1.1/30 interface=ether2 network=10.2.1.0
add address=10.2.1.5/30 interface=ether3 network=10.2.1.4
add address=10.2.2.1/24 interface=Comisaría network=10.2.2.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/IPv6 address
add address=2001:cafe::1 advertise=no interface=ether2
add address=2001:cafe:0:1::1 advertise=no interface=ether3
add address=2001:cafe:1::1 advertise=no interface=Comisaría
```

```
/routing ospf interface
add cost=9 interface=ether2 network-type=point-to-point
add interface=ether3 network-type=point-to-point
add interface=Comisaría network-type=point-to-point
/routing ospf network
add area=backbone network=10.2.1.0/30
add area=backbone network=10.2.1.4/30
add area=backbone network=10.2.2.0/24
/routing ospf-v3 interface
add area=backbone cost=9 interface=ether2 network-type=point-to-point
add area=backbone interface=ether3 network-type=point-to-point
add area=backbone interface=Comisaría
/system identity
set name=Comisaría01
/tool mac-server
set allowed-interface-list=none
```

Comisaría 02

```
/interface bridge
add name=Comisaría02
add name=Loopback
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=10.3.0.1
/routing ospf-v3 instance
set [ find default=yes ] router-id=10.3.0.1
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/IPv6 settings
```

```
set accept-router-advertisements=no
/interface list member
add interface=ether1 list=Admin
/IP address
add address=10.3.0.1 interface=Loopback network=10.3.0.3
add address=10.3.1.1/30 interface=ether2 network=10.3.1.0
add address=10.3.1.5/30 interface=ether3 network=10.3.1.4
add address=10.3.2.1/24 interface=Comisaría02 network=10.3.2.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/IPv6 address
add address=2001:cafe:1000::1 advertise=no interface=ether2
add address=2001:cafe:1000:1::1 advertise=no interface=ether3
add address=2001:cafe:1001::1 advertise=no interface=Comisaría02
/routing ospf interface
add cost=9 interface=ether2 network-type=point-to-point
add interface=ether3 network-type=point-to-point
/routing ospf network
add area=backbone network=10.3.1.0/30
add area=backbone network=10.3.1.4/30
add area=backbone network=10.3.2.0/24
/routing ospf-v3 interface
add area=backbone cost=9 interface=ether2 network-type=point-to-point
add area=backbone interface=ether3 network-type=point-to-point
add area=backbone interface=Comisaría02
/system identity
set name=Comisaría02
```

```
/tool mac-server
set allowed-interface-list=none
```

Router Borde 01

```
/interface bridge
add name=Loopback
/interface vlan
add interface=ether2 name=vlan3 vlan-id=3
add interface=ether2 name=vlan4 vlan-id=4
add interface=ether2 name=vlan6 vlan-id=6
add interface=ether2 name=vlan100 vlan-id=100
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=20 client-to-client-reflection=no name=Muni_Borde_Router01 \
    redistribute-ospf=yes router-id=10.1.0.2
/routing ospf instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.1.0.2
/routing ospf-v3 instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.1.0.2
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/IPv6 settings
set accept-router-advertisements=no
/interface list member
add interface=ether1 list=Admin
/IP address
add address=10.10.10.6/24 interface=vlan100 network=10.10.10.0
add address=10.1.0.2 interface=Loopback network=10.1.0.1
add address=10.1.1.2/30 interface=ether3 network=10.1.1.0
add address=192.168.1.2/24 interface=vlan3 network=192.168.1.0
add address=192.168.2.2/24 interface=vlan6 network=192.168.2.0
/IP service
set telnet disabled=yes
set ssh port=2022
```

```
set WinBox port=8296
/IPv6 address
add address=2001:db8:1::2:1 advertise=no interface=vlan4
add address=2001:db8::2:1 advertise=no interface=vlan100
add address=2001:db8:1000::2 advertise=no interface=ether3
add address=2001:db8:1:2::2 advertise=no interface=vlan6
/routing bgp peer
add in-filter=Principal instance=Muni_Borde_Router01 name=Comisaría01_BR03 \
    out-filter=Out remote-address=10.10.10.8 remote-as=30 use-bfd=yes
add in-filter=Principal instance=Muni_Borde_Router01 name=Comisaría02_BR05 \
    out-filter=Out remote-address=10.10.10.10 remote-as=40 use-bfd=yes
add in-filter=Backup instance=Muni_Borde_Router01 name=Comisaría01_BR04 \
    out-filter=Out remote-address=10.10.10.9 remote-as=30 use-bfd=yes
add in-filter=Backup instance=Muni_Borde_Router01 name=Comisaría02_BR06 \
    out-filter=Out remote-address=10.10.10.11 remote-as=40 use-bfd=yes
add in-filter=Service3 instance=Muni_Borde_Router01 name=Service3 out-filter=\
    Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Muni_Borde_Router01 \
    name=Comisaría01_BR03_IPv6 out-filter=OutIv6 remote-address=2001:db8::3:1 \
    remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Muni_Borde_Router01 \
    name=Comisaría02_BR05_IPv6 out-filter=OutIv6 remote-address=2001:db8::4:1 \
    remote-as=40 use-bfd=yes
add address-families=IPv6 in-filter=Backup instance=Muni_Borde_Router01 name=\
    Comisaría01_BR04_IPv6 out-filter=OutIv6 remote-address=2001:db8::3:2 \
    remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Backup instance=Muni_Borde_Router01 name=\
    Comisaría02_BR06_IPv6 out-filter=OutIv6 remote-address=2001:db8::4:2 \
    remote-as=40 use-bfd=yes
add address-families=IPv6 in-filter=Service4 instance=Muni_Borde_Router01 \
    name=Service4 out-filter=OutIv6 remote-address=2001:db8:1::1:1 remote-as=\
    50 use-bfd=yes
add in-filter=Service3_Bckp instance=Muni_Borde_Router01 name=Service3_Bckp \
    out-filter=Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Service4_Bckp instance=\
    Muni_Borde_Router01 name=Service4_Bckp out-filter=OutIv6 remote-address=\
    2001:db8:1:2::1 remote-as=50 use-bfd=yes
/routing filter
add action=accept chain=Out prefix=10.1.2.0/24
add action=discard chain=Out
add action=accept chain=Principal prefix=10.2.2.0/24
add action=accept chain=Principal prefix=10.3.2.0/24
add action=accept chain=Principal prefix=192.168.50.0/24
add action=accept chain=Principal prefix=2001:db8:1:1::/64
```

