

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN



**“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”**

**TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN
ELECTRÓNICA Y REDES DE COMUNICACIÓN**

AUTOR:

STYVEN OBRAYAN BUSTOS REPETTO

DIRECTOR:

MSC. CARLOS ALBERTO VÁSQUEZ AYALA

IBARRA, 2023



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

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

IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

| DATOS DEL CONTACTO | |
|---------------------|--|
| Cédula de identidad | 1003270830 |
| Apellidos y nombres | Bustos Repetto Styven Obrayan |
| Dirección | Ibarra, cdla del Chofer II etapa, Panamá y Brasil |
| E-mail | sobustos@utn.edu.ec |
| Teléfono móvil | 0991846642 |
| DATOS DE LA OBRA | |
| Título | “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” |
| Autor | Bustos Repetto Styven Obrayan |
| Fecha | 1 de diciembre de 2023 |
| Programa | Pregrado |
| Título | Ingeniero en Electrónica y Redes de Comunicación |
| Director | Ing. Carlos Alberto Vásquez, MSC |

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 esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 1 días del mes de diciembre de 2023

EL AUTOR



Bustos Repetto Styven Obrayan

CI: 1003270830

CERTIFICADO

MAGISTER CARLOS VÁSQUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de Titulación "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" Ha sido desarrollado por el señor Styven Obryan Bustos Repetto bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad



.....
MSc. Carlos Alberto Vásquez Ayala

CI: 1002424982

DIRECTOR

DEDICATORIA

Al culminar este arduo y gratificante viaje académico, no puedo dejar de expresar mi más profundo agradecimiento a quienes han sido mi apoyo incondicional a lo largo de este camino. Ustedes, mis queridos padres y amada familia han sido la fuente inagotable de inspiración, aliento y amor que me ha impulsado a alcanzar este logro significativo. Cada paso, cada desafío superado y cada triunfo obtenido, lleva impresa la marca de su inquebrantable respaldo. Su sacrificio, paciencia y dedicación han sido los cimientos sobre los cuales he construido este proyecto de vida académica. A ustedes les dedico con profundo cariño y gratitud mi trabajo de grado, como testimonio de que cada página escrita ha sido posible gracias a su incansable apoyo. Este logro es tan suyo como mío, y con humildad y amor les entrego el fruto de este esfuerzo conjunto. Gracias por ser mi mayor motivación y mi refugio constante. Este éxito es nuestro, y lo celebro con ustedes en el corazón.

Con todo mi amor y agradecimiento,

Styven Obryan Bustos Repetto

AGRADECIMIENTOS

Quiero expresar mi profundo agradecimiento a quienes han sido pilares fundamentales en el éxito de mi trabajo de grado. En primer lugar, a mi dedicado director de tesis, el Msc. Carlos Vásquez Ayala, cuya guía experta y apoyo constante han sido el faro que iluminó el camino a lo largo de esta travesía académica. Su sabiduría, paciencia y compromiso han sido esenciales para convertir este proyecto en una realidad, y estoy eternamente agradecido por su liderazgo inspirador.

También deseo extender mi gratitud a mi asesor de tesis, Msc. Jaime Michilena Calderón, cuyos valiosos aportes y perspectivas enriquecieron significativamente mi investigación. Su asesoramiento experto y su disposición a compartir su conocimiento han sido un regalo invaluable que ha dejado una marca indeleble en mi desarrollo académico.

A mi amada familia, quiero expresarles mi más sincero agradecimiento. Su constante respaldo emocional, comprensión y aliento fueron la fuerza motriz que me impulsó a superar los desafíos y alcanzar este logro significativo. Cada logro en este viaje lleva la huella de su amor incondicional. Gracias por ser mi fuente inagotable de inspiración y mi red de apoyo constante.

Este logro no solo representa mi esfuerzo individual, sino también el resultado de un trabajo en equipo donde cada uno de ustedes desempeñó un papel crucial. Con profundo agradecimiento y humildad, celebro este hito junto a ustedes.

Con gratitud, Styven Obryan Bustos Repetto

ÍNDICE

| | |
|--|-----------|
| IDENTIFICACIÓN DE LA OBRA..... | 1 |
| CONSTANCIAS..... | 2 |
| CERTIFICADO | 3 |
| DEDICATORIA | 4 |
| AGRADECIMIENTOS | 5 |
| ÍNDICE | 6 |
| ÍNDICE DE FIGURAS..... | 11 |
| ÍNDICE DE TABLAS | 14 |
| ÍNDICE DE ANEXOS | 15 |
| RESUMEN | 16 |
| ABSTRAC | 17 |
| Capítulo 1. Antecedentes | 18 |
| 1.1. Tema | 18 |
| 1.2. Problema | 18 |
| 1.3. Objetivos | 20 |
| <i>1.3.1. Objetivo general.....</i> | <i>20</i> |
| <i>1.3.2. Objetivos específicos.....</i> | <i>20</i> |
| 1.4. Alcance | 20 |
| 1.5. Justificación | 23 |
| Capítulo 2. Fundamentación Teórica | 25 |
| 2.1. Redes de área extendida tradicionales | 25 |
| <i>2.1.1. Funcionamiento WAN.....</i> | <i>26</i> |
| <i>2.1.2. Desventajas WAN.....</i> | <i>26</i> |

| | |
|---|----|
| 2.2. Multiprotocol label switching (MPLS)..... | 28 |
| 2.2.1. <i>Fundamentos MPLS</i> | 28 |
| 2.2.2. <i>Componentes MPLS</i> | 29 |
| 2.2.3. <i>Funcionamiento MPLS</i> | 30 |
| 2.2.4. <i>Desventajas de MPLS</i> | 30 |
| 2.3. Software defined network (SDN) | 31 |
| 2.3.1. <i>Arquitectura SDN</i> | 32 |
| 2.3.2. <i>Protocolo openflow</i> | 33 |
| 2.3.3. <i>Beneficios SDN</i> | 35 |
| 2.3.4. <i>Desafíos SDN</i> | 36 |
| 2.4. Software-Defined Wide Area Network (SD-WAN)..... | 37 |
| 2.4.1. <i>Definición SD-WAN</i> | 39 |
| 2.4.2. <i>Arquitectura SD-WAN</i> | 39 |
| 2.4.3. <i>Componentes SD-WAN</i> | 40 |
| 2.4.4. <i>Funcionamiento SD-WAN</i> | 40 |
| 2.4.5. <i>Tipos de arquitectura SD-WAN</i> | 42 |
| 2.4.6. <i>Beneficios de la SD-WAN</i> | 42 |
| 2.5. Redes de acceso | 44 |
| 2.5.1. <i>Arquitectura de la red de acceso</i> | 44 |
| 2.5.2. <i>Tipos de tecnologías de acceso</i> | 44 |
| 2.6. Graphical Network Simulator (GNS3) | 45 |

| | |
|--|----|
| 2.6.1. <i>Arquitectura GNS3</i> | 46 |
| 2.6.2. <i>Emulación y Simulación en GNS3</i> | 46 |
| 2.6.3. <i>Requerimientos de GNS3</i> | 47 |
| 2.6.4. <i>Ventajas y desventajas de GNS3</i> | 48 |
| 2.7. Fortinet..... | 49 |
| 2.7.1. <i>SD-WAN segura</i> | 50 |
| 2.7.2. <i>FortiGate</i> | 52 |
| 2.7.3. <i>FortiManager</i> | 52 |
| 2.7.4. <i>FortiAnalyzer</i> | 53 |
| Capítulo 3. Plan de Migración | 54 |
| 3.1. Requerimientos de la red WAN..... | 54 |
| 3.1.1. <i>Diseño de topología de red WAN tradicional</i> | 54 |
| 3.1.2. <i>Direccionamiento IP</i> | 57 |
| 3.1.3. <i>Funcionamiento de redes LAN</i> | 60 |
| 3.1.4. <i>Funcionamiento de redes WAN</i> | 61 |
| 3.1.5. <i>Tabla de requerimientos</i> | 64 |
| 3.1.6. <i>Criterios de configuración de la red tradicional</i> | 67 |
| 3.2. Selección de hardware y software | 68 |
| 3.2.1. <i>Análisis de Benchmark</i> | 68 |
| 3.2.2. <i>IEEE 29148</i> | 70 |
| 3.2.3. <i>Etapas de configuración de la topología</i> | 72 |
| 3.3. Emulación de la red | 73 |

| | |
|--|-----|
| 3.3.1. <i>Direccionamiento Ip</i> | 74 |
| 3.3.2. <i>Enrutamiento</i> | 74 |
| 3.4. Gestión de la red | 77 |
| 3.4.1. <i>FCAPS</i> | 77 |
| 3.4.2. <i>Protocolos de gestión de red</i> | 78 |
| 3.4.2. <i>Monitoreo de red WAN</i> | 79 |
| 3.5. Plan de migración | 83 |
| 3.5.1. <i>Etapas del plan de migración</i> | 83 |
| 3.5.2. <i>Evaluación y planificación</i> | 85 |
| 3.5.3. <i>Diseño de la arquitectura SD-WAN</i> | 89 |
| 3.5.4. <i>Selección del proveedor SD-WAN</i> | 90 |
| Capítulo 4. Emulación y análisis de resultados | 95 |
| 4.1. Emulación de la red SD-WAN | 95 |
| 4.1.1. <i>Configuración de puertos</i> | 96 |
| 4.1.2. <i>Configuración de enlaces SD-WAN</i> | 97 |
| 4.1.3. <i>Políticas de enrutamiento</i> | 98 |
| 4.1.4. <i>Reglas SD-WAN</i> | 103 |
| 4.2. Monitoreo de la red SD-WAN | 106 |
| 4.2.1. <i>Conectividad</i> | 108 |
| 4.2.2. <i>Ancho de banda</i> | 108 |
| 4.2.3. <i>Perdida de paquetes</i> | 109 |
| 4.2.4. <i>Latencia</i> | 110 |

| | |
|---|-----|
| | 10 |
| 4.2.5. <i>Jitter</i> | 111 |
| 4.3. Análisis de resultados | 112 |
| 4.3.1. <i>Emulación</i> | 112 |
| 4.3.2. <i>Transporte múltiple</i> | 112 |
| 4.3.3. <i>Monitoreo uso de enlaces SD-WAN</i> | 114 |
| 4.3.4. <i>Monitoreo calidad de enlaces SD-WAN</i> | 115 |
| 4.3.5. <i>Verificación de enrutamiento del tráfico SD-WAN</i> | 118 |
| CONCLUSIONES | 121 |
| RECOMENDACIONES..... | 123 |
| BIBLIOGRAFÍA | 125 |
| ANEXOS | 130 |

ÍNDICE DE FIGURAS

| | |
|---|----|
| Figura 1 Arquitectura de red SD-WAN FORTINET..... | 22 |
| Figura 2 Sistema tradicional WAN..... | 25 |
| Figura 3 Ejemplo de una red MPLS | 29 |
| Figura 4 Funcionamiento de una red MPLS | 30 |
| Figura 5 Arquitectura SDN..... | 32 |
| Figura 6 Arquitectura de openflow | 35 |
| Figura 7 Evolución de servicios en la nube | 38 |
| Figura 8 Arquitectura SD-WAN..... | 39 |
| Figura 9 Componentes SD-WAN | 40 |
| Figura 10 Funcionamiento SD-WAN..... | 41 |
| Figura 11 Arquitectura red de acceso óptico | 44 |
| Figura 12 Tecnologías red de acceso | 45 |
| Figura 13 Cuadrante mágico de Gartner para SD-WAN | 52 |
| Figura 14 Topología LAN Matriz | 55 |
| Figura 15 Topología LAN Sucursal-1 | 55 |
| Figura 16 Topología LAN Sucursal-2 | 56 |
| Figura 17 Topología de la red MPLS | 57 |
| Figura 18 Topología completa de ISP tradicional | 57 |
| Figura 19 Direccionamiento IP y topología de red tradicional..... | 59 |
| Figura 20 Red MPLS y sus componentes..... | 62 |
| Figura 21 Enlace de acceso a internet de la red..... | 64 |
| Figura 22 Configuración direccionamiento router “MATRIZ” | 74 |
| Figura 23 Configuración direccionamiento loopback router “R3”..... | 75 |
| Figura 24 Configuración OSPF del router R3 | 75 |

| | |
|--|-----|
| Figura 25 Configuración de protocolo MPLS | 76 |
| Figura 26 Asignación de interfaces que conforman MPLS | 76 |
| Figura 27 Routers y rutas aprendidas del R3 mediante MPLS..... | 77 |
| Figura 28 Prueba de conectividad entre el router “Matriz” y “LAN-SUCURSAL-1” | 79 |
| Figura 29 Prueba AB del router “Matriz” a “LAN-SUCURSAL-1”..... | 80 |
| Figura 30 Prueba de pérdida de paquetes entre router “MATRIZ” y “SUCURSAL-1” | 81 |
| Figura 31 Prueba de latencia entre router “MATRIZ” y “SUCURSAL-1” | 82 |
| Figura 32 Prueba de Jitter entre router “MATRIZ” y “SUCURSAL-1” | 83 |
| Figura 33 Diseño de solución SD-WAN | 89 |
| Figura 34 Cuadrante mágico de Gartner para SD-WAN | 91 |
| Figura 35 Configuración puerto 2 de la matriz..... | 97 |
| Figura 36 Configuración miembros SD-WAN matriz..... | 98 |
| Figura 37 Políticas de la matriz | 100 |
| Figura 38 Políticas de la sucursal 1 | 102 |
| Figura 39 Políticas de la sucursal 2 | 103 |
| Figura 40 Reglas de la matriz | 104 |
| Figura 41 Reglas sucursal 1 | 105 |
| Figura 42 Reglas sucursal 2 | 106 |
| Figura 43 Monitoreo de enlaces matriz | 107 |
| Figura 44 Monitoreo de enlaces sucursal 1 | 107 |
| Figura 45 Monitoreo de enlaces sucursal 2 | 108 |
| Figura 46 Conectividad entre matriz y sucursal 1 | 108 |
| Figura 47 Medición ancho de banda enlaces SD-WAN matriz..... | 109 |
| Figura 48 Medición pérdida de paquetes enlace SD-WAN matriz | 110 |

| | |
|---|-----|
| Figura 49 Medición latencia enlace SD-WAN matriz..... | 111 |
| Figura 50 Medición l jitter enlace SD-WAN matriz..... | 111 |
| Figura 51 Ping entre host matriz y host sucursal 1 por mdio de MPLS | 113 |
| Figura 52 Ping entre host matriz y host sucursal 1 por medio de tunel Ipvsec | 113 |
| Figura 53 Monitoreo enlaces sd-wan de la matriz..... | 114 |
| Figura 54 Monitoreo QoS enlaces sd-wan de la matriz..... | 116 |
| Figura 55 Latencia del ping MTZ a L-S1 | 117 |
| Figura 56 Monitoreo en base a SLA | 117 |
| Figura 57 Monitoreo trafico local matriz..... | 119 |

ÍNDICE DE TABLAS

| | |
|---|----|
| Tabla 1 Ventajas de las redes SDN..... | 35 |
| Tabla 2 Desafíos de las redes SDN..... | 36 |
| Tabla 3 Requisitos óptimos para un entorno Windows GNS3 | 47 |
| Tabla 4 Ventajas y desventajas de GNS3 | 48 |
| Tabla 5 Clase de direcciones IP privadas..... | 58 |
| Tabla 6 Distribución de direcciones IP completa para la emulación del ISP tradicional | 59 |
| Tabla 7 Interfaces de Loopback | 62 |
| Tabla 8 Requerimientos ancho de banda | 65 |
| Tabla 9 Requerimientos de pérdida de paquetes, latencia, jitter y disponibilidad..... | 66 |
| Tabla 10 Selección de hardware | 69 |
| Tabla 11 Selección de software d emulación de red..... | 71 |
| Tabla 12 Características del computador utilizado en la simulación..... | 73 |
| Tabla 13 FCAPS | 78 |
| Tabla 14 Comparativa de proveedores líderes en SD-WAN | 94 |

ÍNDICE DE ANEXOS

| | |
|--|-----|
| ANEXO A. Configuración de direccionamiento ip | 130 |
| ANEXO B. Configuración OSPF y MPLS | 132 |
| ANEXO C. Configuración miembros SD-WAN de la sucursal 1 y 2 | 137 |
| ANEXO D. Topología completa de red SD-WAN | 138 |

RESUMEN

El proyecto actual se centra en el desarrollo de un plan de migración de una red tradicional de un ISP a una red SD-WAN, con el propósito brindar mejoras en el rendimiento y administración de una red. Este plan se desarrolló por medio de herramientas de virtualización, lo que posibilitó emular ambas redes lo más cercano a la realidad posible. De este modo, a través de configuraciones sobre imágenes ISO, de distintos proveedores se llevó a cabo el diseño de las redes a emular.

En cuanto al desarrollo práctico, las redes, se configuraron de acuerdo con requerimientos obtenidos en el estudio del estado del arte recolectado en el capítulo II, De acuerdo con esto se procedió al desarrollo del diseño y configuración de las redes con sus respectivos protocolos de enrutamiento y asignación de ips. Creando escenarios de evaluación de rendimiento y administración.

En relación con las pruebas de funcionamiento, estas fueron realizadas entorno a parámetros como conectividad, ancho de banda, pérdida de paquetes, latencia y jitter. Donde finalmente tras ser comparado ambos escenarios se llega a la conclusión que la migración de una red tradicional a una red SD-WAN presenta varias mejoras tanto en rendimiento como en administración.

ABSTRAC

The current project focuses on the development of a migration plan from a traditional ISP network to an SD-WAN network, with the purpose of providing improvements in the performance and management of a network. This plan was developed through virtualization tools, which made it possible to emulate both networks as close to reality as possible. In this way, through configurations on ISO images from different suppliers, the design of the networks to emulate was carried out.

Regarding the practical development, the networks were configured in accordance with requirements obtained in the study of the state of the art collected in chapter II. According to this, the development of the design and configuration of the networks with their respective routing protocols was carried out. and ips assignment. Creating performance evaluation and administration scenarios.

In relation to the performance tests, these were carried out around parameters such as connectivity, bandwidth, packet loss, latency and jitter. Where finally, after comparing both scenarios, the conclusion is reached that the migration from a traditional network to an SD-WAN network presents several improvements in both performance and administration.

Capítulo 1. Antecedentes

El primer capítulo se orientó a la explicación de la necesidad del desarrollo de un plan de migración de una red de un proveedor de servicios tradicional a una red SD-WAN, 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

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.

1.2. Problema

En los últimos años, la comunicación y las redes tradicionales han ido evolucionando de manera acelerada, a tal punto que, las redes se están actualizando a “Redes Definidas por Software”, una tecnología que pretende revolucionar el uso de las redes tradicionales, encaminando a los proveedores de servicios y compañías a un mundo tecnológico evolucionado en la nube (Moreno. S, 2021). Las SDN (Software-Defined Network) son consideradas como una arquitectura emergente que es manejable, rentable y adaptable, lo que la hace ideal para las aplicaciones actuales que requieren gran ancho de banda. Esta arquitectura desacopla el control de red y las funciones de reenvío de datos, permitiendo que el control de la red se vuelva directamente programable y que la infraestructura subyacente se abstraiga para las aplicaciones y los servicios de red (López, 2020).

En el año 2020 la sociedad mundial sufrió uno de los mayores problemas que ha presentado la humanidad debido al virus SARS-CoV-2 (COVID-19), mismo que obligó a tomar medidas de confinamiento en todo el mundo generando nuevas necesidades tecnológicas en las organizaciones por el incremento en el uso de recursos digitales a través de Internet, el

cloud computing y de modelos de software como servicio (SaaS); llevando a las empresas a reconsiderar la forma en que se une e interconecta la red. (Moreno. S, 2021). A raíz de esto, en el mundo post-COVID, se puede evidenciar una gran demanda de tráfico por aplicaciones de video Streaming tales como Netflix, Skype o llamadas de Whatsapp entre otras(TELDAT, 2021). El fenómeno tecnológico (WFH) mejor conocido como teletrabajo supone un reto para empresas con múltiples sedes garantizar la continuidad de la actividad y la productividad, para ello, se busca soluciones optimas y simplificadas para mitigar los desafíos, con un alto nivel de calidad de servicios en la videoconferencia, el chat instantáneo y otros medios de comunicación. (LANNER, 2020)

Debido al aumento de tráfico, la complejidad de las redes y la seguridad que se requiere en la protección de datos, los equipos de TI demandan una exhaustiva administración, por lo cual se requiere una tecnología capaz de simplificar el trabajo diario. Es así como surge el interés de interactuar una red definida por software y hardware denominado SD-WAN. (López, 2020)

La nube, la virtualización, la movilidad, la IoT, el uso de la inteligencia artificial y el aprendizaje automático contribuyen con grandes cantidades de tráfico y datos en las WAN de las empresas. Desafortunadamente, también generan desafíos en cuanto a la confiabilidad y el rendimiento de la red y provocan vulnerabilidades de seguridad al ampliar exponencialmente la superficie de ataque. Estas tecnologías han creado la necesidad de los proveedores de servicios, actualizar su infraestructura de TI a una red simplificada y consolidada. Los sólidos servicios de redes y seguridad basados en VNF nativos en la nube son necesarios en el núcleo del proveedor de servicios, o en la infraestructura de TI empresarial central, y dentro de los perímetros de la red. (Versa Networks, 2022)

Por lo expuesto, se plantea realizar un plan de migración de una red de área extensa de un proveedor de servicios de internet tradicional a una red definida por software SD-WAN, a

fin de comprender esta tecnología de forma teórica y práctica, así como también atender y aportar al crecimiento investigativo en ciencia y tecnología en el área de redes y networking.

1.3. Objetivos

1.3.1. Objetivo general

Desarrollar un plan de migración de una red de área extensa (WAN) a una red SD-WAN de un proveedor de servicios de internet para optimizar el tráfico y disminuir la necesidad de carga operativa de administración.

1.3.2. Objetivos específicos

- Realizar un estudio del arte de una red tradicional de un proveedor de servicios, así como también de los elementos y funcionamiento de una red definida por software.
- Emular una arquitectura de red de un proveedor de servicios para entender e identificar vulnerabilidades que presente la misma.
- Elaborar un plan de migración de una red tradicional de un proveedor de servicio de internet a una red SD-WAN mediante la metodología PMBOK.
- Diseñar una red SD-WAN aplicada a un proveedor de servicios para evaluar el rendimiento que tiene una tecnología sobre la otra.
- Comparar los resultados obtenidos para determinar ventajas y desventajas encontradas en el desarrollo del plan de migración.

