UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"REINGENIERÍA DE LA RED DE DATOS MEDIANTE TECNOLOGÍA VPLS PARA LA ZONA DE IBARRA EN LA EMPRESA MIKRO-NET S.A"

Trabajo de grado previo a la obtención del título de Ingeniero en Electrónica y Redes de Comunicación

AUTOR:

RENÁN GONZALO ARIAS YANDÚN

DIRECTOR:

MSc. CARLOS ALBERTO VÁSQUEZ AYALA

Ibarra, 2025

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1002932166		
APELLIDOS Y NOMBRES:	Arias Yandún Renán Gonzalo		
DIRECCIÓN:	Maldonado 14-104 y Guillermina García		
EMAIL:	rgariasy@utn.edu.ec		
TELÉFONO FIJO:	062602235	**TELÉFONO MÓVIL:**	0939048197

DATOS DE LA OBRA	
TÍTULO:	"Reingeniería de la Red de datos mediante tecnología VPLS para la zona de Ibarra en la empresa Mikro-Net S. A"
AUTOR (ES):	Arias Yandún Renán Gonzalo
FECHA: DD/MM/AAAA	07/02/2025
PROGRAMA:	☒ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación
DIRECTOR:	Ing. Carlos Vásquez Ayala, MSc

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Renán Gonzalo Arias Yandún, con cédula de identidad Nro. 100293216-6, en calidad de autor (es) y titular (es) de los derechos patrimoniales de la obra o trabajo de integración curricular descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

Ibarra, a los 25 días del mes de febrero de 2025

EL AUTOR:

.....

Arias Yandún Renán Gonzalo

CI: 1002932166

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 25 días del mes de febrero del 2025.

EL AUTOR:

Arias Yandún Renán Gonzalo

CI: 1002932166

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 07 de febrero del 2025

Magíster Carlos Alberto Vásquez Ayala

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

.....

MSc. Carlos Vásquez Ayala

C.C.: 1002424982

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificador del trabajo de Integración Curricular "Reingeniería de la Red de datos mediante tecnología VPLS para la zona de Ibarra en la empresa Mikro-Net S. A" elaborado por Arias Yandún Renán Gonzalo, previo a la obtención del título de Ingeniero en Electrónica y Redes de Comunicación, aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

(f): .....
MSc. Carlos Alberto Vásquez Ayala
C.C.: 1002424982

(f): .....
MSc. Jaime Roberto Michilena Calderón
C.C.: 1002198438

DEDICATORIA

Con mucho cariño y gratitud dedico este trabajo a mi esposa Sonia y a mis hijos, quienes siempre han sido mi mayor inspiración, lo que hizo posible la culminación de esta obra. Su amor incondicional y su apoyo constante han sido mi motor en los momentos más desafiantes.

Renán Gonzalo Arias Y.

AGRADECIMIENTO

Agradezco a Dios, por la oportunidad y por mantenerme de pie ante las adversidades, agradezco a todas las personas que de alguna manera fueron parte y ayuda para la realización y finalización de mi trabajo de grado, de manera especial a mi esposa, por la paciencia y apoyo constante, gracias por creer en mí, alentarme a perseguir mis sueños y enseñarme que con esfuerzo y dedicación se pueden alcanzar grandes logros.

A mis hijos, que han sido el motor y las fuerzas para seguir adelante, a mi amada madre que, con su respaldo y aliento, fueron impulso para no decaer en el camino, y a todos los amigos y profesionales que en algún momento compartieron un poco de su conocimiento, mismo que sirvió de ayuda para la realización de este trabajo.

A la Universidad, en especial a la Facultad de Ingeniería en Ciencias Aplicadas, así como a los docentes que a lo largo de la carrera orientaron y compartieron sus conocimientos y fueron participes importantes en mi formación como profesional. A mi director de tesis, Ing. Carlos Vásquez, y a mi asesor, Ing. Jaime Michilena, por el valioso tiempo y colaboración, además de la orientación que conjuntamente con sus valiosos conocimientos, fueron de ayuda, no solo en la elaboración de este trabajo de titulación, sino a lo largo de todo este arduo pero gratificante trayecto académico.

Renán Gonzalo Arias Y

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El proyecto actual se centra en el desarrollo de un plan de reingeniería de una red tradicional de tipo plana, a una con segmentación, protocolos de enrutamiento e implementación de la tecnología VPLS, con el fin de obtener mejorías en el rendimiento y administración de una red. Este plan se desarrolló por medio de herramientas de virtualización, lo que posibilitó emular la red lo más cercano a la realidad posible. De este modo, a través de configuraciones sobre imágenes ISO, se llevó a cabo el diseño y la emulación.

El desarrollo del proyecto se dio en base al sistema digital de gestión llamado PMBOK, reconocido internacionalmente por su metodología y gestión de proyectos, inicialmente se documentaron los inconvenientes encontrados en la red, posteriormente se planificó el desarrollo a seguir, para que luego se dé la implementación sin inconvenientes y finalmente dar por cerrado el proyecto después de haber realizado las pruebas.

En el tercer capítulo se analizaron los requerimientos dados en base al análisis previo, y en base a ello se procedió con el diseño de la nueva topología de red la cual se realizó con directrices puntuales en cuanto a la segmentación, direccionamiento IP, protocolos de enrutamientos e implementación de tecnologías como MPLS y VPLS.

Finalmente se realizaron las pruebas respectivas, las emulaciones y configuraciones previas fueron detalladas en el capítulo cuatro, donde se realizaron pruebas de convergencia, segmentación y confiabilidad de la red, mismas que se llevaron a cabo de una en una, pruebas que sustentaron que la reingeniería y las tecnologías empleadas son la solución a los problemas citados de inicio en el capítulo uno.

ABSTRACT

The current project focuses on the development of a reengineering plan of a traditional flat network, to one with segmentation, routing protocols and implementation of VPLS technology, in order to obtain improvements in the performance and management of a network. This plan was developed by means of virtualization tools, which made it possible to emulate the network as close to reality as possible. Thus, through configurations on ISO images, the design and emulation were carried out.

The development of the project was based on the digital management system called PMBOK, internationally recognized for its methodology and project management, initially documented the problems encountered in the network, then planned the development to follow, so that then the implementation is given without problems and finally close the project after having performed the tests.

In the third chapter, the requirements were analyzed based on the previous analysis, and based on this, the design of the new network topology was carried out with specific guidelines regarding segmentation, IP addressing, routing protocols and implementation of technologies such as MPLS and VPLS.

Finally, the respective tests were carried out, the emulations and previous configurations were detailed in chapter four, where convergence, segmentation and reliability tests of the network were carried out one by one, tests that supported that the reengineering and the technologies used are the solution to the problems mentioned at the beginning of chapter one.

Capítulo 1. Antecedentes

El primer capítulo se orientó a la explicación de la necesidad del desarrollo de una reingeniería de la red actual de la empresa Mikro-Net SA, el plan de migración de la red plana a una red con uso de protocolos de ruteo dinámico se la realiza con la finalidad de optimizar la gestión de red y garantizar su competitividad en el área de las TIC´s, reconociendo la situación actual de las redes tradicionales y su problemática. De igual forma se justificó y delimitó la propuesta del plan de migración.

1.1. Tema

REINGENIERÍA DE LA RED DE DATOS MEDIANTE TECNOLOGÍA VPLS PARA LA ZONA DE IBARRA EN LA EMPRESA MIKRO-NET S.A

1.2. Problema

Mikro-Net SA fue constituida el año 2017 en Ibarra con el objetivo de ofrecer servicios de acceso a internet, a través del tiempo la tecnológica ha ido en gran crecimiento y actualización y la necesidad de las personas en acceder al servicio de conexión a internet fue incrementando por lo que la empresa siguió ampliando su red a diferentes sectores de la ciudad para garantizar cobertura del servicio en muchos más lugares de la zona.

Al tener una conexión de red plana y crecimiento sin planificación ni diseño especifico, la empresa presenta problemas en la disponibilidad de la red lo que se refleja en dificultades de navegación de los usuarios, debido a la excesiva cantidad de paquetes de difusión, mismos que provocan tormentas de broadcast en la red de transmisión, generando loops en la misma y con ello que los equipos terminen inhibidos o con la memoria saturada.

A continuación, en la Figura 1, se describe el problema en el siguiente diagrama de Ishikawa:

Figura 1.

Diagrama de Ishikawa.

Nota. Se muestran los factores e inconvenientes que provocaron el problema.
Fuente. Elaborado por el autor. *Fuente. Autoría Propia*

Después de un análisis de los acontecimientos surge la necesidad de segmentar y diseñar una red en la que se deba solventar los inconvenientes presentes, el uso de protocolos de ruteo dinámico y modificaciones en la topología de red terminaría con los problemas y se daría solución de manera eficiente y oportuna garantizando un buen servicio al cliente.

1.3. Objetivos

1.3.1. Objetivo general

Realizar la reingeniería en la red de datos con el uso de protocolos de enrutamiento dinámico VPLS de la empresa Mikro-Net SA que solucione los problemas de servicio de los usuarios.

1.3.2. Objetivos específicos

- Identificar el estado actual de la red LAN y documentarla.
- Diseñar la segmentación de la nueva red con tecnología VPLS y el enrutamiento dinámico ospfv2.
- Realizar un plan de mejoras para la migración de la red plana a la red diseñada usando las etapas de la metodología PMBOK.
- Identificar las mejoras obtenidas en la red de datos de la empresa Mikro-Net SA

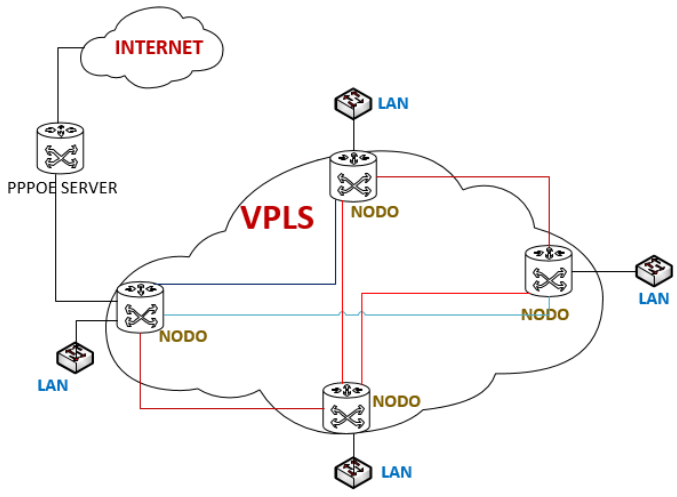
1.4.Alcance

Mediante la realización de este proyecto se espera estabilizar la red, en cuanto a manejar de manera óptima la escalabilidad, administración, segmentación, enrutamiento y tiempos de respuesta jitter y latencia. Para ello se realizará un plan de migración de red plana a una red con uso de protocolos de enrutamiento y tecnologías actuales para la optimización de recursos y desempeño de la red.

A continuación, el diagrama de la red con implementación VPLS, se muestra en la Figura 2.

Figura 2.

Diagrama de red.



Nota. se puede evidenciar la conexión entre nodos en el que cada uno llevará en su configuración la implementación de VPLS. *Fuente*. Elaborado por el autor.

El desarrollo del proyecto se dará por la orientación de un sistema digital de gestión llamado PMBOK, reconocido internacionalmente por su metodología y gestión de proyectos dado en 5 pasos: inicio, planificación, ejecución, desempeño y cierre.

En la etapa INICIO se evaluará el estado actual, la arquitectura de red inicial y los problemas inmersos en ella, opciones de despliegue, expansión y funcionamiento, con ello el levantamiento de la información inicial necesaria para llevar a cabo los objetivos planteados.

En la PLANIFICACIÓN se elaborará un nuevo diseño de red del ISP en el que se defina la segmentación y los posibles requerimientos en software y hardware necesarios para la implementación y las configuraciones que a ello conllevan.

En la EJECUCIÓN se iniciará con las pruebas y simulaciones del nuevo diseño de red, en esta instancia la red sufrirá cambios en la topología inicial debido a la segmentación y la implementación del protocolo de ruteo dinámico OSPFv2 y VPLS.

Finalmente, en el DESEMPEÑO se identificarán las mejoras obtenidas en el diseño realizado, se mostrará los cambios y progreso de la red en cuanto a la escalabilidad, administración y tiempos de respuesta jitter y latencia.

Con ello se realizará el CIERRE y se extraerán las conclusiones, mismas que servirán para la deducción de ventajas y desventajas de la red implementada respecto a la red anterior.

1.5. Justificación.

La empresa Mikro-Net S.A comenzó brindando el servicio de internet como ISP en el año 2017, su red de datos inició sin planificación de crecimiento y escalabilidad, con crecimiento basado en criterios empíricos y sin ningún esquema técnico o modelo

apropiado, el auge de las telecomunicaciones especialmente la de venta de servicios de internet se da en temporada de pandemia provocada por el COVID, la alta demanda del servicio hizo que algunas empresas entre ellas Mikro-Net SA aumenten considerablemente la cantidad de abonados y con ello la expansión de red de cobertura para ciertos sectores, esto causó que la red sufra modificaciones y que con ello se susciten problemas de jitter, latencias altas y loops de red además de la falta de personal técnico capacitado en el área de networking que logre identificar y solventar estos inconvenientes.

La VISION de la empresa al año 2026 se enfoca en ser referente de excelencia en atención al cliente, además de ofrecer servicios de alta calidad cumpliendo con los requerimientos y demandas del mercado, en base a ello se procederá con soluciones que permitan enrutamiento de tráfico VPLS en la red de datos y terminar con los problemas suscitados actualmente con el único fin de garantizar robustez y fiabilidad en la red.

Según el ODS 9.1(OBJETIVO DE DESARROLLO SOSTENIBLE) que consiste en desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad, para apoyar el desarrollo económico y el bienestar humano, haciendo hincapié en el acceso asequible y equitativo para los usuarios, se considera necesario la implementación de tecnologías útiles con el fin de resolver los problemas de red y modernizar las telecomunicaciones en la empresa.

Capítulo 2. Fundamentación Teórica

El presente capítulo citará los conceptos básicos de redes WAN y LAN tradicionales, así como una breve explicación de lo que es una red plana, además de problemas comunes como lo son los loops de red, jitter y latencia para posteriormente profundizar los conceptos de protocolos de enrutamiento dinámico haciendo énfasis en el protocolo OSPFv2, finalmente se verá el funcionamiento de MPLS y VPLS y las implicaciones que conllevan para su implementación.

2.1. Redes tradicionales y problemas frecuentes.

Las redes de área extensa WAN son la abreviatura de Wide Área Network en inglés, una red de telecomunicaciones que conecta entre sí varias redes LAN. En una empresa una WAN puede incluir conexiones entre sucursales, acceso a aplicaciones y servicios en la nube, normalmente se utiliza enrutadores para las comunicaciones y las VPN son una de las herramientas que facilitan conectividades entre ellas.

2.1.1. Funcionamiento WAN y LAN

Una red de área local (LAN) conecta dispositivos que están físicamente cerca unos de otros mediante conectores como enrutadores y conmutadores. Permite que los dispositivos intercambien datos y se comuniquen de forma segura a pequeña escala. Una red de área extendida (WAN) se extiende más allá de un edificio o de un gran recinto para incluir múltiples ubicaciones repartidas a lo largo de una zona geográfica concreta, o incluso del mundo. Las organizaciones utilizan las WAN para facilitar las interacciones digitales y el intercambio de datos entre empleados y clientes en diferentes regiones o países.

Las WAN a través de conexiones de red cableadas con enlaces directos de fibra óptica ofrecen mejor rendimiento y confiabilidad y por ende son las preferidas para la

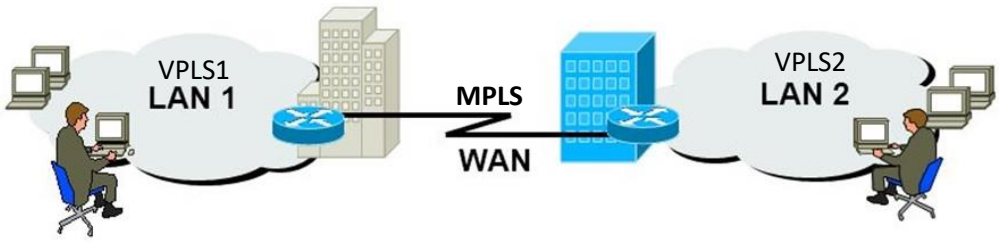
mayoría de empresas, pero las tecnologías inalámbricas como el caso de las 4G LTE, conexiones WIFI o Satelitales se hacen cada vez más comunes. (Díaz, 2017).

López (2020) expone que las redes WAN convencionales operan mediante la adquisición e implementación de circuitos exclusivos para dirigir servicios de IP hacia sus destinatarios previstos. Entre las tecnologías de transmisión de datos en las WAN, la más popular es el MPLS, ya que proporciona un rendimiento de red garantizado con políticas de calidad de servicio (QoS) que administran el rendimiento, el retraso y la fluctuación.

Por otro lado, VPLS es un servicio que utiliza tecnología MPLS para la conectividad como servicio base, VPLS es una conexión L2 entre redes mientras que MPLS puede ser L3 o L2 dependiendo del requisito, VPLS se transmite a través de redes IP y puede ser conexión punto-punto o punto-multipunto lo que hace a esta tecnología ideal para trabajar usando interfaces ETHERNET en conexiones LAN, tal como se muestra en la figura 3 a continuación.

Figura 3.

Esquema de funcionamiento redes LAN y WAN



Fuente. Modificado de https://diplomadoentelecomunicacionesycontrol.blogspot.com/2017/06/redes-de-area-amplia.html

2.1.2. Problemas de red

Los problemas que se presentan en la red comúnmente se dan en redes LAN con alto tráfico de paquetes broadcast, las redes planas hacen que la latencia fluctúe de manera

que haya pérdidas de paquetes e inhibición de equipos de red, la falta de equipos de gestión adecuados tambien hacen que la red se comporte de manera inestable y se generen retraso en la comunicación de las diferentes conexiones.

Existen herramientas y tecnologías que nos permiten optimizar el desempeño de nuestra red, una herramienta importante es el uso de protocolos de enrutamiento, estos se los puede aplicar y configurar de modo estático o dinámico de acuerdo a las necesidades que se presenten, este proyecto se centrará en el uso del protocolo dinámico OSPFv2 y la adecuación de dicha red para su funcionamiento con VPLS.

Los problemas que se dan en una red tienen que ver con la caída o retardos en la entrega de paquetes que se envían de un punto de la red a otro, estos problemas se los mide en unidades de tiempo y son causados por varios factores donde se evalúa la distancia, medio de transmisión, ancho de banda, congestión de red, entre otros. Los problemas de retardos y caídas de paquetes afectan a la velocidad y la calidad de los servicios de red.

2.1.2.1. Jitter y Latencia

La LATENCIA es el tiempo que se demora un paquete en viajar desde un punto de la red a otro, los problemas de latencia se dan en una red cuando los paquetes tardan más de lo habitual en llegar a su destino, la distancia determina el tiempo que tardan los paquetes en llegar, mientras que el JITTER determina la fluctuación de la latencia, el jitter puede ser de fluctuación alta o baja. (Goodwin, 2023)

Si el jitter es bajo, lo más probable es que la latencia no sea causada por la congestión en algún lugar de la red, ya que la latencia experimentada es relativamente constante. En su lugar, lo más probable es que la disponibilidad de ancho de banda sea

escasa, es el caso que se da en redes móviles, o simplemente que la distancia física entre la red y el servidor sea extensa.

En el caso de Jitter alto con latencia alta, los paquetes tardan más de lo habitual y más de lo deseado en llegar a su destino, la latencia determinará el tiempo que tardará el paquete en llegar a su destino y el jitter determinará el movimiento de la latencia si es de baja o alta fluctuación.

El jitter puede producirse por muchas razones, ya sea en el NAT en el router, en la ruta de transporte, en la capa física y medio de transmisión, como en una VPN. Es preferible una latencia constante a un jitter elevado, porque el jitter puede provocar pérdida de paquetes (Goodwin,2023)

2.1.2.2. Loop de red

El tráfico de broadcast es un componente natural de las redes TCP/IP, y consiste en la comunicación de un terminal origen con todos los terminales de un dominio de Difusión puede ser este una: red, subred o VLAN.

A medida que aumenta el número de hosts en una subred, las tablas ARP de cada uno son más grandes y tienen más entradas, con lo que a medida que crece el número de hosts también aumenta exponencialmente el tráfico ARP de broadcast que circula por la red, este tráfico al conmutarse de manera errónea, producirá bucles o loop de red, lo que generará inestabilidad en toda la red.

Los loop de capa2 de red, o bucle de red se da por la llegada de paquetes a un destino por varias rutas, esto puede ocurrir por problemas en las rutas entre los dispositivos de origen y destino o por casos de problemas en el medio de trasmisión físico. Un bucle de red provocará la inestabilidad de la dirección MAC en un equipo de capa tres y con ello tormenta de difusión de red, el problema se da por la gran cantidad de paquetes

que cursan por la red saturando la CPU de los equipos y en algunos casos la inhibición de los mismos. (Almazán, 2018)

2.2. Open Shortest Path First (OSPF)

OSPFv2 se implementa en el estándar del RFC2328, obtiene su nombre de algoritmo SPF de Dijkstra. El prefijo “significa que es protocolo (OPEN)”, por lo que cualquier persona puede acceder. Las especificaciones de OSPF se pueden encontrar en el RFC-2328 por lo que múltiples fabricantes lo soportan.

OSPF no es protocolo basado en algoritmo de vector Distancia, sino que es un algoritmo de Estado de Enlace (Link State), la palabra enlace(link), se refiere a una interface del router, es decir a la red a la cual está conectada y la palabra estado, se refiere a las características del enlace tales como; su dirección ip, costo o métrica y el estatus operacional (up/down).

Los router que ejecutan OSPF describen el estado de sus enlaces directamente conectados en los paquetes de anuncio de estado de enlace (LSA:Link State Advertisen packets) que se distribuyen a todos los routers. (Escalante,2024)

Para intercambiar información de enrutamiento en una red OSPF, los dispositivos vecinos deben establecer adyacencias. Cada router construye la topología de la red usando todos los paquetes LSA que reciben. La topología de la red se describe matemáticamente en la forma de un gráfico. (Level.14)

Esta base de datos de la topología constituye la entrada para el algoritmo SPF de Dijkstra. Cada router ejecuta el algoritmo SPF para calcular el camino más corto a cada red en el gráfico.

2.2.1. Métrica OSPF

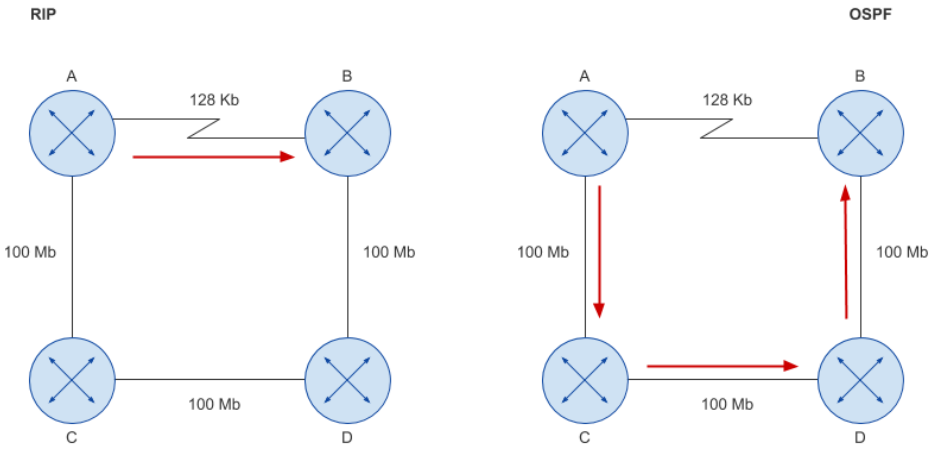
La métrica es la medida usada para decidir la mejor ruta, cada router OSPF ejecuta el algoritmo SFP de Dijkstra para calcular la ruta más corta desde si mismo a cada subred en su área. (Escalante,2016)

Cada protocolo de enrutamiento usa un tipo de métrica distinta, por ejemplo, RIP usa los saltos como métrica, EIGRP usa la métrica basada en el ancho de banda y retraso, mientras que OSPF usa el costo como métrica. (Marcelo, 2020)

A continuación, en la figura 4, se muestra un ejemplo de la métrica usada tanto por RIP y OSPF.

Figura 4.

Funcionamiento de métrica en RIP y OSPF



Fuente. Obtenida de (Macelo,2020). https://ccnadesdecero.com/curso/distancia-administrativa-y-metrica/

En la figura 4 se puede apreciar cómo se comportan los dos protocolos para encontrar la ruta más corta o la ruta más óptima para llegar a su destino, claramente podemos observar que RIP prefiere el camino más corto estipulado su métrica por saltos pese a que el ancho de banda del enlace es menor a los otros, por otro lado, podemos

apreciar que OSPF entiende que el camino más optimo es el que ofrece mayor velocidad dado que en enlaces de mayor velocidad el costo es menor. (Marcelo, 2020)

2.2.2. Costo OSPF

El estándar RFC 2328 no especifica cómo un router debe calcular el costo de una red conectada, este cálculo lo dejará el fabricante, por ejemplo, se podría calcular el coste de una red conectada de la siguiente manera, tal como se muestra en la ecuacion1:

Ecuación 1.

$$\text{Costo} = 10^8 \text{ / AB de la interfaz en bps}$$

Fuente. Datos obtenidos de Ruteo Avanzado con MikroTik RouterOS (Escalante, 2016).

Basado en esta definición, la tabla 1 muestra el costo OSPF para algunos tipos de medios, el costo se redondea hacia abajo, al número entero más cercano.

Tabla 1.

Costo de OSPF, de acuerdo a tipo de tecnología de medio.

TIPO DE MEDIO	ANCHO DE BANDA POR DEFAULT	COSTO POR DEFAULT
ETHERNET	10Mbps	100
FAST ETHERNET	100Mbps	1
FDDI	100Mbps	1
T-1 SERIAL	1,54Kbps	64

Fuente. Modificado de (Escalante, 2016)

2.2.3. Sistema Autónomo (AS)

Un sistema autónomo se define como un grupo de redes IP que poseen una política de ruteo propio e independiente, es decir realiza su propia gestión del tráfico que fluye entre él y otros sistemas autónomos que forman la Internet, cada sistema autónomo es

identificado por un número, mismo que será único en sus redes dentro de Internet. (MUM Honduras, 2018)

La asignación de números de Sistema Autónomo (ASN) en la región de Sudamérica está a cargo de **LACNIC** (Latin American and Caribbean Internet Addresses Registry), este es uno de los cinco Registros Regionales de Internet (**RIRs**) encargados de la asignación y administración de recursos de Internet en diferentes regiones del mundo. (LACNIC)

En la tabla 2 a continuación se muestra los rangos de 16bits usados por LACNIC para la identificación de sistemas autónomos.