```
add action=accept chain=Principal prefix=2001:cafe:1::/64
add action=accept chain=Principal prefix=2001:cafe:1001::/64
add action=discard chain=Principal
add action=accept chain=Backup prefix=10.2.2.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=10.3.2.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:cafe:1::/64 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:cafe:1001::/64 set-bgp-local-pref=\
   3
add action=discard chain=Backup set-bgp-local-pref=3
add action=accept chain=OutIv6 prefix=2001:db8:1001::/64
add action=discard chain=OutIv6
add action=accept chain=Service3 prefix=192.168.50.0/24
add action=discard chain=Service3
add action=accept chain=Service4 prefix=2001:db8:1:1::/64
add action=discard chain=Service4
add action=accept chain=Service3_Bckp prefix=192.168.50.0/24 \
   set-bgp-local-pref=3
add action=discard chain=Service3_Bckp set-bgp-local-pref=3
add action=accept chain=Service4_Bckp prefix=2001:db8:1:1::/64 \
   set-bgp-local-pref=3
add action=discard chain=Service4_Bckp set-bgp-local-pref=3
/routing ospf interface
add interface=ether3 network-type=point-to-point
/routing ospf network
add area=backbone network=10.1.1.0/30
/routing ospf-v3 interface
add area=backbone interface=ether3 network-type=point-to-point
/system identity
set name=Borde_Router01
/tool mac-server
set allowed-interface-list=none
```

Router Borde 02

```
/interface bridge
add name=Loopback
add name=Trunk
/interface vlan
add interface=Trunk name=vlan3 vlan-id=3
add interface=Trunk name=vlan4 vlan-id=4
add interface=Trunk name=vlan6 vlan-id=6
```

```
add interface=Trunk name=vlan100 vlan-id=100
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=20 client-to-client-reflection=no name=Municipalidad_Backup \
    redistribute-ospf=yes router-id=10.1.0.3
/routing ospf instance
set [ find default=yes ] redistribute-bgp=as-type-2 router-id=10.1.0.3
/routing ospf-v3 instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.1.0.3
/interface bridge port
add bridge=Trunk interface=ether2
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/IPv6 settings
set accept-router-advertisements=no
/interface list member
add interface=ether1 list=Admin
/IP address
add address=10.10.10.7/24 interface=vlan100 network=10.10.10.0
add address=10.1.0.3 interface=Loopback network=10.1.0.2
add address=10.1.1.6/30 interface=ether3 network=10.1.1.4
add address=192.168.1.3/24 interface=vlan3 network=192.168.1.0
add address=192.168.2.3/24 interface=vlan6 network=192.168.2.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/IPv6 address
add address=2001:db8:1::2:2 advertise=no interface=vlan4
add address=2001:db8::2:2 advertise=no interface=vlan100
add address=2001:db8:1000:1::2 advertise=no interface=ether3
add address=2001:db8:1:2::3 advertise=no interface=vlan6
/routing bgp peer
add in-filter=Backup instance=Municipalidad_Backup name=Route_Server \
    out-filter=Out remote-address=10.10.10.2 remote-as=50 tcp-md5-key=@qp-IXP \
    use-bfd=yes
add in-filter=Principal instance=Municipalidad_Backup name=Comisaría1_BR03 \
    out-filter=Out remote-address=10.10.10.8 remote-as=30 use-bfd=yes
```

```
add in-filter=Principal instance=Municipalidad_Backup name=Comisaría2_BR05 \
    out-filter=Out remote-address=10.10.10.10 remote-as=40 use-bfd=yes
add address-families=IPv6 in-filter=Backup instance=Municipalidad_Backup \
    name=Route_Server_IPv6 out-filter=OutIv6 remote-address=2001:db8::1:2 \
    remote-as=50 tcp-md5-key=@qp-IXP use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Municipalidad_Backup \
    name=Comisaría1_BR03_IPv6 out-filter=OutIv6 remote-address=2001:db8::3:1 \
    remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Municipalidad_Backup \
    name=Comisaría2_BR05_IPv6 out-filter=OutIv6 remote-address=2001:db8::4:1 \
    remote-as=40 use-bfd=yes
add in-filter=Service3 instance=Municipalidad_Backup name=Service3 \
    out-filter=Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Service4 instance=Municipalidad_Backup \
    name=Service4 out-filter=OutIv6 remote-address=2001:db8:1:2::1 remote-as=\
    50 use-bfd=yes
add in-filter=Service3_Bkp instance=Municipalidad_Backup name=Service3_Bckp \
    out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Service4_Bkp instance=\
    Municipalidad_Backup name=Service4_Bckp out-filter=OutIv6 remote-address=\
    2001:db8:1::1:1 remote-as=50 use-bfd=yes
/routing filter
add action=accept chain=Out prefix=10.1.2.0/24
add action=discard chain=Out
add action=accept chain=Principal prefix=10.2.2.0/24
add action=accept chain=Principal prefix=10.3.2.0/24
add action=accept chain=Principal prefix=192.168.50.0/24
add action=accept chain=Principal prefix=2001:db8:1:1::/64
add action=accept chain=Principal prefix=2001:cafe:1::/64
add action=accept chain=Principal prefix=2001:cafe:1001::/64
add action=discard chain=Principal
add action=accept chain=Backup prefix=10.2.2.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=10.3.2.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:cafe:1::/64 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:cafe:1001::/64 set-bgp-local-pref=\
    3
add action=discard chain=Backup set-bgp-local-pref=3
add action=accept chain=OutIv6 prefix=2001:db8:1001::/64
add action=discard chain=OutIv6
add action=accept chain=Service3 prefix=192.168.50.0/24
add action=discard chain=Service3
add action=accept chain=Service4 prefix=2001:db8:1:1::/64
```

```
add action=discard chain=Service4
add action=accept chain=Service3_Bkp prefix=192.168.50.0/24 \
   set-bgp-local-pref=3
add action=discard chain=Service3_Bkp set-bgp-local-pref=3
add action=accept chain=Service4_Bkp prefix=2001:db8:1:1::/64 \
   set-bgp-local-pref=3
add action=discard chain=Service4_Bkp set-bgp-local-pref=3
/routing ospf interface
add interface=ether3 network-type=point-to-point
/routing ospf network
add area=backbone network=10.1.1.4/30
/routing ospf-v3 interface
add area=backbone interface=ether3 network-type=point-to-point
/system identity
set name=Borde_Router02
/tool mac-server
set allowed-interface-list=none
```

Router Borde 03