1.4. Alcance

La realización del presente proyecto se basa en la necesidad de optimizar una red tradicional de un proveedor de servicios, para mejorar el tiempo de respuesta de gestión de la red entre las sucursales de esta. De tal forma que se pueda simplificar el control y administración de la red, y así garantizar su competitividad en el área de las TIC's. Para ello se realizará un plan de migración de una red área extensa tradicional a una red definida por software, la cual permitirá ser escalable y robusta.

El desarrollo del proyecto será orientado por un sistema de gestión denominado PMBOK reconocido internacionalmente en lo que ha estándares de gestión, metodología, administración y dirección de proyectos se refiere, mismo que consta de 5 etapas las cuales son: Inicio, planificación, ejecución, desempeño y cierre (EAE, 2021). En base al sistema antes mencionado, en la primera etapa denominada “Inicio” se realizará un estudio del estado del arte de todos los conceptos relacionados con las redes de un proveedor de servicios tradicional, tales como situación actual, fundamentos, componentes, arquitectura y funcionamiento. Así como también, definición, arquitectura, opciones de despliegue, tipos de arquitectura y beneficios de una red SD-WAN. Lo cual brindará información necesaria para llevar a cabo los objetivos planteados en el plan de migración.

En la etapa de planificación se procederá a diseñar una red de un proveedor de servicios de internet (ISP) tradicional, en base a investigación realizada en la etapa de “inicio”. Los criterios de configuración se realizarán con la ayuda del software GNS3 que permitirá diseñar la red de tal forma que se pueda evidenciar el funcionamiento e interconexión de una matriz con sus sucursales, tomando en cuenta el hardware de la red y requerimientos determinados en la primera etapa, los cuales serán comparados y analizados mediante indicadores de gestión de red, tales como, pérdida de paquetes, jitter y latencia.

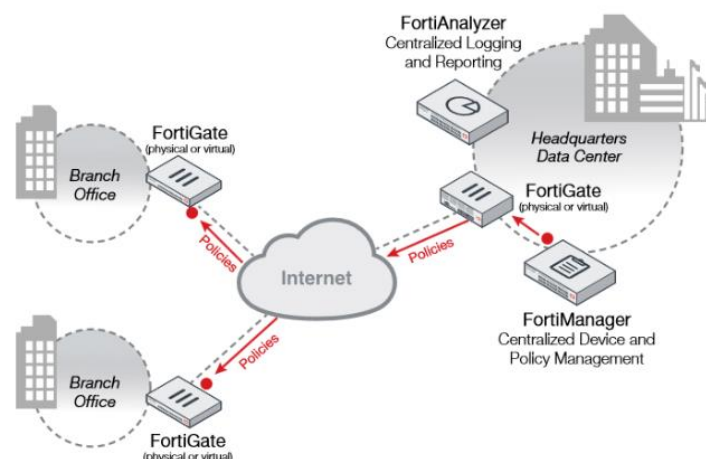
En la etapa de ejecución se procederá a diseñar el plan de migración de la WAN de un proveedor de servicios tradicional a SD-WAN, para ello se definirá los requerimientos de la red, posteriormente se realizará la selección de hardware por medio de un análisis de Benchmark, así como también el software con base a la norma IEEE 29148 los cuales permitirán identificar criterios para el despliegue de red que mejor se adapte a una red SD-WAN de un proveedor de servicios. Para el diseño se tomará en cuenta la arquitectura y elementos de una SDN, misma que cuenta de tres capas: Aplicación, Control y Datos. Estas capas se comunican a través de interfaces virtuales conocidas como API (Application

Programming Interfaces) que ofrecen un conjunto de protocolos para su comunicación, de acuerdo con las capas antes mencionadas se podrá llevar a cabo la selección de aplicaciones, controlador e infraestructura. De igual forma se revisará el protocolo Openflow ya que es el primer estándar que define la interfaz de comunicación entre el controlador y diferentes dispositivos de red SDN. La controladora a usarse es FortiManager cuya función principal es administrar y centralizar los equipos remotos, así como también, configurar las políticas de SD-WAN.

Finalmente, en la etapa de control y monitorización se diseñará una red similar a la realizada en la etapa de planificación con la diferencia que se integrará los equipos de SD-WAN de Fortinet (FortiGate, FortiManager y Forti Analyzer). La cual se pretende emular con una topología de red que cuente con una matriz que actuará como punto centralizado de control de la red y dos sucursales conectadas entre sí, tal como se muestra en la Figura 1. Misma que contarán con servicios que requieran comunicación en tiempo real como VoIP y Streaming para determinar e identificar los beneficios que presenta la red en gestión. Cabe recalcar que la emulación se realizara con la ayuda de las ISO obtenidas en la cuenta oficial de Fortinet.

Figura 1

Arquitectura de red SD-WAN FORTINET



Fuente: <https://app.bibguru.com/p/10a860af-f555-4219-ac34-271001435ff3>

Una vez diseñada y emulada la red del proveedor de servicios en ambos escenarios se procederá a comparar los resultados obtenidos, para sacar las conclusiones del trabajo realizado, así como también, verificar la optimización de la red en gestión, para de esta forma llegar a la etapa de “cierre” y establecer ventajas y desventajas del plan de migración.

1.5. Justificación

El aumento de recursos digitales a través de internet, la necesidad de ofrecer soluciones eficientes a clientes corporativos y la alta demanda de usuarios está dejando en evidencia las limitaciones de las redes WAN tradicionales, con equipos físicos limitados con características no actualizables lo que provoca una gran inversión en equipos físicos. Por este motivo el presente trabajo se realizará en orden práctico debido que las redes definidas por software ayudarían a los clientes corporativos y proveedores de servicios migrar su arquitectura actual a una arquitectura SD-WAN donde puedan administrar la información mucho más rápido, con un tiempo de respuesta progresiva.

La aparición en nuestras vidas del virus SARS-CoV-2 (COVID-19) ha permitido poner a prueba las actuales infraestructuras de red las cuales deben afrontar las nuevas necesidades y el aumento de tráfico en las redes tradicionales. Desde el punto de vista de un administrador de Telecomunicaciones un aspecto fundamental que se toca en esta temática está relacionado con las conexiones VPN utilizadas por los usuarios finales de una organización, de cara a cómo deben ser administradas y soportadas las comunicaciones en un estado de pandemia que se volvió un escenario global para toda organización, convirtiendo las telecomunicaciones en un elemento o recurso fundamental para la explotación del modelo productivo en el mundo a nivel económico, puesto que los usuarios finales aumentaron el uso de las capacidades de la infraestructura (Moncada, I, 2020).

Por lo anterior expuesto, se considera necesario modernizar el ambiente de telecomunicaciones para los próximos años, con el objetivo de realizar un análisis de los

principales recursos de telecomunicaciones en el ámbito nacional, y puntualmente, las WAN definidas por Software (SD-WAN), con un enfoque en el diseño e implementación de una red de área amplia empresarial que utilice redes definidas por software (SDN), con la que se determinará la forma más eficaz y eficiente para enrutar el tráfico hacia ubicaciones remotas, solución que además de garantizar un tráfico y seguridad en la red, permitirá obtener resultados comparables del antes y después, en el ámbito administrativo.

Por tal motivo el presente proyecto de migración de la red WAN de un ISP pretende adoptar las nuevas soluciones tecnológicas en vista de las necesidades y demanda actual (Calidad de servicio, agilidad, robustez, entre otros) y el mercado muestra un alto interés en la implementación SD-WAN, sin embargo, es necesario realizar pruebas de funcionamiento que generen confianza para considerar la migración de la red tradicional.

Capítulo 2. Fundamentación Teórica

El presente capítulo muestra los conceptos fundamentales para la elaboración del proyecto, como punto de inicio estableciendo conceptos fundamentales sobre redes de área extendida tradicionales con el fin de comprender el funcionamiento y elementos que integran una red WAN, así también se dará a conocer los cimientos de MPLS, haciendo énfasis en fundamentos, componentes, funcionamiento y carencias de esta tecnología, por último la explicación de SD-WAN, comenzando por entender desde su definición hasta los beneficios que brindan las redes definidas por software, permitiendo desarrollar posteriormente el diseño de las redes a tratar del proyecto.

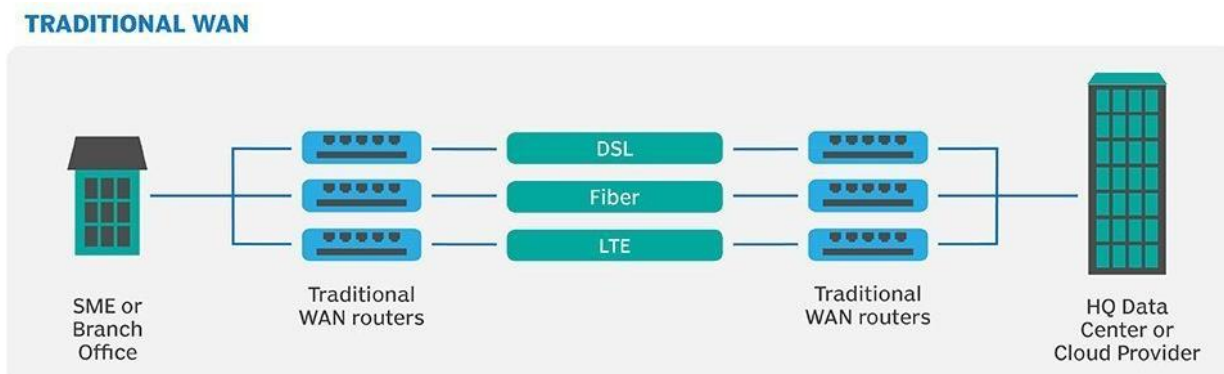
2.1. Redes de área extendida tradicionales

Las redes de área extendida (WAN) tienen la función de conectar varias Redes LAN (Redes de área local) entre sí, a través de routers y VPN's (Redes Privadas Virtuales), que facilitan la comunicación de datos, video y voz entre distintas sucursales y centro de datos ubicadas geográficamente distantes en una empresa. Las Redes de área extendida de acuerdo con el modelo OSI trabajan en las tres primeras capas: física, enlace de datos y red (López, 2020).

En la figura 2 se presenta la estructura de las redes WAN tradicionales.

Figura 2

Sistema tradicional WAN



Fuente: [https:// www.computerweekly.com/es/definicion/WAN-definida-por-software-o-SD-WAN](https://www.computerweekly.com/es/definicion/WAN-definida-por-software-o-SD-WAN)

2.1.1. Funcionamiento WAN

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. Esto implica el uso de capas de hardware subyacentes para completar las redes en su totalidad. La extensión de este tipo de redes hace que la gestión de los equipos de TI (Tecnologías de la Información) sea una tarea tediosa y laboriosa, debido a la gran cantidad de dispositivos de hardware instalados y procesos necesarios para controlar la actividad de la red. Además, para evitar que el tráfico malicioso se filtre en la red, la seguridad se maneja en forma de listas de bloqueo IP y de control de acceso.

La adición de más sucursales remotas requería de configuración de hardware adicional, lo que a su vez se traduce costos elevados para las empresas.

Las redes de área extensa tradicionales frente a las SD-WAN respecto a la escalabilidad es más compleja, ya que se necesita de una exhaustiva planificación, además de la implementación del soporte lógico requerido para establecer la infraestructura necesaria para que funcionen las operaciones.

2.1.2. Desventajas WAN

Como principales desventajas de las redes WAN tenemos las siguientes, según Thomas (2019):

- **Altos costos de configuración:** Las WAN son complicadas y complejas, por lo que su configuración es bastante costosa. Obviamente, cuanto más grande sea la WAN, más costosa será su configuración. Una razón por la que los costos de instalación son altos es la necesidad de conectar áreas remotas alejadas. Sin embargo, al usar redes públicas, se puede configurar una WAN usando solo software (SD-WAN), lo que reduce los costos de configuración. La relación precio/desempeño de las WAN es mejor ahora que hace una década o más.

- **Preocupaciones de seguridad:** Las WAN abren el camino para ciertos tipos de brechas de seguridad internas, como el uso no autorizado, el robo de información y el daño malintencionado de archivos. Si bien muchas empresas tienen algo de seguridad en lo que respecta a las sucursales, implementan la mayor parte de su seguridad en sus centros de datos para controlar y administrar la información enviada a sus localidades. Esta estrategia reduce los costos de administración, pero limita la capacidad de la empresa para lidiar directamente con las brechas de seguridad en sus localidades. Algunas empresas también tienen dificultades para comprimir y acelerar el tráfico SSL sin aumentar significativamente las vulnerabilidades de seguridad y crear nuevos desafíos de administración.
- **Problemas de mantenimiento:** El mantenimiento de una WAN es un desafío, sin duda alguna. Garantizar que el centro de datos esté funcionando 24 horas al día, 7 días a la semana es el mayor desafío de mantenimiento de todos. Los administradores de centros de datos deben poder detectar fallas antes de que ocurran y reducir el tiempo de inactividad del centro de datos tanto como sea posible, independientemente de las razones. El tiempo de inactividad es costoso, de hecho, un estudio realizado por Infonetics Research estima que medianas y grandes empresas en América del Norte pierden tanto como \$100 millones anuales por tiempo de inactividad en TI y tecnología de comunicaciones.
- Otras preocupaciones de mantenimiento incluyen la calidad del enlace y la degradación del desempeño, el rendimiento a pedido, el equilibrio de carga para el centro de datos, la administración del ancho de banda, la escalabilidad y la consolidación y visualización del centro de datos.

2.2. Multiprotocol label switching (MPLS)

Es una arquitectura que proporciona una eficiente designación, enrutamiento, envío y conmutación de flujos de tráfico a través de la red (López, 2020). MPLS enruta el tráfico utilizando la ruta más corta basada en "etiquetas", en lugar de direcciones de red, para manejar el reenvío a través de redes privadas de área amplia. Como solución escalable e independiente del protocolo, MPLS asigna etiquetas a cada paquete de datos, controlando la ruta que sigue el paquete mejorando en gran medida la velocidad del tráfico, por lo que los usuarios no experimentan tiempo de inactividad cuando están conectados a la red (Palo Alto Networks, 2023).

2.2.1. Fundamentos MPLS

CISCO (2018) sostiene que mediante MPLS, los proveedores de servicio de Internet pueden soportar servicios diferenciados o DiffServ (tal como se recoge en la norma RFC 3270). Ante el aumento de la demanda de nuevas aplicaciones, que suponen nuevos requerimientos de ancho de banda y tolerancia a retardos, MPLS ofrece una gran flexibilidad en cuanto a los diferentes servicios ofertados, lo que permite responder a esta demanda de forma óptima.

Además, MPLS ofrece un mecanismo sencillo para crear VPNs, ya que permite la creación de circuitos o túneles virtuales dentro de la red IP, y esto a su vez, garantiza poder aislar el tráfico y el acceso al mismo.

De igual forma, permite ahorrar costes entre un 10%-25% frente a otros servicios de datos, en función de la combinación específica de aplicaciones y de la configuración de red de la empresa. En los últimos años, se han efectuado diversas pruebas que incluso han alcanzado el 40 % de ahorro de costes respecto a ATM o Frame Relay.

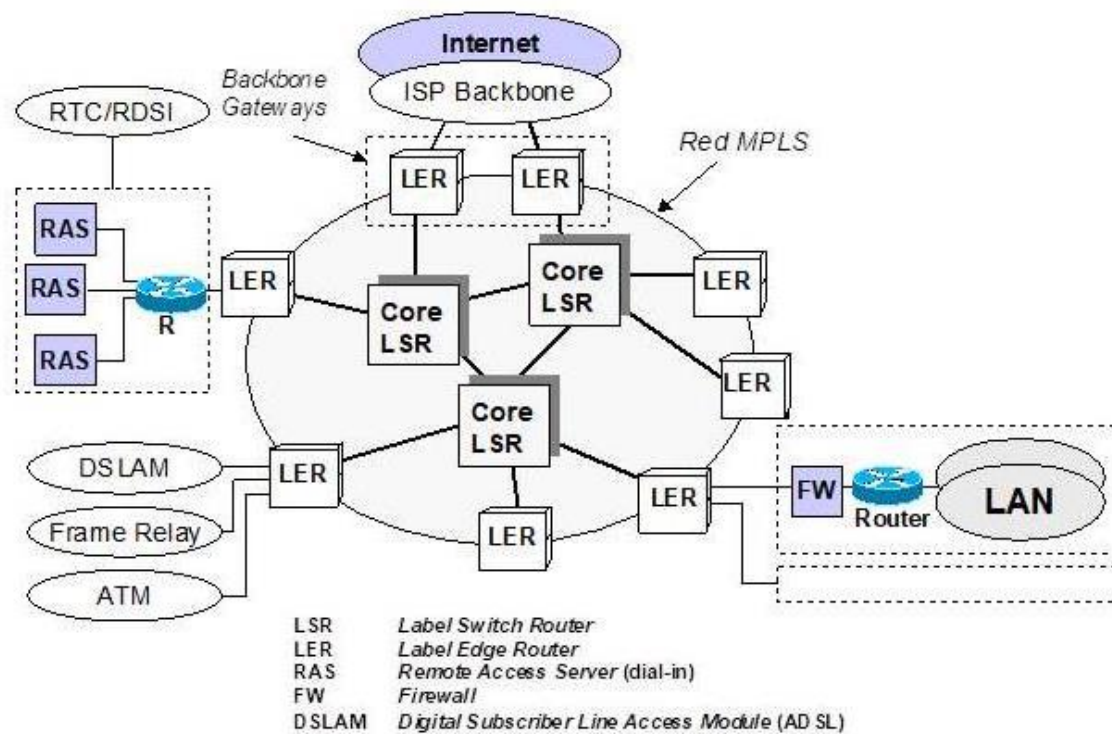
MPLS mejora el rendimiento, ya que al ser su naturaleza “muchos-a-muchos”, los diseñadores de red pueden reducir el número de saltos entre puntos, permitiendo a su vez mejorar los tiempos de respuesta y rendimiento de las aplicaciones.

2.2.2. Componentes MPLS

Una red MPLS está compuesta por dos tipos de routers: LER (Label Edge Router) y LSR (Label Switched Router), como se muestra en la figura 3 (Huidobro & Millán, 2002).

Figura 3

Ejemplo de una red MPLS



Fuente: <https://www.ramonmillan.com/tutoriales/mpls.php#elementosredmpls>

Huidobro & Millán (2002), describen a los routers de la siguiente forma:

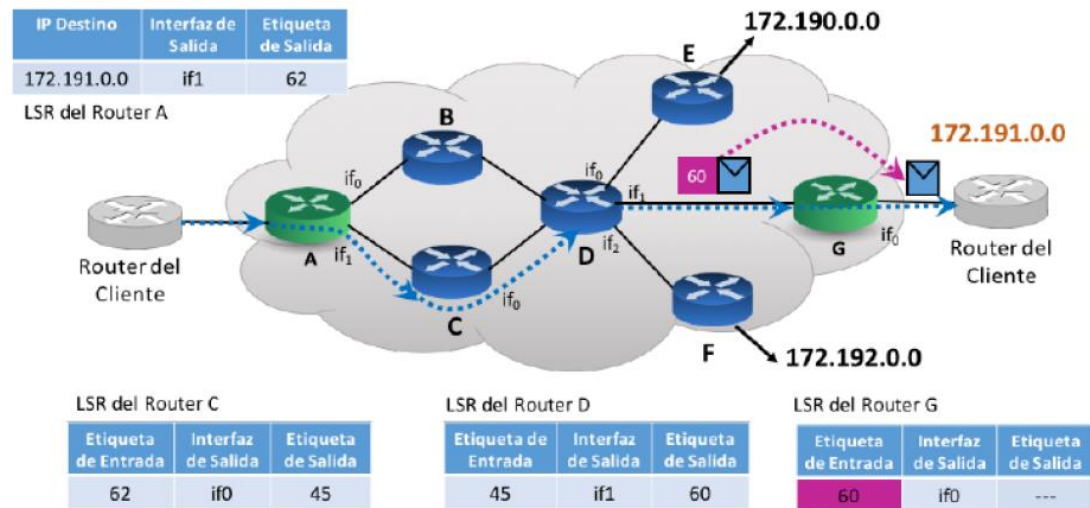
- **LER o PE (Provider Edge):** Son los routers que se encuentran ubicados en el borde de la red MPLS, encargados de encaminar y proporcionar conectividad asignando y retirando las etiquetas en la entrada o salida de la red MPLS.
- **LSR o P (Provider):** Son los routers que se encuentran ubicados en el núcleo de la red MPLS para efectuar encaminamiento de alto rendimiento basado en la conmutación por etiqueta.

2.2.3. Funcionamiento MPLS

En la Figura 4. se puede observar el funcionamiento de una red MPLS, sintetizado en los siguientes pasos: (López, 2020)

Figura 4

Funcionamiento de una red MPLS



Nota. Adaptado de López, J. (2020). Funcionamiento de una red MPLS. Emulación de una red SD-WAN (Software-Defined Wide Area Network) utilizando tecnología Fortinet y el Software GNS3

1. Establecimiento de rutas y asignación de etiquetas, antes de transferir los paquetes.
2. Distribución de etiquetas y creación de tablas.
3. Recepción del paquete e inserción de etiqueta.
4. Conmutación de etiquetas y reenvío del paquete.
5. Extracción de etiqueta y entrega del paquete.

2.2.4. Desventajas de MPLS

- **Despliegue prolongado:** La configuración y el despliegue de los circuitos MPLS es un proceso lento. Las organizaciones que utilizan MPLS tienen

dificultades para reaccionar rápidamente ante aumentos repentinos de la demanda de ancho de banda. (FS | community, 2022)

- **Seguridad:** MPLS no es tan seguro como SD WAN. Una simple mala configuración aumenta el riesgo de una vulnerabilidad de seguridad, y muchas empresas no pueden afrontar ese riesgo en la actualidad. (Parra, 2020)
- **Escalabilidad:** MPLS está diseñado para conectividad punto a punto y no para la nube. Por lo tanto, la WAN no tiene un centro de operaciones centralizado para reconfigurar ubicaciones o implementar nuevas y no permite una escalabilidad rápida. (Webber, 2022)
- **Implementación:** Si una empresa tiene oficinas en diferentes ubicaciones, la instalación y el despliegue a veces pueden llevar meses. (SPTel, 2021)
- **Coste:** El precio por ancho de banda en MPLS es mucho mayor que el de una conexión a Internet de banda ancha. (FS | community, 2022)

Por consiguiente, se puede decir que MPLS es una tecnología difícil de implementar y costosa respecto a tecnologías de nueva generación, además la transición a la nube y el trabajo remoto requiere que las empresas reconsideren su estrategia de red e implementen soluciones más rentables y eficientes por lo que se ha desarrollado redes SD-WAN o SD-WAN Híbridas como solución a los problemas de MPLS.