Tabla 2.

Rangos de ASN

RANGO DE ASN DE 16bits	**DESCRIPCIÓN**
De 1 a 64511	Asignados por la IANA (Internet Assigned Numbers Authority)
De 64512 a 65534	Reservados para pruebas y uso privado
65535	Reservado para ASN de 16 bits que no se pueden utilizar
De 65536 a 65551	Reservados para propósitos especiales

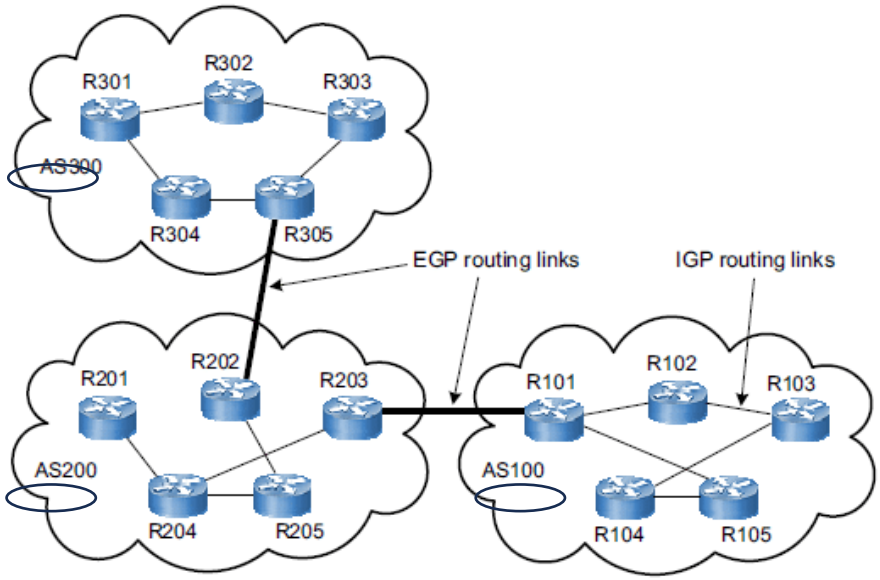
Fuente. Adaptado de (Escalante,2016)

LACNIC es responsable de gestionar los recursos de direcciones IP y ASN para la región de **América Latina** y el **Caribe**, incluyendo los países de Sudamérica. Esto implica asignar bloques de direcciones IP y números de Sistema Autónomo a organizaciones y proveedores de servicios de Internet (**ISPs**) que operan en la región.

A continuación, en la figura 5 se muestra una imagen de la conexión de sistemas autónomos.

Figura 5.

Ejemplo de conexión de diferentes sistemas autónomos.



Fuente. (Barzola, 2023). https://abcxperts.com/que-es-un-sistema-autonomo/?srsltid=AfmBOor5gMITbIBb4Bwt235 -LBZwt8wAIN1SG1RTi5RGotzHITy9YFa-

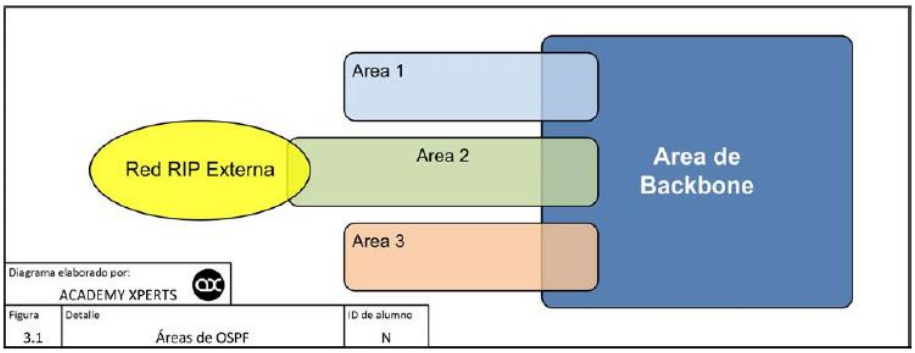
2.2.4. Área OSPF

El algoritmo de Dijkstra es costoso en uso de procesamiento y CPU debido al incremento de la topología de la red lo que puede ser un problema, para ello OSPF puede ser dividida en pequeñas áreas dependiendo de su estructura jerárquica, lo que quiere decir que el algoritmo SPF se ejecutará únicamente en la topología dentro de cada área. (Escalante,2016)

En el diagrama de la figura 6 podemos observar que cada área se comunica o resume sus rutas a un área en común llamada área de Backbone o área cero, por lo tanto, si dos áreas necesitan comunicarse deberán pasar su información inicialmente por el área de backbone. (Barzola, 2023)

Figura 6.

Diagrama de conexión de áreas en protocolo OSPF.



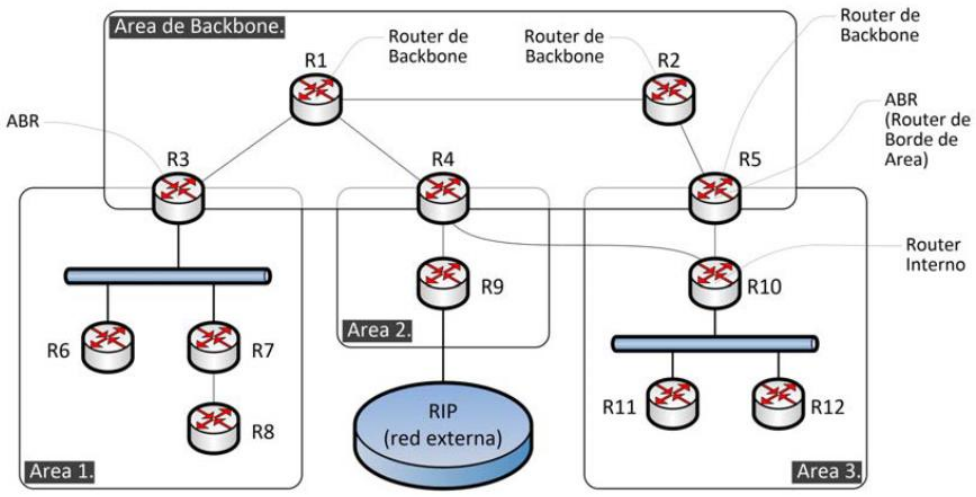
Fuente. Modificado de *(Escalante, 2016)*

Un área es un conjunto de redes contiguas en el cual se comparte un ID único, cada área deberá tener la información sobre su topología y por lo tanto las otras áreas no podrán acceder a esta información, el algoritmo SPF se ejecutará en los enrutadores internos de cada área. (cisco.com)

Todo el tráfico intra-area debe cursar por el área cero, lo que implica que los routers backbone deben contar con la topología completa de la red como se muestra en la figura 7 a continuación.

Figura 7.

Arquitectura OSPF.



Fuente. Modificado de *(Escalante, 2016)*

En la figura 7 anterior, se puede apreciar que R3, R4 y R5 son routers que pertenecen a más de un área, siendo estos troncales junto a R1 y R2 tambien pertenecen al área de backbone o área cero.

Los routers de backbone tienen una base de datos donde recopilan la topología y describen el estado de enlaces y redes ip en las áreas.

Cada red OSPF que se divide en diferentes áreas debe utilizar estas reglas:

- Debe existir un área troncal que combine un conjunto de áreas independientes en un solo dominio.
- Cada área que no es de estructura básica debe estar conectada directamente con la zona de estructura básica.
- El área troncal no debe dividirse (en partes más pequeñas) bajo ninguna condición de falla, como eventos de enlace o routers inactivos.

2.2.4.1. Funcionamiento de OSPF en las áreas

- **Jerarquía OSPF:** OSPF utiliza una jerarquía que divide las redes en áreas más pequeñas para optimizar las actualizaciones de enrutamiento. Todas las áreas deben conectarse a un área backbone (denominada área 0 o área backbone) directamente o a través de un túnel virtual. El área backbone actúa como intermediario para el tráfico entre áreas.
- **LSDB y SPF:** Dentro de una misma área, todos los routers OSPF mantienen una copia idéntica de la base de datos de estado de enlace para esa área y utilizan el algoritmo de Camino Más Corto Primero para calcular las rutas más eficientes dentro del área.

- **Tipos de Áreas:** Existen varios tipos de áreas en OSPF. Cada tipo de área está diseñado para manejar ciertos tipos de tráfico de enrutamiento y casos de uso específicos para optimizar aún más la red.

2.2.4.2. Beneficios de Usar Áreas en OSPF

- **Escalabilidad:** Permite que OSPF escale para manejar grandes redes dividiéndolas en áreas más manejables.
- **Eficiencia:** Reduce la cantidad de información de enrutamiento que debe ser procesada y enviada en la red, disminuyendo así el ancho de banda necesario para las actualizaciones de enrutamiento y el uso de CPU en los routers.
- **Rapidez en la Convergencia:** Minimiza el tiempo de convergencia tras un cambio en la topología de red, ya que los cambios están a menudo confinados a una sola área.
- **Control de Tráfico:** Permite un mayor control sobre el tráfico de enrutamiento y la aplicación de políticas de enrutamiento.

El diseño y la implementación de áreas OSPF deben hacerse cuidadosamente para maximizar los beneficios de rendimiento y escalabilidad mientras se mantienen las operaciones de red simplificadas y eficientes.

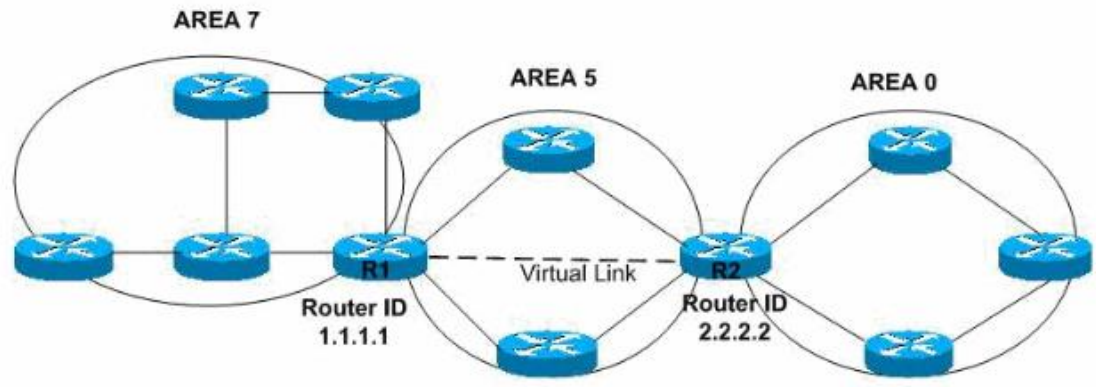
2.2.5. Enlaces Virtuales (VLs)

Todas las áreas en un sistema autónomo deben estar físicamente conectadas al área troncal, pero dado el caso de no existir dicha conexión se podrá conectar a través de un virtual link o enlace virtual, esta conexión virtual es usada para conectar áreas remotas al backbone área a través de un área non-backbone. (cisco.com)

En el diagrama de la figura 8 podemos observar la conexión de un link virtual, para conectar el área 7 a la estructura básica del área.

Figura 8.

Ejemplo de conexión mediante VLs.



Nota. Se debe configurar el area5 virtual-link tanto en los routers R1 y R2.

Fuente. Extraído de https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/13703-8.html

2.2.6. Diseño de una red OSPF

Según (Escalante,2016), para el diseño de una red OSPF es recomendable tener en cuenta algunos parámetros importantes, con el fin de obtener una red eficiente, escalable y estructurada adecuadamente, el diseño se realizará en base a:

- **Jerarquía OSPF.** El diseño de red OSPF debe ser claramente definido, los cambios deben ser acordes a la arquitectura.
- **Direccionamiento IP.** Las direcciones IP deben ser colocadas en bloques que permitan la sumarización de rutas en los ABRs, es recomendable el uso de VLSM con el fin de conservar el espacio de direcciones IP disponible, esto dado a que lo registros OSPF LSA llevan máscaras de subred.
- **Router ID.** Se debe usar direcciones LOOPBACK para asignación de routers-ID, de esto dependerá la elección del DR/BDR

- **DR / BDR.** Para elegir este router se deberá analizar los recursos de, procesador, memoria y ancho de banda, el router elegido como DR/BDR puede tener alto consumo de recursos de memoria y CPU.
- **Área de Backbone.** Analizar el ancho de banda en los enlaces backbone, dado que todo el tráfico inter-area atravesará por el backbone, lo recomendable es tener múltiples enlaces y rutas entre routers, además de no ubicar usuarios o servidores en el backbone.
- **Cantidad de routers en un área.** El máximo número de routers dependerá del número de redes y recursos de cada router, lo recomendable es interconectar máximo entre 40 y 50 routers, con el fin de no sobrecargar el CPU de los equipos.
- **Cantidad de Vecinos.** Cuando el número de vecinos excede a 15, y el DR/BDR presenta problemas de desempeño, es necesario buscar un remplazo de más recursos con más potencia para el DR/BDR.
- **Sumarización de rutas.** Para sumarizar las rutas es recomendable ubicar bloques de direcciones para cada área, basados en los límites de bit.
- **Stub Áreas.** Analizar el uso de VLs, dado que los Stub Areas no soportan este tipo de enlaces, un área con solo un ABR es ideal para un Stub Area.
- **Virtual Links.** Los VLs deben ser usados como correcciones de emergencia, mas no como parte de diseño inicial.
- **Timers OSPF.** Los timers OSPF pueden manejarse con los valores default, sin embargo, en una red OSPF con equipos de marcas distintas, será necesario en algunos casos ajustar los timers a conveniencia para que haya coincidencia.

2.3. Multiprotocol Label Switching (MPLS)

MPLS, es una tecnología de red que se utiliza para mejorar la eficiencia en el enrutamiento y reenvío de paquetes de datos en una red de telecomunicaciones.

(López, 2020). Fue desarrollada con el fin de superar las limitaciones de las redes basadas en IP al agregar capacidades de conmutación de circuitos en las redes de conmutación de paquetes. (Escalante, 2016)

2.3.1. Introducción a MPLS

MPLS, es una tecnología de red que se utiliza para mejorar la eficiencia en el enrutamiento y reenvío de paquetes de datos en una red de telecomunicaciones. (López, 2020). Fue desarrollada con el fin de superar las limitaciones de las redes basadas en IP al agregar capacidades de conmutación de circuitos en las redes de conmutación de paquetes. (Escalante, 2016)

Una Red MPLS implementa enrutadores y etiquetas concretas a la información de diferentes tipos, para poder enviarlas por un camino de baja latencia, de forma que los datos como voz e imágenes viajan entre grandes distancias a mucha velocidad. (Palo Alto Networks, 2023).

Cada enrutador de la red tiene una tabla que indica cómo manejar paquetes de un tipo de FEC específico, por lo que una vez que el paquete ha ingresado a la red, los enrutadores no necesitan realizar un análisis de encabezado. En cambio, los enrutadores posteriores usan la etiqueta como un índice en una tabla que les proporciona una nueva FEC para ese paquete**.**

Esto le da a la red MPLS la capacidad de manejar paquetes con características particulares (como los que provienen de puertos particulares o que transportan tráfico de tipos de aplicaciones particulares) de manera consistente. Los paquetes que transportan tráfico en tiempo real, como voz o vídeo, se pueden asignar fácilmente a rutas de baja latencia a través de la red, algo que es muy complicado con un enrutamiento convencional.

El punto clave de la arquitectura de todo esto es que las etiquetas proporcionan una forma de adjuntar información adicional a cada paquete, información que va más allá de la que tenían los enrutadores anteriormente.

MPLS funciona les dice a los routers exactamente donde buscar en la tabla de enrutamiento por un prefijo específico. Usualmente, un router debe realizar una búsqueda línea por línea en su tabla de enrutamiento por una entrada específica para asi poder reenviar/enrutar apropiadamente un paquete, entonces MPLS hace que se evite este esfuerzo. (Cisco, 2018)

2.3.2. Arquitectura MPLS

La arquitectura MPLS es eficiente, ya que esta mejora el rendimiento mediante el incremento de velocidad de los datos a través de la red por lo que se basa en etiquetas y no en la cabecera IP. Entonces el enrutador utiliza información la cual se asigna a una corrección de errores hacia a delante, (FEC) entonces antes de la transferencia de paquetes se establecen rutas y la asignación de etiquetas para la distribución de estas y la creación de tablas los cuales no afecta a los demás enrutadores internos de la red correspondiente por lo que continúa con la recepción del paquete y la implantación de la etiqueta lo cual esto permite la conmutación de las etiquetas y la correspondiente transferencia del paquete en donde será extraído su etiqueta y finalmente entregar el paquete (Pérez, 2020).

2.3.3. Componentes MPLS

Según (Barzola, 2020), MPLS se conforma principalmente de:

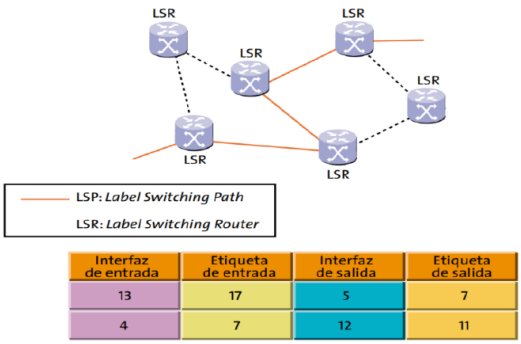
- **Label Switch Router (LSR):** Dispositivo de capa 3 que es parte del proveedor de servicios y realiza el proceso de distribución de etiquetas y transportación de paquetes.
- **Label:** La etiqueta tiene un tamaño de 20 bits la cual representa una FEC.

- **Label Switched Path (LSP):** Camino de un paquete a través de uno o más LSR.
- **Bindings:** Cuando la decisión de asignar una etiqueta a los paquetes depende del siguiente LSR.
- **Label Distribution Protocol (LDP):** Aquellos procedimientos en donde un LSR comunica a otro los bindings realizados.
- **Label Edge Router (LER):** Dispositivos de capa 3 ubicados de conectar diferentes redes (ATM, Frame Relay,etc) e inserta y retira las etiquetas de acuerdo con la información de enrutamiento.
- **Forward Equivalence Class(FEC):** Conjunto de paquetes que tienen mismos requerimientos para ser transmitidos y transportados por un mismo camino.

Como se puede apreciar en la Figura 9 a continuación, MPLS combina la gestión de tráfico capa 2 con la escalabilidad y flexibilidad del enrutamiento de capa 3, y permite que las redes de datagrama funciones como red de conmutación de circuito virtuales. Están compuestas por LSR y LER, los cuales realizan el encaminamiento de acuerdo con la etiqueta MPLS, y las tablas de conmutación que deben encontrarse en todos los nodos. El objetivo es realizar una adecuada gestión de recursos de la red de acuerdo con la reserva de capacidades de transmisión extremo a extremo. (Huidobro & Millán, 2002).

Figura 9.

Arquitectura básica de MPLS.



Nota. La figura muestra los elementos de una red MPLS básica.

Fuente. Telefónica I+D (2015).

2.3.4. Funcionamiento MPLS

El MPLS funciona de manera similar a los conmutadores y enrutadores, ubicándose entre las capas 2 y 3. Utiliza tecnología de envío de paquetes y etiquetas para tomar decisiones sobre el reenvío de datos. La etiqueta se impone entre los encabezados de capa 2 (enlace de datos) y de capa 3 (red). Esto hace posible la confiabilidad de MPLS al aislar virtualmente los paquetes. (Level.14, 2023)

Con MPLS, la ruta óptima a través de una red está predeterminada y se comunica con etiquetas específicas. Cada paquete está estampado con una etiqueta que indica claramente dónde debe ir a continuación. Los enrutadores de conmutador de etiquetas especializados (LSR) colocan etiquetas en cada paquete que pasa a través de ellos para que el próximo enrutador sepa dónde enviarlo. Dado que los enrutadores no tienen que leer largas tablas para averiguar dónde enviar un paquete, MPLS puede mejorar la eficiencia y la velocidad de la red.

Hay otro beneficio importante de tener paquetes de etiquetas LSR. Cuando el tráfico de datos está congestionado, la ruta predeterminada de un paquete de datos podría no ser la más eficiente en ese momento. Las conexiones MPLS se pueden usar para priorizar el tráfico, etiquetar algunos datos como más esenciales y garantizar que se enruten a través de la red más rápidamente. (Ortiz, 2020)

2.3.5. Desventajas de MPLS

- Tiene un costo alto en comparación al costo normal de conectividad de internet y más aún si se tiene más de un proveedor. (FS | community, 2022)
- Demora algún tiempo en el despliegue de una nueva sucursal, y muchas veces no es fácil llevar MPLS a ciertas zonas. (SPTel, 2021)

- Se requiere de una persona en cada sucursal debido a que la WAN no tiene un punto de operaciones centralizado, lo que requiere personal en forma presencial para la configuración lo que implica un aumento de costos de operación. (Webber, 2022)
- No es tan seguro. Una simple mala configuración aumenta el riesgo de una vulnerabilidad de seguridad. (Parra, 2020)

2.3.6. MPLS MTU

El MTU es la cantidad máxima de datos que puede transmitirse en una única unidad sin fragmentarse en pedazos más pequeños. En otras palabras, es el tamaño máximo que puede tener un paquete de datos antes de que deba dividirse en fragmentos más pequeños para su transmisión a través de la red. (ccnadesdecero.com)

Tanto en la Capa 2 como en la Capa 3, el MTU desempeña un papel fundamental en la eficiencia de la comunicación.

El parámetro MPLS MTU define el tamaño máximo de un paquete MPLS que puede ser transmitido a través de un túnel MPLS. El valor predeterminado de MPLS MTU es 1508 bytes, que es el tamaño máximo de un paquete IP con dos etiquetas MPLS.

En el caso de los túneles MPLS, la MTU de capa 3 debe ser al menos 20 bytes mayor que la MTU de capa 2 del enlace de datos. Esto es para permitir que los encabezados MPLS sean añadidos al paquete IP. (Barzola,2020)

2.3.7. Fragmentación de paquetes MPLS

Según (Barzola, 2020), en MPLS la fragmentación de paquetes puede afectar el rendimiento y la eficacia de la red. La fragmentación de paquetes ocurre cuando el tamaño total de un paquete, incluida la cabecera MPLS y los datos, excede el MTU de un enlace

o dispositivo en el camino de la ruta MPLS. Cuando esto sucede, el paquete debe dividirse en fragmentos más pequeños antes de ser transmitido a través del enlace dispositivo MTU más pequeño. Si un LSR recibe un paquete demasiado grande para ser enviado a la DATA LINK LAYER, el paquete debe ser fragmentado. Cuando pasa el LSR quita el level stak, fragmenta el paquete IP, pone el level stak en cada uno de los segmentos, y envía los segmentos.

Es esencial evitar la fragmentación de paquetes siempre que sea posible, ya que pude tener varios efectos negativos en el rendimiento de la red:

- Sobrecarga de la red
- Aumento de Latencia
- Mayor probabilidad de perdida de paquetes
- Degradación del rendimiento

Para evitar la fragmentación de paquetes en una red MPLS, es importante configurar adecuadamente el MTU en todos los enlaces y dispositivos de la ruta. El MTU debe ajustarse para ser lo suficientemente grande como para acomodar el tamaño de los paquetes MPLS más grandes que se transmitirán en la red sin fragmentación. (Barzola, 2020)

2.4. Virtual Private LAN Service (VPLS)

VPLS es una tecnología de red que trabaja en capa2, permitiendo la conexión entre sí de varias ubicaciones geográficas en una misma LAN, a través de una red de proveedores basada en MPLS, VPLS es utilizada para interconectar redes Ethernet multipunto a multipunto, lo que hace de esta tecnología ideal para extender la LAN a través de infraestructura de red del proveedor de servicios. (Ortiz, 2017)

Una solución VPLS es una red privada virtual (VPN) punto a multipunto basada en Ethernet, Además, VPLS admite la conexión de diferentes tipos de redes, como Ethernet, Frame Relay o ATM, lo que permite la integración de tecnologías existentes en la red VPLS.

Las soluciones VPLS, proporcionan un mayor rendimiento, velocidad de transmisión de datos más rápidas y mayor seguridad. Con VPLS, las organizaciones retienen el control total sobre cómo se enrutan los datos a través de sus redes. (Barzola, 2020)

2.4.1. Propiedades de VPLS

El servicio VPLS tiene algunas propiedades, entre ellas:

- **VPLS** es sumamente seguro para la transmisión de datos, ya que utiliza conectividad entre todos, con opciones de conmutación por error integradas.
- **VPLS** es escalable, permite agregar fácilmente nuevas ubicaciones o dispositivos a la red existente sin la necesidad de realizar cambios significativos en la infraestructura.
- **VPLS** ofrece conectividad transparente entre ubicaciones distintas, no requiere cambios en la configuración de los dispositivos, los dispositivos envían tráfico a la red sin saber que se encuentran conectados en una red virtual de gran tamaño.
- **VPLS** permite un ahorro significativo en enlaces físicos entre ubicaciones diferentes, lo que hace que se reduzcan significativamente los costos. (Barzola, 2023)

2.4.2. Implementación de VPLS

La implementación de VPLS implica el uso de etiquetas y túneles para encapsular el tráfico de datos y enviarlo a través de la red. Los paquetes de datos se etiquetan en el punto de entrada a la red VPLS y se enrutan a través de la WAN utilizando túneles. En

los puntos de salida de la red VPLS, los paquetes se desetiquetan y se entregan a su destino final. (Barzola, 2020)

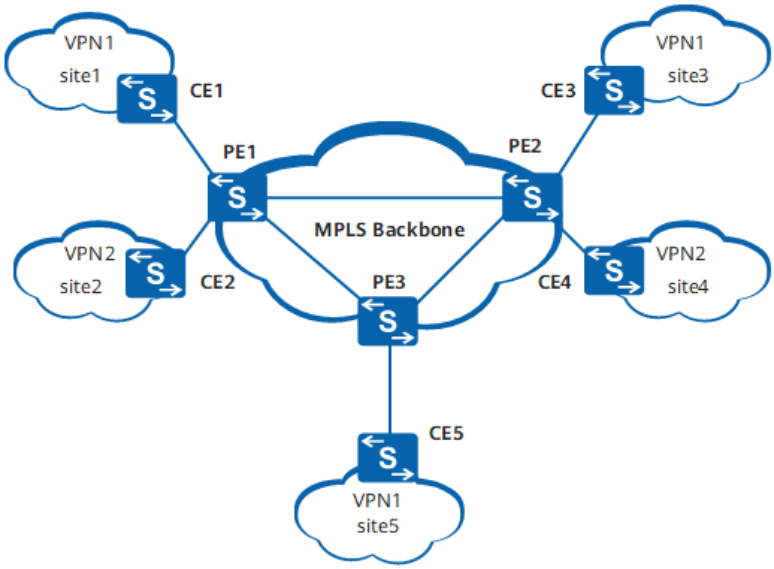
VPLS se implementa para brindar a los hosts remotos una conexión de tipo LAN por medio de VPN. VPLS es compatible con la mayoría de los tipos de conectividad de red, incluidos punto a punto, punto a multipunto, multipunto a multipunto y más. Cuando los usuarios inician sesión en la VPN, se les proporcionan las funciones de una conexión LAN estándar. El VPLS usa una VPN para crear y administrar conexiones y para mover datos de usuarios dentro de la red. Además, el suscriptor puede cambiar de ubicación y aun así conectarse a la LAN virtual. (Goodwin, 2023)

2.4.3. Funcionamiento VPLS

VPLS usa el protocolo de conmutación de etiquetas multiprotocolo para brindar una interfaz o conexión Ethernet a los clientes o suscriptores en una conexión a Internet tal como se muestra en la figura 10, a continuación. (*Level.14,* 2023)

Figura 10.