```
/interface bridge
add name=LoopBack
add name=Trunk
/interface vlan
add interface=Trunk name=vlan3 vlan-id=3
add interface=Trunk name=vlan4 vlan-id=4
add interface=Trunk name=vlan6 vlan-id=6
add interface=Trunk name=vlan100 vlan-id=100
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=30 client-to-client-reflection=no name=Comi_Borde_Router03 \
   redistribute-ospf=yes router-id=10.2.0.2
/routing ospf instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.2.0.2
/routing ospf-v3 instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.2.0.2
/interface bridge port
add bridge=Trunk interface=ether2
/IP neighbor discovery-settings
```

```
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/IPv6 settings
set accept-router-advertisements=no
/interface list member
add interface=ether1 list=Admin
/IP address
add address=10.10.10.8/24 interface=vlan100 network=10.10.10.0
add address=10.2.0.2 interface=LoopBack network=10.2.0.1
add address=10.2.1.2/30 interface=ether3 network=10.2.1.0
add address=192.168.1.4/24 interface=vlan3 network=192.168.1.0
add address=192.168.2.4/24 interface=vlan6 network=192.168.2.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/IPv6 address
add address=2001:db8::3:1 advertise=no interface=vlan100
add address=2001:db8:1::3:1 advertise=no interface=vlan4
add address=2001:cafe::2 advertise=no interface=ether3
add address=2001:db8:1:2::4 advertise=no interface=vlan6
/routing bgp peer
add in-filter=Principal instance=Comi_Borde_Router03 name=Municipalidad_BR01 \
   out-filter=Out remote-address=10.10.10.6 remote-as=20 use-bfd=yes
add in-filter=Backup instance=Comi_Borde_Router03 name=MunicIPlaidad_BR02 \
   out-filter=Out remote-address=10.10.10.7 remote-as=20 use-bfd=yes
add in-filter=Principal instance=Comi_Borde_Router03 name=Comisaría2_BR05 \
   out-filter=Out remote-address=10.10.10.10 remote-as=40 use-bfd=yes
add in-filter=Backup instance=Comi_Borde_Router03 name=Comisaría2_BR06 \
   out-filter=Out remote-address=10.10.10.11 remote-as=40 use-bfd=yes
add in-filter=Service3 instance=Comi_Borde_Router03 name=Service3 out-filter=\
   Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Comi_Borde_Router03 \
   name=Municipalidad_BR01_IPv6 out-filter=OutIPv6 remote-address=\
   2001:db8::2:1 remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Backup instance=Comi_Borde_Router03 name=\
   MunicIPlaidad_BR02_IPv6 out-filter=OutIPv6 remote-address=2001:db8::2:2 \
   remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Comi_Borde_Router03 \
   name=Comisaría2_BR05_IPv6 out-filter=OutIPv6 remote-address=2001:db8::4:1 \
   remote-as=40 use-bfd=yes
add address-families=IPv6 in-filter=Backup instance=Comi_Borde_Router03 name=\
   Comisaría2_BR06_IPv6 out-filter=OutIPv6 remote-address=2001:db8::4:2 \
```

```
   remote-as=40 use-bfd=yes
add address-families=IPv6 in-filter=Service4 instance=Comi_Borde_Router03 \
   name=Service4 out-filter=OutIPv6 remote-address=2001:db8:1::1:1 \
   remote-as=50 use-bfd=yes
add in-filter=Service3_Bckp instance=Comi_Borde_Router03 name=Service3_Bckp \
   out-filter=Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Service4 instance=Comi_Borde_Router03 \
   name=Service4_Bckp out-filter=OutIPv6 remote-address=2001:db8:1:2::1 \
   remote-as=50 use-bfd=yes
/routing filter
add action=accept chain=Principal prefix=10.1.2.0/24
add action=accept chain=Principal prefix=10.3.2.0/24
add action=accept chain=Principal prefix=192.168.50.0/24
add action=accept chain=Principal prefix=2001:db8:1:1::/64
add action=accept chain=Principal prefix=2001:db8:1001::/64
add action=accept chain=Principal prefix=2001:cafe:1001::/64
add action=discard chain=Principal
add action=accept chain=Backup prefix=10.1.2.0/24 set-bgp-prepend=3
add action=accept chain=Backup prefix=10.3.2.0/24 set-bgp-prepend=3
add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-prepend=3
add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-prepend=3
add action=accept chain=Backup prefix=2001:db8:1001::/64 set-bgp-prepend=3
add action=accept chain=Backup prefix=2001:cafe:1001::/64 set-bgp-prepend=3
add action=discard chain=Backup set-bgp-prepend=3
add action=accept chain=Out prefix=10.2.2.0/24
add action=discard chain=Out
add action=accept chain=OutIPv6 prefix=2001:cafe:1::/64
add action=discard chain=OutIPv6
add action=accept chain=Service3 prefix=192.168.50.0/24
add action=discard chain=Service3
add action=accept chain=Service4 prefix=2001:db8:1:1::/64
add action=discard chain=Service4
add action=accept chain=Service3_Bckp prefix=192.168.50.0/24 \
   set-bgp-local-pref=3
add action=discard chain=Service3_Bckp set-bgp-local-pref=3
add action=accept chain=Service4_Bckp prefix=2001:db8:1:1::/64 \
   set-bgp-local-pref=3
add action=discard chain=Service4_Bckp set-bgp-local-pref=3
/routing ospf interface
add interface=ether3 network-type=point-to-point
/routing ospf network
add area=backbone network=10.2.1.0/30
/routing ospf-v3 interface
add area=backbone interface=ether3 network-type=point-to-point
```

```
/system identity
set name=Borde_Router03
/tool mac-server
set allowed-interface-list=none
```

Router Borde 04