2.3. Software defined network (SDN)

Valencia & Santacruz (2015) sostienen que las (SDN) son un paradigma de redes emergentes que pretende cambiar las limitaciones de las infraestructuras de red actuales. En primer lugar, se rompe la integración vertical mediante la separación de la lógica de control de la red (el plano de control) de los routers y switches subyacentes que reenvían el tráfico (el plano de datos). En segundo lugar, con la separación de los planos de control y de datos, los conmutadores de red se convierten en dispositivos de reenvío simples y la lógica de control se

implementa en un controlador de lógica centralizado (o un sistema operativo de red), simplificando la aplicación de políticas y la reconfiguración.

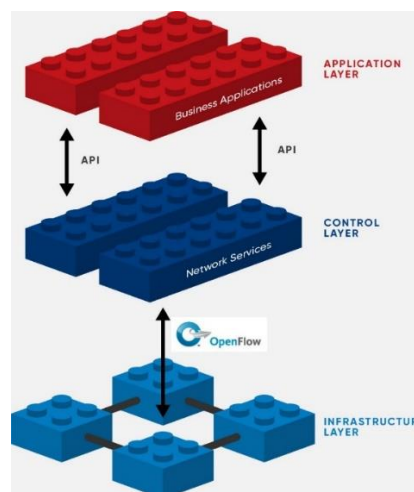
En resumen, las redes definidas por software tienen como objetivo principal separar el plano de control y el plano de datos de una red, lo que permite crear redes que son altamente programables, automatizables y flexibles según sus necesidades prioritarias gracias a la capacidad del servidor para tomar decisiones.

2.3.1. Arquitectura SDN

Según ONF (2023). La estructura de la red definida por software (SDN) se compone de tres niveles principales: la capa de aplicación, la capa de control y la capa de infraestructura o datos. Estos niveles se interconectan mediante interfaces southbound y northbound, también llamadas Application Programming Interfaces (API), que proporcionan un conjunto de protocolos para facilitar la comunicación entre dos aplicaciones, tal como se presenta en la figura 5.

Figura 5

Arquitectura SDN



Fuente: <https://opennetworking.org/sdn-definition/>

Donde la SDN es:

- **Directamente programable.** - El control de la red es programable de manera directa debido a que se encuentra separado de las funciones de reenvío.

- **Ágil.** - La separación del control y el reenvío brinda la posibilidad a los administradores de ajustar de forma dinámica el flujo de tráfico en toda la red para adaptarse a las demandas en constante cambio.
- **Administrado centralmente.** - La inteligencia de la red se encuentra concentrada de manera lógica en controladores SDN basados en software, los cuales poseen una visión integral de la red y se presentan a las aplicaciones y motores de políticas como un único conmutador lógico.
- **Configurado programáticamente.** - Gracias a SDN, los administradores de redes pueden configurar, gestionar, asegurar y optimizar los recursos de la red de manera ágil mediante programas dinámicos y automatizados, los cuales pueden ser escritos por ellos mismos, ya que no dependen de software propietario. Esto permite una mayor rapidez en las tareas de administración de la red.
- **Basados en estándares abiertos y proveedor neutral.** - Cuando se adopta mediante estándares abiertos, SDN simplifica la estructura y el funcionamiento de la red, ya que los controladores SDN se encargan de proporcionar las instrucciones en lugar de depender de múltiples dispositivos y protocolos específicos de cada proveedor. Esto facilita tanto el diseño como la operación de la red.

2.3.2. Protocolo openflow

OpenFlow es un protocolo de código abierto empleado para facilitar la comunicación entre el controlador y los dispositivos de conmutación. Estos dispositivos de conmutación, junto con el controlador, forman lo que se conoce como plano de control y plano de datos, respectivamente. El controlador OpenFlow asume la responsabilidad de determinar qué

acciones deben ser ejecutadas por el conmutador. Este enfoque de toma de decisiones puede ser reactivo o proactivo (Valencia & Santacruz, 2015).

Según (Tapia, 2022), el protocolo OpenFlow utiliza el puerto 6653 del protocolo TCP para las versiones v1.0 y v1.3 de OpenFlow. Antes de llevar a cabo cualquier acción, el protocolo establece un canal de intercambio de instrucciones entre el controlador y el conmutador conocido como canal OpenFlow. Este canal se forma mediante una exitosa conexión TCP a través de un proceso de enlace de tres vías (llamado así porque consta de tres pasos para establecer una conexión TCP). A partir de este punto, el protocolo OpenFlow se divide en dos partes, distribuyendo sus funciones de acuerdo con lo descrito a continuación:

En la primera parte, se inicia una sesión de control que implica la definición de una estructura de mensajes para intercambiar cambios en el flujo y recopilar estadísticas. Esto permite establecer una canalización lógica dentro de un conmutador con el fin de manejar diversos flujos de paquetes en una red.

La segunda parte del protocolo OpenFlow consiste en un proceso de configuración y administración que se basa en el Protocolo de Configuración de Red (NETCONF). Este proceso se encarga de asignar los puertos de un conmutador a un controlador específico y también establece los comportamientos a seguir en caso de una falla en la conexión del controlador.

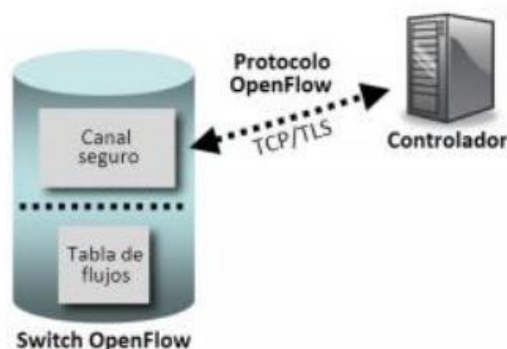
En la figura 6 se presenta el funcionamiento del protocolo OpenFlow, el cual constituye tres elementos básicos que son: (Machado, 2014)

- **Hardware:** Un switch que soporte el estándar OpenFlow.
- **Software (Controlador):** Un software que será el controlador de los dispositivos de red, donde el administrador de red define la manera de funcionamiento del dispositivo de red, ya sea como switch o como router.

- **Protocolo:** El protocolo OpenFlow que se encargará de la comunicación entre el hardware y el software.

Figura 6

Arquitectura de openflow



Nota. Adaptado de López, J. (2020). Arquitectura de OpenFlow. Emulación de una red SD-WAN (Software-Defined Wide Area Network) utilizando tecnología Fortinet y el Software GNS3

En resumen, el protocolo OpenFlow dirige el flujo de tráfico en función de los parámetros y requisitos específicos de las aplicaciones. Además, OpenFlow se puede implementar de manera sencilla en una red existente, ya sea física o virtual.

2.3.3. Beneficios SDN

De acuerdo con Maya (2021). En la tabla 1 se expone las ventajas de las redes definidas por software (SDN), fundamentadas por trabajos investigativos.

Tabla 1

Ventajas de las redes SDN

| Ventajas | Descripción |
|---|---|
| Visión general de la red | El controlador obtiene una visión general de toda la red, por consiguiente, se puede crear protocolos eficientes para la aplicación en el plano de datos. |
| Ahorro en el costo de desarrollo de la red | SDN se basa en sistemas de softwares libres y estándares abiertos. |

| | |
|--|---|
| Hardware y Software reducido | Al reducir los planos de datos con el plano de control se obtiene una mayor facilidad en el manejo, y los costes también se reducen al formarse elementos más sencillos. |
| Mayor fiabilidad y menor tiempo de inactividad. | SDN nos proporciona herramientas para aumentar la fiabilidad y reducir caídas de la red al momento de realizar una actividad de mayor demanda |
| Fácilmente Programable | SDN ofrece la capacidad de programar y configurar el plano de control con mayor facilidad al estar separado de la capa de datos. Los administradores pueden gestionar y optimizar los recursos de la red mediante programas automatizados que ellos mismos pueden crear |
| Más y mejor oferta de servicios de red. | SDN permite crear y operar de una manera segura las nuevas redes privadas para alojamiento de servicios como centro de cómputo laboratorios virtuales, entre otros |
| Mayor desempeño y flexibilidad de sus redes | SDN permite el uso de protocolos abiertos y desarrollo de sistemas, también permite el uso de interfaces abiertas denominadas API |
| Seguridad | Las SDN permiten crear redes privadas encriptadas compartiendo una infraestructura física igual |

Fuente: Adaptado de (Maya,2021)

2.3.4. Desafíos SDN

En la tabla 2, se expone los desafíos de las redes SDN según Maya (2021):

Tabla 2

Desafíos de las redes SDN

| Desafíos | Descripción |
|-----------------|---|
| Latencia | La latencia sería uno de los principales problemas ya que esta depende de la disponibilidad de los recursos virtualizados |

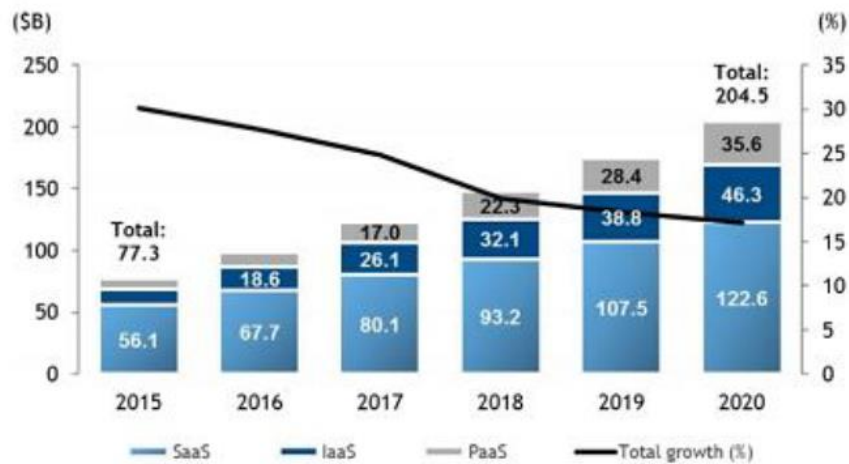
| | |
|--|---|
| Gestión limitada de los recursos | Todos los dispositivos con frecuencia deben de ser actualizados para que puedan funcionar |
| Mejores prácticas de Implementación | Por ser una tecnología nueva, la implementación puede ser un poco compleja que otros recursos en la red, por lo que es imprescindible comprender los factores que se deben tener en cuenta |
| Recursos de Desaprovisionamiento | Permite la implementación de recursos rápidamente lo cual debe gestionarse para tener buen rendimiento |
| Monitoreo de red | Para monitorear una red se necesita una API para que un SDN se pueda integrar. Cabe recalcar que hay pocos productos compatibles con el SDN |
| Seguridad | Como toda nueva tecnología es propensa a los riesgos de seguridad, como medida de seguridad es recomendable tener un listado de las amenazas para poder abordarlas, también se pueden implementar prácticas para mantener protegido el servicio |

Fuente: Adaptado de (Maya,2021)

2.4. Software-Defined Wide Area Network (SD-WAN)

SD-WAN es una SDN (Red Definida por Software) hecha con el objetivo de simplificar la gestión e implementación de una red de área amplia (WAN). Su particularidad es brindar un control centralizado, mayor tráfico de datos en la nube, mayor rendimiento, facilidad en automatización de procesos, mayor seguridad y notoriedad de aplicaciones e infraestructura. Perfecto para proveedores que buscan una evolución digital a bajo costo y funcional (Moreno, 2021).

El crecimiento de servicios en la nube es notorio, considerando los servicios: Software as a Service (Saas), Platform as a Service (PaaS) e Infrastructure as a Service (IaaS), Tal como se puede evidenciar en la Figura 7 (López, 2020).

Figura 7*Evolución de servicios en la nube*

Nota. Adaptado de López, J. (2020). Evolución de servicios en la nube. Emulación de una red SD-WAN (Software-Defined Wide Area Network) utilizando tecnología Fortinet y el Software GNS3

Dentro de los objetivos que las organizaciones buscan cumplir al implementar una red SD-WAN podemos encontrar los siguientes: (Juniper Networks, 2020)

- Operaciones simplificadas con una mayor resistencia de red
- Determinación de rutas, orquestación y agilidad más eficaces
- Capacidad de integrar la lógica y las políticas de la empresa en la red
- Reducción de los costos de transporte y optimización del uso de los recursos
- Mejora de la observabilidad y los análisis de las aplicaciones
- Aceleración de las aplicaciones (cada vez más para aplicaciones de la SaaS sensibles a la latencia, las pérdidas y la vibración)
- Refuerzo de la seguridad mediante un control de políticas detallado
- Mejora de la experiencia de usuario y de la calidad de servicio
- Programabilidad, mayor automatización y API más modernas

2.4.1. Definición SD-WAN

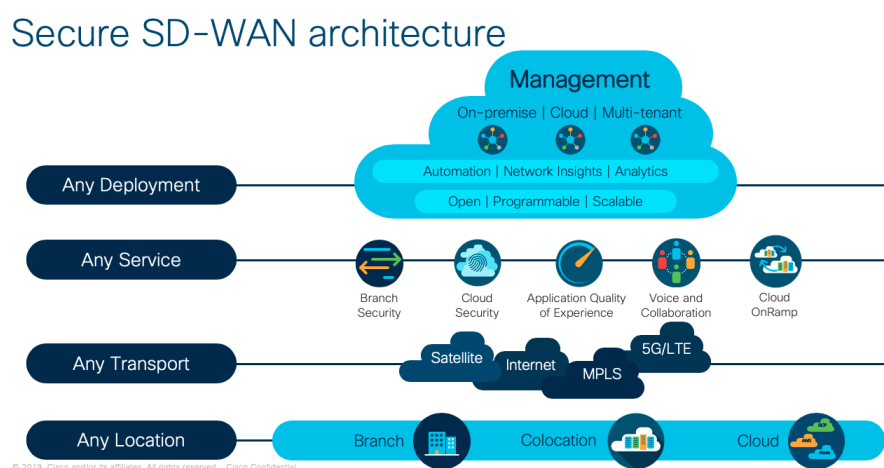
SD-WAN, es una tecnología que tiene la posibilidad de transformar el sector de las redes de área extendida encaminándose como sustituto de los servicios de optimización WAN, VPN-MPLS, automatización y administración de redes. Además, SD-WAN se puede comprender como un enfoque único que permite a los proveedores enrutar el tráfico a ubicaciones remotas, por medio de medios de transporte más adecuados, facilitando el monitoreo y administración del tráfico de la red en tiempo real (López, 2020).

2.4.2. Arquitectura SD-WAN

La arquitectura SD-WAN es una forma de construir una red de área amplia simplificada entre sitios y aplicaciones que pueden residir en cualquier lugar mientras aprovechan cualquier tipo de conectividad (es decir, banda ancha, LTE/5G, MPLS). La arquitectura está impulsada por aplicaciones que permite un acceso más rápido, confiable y seguro a las aplicaciones, tal como se muestra en la figura 8 (FORTINET, 2023).

Figura 8

Arquitectura SD-WAN



Fuente: <https://layots.com/sd-wan-over-mpls-explained/>

SD-WAN utiliza una arquitectura abstracta para su red. La red se divide en dos partes: el plano de control y el plano de reenvío. Su arquitectura puede estar basada en la nube con una red troncal o solo en las instalaciones (Layots, 2022).

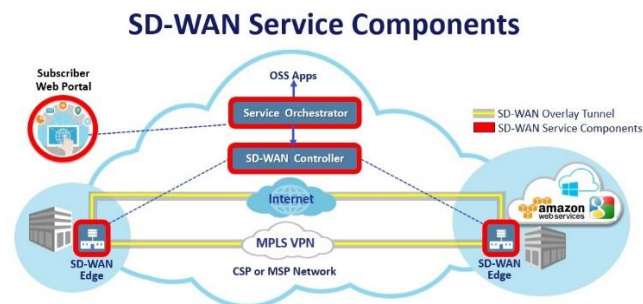
2.4.3. Componentes SD-WAN

Existen tres componentes principales en una red SD-WAN: El borde SD-WAN, el controlador y el orquestador. (Layots, 2022).

En la figura 9 se puede apreciar los componentes de la red SD-WAN con su respectiva descripción.

Figura 9

Componentes SD-WAN

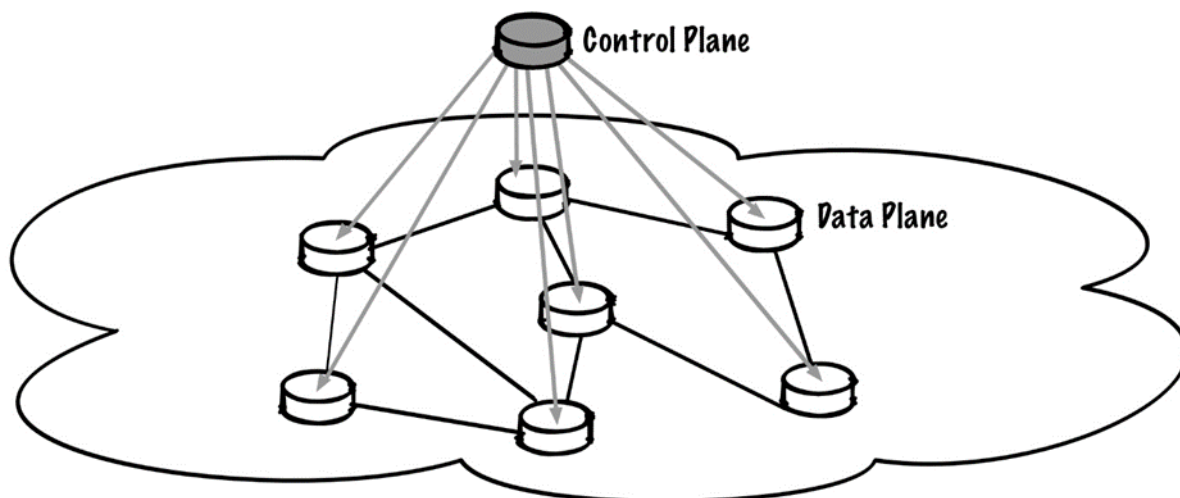


Fuente: <https://layots.com/sd-wan-over-mpls-explained/>

1. **El borde SD-WAN** es donde residen los puntos finales de la red. Puede ser una sucursal, un centro de datos remoto o una plataforma en la nube.
2. **Un SD-WAN Orchestrator** es el administrador virtualizado de la red, supervisa el tráfico y aplica la política y el protocolo establecidos por los operadores.
3. **El controlador SD-WAN** centraliza la administración y permite a los operadores ver la red a través de un único panel de vidrio y establecer políticas para que las ejecute el orquestador.

2.4.4. Funcionamiento SD-WAN

SD-WAN es solapamiento a una red actual, es decir una superposición a una red existente. Utiliza soluciones de tunelización para diferenciar la red física de la lógica, como se muestra en la figura 10 (López, 2020).

Figura 10*Funcionamiento SD-WAN*

Fuente: <https://www.juniper.net/mx/es/research-topics/sd-wan-explained.html>

SD-WAN implementa un controlador centralizado, que actúa como un panel único para administrar toda la solución. Se utiliza para establecer y mantener políticas. Esta política se utiliza para controlar las rutas de tráfico, los SLA, la conmutación por error, la supervisión, etc. Una vez definidas las políticas, se envían desde ese controlador centralizado a cada nodo SD-WAN para una configuración más dinámica (Layots, 2022).

Los nodos al adquirir de forma dinámica las configuraciones de las políticas, SD-WAN monitorea de forma inteligente el desempeño de los enlaces y envía el tráfico por la mejor ruta basada en los SLA. Llegado a este punto, desaparece cualquier interrupción del circuito al desviar el tráfico a un enlace de respaldo o redundante (López, 2020).

De esta forma SD-WAN permite a las empresas centradas en la nube ofrecer a los usuarios una calidad de experiencia de aplicación superior (QoEx). Al identificar las aplicaciones, una SD-WAN proporciona un enrutamiento inteligente que detecta aplicaciones a través de la WAN. Cada clase de aplicación recibe la QoS adecuada y la aplicación de directivas de seguridad, todo ello de acuerdo con las necesidades del negocio. El redireccionamiento a Internet local seguro del tráfico de aplicaciones de IaaS y SaaS desde la

sucursal proporciona los niveles más altos de rendimiento de la nube, al tiempo que protege a la empresa de las amenazas (aruba, 2022).

2.4.5. Tipos de arquitectura SD-WAN

Según Smith (2017) SD-WAN tiene tres principales arquitecturas: local, nube e híbrido.

1. **Local**, este tipo de arquitectura tiene por objeto comunicar entre cada dispositivo perimetral mediante instrucciones proporcionadas por el orquestador centralizado. El propósito de esta solución SD-WAN es reemplazar o aumentar la eficacia de una red privada ya existente. Con esta solución podrá realizar el modelado del tráfico en tiempo real.(BCM, 2023)
2. **Nube**, es una arquitectura SD-WAN habilitada para la nube, en esta solución se ofrece un dispositivo SD-WAN en el sitio que se conecta a una puerta de enlace (virtual) en la nube. Con esta arquitectura las empresas obtienen beneficios de una arquitectura local (es decir, modelado de tráfico en tiempo real y balanceo de carga/conmutación por error de múltiples circuitos), además de un mayor rendimiento y confiabilidad de sus aplicaciones en la nube (Smith, 2017).
3. **Híbrido**, combina las arquitecturas mencionadas anteriormente y es capaz de brindar una infraestructura WAN de malla completa confiable y conectividad a la nube de alto rendimiento. Este modelo híbrido permite mayor flexibilidad, sin embargo, en aspectos de configuración y seguridad se vuelve más complejo que en las soluciones anteriores (López, 2020).