Arquitectura de VPLS.



Fuente. Extraído de https://forum.huawei.com/enterprise/es/servicio-de-lan-privada-virtual-vpls/thread/667234578588385280-667212883219591168

VPLS implica la transmisión de paquetes de datos mediante protocolos de enrutamiento internos, en lugar de los de un proveedor de servicios. Como resultado, los proveedores de servicios no obtienen visibilidad de información como direcciones IP o rutas de enrutamiento, y las empresas conservan el control total de cómo se transmiten sus datos. Fundamentalmente, esta seguridad adicional viene sin comprometer la velocidad o la latencia. (Barzola, 2023)

Para que VPLS pueda transportar paquetes MPLS, uno de los protocolos de distribución de etiquetas ya debe estar etiquetándose en la red, puede ser LDP o enlaces estáticos. (cisco.com)

Para el caso de uso de BGP como protocolo de descubrimiento VPLS, la red debe ejecutar dicho protocolo como router reflector, para el caso de uso de OSPF se debe inicialmente configurar el direccionamiento de red y OSPF ya debe estar configurado de tal modo que las direcciones de loopback deben estar distribuyéndose en los routers de la red. (Barzola,2020)

2.4.4. Túneles VPLS

La interfaz VPLS puede considerarse de túnel a igual que EoIP, los túneles se establecerán de tal modo que se logre el reenvío transparente del segmento de ethernet entre los sitios del cliente. (Barzola, 2020)

La configuración de cada túnel implica que VPLS se configure en ambos puntos finales del túnel, la negociación entre túneles se realiza mediante LDP, el reenvío de datos en el túnel se produce imponiendo dos etiquetas en los paquetes, etiqueta de túnel y etiqueta de transporte.

Los túneles VPLS se configuran en las interfaces VPLS, VPLS las identifica y deben ser únicos para cada túnel entre este y el peer remoto.

La configuración del túnel VPLS hace que se cree un vecino LDP dinámico y que se establezca una sesión LDP, la sesión de LDP es una sesión que se establece entre dos conmutadores que no son vecinos directos, hay que tener en cuenta que las etiquetas para las rutas IP también se intercambian entre peers VPLS, aunque no exista la posibilidad de que ninguna de ellas sea utilizada.

2.4.5. Bridge VPLS

Los túneles VPLS proporcionan un enlace virtual de Ethernet entre enrutadores. Para conectar en forma transparente dos segmentos físicos de ethernet, se deben unir con el túnel VPLS, en general se usa de la misma manera que con las interfaces EoIP. (Barzola, 2020)

Hay que tener en cuenta que en el bridge no es necesario ejecutar el protocolo SPT, esto dependerá de si existe enlaces o no entre segmentos de un enrutador y de otro, hay que verificar inicialmente si hay el túnel único entre los enrutadores.

Capítulo 3. Requerimientos y diseño de Red

En este capítulo se realizará el levantamiento de información del estado inicial de la red en funcionamiento, además se realizará un plan de mejoras para la migración de la red plana a una nueva diseñada con segmentación e implementación de ruteo dinámico OSPF y VPLS. Todo esto se realizará con la metodología de gestión de proyectos PMBOK.

3.1. Estado Actual.

Mediante el análisis de los requerimientos que se implementaran en el proyecto, así como de los servicios de la red y topología proyectados, habría que tener en cuenta algunos aspectos, puesto que, en la realización de una red o la modificación de una ya existente, hace que se elabore una serie de materiales y o equipos que habría que añadir o remplazar en la topología de red.

Los protocolos de enrutamiento dinámico en especial el OSPF y tecnologías como la VPLS, hacen que cada vez las redes sean más robustas y fiables, añadiendo escalabilidad y seguridad, por lo que es común la implementación de estas tecnologías en las empresas.

Luego de haber levantado la información inicial de la red en funcionamiento se encuentra con lo siguiente:

- Red plana con enlaces entre nodos sin implementación de ruteo de ningún tipo.
- Red sin segmentación.
- Host en un solo dominio de broadcast.
- Loop’s presentes en la red.
- Equipos de capa 2 no administrables en cada nodo como conmutadores.

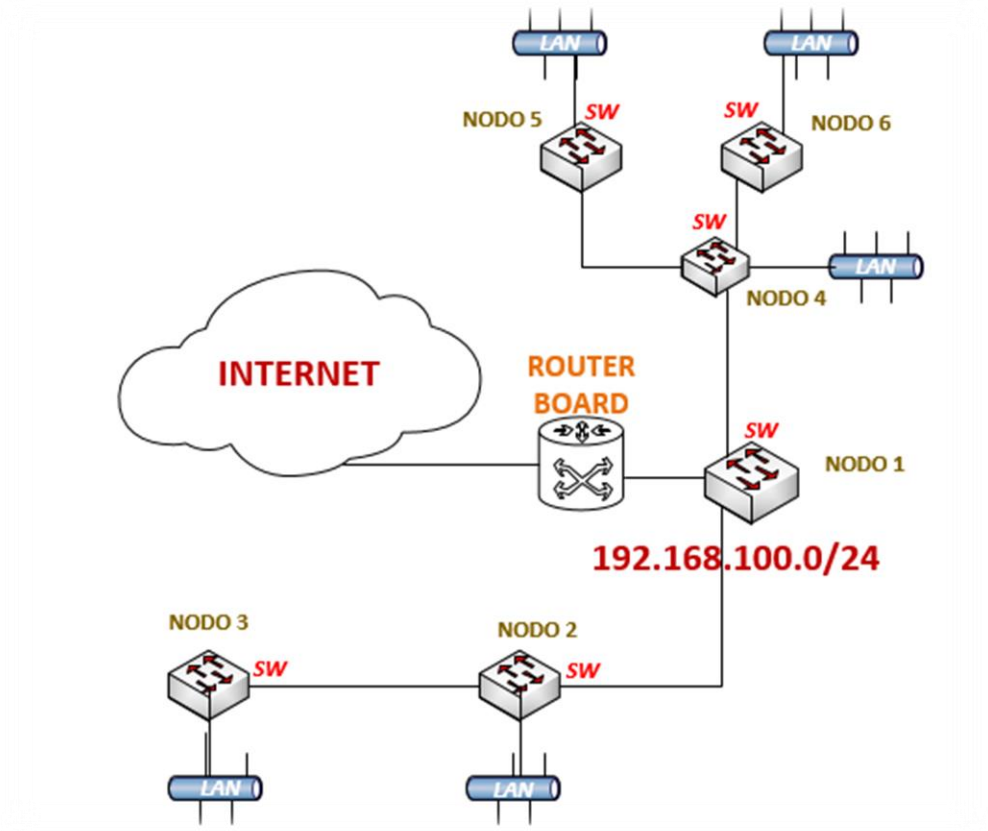
3.1.1. Topología inicial

Para la elaboración de la topología en uso, se recopiló información tanto de equipos y de información lógica con la que actualmente funciona la red, luego de aquello se procedió con el levantamiento de la topología, donde fue evidente que la red en funcionamiento es de tipo PLANO. Esta red está conformada por equipos de conmutación capa2 (switch), mismo que son de tipo ¨no administrable¨, estos están en cada nodo presente y únicamente existe un enrutador instalado, consta como principal y actualmente es el borde de la red.

En el diagrama de la figura 11, se muestra la topología de la red actual de la empresa Mikro-Net SA.

Figura 11.

Diagrama de red actual en funcionamiento.



Fuente. Autoría propia.

3.1.2. Problemas de Software

De acuerdo al estudio realizado, se puede evidenciar que el software actual que se usa para monitoreo y gestión de red es únicamente el OS de mikrotik, mismo que consta o está habilitada en el router board instalado como principal. Al no tener configurado ruteo de ningún tipo ni tecnologías para gestionamiento y monitorización de la red, no hubo la necesidad inicial de instalar equipos capa 3 administrables y mucho menos configurar ruteo dinámico.

3.1.3 Problemas de Hardware.

En cuanto al hardware encontrado se presentan deficiencias en el tipo de equipos usados en la conmutación en cada nodo, al ser una red plana, la red no exigió equipos de capa3 en sus nodos, la implementación que se dio inicialmente se fue en torno a la instalación de equipos capa2 no administrables y en la mayoría de casos los problemas suscitados como inhibición de equipos, latencia y jitter altos en la red fueron a causa de estos equipos.

3.1.4 Problemas Lógicos

En cuanto a problemas lógicos encontrados, los más presentes son las de latencias y jitter altos, además de usuarios con problemas en el uso de aplicaciones sobre internet, dado esta serie de eventos e inconvenientes en muchos casos se presenta perdida notable de información y paquetes. La falta de confiabilidad en la red hizo que la comunicación entre dispositivos dentro de la red no sea eficaz, pues al no haber garantía en la transmisión de datos y fallas constantes en la comunicación, hubo casos de host’s y equipos que resultaron inhibidos causa a loopback’s y paquetes de broadcast difundidos en la red sin control.

3.2. Tabla de Requerimientos

Al diseñar la red, principalmente se debe elegir el tipo de red o tipo de topología que se adapte y más que todo solucione las necesidades de la existente en la organización. Algunas de las decisiones de planificación y requerimientos que se debe tomar están relacionadas con el hardware y software de red, a ello también es necesario enfocarse en puntos específicos como lo son:

- La topología de red, el diseño y las conexiones del hardware de red
- El número de host que admitirá la red y su direccionamiento
- Ancho de banda de las interfaces
- Si necesita puentes o enrutadores que extiendan la red actualmente y a futuro.
- Los tipos de host que admite la red
- Los tipos de servidores que puede necesitar
- El tipo de medio de red que utilizará: Ethernet, Token Ring, FDDI, etc.

Teniendo en cuenta estos factores, podemos determinar el tamaño de la red y los recursos necesarios que conllevan el levantamiento de su funcionamiento. (Oracle, 2011).

Luego de haber realizado el estudio de la red, podemos evidenciar los problemas actuales que presenta, los periféricos que son necesarios serán citados con criterio técnico en base a tablas comparativas que nos guíen a las mejores opciones, con ello se obtendrá una red con excelente desempeño, así como del soporte de cambios en la topología en casos futuros.

En la tabla 3 a continuación, se detallará los requerimientos importantes que son necesarios para la nueva red, dichos requerimientos se citaran en torno a la implementación del ruteo dinámico OSPFv2 y VPLS.

Tabla 3

Requerimientos necesarios para la red.

REQUERIMIENTO	DESCRIPCIÓN
TOPOLOGIA	Funcional y Escalable para mejorar la arquitectura de red
DIRECCIONAMIENTO	Uso de VLSM, redes y subredes para enlaces PTP y LAN
SOFTWARE	Debe soportar la configuración de OSPFv2 y VPLS
HARDWARE	Equipos de tipo Administrable en cada nodo (Enrutadores) e interfaces con ancho de banda considerable.

Fuente. Autoría Propia

Los objetivos de las redes se enfocan en dos aspectos principales: compartir recursos y proporcionar un medio de comunicación eficaz entre hosts. Esto implica garantizar que todos los programas, datos y equipos estén accesibles para cualquier usuario de la red, sin importar la ubicación del recurso ni del usuario. Por esto, en la tabla 4, se ha resumido los requerimientos mínimos de ancho de banda necesarios para diferentes aplicaciones o servicios que pueden cursar en la red.

Tabla 4

Requerimientos de Ancho de Banda.

APLICACIÓN O SERVICIOS	ANCHO DE BANDA (kbps)	
Internet	678 kbps	Según Espinoza & Álvarez (2011) para uso de internet el ancho de banda mínimo es de 768 kbps
Video conferencia y herramientas colaborativas.	768 kbps	De acuerdo con Espinosa & Álvarez (2011), 768 kbps es el mínimo de ancho de banda para transmisión de video en High Definition
Voz sobre internet	42 kbps	Según, centralip (2023). El ancho de banda mínimo para establecer una comunicación viable suele estar entre los 42 kbps
Otras aplicaciones	1500 kbps	Según CenturyLink (2023), para navegación web general se requiere 1.5 Mbps

Fuente. Autoría Propia

Además del ancho de banda, en la tabla 5, de acuerdo con Espinosa & Álvarez (2011). Se expone los requerimientos de pérdida de paquetes, latencia, jitter y disponibilidad, debido a su influencia directa en la calidad y confiabilidad de las comunicaciones ya que la pérdida de paquetes afecta la integridad de la información transmitida, lo que puede causar retrasos, reenvíos o incluso la corrupción de datos, lo que resulta especialmente crítico en aplicaciones sensibles como la transmisión de voz o video.

La latencia, o el retraso en la transmisión de datos, puede impactar la experiencia del usuario final, siendo crucial en aplicaciones en tiempo real. El jitter, la variabilidad en el retardo de la transmisión puede causar problemas de sincronización y calidad de audio o video.

Finalmente, la disponibilidad es esencial, ya que garantiza que la red esté operativa cuando se la necesita, minimizando tiempos de inactividad que podrían afectar las operaciones comerciales. Cumplir con estos requisitos no solo mejora la eficiencia operativa, sino que también garantiza una experiencia de usuario consistente y confiable en la red.

Tabla 5

Requerimientos de disponibilidad

APLICACIÓN o SERVICIO	LATENCIA	JITTER	PÉRDIDA DE PAQUETES	DISPONIBILADAD
Video conferencia y herramientas colaborativas	BAJA < 150ms	BAJO < 30ms	BAJA < 1%	ALTA
Voz sobre internet	BAJA < 150ms	BAJO < 30ms	BAJA < 1%	ALTA

Sistemas de información y otras aplicaciones (Web, sistemas financieros, control de personal, mail, ftp)	NO CRÍTICO	NO CRÍTICO	NO CRÍTICO	MEDIA

Fuente. Autoría Propia

3.3. Requerimientos necesarios para la nueva red

De acuerdo a los requerimientos citados en la tabla 2, se procederá con el desarrollo y diseño de lo necesario para llegar a cumplir el propósito del proyecto que es la implementación de OSPFv2 y VPLS en la red.

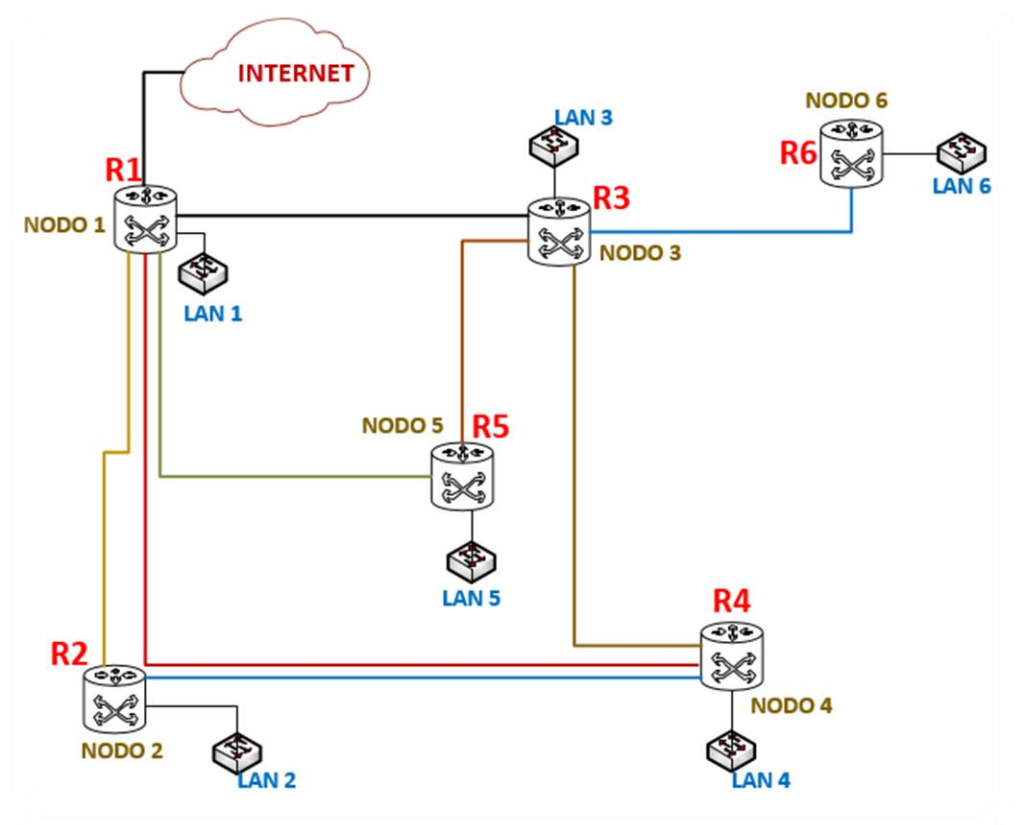
3.3.1. Diseño de nueva topología

La funcionalidad de una red se logra cuando es capaz de soportar cambios de modificación y expansión de nodos sin alterar el diseño, el nuevo diseño tendrá que presentar un esquema que permita un crecimiento flexible en la cantidad de nodos, mismos que tendrán la capacidad de adherirse y soportar los requerimientos que cada nodo presente o la red necesite.

La red se ha diseñado en base lo requerido para el mejoramiento de la arquitectura, en el diagrama de la figura 12 podemos observar cómo queda la topología y los cambios que sufre la misma para lograr eficiencia. Cada nodo constará de un enrutador y de un conmutador, esto con el fin de que cada nodo nos permita la configuración del ruteo dinámico y de la tecnología VPLS.

Figura 12.

Topología general de red actualizada y modificada



Fuente. Autoría propia.

3.4. Plan de mejoras para la migración

La implementación de un plan de mejora nos permitirá realizar un análisis profundo del proceso. Esto con el fin de identificar las deficiencias y problemas que pueden haberse quedado y con ello poder corregir el camino a tiempo.

El plan de mejoras contiene información, métodos y tareas para optimizar los procesos de la migración. Se desarrollará con un enfoque sistemático y estructurado para lograr cambios efectivos y alcanzar el objetivo, de esta manera la empresa Mikro-Net SA podrá seguir este plan elaborado y paso a paso cumplir con el cambio total de su red.

La metodología empleada para la elaboración del plan de mejoras, es la herramienta digital llamada PMBOK, los pasos de esta tecnología fueron claves para la optimización de recursos y de procesos, inicialmente se diseñará la distribución de las

direcciones de red a cada enrutador y segmentos que llevan cada uno, luego se planificará la indagación del software y hardware necesarios para la implementación de las tecnologías requeridas, esto se lo realizara con tablas comparativas entre algunas marcas y fabricantes, en el paso 3 llamado ejecución, se procederá con la implementación del diseño en simuladores, esto hará que tengamos datos mas apegados a la realidad sobre el uso de las tecnologías y protocolos, en este paso se implementan las configuraciones necesarias para el funcionamiento de la nueva red, para que después en el desempeño podamos realizar pruebas y analizar las mejoras y cambios que sufrió la misma. Finalmente se realiza el cierre concluyendo y deduciendo las ventajas y desventajas de la red obtenida.

Una vez elaborado nuestro plan y detallados los pasos a seguir, procedemos con la elaboración de una tabla que nos permita mantener de manera ordenada las tareas en orden a realizar. A continuación, en la Tabla 6, se muestra la tabla del plan de mejoras.

Tabla 6

Plan de mejoras.

DESCRIP_ CION	TAREAS	RESPON_ SABLE	RECURSOS	FINANCIA_ CION	SEGUI_ MIENTO
MIGRACION DE LA RED PLANA A UNA NUEVA DISEÑADA CON TECNOLOGIA VPLS	1. DISEÑAR EL DIRECCIONAMIENTO IP PARA LA RED 2. BUSCAR SOFTWARE Y HARDWARE NECESARIO 3. EMULAR RED NUEVA 4. IMPLEMNTAR PROTOCOLOS Y TECNOLOGIAS A LA RED 5. PROBAR SERVICIOS 6. CONCLUIR LAS TAREAS	1. NOC MIKRONET 2. DEPARTAMENTO ADMINISTRATIVO 3. RECURSOS HUMANOS	HUMANOS, se requiere de una persona capacitada que elabore y se desempeñe en los procesos requeridos sin ningún problema. TECNOLÓGICOS, se requiere del uso de herramientas tecnológicas para el cumplimiento de las tareas.	Todo el presupuesto será designado por la empresa beneficiaria, Mikro-Net SA	El seguimiento del desarrollo del proyecto la llevará a cabo el GERENTE de la empresa Mikro-Net SA en conjunto con encargados del departamento técnico y NOC.

Fuente. Autoría propia.

Una vez elaborado nuestra tabla del plan de mejoras, debemos proseguir con el desarrollo de las tareas tal cual nos muestra la tabla 6, anterior, como la topología de la nueva red ya está definida, procedemos inicialmente con el diseño del direccionamiento y distribución IP para los dispositivos de la red.

3.4.1. Direccionamiento IP

En esta sección, procedemos con el detalle sobre el direccionamiento IP, el cual implica asignar una dirección IP a cada equipo de la red, utilizamos VLSM (Variable Length Subnet Masking) tal como se recomienda en casos de uso de enrutamientos dinámicos.

En este caso particular, al tratarse de una emulación para realizar las pruebas y simulaciones, se han utilizado direcciones IP privadas para toda la red, mismas que están en base a las utilizadas en la red actual.

En líneas generales, la red consta de enlaces que van con conexiones de router a router, básicamente estos son enlaces punto a punto, y enlaces punto a multipunto en cada router como LAN. Para distinguir entre las redes de área local, redes de enlaces y redes para loopbacks, se utilizan direcciones de clase A, clase B y clase C, donde:

- Para las IP loopback de cada router se utilizará un direccionamiento ip clase A.
- Las conexiones de enlaces PTP y PTMP utilizarán un direccionamiento clase B.
- Finalmente, las ips de los clientes serán de direccionamiento clase C.

Considerando las recomendaciones anteriores citadas en el capitulo2, se ha aplicado la técnica de VLSM (Variable Length Subnet Masking), de acuerdo a esto se ha elaborado y organizado las direcciones IP en la red tal como se muestra en la Tabla 7, a continuación.

Tabla 7

Distribución de direcciones IP completa para la emulación de la red

DESC.	TIPO	RED	IP INICIAL	IP FINAL	BROADCAST
R1	LO	10.0.0.1/32			
R2	LO	10.0.0.2/32			
R3	LO	10.0.0.3/32			
R4	LO	10.0.0.4/32			
R5	LO	10.0.0.5/32			
R6	LO	10.0.0.6/32			
R1 LAN	PTMP	172.16.20.0/24	172.16.20.1	172.16.20.254	172.16.20.255
R2 LAN	PTMP	172.16.21.0/24	172.16.21.1	172.16.21.254	172.16.21.255
R3 LAN	PTMP	172.16.22.0/24	172.16.22.1	172.16.22.254	172.16.22.255
R4 LAN	PTMP	172.16.23.0/24	172.16.23.1	172.16.23.254	172.16.23.255
R5 LAN	PTMP	172.16.24.0/24	172.16.24.1	172.16.24.254	172.16.24.255
R6 LAN	PTMP	172.16.25.0/24	172.16.25.1	172.16.25.254	172.16.25.255
R1-R2	PTP	172.16.26.0/29	172.16.26.1	172.16.26.6	172.16.26.7
R1-R3	PTP	172.16.26.8/29	172.16.26.9	172.16.26.14	172.16.26.15
R1-R4	PTP	172.16.26.16/29	172.16.26.17	172.16.26.22	172.16.26.23
R1-R5	PTP	172.16.26.24/29	172.16.26.25	172.16.26.30	172.16.26.31
R2-R4	PTP	172.16.26.32/29	172.16.26.33	172.16.26.38	172.16.26.39
R3-R4	PTP	172.16.26.40/29	172.16.26.41	172.16.26.46	172.16.26.47
R3-R5	PTP	172.16.26.48/29	172.16.26.49	172.16.26.54	172.16.26.55
R3-R6	PTP	172.16.26.56/29	172.16.26.57	172.16.26.62	172.16.26.63

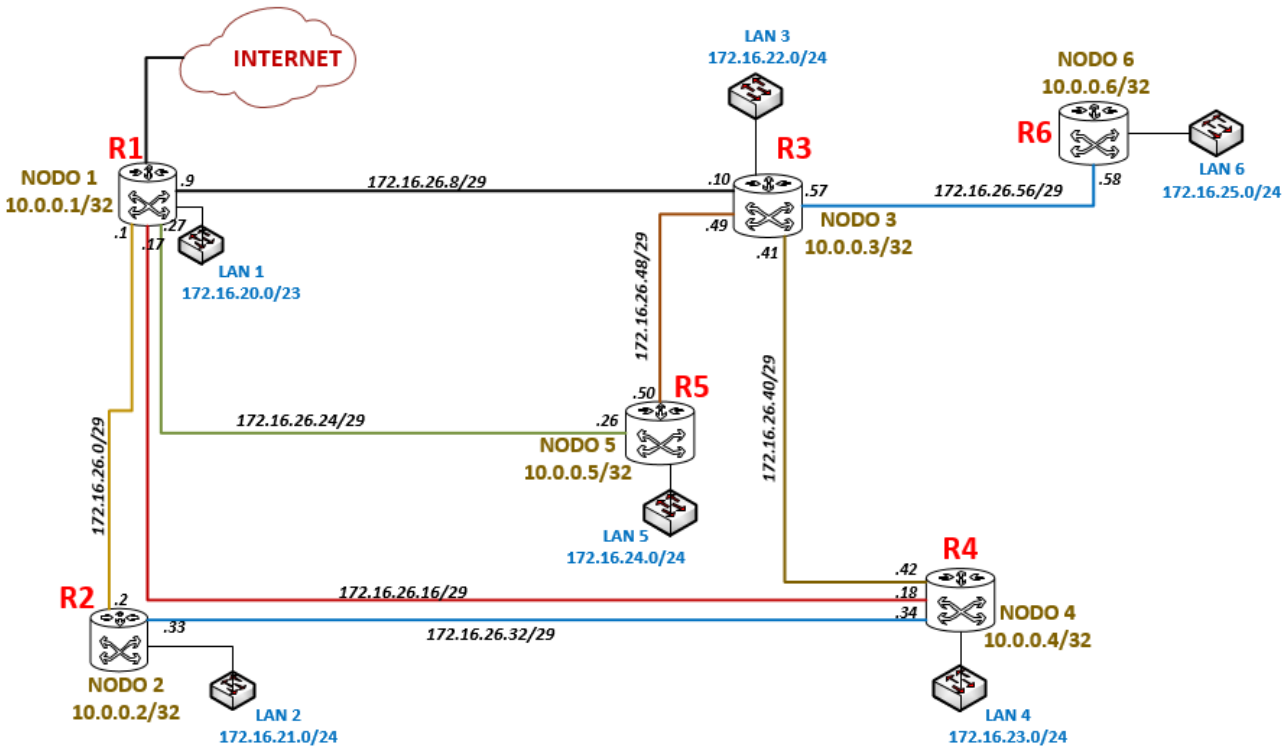
Nota. El tipo “LO”, hace referencia a una interfaz loopback. *Fuente.* Autoría propia.