```
/interface bridge
add name=Loopback
add name=Trunk
/interface vlan
add interface=Trunk name=vlan3 vlan-id=3
add interface=Trunk name=vlan4 vlan-id=4
add interface=Trunk name=vlan6 vlan-id=6
add interface=Trunk name=vlan100 vlan-id=100
/interface list
add exclude=static include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=30 client-to-client-reflection=no name=Comisaría01_Backup \
    redistribute-ospf=yes router-id=10.2.0.3
/routing ospf instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.2.0.3
/routing ospf-v3 instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.2.0.3
/interface bridge port
add bridge=Trunk interface=ether2
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/IPv6 settings
set accept-router-advertisements=no
/interface list member
add interface=ether1 list=Admin
/IP address
add address=10.10.10.9/24 interface=vlan100 network=10.10.10.0
add address=10.2.0.3 interface=Loopback network=10.2.0.2
add address=10.2.1.6/30 interface=ether3 network=10.2.1.4
add address=192.168.1.5/24 interface=vlan3 network=192.168.1.0
add address=192.168.2.5/24 interface=vlan6 network=192.168.2.0
```

```
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/IPv6 address
add address=2001:db8::3:2 advertise=no interface=vlan100
add address=2001:db8:1::3:2 advertise=no interface=vlan4
add address=2001:cafe:0:1::2 advertise=no interface=ether3
add address=2001:db8:1:2::5 advertise=no interface=vlan6
/routing bgp peer
add in-filter=Backup instance=Comisaría01_Backup name=Router_Server02 \
    out-filter=Out remote-address=10.10.10.2 remote-as=50 tcp-md5-key=@qp-IXP \
    use-bfd=yes
add in-filter=Principal instance=Comisaría01_Backup name=Municipalidad_BR01 \
    out-filter=Out remote-address=10.10.10.6 remote-as=20 use-bfd=yes
add in-filter=Principal instance=Comisaría01_Backup name=Comisaría2_BR05 \
    out-filter=Out remote-address=10.10.10.10 remote-as=40 use-bfd=yes
add in-filter=Service3_Bkp instance=Comisaría01_Backup name=Service3_Bckp \
    out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Backup instance=Comisaría01_Backup name=\
    Route_Server02_IPv6 out-filter=OutIPv6 remote-address=2001:db8::1:2 \
    remote-as=50 tcp-md5-key=@qp-IXP use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Comisaría01_Backup \
    name=Municipalidad_BR01_IPv6 out-filter=OutIPv6 remote-address=\
    2001:db8::2:1 remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Comisaría01_Backup \
    name=Comisaría2_BR05_IPv6 out-filter=OutIPv6 remote-address=2001:db8::4:1 \
    remote-as=40 use-bfd=yes
add address-families=IPv6 in-filter=Service4_Bkp instance=Comisaría01_Backup \
    name=Service4_Bckp out-filter=OutIPv6 remote-address=2001:db8:1::1:1 \
    remote-as=50 use-bfd=yes
add in-filter=Service3 instance=Comisaría01_Backup name=Service3 out-filter=\
    Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Service4 instance=Comisaría01_Backup \
    name=Service4 out-filter=OutIPv6 remote-address=2001:db8:1:2::1 \
    remote-as=50 use-bfd=yes
/routing filter
add action=accept chain=Principal prefix=10.1.2.0/24
add action=accept chain=Principal prefix=10.3.2.0/24
add action=accept chain=Principal prefix=192.168.50.0/24
add action=accept chain=Principal prefix=2001:db8:1:1::/64
add action=accept chain=Principal prefix=2001:db8:1001::/64
add action=accept chain=Principal prefix=2001:cafe:1001::/64
add action=discard chain=Principal
```

```
add action=accept chain=Backup prefix=10.1.2.0/24 set-bgp-prepend=3
add action=accept chain=Backup prefix=10.3.2.0/24 set-bgp-prepend=3
add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-prepend=3
add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-prepend=3
add action=accept chain=Backup prefix=2001:db8:1001::/64 set-bgp-prepend=3
add action=accept chain=Backup prefix=2001:cafe:1001::/64 set-bgp-prepend=3
add action=discard chain=Backup set-bgp-prepend=3
add action=accept chain=Out prefix=10.2.2.0/24
add action=discard chain=Out
add action=accept chain=OutIPv6 prefix=2001:cafe:1::/64
add action=discard chain=OutIPv6
add action=accept chain=Service3 prefix=192.168.50.0/24
add action=discard chain=Service3
add action=accept chain=Service4 prefix=2001:db8:1:1::/64
add action=discard chain=Service4
add action=accept chain=Service3_Bkp prefix=192.168.50.0/24 \
   set-bgp-local-pref=3
add action=discard chain=Service3_Bkp set-bgp-local-pref=3
add action=accept chain=Service4_Bkp prefix=2001:db8:1:1::/64 \
   set-bgp-local-pref=3
add action=discard chain=Service4_Bkp set-bgp-local-pref=3
/routing ospf interface
add interface=ether3 network-type=point-to-point
/routing ospf network
add area=backbone network=10.2.1.4/30
/routing ospf-v3 interface
add area=backbone interface=ether3 network-type=point-to-point
/system identity
set name=Borde_Router04
/tool mac-server
set allowed-interface-list=none
```

Router Borde 05

```
/interface bridge
add name=Loopback
add name=Trunk
/interface vlan
add interface=Trunk name=vlan3 vlan-id=3
add interface=Trunk name=vlan4 vlan-id=4
add interface=Trunk name=vlan6 vlan-id=6
add interface=Trunk name=vlan100 vlan-id=100
/interface list
```

```
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=40 client-to-client-reflection=no name=Comisaría_Borde_Router05 \
    redistribute-ospf=yes router-id=10.3.0.2
/routing ospf instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.3.0.2
/routing ospf-v3 instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.3.0.2
/interface bridge port
add bridge=Trunk interface=ether2
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IPv6 settings
set accept-router-advertisements=no
/interface list member
add interface=ether1 list=Admin
/IP address
add address=10.10.10.10/24 interface=vlan100 network=10.10.10.0
add address=10.3.0.2 interface=Loopback network=10.3.0.1
add address=10.3.1.2/30 interface=ether3 network=10.3.1.0
add address=192.168.1.6/24 interface=vlan3 network=192.168.1.0
add address=192.168.2.6/24 interface=vlan6 network=192.168.2.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/IPv6 address
add address=2001:db8::4:1 advertise=no interface=vlan100
add address=2001:db8:1::4:1 advertise=no interface=vlan4
add address=2001:cafe:1000::2 advertise=no interface=ether3
add address=2001:db8:1:2::6 advertise=no interface=vlan6
/routing bgp peer
add in-filter=Principal instance=Comisaría_Borde_Router05 name=\
    Municipalidad_BR01 out-filter=Out remote-address=10.10.10.6 remote-as=20 \
    use-bfd=yes
add in-filter=Principal instance=Comisaría_Borde_Router05 name=\
    Comisaría1_BR03 out-filter=Out remote-address=10.10.10.8 remote-as=30 \
    use-bfd=yes
add in-filter=Backup instance=Comisaría_Borde_Router05 name=\
    Municipalidad_BR02 out-filter=Out remote-address=10.10.10.7 remote-as=20 \
    use-bfd=yes
```