2.4.6. Beneficios de la SD-WAN

De acuerdo con López (2020) los principales beneficios de una red SD-WAN respecto a las WAN tradicionales son las siguientes:

- Reducción de costos de circuito al utilizar opciones de conectividad de menor costo y mayor velocidad.
- Rentabilidad y fuerte impacto en redes empresariales: los límites geográficos desaparecen y el modelo de pago es en función del crecimiento.
- Mejora la visibilidad, es decir, identifican de manera inteligente las aplicaciones desde el primer paquete de tráfico de datos, con el fin de tomar decisiones más inteligentes.
- Control de múltiples rutas ya que permite diferentes conexiones para que fluya el tráfico como MPLS, conexión de banda ancha, un túnel IPsec, etc.
- Reduce la complejidad, es decir, su administración y control es a través de un único panel, el cual tiene una interfaz gráfica amigable para el usuario.
- Adopción de servicios basados en la nube. El tráfico en las WAN tradicionales generalmente pasa por el centro de datos para permitir un filtrado constante; esto origina una mayor latencia para servicios alojados en la nube. Por lo tanto, con SD-WAN se elimina la necesidad del tráfico de backhaul y mejora el rendimiento de aplicaciones en la nube.
- SD-WAN proporciona QoS ya que realiza un monitoreo de tráfico en tiempo real.
- Capacidad de admitir aplicaciones de gran ancho de banda de manera simultánea.
- Alto nivel de seguridad al contar con funciones como cifrado extremo a extremo y autenticación de los dispositivos.
- Tiempos de implementación más cortos ya que no necesita contar con una planificación anticipada, ni apoyo logístico para su implementación (ZTP). Por lo tanto, mejora la escalabilidad.

2.5. Redes de acceso

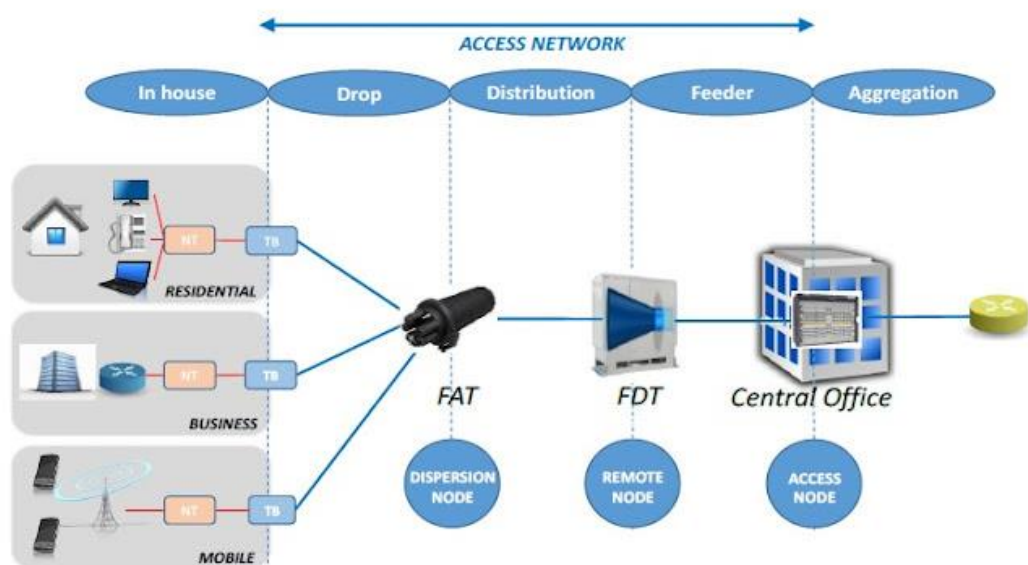
Las redes de acceso conocidas también como “última milla” es el segmento de red de telecomunicaciones que ofrece conectividad a los clientes finales con la red del proveedor (López, 2020).

2.5.1. Arquitectura de la red de acceso

Para entender mejor la arquitectura de una red de acceso, en la figura 11 se muestra la arquitectura de un tipo de red de acceso óptico, ya que en la actualidad es el más usado y mejora ampliamente el rendimiento de la red satisfaciendo eficazmente las demandas de los usuarios en servicios de banda ancha. En ella se puede observar cómo se conecta la red del proveedor hacia el cliente final cruzando por el nodo de acceso, remoto y dispersión (Technopedia, 2023).

Figura 11

Arquitectura red de acceso óptico



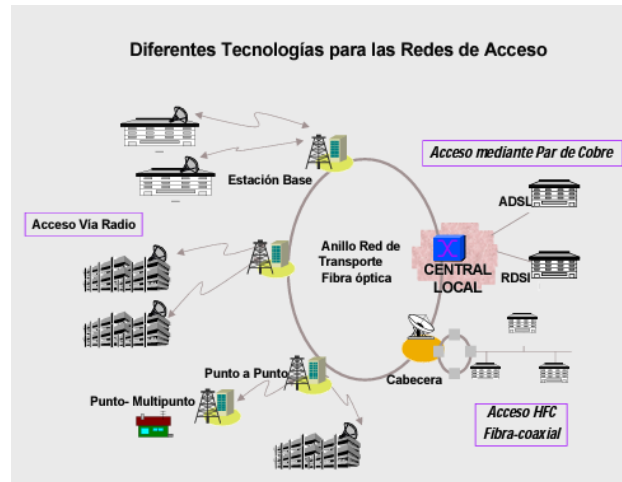
Fuente: <https://www.technopiasite.com/2018/12/what-is-access-networks-its-general.html>

2.5.2. Tipos de tecnologías de acceso

En la figura 12 se puede observar los diferentes tipos de tecnologías de acceso, mismas que se pueden clasificar en tres grupos: cableadas, inalámbricas y móviles (Avance Digital, 2023).

Figura 12

Tecnologías red de acceso



Nota. Adaptado de Veá i Baró, A. (2004). Diferentes Tecnologías para las redes de acceso. Historia, Sociedad, Tecnología y Crecimiento de la Red. Una aproximación divulgativa a la realidad más desconocida de Internet.

2.6. Graphical Network Simulator (GNS3)

GNS3 es un simulador de red que permite emular distintas topologías de red medianamente complejas y simular la red en gestión (Rejón, 2019).

A diferencia de Cisco Packet Tracer, el software permite emular tarjetas de red reales que permite utilizar puertos ethernet de forma física y lógica. (Todos hacemos TIC, 2015)

(AJPD soft, 2020) menciona que GNS3 para permitir completar las simulaciones, incluye:

- **Dynamips:** Un emulador de IOS que permite a los usuarios ejecutar binarios de imágenes IOS de Cisco Systems.
- **Dynagen:** Front-end basado en texto para Dynamips, Qemu y VirtualBox. Permite utilizar máquinas virtuales como un firewall PIX.
- **VPCS:** Emulador de PC con funciones básicas de networking (ping, traceroute, etc.).
- **IOU (IOS on Unix):** Compilaciones especiales de IOS provistas por Cisco para ejecutarse directamente en sistemas UNIX y derivados.

2.6.1. Arquitectura GNS3

(Teletrónica, 2018) indica que GNS3 tiene dos principales componentes: software GNS3 todo en uno (GUI) y Servidor/Máquina virtual GNS3.

2.6.1.1. Software GNS3 todo en uno (GUI)

Es la interfaz gráfica de usuario (GUI) de GNS3 y la parte de software necesaria para su operación. Este paquete instala el software todo en uno en la PC local (Windows, MAC, Linux), con lo cual se puede crear topologías utilizando el software incluido.

2.6.1.2. Servidor/Máquina virtual GNS3

Al crear topologías en GNS3 se utiliza la interfaz gráfica de usuario (GUI), los dispositivos creados deben estar alojados y ejecutados por una máquina virtual o servidor. Se tiene dos opciones:

2.6.1.2.1. Servidor local GNS3

Se ejecuta localmente en la misma PC donde instaló el software todo en uno GNS3. Por ejemplo, si está utilizando una PC con Windows, tanto la GUI como el servidor local se están ejecutando como procesos en Windows. Procesos adicionales como Dynamips también se ejecutarán en la PC.

2.6.1.2.2. Máquina Virtual GNS3

Si se decide usar la máquina virtual GNS3 (recomendado), se puede ejecutar la máquina virtual localmente en la PC utilizando software de virtualización como VMware Workstation o Virtualbox; o se puede ejecutar la máquina virtual GNS3 de forma remota en un servidor utilizando VMware ESXi o incluso en la nube.

2.6.2. Emulación y Simulación en GNS3

(GNS3, 2023) explica que el software admite dispositivos emulados y simulados.

- **Emulación:** GNS3 imita o emula el hardware de un dispositivo y ejecuta imágenes reales en el dispositivo virtual. Por ejemplo, podría copiar el IOS de

Cisco de un enrutador Cisco físico real y ejecutarlo en un enrutador Cisco emulado virtual en GNS3.

- **Simulación:** GNS3 simula las características y la funcionalidad de un dispositivo como un interruptor. No está ejecutando sistemas operativos reales (como Cisco IOS), sino un dispositivo simulado desarrollado por GNS3, como el conmutador de capa 2 integrado.

2.6.3. Requerimientos de GNS3

(GNS3, 2023) expone que para aprovechar al máximo las características de virtualización y emulación en un entorno avanzado. Se debería contar con los requerimientos óptimos expuestos en la Tabla 3.

Tabla 3

Requisitos óptimos para un entorno Windows GNS3

| Artículo | Requisito |
|--------------------------|--|
| Sistema operativo | Windows 7 (64 bits) o posterior |
| Procesador | CPU Intel Core i7 o i9 / CPU AMD R7 o R9 / 8 o más núcleos lógicos - Serie AMD-V / RVI o Intel VT-X / EPT |
| Virtualización | Se requieren extensiones de virtualización. Deberá habilitar esto a través del BIOS de su computadora. |
| Memoria | 32GB RAM |
| Almacenamiento | Unidad de estado sólido (SDD) con 80 GB de espacio disponible |
| Notas adicionales | La virtualización de dispositivos requiere un uso intensivo del procesador y la memoria. Más es mejor, pero un dispositivo configurado correctamente supera a la RAM y la potencia de procesamiento. |

Fuente: Adaptado de (GNS3,2023)

2.6.4. Ventajas y desventajas de GNS3

(GNS3, 2023) muestra que el software GNS3 ofrece varias ventajas sobre otros simuladores de red. Sin embargo, así como posee grandes virtudes presenta también ciertas desventajas que se detallan en la tabla 4.

Tabla 4

Ventajas y desventajas de GNS3

| Ventajas | Desventajas |
|--|--|
| Software libre | |
| Software de código abierto | |
| Sin tarifas de licencia mensuales o anuales | Las imágenes de Cisco deben ser proporcionadas por el usuario (descárguelas de Cisco.com, compre una licencia VIRT o copie desde un dispositivo físico). |
| No hay limitación en la cantidad de dispositivos compatibles (la única limitación es su hardware: CPU y memoria) | |
| Admite múltiples opciones de conmutación (módulo Etherswitch NM-ESW16, imágenes IOU/IOL Layer 2, VIRT IOSvL2) | |
| Admite todas las imágenes VIRT (IOSv, IOSvL2, IOS-XRv, CSR1000v, NX-OSv, ASA v) | No es un paquete autónomo, pero requiere una instalación local de software (GUI). |
| Admite entornos de múltiples proveedores | |
| Se puede ejecutar con o sin hipervisores | |
| Admite hipervisores gratuitos y de pago (Virtualbox, estación de trabajo VMware, reproductor VMware, ESXi, Fusion) | |
| Dispositivos descargables, gratuitos, preconfigurados y optimizados disponibles para simplificar la implementación | |

| | |
|---|---|
| Soporte nativo para Linux sin necesidad de software de virtualización adicional | GNS3 puede verse afectado por la configuración y las limitaciones de su PC debido a la instalación local (cortafuegos y configuración de seguridad, políticas de portátiles de la empresa, etc.). |
| Software de múltiples proveedores disponible gratuitamente | |
| Comunidad grande y activa (más de 800 000 miembros) | |

Fuente: Adaptado de (GNS3,2023)

2.7. Fortinet

Fortinet es una compañía multinacional de Estados Unidos que se dedica a la seguridad en redes y la seguridad informática fundada en el año 2000. La visión de Fortinet es de suministrar una seguridad amplia, integrada y de alto rendimiento en toda la infraestructura tecnológica de las empresas (Lemus, 2020).

Además, Fortinet ofrece productos de seguridad de red y contenido de alta calidad, así como productos de acceso seguro que trabajan juntos en un sistema corporativo llamado Security Fabric. El Security Fabric es exclusivo de Fortinet y utiliza procesadores de seguridad, un sistema operativo intuitivo y datos de amenazas para proporcionar una seguridad confiable, un rendimiento excelente y una administración sencilla. El enfoque unificado de Fortinet a través de su Security Fabric es integral, automatizado y amplio, lo que permite reducir y administrar la superficie de ataque a través de una amplia visibilidad integrada, detener amenazas avanzadas con la prevención integrada de amenazas basada en la IA y simplificar las operaciones a través de la automatización y la orquestación (FORTINET, 2023).

FORTINET cuenta con una amplia gama de productos de hardware y software que están diseñados para ofrecer servicios de conexión, autenticación, VoIP, SD-WAN y otras aplicaciones. Entre los productos más destacados se encuentran FortiGate, FortiManager y FortiAnalyzer. Estos dispositivos y su funcionalidad de Secure SD-WAN son importantes temas de emulación que se explican en detalle (López, 2020).

2.7.1. SD-WAN segura

FortiGate proporciona una solución de SD-WAN segura, escalable, rápida y flexible tanto en las instalaciones como en la nube. La solución de SD-WAN segura de Fortinet es adecuada para empresas globales que dan prioridad a la seguridad y a la nube, así como para fuerzas laborales híbridas. Su enfoque de redes seguras utiliza un sistema operativo que integra SD-WAN, next-generation firewall (NGFW), enrutamiento avanzado y funciones de puerta de enlace de aplicaciones ZTNA para: (FORTINET, 2023)

- Construir una plataforma fundamental para una transición sin problemas a SASE y arquitectura de sucursales SD.
- Brindar una calidad de experiencia superior en cualquier escala.
- Acelerar la convergencia de la red y la seguridad para todos los usuarios, y simplificar la arquitectura WAN.
- Orquestar políticas de seguridad y red coherentes sin importar dónde se encuentren los usuarios.
- Lograr eficiencias operativas a través de la automatización, el análisis profundo y la autorrecuperación.

Las empresas están adoptando estrategias de confianza cero para mejorar la seguridad en entornos altamente distribuidos. La solución de SD-WAN segura de Fortinet, combinada con FortiManager y FortiAnalyzer, proporciona una visibilidad detallada del tráfico de red, analiza los datos de tráfico y automatiza la respuesta basándose en los resultados. Estas características son necesarias para acelerar las iniciativas de confianza cero (FORTINET, 2023).

(Forti One, 2023) indica 6 razones por las que Secure SD WAN de Fortinet es una buena opción:

1. **Seguridad avanzada:** Una SD WAN segura de Fortinet cuenta con funciones de seguridad de vanguardia, como cortafuegos de nueva generación, detección y prevención de intrusiones, filtrado de URL, cifrado y mucho más.
2. **Conectividad optimizada:** con Secure SD WAN de Fortinet, las empresas pueden aprovechar al máximo su conectividad, incluyendo la utilización de múltiples conexiones de red y la optimización del tráfico de datos.
3. **Gestión simplificada:** la solución se gestiona de forma centralizada, lo que permite a las empresas gestionar fácilmente sus redes y dispositivos de seguridad desde una única ubicación.
4. **Flexibilidad:** La Secure SD WAN de Fortinet es altamente personalizable y escalable, lo que permite a las empresas adaptar la solución a sus necesidades específicas.
5. **Reducción de costes:** Al aprovechar múltiples conexiones de red, la Secure SD WAN de Fortinet ayuda a las empresas a reducir sus costes de ancho de banda y aumentar la eficiencia de la red.
6. **Adopción más fácil:** Con Gartner prediciendo que 25% de las empresas adoptarán SD WAN en los próximos dos años, Secure SD WAN de Fortinet ofrece una solución fácil de adoptar y desplegar para las empresas que buscan una solución WAN segura y eficiente.

En la figura 13, se muestra el cuadrante mágico de Gartner donde Fortinet fue nombrada líder tres años seguidos y obtuvo el puesto más alto en capacidad de ejecución dos años seguidos (FORTINET, 2023).

Figura 13

Cuadrante mágico de Gartner para SD-WAN



Fuente: <https://www.fortinet.com/lat/solutions/gartner-wan-edge>

2.7.2. *FortiGate*

Este tipo de dispositivo o software se puede describir como un sistema "todo en uno" que permite la creación de redes seguras. Incluye características como prevención de intrusos (IPS), filtrado web, inspección SSL, SD-WAN, y más. Estos dispositivos son capaces de satisfacer las necesidades de rendimiento de las arquitecturas de TI híbridas altamente escalables, lo que reduce la complejidad y administra los riesgos de seguridad. Pueden ser implementados como hardware local, administrados como máquina virtual, o a través de SaaS en la nube. Los dispositivos de nivel de entrada tienen un precio inicial de alrededor de \$500, mientras que los modelos de gama alta para empresas pueden llegar a costar hasta \$350,000, como es el caso del modelo 7060E-8 (López, 2020).

2.7.3. *FortiManager*

Los equipos FortiManager ofrecen una solución centralizada para administrar cualquier cantidad de dispositivos de seguridad Fortinet, desde unos pocos hasta varios miles. Esto incluye FortiGate, FortiWifi, FortiCarrier, así como otros productos como FortiAP, FortiSwitch y FortiExtender. Los administradores de redes pueden mejorar la gestión de sus dispositivos al agruparlos en dominios de administración (ADOMS), aplicar políticas de

manera más eficiente y distribuir actualizaciones de firmware y contenido de seguridad. FortiManager es un dispositivo de seguridad muy versátil que ofrece una amplia gama de opciones de despliegue, flexibilidad de crecimiento, personalización avanzada mediante APIs y un proceso de licenciamiento sencillo (FORTINET, 2023).

2.7.4. FortiAnalyzer

Este dispositivo ofrece una herramienta robusta para administrar y analizar registros, generar informes personalizados automáticamente, ejecutar diferentes utilidades de diagnóstico y herramientas complementarias de análisis de vulnerabilidades o escaneo de redes. Además, permite reportar y almacenar eventos de seguridad, tráfico de red, contenido web y mensajes para medir el cumplimiento de las políticas de una organización. Funciona en completa sincronización con FortiManager como punto central de control, lo que significa que se puede gestionar tanto las funcionalidades de FortiAnalyzer como de FortiManager desde un solo dispositivo, ya sea en hardware o en modo virtual (López, 2020).

Estos tres dispositivos tienen la ventaja de contar con una interfaz gráfica intuitiva y fácil de usar, lo que permite que los administradores de redes comprendan el despliegue de la red con mayor facilidad y encuentren fallos o problemas de forma más eficiente.

Capítulo 3. Plan de Migración

En el presente capítulo se describe el plan de migración de una red tradicional a una red SD-WAN, la cual se ha dividido en 6 etapas (Evaluación y planificación, diseño, selección de proveedor, implementación, migración y monitoreo). La primera etapa está enfocada a identificar y recopilar requerimientos de una red tradicional, lo cual es fundamental para la etapa de diseño, donde se procede a identificar métricas fundamentales en el funcionamiento de la red, posterior se realiza el análisis y selección de hardware y software, para continuar, se emula la red WAN tradicional con sus respectivos criterios de configuración dando paso a la etapa de desempeño, donde se procede a medir el rendimiento de la red emulada para obtener resultados que permiten determinar carencias de gestión y rendimiento de la red tradicional. Posteriormente se aplican los mismos pasos realizados en la construcción de la red tradicional, pero adaptándola a la tecnología SD-WAN para finalmente comparar resultados entre ambas arquitecturas y así poder tener una comparativa de resultados obtenidos en ambas topologías.

3.1. Requerimientos de la red WAN

En lo referente a la recopilación de los requerimientos de la red WAN, se procede a diseñar una topología de red de un ISP tradicional con su respectivo direccionamiento ip, mismas que permiten tener una visión general de la infraestructura actual y comprender como trabajará la emulación.

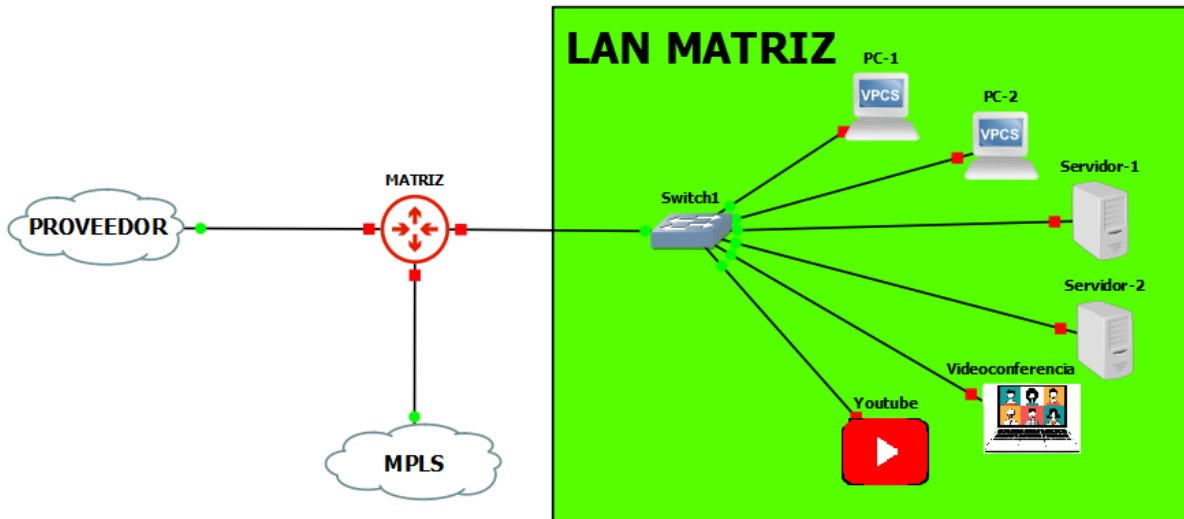
3.1.1. Diseño de topología de red WAN tradicional

En esta sección se proporciona información detallada sobre la topología de la red, así como los componentes de las redes de área local (LAN) y de área extendida (WAN), con sus respectivas ubicaciones. La arquitectura de la red consta de tres redes de área local (LAN) ubicadas en diferentes lugares geográficos, cada una desempeñando un papel específico. La primera LAN se encuentra en la sede principal y se le denomina "Matriz". Esta sede principal

alberga recursos a los que las demás LAN necesitan acceder, y también sirve como punto de control centralizado de toda la red, como se muestra en la figura 14.