Una vez definida la parte del direccionamiento IP, tal como se evidencia en ala tabla 7 anterior, procedemos con la asignación de dirección IP a cada router y enlace PTP así como también de las LAN que requieran de dirección IP, además deben distribuirse los ID de cada router, el siguiente paso será la asignación de las direcciones de red a cada dispositivo en la topología.

En la figura 13 podemos observar el direccionamiento empleado y las distintas redes y subredes aplicadas en la topología.

Figura 13.

Topología de red con direccionamiento IP



Fuente. Autoría Propia

3.4.2. Hardware

Para determinar la opción de hardware más adecuada, es necesario considerar los requisitos y los problemas previamente suscitados.

En lo que respecta al hardware, se optará por seleccionar entre tres fabricantes los cuales son: Cisco, MikroTik y Juniper, además de usar IOS de routers reales para las emulaciones, con esto lograremos que la simulación sea lo más cercano a la realidad posible, inicialmente se buscará una imagen ISO de un proveedor que satisfaga las necesidades presentadas para la reingeniería de la red. Estas imágenes desempeñarán la función tanto en la simulación como en la implementación con equipos reales cuando esta sea necesaria.

Durante el proceso de elección del hardware, se evaluaron diversas opciones disponibles en el mercado. De entre estas opciones, se seleccionaron tres que mejor se adecuan a las necesidades del sistema.

Las imágenes de los sistemas operativos de Cisco, MikroTik y Juniper son comúnmente preferidas para emulaciones en GNS3 debido a su amplio uso en el mundo de las redes y la diversidad de funcionalidades que ofrecen.

En el caso de las IOS de Cisco, son altamente demandadas debido a la predominancia de los dispositivos Cisco en entornos de red empresariales, lo que hace que la familiaridad con sus sistemas operativos sea fundamental. Esto permite a los profesionales de redes practicar configuraciones, pruebas y escenarios de red en un entorno simulado antes de implementar en la red real.

Por otro lado, MikroTik y Juniper son opciones valiosas para emulaciones debido a sus respectivas presencias en diferentes ámbitos de red. Las imágenes de RouterOS de MikroTik son populares entre proveedores de servicios de internet y en entornos de redes de pequeñas y medianas empresas. Mientras que JunOS de Juniper es común en redes de operadores, centros de datos y entornos de empresas donde se buscan soluciones de enrutamiento y conmutación avanzadas.

En la tabla 8 se toma en cuenta cinco requerimientos principales, para la selección del Hardware a usar. Posteriormente, se evalúa cada una de estas, considerando los requerimientos expuestos en el apartado 3.2. Posteriormente se indica cuál fue el elegido y se proporciona los argumentos que respaldan esta decisión.

Tabla 8.

Selección de marca de hardware

FABRICANTE	REQUERIMIENTOS					VALORACIÓN
	SOPORTA OSPFv2	SOPORTA MPLS y VPLS	SOFTWARE DISPONIBLE PARA EMULACIÓN	COSTO	INTERFAZ FÁCIL DE USAR	
CISCO	1	1	1	0	1	**4**
MIKROTIK	1	1	1	1	1	**5**
JUNIPER	1	1	1	0	0	**3**

Nota. *1 Sí cumple, y 0 No cumple. Para el costo; "0" para el caso de costoso, y "1" para el caso de económico.*

Fuente. Autoría propia.

La elección nos lleva hacia el fabricante MikroTik con su sistema (RouterOS), esta elección se da de acuerdo que esta marca cumple con la valoración más alta en la comparativa frente a otros fabricantes, solo por encima de la marca CISCO, además de cumplir con los requisitos tanto para la emulación como para cuando se dé la implementación en la red física.

La marca elegida nos permite escoger entre una gran variedad de dispositivos entre software y hardware de acuerdo los recursos que la red requiera, para nuestro caso de diseño evaluaremos los requerimientos mínimos necesarios para que en un dispositivo funcione sin problemas el ruteo dinámico OSPv2, MPLS y VPLS respectivamente, para esto se tomara tres modelos de equipos MikroTik en base a los más comunes y disponibles en el mercado local.

Inicialmente hay que tener en cuenta que; OSPF consume un gran número de CPU y memoria debido al algoritmo SPF y al mantenimiento de múltiples copias de información de enrutamiento al ser un protocolo más complejo de implementar en comparación con RIP. (Excalante,2016)

A partir de lo mencionado anteriormente, los requerimientos mínimos de la marca respecto al uso de las tecnologías a emplear son detallados en la tabla 9 a continuación.

Tabla 9.

Requerimentos básicos de cada protocolo.

	REQUERIMIENTOS		
PROTOCOLO	**MEMORIA RAM MINIMA REQUERIDA**	**VELOCIDAD DE CPU MINIMO REQUERIDO**	**ESTANDARES REQUERIDOS**
OSPF	64Mb	400MHz	RFC2328
MPLS	128Mb	500MHz	RFC3031
VPLS	128Mb	500MHz	RFC4761

Fuente. Autoría propia.

Una vez conocidos los recursos tanto de memoria RAM como de CPU necesarios para que funcionen las tecnologías a emplear, realizamos la comparativa entre modelos de la marca MikroTik que se sujetan y aproximan a las características necesarias para que nuestra red tenga el desempeño y el funcionamiento requerido.

A continuación, en la tabla 10, se muestra una comparativa entre tres modelos de Router Board de 4 núcleos, con el fin de encontrar el adecuado y que más se apegue a los requerimientos.

Tabla 10.

Selección de modelo de hardware

MODELO	**ESPECIFICACIONES**					
	MEM. RAM	**MEM. ROM**	**VELOCIDAD DE INTERFAZ**	**NUMERO DE INTERFACES**	**ARQUITECTURA DE PROCESADOR**	**PRECIO ESTIMADO**
RB1100AHx4	1Gb	128Mb	1G	13xEthernet	ARM 32bit 1,4 GHz	**$380.00**
CCR2004-16	4Gb	128Mb	1G, 10G	16xEthernet 2x10G SFP	ARM 64bit 1700MHz	**$465.00**
RB 4011RM	1Gb	512Mb	1G	10xEthernet 1x1G SFP	ARM 32bit 1900MHz	**$219.00**

Fuente. *Autoría propia.*

La elección se ha dado teniendo en cuenta que para el nodo principal (NODO 1) ya existe un equipo R1 de marca MikroTik modelo RB1100AHx4 dude edition, dado esto se toma como mejor opción el modelo RB 4011RM para los enrutadores R2, R3, R4, R5 y R6, teniendo en cuenta que los requerimientos de procesamiento y cantidad de memoria RAM para que funcione correctamente el OSPFv2 y VPLS se describieron en la tabla 7.

3.4.3. Software

Al ser elegido MikroTik como marca a usar en hardware, el software que por defecto se usará es OS de MikroTik llamado RouterOS, este software o sistema operativo y sus actualizaciones y paquetes extra de la marca MikroTik, está disponible para descargas en la página web oficial, misma que consta con versiones inclusive que son compatibles con procesadores de computador tanto para arquitecturas x86 y x64.

A continuación, en la tabla 11, se muestra una comparativa entre RouterOS de mikrotik y otros dos tipos de software, en este caso IOS de CISCO y Junos OS de JUNIPER. El fin de la comparativa es destacar el uso del sistema elegido con características validas y funcionales que nos servirán para la implementación de las configuraciones requeridas.

Tabla 11.

Comparación entre softwares.

NOMBRE	**CARACTERISTICAS**					**VALORACIÓN**
	FABRICANTE	**SOPORTA OSPFv2**	**SOPORTA MPLS**	**INTERFAZ FÁCIL DE USAR**	**SOFTWARE DISPONIBLE PARA SIMULACIÓN**	
RouterOS	MikroTik	1	1	1	1	**5**
IOS	Cisco	1	1	0	1	**4**
Junos OS	Juniper	1	1	0	1	**4**

Nota. 1 Sí cumple, y 0 No cumple

Fuente. Autoría propia.

En conclusión, RouterOS de MikroTik es el adecuado para la adecuación y la implementación, esto debido a que en la comparativa presenta más beneficios en características por así decirlo, dado que en las implementaciones físicas marcas como CISCO y JUNIPER son más costosas debido a su alto desempeño y predominancia, siendo CISCO más recomendado para ámbitos empresariales y JUNIPER para uso en centros de datos con conmutación avanzada.

La elección se da por el software que nos presenta MikroTik, con ello nos permitirá las funcionalidades requeridas para la emulación, y en caso de implementación física se adecúa sin problemas con una alta variedad de equipos que en relación con otras marcas son más económicas.

MikroTik presenta herramientas de software para gestión y monitorización de red, el caso más común es THE DUDE, una aplicación dedicada a la ayuda en tareas de monitoreo simplificando tareas y siendo de gran ayuda para la gestión a la red, este programa puede encontrarse en la página oficial de MikroTik y debe descargarse de acuerdo a la arquitectura de los recursos del equipo o dispositivo hardware en el que se lo vaya a instalar.

En la tabla 12, a continuación, se presenta algunas de las características comparativas entre DUDE y otros tipos de software dedicados a la gestión, administración y monitorización de la red.

Tabla 12.

Comparación de software de monitoreo y gestión de red

NOMBRE	ESPECIFICACIONES					
	MEMORIA RAM MINIMA NECESARIA	**MEMORIA ROM MINIMO NECESARIO**	**MARCA PROPIETARIA**	**COMPATIBILIAD MULTIMARCA**	**NOTIFICACIONES**	**COSTO**
THE DUDE	512Mb	16Mb en el Rb y 16Gb en USB o SD	MikroTik	SI	SI	**GRATIS**
PRTG	512Mb	50Mb	PAESSLER	SI	SI	**SI, BAJO**
NAGIOS	1Gb	8Gb	NAGIOS	SI	SI	**SI, ALTO**

Fuente. Autoría propia.

Luego del análisis comparativo entre estos tres softwares de monitorización, se elige THE DUDE propiedad de MikroTik, debido a la gran variedad de funciones y principalmente porque es software de tipo GRATUITO, existe modelos específicos de la marca que vienen con los recursos necesarios para que se habilite y se pueda usar las funciones de THE DUDE, una muestra de ello es el Router Board modelo Rb1100AXH4 Dude-Edition, un equipo con grandes recursos para llevar a cabo las funciones de monitorización en la red además de su desempeño con funciones de enrutador y conmutador de acuerdo a lo que la red requiera.

Una de las características destacadas de esta marca, es que la configuración se la puede realizar a través de la interfaz gráfica, esta ofrece una amplia gama de funciones que son relevantes para su implementación, incluyendo la capacidad de configurar protocolos de enrutamiento como OSPF y la configuración de MPLS en entornos físicos y simulados.

Finalmente, MikroTik es conocido por su asequibilidad siendo una opción popular en entornos donde se busca una solución de red rentable. Su versatilidad y costos accesibles hacen que sea una opción atractiva para aprender y experimentar con cualquier protocolo de enrutamiento dinámico en emulaciones.

Para la elección del software que nos permita realizar la emulación, analizaremos en la tabla 13, las posibles características de dos populares programas que nos permitan trabajar con las imágenes tipo ISO de los OS que vamos a usar, a continuación, una breve comparación entre estos tipos de software comúnmente usados:

Tabla 13.

Comparación entre softwares para emulación.

NOMBRE	**CARACTERISTICAS**				
	FABRICANTE	**COSTO**	**SOPORTA RouterOS**	**TRABAJA CON VIRTUALIZACION**	**INTERFAZ FÁCIL DE USAR**
GNS3	SolarWinds	gratuito	1	1	1
P TRACERT	Cisco	gratuito	0	0	1

***Nota**. 1 Sí cumple, y 0 No cumple*

Fuente. Autoría propia.

El software Cisco Packet Tracer es de distribución pagada y está diseñada específicamente para dispositivos Cisco, que a nivel CCNA es suficiente ya que permite emular topologías físicas y lógicas de forma profesional, pero en nuestro caso necesitamos que el emulador funcione con virtualización y uso del OS de MikroTik.

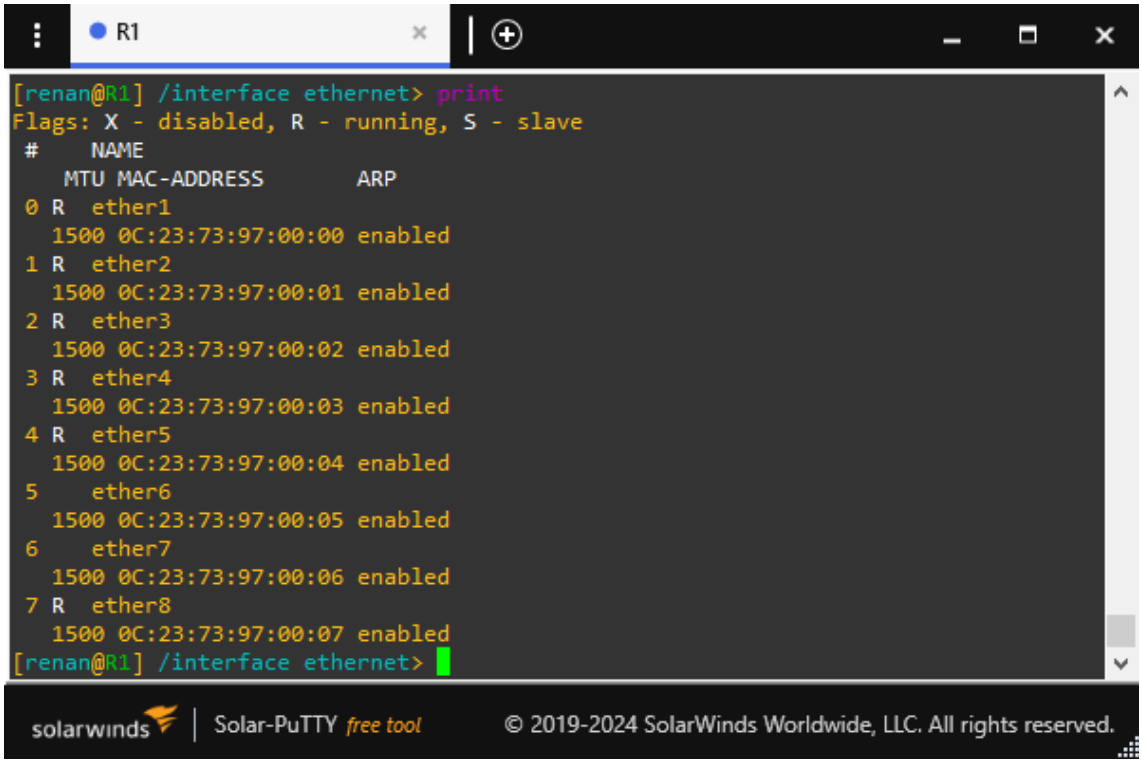
La interfaz gráfica de GNS3 facilita la creación y administración de topologías complejas, ofreciendo un entorno robusto para simular, probar y aprender sobre implementaciones como MPLS y VPLS en una amplia variedad de contextos de red. Por estas razones, se ha seleccionado GNS3 para el desarrollo de la emulación de la topología de red y las tecnologías que esta conlleva.

3.4.4. Configuraciones Lógicas

En las configuraciones lógicas se dará inicio con las configuraciones básicas en cada enrutador, estas consisten en la asignación de las direcciones IP a cada interfaz, bridge o segmento según corresponda, en la figura 14 podemos evidenciar que las interfaces se encuentran conectadas (modo running), el primer paso será darles un nombre o identificativo a cada interfaz, en este caso vamos a colocar el nombre en base al enrutador al cual se conecta la interfaz, por ejemplo: la interfaz Ether1 será designada para el ingreso de internet, la Ether2 será la conexión hasta el enrutador R2 y así sucesivamente.

Figura 14.

Visualización de interfaces enrutador R1



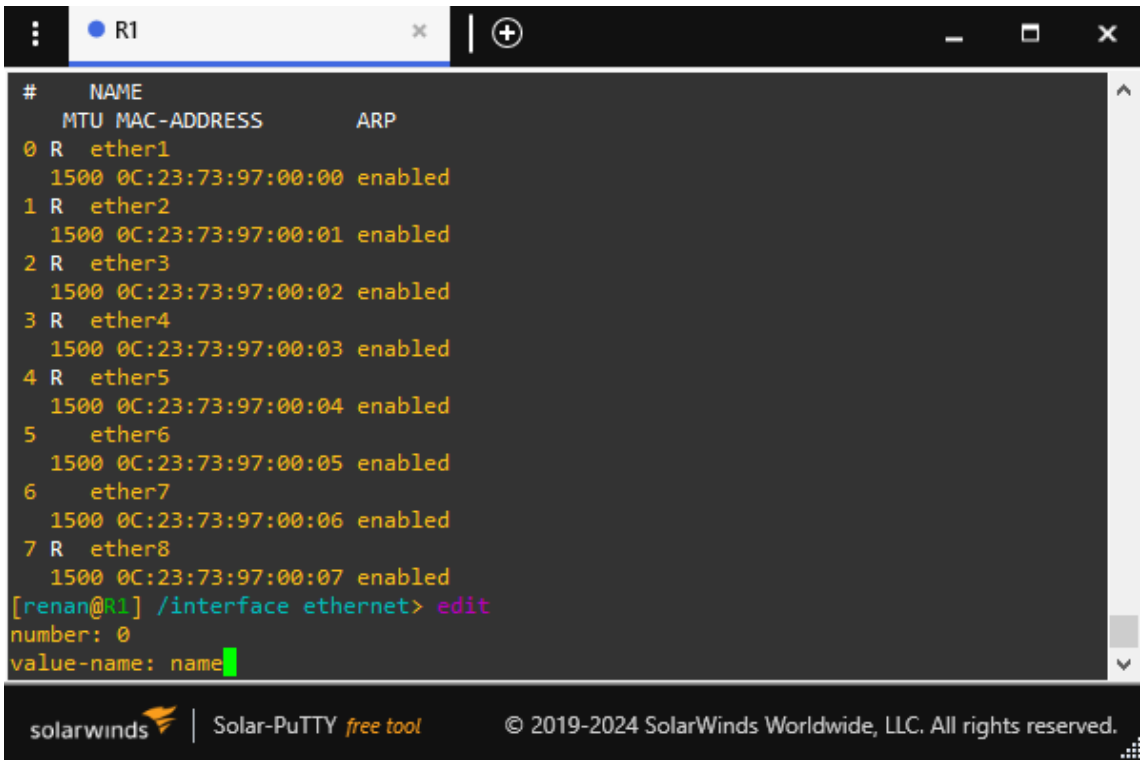
Fuente. GNS3

Una vez visualizadas e identificadas las interfaces, procedemos a editar los nombres de cada una de ellas, este proceso es opcional, para es caso lo haremos con el fin

de tener un mejor registro de las interfaces para que no haya confusión, el comando de configuración se la detalla en la figura 15 a continuación:

Figura 15

Comando para renombrar a interfaz en R1

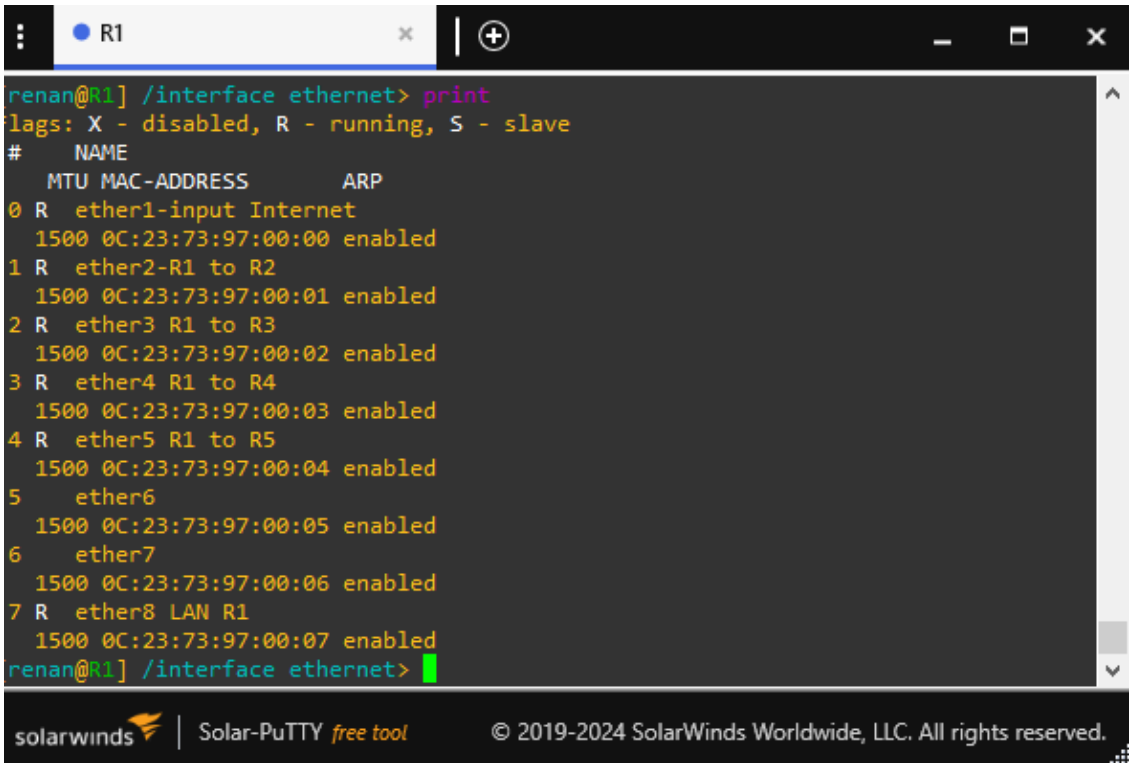


Fuente. GNS3

Ya renombradas o identificadas las interfaces, hacemos un ‘’print’’ o captura de las interfaces para ver nuestras interfaces con el identificativo que fue colocado anteriormente tal como podemos evidenciar en la figura 16 a continuación.

Figura 16

Visualización de interfaces y sus nombres.



Fuente. GNS3

El siguiente paso es crear la interfaz de loopback, para esto crearemos un bridge y lo nombraremos como ‘’loopback’’ o simplemente ”lo”, esta interfaz es importante y obligatoria crearla, independientemente del nombre que esta lleve, esta llevara la ip de loopback la cual será el identificativo “ID” de cada router, para el caso de versiones de RouterOS 6.x la interfaz se crea en un bridge simple, si la versión del RouterOS es 7.x, no es necesario crear la interfaz o crear el bridge ya que en estas versiones de firmware viene una interfaz lógica por defecto llamada “lo”.

Como en nuestra simulación estamos trabajando con versión de firmware 6.49.8, vamos a crear nuestro bridge y este será la que funcione como interfaz de loopback, tal como podemos evidenciar en la figura 17 a continuación.

Figura 17

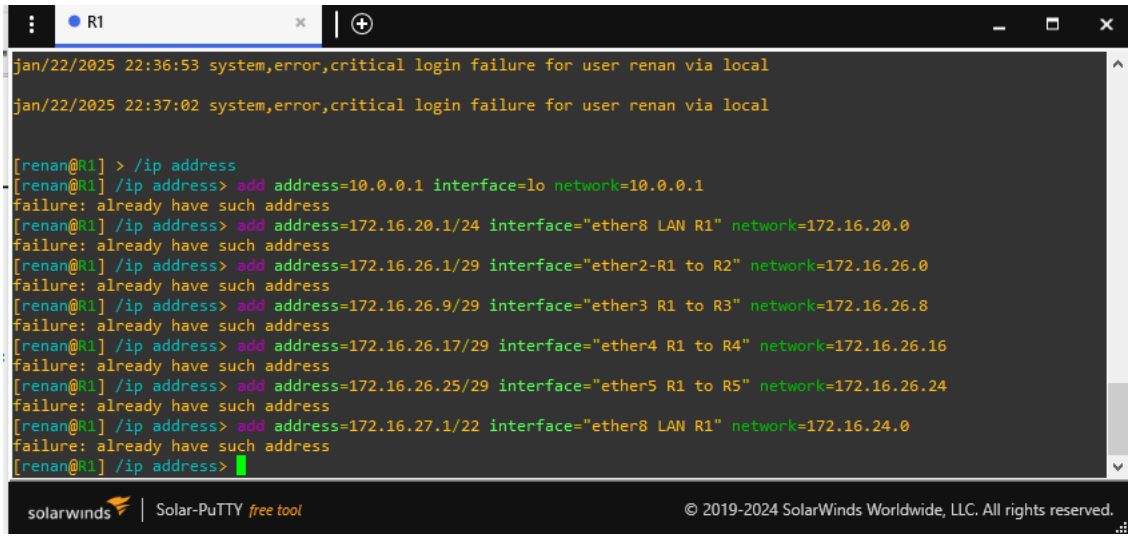
Creación de interfaz loopback en enrutador R1

Fuente. GNS3

Una vez creada la interfaz de loopback nos queda como pendiente insertar y distribuir las direcciones IP en cada interfaz según correspondan, para esto nos basaremos en la tabla 6 y para más seguridad también en la topología tal como podemos evidenciar en la figura 18 a continuación. En el anexo A, podemos observar los direccionamientos IP de los demás enrutadores.

Figura 18

Comando para asignación de Ip's a las interfaces.