```
add in-filter=Backup instance=Comisaría_Borde_Router05 name=Comisaría1_BR04 \
    out-filter=Out remote-address=10.10.10.9 remote-as=30 use-bfd=yes
add in-filter=Service3 instance=Comisaría_Borde_Router05 name=Service3 \
    out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=\
    Comisaría_Borde_Router05 name=Municipalidad_BR01_IPv6 out-filter=OutIPv6 \
    remote-address=::::2:1 remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=\
    Comisaría_Borde_Router05 name=Comisaría1_BR03_Iv6 out-filter=OutIPv6 \
    remote-address=2001:db8::3:1 remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=\
    Comisaría_Borde_Router05 name=Comisaría1_BR04_IPv6 out-filter=OutIPv6 \
    remote-address=2001:db8::3:2 remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Backup instance=Comisaría_Borde_Router05 \
    name=Municipalidad_BR02_IPv6 out-filter=OutIPv6 remote-address=\
    2001:db8::2:2 remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Service4 instance=\
    Comisaría_Borde_Router05 name=Service4 out-filter=OutIPv6 remote-address=\
    2001:db8:1::1:1 remote-as=50 use-bfd=yes
add in-filter=Service3_Bckp instance=Comisaría_Borde_Router05 name=\
    Service3_Bckp out-filter=Out remote-address=192.168.2.1 remote-as=50 \
    use-bfd=yes
add address-families=IPv6 in-filter=Service4_Bckp instance=\
    Comisaría_Borde_Router05 name=Service4_Bckp out-filter=OutIPv6 \
    remote-address=2001:db8:1:2::1 remote-as=50 use-bfd=yes
/routing filter
add action=accept chain=Principal prefix=10.1.2.0/24
add action=accept chain=Principal prefix=10.2.2.0/24
add action=accept chain=Principal prefix=192.168.50.0/24
add action=accept chain=Principal prefix=2001:db8:1:1::/64
add action=accept chain=Principal prefix=2001:db8:1001::/64
add action=accept chain=Principal prefix=2001:cafe:1::/64
add action=accept chain=Backup prefix=10.1.2.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=10.2.2.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:db8:1001::/64 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:cafe:1::/64 set-bgp-local-pref=3
add action=accept chain=Out prefix=10.3.2.0/24
add action=discard chain=Out
add action=accept chain=OutIPv6 prefix=2001:cafe:1001::/64
add action=discard chain=OutIPv6
add action=accept chain=Service3 prefix=192.168.50.0/24
add action=discard chain=Service3
```

```
add action=accept chain=Service4 prefix=2001:db8:1:1::/64
add action=discard chain=Service4
add action=accept chain=Service3_Bckp prefix=192.168.50.0/24 \
   set-bgp-local-pref=3
add action=discard chain=Service3_Bckp set-bgp-local-pref=3
add action=accept chain=Service4_Bckp prefix=2001:db8:1:1::/64 \
   set-bgp-local-pref=3
add action=discard chain=Service4_Bckp set-bgp-local-pref=3
/routing ospf interface
add interface=ether3 network-type=point-to-point
/routing ospf network
add area=backbone network=10.3.1.0/30
/routing ospf-v3 interface
add area=backbone interface=ether3 network-type=point-to-point
/system identity
set name=Borde_Router05
/tool mac-server
set allowed-interface-list=none
```

Router Borde 06

```
/interface bridge
add name=Loopback
add name=Trunk
/interface vlan
add interface=Trunk name=vlan3 vlan-id=3
add interface=Trunk name=vlan4 vlan-id=4
add interface=Trunk name=vlan6 vlan-id=6
add interface=Trunk name=vlan100 vlan-id=100
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=40 client-to-client-reflection=no name=Comisaría02_Backup \
   redistribute-ospf=yes router-id=10.3.0.3
/routing ospf instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.3.1.3
/routing ospf-v3 instance
set [ find default=yes ] redistribute-bgp=as-type-1 router-id=10.3.1.3
/interface bridge port
add bridge=Trunk interface=ether2
```

```
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/IPv6 settings
set accept-router-advertisements=no
/interface list member
add interface=ether1 list=Admin
/IP address
add address=10.10.10.11/24 interface=vlan100 network=10.10.10.0
add address=10.3.0.3 interface=Loopback network=10.3.0.2
add address=10.3.1.6/30 interface=ether3 network=10.3.1.4
add address=192.168.1.7/24 interface=vlan3 network=192.168.1.0
add address=192.168.2.7/24 interface=vlan6 network=192.168.2.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/IPv6 address
add address=2001:db8:1::4:2 advertise=no interface=vlan4
add address=2001:db8::4:2 advertise=no interface=vlan100
add address=2001:cafe:1000:1::2 advertise=no interface=ether3
add address=2001:db8:1:2::7 advertise=no interface=vlan6
/routing bgp peer
add in-filter=Backup instance=Comisaría02_Backup name=Route_Server02 \
   out-filter=Out remote-address=10.10.10.2 remote-as=50 tcp-md5-key=@qp-IXP \
   use-bfd=yes
add in-filter=Principal instance=Comisaría02_Backup name=Municipalidad_BR01 \
   out-filter=Out remote-address=10.10.10.6 remote-as=20 use-bfd=yes
add in-filter=Principal instance=Comisaría02_Backup name=Comisaría1_BR03 \
   out-filter=Out remote-address=10.10.10.8 remote-as=30 use-bfd=yes
add in-filter=Service3_Bkp instance=Comisaría02_Backup name=Service3_Bckp \
   out-filter=Out remote-address=192.168.1.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Backup instance=Comisaría02_Backup name=\
   Route_Server_IPv6 out-filter=OutIPv6 remote-address=2001:db8::1:2 \
   remote-as=50 tcp-md5-key=@qp-IXP use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Comisaría02_Backup \
   name=Municipalidad_BR01_IPv6 out-filter=OutIPv6 remote-address=\
   2001:db8::2:1 remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Principal instance=Comisaría02_Backup \
   name=Comisaría1_BR03_IPv6 out-filter=OutIPv6 remote-address=2001:db8::3:1 \
   remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Service4_Bkp instance=Comisaría02_Backup \
   name=Service4_Bckp out-filter=OutIPv6 remote-address=2001:db8:1::1:1 \
```