Figura 14

Topología LAN Matriz

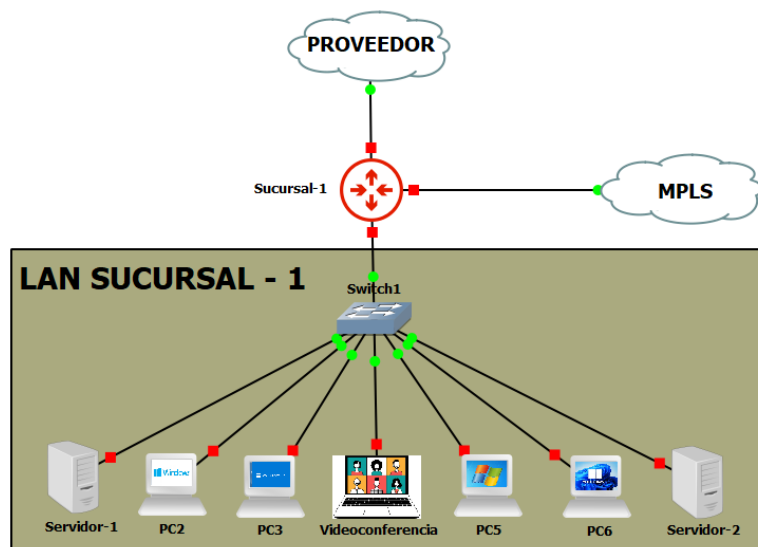


Fuente: GNS3(2.2.37)

En segundo lugar, se encuentra una red de área local (LAN) conocida como "Sucursal-1" que funciona como una sucursal convencional, lo que implica que requiere acceder a los recursos de la "Matriz", tal y como se indica en la figura 15.

Figura 15

Topología LAN Sucursal-1

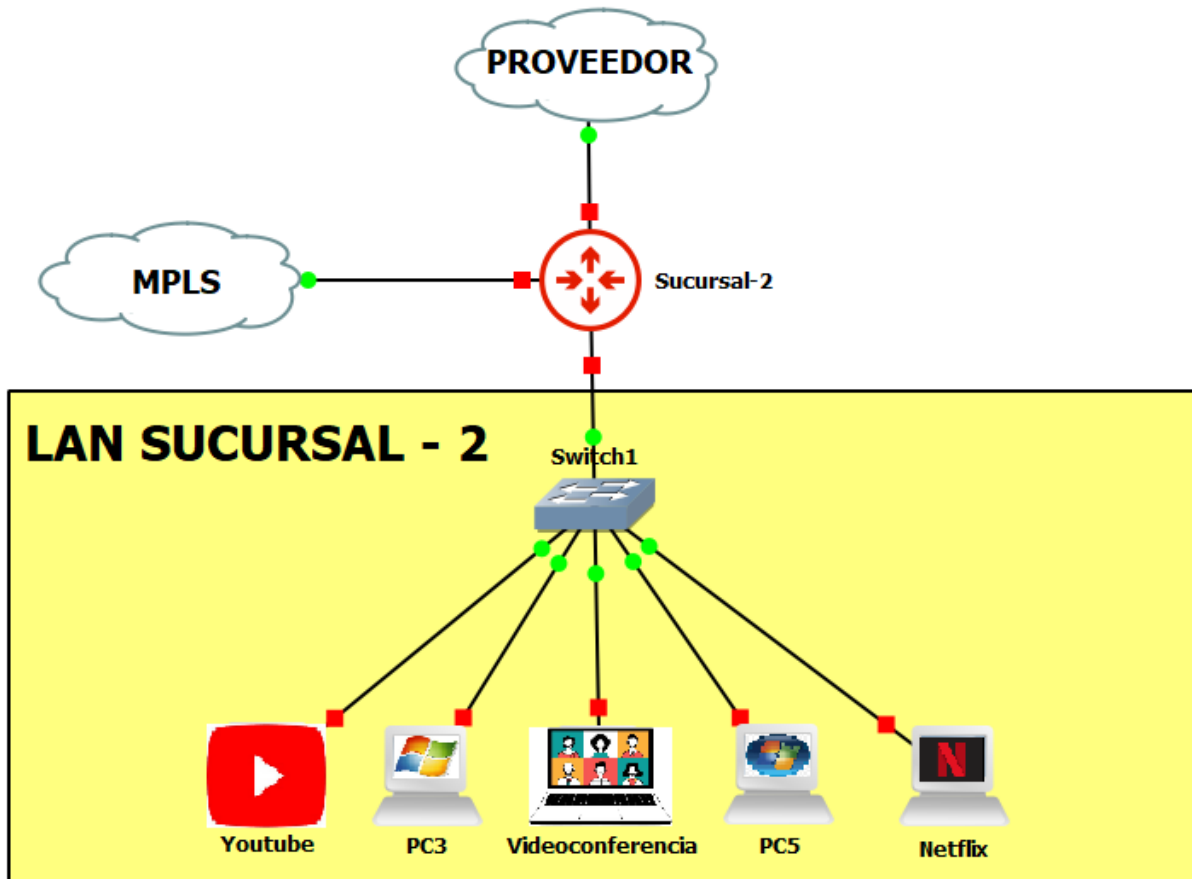


Fuente: GNS3(2.2.37)

En la figura 16 se muestra la LAN denominada "Sucursal-2", cuya finalidad es similar a la de la Sucursal-1: tener acceso a los recursos de la matriz.

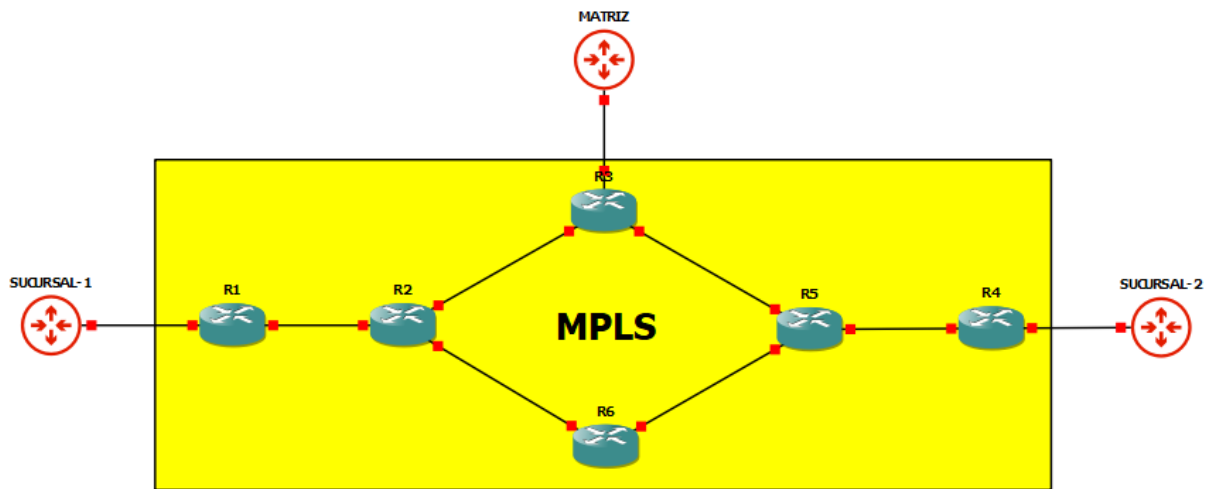
Figura 16

Topología LAN Sucursal-2



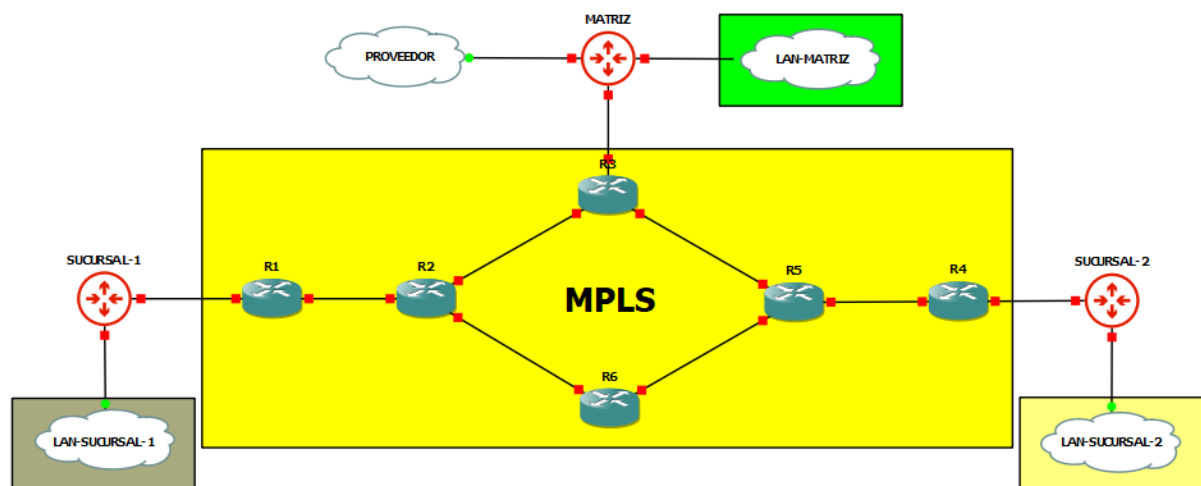
Fuente: GNS3(2.2.37)

Adicionalmente, se encuentra una red MPLS que constituye la infraestructura de red convencional de una empresa, la cual se utiliza para interconectar la "Matriz" con las sucursales 1 y 2. A continuación, se proporciona una explicación detallada sobre el funcionamiento de la red MPLS, y en la figura 17 se presenta un esquema que muestra su topología.

Figura 17*Topología de la red MPLS*

Fuente: GNS3(2.2.37)

Por último, en la figura 18 se muestra la topología integral de la red, que incluye todas las áreas mencionadas previamente. A continuación, se establece la configuración de direcciones IP y se proporciona una explicación exhaustiva sobre el funcionamiento de cada una de las redes de área local y área extendida, junto con sus respectivos dispositivos internos.

Figura 18*Topología completa de ISP tradicional*

Fuente: GNS3(2.2.37)

3.1.2. Direccionamiento IP

En esta sección, se proporciona información detallada sobre el direccionamiento IP, el cual implica asignar una dirección IP a cada equipo de la empresa para que puedan utilizar los

servicios ofrecidos por la red. En este caso particular, al tratarse de una emulación, se han utilizado direcciones IP privadas para toda la red. En un entorno real, se utilizarían direcciones IP públicas proporcionadas por el proveedor de servicios de Internet (ISP) para acceder a Internet.

La Tabla 5 presenta los intervalos de direcciones IP privadas para las clases A, B y C, con el objetivo de facilitar la comprensión del direccionamiento. En líneas generales, la red consta de una sede central y dos sucursales. Para distinguir entre las redes de área local, la red de área extendida y la red MPLS, se utilizan direcciones de clase A, clase B y clase C, donde:

- Para las conexiones de los routers de administración con el proveedor se utilizará un direccionamiento ip clase A.
- Para las conexiones entre la matriz y las sucursales por medio de la nube MPLS se utilizará un direccionamiento clase B.
- Finalmente, las redes LAN con un direccionamiento clase C.

Tabla 5

Clase de direcciones IP privadas

| RANGO DE DIRECCIONES IP PRIVADAS | | |
|---|--------------|-----------------|
| Tipo | Desde | Hasta |
| Clase A | 10.0.0.0 | 10.255.255.255 |
| Clase B | 172.16.0.0 | 172.31.255.255 |
| Clase C | 192.168.0.0 | 192.168.255.255 |

Fuente: Autoría

Considerando que el enfoque no se centra en el direccionamiento IP, no se ha aplicado la técnica de VLSM (Variable Length Subnet Masking), sino que se ha utilizado una distribución simple de direcciones IP como se detalló anteriormente. A partir de una dirección IP privada de cada clase, la Tabla 6 muestra la organización de las direcciones IP de toda la red.

Tabla 6

Distribución de direcciones IP completa para la emulación del ISP tradicional

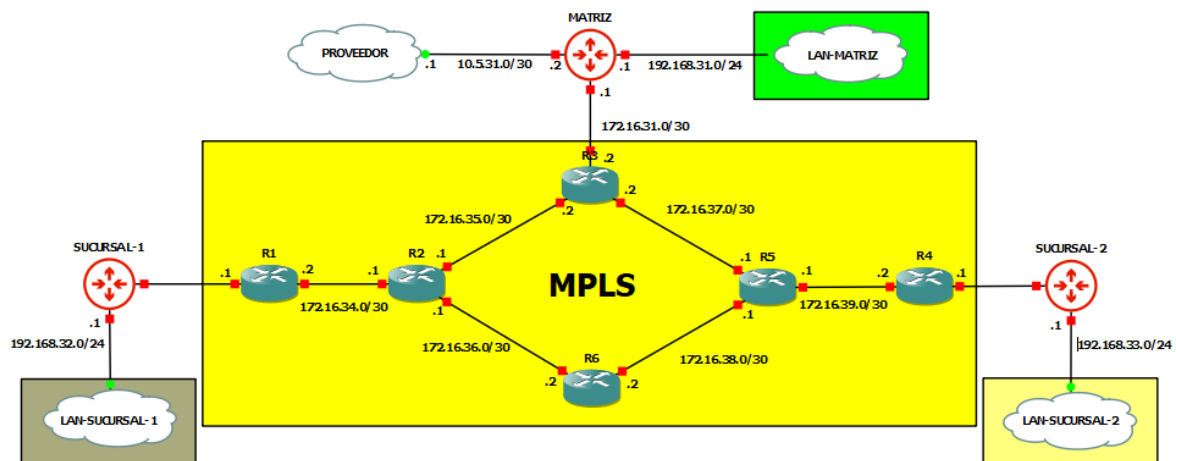
| DESCRIPCIÓN | RED | IP INICIAL | IP FINAL | BROADCAST |
|---------------|-----------------|--------------|----------------|----------------|
| PR-MATRIZ | 10.5.31.0/30 | 10.5.31.1 | 10.5.31.2 | 10.5.31.3 |
| PR-SUCURSAL1 | 10.5.32.0/30 | 10.5.32.1 | 10.5.32.2 | 10.5.32.3 |
| PR-SUCURSAL2 | 10.5.33.0/30 | 10.5.33.1 | 10.5.33.2 | 10.5.33.3 |
| MAT-R3 | 172.16.31.0/30 | 172.16.31.1 | 172.16.31.2 | 172.16.31.3 |
| SUC1-R1 | 172.16.32.0/30 | 172.16.32.1 | 172.16.32.2 | 172.16.32.3 |
| SUC2-R4 | 172.16.33.0/30 | 172.16.33.1 | 172.16.33.2 | 172.16.33.3 |
| R1-R2 | 172.16.34.0/30 | 172.16.34.1 | 172.16.34.2 | 172.16.34.3 |
| R2-R3 | 172.16.35.0/30 | 172.16.35.1 | 172.16.35.2 | 172.16.35.3 |
| R2-R6 | 172.16.36.0/30 | 172.16.36.1 | 172.16.36.2 | 172.16.36.3 |
| R3-R5 | 172.16.37.0/30 | 172.16.37.1 | 172.16.37.2 | 172.16.37.3 |
| R6-R5 | 172.16.38.0/30 | 172.16.38.1 | 172.16.38.2 | 172.16.38.3 |
| R5-R4 | 172.16.39.0/30 | 172.16.39.1 | 172.16.39.2 | 172.16.39.3 |
| LAN MATRIZ | 192.168.31.0/24 | 192.168.31.1 | 192.168.31.253 | 192.168.31.254 |
| LAN SUCURSAL1 | 192.168.32.0/24 | 192.168.32.1 | 192.168.32.253 | 192.168.32.254 |
| LAN SUCURSAL2 | 192.168.33.0/24 | 192.168.33.1 | 192.168.33.253 | 192.168.33.254 |

Fuente: Autoría

En la Figura 19 se muestra la topología de red junto con el direccionamiento, lo que permite una mejor comprensión de la distribución de las direcciones IP.

Figura 19

Direccionamiento IP y topología de red tradicional



Fuente: GNS3(2.2.37)

3.1.3. Funcionamiento de redes LAN

En esta sección, se detalla la función de cada red de área local (LAN), es decir, de la Matriz, Sucursal-1 y Sucursal-2, así como la descripción de cada uno de los dispositivos que forman parte de ellas.

3.1.3.1. LAN Matriz

La LAN ubicada en la matriz desempeña un papel fundamental como sede central o principal, donde se concentran las funciones más importantes y desde donde se emiten las órdenes. También se considera el punto central de administración para las sedes secundarias.

La red de área local de la matriz se divide en 3 áreas distintas: un área de servidores que proporciona recursos necesarios para que las demás LAN accedan a ellos, un área de atención al cliente donde los empleados realizan actualizaciones o tareas de trabajo sencillas y un área de teletrabajo destinada a realizar videoconferencias.

Para cumplir con los requisitos de memoria RAM y capacidad de procesamiento, se ha configurado un servidor DNS y un servidor TFTP en el área de servidores, 2 computadoras en el área de atención al cliente, 2 computadoras en el área de teletrabajo. En la Figura 14 de la sección de diseño de topología de red WAN tradicional se puede observar cada uno de los dispositivos presentes en la LAN de la matriz.

La capacidad para agregar más dispositivos en cada área está limitada por los recursos de hardware disponibles en la PC utilizada para la emulación. En este caso, se está utilizando el 100% de los recursos disponibles, ya que el dispositivo de control y administración requiere una cantidad considerable de memoria RAM (4096 Megabytes) y capacidad de procesamiento.

3.1.3.2. LAN Sucursal-1

La LAN de la sucursal 1 cumple el rol de un Centro de Datos, que está compuesto por servidores y computadoras en red para el procesamiento, almacenamiento y distribución de grandes volúmenes de datos. Por lo general, las empresas dependen de los servicios y datos

contenidos en un Centro de Datos, lo que lo convierte en un elemento crucial de la red, ya que proporciona recursos necesarios a los cuales las demás redes deben acceder.

La LAN de la sucursal 1 se divide en 3 áreas, que son similares a las de la matriz, donde se han instalado dispositivos que incluyen un servidor de Correo y un servidor Syslog en el área de servidores, 3 computadoras en el área de atención al cliente y 1 computadora en el área de teletrabajo. En la Figura 15 de la sección de diseño de topología de la red WAN tradicional se pueden observar cada uno de los dispositivos presentes en la LAN de la sucursal 1.

3.1.3.3. LAN Sucursal-2

Por último, la LAN de la sucursal 2 funciona como una sucursal normal, siendo una oficina más pequeña y remota con un conjunto reducido de funciones y sin ningún recurso o servidor al cual las otras redes necesiten acceder. En consecuencia, la LAN de la sucursal 2 se divide únicamente en dos áreas: el área de atención al cliente y el área de teletrabajo. Por lo tanto, no se cuenta con servidores ni dispositivos de administración, ya que su función se limita a ser una sucursal. En la Figura 16 de la sección de diseño de topología de la red WAN tradicional se pueden observar todos los dispositivos presentes en la sucursal 2.

3.1.4. Funcionamiento de redes WAN

En esta parte, se proporciona una explicación exhaustiva sobre el funcionamiento de la red MPLS, incluyendo su protocolo de enrutamiento, ingeniería de tráfico, túneles y otros elementos relevantes. También se describe en detalle el funcionamiento de la WAN utilizada para acceder a Internet.

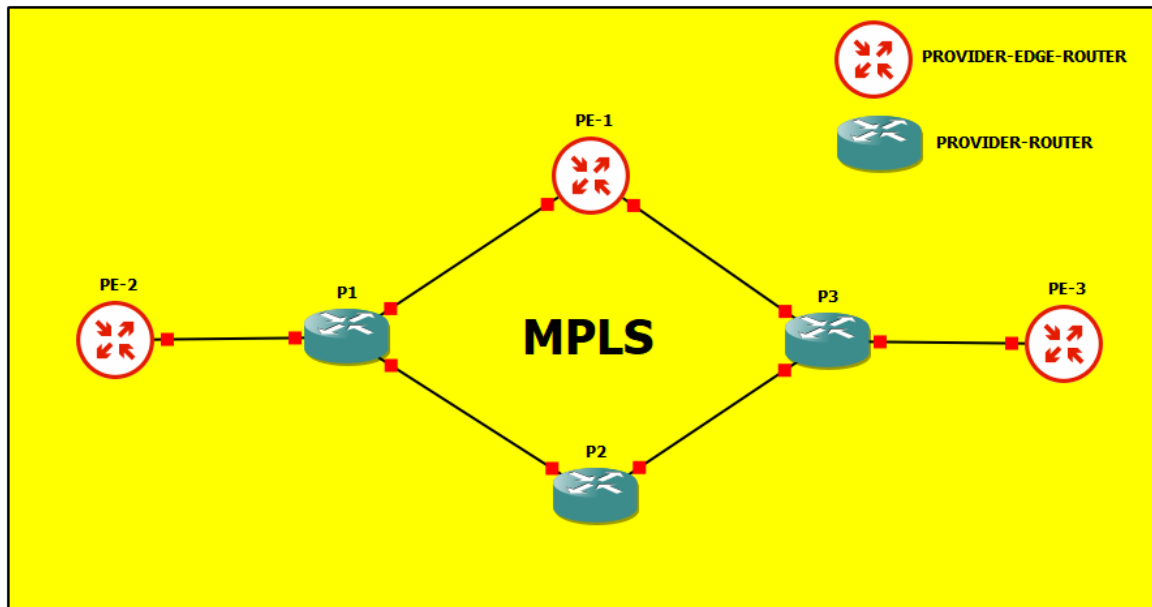
3.1.4.1. MPLS

Se ha implementado la infraestructura de MPLS en la red, ya que muchas empresas utilizan esta tecnología para la comunicación con sus sucursales remotas. La función principal de MPLS es conectar la matriz con la sucursal 1 y 2. Esta infraestructura consta de 6 enrutadores,

de los cuales 3 actúan como enrutadores de borde del proveedor (Provider Edge Router) y 3 actúan como enrutador proveedor (Provider Router), como se muestra en la Figura 20.

Figura 20

Red MPLS y sus componentes



Fuente: GNS3(2.2.37)

Además de la explicación del direccionamiento IP en la sección 3.1.2, se ha configurado un conjunto de direcciones IP para las interfaces de Loopback con el propósito de facilitar ciertos aspectos de configuración relacionados con el protocolo de enrutamiento. En la Tabla 7 se presentan las interfaces de Loopback utilizadas en cada enrutador.

Tabla 7

Interfaces de Loopback

| INTERFACES | DIRECCIÓN IP |
|-------------------|---------------------|
| Loopback 10 | 1.1.1.1/32 |
| Loopback 20 | 2.2.2.2/32 |
| Loopback 30 | 3.3.3.3/32 |
| Loopback 40 | 4.4.4.4/32 |
| Loopback 50 | 5.5.5.5/32 |
| Loopback 60 | 6.6.6.6/32 |

Fuente: Autoría

El protocolo de enrutamiento empleado es Open Shortest Path First (OSPF), el cual es un protocolo de estado de enlace. Este protocolo se caracteriza por su rápida convergencia y proporciona a todos los dispositivos una visión completa de toda la red. Solo realiza actualizaciones cuando detecta cambios en la red y utiliza métricas superiores en comparación con los protocolos vector-distancia. Además, OSPF no tiene restricciones en cuanto al número de saltos y su base de datos se utiliza para construir un árbol con los enlaces de menor costo. En caso de que existan múltiples rutas con el mismo costo, la política consiste en distribuir el tráfico de forma equitativa.