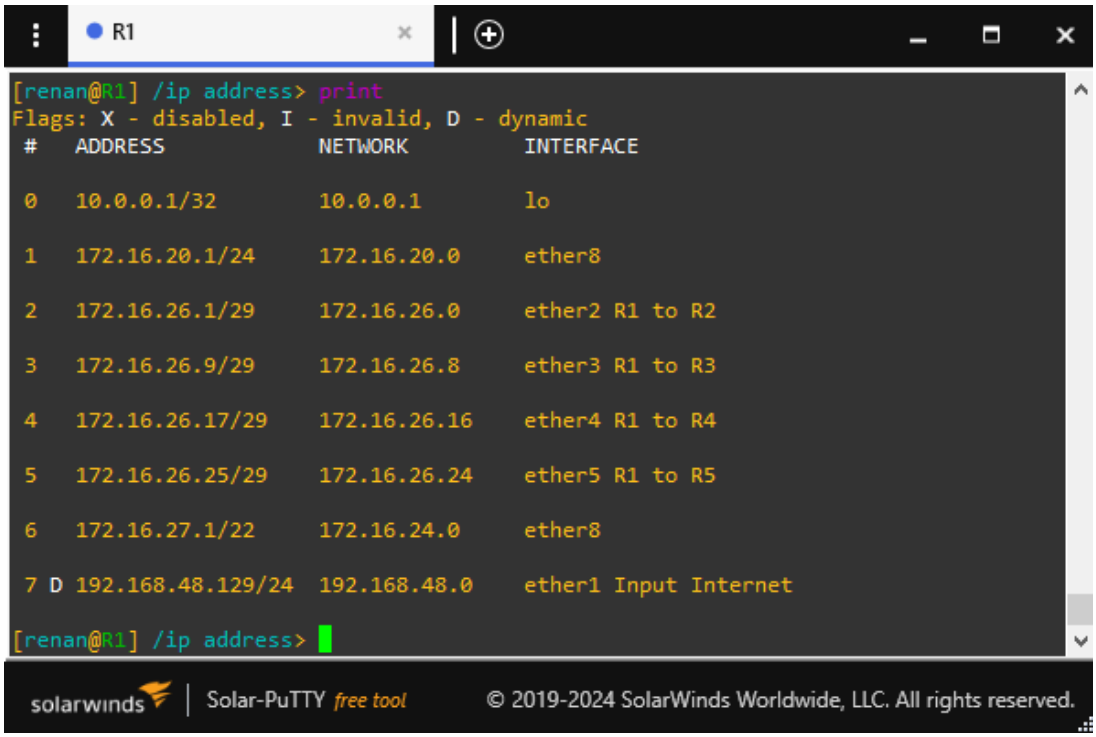


Fuente. GNS3

Finalmente, en la figura 19 a continuación, vamos a comprobar si las direcciones de red se insertaron de manera correcta y a la interfaz correcta.

Figura 19

Visualización de interfaces con sus respectivas direcciones ip en R1



Fuente. GNS3

Una vez finalizadas estas configuraciones lógicas en todos los enrutadores, el siguiente paso será la implementación del protocolo de enrutamiento y de las tecnologías necesarias. Las configuraciones lógicas de las interfaces de los demás routers están mostradas en el Anexo A.

Capítulo 4. Emulación y Funcionamiento

En este capítulo, se procede con la etapa de "implementación", donde se simula una red con los protocolos mencionados anteriormente, en base a la diseñada en el capítulo III, para posteriormente monitorear la misma. En primer lugar, se explica el desarrollo inicial de la implementación, las configuraciones iniciales que consisten en la verificación de enlaces e interfaces, su distribución de direcciones de red para posteriormente iniciar con el levantamiento de protocolos y tecnologías a emplear, al finalizar se dará las pruebas de funcionamiento y adyacencia de los dispositivos de red, es importante recalcar que este proyecto está enfocado a soluciones para adaptación de infraestructuras y a cubrir las necesidades de gestión de red de las empresas.

4.1. Desarrollo de la Emulación.

En esta sección se detalla con precisión la configuración de cada equipo, de manera que se ajuste al funcionamiento deseado en la red. Cabe recalcar que la simulación se realizó en un computador que contiene las características detalladas en la tabla 14 que se presenta a continuación, por ello las pruebas y resultados obtenidos pueden variar ligeramente de acuerdo con las prestaciones del pc.

Tabla 14.

Características del computar usado en la emulación con GNS3.

DESCRIPCIÓN	CARACTERISTICAS
Procesador	CPU Intel core i7/ 4 cores
Memoria RAM	12Gb
Almacenamiento	SSD 480Gb, 200Gb disponibles
Sistema Operativo	Windows 10 Pro X64

Fuente. Autoría propia.

Para la emulación se opta por el software GNS3, debido a que podemos simular con OS de los routers originales, dando un mejor apego a la realidad.

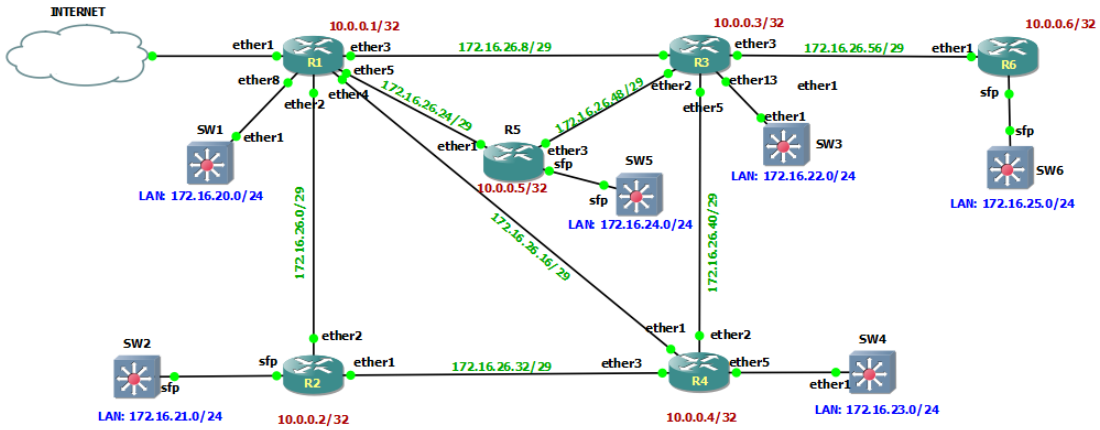
De igual forma tal y como se realiza la configuración con los equipos físicos, se iniciará con las configuraciones en el siguiente orden: primero se levantará la topología en el emulador, luego se levantan las interfaces, una vez lista y definida la topología, se añadirá las direcciones IP a las interfaces en cada router según correspondan, para posteriormente proceder con la configuración OSPFv2 para finalmente implementar el VPLS y MPLS.

Si la configuración de varios dispositivos es similar, se proporciona únicamente el detalle de uno de ellos. El resto de las configuraciones están expuestas en el anexo A, B, C, D, según corresponda.

En la figura 20, a continuación, se muestra la configuración y levantamiento de la topología en el emulador.

Figura 20.

Topología de red en GNS3 con direccionamiento IP.



Fuente. Desarrollada por el autor en GNS3

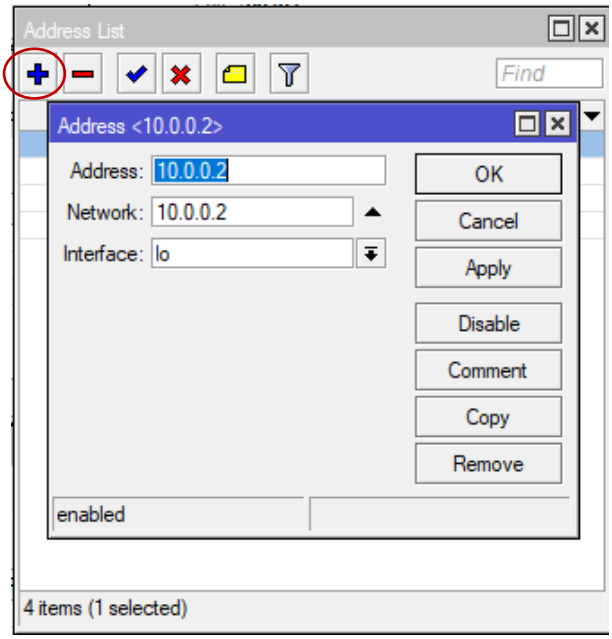
4.1.1. Configuración de Puertos

Inicialmente se configura un direccionamiento a una interfaz loopback, este paso ya se lo realizó en las configuraciones lógicas iniciales, la misma configuración deberá

realizarse en los demás routers, la dirección de red es sin asignación a puerto físico sino a un puente bridge antes creado, esta vez lo haremos usando la interfaz gráfica de MikroTik a través de WinBox, como se muestra en la figura 21.

Figura 21.

Configuración direccionamiento loopback router usando WinBox.



Fuente: WinBox

4.1.2. Configuración de rutas OSPFv2

Para establecer la configuración de enrutamiento OSPF se debe activar dicha opción, esto se realiza en la sección de Routing/OSPF/INSTANCE si es el caso de configuración mediante interfaz gráfica, aquí inicialmente se colocará el identificador del enrutador, para el caso del enrutador R1, el ID es la ip de loopback antes creada que en este enrutador sería: 10.0.0.1/32.

En la figura 22 a continuación, configuraremos el Router ID con el siguiente comando:

Figura 22.

Configuración ID OSPF del enrutador R1

```
[renan@R1] > /routing ospf instance
[renan@R1] /routing ospf instance> set [ find default=yes ] redistribute-connected
=as-type-1 router-id=10.0.0.1
[renan@R1] /routing ospf instance>
```

Fuente: WinBox

El siguiente paso es la configuración y asignación de las redes, esto se lo realiza en el apartado Routing/OSPF/Networks, donde se colocan las redes directamente conectadas al enrutador, la figura 23 a continuación, muestra las redes 172.16.26.0/29, 172.16.26.16/29 y 172.16.26.24 ya que son las redes que participan en OSPF del enrutador R1.

Figura 23.

Asignación de direcciones de red en OSPF para el enrutador R1

```
[renan@R1] > /routing ospf network
[renan@R1] /routing ospf network> add area=backbone network=172.16.26.0/29
[renan@R1] /routing ospf network> add area=backbone network=172.16.26.8/29
[renan@R1] /routing ospf network> add area=backbone network=172.16.26.16/29
[renan@R1] /routing ospf network> add area=backbone network=172.16.26.24/29
[renan@R1] /routing ospf network>
```

Fuente: WinBox

Una vez realizadas estas configuraciones en todos los enrutadores involucrados en la red, habría que revisar las tablas de enrutamiento para verificar si el OSPF está en funcionamiento, además podemos revisar la tabla y lista de LSA en la red, así como de los vecinos “Neighbor” que mostraron adyacencia en la red.

Para esto iniciamos revisando la tabla de enrutamiento general del enrutador tal como se describe en la figura 24.

Figura 24.

Revisión de tabla de enrutamiento general en el enrutador R1

```
[renan@R1] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  10.0.0.1/32        10.0.0.1        lo                        0
 1 ADo  10.0.0.2/32                        172.16.26.2             110
 2 ADo  10.0.0.3/32                        172.16.26.10            110
 3 ADo  10.0.0.4/32                        172.16.26.18            110
 4 ADo  10.0.0.5/32                        172.16.26.26            110
 5 ADo  10.0.0.6/32                        172.16.26.10            110
 6 ADC  172.16.20.0/24     172.16.20.1     ether8 LAN R1             0
 7 ADo  172.16.21.0/24                     172.16.26.2             110
 8 ADo  172.16.22.0/24                     172.16.26.10            110
 9 ADo  172.16.23.0/24                     172.16.26.18            110
10 ADo  172.16.24.0/24                     172.16.26.26            110
11 ADo  172.16.25.0/24                     172.16.26.10            110
12 ADC  172.16.26.0/29     172.16.26.1     ether2 R1 to R2           0
13 ADC  172.16.26.8/29     172.16.26.9     ether3 R1 to R3           0
14 ADC  172.16.26.16/29    172.16.26.17    ether4 R1 to R4           0
15 ADC  172.16.26.24/29    172.16.26.25    ether5 R1 to R5           0
16 ADo  172.16.26.32/29                    172.16.26.18            110
                                           172.16.26.2
17 ADo  172.16.26.40/29                    172.16.26.10            110
                                           172.16.26.18
18 ADo  172.16.26.48/29                    172.16.26.10            110
                                           172.16.26.26
19 ADo  172.16.26.56/29                    172.16.26.10            110
20 ADC  192.168.48.0/24    192.168.48.129  ether1 Input In...        0

[renan@R1] >
```

Fuente: WinBox

Podemos observar en la figura 24 anterior, que en la tabla de enrutamiento nos muestra las redes alcanzadas, sin nos fijamos detenidamente podemos evidenciar redes sumarizada, esto dado a que usamos VLSM, además que las rutas alcanzadas a través del OSPF están señaladas con Flags (las letras “ADo”), que significa que la red se encuentra conectada, es de tipo dinámica y esta funcionado a través de OSPF.

Para corroborar las rutas y redes alcanzadas, vamos a revisar la tabla de enrutamiento de OSPF, con esta revisión de rutas podemos saber datos más detallados de las rutas alcanzadas tales como: costo, estado e interfaz por la cual fue alcanzada dicha ruta, a continuación, visualizamos las rutas en la figura 25.

Figura 25.

Revisión de tabla de rutas de OSPF en el enrutador R1

```
[renan@R1] > routing ospf route print
 # DST-ADDRESS        STATE          COST                    GATEWAY         INTERFACE
 0 10.0.0.1/32        imported-ext-1 20
 1 10.0.0.2/32        ext-1          30                      172.16.26.2     ether2 R1 to R2
 2 10.0.0.3/32        ext-1          30                      172.16.26.10    ether3 R1 to R3
 3 10.0.0.4/32        ext-1          30                      172.16.26.18    ether4 R1 to R4
 4 10.0.0.5/32        ext-1          30                      172.16.26.26    ether5 R1 to R5
 5 10.0.0.6/32        ext-1          40                      172.16.26.10    ether3 R1 to R3
 6 172.16.20.0/24     imported-ext-1 20
 7 172.16.21.0/24     ext-1          30                      172.16.26.2     ether2 R1 to R2
 8 172.16.22.0/24     ext-1          30                      172.16.26.10    ether3 R1 to R3
 9 172.16.23.0/24     ext-1          30                      172.16.26.18    ether4 R1 to R4
10 172.16.24.0/24     ext-1          30                      172.16.26.26    ether5 R1 to R5
11 172.16.25.0/24     ext-1          40                      172.16.26.10    ether3 R1 to R3
12 172.16.26.0/29     intra-area     10                      0.0.0.0         ether2 R1 to R2
13 172.16.26.8/29     intra-area     10                      0.0.0.0         ether3 R1 to R3
14 172.16.26.16/29    intra-area     10                      0.0.0.0         ether4 R1 to R4
15 172.16.26.24/29    intra-area     10                      0.0.0.0         ether5 R1 to R5
16 172.16.26.32/29    intra-area     20                      172.16.26.2     ether2 R1 to R2
                                                             172.16.26.18    ether4 R1 to R4
17 172.16.26.40/29    intra-area     20                      172.16.26.10    ether3 R1 to R3
                                                             172.16.26.18    ether4 R1 to R4
18 172.16.26.48/29    intra-area     20                      172.16.26.10    ether3 R1 to R3
                                                             172.16.26.26    ether5 R1 to R5
19 172.16.26.56/29    intra-area     20                      172.16.26.10    ether3 R1 to R3
20 192.168.48.0/24    imported-ext-1 20
[renan@R1] >
```

Fuente: WinBox

Seguimos con la verificación del funcionamiento de OSPF y procedemos a verificar si los vecinos están en línea y su tiempo de adyacencia, observemos la figura 26 y analicemos los parámetros que nos muestra la tabla de vecinos en el enrutador R1.

Figura 26.

Revisión de NEIGHBORS (vecinos) OSPF en el enrutador R1

```
[renan@R1] > routing ospf neighbor print
 0 instance=default router-id=10.0.0.3 address=172.16.26.10 interface=ether3 R1 to R3 priority=1
   dr-address=172.16.26.10 backup-dr-address=172.16.26.9 state="Full" state-changes=6
   ls-retransmits=0 ls-requests=0 db-summaries=0 adjacency=26m20s

 1 instance=default router-id=10.0.0.2 address=172.16.26.2 interface=ether2 R1 to R2 priority=1
   dr-address=172.16.26.2 backup-dr-address=172.16.26.1 state="Full" state-changes=6
   ls-retransmits=0 ls-requests=0 db-summaries=0 adjacency=26m25s

 2 instance=default router-id=10.0.0.5 address=172.16.26.26 interface=ether5 R1 to R5 priority=1
   dr-address=172.16.26.26 backup-dr-address=172.16.26.25 state="Full" state-changes=6
   ls-retransmits=0 ls-requests=0 db-summaries=0 adjacency=26m26s

 3 instance=default router-id=10.0.0.4 address=172.16.26.18 interface=ether4 R1 to R4 priority=1
   dr-address=172.16.26.18 backup-dr-address=172.16.26.17 state="Full" state-changes=6
   ls-retransmits=0 ls-requests=0 db-summaries=0 adjacency=26m29s
[renan@R1] >
```

Fuente: WinBox

Al observar la figura 26 anterior, podemos evidenciar que cada vecino presenta un "router-id", no es más que la ip de loopback asignada al bridge que creamos inicialmente, nos muestra datos como el tiempo de adyacencia de cada enrutar que consta como vecino, así como la dirección de red de la interfaz del salto y de la interfaz por la que sale la ruta.

En la figura 27 a continuación, revisamos los LSA, haciendo hincapié en la teoría, veremos que los datos e información de la topología se encuentran aquí, entonces es posible visualizar redes conectadas a enrutadores vecinos.

Figura 27.

Revisión de LSA OSPF en el enrutador R1

```
[renan@R1] > routing ospf lsa print
AREA                            TYPE         ID              ORIGINATOR      SEQUENCE-NUMBER         AGE
backbone                        router       10.0.0.1        10.0.0.1             0x8000000C         362
backbone                        router       10.0.0.2        10.0.0.2             0x80000009         367
backbone                        router       10.0.0.3        10.0.0.3             0x80000009         364
backbone                        router       10.0.0.4        10.0.0.4             0x8000000A         368
backbone                        router       10.0.0.5        10.0.0.5             0x80000009         365
backbone                        router       10.0.0.6        10.0.0.6             0x80000006        1794
backbone                        network      172.16.26.2     10.0.0.2             0x80000005         369
backbone                        network      172.16.26.10    10.0.0.3             0x80000005         364
backbone                        network      172.16.26.18    10.0.0.4             0x80000005         373
backbone                        network      172.16.26.26    10.0.0.5             0x80000005         369
backbone                        network      172.16.26.34    10.0.0.4             0x80000004        1791
backbone                        network      172.16.26.42    10.0.0.4             0x80000004        1796
backbone                        network      172.16.26.50    10.0.0.5             0x80000004        1796
backbone                        network      172.16.26.58    10.0.0.6             0x80000004        1794
external                        as-external  10.0.0.1        10.0.0.1             0x80000002         369
external                        as-external  10.0.0.2        10.0.0.2             0x80000005          30
external                        as-external  10.0.0.3        10.0.0.3             0x80000005          35
external                        as-external  10.0.0.4        10.0.0.4             0x80000005          55
external                        as-external  10.0.0.5        10.0.0.5             0x80000005          44
external                        as-external  10.0.0.6        10.0.0.6             0x80000005          42
external                        as-external  172.16.20.0     10.0.0.1             0x80000002         369
external                        as-external  172.16.21.0     10.0.0.2             0x80000005          30
external                        as-external  172.16.22.0     10.0.0.3             0x80000005          35
external                        as-external  172.16.23.0     10.0.0.4             0x80000005          55
external                        as-external  172.16.24.0     10.0.0.5             0x80000005          44
external                        as-external  172.16.25.0     10.0.0.6             0x80000005          42
external                        as-external  192.168.48.0    10.0.0.1             0x80000002         369
[renan@R1] >
```

Fuente: WinBox

Finalmente observamos los ASBR, los ROUTERES DE BORDE AS son importantes porque publican información de enrutamiento sobre direcciones IP de destino que no se obtienen de OSPF.

En la figura 28 a continuación, podemos evidenciar que se muestran los ROUTERID de los enrutadores que están adyacentes al enrutador R1, cada uno con su respectivo costo.

Figura 28.

Revisión de los ASBR OSPF en el enrutador R1

```
[renan@R1] > routing ospf as-border-router print
 # ROUTERID        STATE      GATEWAY          COST
 0 10.0.0.1        intra-area                  0
 1 10.0.0.2        intra-area 172.16.26.2      10
 2 10.0.0.3        intra-area 172.16.26.10     10
 3 10.0.0.4        intra-area 172.16.26.18     10
 4 10.0.0.5        intra-area 172.16.26.26     10
 5 10.0.0.6        intra-area 172.16.26.10     20
[renan@R1] >
```

Fuente: WinBox

4.1.3. Configuración de MPLS

Para la configuración a través de interfaz gráfica, la opción MPLS se habilita en la sección de MPLS, para lo cual seleccionamos la opción LDP Settings, habilitamos en Enabled y se añade el identificativo Loopback 10.0.0.1 en LSR ID y Transport Address. Si la configuración se la realiza por telnet, lo haremos con los comandos tal como se muestra en la figura 29.

Figura 29.

Configuración de LDP en MPLS, para enrutador R1

```
[renan@R1] > /mpls ldp
[renan@R1] /mpls ldp> set enabled=yes lsr-id=10.0.0.1 transport-address=10.0.0.1
[renan@R1] /mpls ldp>
```

Fuente: WinBox

A continuación, en la figura 30, se añaden las interfaces que forman parte de los saltos entre cada router. En este caso la interfaz ether1, ether2 y Loopback 10. Con esto estará habilitado el enrutamiento en este router.

Figura 30.

Configuración de interfaces MPLS en el enrutador R1

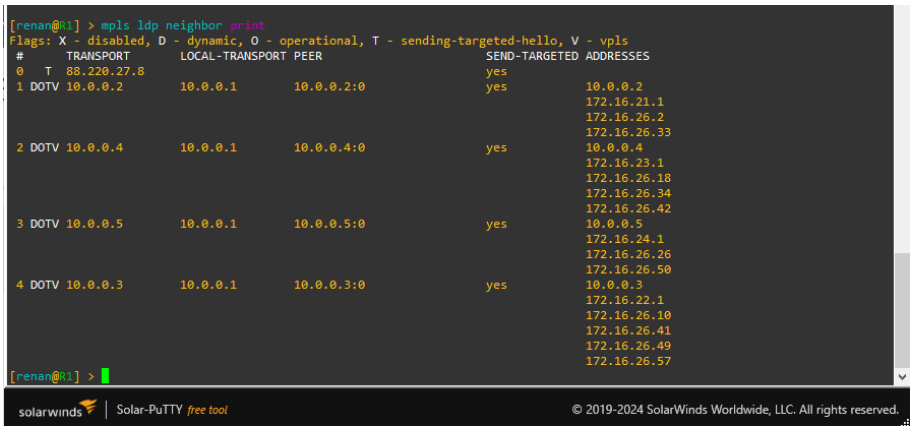
```
[renan@R1] > /mpls ldp interface
[renan@R1] /mpls ldp interface> add interface="ether2 R1 to R2"
[renan@R1] /mpls ldp interface> add interface="ether3 R1 to R3"
[renan@R1] /mpls ldp interface> add interface="ether4 R1 to R4"
[renan@R1] /mpls ldp interface> add interface="ether5 R1 to R5"
[renan@R1] /mpls ldp interface> add interface="ether8 LAN R1"
[renan@R1] /mpls ldp interface> add interface=lo
[renan@R1] /mpls ldp interface>
```

Fuente: WinBox

Una vez habilitado en toda la red las configuraciones previas con el respectivo direccionamiento tendríamos que ver una lista de las rutas aprendidas de cada router vecino en la opción de LDP Neighbor, como se observa en la figura 31

Figura 31.

Visualización de vecinos LDP MPLS en el enrutador R1



Fuente: WinBox

En la figura 31 anterior, podemos visualizar que los vecinos son identificados tal como se muestra en la figura, cada vecino detectado cuenta con un flag donde nos informa el origen y tipo de vecino, por ejemplo el numeral 1 nos muestra el ROUTERID que corresponde a R2, al final las direcciones ip alcanzadas a través de R2 y en el flag nos muestra que es de tipo dinámico, esta operacional y enviando el mensaje de saludo y finalmente nos informa que está corriendo sobre el ruteo la tecnología VPLS.

4.1.4. Configuración de VPLS

Una vez ya configurado e insertadas las interfaces de nuestro MPLS, hay que proceder con la implementación de los VPLS-ID, estos serán el identificativo que se insertará a cada enlace ptp y ptmp, además de la ip del routerid del siguiente salto, a continuación, en la figura 32, configuramos las interfaces VPLS con los siguientes comandos:

Figura 32.

Implementación de interfaces y creación de los VPLS-ID en el enrutador R1

```
[renan@R1] > /interface vpls
[renan@R1] /interface vpls> add disabled=no l2mtu=1500 name=vpls1 remote-peer=10.0.0.2 vpls-id=1:2
[renan@R1] /interface vpls> add disabled=no l2mtu=1500 name=vpls2 remote-peer=10.0.0.4 vpls-id=1:4
[renan@R1] /interface vpls> add disabled=no l2mtu=1500 name=vpls3 remote-peer=10.0.0.5 vpls-id=1:5
[renan@R1] /interface vpls> add disabled=no l2mtu=1500 name=vpls4 remote-peer=10.0.0.3 vpls-id=1:3
[renan@R1] /interface vpls>
```

Fuente: WinBox

Una vez creadas las interfaces, procedemos a verificar si las interfaces creadas están en línea, en la figura 33 a continuación, hacemos un "print" de las interfaces VPLS creadas para verificar su estado.

Figura 33.