```
   remote-as=50 use-bfd=yes
add in-filter=Service3 instance=Comisaría02_Backup name=Service3 out-filter=\
   Out remote-address=192.168.2.1 remote-as=50 use-bfd=yes
add address-families=IPv6 in-filter=Service4 instance=Comisaría02_Backup \
   name=Service4 out-filter=OutIPv6 remote-address=2001:db8:1:2::1 \
   remote-as=50 use-bfd=yes
/routing filter
add action=accept chain=Principal prefix=10.1.2.0/24
add action=accept chain=Principal prefix=10.2.2.0/24
add action=accept chain=Principal prefix=192.168.50.0/24
add action=accept chain=Principal prefix=2001:db8:1:1::/64
add action=accept chain=Principal prefix=2001:db8:1001::/64
add action=accept chain=Principal prefix=2001:cafe:1::/64
add action=accept chain=Backup prefix=10.1.2.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=10.2.2.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=192.168.50.0/24 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:db8:1:1::/64 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:db8:1001::/64 set-bgp-local-pref=3
add action=accept chain=Backup prefix=2001:cafe:1::/64 set-bgp-local-pref=3
add action=accept chain=Out prefix=10.3.2.0/24
add action=discard chain=Out
add action=accept chain=OutIPv6 prefix=2001:cafe:1001::/64
add action=discard chain=OutIPv6
add action=accept chain=Service3 prefix=192.168.50.0/24
add action=discard chain=Service3
add action=accept chain=Service4 prefix=2001:db8:1:1::/64
add action=discard chain=Service4
add action=accept chain=Service3_Bkp prefix=192.168.50.0/24 \
   set-bgp-local-pref=3
add action=discard chain=Service3_Bkp set-bgp-local-pref=3
add action=accept chain=Service4_Bkp prefix=2001:db8:1:1::/64 \
   set-bgp-local-pref=3
add action=discard chain=Service4_Bkp set-bgp-local-pref=3
/routing ospf interface
add interface=ether3 network-type=point-to-point
/routing ospf network
add area=backbone network=10.3.1.4/30
/routing ospf-v3 interface
add area=backbone interface=ether3 network-type=point-to-point
/system identity
set name=Borde_Router06
/tool mac-server
set allowed-interface-list=none
```

Router Server

enable

configure terminal

hostname Route_Server

username tesis privilege 15 password t2s1s21

line vty 0 4

privilege level 15

login local

transport input telnet

transport input telnet ssh

exit

interface FastEthernet0/0.100

encapsulation dot1q 100

IP address 10.10.10.2 255.255.255.0

IPv6 address 2001:db8::1:2/64

no shutdown

exit

interface FastEthernet0/0

no shutdown

exit

IPv6 Unicast-routing

router bgp 50

bgp log-neighbor-changes

neighbor IXP peer-group

neighbor IXP password @qp-IXP

neighbor 10.10.10.7 remote-as 20

neighbor 10.10.10.7 peer-group IXP

neighbor 10.10.10.9 remote-as 30

neighbor 10.10.10.9 peer-group IXP

neighbor 10.10.10.11 remote-as 40

neighbor 10.10.10.11 peer-group IXP

address-family IPv4

exit

exit

router bgp 50

bgp log-neighbor-changes

neighbor 1xp peer-group

neighbor 1xp password @qp-IXP

neighbor 2001:db8::2:2 remote-as 20

neighbor 2001:db8::2:2 peer-group 1xp

neighbor 2001:db8::3:2 remote-as 30

neighbor 2001:db8::3:2 peer-group 1xp

neighbor 2001:db8::4:2 remote-as 40

neighbor 2001:db8::4:2 peer-group 1xp

address-family IPv6

neighbor 2001:db8::2:2 activate

neighbor 2001:db8::3:2 activate

neighbor 2001:db8::4:2 activate

exit

Switch Borde 01

/interface bridge
add name=Trunk priority=0x4000
/interface vlan
add interface=Trunk name=vlan5 vlan-id=5
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [find default=yes] supplicant-identity=MikroTik
/interface bridge filter
add action=drop chain=forward disabled=yes in-bridge=Trunk in-interface=\

```
    ether3 src-mac-address=!50:DA:D7:00:01:01/FF:FF:FF:FF:FF:FF
/interface bridge port
add bridge=Trunk interface=ether3
add bridge=Trunk interface=ether4
add bridge=Trunk interface=ether5
add bridge=Trunk interface=ether6 pvid=100
add bridge=Trunk interface=ether7 path-cost=15
add bridge=Trunk interface=ether1
add bridge=Trunk interface=ether2 path-cost=15
/IP neighbor discovery-settings
set discover-interface-list=Admin
/interface list member
add interface=ether8 list=Admin
/IP address
add address=11.11.11.4/24 interface=vlan5 network=11.11.11.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/system identity
set name=Sw_Borde01
/tool mac-server
set allowed-interface-list=none
```

Switch Borde 02

```
/interface bridge
add name=Trunk priority=0x5000
/interface vlan
add interface=Trunk name=vlan5 vlan-id=5
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge filter
add action=drop chain=forward disabled=yes in-bridge=Trunk in-interface=\
    ether3 src-mac-address=!50:DA:D7:00:01:01/FF:FF:FF:FF:FF:FF
/interface bridge port
add bridge=Trunk interface=ether3
add bridge=Trunk interface=ether4
add bridge=Trunk interface=ether5
add bridge=Trunk interface=ether6 pvid=100
add bridge=Trunk interface=ether7 path-cost=15
```

```
add bridge=Trunk interface=ether1
add bridge=Trunk interface=ether2
/IP neighbor discovery-settings
set discover-interface-list=Admin
/interface list member
add interface=ether8 list=Admin
/IP address
add address=11.11.11.5/24 interface=vlan5 network=11.11.11.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/system identity
set name=Sw_Borde02
/tool mac-server
set allowed-interface-list=none
```

Switch Core 01