Este protocolo se implementa en los enrutadores de la red MPLS y en las interfaces de los dispositivos administradores de cada LAN que conectan la matriz con la sucursal 1 y 2. En la red MPLS, los dispositivos de administración funcionan como enrutadores de borde del cliente (Customer Edge Routers), lo que significa que la conmutación multiprotocolo de etiquetas solo está habilitada en las interfaces que se dirigen a los enrutadores de borde del proveedor (PE o P routers), y no en las interfaces que se dirigen hacia la LAN.

3.1.4.2. WAN de acceso a internet

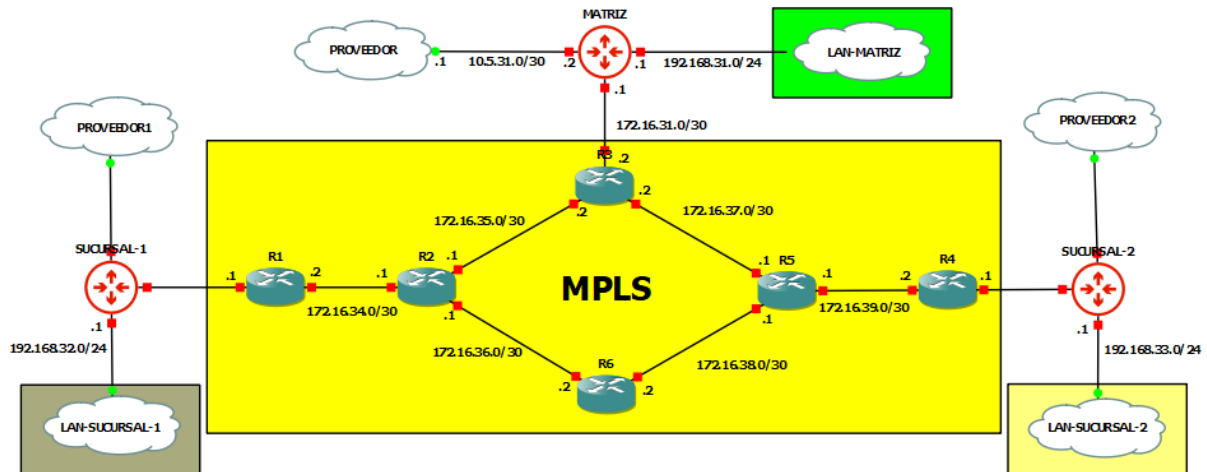
El modo en que operan las redes WAN se basa en la conexión de numerosos ordenadores entre sí a través de un medio de transmisión, como cables o fibra óptica en su mayoría, con el objetivo de permitir la comunicación entre diferentes centrales ubicadas a distancias considerables, a menudo de cientos de kilómetros entre sí. De esta forma, podemos comprender que la WAN con acceso a Internet simplemente consiste en un enlace público de Internet de bajo costo que se encuentra conectado desde los routers de administración ubicados en la matriz, Sucursal-1 y 2.

Por último, la Figura 21 muestra todas las conexiones a Internet desde cada uno de los sitios. Es importante destacar que, en la emulación, no se especifica el tipo de transporte IP, como fibra, cable, DSL u otros, ya que los clientes tienen la flexibilidad de admitir varios tipos.

Por lo tanto, la elección del medio de transporte depende de la preferencia de la empresa. En la emulación, se representan como líneas de banda ancha en general.

Figura 21

Enlace de acceso a internet de la red



Fuente: GNS3(2.2.37)

3.1.5. Tabla de requerimientos

Los objetivos de las redes se enfocan en dos aspectos principales: compartir recursos, que es su objetivo básico, y proporcionar un medio de comunicación eficaz entre personas que se encuentran distanciadas entre sí. 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. Asimismo, se busca garantizar una alta confiabilidad al contar con fuentes alternativas de suministro. Por esto, en la tabla 8, se ha resumido los requerimientos mínimos de ancho de banda necesarios para diferentes aplicaciones o servicios en la red WAN.

Tabla 8*Requerimientos ancho de banda*

| ITEM | APLICACIÓN O SERVICIOS | ANCHO DE BANDA (kbps) | OBSERVACIONES |
|-------------|--|------------------------------|---|
| 1 | Vídeo conferencia y herramientas colaborativas | 768 | De acuerdo con Espinosa & Alavarez (2011), 768 kbps es el mínimo de ancho de banda para transmisión de vídeo en High Definition |
| 2 | Voz sobre internet | 42 | Según, centralip (2023). El ancho de banda mínimo para establecer una comunicación viable suele estar entre los 42 kbps |
| 3 | Sistemas de información y otras aplicaciones (Web, sistemas financieros, control de personal, mail, ftp) | 15000 | Según CenturyLink (2023), para navegación web general se requiere 1.5 Mbps |
| 4 | Internet | 768 | Según Espinoza & Álvarez (2011) para uso de internet el ancho de banda mínimo es de 768 kbps |

Fuente: Autoría

Además del ancho de banda, en la tabla 9, de acuerdo con Espinosa & Alavarez (2011). Se expone los requerimientos de pérdida de paquetes, latencia, jitter y disponibilidad, fundamentales en una red de área amplia (WAN) 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 una red WAN, siendo esencial para el funcionamiento exitoso de las empresas en el entorno actual altamente interconectado.

Tabla 9

Requerimientos de pérdida de paquetes, latencia, jitter y disponibilidad

| ITEM | APLICACIÓN O SERVICIOS | LATENCIA | JITTER | PERDIDA DE PAQUETES | DISPONIBILIDAD |
|-------------|--|------------------|-----------------|------------------------------------|-----------------------|
| 1 | Video conferencia y herramientas colaborativas | Baja < 150 ms | Bajo < 30 ms | Baja < 1% | Alta |
| 2 | Voz sobre internet | Baja < 150 ms | Bajo < 30 ms | Baja < 1% | Alta |
| 3 | Sistemas de información y otras aplicaciones (Web, sistemas financieros, control de personal, mail, ftp) | No critico | No critico | No critico | Media |

Fuente: Adaptado de (Espinosa & Alavarez, 2011).

3.1.6. Criterios de configuración de la red tradicional

Este apartado tiene como objetivo establecer la importancia y la necesidad de implementar una red IP MPLS para que un proveedor de telecomunicaciones pueda ofrecer servicios IP de extremo a extremo con fiabilidad y seguridad.

Para poder brindar estos servicios, es esencial que el diseño de la red sea efectivo y se ajuste a los requisitos del operador, lo cual le permitirá ofrecer una amplia gama de servicios a diversos clientes.

La funcionalidad de una red se logra cuando es capaz de expandirse en términos de nodos sin necesidad de modificar su diseño. En este caso, se emplea un esquema que permite un crecimiento flexible en cuanto al número de nodos, brindando total libertad en ese aspecto.

En la red, se establecen 3 o 4 categorías de equipos en función de su rol y función dentro del sistema. Podemos resumir algunas de sus características funcionales de la siguiente manera:

- **Equipos de núcleo o CORE:** Estos dispositivos están equipados con interfaces de alta capacidad que posibilitan el intercambio de tráfico a velocidades superiores a los 100Gbps. Mediante la agrupación de múltiples interfaces, se puede alcanzar una capacidad cercana a Tbit/s (1000Gbps).
- **Equipos de acceso:** Estos dispositivos se encuentran en una posición intermedia entre el núcleo (CORE) y los equipos de cliente (EDC). Están equipados con interfaces de velocidad media, una alta densidad de puertos y tarjetas con múltiples enlaces y capacidad. Las interfaces de conexión habituales incluyen velocidades de 10Gbps, 1Gbps, 100Mbps, E1, T1, E3, T3, RDSI, entre otros.
- **Equipos de cliente:** Estos dispositivos son empleados para establecer la conexión entre los clientes y la red del proveedor de servicios. Por lo general, estos equipos cuentan con tarjetas WAN (como Ethernet, FRAME-RELAY,

ATM, RDSI o conexiones seriales) para conectarse con el proveedor de servicios, así como una o varias interfaces LAN de mayor velocidad para proporcionar conectividad a nivel local dentro de las instalaciones del cliente.

El objetivo de la red es posibilitar la interconexión de un gran número de clientes, incluyendo sus sedes remotas, asegurando la provisión de servicios de extremo a extremo de manera confiable.

3.2. Selección de hardware y software

En esta sección, se presenta el enfoque utilizado para recopilar las necesidades de los usuarios de la red. Para esto, se empleó herramientas de investigación. Posteriormente, se procede a analizar los requisitos identificados.

3.2.1. Análisis de Benchmark

Para determinar la opción de hardware más adecuada, es necesario considerar los requisitos previamente analizados en el apartado 3.1.6 (criterios de configuración de la red tradicional). En lo que respecta al hardware, se optará por seleccionar ISOs de routers reales para que la emulación sea lo más cercano a la realidad posible, a partir del cual se buscará una imagen ISO de un proveedor que satisfaga las necesidades del usuario. Estas imágenes desempeñarán la función de simular y procesar el funcionamiento de la red en gestión, respectivamente.

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 la emulación 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 emular en GNS3 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 10 se toma en cuenta cinco requerimientos principales, para la selección de las imágenes ISO a usarse. Posteriormente, se evalúa cada una de estas, considerando los requerimientos expuestos en el apartado 3.1. Posteriormente se indica cuál fue la imagen ISO elegida y se proporciona los argumentos que respaldan esta decisión.

Tabla 10

Selección de hardware

| HARDWARE ROUTER (ISO) | REQUERIMIENTOS | | | | | VALORACIÓN TOTAL |
|-----------------------------|----------------|----------------------|---------------------|-------|------------------|---------------------|
| | 1 | 2 | 3 | 4 | 5 | |
| | SOPORTA MPLS | ADMINISTRACIÓN (GUI) | COMPATIBLE CON GNS3 | COSTO | FACILIDAD DE USO | |
| CISCO | 1 | 1 | 1 | 0 | 0 | 3 |
| MIKRO TIK | 1 | 1 | 1 | 1 | 1 | 5 |
| JUNIPER | 1 | 1 | 1 | 0 | 0 | 3 |

1 Cumple

0 No cumple

Fuente: Autoría

Elección:

La elección se dirige hacia la ISO de Mikro Tik (RouterOS) debido a que cumple con los requisitos principales para la emulación, obteniendo la puntuación más alta en comparación con las otras opciones disponibles. Una de las características destacadas de esta, es su facilidad de uso por medio de su intuitiva interfaz gráfica de usuario, lo que hace más sencillo la configuración de MPLS en un entorno simulado, además, ofrece una amplia gama de funciones que son relevantes para su implementación, incluyendo la capacidad de configurar protocolos de enrutamiento como OSPF. Finalmente, Mikro Tik 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 MPLS en GNS3.

3.2.2. IEEE 29148

Se realiza la elección del software con la ayuda del estándar ISO/IEC/IEEE 29148-2011, ya que incluye cláusulas que abarcan los procedimientos y productos vinculados a la ingeniería de requisitos para sistemas, productos de software y servicios durante todo el ciclo de vida. El contenido de esta norma se puede integrar con los procesos de ciclo de vida existentes relacionados con los requisitos establecidos por ISO/IEC 12207 o ISO/IEC 15288, o puede utilizarse de forma independiente. Se realizó una búsqueda de software compatible y disponible en el mercado basándose en el hardware, considerando opciones de código abierto.

En la tabla 11 presentada a continuación, se muestra las diferentes opciones de software disponibles en el mercado en la primera columna. En la siguiente columna se detallan algunos requerimientos que deben ser analizados para la selección. Por último, la columna de valoración total muestra el puntaje obtenido por cada opción de software. Para evaluar, se ha establecido que se otorgue un valor de 1 si cumple el requisito y un valor de 0 si no lo cumple. En la parte

inferior de la tabla 11 se incluye una sección donde se explica la elección realizada y la justificación correspondiente.

Con relación al software de emulación de red, se han identificado tres alternativas de las más populares para simular redes que son ampliamente utilizados en la industria y en entornos educativos para propósitos de aprendizaje, prueba y desarrollo. A continuación, se realiza un análisis detallado de estas opciones en la tabla 11.

Tabla 11

Selección de software de emulación de red

| SOFTWARE DE EMULACIÓN DE RED | REQUERIMIENTOS | | | | VALORACIÓN TOTAL |
|---------------------------------------|---------------------------|--|---|--|------------------|
| | 1 ES DE CODIGO ABIERTO | 2 INTERFAZ GRÁFICA DE USUARIO (GUI) | 3 COMPATIBILIDAD CON DISPOSITIVOS Y PROTOCOLOS | 4 SOPORTE PARA VIRTUALIZACIÓN Y SDN | |
| GNS3 | 1 | 1 | 1 | 1 | 4 |
| CISCO PACKET TRACER | 0 | 1 | 0 | 0 | 1 |
| MININET | 1 | 1 | 0 | 1 | 2 |
| 1 Cumple 0 No cumple | | | | | |

Fuente: Autoría

Elección:

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. Por otro lado, Mininet se centra en entornos SDN basados en OpenFlow, el software GNS3 permite la integración de imágenes de sistemas operativos reales de diversos proveedores, incluyendo Cisco, Mikro Tik, entre otros. Esto proporciona una flexibilidad necesaria para replicar entornos de red que involucren dispositivos de diferentes fabricantes, así como para experimentar con configuraciones y escenarios más avanzados. 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 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 tradicional.

3.2.3. Etapas de configuración de la topología

En este apartado se detallan los pasos necesarios para diseñar una infraestructura destinada a configurar una topología de red, con el fin de levantar el diseño de forma organizada. Aunque no es obligatorio llevar a cabo estas tareas en un orden particular durante la fase de planificación.

1. **Enlistar el software y hardware requerido:** De acuerdo con la topología planteada y los requerimientos de hardware y software expuestos anteriormente, enlistar todos los componentes existentes.
2. **Instalación de hardware y software:** Una vez obtenida la lista de hardware y software, se procede a la instalación de todos los programas necesarios para el levantamiento de la infraestructura de red.
3. **Integración de hardware y software:** Una vez instalados los programas, se procede a integrar entre ellos, de tal forma que trabajen en conjunto.
4. **Levantamiento de topología:** Se procede a el desarrollo de la topología planteada con todos sus componentes.

5. **Configurar interfaces ip del sistema:** Se asigna las direcciones ip a las interfaces, de acuerdo con el direccionamiento establecido en los requerimientos de la red.
6. **Enrutar la topología:** Se configura el enrutamiento con los protocolos mencionados en los criterios de configuración de la red.
7. **Convergencia de la red:** Se realiza pruebas de conectividad para comprobar que exista comunicación entre toda la red.
8. **Pruebas de funcionamiento:** Se procede a realizar pruebas de acuerdo con los parámetros de rendimiento y gestión mencionados en los criterios de configuración.
9. **Análisis de resultados:** Se documenta los resultados obtenidos para sacar conclusiones del funcionamiento de la red WAN tradicional.

3.3. Emulación de la red

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 12, las pruebas y resultados obtenidos pueden variar ligeramente de acuerdo con las prestaciones del computador.

Tabla 12

Características del computador utilizado en la simulación.

| Descripción | Características |
|--------------------------|---|
| Sistema operativo | Windows 10 (64 bits) |
| Procesador | CPU Intel Core i7 / 4 núcleos lógicos |
| Memoria | 8GB RAM |
| Almacenamiento | Unidad de disco duro (HDD) con 200 GB de espacio disponible |

Fuente: Autoría

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 respectivo.

3.3.1. *Direccionamiento Ip*

Los enrutadores de administración y de la red MPLS comparten el mismo proceso de configuración de direccionamiento, con la única diferencia en las interfaces y direcciones IP. Por lo tanto, se proporciona la explicación de la configuración de un enrutador de frontera del proveedor (CE), el cual esta denominado como “MATRIZ”.

Tanto en el enrutador CE como en el enrutador PE y P, se comienza configurando las direcciones IP de las interfaces ethernet para después continuar con la configuración del protocolo de enrutamiento OSPF mencionado. La figura 22 muestra la configuración del direccionamiento de las interfaces del router “MATRIZ”. La configuración del direccionamiento del resto de routers se encuentra en el anexo A (Configuración de direccionamiento ip de routers).

Figura 22

Configuración direccionamiento router “MATRIZ”

```
[admin@mikroTik] > ip address add address=172.16.31.1/30 interface=ether1
[admin@mikroTik] > ip address add address=10.5.31.2/30 interface=ether2
[admin@mikroTik] > ip address add address=192.168.31.1/24 interface=ether3
[admin@mikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS          NETWORK          INTERFACE
0  172.16.31.1/30    172.16.31.0     ether1
1  10.5.31.2/30     10.5.31.0      ether2
2  192.168.31.1/24  192.168.31.0   ether3
```

Fuente: Solar-Putty (4.0.0.47)

3.3.2. *Enrutamiento*

Seguidamente, se procede a configurar OSPF, que tiene la responsabilidad de interconectar la sede principal con sus sucursales mediante la red MPLS. Los parámetros de OSPF en la interfaz gráfica de usuario (GUI) de Mikrotik (Winbox) son idénticos a los que se

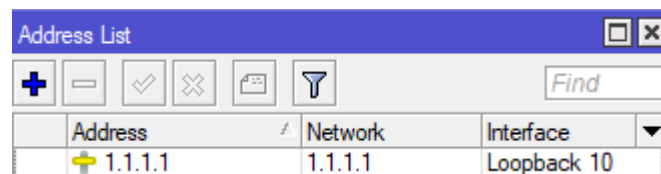
configuran a través de la interfaz de línea de comandos (CLI), como el área, las redes directamente conectadas y las interfaces.

El proceso de configuración de OSPF y MPLS se va a realizar en todos los routers que participan de la nube MPLS por lo tanto en este apartado se muestra la configuración paso a paso del router “MATRIZ” y la configuración del resto de routers se encuentra en el anexo B (Configuración OSPF y MPLS).

Inicialmente se configura un direccionamiento a una interfaz loopback sin asignación a puerto físico sino a un puente bridge, esto se realiza de la siguiente manera: primero se crea un puente bridge en la sección de Bridge y se coloca el nombre de Loopback, como se muestra en la figura 23.

Figura 23

Configuración direccionamiento loopback router “R3”



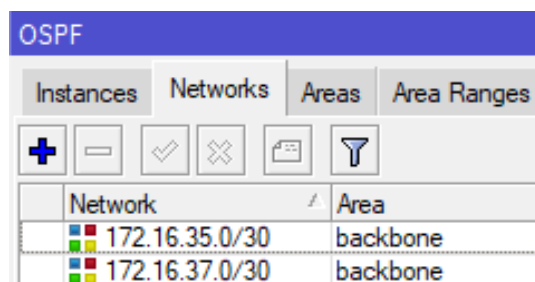
| Address | Network | Interface |
|---------|---------|-------------|
| 1.1.1.1 | 1.1.1.1 | Loopback 10 |

Fuente: WinBox (3.38)

Para establecer la configuración de enrutamiento OSPF se debe activar dicha opción, esto se realiza en la sección de **Routing/OSPF/Networks** donde se colocan las redes directamente conectadas al router, la figura 24 muestra las redes 172.16.35.0/30 y 172.16.37.0/30 ya que son las redes que participan en OSPF del R3.

Figura 24

Configuración OSPF del router R3



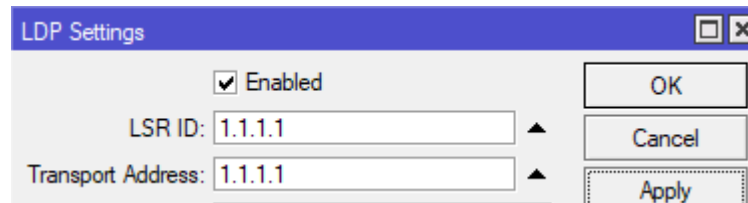
| Network | Area |
|----------------|----------|
| 172.16.35.0/30 | backbone |
| 172.16.37.0/30 | backbone |

Fuente: WinBox (3.38)

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 1.1.1.1 en **LSR ID** y **Transport Address**. Tal como se muestra en la figura 25.

Figura 25

Configuración de protocolo MPLS



Fuente: WinBox (3.38)

A continuación, en la figura 26, 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 26

Asignación de interfaces que conforman MPLS

| MPLS | | | | | | |
|---|---|----------------|-----------|-------------------|------------------|------------------|
| LDP Interface | | LDP Neighbor | | Accept Filter | Advertise Filter | Forwarding Table |
| + - ✓ ✗ 📄 🗑️ MPLS Settings LDP Settings | | | | | | |
| Interface | ? | Hello Interval | Hold Time | Transport Address | Accept Dy... | |
| Loopback 10 | | 00:00:05 | 00:00:15 | | yes | |
| ether1 | | 00:00:05 | 00:00:15 | | yes | |
| ether2 | | 00:00:05 | 00:00:15 | | yes | |

Fuente: WinBox (3.38)

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 27.

Figura 27

Routers y rutas aprendidas del R3 mediante MPLS

The screenshot shows the MPLS configuration window in WinBox. It has several tabs: LDP Interface, LDP Neighbor, Accept Filter, Advertise Filter, Forwarding Table, MPLS Interface, Local Bindings, and Rem. Below the tabs are several icons: a plus sign, a minus sign, a checkmark, a cross, a speech bubble, and a funnel. Below the icons is a table with the following data:

| | Transport | Send ... | Peer | Local Transport | Addresses |
|----|-----------|----------|-----------|-----------------|--|
| DO | 2.2.2.2 | no | 2.2.2.2:0 | 1.1.1.1 | 2.2.2.2, 172.16.34.2, 172.16.35.1, 172.16.36.1 |
| DO | 5.5.5.5 | no | 5.5.5.5:0 | 1.1.1.1 | 5.5.5.5, 172.16.37.1, 172.16.38.2, 172.16.39.1 |

Fuente: WinBox (3.38)

3.4. Gestión de la red

Esta actividad es llevada a cabo por los gestores de redes con el propósito de evaluar el rendimiento de la red en términos de enlaces, dispositivos y conexiones físicas. Su objetivo principal es asegurar que se cumplan los acuerdos de niveles de servicio contratados.