Visualización de estado de interfaces VPLS en el enrutador R1

```
[renan@R1] /interface vpls> print
Flags: X - disabled, R - running, D - dynamic, B - bgp-signaled, C - cisco-bgp-signaled
 0 R   name="vpls1" mtu=1500 l2mtu=1500 mac-address=02:3F:0E:B5:28:26 arp=enabled arp-timeout=auto disable-running-check=no
       remote-peer=10.0.0.2 vpls-id=1:2 cisco-style=no cisco-style-id=0 advertised-l2mtu=1500 pw-type=raw-ethernet
       use-control-word=default

 1 R   name="vpls2" mtu=1500 l2mtu=1500 mac-address=02:B9:A6:EA:F4:F5 arp=enabled arp-timeout=auto disable-running-check=no
       remote-peer=10.0.0.4 vpls-id=1:4 cisco-style=no cisco-style-id=0 advertised-l2mtu=1500 pw-type=raw-ethernet
       use-control-word=default

 2 R   name="vpls3" mtu=1500 l2mtu=1500 mac-address=02:FB:C0:D0:A8:1A arp=enabled arp-timeout=auto disable-running-check=no
       remote-peer=10.0.0.5 vpls-id=1:5 cisco-style=no cisco-style-id=0 advertised-l2mtu=1500 pw-type=raw-ethernet
       use-control-word=default

 3 R   name="vpls4" mtu=1500 l2mtu=1500 mac-address=02:F5:B4:AE:B4:77 arp=enabled arp-timeout=auto disable-running-check=no
       remote-peer=10.0.0.3 vpls-id=1:3 cisco-style=no cisco-style-id=0 advertised-l2mtu=1500 pw-type=raw-ethernet
       use-control-word=default
[renan@R1] /interface vpls>
solarwinds | Solar-PuTTY free tool   © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.
```

Fuente: WinBox

Como se observa en la figura 33 anterior, las interfaces creadas en VPLS tienen el flag de tipo "R" lo que nos informa que la interfaz está en estado "RUNNING", con esto

podemos evidenciar que la red se encuentra en estado operativo con los protocolos y tecnologías implementadas en perfecto funcionamiento.

4.2. Pruebas de funcionamiento

Finalmente se procede con el desarrollo de las pruebas necesarias para tratar de obtener los errores y fallas que pueden suscitarse en la red, las pruebas nos demostrarán lo eficiente y confiable que resulta la red con la reingeniería empleada.

A continuación, los resultados de las pruebas realizadas en la emulación de la topología de red con los protocolos y tecnologías empleadas en funcionamiento.

4.2.1. Pruebas de Servicios

En este apartado comenzaremos con las pruebas de segmentación para comprobar que distintos segmentos de la red tengan comunicación garantizada, y con ello puedan compartir información de manera fiable entre ellos. Luego se realizarán pruebas del enrutamiento dinámico, aquí se evaluará las tablas de enrutamiento y se verificará la comunicación entre distintos segmentos de red.

Las pruebas de administración se las realizará a cada enrutador, demostrando que haya disponibilidad de comunicación y administración remota mediante ssh, luego probaremos la escalabilidad de tal manera que la red demuestre que puede acoplar dispositivos nuevos sin inconvenientes y no altere el funcionamiento de la red.

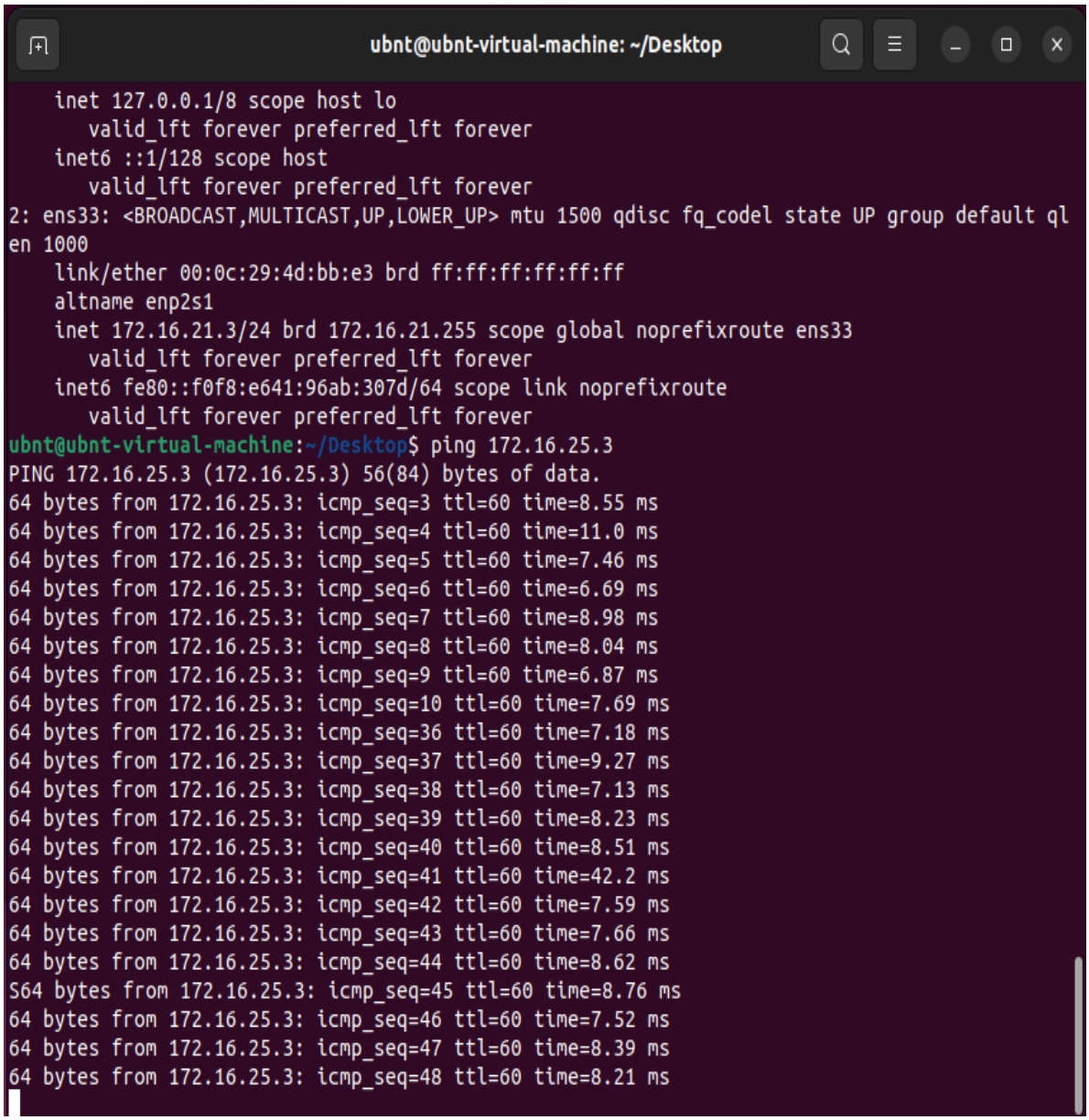
Finalmente se realizarán pruebas de latencia y jitter, esta primera se demostrará con la realización de pines de un enrutador hacia otro y entre dispositivos distintos de segmentos de red, por otra parte, la prueba de jitter la analizaremos en los paquetes presentes en una llamada de tipo VoIP realizada entre dos dispositivos que serán insertados en distintos segmentos de red.

4.2.1.1 Pruebas de Segmentación

Las pruebas de segmentación se realizan en base a la comunicación que tienen los hosts de la LAN de un enrutador con los de otra LAN de otro enrutador, es decir; los hosts de la red podrán comunicarse y compartir información independientemente del segmento al que pertenezcan, en la figura 34 a continuación, se realizarán pines de un host del segmento de red 172.16.21.0/24 hasta otro del segmento 172.16.25.0/24 y viceversa.

Figura 34.

Prueba 1 de comunicación entre dos segmentos distintos de la red.

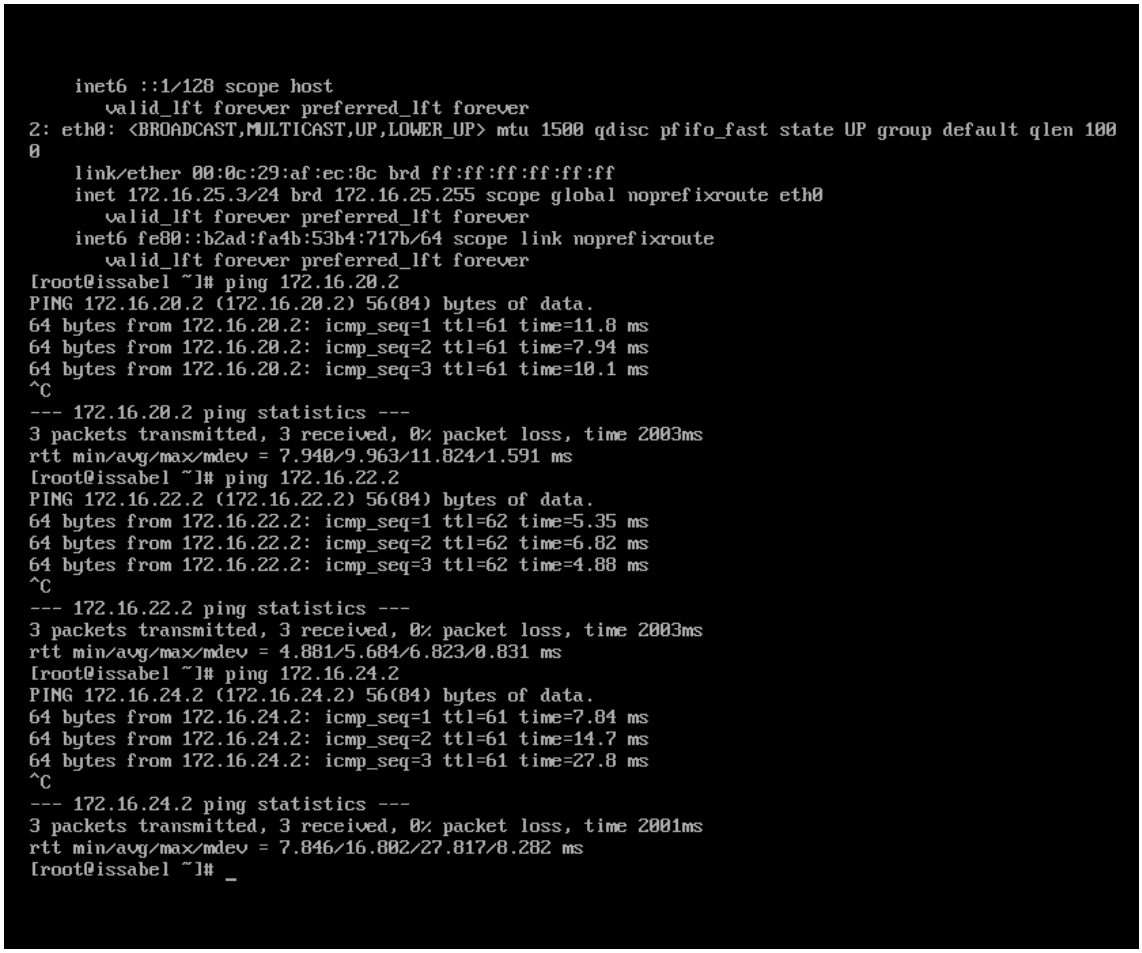


Fuente: GNS3

En la figura 35 continuación, se muestra la prueba desde un host de la LAN de segmento 172.16.25.0/24 hasta algunos hosts de segmentos distintos.

Figura 35.

Prueba 2 de comunicación entre dos segmentos distintos de la red.

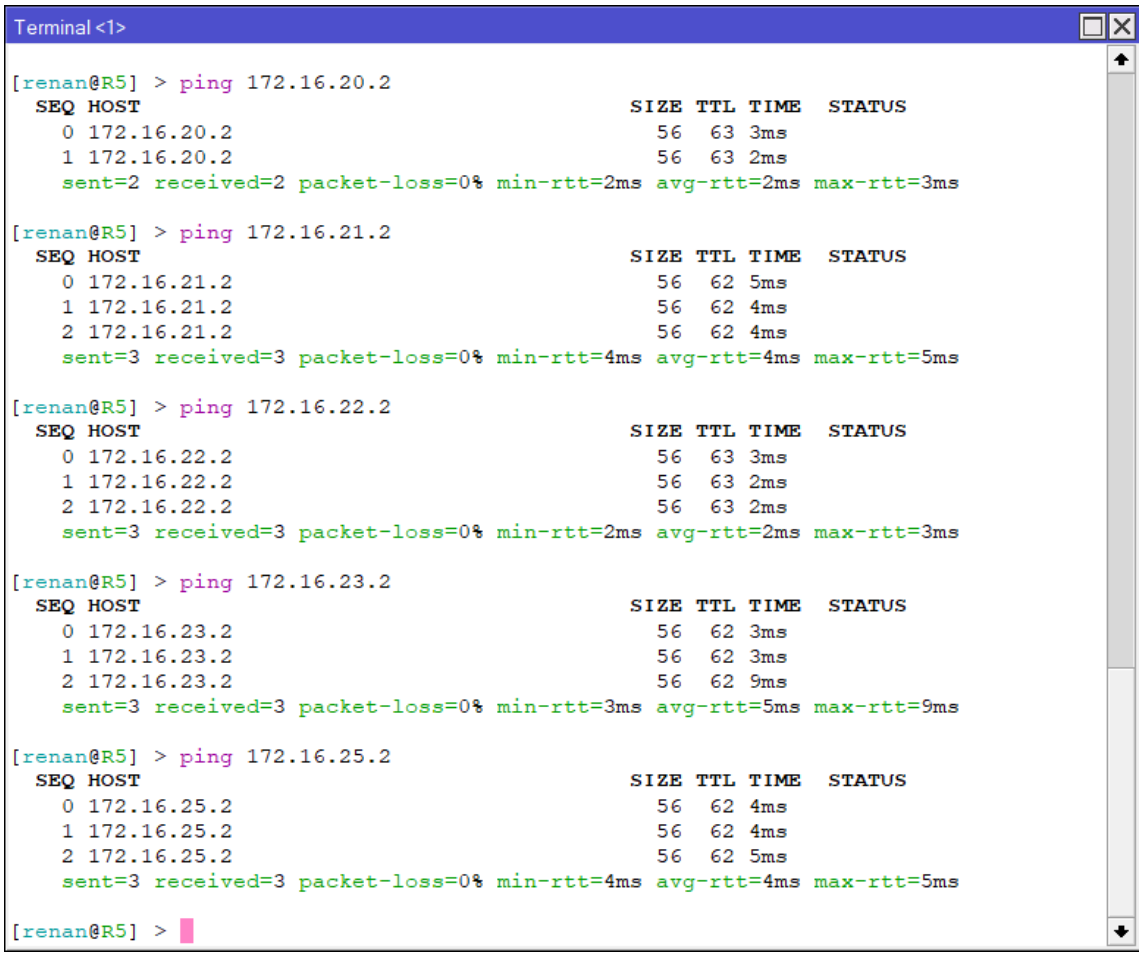


Fuente: VMWARE

De igual forma, los enrutadores deberían lograr comunicarse a cualquier LAN de cualquier segmento de red, en la figura 36, continuación, se muestra las respuestas a los pines realizados desde el enrutador R5 a los hosts de los segmentos de las LAN de enrutadores vecinos en la red.

Figura 36.

Prueba 3 de comunicación entre dos segmentos distintos de la red.



Fuente: WinBox

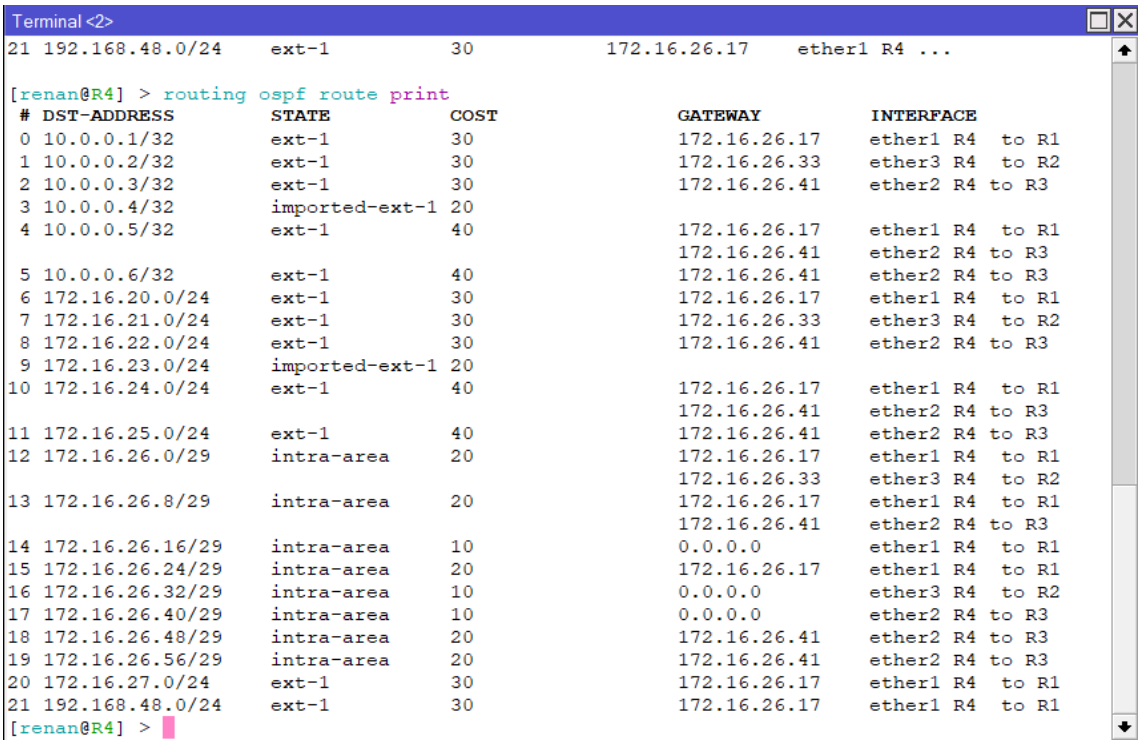
4.2.1.2. Pruebas de enrutamiento

Las pruebas de enrutamiento las realizamos probando las convergencias del protocolo de enrutamiento, para ello vamos a verificar las tablas de enrutamiento de los enrutadores así como de los LSA, NEIGHBOR Y ASBR.

En la figura 37 a continuación, vamos a mostrar la tabla de enrutamiento OSPF del enrutador R4, las demás tablas de enrutamiento y pruebas de los otros enrutadores, las podemos observar en el anexo correspondiente.

Figura 37.

Prueba 1 de enrutamiento, Tabla de rutas de enrutador R4.



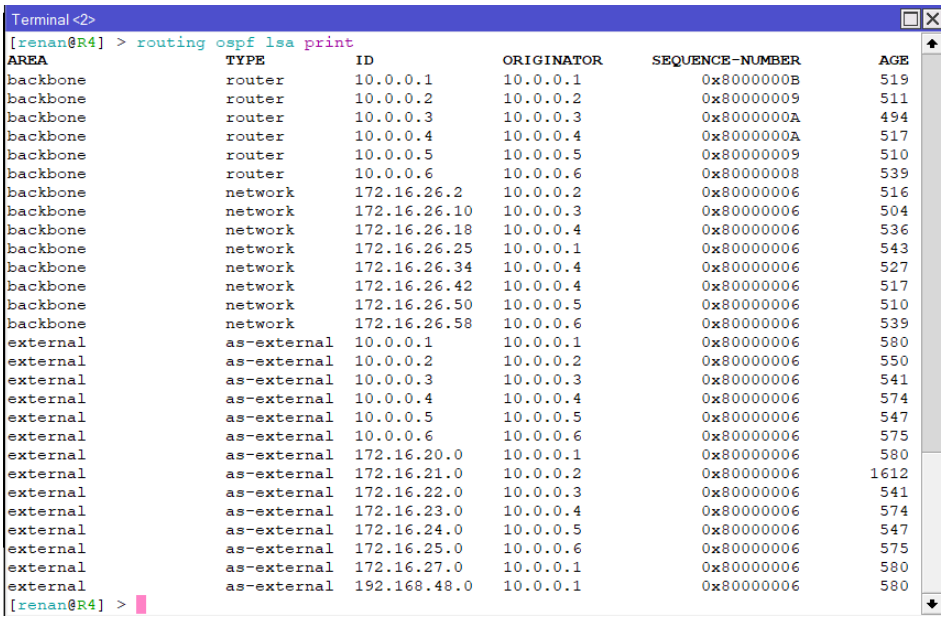
```
Terminal <2>
21 192.168.48.0/24     ext-1           30          172.16.26.17     ether1 R4 ...

[renan@R4] > routing ospf route print
 # DST-ADDRESS         STATE           COST              GATEWAY          INTERFACE
 0 10.0.0.1/32         ext-1           30                172.16.26.17     ether1 R4  to R1
 1 10.0.0.2/32         ext-1           30                172.16.26.33     ether3 R4  to R2
 2 10.0.0.3/32         ext-1           30                172.16.26.41     ether2 R4 to R3
 3 10.0.0.4/32         imported-ext-1  20
 4 10.0.0.5/32         ext-1           40                172.16.26.17     ether1 R4  to R1
                                                         172.16.26.41     ether2 R4 to R3
 5 10.0.0.6/32         ext-1           40                172.16.26.41     ether2 R4 to R3
 6 172.16.20.0/24      ext-1           30                172.16.26.17     ether1 R4  to R1
 7 172.16.21.0/24      ext-1           30                172.16.26.33     ether3 R4  to R2
 8 172.16.22.0/24      ext-1           30                172.16.26.41     ether2 R4 to R3
 9 172.16.23.0/24      imported-ext-1  20
10 172.16.24.0/24      ext-1           40                172.16.26.17     ether1 R4  to R1
                                                         172.16.26.41     ether2 R4 to R3
11 172.16.25.0/24      ext-1           40                172.16.26.41     ether2 R4 to R3
12 172.16.26.0/29      intra-area      20                172.16.26.17     ether1 R4  to R1
                                                         172.16.26.33     ether3 R4  to R2
13 172.16.26.8/29      intra-area      20                172.16.26.17     ether1 R4  to R1
                                                         172.16.26.41     ether2 R4 to R3
14 172.16.26.16/29     intra-area      10                0.0.0.0          ether1 R4  to R1
15 172.16.26.24/29     intra-area      20                172.16.26.17     ether1 R4  to R1
16 172.16.26.32/29     intra-area      10                0.0.0.0          ether3 R4  to R2
17 172.16.26.40/29     intra-area      10                0.0.0.0          ether2 R4 to R3
18 172.16.26.48/29     intra-area      20                172.16.26.41     ether2 R4 to R3
19 172.16.26.56/29     intra-area      20                172.16.26.41     ether2 R4 to R3
20 172.16.27.0/24      ext-1           30                172.16.26.17     ether1 R4  to R1
21 192.168.48.0/24     ext-1           30                172.16.26.17     ether1 R4  to R1
[renan@R4] >
```

Fuente: WinBox

En la figura 38, a continuación, muestra de las tablas de LSA OSPF en R4.

Figura 38.

Prueba 2 de enrutamiento, Tabla de LSA de enrutador R4



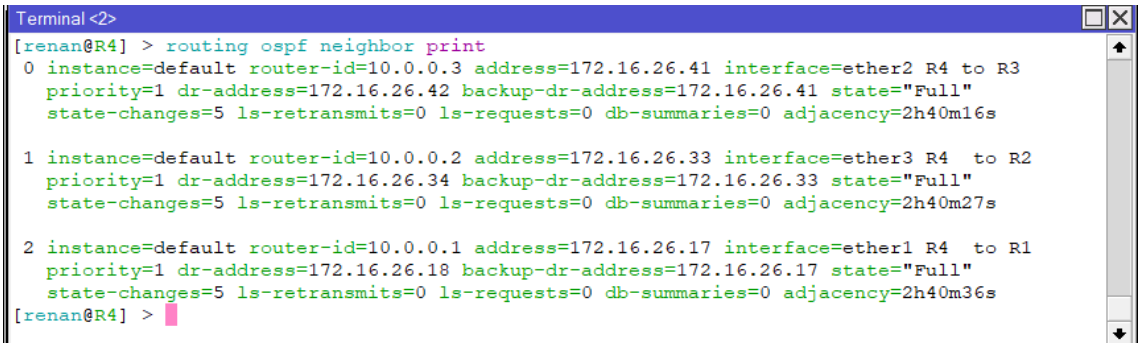
```
Terminal <2>
[renan@R4] > routing ospf lsa print
AREA                TYPE         ID              ORIGINATOR      SEQUENCE-NUMBER      AGE
backbone            router       10.0.0.1        10.0.0.1            0x8000000B       519
backbone            router       10.0.0.2        10.0.0.2            0x80000009       511
backbone            router       10.0.0.3        10.0.0.3            0x8000000A       494
backbone            router       10.0.0.4        10.0.0.4            0x8000000A       517
backbone            router       10.0.0.5        10.0.0.5            0x80000009       510
backbone            router       10.0.0.6        10.0.0.6            0x80000008       539
backbone            network      172.16.26.2     10.0.0.2            0x80000006       516
backbone            network      172.16.26.10    10.0.0.3            0x80000006       504
backbone            network      172.16.26.18    10.0.0.4            0x80000006       536
backbone            network      172.16.26.25    10.0.0.1            0x80000006       543
backbone            network      172.16.26.34    10.0.0.4            0x80000006       527
backbone            network      172.16.26.42    10.0.0.4            0x80000006       517
backbone            network      172.16.26.50    10.0.0.5            0x80000006       510
backbone            network      172.16.26.58    10.0.0.6            0x80000006       539
external            as-external  10.0.0.1        10.0.0.1            0x80000006       580
external            as-external  10.0.0.2        10.0.0.2            0x80000006       550
external            as-external  10.0.0.3        10.0.0.3            0x80000006       541
external            as-external  10.0.0.4        10.0.0.4            0x80000006       574
external            as-external  10.0.0.5        10.0.0.5            0x80000006       547
external            as-external  10.0.0.6        10.0.0.6            0x80000006       575
external            as-external  172.16.20.0     10.0.0.1            0x80000006       580
external            as-external  172.16.21.0     10.0.0.2            0x80000006      1612
external            as-external  172.16.22.0     10.0.0.3            0x80000006       541
external            as-external  172.16.23.0     10.0.0.4            0x80000006       574
external            as-external  172.16.24.0     10.0.0.5            0x80000006       547
external            as-external  172.16.25.0     10.0.0.6            0x80000006       575
external            as-external  172.16.27.0     10.0.0.1            0x80000006       580
external            as-external  192.168.48.0    10.0.0.1            0x80000006       580
[renan@R4] >
```

Fuente: WinBox

En la figura 39 a continuación, muestra de vecinos OSPF en el enrutador R4

Figura 39.