```
/interface bridge
add name=Trunk priority=0x1000
/interface vlan
add interface=Trunk name=vlan5 vlan-id=5
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=Trunk interface=ether3
add bridge=Trunk interface=ether4
add bridge=Trunk interface=ether2
add bridge=Trunk interface=ether1
add bridge=Trunk interface=ether5
/IP neighbor discovery-settings
set discover-interface-list=Admin
/interface list member
add interface=ether6 list=Admin
/IP address
add address=11.11.11.2/24 interface=vlan5 network=11.11.11.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
```

```
/system identity
set name=Sw_Core01
/tool mac-server
set allowed-interface-list=none
```

Switch Core 02

```
/interface bridge
add name=Trunk priority=0x2000
/interface vlan
add interface=Trunk name=vlan5 vlan-id=5
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=Trunk interface=ether3 path-cost=30
add bridge=Trunk interface=ether4
add bridge=Trunk interface=ether1 path-cost=15
add bridge=Trunk interface=ether2
add bridge=Trunk interface=ether5
/IP neighbor discovery-settings
set discover-interface-list=Admin
/interface list member
add interface=ether6 list=Admin
/IP address
add address=11.11.11.3/24 interface=vlan5 network=11.11.11.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/system identity
set name=Sw_Core02
/tool mac-server
set allowed-interface-list=none
```

Switch Service 01

```
/interface bridge
add name=Trunk priority=0x6000
/interface vlan
add interface=Trunk name=vlan5 vlan-id=5
/interface list
```

```
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=Trunk interface=ether1
add bridge=Trunk interface=ether3
add bridge=Trunk interface=ether4
add bridge=Trunk interface=ether2 path-cost=30
/IP neighbor discovery-settings
set discover-interface-list=Admin
/interface list member
add interface=ether6 list=Admin
/IP address
add address=11.11.11.6/24 interface=vlan5 network=11.11.11.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/system identity
set name=Sw_Service01
/tool mac-server
set allowed-interface-list=none
```

Switch Service 02

```
/interface bridge
add name=Trunk priority=0x7000
/interface vlan
add interface=Trunk name=vlan5 vlan-id=5
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=Mikrotik
/interface bridge port
add bridge=Trunk interface=ether1
add bridge=Trunk interface=ether2
add bridge=Trunk interface=ether3 path-cost=50
add bridge=Trunk interface=ether4
/IP neighbor discovery-settings
set discover-interface-list=Admin
/interface list member
add interface=ether6 list=Admin
/IP address
```

```
add address=11.11.11.7/24 interface=vlan5 network=11.11.11.0
add disabled=no interface=ether1
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/system identity
set name=Sw_Service02
/tool mac-server
set allowed-interface-list=none
```

Router Service 3

```
/interface bridge
add name=Loopback
add name=Trunk
/interface vlan
add interface=Trunk name=vlan3 vlan-id=3
add interface=Trunk name=vlan5 vlan-id=5
add interface=ether3 name=vlan6 vlan-id=6
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=50 client-to-client-reflection=no name=Service3 router-id=10.10.9.2
/interface bridge port
add bridge=Trunk interface=ether1 path-cost=1
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/interface list member
add interface=ether4 list=Admin
/IP address
add address=192.168.1.1/24 interface=vlan3 network=192.168.1.0
add address=192.168.50.1/24 interface=ether2 network=192.168.50.0
add address=10.10.9.2 interface=Loopback network=10.10.9.2
add address=11.11.11.8/24 interface=vlan5 network=11.11.11.0
add address=192.168.2.1/24 interface=vlan6 network=192.168.2.0
/IP service
set telnet disabled=yes
```

```
set ssh port=2022
set WinBox port=8296
/routing bgp network
add network=192.168.50.0/24 synchronize=no
/routing bgp peer
add in-filter=Muni_Principal instance=Service3 name=Municipalidad_BR01 \
    out-filter=Out remote-address=192.168.1.2 remote-as=20 use-bfd=yes
add in-filter=Comisaría1_Principal instance=Service3 name=Comisaría1_BR03 \
    out-filter=Out remote-address=192.168.1.4 remote-as=30 use-bfd=yes
add in-filter=Comisaría1_Bckp instance=Service3 name=Comisaría1_BR04_Bckp \
    out-filter=Out remote-address=192.168.1.5 remote-as=30 use-bfd=yes
add in-filter=Comisaría2_Principal instance=Service3 name=Comisaría2_BR05 \
    out-filter=Out remote-address=192.168.1.6 remote-as=40 use-bfd=yes
add in-filter=Comisaría2_Bckp instance=Service3 name=Comisaría2_BR06_Bckp \
    out-filter=Out remote-address=192.168.1.7 remote-as=40 use-bfd=yes
add hold-time=5s in-filter=Muni_Backup instance=Service3 name=\
    Municipalidad_BR02 out-filter=Out remote-address=192.168.2.3 remote-as=20 \
    use-bfd=yes
add in-filter=Muni_Principal instance=Service3 name=Municipalidad_BR01_Bckp \
    out-filter=Out remote-address=192.168.2.2 remote-as=20 use-bfd=yes
add hold-time=5s in-filter=Muni_Backup instance=Service3 name=\
    Municipalidad_BR02_Bckp out-filter=Out remote-address=192.168.1.3 \
    remote-as=20 use-bfd=yes
add in-filter=Comisaría1_Bckp instance=Service3 name=Comisaría1_BR03_Bckp \
    out-filter=Out remote-address=192.168.2.4 remote-as=30 use-bfd=yes
add in-filter=Comisaría1_Principal instance=Service3 name=Comisaría1_BR04 \
    out-filter=Out remote-address=192.168.2.5 remote-as=30 use-bfd=yes
add in-filter=Comisaría2_Bckp instance=Service3 name=Comisaría2_BR05_Bckp \
    out-filter=Out remote-address=192.168.2.6 remote-as=40 use-bfd=yes
add in-filter=Comisaría2_Principal instance=Service3 name=Comisaría2_BR06 \
    out-filter=Out remote-address=192.168.2.7 remote-as=40 use-bfd=yes
/routing filter
add action=accept chain=Muni_Principal prefix=10.1.2.0/24
add action=discard chain=Muni_Principal
add action=accept chain=Muni_Backup prefix=10.1.2.0/24 set-bgp-local-pref=3
add action=discard chain=Muni_Backup set-bgp-local-pref=3
add action=accept chain=Out prefix=192.168.50.0/24
add action=discard chain=Out
add action=accept chain=Comisaría1_Principal prefix=10.2.2.0/24
add action=discard chain=Comisaría1_Principal
add action=accept chain=Comisaría1_Bckp prefix=10.2.2.0/24 \
    set-bgp-local-pref=3
add action=discard chain=Comisaría1_Bckp set-bgp-local-pref=3
add action=accept chain=Comisaría2_Principal prefix=10.3.2.0/24
```