Las pruebas activas implican la inserción de tráfico en la red o el envío de paquetes a servidores para verificar aspectos como los tiempos de respuesta, el rendimiento de transferencia de datos, la variabilidad en la llegada de paquetes y otros parámetros relevantes.

Después de llevar a cabo estas pruebas, es necesario analizar y comparar los resultados con las métricas y umbrales establecidos para determinar el desempeño de la infraestructura y decidir si se requiere alguna acción correctiva o preventiva de mantenimiento.

3.4.1. FCAPS

Con el fin de garantizar la entrega efectiva de servicios, es indispensable disponer de una sólida base de información que nos permita identificar todos los posibles escenarios que podrían afectar el funcionamiento normal de la infraestructura de red. Para cumplir con este requisito, es necesario llevar a cabo un monitoreo exhaustivo, familiarizarnos con todas las características relevantes y, lo más importante, contar con un marco de referencia que nos permita obtener la información necesaria.

Podemos apoyarnos en estándares ya comprobados para la gestión, como es el caso de FCAPS (Fault, Configuration, Accounting, Performance, Security). FCAPS es una norma

ampliamente utilizada en el campo de las telecomunicaciones y nos brinda una base sólida para adaptar un formato similar aplicado a las redes de datos. Los aspectos principales que abarca este estándar se describen en la tabla 13. (Arias, 2011)

Tabla 13

FCAPS

| F | C | A | P | S |
|------------------|----------------------|---|-------------------------------|---|
| Alarm generation | Remote configuration | Audits | Problem reporting | Security related information distribution |
| Diagnost test | Copy configuration | Fraud reporting | Performance data analysis | Data privacy |
| Fault correction | Auto-discovery | Support for different modes of accounting | Performance data collection | Access logs |
| Error handling | Backup and restore | Combine cost for multiple resources | Performance report generation | Security alarm / even reporting |

Fuente: Adaptado de (Arias, 2011)

3.4.2. Protocolos de gestión de red

Un conjunto de convenciones y reglas que definen el procedimiento de intercambio de datos y comandos, con el propósito de transmitir y recibir información entre los componentes de una red, se denomina protocolo de red o protocolo de comunicación. Estas normas establecen pautas para el contenido, formato y velocidad (emisor-receptor) de los datos, así como para la gestión de errores a lo largo de la red. Algunos de los protocolos más destacados y ampliamente utilizados en la gestión de redes incluyen: (CUAED, 2017)

- SNMP (Simple Network Management Protocol)
- CMIP (Common Management Information Protocol)
- CORBA (Common Object Request Broker Architecture)

3.4.2. Monitoreo de red WAN

Después de establecer los componentes de la red, la administración se debe realizar mediante herramientas gráficas y de notificación para solucionar los problemas identificados o anticipados, desempeñando un papel complementario en el buen funcionamiento de la red.

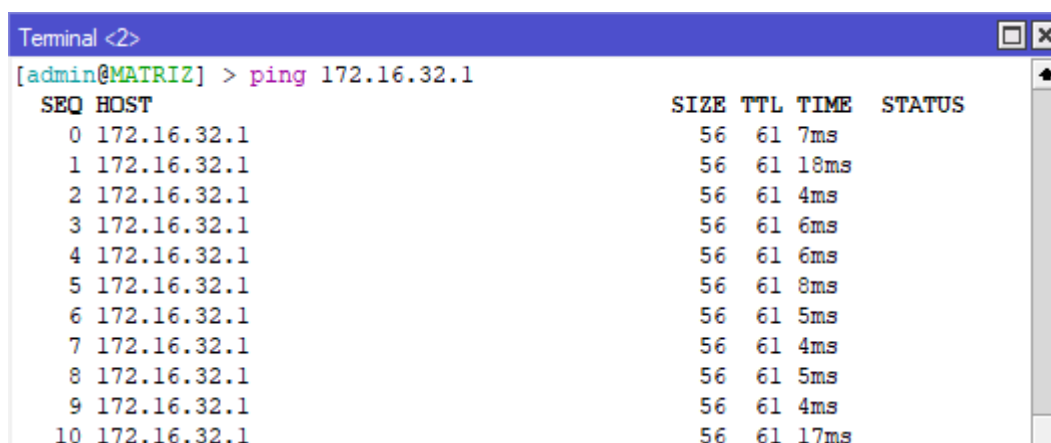
Dentro de las tareas de gestión, se ha tomado en cuenta la necesidad de hacer referencia a los requisitos del NOC (Centro de Operaciones de Red) junto con los parámetros mencionados en la sección 3.1.5 para realizar la supervisión de la red. Estos parámetros incluyen la conectividad, ancho de banda, pérdida de paquetes, latencia y jitter.

Conectividad

La primera herramienta utilizada pertenece al protocolo ICMP llamada ping. La función del ping es ofrecer el estatus de conexión entre 1 o varios hosts. En la figura 28 se puede observar la conexión entre el router de administración “MATRIZ” y el router “SUCURSAL-1”.

Figura 28

Prueba de conctividad entre el router “Matriz” y “LAN-SUCURSAL-1”



```

Terminal <2>
[admin@MATRIZ] > ping 172.16.32.1
  SEQ HOST                SIZE TTL  TIME  STATUS
   0 172.16.32.1           56  61   7ms
   1 172.16.32.1           56  61  18ms
   2 172.16.32.1           56  61   4ms
   3 172.16.32.1           56  61   6ms
   4 172.16.32.1           56  61   6ms
   5 172.16.32.1           56  61   8ms
   6 172.16.32.1           56  61   5ms
   7 172.16.32.1           56  61   4ms
   8 172.16.32.1           56  61   5ms
   9 172.16.32.1           56  61   4ms
  10 172.16.32.1           56  61  17ms
  
```

Fuente: WinBox (3.38)

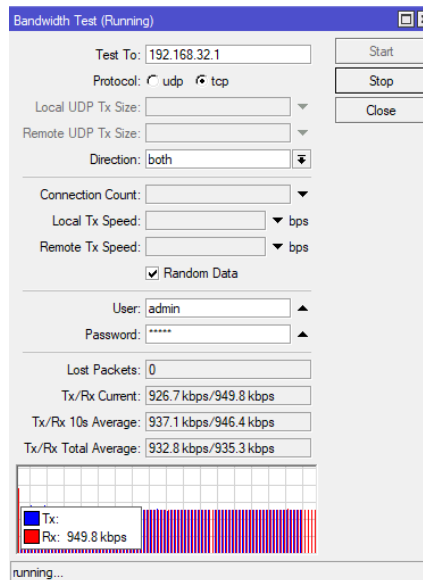
Ancho de banda

La congestión y el abuso del ancho de banda representan uno de los desafíos más críticos y complicados de diagnosticar si no se cuenta con las herramientas adecuadas. Es

fundamental realizar un análisis de tráfico para obtener una visión clara de la red. En esta ocasión en la figura 29, se presenta una gráfica útil que permite medir el ancho de banda de manera efectiva.

Figura 29

Prueba AB del router “Matriz” a “LAN-SUCURSAL-1”



Fuente: WinBox (3.38)

Perdida de paquetes

La pérdida de paquetes ocurre cuando uno o varios paquetes que viajan a través de una conexión de red no alcanzan su destino final. Esto implica que los paquetes se extravían, se retrasan o desaparecen en algún punto de los concentradores mientras atraviesan la red.

Cuando un paquete se retrasa, eventualmente será superado por otros y se reemplazará. Si no se envía ningún paquete para efectuar dicho reemplazo, el receptor recibirá partes de los datos o mensajes solicitados de manera inconsistente, incompleta, defectuosa o dañada. A lo largo del tiempo, todos los paquetes llegarán, pero lo harán con retraso, lo que afectará el rendimiento de la red.

Las causas de la pérdida de paquetes pueden ser errores o problemas durante la transmisión de datos en una red inalámbrica específica o debido a la congestión en la red. Estos problemas pueden estar relacionados con cables defectuosos, falta de ancho de banda o

hardware insuficiente, errores de software, amenazas de seguridad o dispositivos sobrecargados, entre otros. En la figura 30 se puede observar el resultado de pérdida de paquetes entre el router “MATRIZ” y “SUCURSAL-1”.

Figura 30

Prueba de pérdida de paquetes entre router “MATRIZ” y “SUCURSAL-1”

```

Terminal <2>
[admin@MATRIZ] > ping 172.16.32.1
  SEQ HOST                SIZE TTL  TIME   STATUS
  --- ---                --- ---  ---    ---
  0 172.16.32.1            56  61   7ms
  1 172.16.32.1            56  61  18ms
  2 172.16.32.1            56  61   4ms
  3 172.16.32.1            56  61   6ms
  4 172.16.32.1            56  61   6ms
  5 172.16.32.1            56  61   8ms
  6 172.16.32.1            56  61   5ms
  7 172.16.32.1            56  61   4ms
  8 172.16.32.1            56  61   5ms
  9 172.16.32.1            56  61   4ms
 10 172.16.32.1            56  61  17ms
 11 172.16.32.1            56  61  12ms
 12 172.16.32.1            56  61   4ms
 13 172.16.32.1            56  61  16ms
 14 172.16.32.1            56  61   7ms
 15 172.16.32.1            56  61   3ms
 16 172.16.32.1            56  61   3ms
 17 172.16.32.1            56  61  10ms
 18 172.16.32.1            56  61  10ms
 19 172.16.32.1            56  61   4ms
  sent=20 received=20 packet-loss=0% min-rtt=3ms avg-rtt=7ms
  max-rtt=18ms
  
```

Fuente: WinBox (3.38)

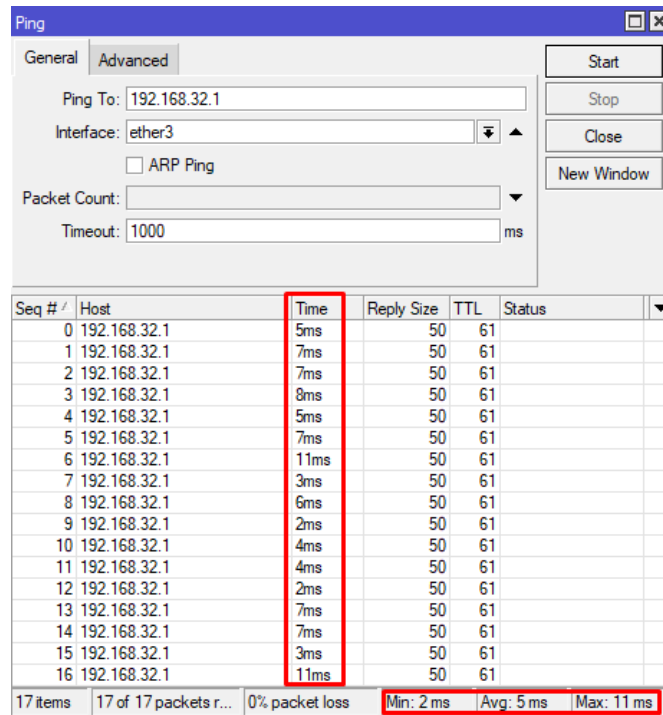
Latencia

La latencia de red se refiere al retraso en la comunicación de la red, es decir, el tiempo que tardan los datos en ser transferidos a través de ella. Las redes con un retraso mayor presentan una latencia alta, mientras que aquellas con tiempos de respuesta rápidos tienen una latencia baja. Las empresas buscan una latencia baja y una comunicación rápida en la red para lograr una mayor productividad y operaciones comerciales más eficientes. Algunas aplicaciones, como la dinámica de fluidos y otras de alto rendimiento computacional, requieren una latencia de red baja para satisfacer sus demandas de procesamiento. Por otro lado, una latencia alta provoca una degradación del rendimiento de las aplicaciones y aumenta la probabilidad de errores a niveles significativos. (Amazon, 2023)

En conclusión, la latencia mide el retraso en la llegada de un paquete al destino. Se mide en unidades de tiempo, como milisegundos. En la figura 31 se muestra la latencia entre el router “MATRIZ” y “SUCURSAL-1”.

Figura 31

Prueba de latencia entre router “MATRIZ” y “SUCURSAL-1”



| Seq # / | Host | Time | Reply Size | TTL | Status |
|---------|--------------|------|------------|-----|--------|
| 0 | 192.168.32.1 | 5ms | 50 | 61 | |
| 1 | 192.168.32.1 | 7ms | 50 | 61 | |
| 2 | 192.168.32.1 | 7ms | 50 | 61 | |
| 3 | 192.168.32.1 | 8ms | 50 | 61 | |
| 4 | 192.168.32.1 | 5ms | 50 | 61 | |
| 5 | 192.168.32.1 | 7ms | 50 | 61 | |
| 6 | 192.168.32.1 | 11ms | 50 | 61 | |
| 7 | 192.168.32.1 | 3ms | 50 | 61 | |
| 8 | 192.168.32.1 | 6ms | 50 | 61 | |
| 9 | 192.168.32.1 | 2ms | 50 | 61 | |
| 10 | 192.168.32.1 | 4ms | 50 | 61 | |
| 11 | 192.168.32.1 | 4ms | 50 | 61 | |
| 12 | 192.168.32.1 | 2ms | 50 | 61 | |
| 13 | 192.168.32.1 | 7ms | 50 | 61 | |
| 14 | 192.168.32.1 | 7ms | 50 | 61 | |
| 15 | 192.168.32.1 | 3ms | 50 | 61 | |
| 16 | 192.168.32.1 | 11ms | 50 | 61 | |

17 items | 17 of 17 packets r... | 0% packet loss | Min: 2 ms | Avg: 5 ms | Max: 11 ms

Fuente: WinBox (3.38)

Jitter

El jitter es una fluctuación o retraso en la entrega de paquetes de datos a través de una red, lo que implica una diferencia entre el momento de transmisión y recepción de una señal. El cambio o variación en el tiempo representa una interrupción en la secuencia normal de envío de paquetes de datos y se cuantifica en milisegundos (ms). (IDT, 2023)

En la figura 32 se muestra la desviación estándar de la latencia entre el router “MATRIZ” y “SUCURSAL-1”

Figura 32

Prueba de Jitter entre router "MATRIZ" y "SUCURSAL-1"

| Traceroute | | | | | | | | | | |
|----------------------------------|--------------|------|------|-------|------|-------------------------------------|-------|-----------|---------|-----------------|
| Basic | | | | | | Advanced | | | | |
| Traceroute To: 192.168.32.1 | | | | | | Count: <input type="text"/> | | | | |
| Packet Size: 56 | | | | | | Max Hops: <input type="text"/> | | | | |
| Timeout: 1000 ms | | | | | | Src. Address: <input type="text"/> | | | | |
| Protocol: icmp | | | | | | Interface: <input type="text"/> | | | | |
| Port: 33434 | | | | | | DSCP: <input type="text"/> | | | | |
| <input type="checkbox"/> Use DNS | | | | | | Routing Table: <input type="text"/> | | | | |
| Hop | Host | Loss | Sent | Last | Avg. | Best | Worst | Std. Dev. | History | Status |
| 1 | 172.16.31.2 | 0.0% | 157 | 1.2ms | 2.4 | 0.7 | 40.3 | 3.7 | | |
| 2 | 172.16.35.1 | 0.0% | 157 | 3.0ms | 6.8 | 2.4 | 36.1 | 4.4 | | <MPLS:L=23,E=0> |
| 3 | 172.16.34.1 | 0.0% | 157 | 2.7ms | 6.6 | 2.4 | 68.2 | 6.5 | | <MPLS:L=24,E=0> |
| 4 | 192.168.32.1 | 0.0% | 157 | 2.9ms | 6.7 | 2.2 | 218.1 | 17.2 | | |

Fuente: WinBox (3.38)

3.5. Plan de migración

Este apartado tiene la finalidad de guiar el proceso de transición de la red MPLS existente a una red SD-WAN altamente eficiente y flexible. Con el objetivo de mejorar la agilidad de nuestra infraestructura de red, reducir costos y aumentar la capacidad de adaptación a las demandas empresariales en constante evolución. Este plan detallado proporcionará una hoja de ruta clara y sistemática para asegurar una migración exitosa, minimizando las interrupciones en las operaciones comerciales y maximizando los beneficios que ofrece la tecnología SD-WAN. En el proceso, se espera garantizar la continuidad del negocio, optimizar el rendimiento de la red y mantener la seguridad de los datos mientras se adapta a un entorno de red moderno y más flexible.

3.5.1. Etapas del plan de migración

La migración de una red MPLS (Multiprotocol Label Switching) a SD-WAN (Software-Defined Wide Area Network) implica varios pasos para garantizar una transición exitosa. A continuación, se describen los pasos generales que se deben seguir:

1. Evaluación y planificación:

- Realizar un análisis exhaustivo de la red actual MPLS, incluyendo topología, ancho de banda, políticas de enrutamiento, aplicaciones críticas, etc.
- Identificar los objetivos y requisitos de la organización para la migración a SD-WAN.
- Considerar aspectos como la ubicación de los dispositivos SD-WAN, los proveedores de servicios y las soluciones disponibles en el mercado.

2. Diseño de la arquitectura SD-WAN:

- Definir la arquitectura SD-WAN que mejor se adapte a las necesidades. Se puede optar por una implementación en la nube, en las instalaciones (on-premise) o una combinación de ambas.
- Decidir qué tecnologías SD-WAN se utilizará, como VPN (Red Privada Virtual), enrutamiento basado en políticas, optimización del tráfico, seguridad, etc.
- Considerar la integración de diferentes tipos de conexiones de red, como líneas dedicadas, conexiones de banda ancha, LTE/5G, etc.

3. Selección del proveedor SD-WAN:

- Investigar y evaluar los diferentes proveedores de soluciones SD-WAN en el mercado.
- Comparar características, funcionalidades, costos, soporte técnico y reputación de los proveedores.
- Elegir el proveedor que mejor se ajuste a las necesidades y presupuesto.

4. Implementación:

- Configurar los dispositivos SD-WAN de acuerdo con el diseño de la arquitectura establecida.

- Establecer las políticas de enrutamiento, priorización de tráfico y seguridad necesarias.
- Conectar los enlaces de red a los dispositivos SD-WAN y realiza las pruebas necesarias para asegurar su correcto funcionamiento.
- Implementar la conectividad con las sucursales o sitios remotos, asegurándose de que estén correctamente integrados en la infraestructura SD-WAN.

5. Migración gradual:

- Definir una estrategia de migración gradual para minimizar el impacto en la operación de la red.
- Comenzar migrando sucursales o ubicaciones piloto a la nueva arquitectura SD-WAN.
- Realizar pruebas exhaustivas en las ubicaciones migradas para verificar el rendimiento, la calidad del servicio y la seguridad.

6. Monitoreo y ajuste:

- Implementar herramientas de monitoreo y gestión de red para supervisar el rendimiento de la nueva infraestructura SD-WAN.
- Analizar los datos recopilados y realizar ajustes en las políticas de enrutamiento, priorización de tráfico y seguridad según sea necesario.
- Realizar un seguimiento continuo de la red para garantizar su estabilidad y eficiencia.

3.5.2. Evaluación y planificación

La migración de la red MPLS a SD-WAN se ha convertido en una tendencia creciente debido a varias razones. En primer lugar, la red MPLS tradicional puede ser costosa de mantener, ya que requiere hardware especializado y contratos de servicio a largo plazo con

proveedores de servicios. En contraste, SD-WAN aprovecha la conectividad de Internet y la tecnología de virtualización para ofrecer una solución más flexible y rentable.

Además, SD-WAN brinda una mayor agilidad y capacidad de gestión. Permite la implementación y configuración rápida de nuevas sucursales o sitios remotos, lo que facilita la expansión y adaptación de la red a medida que las necesidades empresariales evolucionan. La administración centralizada y basada en políticas proporcionada por SD-WAN simplifica las tareas de monitoreo, seguridad y optimización del tráfico, lo que reduce la carga operativa y mejora la eficiencia.

Otra ventaja importante de la migración a SD-WAN es la capacidad de aprovechar múltiples conexiones de Internet, incluidas conexiones de banda ancha, fibra y LTE. Esto mejora la resiliencia de la red al proporcionar redundancia y la posibilidad de equilibrar la carga del tráfico en diferentes enlaces. Además, SD-WAN puede implementar técnicas avanzadas de enrutamiento y gestión del tráfico, como la selección dinámica de la ruta óptima en función de las condiciones de la red en tiempo real.

La adopción de SD-WAN también facilita la integración con servicios en la nube y aplicaciones SaaS (Software as a Service). Al aprovechar las capacidades de SD-WAN, las empresas pueden optimizar el rendimiento de estas aplicaciones y mejorar la experiencia del usuario final, al tiempo que garantizan la seguridad y la calidad del servicio.

De acuerdo con lo expuesto, migrar de una red MPLS a SD-WAN ofrece beneficios significativos en términos de costo, flexibilidad, agilidad y rendimiento. SD-WAN se ha convertido en una solución atractiva para las empresas que buscan mejorar la eficiencia de sus redes, aprovechar la conectividad de Internet y adaptarse rápidamente a las demandas cambiantes del negocio.

La migración de MPLS a SD-WAN puede tener varios objetivos y requisitos, dependiendo de las necesidades específicas de cada organización. A continuación, se presentan algunos objetivos comunes para la migración:

Objetivos:

Reducción de costos: Uno de los objetivos principales suele ser reducir los costos asociados con la infraestructura MPLS, incluyendo los contratos de servicio y los equipos especializados. SD-WAN ofrece una alternativa más rentable al aprovechar conexiones de Internet de menor costo y optimizar el uso de los recursos disponibles.

Mayor agilidad y flexibilidad: La capacidad de implementar y gestionar rápidamente nuevas sucursales o sitios remotos es otro objetivo clave. SD-WAN facilita la expansión y adaptación de la red, permitiendo una rápida provisión de servicios y cambios en la configuración de la red.

Mejora del rendimiento y la experiencia del usuario: SD-WAN ofrece técnicas avanzadas de enrutamiento y gestión del tráfico, lo que permite optimizar el rendimiento de las aplicaciones y mejorar la experiencia del usuario final. Esto puede lograrse mediante la selección dinámica de rutas óptimas, la priorización de tráfico crítico y la optimización del ancho de banda.

Mayor seguridad: La seguridad de la red es un objetivo crítico en cualquier migración. SD-WAN debe proporcionar capacidades de seguridad sólidas, como cifrado de datos, autenticación, segmentación de la red y prevención de amenazas avanzadas. Además, debe integrarse de manera segura con soluciones de seguridad existentes.