Prueba 3 de enrutamiento, Tabla de Neighbors de enrutador R4

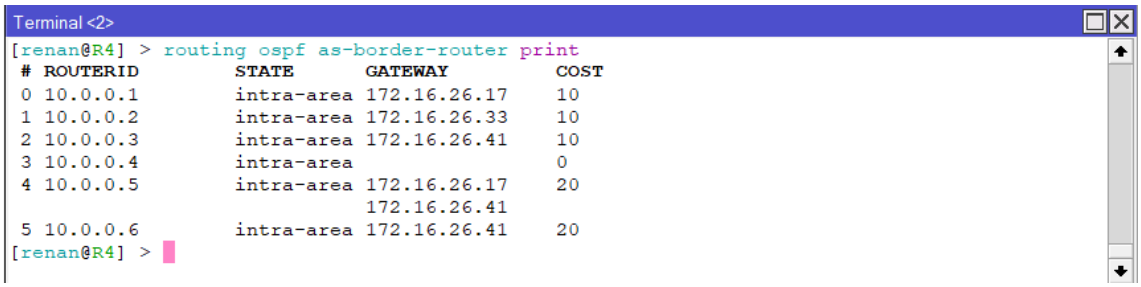


Fuente: WinBox

En la figura 40 a continuación, muestra ASBR y costos OSPF, en el enrutador R4

Figura 40.

Prueba 4 de enrutamiento, Tabla de ASBR de enrutador R4



Fuente: WinBox

4.2.1.3. Pruebas de administración de acceso

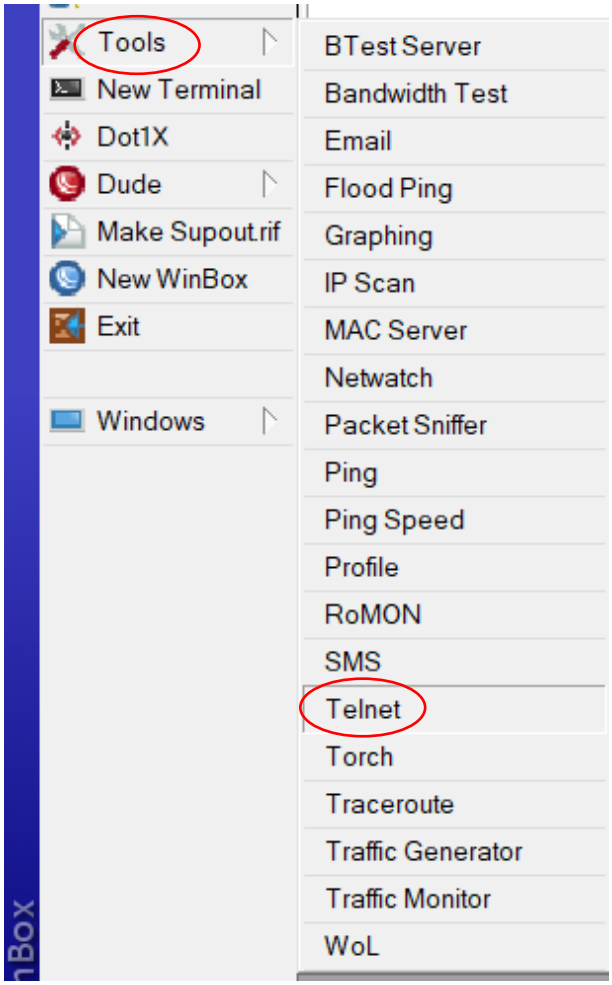
Las pruebas de administración de acceso se las realiza haciendo comunicaciones a routers involucrados en la red, a través del uso de SSH, cada router podrá comunicarse con el que requiera a través de este protocolo, se optó por este protocolo en vista de la seguridad mejorada respecto al usado comúnmente ¨telnet¨.

A continuación, se muestran los resultados de las pruebas de comunicación a través de SSH, como ejemplo, se realizó la comunicación desde el enrutador R6 hasta el enrutador R2, para ello se procedió de la siguiente manera: inicialmente accedemos a la

opción ¨telnet¨ del apartado de las herramientas ¨tools¨ del enrutador del cual se va a realizar la petición SSH, tal como se evidencia en la figura 41.

Figura 41.

Prueba 1 de administración de acceso, petición desde el enrutador R6

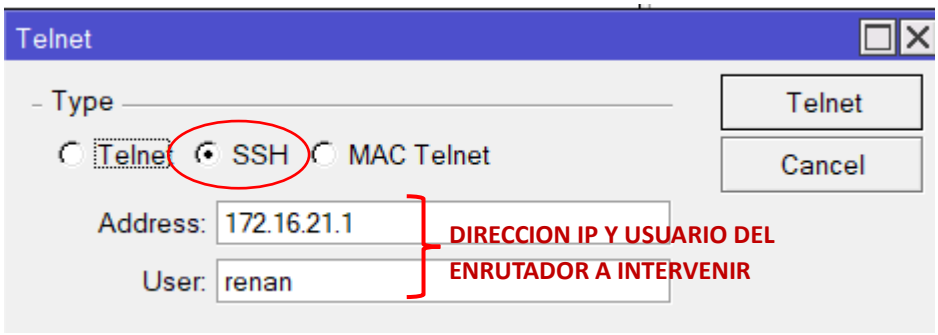


Fuente: WinBox

El siguiente paso será seleccionar SSH en la ventana que se muestra en la figura 42, después de haber realizado la selección, solicita la dirección de red del host al que queremos alcanzar y el usuario de este, en este caso intentaremos realizar la comunicación hasta el enrutador R2.

Figura 42.

Configuración de dirección de red y usuario para acceso SSH en enrutador R6.



Fuente: WinBox

Después de haber insertado la dirección de red y el usuario, como se muestra en la figura 42 anterior, al hacer click en el botón ¨telnet¨, se despliega una nueva ventana, misma que solicitará la clave de acceso del enrutador, tal como se muestra en la figura 43 a continuación.

Figura 43.

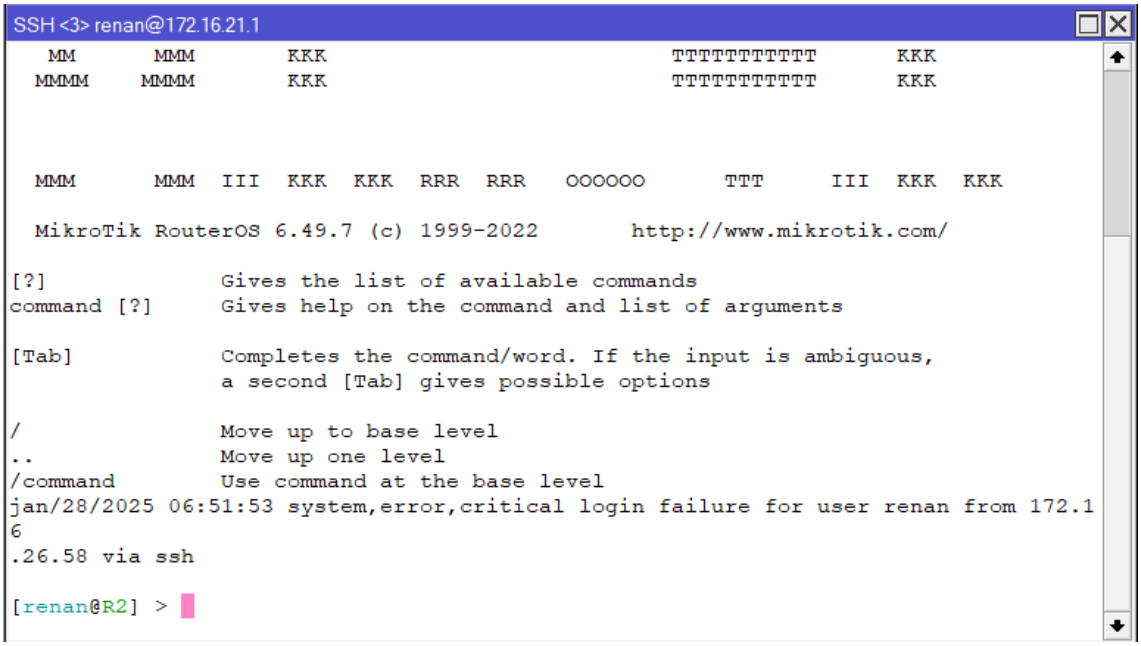
Configuración de clave de acceso del enrutador R2 solicitado mediante SSH

Fuente: WinBox

Una vez insertado la clave de acceso para el enrutador R2, nos muestra en la ventana el terminal del enrutador alcanzado, con ello ya se puede configurar y realizar lo que se requiera en este enrutador, ya que se logró la comunicación SSH de manera exitosa.

Figura 44.

Muestra de comunicación exitosa a través de SSH, entre R6 hacia R2



Fuente: WinBox

4.2.1.4. Pruebas de escalabilidad

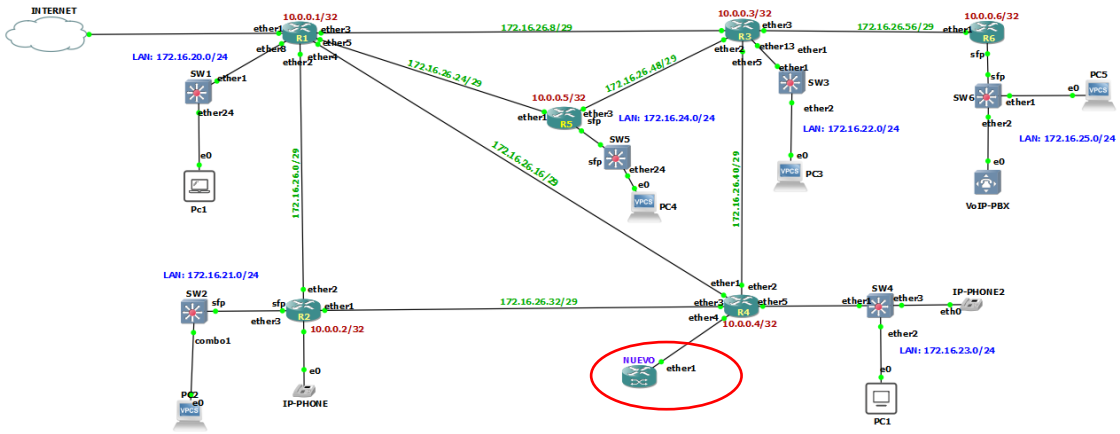
Estas pruebas se realizaron en razón de los posibles incrementos de dispositivos de red que pueden darse en un futuro, la red al ser escalable, podrá crecer sin perder la disponibilidad y la fiabilidad, lo que significa que la red estará disponible y logrará expandirse de manera eficaz y fácil.

Vamos a observar el diseño de la red hasta ahora, y observamos que dado el caso que se aumente un enrutador dependiendo de donde este ubicado, los enlaces necesarios o requeridos para incluir al enrutador en el área, dependerá del criterio que tome el administrador de la red y de las funciones que este equipo vaya a desempeñar en la red. Para nuestro caso añadiremos el enrutador de nombre ¨NUEVO¨, tal como se aprecia en

la figura 45, a este le incluiremos un enlace que se conectara al enrutador que más cerca se encuentra.

Figura 45.

Topología de red, con un enrutador extra, incluido recientemente.



Fuente: GNS3

En la figura 45 anterior, podemos visualizar que este equipo incluido en la red tiene conexión física al enrutador R4, en este caso cuenta solo con un enlace, pero si es necesario la conexión de dos o más enlaces, se los realiza en base al criterio y las necesidades que este router requiera.

El enrutador ¨NUEVO¨, no consta de direccionamiento de ip para sus interfaces tanto para la conexión de enlaces como para la interfaz loopback, de tal manera que será necesario revisar la tabla 6 y establecer el direccionamiento respectivo.

Analizada la tabla 6 anterior, se determinan las siguientes direcciones de red para nuestro nuevo equipo, las detallamos a continuación en la tabla 15.

Tabla 15.

Distribución de direcciones IP para el enrutador NUEVO

DESCRIPCIÓN	*TIPO*	RED	IP INICIAL	IP FINAL	BROADCAST
RNUEVO	LOOPBACK	10.0.0.7/32			
RN LAN	PTMP	172.16.27.0/24	172.16.27.1	172.16.27.254	172.16.27.255
RN-R4	PTP	172.16.26.64/29	172.16.26.65	172.16.26.70	172.16.26.72

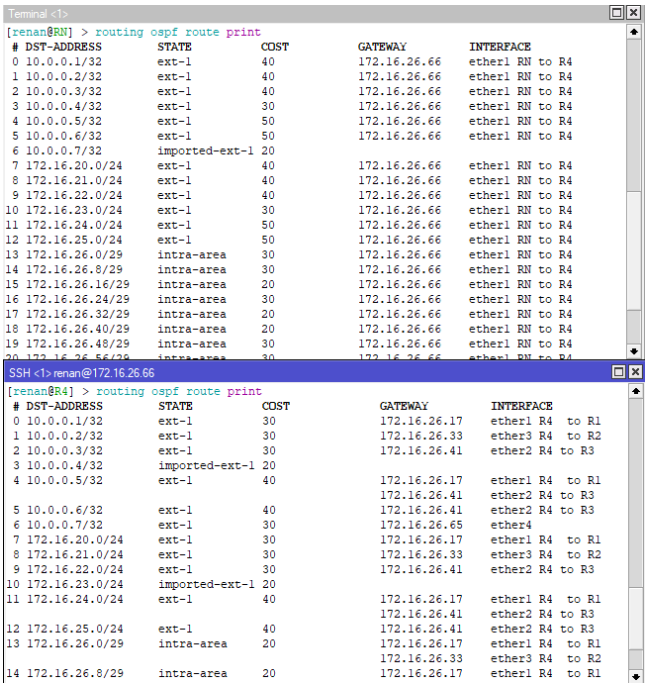
Fuente. Autoría propia.

Una vez conocidos los direccionamientos de las interfaces de nuestro enrutador recién incluido en la red, procedemos a configurar de la misma forma que se realizó la configuración de los enrutadores anteriores, las configuraciones de este enrutador la podemos ver en el anexo al final, lo que si vamos a citar es la prueba de que este equipo se encuentre con adyacencia en la red, funcional y operativo sin que los enrutadores anteriores hayan sufrido de cambios o modificaciones en la red.

En la figura 46 a continuación, vemos la tabla de enrutamiento tanto del enrutador R4 como del enrutador nuevo, podemos ver que hay convergencia total hacia el nuevo equipo, asi mismo es reconocido en la red por los demás enrutadores.

Figura 46.

Tabla de enrutamiento de RN y de R4.

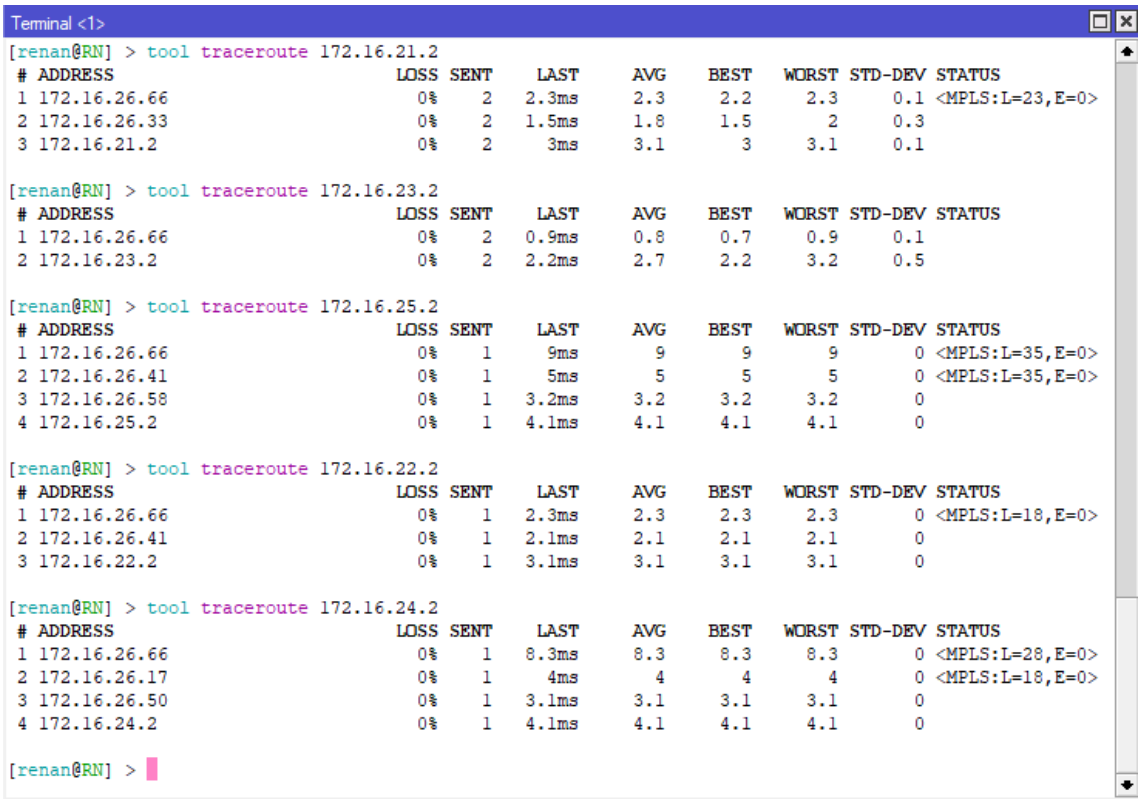


Fuente: GNS3

Como se observa en la figura 46 anterior, nuestro router instalado tiene convergencia y ya es parte del área OSPF en la red, eso quiere decir que VPLS ya está encapsulando los paquetes de este router en la red, continuación en la figura 47, podemos observar que nuestro equipo ya tiene comunicación ping hacia cualquier host de la red.

Figura 47.

Prueba de respuesta de algunos hosts de la red a RN.



Fuente: GNS3

De esta manera pudimos comprobar que nuestra red es escalable y tiene la capacidad para adaptarse de manera eficiente al crecimiento de las demandas, ya sea aumentando la cantidad de usuarios, dispositivos conectados, tráfico o servicios ofrecidos.

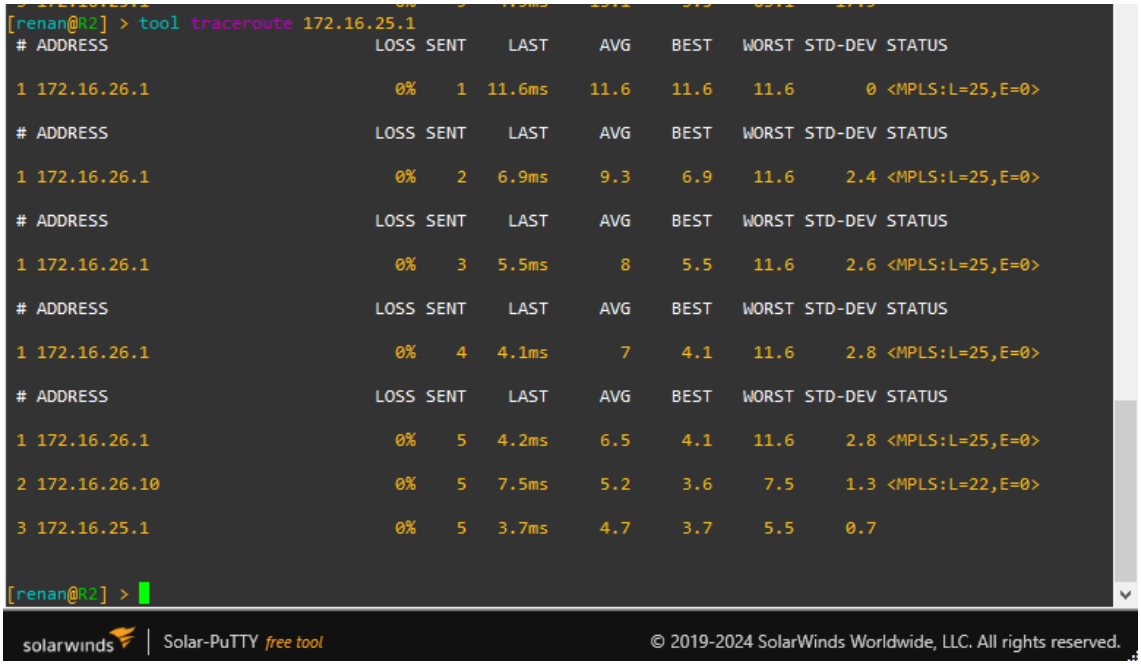
4.2.1.5. Pruebas de latencia

Para probar la latencia y tiempos de respuesta de un dispositivo en la red, vamos a usar la herramienta ¨Traceroute¨, esta herramienta nos permite visualizar los tiempos de respuesta en los saltos de un dispositivo a otro, así como la dirección IP de cada router o switch por el que pasa el paquete y si se agotó o no el tiempo de espera en algún salto.

Como podemos observar en la figura 48 a continuación, se evidencia un tanto de 3 saltos para llegar a este destino, además de los tiempos de respuesta y el estado de la comunicación de salto a salto.

Figura 48.

Visualización de tiempos de respuesta solicitados por el enrutador R2 al enrutador R6



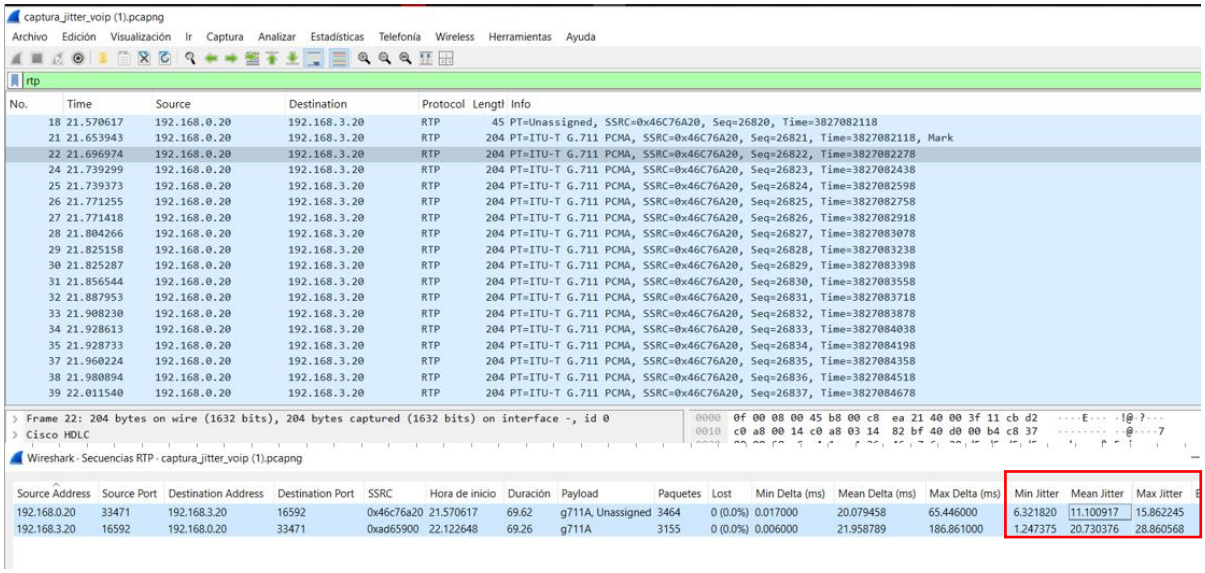
Fuente: GNS3

4.2.1.6. Pruebas de Jitter

Las pruebas de jitter se muestran en la figura 49 a continuación, para ello se realiza una llamada VoIP, entre dos dispositivos en la red, para ello, se montó una PBX en un segmento de la red y los teléfonos IP ubicados en segmentos distintos.

Figura 49.

Captura de tráfico con ¨wireshark¨ para visualizar el jitter de los paquetes durante la llamada telefónica entre dos dispositivos IP en la red.



Fuente: Wireshark

4.4. Identificación de las mejoras obtenidas en la red

Las pruebas iniciales realizadas sin configuraciones de OSPF y VPLS en la red plana reflejan las limitaciones de una red sin mecanismos de seguridad y fiabilidad en el transporte de información, donde los distintos flujos compiten por los recursos disponibles, lo que genera fluctuaciones y pérdidas significativas. En esta sección, se presenta la evaluación de los escenarios planteados, ahora con configuraciones de ruteo dinámico OSPF y tecnología VPLS. Estas tecnologías permiten seguridad en la gestión ya hacen más eficiente al envío de información entre segmentos distintos dentro de la red, mejorando el rendimiento y la disponibilidad de la red.

Los servicios probados luego de la implementación de las tecnologías en la nueva red de datos, nos demuestran las mejoras obtenidas, los resultados muestran mejoría notable en aspectos importantes como la seguridad y fiabilidad en el transporte de paquetes entre dispositivos de la red, administración segura a través de ssh a cualquier dispositivo de la red y respuestas rápidas con latencias y jitter bajos, además la red

muestra escalabilidad lo que hace que la red sea funcional y dinámica y por ende segura al incremento de dispositivos en la red y modificaciones en la topología.

A continuación, en la tabla 16, podemos evidenciar una comparativa de la red plana inicial con la red nueva con VPLS, de ahí deduciremos los altos y bajos en cada escenario tanto en el anterior como en el actual.

Tabla 16.

Comparativa de funcionamiento de servicios en las redes anterior y actual.

DESC.	LATENCIA	JITTER	DIFUSIÓN BROADCAST	LOOP´S	DISPONI_ BILIDAD	SEGURI_ DAD
RED PLANA	ALTA	ALTO	EN TODA LA RED	CONSTANTES EN LA RED	BAJA	BAJA
RED ACTUAL VPLS	BAJA	BAJO	EN CADA SEGMENTO DE RED	OCACIONALES SOLO EN EL SEGMENTO	ALTA	ALTA

Fuente. Autoría propia.

En la tabla 16 anterior, podemos evidenciar que mejoraron muchos aspectos de manera general en la red respecto a la red inicial, en la tabla 17 a continuación, podremos observar el detalle específico de las mejoras obtenidas.

Tabla 17.

Detalle de mejoras obtenidas con el diseño de la nueva red de datos.

SERVICIO	MEJORÍA
LATENCIA	• La red actual, muestra claramente seguridad y fiabilidad en el transporte de datos, además de presentar tiempos de respuesta menor, mostrando claramente mejoría en la latencia y estabilidad en el jitter, siendo este ultimo de tipo bajo en relación al de la red plana.
LOOP DE RED	• La red actual, presenta equipos de capa 3 en cada nodo, mismo que utiliza el enrutamiento dinámico y etiquetas VPLS, además de usar diferentes segmentos de red, lo que hace que no se presenten ráfagas de broadcast ni loops difundidos en toda la red.
ADMNISTRACIÓN REMOTA	• La red diseñada presenta administración a través de SSH, lo que hace que el acceso a los dispositivos de la red sea seguro.