```
add action=discard chain=Comisaría2_Principal
add action=accept chain=Comisaría2_Bckp prefix=10.3.2.0/24 \
   set-bgp-local-pref=3
add action=discard chain=Comisaría2_Bckp set-bgp-local-pref=3
/system identity
set name="Router Service 3"
/tool mac-server
set allowed-interface-list=none
```

Router Service 4

```
/interface bridge
add name=Loopback
add name=Service
/interface vlan
add interface=ether3 name=vlan4 vlan-id=4
add interface=ether1 name=vlan5 vlan-id=5
add interface=ether1 name=vlan6 vlan-id=6
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=50 client-to-client-reflection=no name=Service4 router-id=10.1.0.254
/IP neighbor discovery-settings
set discover-interface-list=Admin
/IP settings
set arp-timeout=4h
/IPv6 settings
set accept-router-advertisements=yes
/interface list member
add interface=ether4 list=Admin
/IP address
add address=10.1.0.254 interface=Loopback network=10.1.0.254
add address=11.11.11.9/24 interface=vlan5 network=11.11.11.0
add address=1.1.1.1 interface=ether3 network=1.1.1.1
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/IPv6 address
add address=2001:db8:1::1:1 advertise=no interface=vlan4
```

```
add address=2001:db8:1:1::1 interface=ether2
add address=2001:db8:1:2::1 advertise=no interface=vlan6
/IPv6 nd
set [ find default=yes ] advertise-dns=no advertise-mac-address=no disabled=\
    yes other-configuration=yes
add interface=ether2 managed-address-configuration=yes other-configuration=\
    yes
/routing bgp network
add network=2001:db8:1:1::/64 synchronize=no
/routing bgp peer
add address-families=IPv6 in-filter=Muni_Principal instance=Service4 name=\
    Municipalidad_BR01 out-filter=Out remote-address=2001:db8:1::2:1 \
    remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Comisaría1_Principal instance=Service4 \
    name=Comisaría1_BR03 out-filter=Out remote-address=2001:db8:1::3:1 \
    remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Comisaría1_Bckp instance=Service4 name=\
    Comisaría1_BB04_Bckp out-filter=Out remote-address=2001:db8:1::3:2 \
    remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Comisaría2_Principal instance=Service4 \
    name=Comisaría2_BR05 out-filter=Out remote-address=2001:db8:1::4:1 \
    remote-as=40 use-bfd=yes
add address-families=IPv6 in-filter=Comisaría2_Principal instance=Service4 \
    name=Comisaría2_BR06 out-filter=Out remote-address=2001:db8:1::4:2 \
    remote-as=40 use-bfd=yes
add address-families=IPv6 in-filter=Muni_Backup instance=Service4 name=\
    Municipalidad_BR02_Bckp out-filter=Out remote-address=2001:db8:1:2::3 \
    remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Muni_Principal instance=Service4 name=\
    Municipalidad_BR02 out-filter=Out remote-address=2001:db8:1::2:2 \
    remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Muni_Backup instance=Service4 name=\
    Municipalidad_BR01_Bckp out-filter=Out remote-address=2001:db8:1:2::2 \
    remote-as=20 use-bfd=yes
add address-families=IPv6 in-filter=Comisaría1_Bckp instance=Service4 name=\
    Comisaría1_BR03_Backup out-filter=Out remote-address=2001:db8:1:2::4 \
    remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Comisaría1_Principal instance=Service4 \
    name=Comisaría1_BB04 out-filter=Out remote-address=2001:db8:1:2::5 \
    remote-as=30 use-bfd=yes
add address-families=IPv6 in-filter=Comisaría2_Bckp instance=Service4 name=\
    Comisaría2_BR05_Bckp out-filter=Out remote-address=2001:db8:1:2::6 \
    remote-as=40 use-bfd=yes
add address-families=IPv6 in-filter=Comisaría2_Bckp instance=Service4 name=\
```

```
   Comisaría2_BR06_Bckp out-filter=Out remote-address=2001:db8:1:2::7 \
   remote-as=40 use-bfd=yes
/routing filter
add action=accept chain=Muni_Principal prefix=2001:db8:1001::/64
add action=discard chain=Muni_Principal
add action=accept chain=Muni_Backup prefix=2001:db8:1001::/64 \
   set-bgp-local-pref=3
add action=discard chain=Muni_Backup set-bgp-local-pref=3
add action=accept chain=Out prefix=2001:db8:1:1::/64
add action=discard chain=Out prefix=2001:db8:1:1::/64
add action=accept chain=Comisaría1_Principal prefix=2001:cafe:1::/64
add action=accept chain=Comisaría1_Bckp prefix=2001:cafe:1::/64 \
   set-bgp-local-pref=3
add action=discard chain=Comisaría1_Principal
add action=discard chain=Comisaría1_Bckp set-bgp-local-pref=3
add action=accept chain=Comisaría2_Principal prefix=2001:cafe:1001::/64
add action=discard chain=Comisaría2_Principal
add action=accept chain=Comisaría2_Bckp prefix=2001:cafe:1001::/64 \
   set-bgp-local-pref=3
add action=discard chain=Comisaría2_Bckp set-bgp-local-pref=3
/system identity
set name=Router_Service4
/tool mac-server
set allowed-interface-list=none
```

Noc Router

```
/interface bridge
add name=Trunk
/interface ethernet
set [ find default-name=ether1 ] disabled=yes
/interface vlan
add interface=Trunk name=vlan5 vlan-id=5
add interface=Trunk name=vlan100 vlan-id=100
/interface bonding
add mode=active-backup name=bonding1 primary=ether1 slaves=ether1,ether2
/interface list
add exclude=all include=static name=Admin
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=Trunk interface=bonding1
/IP neighbor discovery-settings
```

```
set discover-interface-list=Admin
/interface list member
add interface=ether9 list=Admin
/IP address
add address=11.11.11.1/24 interface=vlan5 network=11.11.11.0
add address=10.10.10.1/24 interface=vlan100 network=10.10.10.0
/IP service
set telnet disabled=yes
set ssh port=2022
set WinBox port=8296
/system identity
set name=NOC
/tool mac-server
set allowed-interface-list=none
```