SEGMENTACIÓN	• La segmentación de la red hace que los problemas sean identificados de manera más rápida y oportuna, esto debido a que, si se presenta un inconveniente proveniente de algún dispositivo de la red, este problema se aislará y permanecerá únicamente en el segmento donde se suscite esto, desafectando al resto de segmentos de la red del problema.
ESCALABILIDAD	• Al tener enrutamiento dinámico configurado en la red actual, hace que la escalabilidad sea segura y más eficiente, esto debido a la adaptabilidad que tiene OSPF, entonces; si un dispositivo se incluye en la red a futuro, podrá tener adyacencia rápida independientemente del punto de la red donde este sea incluido, haciendo se pueda incluir enrutadores y conmutadores sin saturar la red.
DISPONIBILIDAD	• La red actual tiene la capacidad para enrutar el tráfico a través de múltiples enlaces mejorando la eficiencia de la red al equilibrar la carga, además de rutas de respaldo lo que permite una conmutación rápida en caso de una falla en un enlace o en un equipo de red, garantizando una alta disponibilidad.
SEGURIDAD	• La red actual al tener implementado VPLS, cuenta con seguridad en la transmisión de los datos, esto debido a que VPLS usa protocolos de enrutamiento internos y técnicas de encriptación de datos.

Fuente. Autoría propia.

La implementación de la tecnología VPLS en la red, y con ello la reingeniería empleada, hacen que el objetivo principal de “mejorar el servicio a los usuarios” se haya cumplido a cabalidad, los protocolos y el diseño propuesto hicieron que la red sea fiable y se garantice la mejora en el servicio en los clientes, con ello estabilidad y seguridad.

CONCLUSIONES

Con la implementación de protocolos de enrutamiento en la red, se obtiene mejoras en el rendimiento, esto debido a que los paquetes son enviados con criterios de optimización, además de obtener mejor nivel de crecimiento, esto hace que la empresa Mikro-Net SA pueda incrementar el número de sus nodos y usuarios, garantizando mejora en la calidad de servicios que reciben los clientes.

La implementación de MPLS en la red, hace que la empresa Mikro-Net SA cuente con eficiencia y velocidad en la red, esto debido a los paquetes LSR difundidos lo que hace que no se use la tabla de enrutamiento completamente sino únicamente la ruta de destino del paquete, garantizando más eficiencia en la navegación y optimización del ancho de banda en los clientes.

Cuando un paquete encapsulado con la etiqueta VPLS, se envía a través de una red MPLS, este se desencapsula en el destino, lo que hace que las conexiones remotas sean optimas aun si el extremo no se encuentra en la red física, esto hace que las conexiones físicas dedicadas no sean necesarias en algunos casos y que con ello la empresa Mikro-Net SA reduzca costos en algunos casos.

A medida que la red de la empresa Mikro-Net SA crece, también lo hace la cantidad de tráfico que cursa por las interfaces, por eso la escalabilidad es un factor que se ha tomado muy en cuenta en la planificación de diseño de red, ya que la flexibilidad de crecimiento hará que los incrementos y modificaciones que Mikro-Net SA requiera hacer en la red, a futuro no afecten el funcionamiento existente. Para ello, la empresa ya cuenta con soluciones tecnológicas que simplifican este proceso.

Las emulaciones son pruebas que pueden apegarse a la realidad, es lo más cercano que podemos obtener para pruebas de simulaciones de redes, en vista de la facilidad de

uso de imágenes reales de sistemas OS de marcas conocidas y el uso de servidores en máquinas virtuales, esto hace que tengamos una herramienta bastante útil, perfecta para diseñar redes e implementar protocolos y tecnologías.

RECOMENDACIONES

Antes de iniciar con el diseño para un trabajo o proyecto cualquiera, es necesario realizar con exhaustividad y análisis profundo, el alcance del proyecto, si se desea lograr un objetivo en específico habría que estipular los recursos necesarios involucrados, tanto económicos, personales, software, hardware, etc. Esto con la finalidad de que al final no haya que detener el proyecto o cambiar los objetivos por la falta de algún requerimiento no estipulado al inicio.

Para el caso de pruebas en simuladores y emuladores, es necesario percatarse de los recursos que conllevan el uso de estos tipos de software, si realizamos emulaciones en equipos con pocos recursos, estamos propensos a que se susciten posibles fallas y en algunos casos pérdidas de la información causadas por el no dimensionamiento inicial de software y hardware.

Cuando se va a realizar emulaciones, en lo posible buscar y apegarse a modelos de hardware y tipos de software lo más semejante a modelos disponibles en el mercado local, esto con el fin de que el diseño sea en lo posible lo más apegado a la realidad, porque dado el caso de que el diseño sea un éxito y su implementación un hecho, no se presenten inconvenientes al tratar de adquirir los equipos para su instalación.

BIBLIOGRAFÍA

CISCO. (2018). Fundamentos de MPLS. https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKCQEA4/introducci%C3%B3n-a-mpls

López, J. (2020). Emulación de una red sd-wan (software-defined wide area network) utilizando tecnología fortinet y el software gns3. Escuela Politécnica Nacional.

EAE. (2021, April 19). Guía PMBOK: definición, estructura y tips de estudio. Retos En Supply Chain. https://retos-operaciones-logistica.eae.es/que-es-la-guia-pmbok-y-como-influye-en-la-administracion-de-proyectos/

Moreno, S. (2021). Comparación de aspectos operativos y económicos entre SD-WAN y MPLS para establecer la mejor opción de una empresa corporativa a nivel nacional e internacional. Universidad Santo Tomás de Aquino.

Benson, T., Akella, A., & Maltz, D. A. (2010, November). Las características del tráfico de red de centros de datos en el medio silvestre. In Proceedings of the 10th ACM SIGCOMM conference on Internet measurement (pp. 267-280). ACM

Webber, E. (2022). Pros and Cons of MPLS: Is It Right for Your Network? CATO. https://www.catonetworks.com/blog/pros-and-cons-of-mpls/

Bustos, S. (2023). Desarrollo de un plan de migración de una red de área extensa de un proveedor de servicios de internet a una red definida por software SD-WAN". Universidad Técnica del Norte.

Ghein, L. (2006). MPLS Fundamentals 1st edition by De Paperback, USA, Editorial Cisco Press

Amazon. (2023). ¿Qué es la latencia de red? Amazon Web Services. https://aws.amazon.com/es/what-is/latency/

GNS3. (2023). Primeros pasos con GNS3. Docs.Gns3.Com. https://docs.gns3.com/docs/

Stallings, W. (2007). Comunicaciones Y Redes De Computadoras 7ma Ed, Madrid, España: PEARSON EDUCATION SA.

Behrouz, A. (2002). Transmisión de Datos y Redes de Comunicaciones, 2da Ed, Madrid, España: Editora Concepción Fernández Madrid.

Barzola, D. (2020). Administración avanzada de BGP y MPLS con Mikrotik RouterOS, v6.46.4.01, Academy Xperts

Escalante, M. (2016). Ruteo avanzado y Alta disponibilidad con Mikrotik RouterOS, v6.33.5.01, Academy Xperts

Martínez, E. (2012). Fundamentos de Telecomunicaciones y Redes, 1era Ed, CA, USA. Editorial: CreateSpace Independent Publishing Platform

Oracle, P. (2011, Agosto). Administración de TCP/IP

https://docs.oracle.com/cd/E24842_01/html/820-2981/ipplan-2.html

Bellagamba, P. (2009). Interconnecting Data Centers Using VPLS, 1st Ed, USA Editorial Pearson India Education

Zhuo, X. (2010). Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services, 1st Ed San Jose, CA, Estados Unidos de América. Editorial: Wiley

Juniper Networks. (2025). Descripción de las pruebas de políticas de enrutamiento. https://www.juniper.net/documentation/mx/es/software/junos/93outing-policy/topics/concept/policy-testing-routing-policies.html

Marcelo. (2020, Agosto 10). ¿Qué es la Distancia Administrativa? https://ccnadesdecero.es/redes-escalables/#:~:text=Escalabilidad%20es%20el%20término%20para,de%20manera%20eficaz%20y%20fácil.

AJPD soft. (2020, May 23). Primer proyecto de laboratorio de red virtual con GNS3 en Windows e instalación de router Cisco 7200. Proyectoa.Com. https://proyectoa.com/primer-proyecto-de-laboratorio-de-red-virtual-con-gns3-e-instalacion-de-router-cisco-7200/

Díaz, P. (2017, Junio 25). Redes De Área Amplia. https://diplomadoentelecomunicacionesycontrol.blogspot.com/2017/06/redes-de-area-amplia.html

Goodwin, M (2023, Agosto 15). ¿Qué es la Latencia? https://www.ibm.com/es-es/topics/latency#:~:text=El%20jitter%2C%20tambi%C3%A9n%20conocido%20como,nunca%20llegan%20a%20su%20destino.

Barzola, D (2023, Julio 3). ¿Qué es un Sistema Autónomo? https://abcxperts.com/que-es-un-sistema-autonomo/?srsltid=AfmBOor5gMITbIBb4Bwt235-LBZwt8wAIN1SG1RTi5RGotzHITy9YFa-

Level.14 (2023, Noviembre 16). Introducción a OSPF, BGP e IS-IS https://forum.huawei.com/enterprise/intl/es/thread/introducci%C3%B3n-a-ospf-bgp-e-is-is/72525641844301824 0?blogId=725256418443018240

Ortíz, A. (2020, Abril 10). VPLS vs MPLS: diferencias y por qué necesita ambos https://blog.hostdime.com.co/vpls-vs-mpls-diferencias-y-por-que-necesita-ambos/

ANEXOS

ANEXO A. *Configuración de direccionamiento ip*

```
[renan@R2] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.2/32        10.0.0.2        lo
 1   172.16.21.1/24     172.16.21.0     bridgeLAN R2
 2   172.16.26.2/29     172.16.26.0     ether1 R2 to R1
 3   172.16.26.33/29    172.16.26.32    ether2 R2 to R4
[renan@R2] >
```


Ilustración 1. Direccionamiento ip enrutador R2

```
[renan@R3] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.3/32        10.0.0.3        lo
 1   172.16.22.1/24     172.16.22.0     ether13 LAN R3
 2   172.16.26.10/29    172.16.26.8     ether1 R3  to R1
 3   172.16.26.41/29    172.16.26.40    ether2 R3  to R4
 4   172.16.26.57/29    172.16.26.56    ether3 R3  to R6
 5   172.16.26.49/29    172.16.26.48    ether5 R3  to R5
[renan@R3] >
```


Ilustración 2. Direccionamiento ip enrutador R3

```
[renan@R4] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE

 0   10.0.0.4/32        10.0.0.4        lo

 1   172.16.23.1/24     172.16.23.0     ether5 LAN R4

 2   172.16.26.18/29    172.16.26.16    ether1 R4  to R1

 3   172.16.26.42/29    172.16.26.40    ether2 R4 to R3

 4   172.16.26.34/29    172.16.26.32    ether3 R4  to R2

 5   172.16.26.66/29    172.16.26.64    ether4 R4 to RN

[renan@R4] >
```


Ilustración 3. Direccionamiento ip enrutador R4

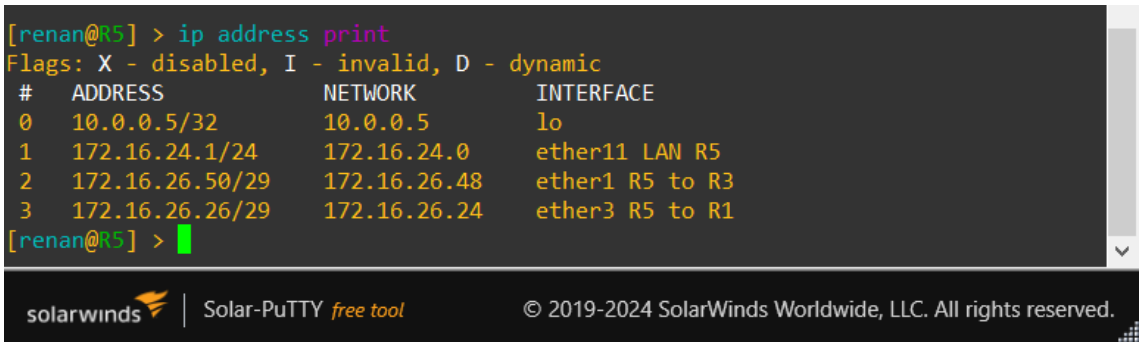


Ilustración 4. Direccionamiento ip enrutador R5

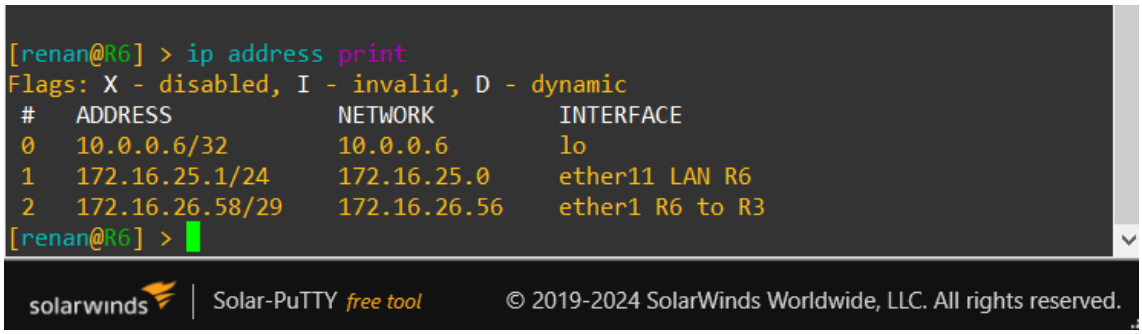


Ilustración 5. Direccionamiento ip enrutador R6

ANEXO B. *Configuración de rutas OSPF*

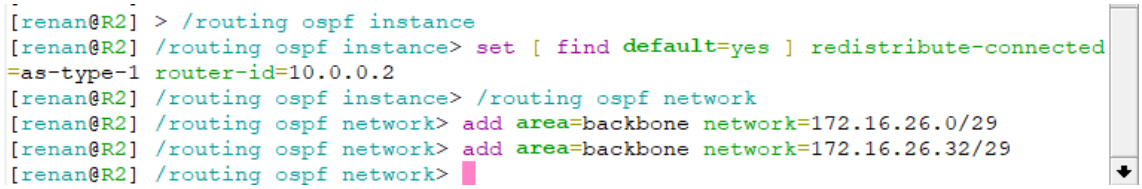


Ilustración 9. Configuración de rutas OSPF en enrutador R2

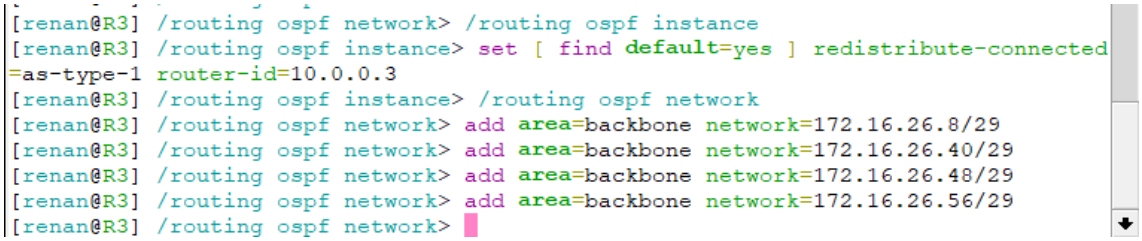


Ilustración 10. Configuración de rutas OSPF en enrutador R3

```
[renan@R4] /routing ospf network> /routing ospf instance
[renan@R4] /routing ospf instance> set [ find default=yes ] mpls-te-area=backbone red
istribute-connected=as-type-1 router-id=10.0.0.4
[renan@R4] /routing ospf instance> /routing ospf network
[renan@R4] /routing ospf network> add area=backbone network=172.16.26.16/29
[renan@R4] /routing ospf network> add area=backbone network=172.16.26.32/29
[renan@R4] /routing ospf network> add area=backbone network=172.16.26.40/29
[renan@R4] /routing ospf network>
```

Ilustración 11. Configuración de rutas OSPF en enrutador R4

```
[renan@R5] /routing ospf network>
[renan@R5] /routing ospf network> /routing ospf instance
[renan@R5] /routing ospf instance> set [ find default=yes ] redistribute-connected=as
-type-1 router-id=10.0.0.5
[renan@R5] /routing ospf instance> /routing ospf network
[renan@R5] /routing ospf network> add area=backbone network=172.16.26.24/29
[renan@R5] /routing ospf network> add area=backbone network=172.16.26.48/29
[renan@R5] /routing ospf network>
```

Ilustración 12. Configuración de rutas OSPF en enrutador R5

```
[renan@R6] /routing ospf network> /routing ospf instance
[renan@R6] /routing ospf instance> set [ find default=yes ] redistribute-connected=as
-type-1 router-id=10.0.0.6
[renan@R6] /routing ospf instance> /routing ospf network
[renan@R6] /routing ospf network> add area=backbone network=172.16.26.56/29
[renan@R6] /routing ospf network>
[renan@R6] /routing ospf network>
[renan@R6] /routing ospf network>
```

Ilustración 13. Configuración de rutas OSPF en enrutador R6

ANEXO C. *Configuración de MPLS*

```
[renan@R2] > /mpls ldp
[renan@R2] /mpls ldp> set enabled=yes lsr-id=10.0.0.2 transport-address=10.0.0.2

[renan@R2] /mpls ldp> /mpls ldp interface
[renan@R2] /mpls ldp interface> add interface="ether1 R2 to R1"
[renan@R2] /mpls ldp interface> add interface="ether2 R2 to R4"
[renan@R2] /mpls ldp interface> add interface="ether9 LAN R2"
[renan@R2] /mpls ldp interface> add interface=lo
[renan@R2] /mpls ldp interface> /mpls ldp neighbor
[renan@R2] /mpls ldp neighbor> add transport=136.128.28.8
[renan@R2] /mpls ldp neighbor>
```

Ilustración 14. Configuración de MPLS en enrutador R2

```
[renan@R3] > /mpls ldp
[renan@R3] /mpls ldp> set enabled=yes lsr-id=10.0.0.3 transport-address=10.0.0.3

[renan@R3] /mpls ldp> /mpls ldp interface
[renan@R3] /mpls ldp interface> add interface="ether1 R3  to R1"
[renan@R3] /mpls ldp interface> add interface="ether2 R3  to R4"
[renan@R3] /mpls ldp interface> add interface="ether3 R3  to R6"
[renan@R3] /mpls ldp interface> add interface="ether5 R3  to R5"
[renan@R3] /mpls ldp interface> add interface=lo
[renan@R3] /mpls ldp interface> /mpls ldp neighbor
[renan@R3] /mpls ldp neighbor> add transport=104.224.28.8
[renan@R3] /mpls ldp neighbor>
```

Ilustración 15. Configuración de MPLS en enrutador R3

```
[renan@R4] /mpls ldp neighbor> /mpls ldp
[renan@R4] /mpls ldp> set enabled=yes lsr-id=10.0.0.4 transport-address=10.0.0.4

[renan@R4] /mpls ldp> /mpls ldp interface
[renan@R4] /mpls ldp interface> add interface="ether1 R4  to R1"
[renan@R4] /mpls ldp interface> add interface="ether2 R4 to R3"
[renan@R4] /mpls ldp interface> add interface="ether3 R4  to R2"
[renan@R4] /mpls ldp interface> add interface="ether5 LAN R4"
[renan@R4] /mpls ldp interface> add interface=lo
[renan@R4] /mpls ldp interface>
```

Ilustración 16. Configuración de MPLS en enrutador R4

```
[renan@R5] /mpls ldp> set enabled=yes lsr-id=10.0.0.5 transport-address=10.0.0.5

[renan@R5] /mpls ldp> /mpls ldp interface
[renan@R5] /mpls ldp interface> add interface="ether1 R5 to R3"
[renan@R5] /mpls ldp interface> add interface="ether3 R5 to R1"
[renan@R5] /mpls ldp interface> add interface="ether11 LAN R5"
[renan@R5] /mpls ldp interface> add interface=lo
[renan@R5] /mpls ldp interface> /mpls ldp neighbor
[renan@R5] /mpls ldp neighbor> add transport=152.118.28.8
```

Ilustración 17. Configuración de MPLS en enrutador R5

```
[renan@R6] /mpls ldp neighbor> /mpls ldp
[renan@R6] /mpls ldp> set enabled=yes lsr-id=10.0.0.6 transport-address=10.0.0.6
[renan@R6] /mpls ldp> /mpls ldp interface
[renan@R6] /mpls ldp interface> add interface="ether1 R6 to R3"
[renan@R6] /mpls ldp interface> add interface="ether11 LAN R6"
[renan@R6] /mpls ldp interface> add interface=lo
[renan@R6] /mpls ldp interface> /mpls ldp neighbor
[renan@R6] /mpls ldp neighbor> add disabled=yes transport=136.145.28.8
[renan@R6] /mpls ldp neighbor>
```

Ilustración 18. Configuración de MPLS en enrutador R6

```
[renan@R2] > /interface vpls
[renan@R2] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:A2:14:4C:D2:A4
name=vpls1 remote-peer=10.0.0.1 vpls-id=1:2
[renan@R2] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:14:5E:96:E0:19
name=vpls2 remote-peer=10.0.0.4 vpls-id=2:4
[renan@R2] /interface vpls>
```

Ilustración 19. Configuración de VPLS en enrutador R2

```
[renan@R3] > /interface vpls
[renan@R3] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:40:CB:AA:05:2D
name=vpls1 remote-peer=10.0.0.1 vpls-id=1:3
[renan@R3] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:59:44:CE:E3:62
name=vpls2 remote-peer=10.0.0.5 vpls-id=5:3
[renan@R3] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:20:E9:43:DF:31
name=vpls3 remote-peer=10.0.0.6 vpls-id=3:6
[renan@R3] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:93:0F:38:96:70
name=vpls4 remote-peer=10.0.0.4 vpls-id=3:4
[renan@R3] /interface vpls>
```

Ilustración 20. Configuración de VPLS en enrutador R3

```
[renan@R4] /interface vpls> /interface vpls
[renan@R4] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:87:A3:07:0F:D0
name=vpls1 remote-peer=10.0.0.3 vpls-id=3:4
[renan@R4] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:79:30:E6:47:D7
name=vpls2 remote-peer=10.0.0.2 vpls-id=2:4
[renan@R4] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:2F:24:E5:70:D2
name=vpls3 remote-peer=10.0.0.1 vpls-id=1:4
[renan@R4] /interface vpls>
```

Ilustración 21. Configuración de VPLS en enrutador R4

```
[renan@R5] >
[renan@R5] > /interface vpls
[renan@R5] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:C4:E7:BF:04:A0
name=vpls1 remote-peer=10.0.0.3 vpls-id=5:3
[renan@R5] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:15:87:12:8E:10
name=vpls2 remote-peer=10.0.0.1 vpls-id=1:5
[renan@R5] /interface vpls>
```

Ilustración 22. Configuración de VPLS en enrutador R5

```
[renan@R6] > /interface vpls
[renan@R6] /interface vpls> add disabled=no l2mtu=1500 mac-address=02:79:8D:18:B5:EB
name=vpls1 remote-peer=10.0.0.3 vpls-id=3:6
[renan@R6] /interface vpls>
[renan@R6] /interface vpls>
```

Ilustración 23. Configuración de VPLS en enrutador R6

ANEXO E. *Topología completa de la red.*

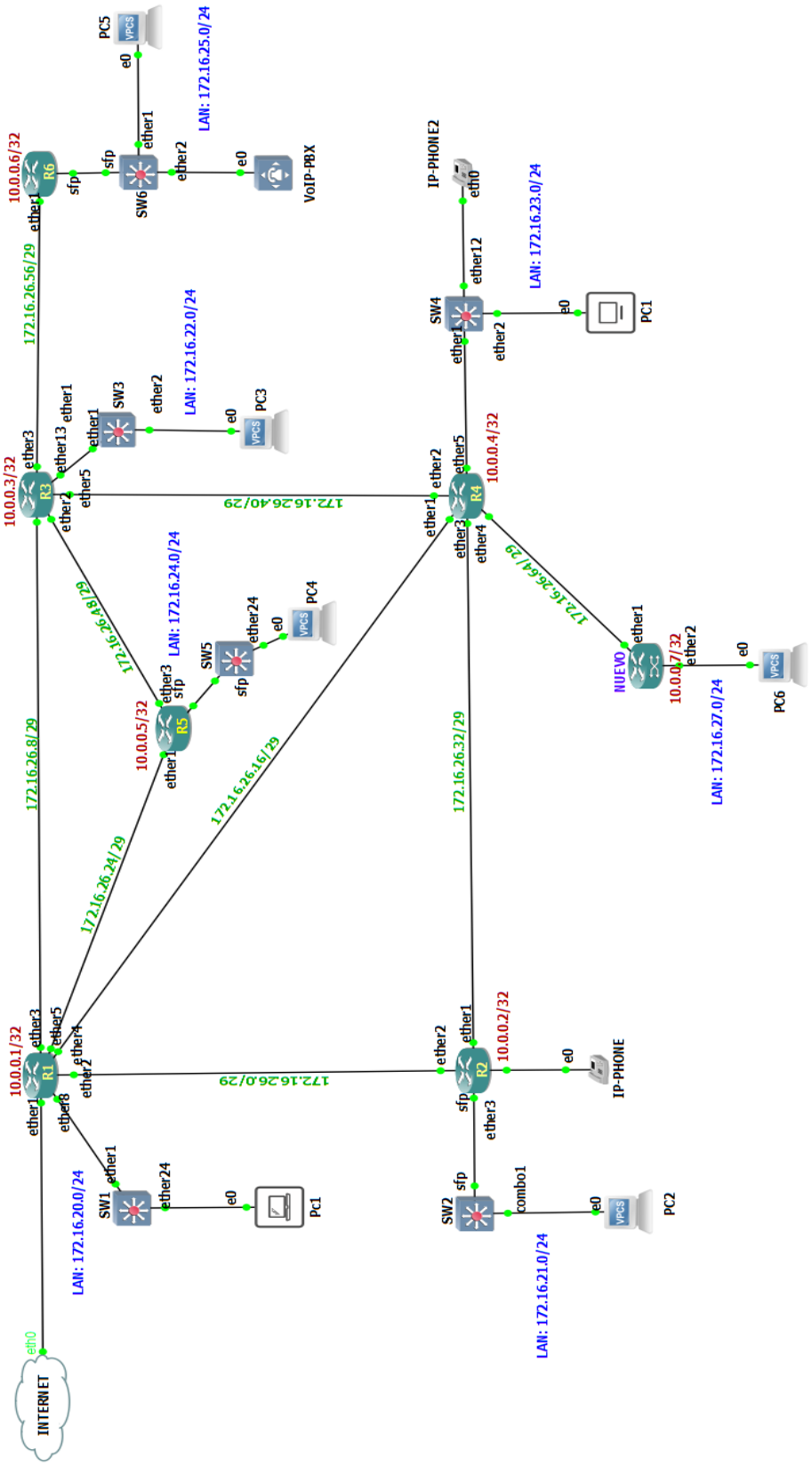


Ilustración 24. Topología final de red