SD-WAN (Software-Defined Wide Area Network) ofrece varias ventajas significativas en términos de la cantidad de sucursales y sitios remotos que una organización puede gestionar de manera eficiente. Algunas formas en las que SD-WAN ayuda en este sentido son:

Simplificación de la implementación: SD-WAN permite una implementación más rápida y sencilla de nuevas sucursales. Utilizando tecnologías de virtualización y administración centralizada, las configuraciones de red se pueden definir y desplegar de forma remota, eliminando la necesidad de enviar técnicos a cada ubicación física.

Gestión centralizada: Con SD-WAN, todas las sucursales y sitios remotos se pueden administrar y controlar desde una ubicación central. Esto simplifica las tareas de monitoreo, configuración, solución de problemas y actualizaciones de software. Los cambios en la configuración y las políticas de red se pueden aplicar de manera consistente en todas las sucursales, lo que mejora la eficiencia y reduce los errores humanos.

Optimización del tráfico: SD-WAN ofrece capacidades avanzadas de gestión del tráfico que ayudan a optimizar el rendimiento de las aplicaciones en todas las sucursales. Utiliza algoritmos y políticas de enrutamiento inteligentes para dirigir el tráfico a través de las rutas más eficientes y equilibrar la carga de manera óptima. Esto permite aprovechar múltiples enlaces de red y garantizar una experiencia de usuario consistente en todas las ubicaciones.

Mejora de la resiliencia: SD-WAN mejora la resiliencia de la red al permitir la utilización de múltiples conexiones de Internet en cada sucursal. Esto puede incluir conexiones de banda ancha, fibra óptica y enlaces de LTE. Al utilizar técnicas como el enrutamiento basado en políticas y la conmutación por error, SD-WAN puede garantizar una mayor disponibilidad y recuperación rápida en caso de fallas en los enlaces o interrupciones de servicio.

Ahorro de costos: SD-WAN puede ayudar a reducir los costos asociados con la gestión de múltiples sucursales. Al aprovechar conexiones de Internet de menor costo en lugar de una infraestructura MPLS tradicional, las organizaciones pueden obtener ahorros significativos en sus presupuestos de red.

En resumen, SD-WAN ofrece una solución altamente escalable y eficiente para gestionar una gran cantidad de sucursales y sitios remotos. Simplifica la implementación,

mejora la gestión centralizada, optimiza el rendimiento de las aplicaciones, aumenta la resiliencia de la red y reduce los costos operativos. Esto hace que SD-WAN sea una opción atractiva para las organizaciones con una amplia presencia de sucursales distribuidas geográficamente.

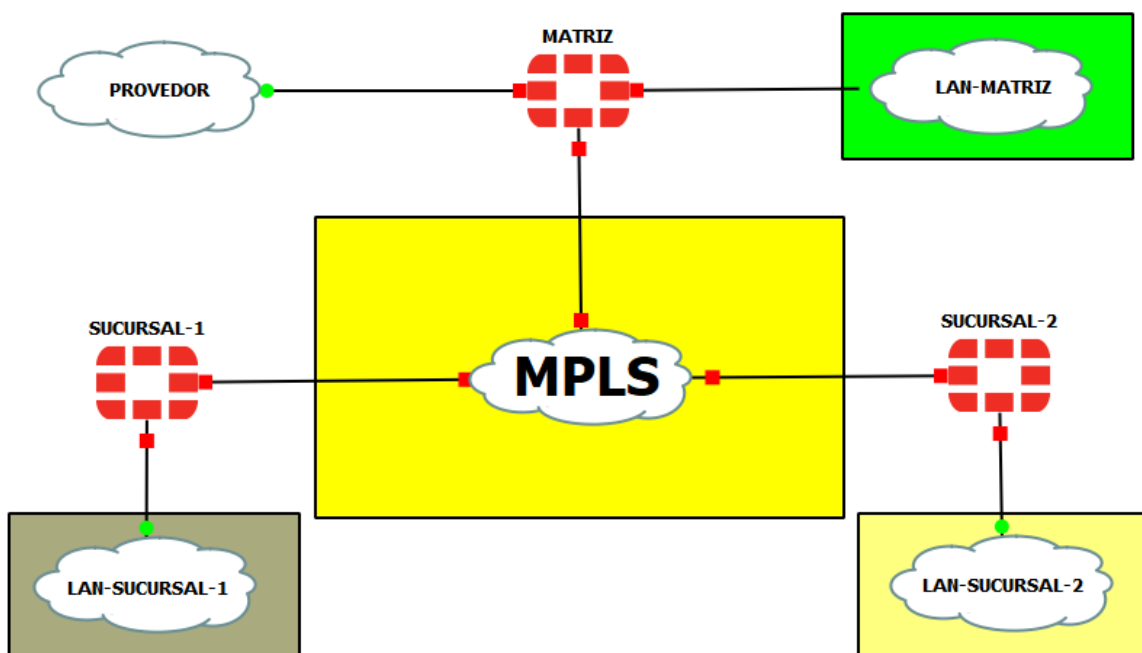
3.5.3. Diseño de la arquitectura SD-WAN

Para lograr el diseño e implementación adecuado, se utilizará el mismo software de emulación (GNS3), que permite implementar y configurar los equipos de red como routers, switches, computadoras, y otros. Este software tiene la capacidad de proporcionar permisos y privilegios para el acceso a Internet, la configuración de puertos, entre otras funcionalidades.

En este diseño, cada sucursal está equipada con un dispositivo SD-WAN que proporciona conectividad a través de la red MPLS. Los dispositivos SD-WAN están interconectados entre sí mediante la infraestructura MPLS existente, tal como se observa en la figura 33.

Figura 33

Diseño de solución SD-WAN



Fuente: GNS3 (2.2.37)

Cada dispositivo SD-WAN en las sucursales tiene múltiples interfaces de red para conectarse a diferentes enlaces, incluyendo los enlaces MPLS. Estos dispositivos SD-WAN utilizan técnicas avanzadas de enrutamiento y gestión del tráfico para optimizar el rendimiento y la utilización de los enlaces MPLS.

Además de la interconexión MPLS, los dispositivos SD-WAN también pueden aprovechar otras conexiones de Internet, como enlaces de banda ancha o LTE, para mejorar la resiliencia y la capacidad de ancho de banda de la red.

En la implementación de SD-WAN, se establecerán políticas de enrutamiento y gestión del tráfico para dirigir el tráfico de manera eficiente a través de los enlaces MPLS. Estas políticas pueden basarse en criterios como la calidad de servicio (QoS), la disponibilidad de los enlaces y la carga de los enlaces, entre otros.

Además, los dispositivos SD-WAN proporcionarían capacidades de seguridad integradas, como cifrado de datos y VPN, para proteger las comunicaciones entre las sucursales.

Es importante destacar que este diseño es la propuesta realizada para la topología existente y se puede personalizar según las necesidades y requisitos específicos de una organización.

3.5.4. Selección del proveedor SD-WAN

(FORTINET, 2023) destaca que los proveedores líderes en el mercado de SD-WAN incluyen Fortinet, Cisco/Viptela, HPE/Silver Peak, VMware/VeloCloud, Versa Networks y Palo Alto Networks/CloudGenix, tal como se muestra en la figura 34.

Figura 34

Cuadrante mágico de Gartner para SD-WAN



Fuente: <https://www.fortinet.com/lat/solutions/gartner-wan-edge>

Aunque la mayoría de los proveedores ofrecen facilidad de administración y optimización del tráfico en sus soluciones SD-WAN, cada uno tiene características y enfoques diferentes. Además del costo inicial y el costo total de propiedad (TCO), es esencial evaluar la capacidad de una solución SD-WAN para cumplir con los requisitos comerciales específicos en cuanto al rendimiento y la seguridad de las aplicaciones.

Una distinción clave entre varios proveedores de SD-WAN radica en si su solución ofrece SD-WAN o SD-WAN segura. SD-WAN por sí sola está diseñada para mejorar el rendimiento de la red de área amplia (WAN) de una organización mediante la optimización del enrutamiento del tráfico. Por otro lado, Secure SD-WAN integra la infraestructura de seguridad, como un firewall de próxima generación (NGFW), en una solución SD-WAN, lo

que capacita al departamento de TI, mejora la efectividad de la postura de seguridad y permite una mayor simplificación de la gestión.

Aunque muchos proveedores de SD-WAN afirman ofrecer soluciones de seguridad integradas, a menudo esto se logra mediante una cadena de herramientas de seguridad y redes independientes que no están realmente integradas y requieren múltiples consolas de administración. Este enfoque puede cumplir con ciertas necesidades de seguridad, pero a menudo se hace a expensas del rendimiento de la red y de un mayor costo total de propiedad (TCO). Las soluciones de seguridad independientes no están diseñadas para integrarse de forma nativa con otras soluciones, lo que resulta en una implementación, monitoreo y mantenimiento complejos de múltiples dispositivos, lo que aumenta los gastos generales asociados con la infraestructura SD-WAN de una organización. Esto a menudo anula los ahorros de costos esperados que las inversiones en SD-WAN generalmente ofrecen.

Cuando se elige entre proveedores de SD-WAN, es crucial buscar una optimización en términos de rendimiento, seguridad y costo total de propiedad (TCO) de la red.

Dentro de una oferta de Secure SD-WAN, diversas características contribuyen a su capacidad para cumplir con cada uno de estos tres objetivos. Existen seis puntos esenciales que se deben considerar al comparar las soluciones de Secure SD-WAN, que incluyen:

SD-WAN acelerada por ASIC: Un circuito integrado de aplicaciones específicas (ASIC) para SD-WAN es un componente de hardware diseñado y fabricado específicamente para optimizar las operaciones de SD-WAN. Esto permite que un dispositivo SD-WAN alcance una mayor escala y eficiencia sin degradación del rendimiento, a diferencia de las soluciones SD-WAN que se ejecutan en hardware comercial estándar (COTS) listo para su uso.

NGFW integrado: Una solución de SD-WAN segura debe incluir de manera nativa un NGFW (Next-Generation Firewall) integrado, lo que elimina la necesidad de implementar soluciones independientes de seguridad adicionales. Esta capacidad de integración debe

proporcionar protección desde la Capa 4 hasta la Capa 7, lo que incluye inspección de tráfico cifrado SSL/TLS y segmentación para detener el movimiento lateral de amenazas en ubicaciones distribuidas.

Disponibilidad multiplataforma: Los dispositivos SD-WAN deben contar con factores de forma físicos y virtuales que les permitan ser implementados en todos los ámbitos de la WAN corporativa. Esto incluye centros de datos, sucursales y despliegues en entornos de nube pública o privada.

Autosanación: La SD-WAN mejora la resiliencia de la red al seleccionar de manera dinámica rutas y realizar conmutación por error en milisegundos, junto con técnicas de remediación de WAN como Forward Error Correction (FEC) y duplicación de paquetes. Estas características permiten que una solución SD-WAN garantice tanto el rendimiento como la disponibilidad de las aplicaciones.

Rama SD segura: Secure SD-Branch integra las operaciones y elimina los compartimentos aislados. La combinación de la WAN, la seguridad y la capa de acceso (cableada e inalámbrica) permite la consolidación de la gestión, la reducción del riesgo y el aumento de la agilidad.

SASE de un solo proveedor: La arquitectura de Secure Access Service Edge (SASE) de un único proveedor amplía el acceso seguro y la conectividad de alto rendimiento a los usuarios, sin importar dónde se encuentren geográficamente.

De acuerdo con estos factores importantes que hay que tomar en cuenta para la selección del hardware que mejor se adapte a los requerimientos del diseño de una red SD-WAN segura, en la tabla 14 se realiza una comparativa para seleccionar la mejor opción de entre los principales proveedores destacados anteriormente.

Tabla 14*Comparativa de proveedores líderes en SD-WAN*

| PROVEEDOR | REQUERIMIENTOS | | | | | | VALORACIÓN TOTAL |
|-------------------------|---------------------------|----------------|--------------------------------|-----------------------------------|-----------------|---------------------------|------------------|
| | SD-WAN acelerado por ASIC | NGFW integrado | Disponibilidad multiplataforma | SD-WAN de recuperación automática | Ram a SD segura | SASE de un solo proveedor | |
| Fortinet | 1 | 1 | 1 | 1 | 1 | 1 | 6 |
| Cisco Viptela | 0 | 1 | 1 | 1 | 0 | 1 | 4 |
| HPE Silver Peak | 0 | 0 | 1 | 1 | 0 | 1 | 3 |
| VMware VeloCloud | 0 | 0 | 1 | 1 | 0 | 1 | 3 |
| Palo Alto Prisma SD-WAN | 0 | 0 | 1 | 0 | 0 | 1 | 2 |
| Versa Networks | 0 | 1 | 1 | 0 | 0 | 1 | 3 |

1 Cumple
0 No cumple

Fuente: Adaptado de (FORTINET, 2023)

Se ha decidido optar por el NGFW de Fortinet como elección, ya que satisface los requisitos fundamentales de Secure SD-WAN y supera en rendimiento a las demás alternativas disponibles en el mercado. Una de las cualidades destacadas de este NGFW elegido es su aceleración por ASIC, que cuenta con las funcionalidades necesarias para una optimización de las operaciones de SD-WAN a diferencia de los otros proveedores que carecían de esta cualidad.

Capítulo 4. Emulación y análisis de resultados

En este capítulo, se procede con la etapa de “implementación”, donde se simula una red SD-WAN (Software-Defined Wide Area Network) en base a la simulada en el capítulo III, para posteriormente monitorear la misma. En primer lugar, se explica el concepto y los principios fundamentales de una red SD-WAN, destacando su capacidad para optimizar el tráfico de datos en entornos distribuidos y su flexibilidad para adaptarse a las necesidades cambiantes de las empresas.

Posteriormente, se procede a emular la red SD-WAN utilizando las mismas herramientas de virtualización y configuración específicas. Se describe el proceso paso a paso, incluyendo la creación de nodos, la definición de políticas de enrutamiento, la implementación de funciones de seguridad y la configuración de diferentes enlaces de conexión.

Una vez establecida la red SD-WAN simulada, se aborda el tema del monitoreo y la gestión. Donde se presenta diversas soluciones y herramientas utilizadas para supervisar el rendimiento de la red, identificar posibles cuellos de botella y realizar ajustes en tiempo real para garantizar una óptima experiencia de usuario.

Finalmente, se realiza una comparativa entre la red SD-WAN emulada y la red tradicional de área amplia. Se evalúan aspectos como el rendimiento, la escalabilidad, la seguridad y la gestión de ambas infraestructuras. Esta comparativa permite comprender las ventajas y desventajas de adoptar una red SD-WAN en lugar de una red convencional y proporciona una visión clara de cómo esta tecnología puede mejorar la eficiencia y la agilidad de las redes empresariales en la actualidad.

4.1. Emulación de la red SD-WAN

En esta sección se detalla la emulación de la red SD-WAN en un entorno virtual replicando las características y funcionalidades expuestas anteriormente en un entorno controlado. La simulación permite comprender a profundidad como opera y responde la red en

situaciones diversas. Durante este proceso se utilizó las mismas herramientas de virtualización usadas en la emulación de la red tradicional para emular los dispositivos, enlaces y políticas de enrutamiento que componen la red SD-WAN. 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 respectivo.

4.1.1. Configuración de puertos

En esta sección se detalla minuciosamente los parámetros que debe configurarse para un puerto específico, ya que los demás puertos seguirán el mismo procedimiento. En el ejemplo, se toma como referencia la sede principal. En la configuración de interfaces, se brinda la facilidad de asignar un nombre y un rol. En este caso, se utiliza como ejemplo la configuración del puerto conectado a la red MPLS de la sede principal, denominado "MTZ-R3". La opción de asignar una dirección IP de forma manual o mediante DHCP está disponible, y en el proceso de emulación se seleccionó la configuración manual. Los accesos administrativos permitidos son de gran importancia, ya que varían según el rol de cada puerto. En esta situación específica, se necesita acceso a "HTTPS", "HTTP" y "PING". La figura 35 muestra la configuración del puerto 2 de la matriz.

Figura 35

Configuración puerto 2 de la matriz

The screenshot shows the 'Edit Interface' configuration page in FortiOS v7.0.5. The left sidebar contains the navigation menu with 'Network' expanded and 'Interfaces' selected. The main configuration area is titled 'Edit Interface' and contains the following fields:

- Name:** port2
- Alias:** MTZ-R3
- Type:** Physical Interface
- VRF ID:** 0
- Role:** Undefined
- Dedicated Management Port:** Disabled
- Addressing mode:** Manual (selected), DHCP, Auto-managed by IPAM, One-Arm Sniffer
- IP/Netmask:** 172.16.31.1/255.255.255.252
- Secondary IP address:** Disabled
- Administrative Access (IPv4):**
 - HTTPS
 - PING
 - SSH
 - SNMP
 - RADIUS Accounting
 - Security Fabric Connection
 - FMG-Access
 - FTM
 - Speed Test
- Receive LLDP:** Use VDOM Setting, Enable, Disable
- Transmit LLDP:** Use VDOM Setting, Enable, Disable

At the bottom right, there are 'OK' and 'Cancel' buttons.

Fuente: FortiOS v7.0.5

4.1.2. Configuración de enlaces SD-WAN

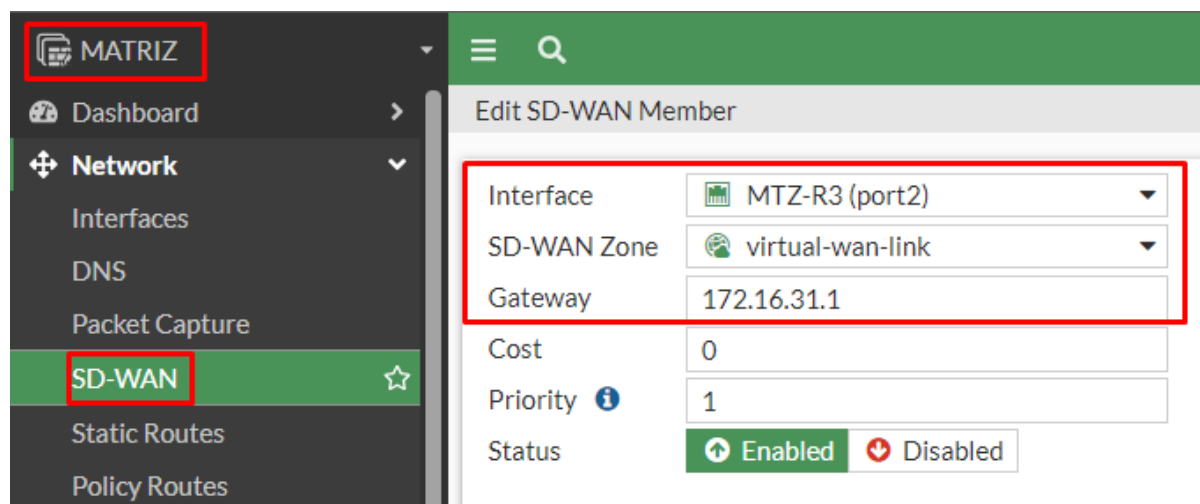
La SD-WAN en el FortiGate de la sede principal comprende el enlace que conecta con la nube MPLS. La figura 36 ilustra la red involucrada en la SD-WAN del FortiGate de la sede principal. El objetivo es permitir la interacción y el control entre las redes ubicadas en la matriz, sucursal 1 y 2 desde un único punto de administración. Esto crea una red automatizada, centralizada e inteligente que optimiza el rendimiento de cada enlace en base a reglas o políticas, las cuales se detallan posteriormente. Cabe destacar que los FortiGate de la sucursal 1 y 2 siguen un esquema similar al asociar sus enlaces directamente conectados a la SD-WAN, tal como se muestra en el anexo C.

Para la creación de la interfaz virtual SD-WAN: Dentro del panel de configuración, se crea una interfaz virtual SD-WAN. Esta interfaz podría agrupar la interfaz física WAN con

otras conexiones (por ejemplo, una interfaz de Internet de respaldo). En este caso se ha agregado solo las interfaces WAN.

Figura 36

Configuración miembros SD-WAN matriz



| | Interfaces | Gateway | Cost |
|--|------------------|-------------|------|
| | virtual-wan-link | | |
| | MTZ-R3 (port2) | 172.16.31.1 | 0 |

Fuente: FortiOS v7.0.5

4.1.3. Políticas de enrutamiento

Previo a continuar con las políticas, es esencial destacar que una vez que todos los enlaces de la SD-WAN se han agregado tanto en la matriz, sucursal 1 y 2, en términos generales, se configura una única ruta estática (0.0.0.0/0) para la SD-WAN con el fin de habilitar el acceso a Internet. Esto debe realizarse en cada FortiGate. Sin embargo, cabe resaltar que esto no implica que se pueda navegar por Internet. Aquí es donde entra en juego la relevancia de las políticas, que son las encargadas de definir los puertos a través de los cuales el tráfico entra y sale, así como los objetos que establecen las subredes de origen y destino del tráfico. Estas políticas juegan un papel crucial en la seguridad, ya que determinan el tipo de

protección a utilizar; este aspecto será explicado con mayor detalle en secciones posteriores del documento, específicamente en el apartado 4.1.3.1 referente a las políticas de la matriz.

4.1.3.1. Políticas de la matriz

En la sede principal se establecen un total de 5 políticas, donde una de ellas es una política implícita o predeterminada presente en todos los dispositivos FortiGate. Esta política, denominada "Implicit Deny," tiene la función de rechazar cualquier tipo de tráfico dirigido hacia cualquier destino. Además de esta política implícita, se creó otras 4 políticas adicionales para gestionar el tráfico de manera específica.

La política denominada "Acceso a Internet" establece que el puerto de entrada es el puerto 3, el cual se encuentra conectado a la LAN de la matriz, mientras que el puerto de salida es el puerto 1. En esta política, hay una característica especial que se refiere a la SD-WAN como puerto de entrada con el propósito de permitir a la sucursal 1 acceder a Internet utilizando su enlace de banda ancha a través de la red MPLS en situaciones donde exista saturación o pérdida de paquetes en su único enlace de banda ancha. Las subredes de origen que se incluyen en esta política son la "L-MTZ" o LAN de la matriz, la "L-S1" o LAN de la sucursal 1 y la nube "MPLS". El destino está definido como "all", que hace referencia a Internet. De esta manera, la política permite que la matriz y la sucursal 1 pueda navegar por Internet aprovechando la flexibilidad de la SD-WAN para utilizar los enlaces de banda ancha disponibles según las necesidades y condiciones de la red.

La política "To_L-MTZ" configura la LAN como punto de entrada y la SD-WAN como punto de salida. Se permiten conexiones unidireccionales desde la matriz hacia la sucursal 1 y 2, usando la subred de origen "L-MTZ" y las subredes de destino "L-S1" y "L-S2 ". En cuanto al tráfico en dirección contraria, se aplica la política "From_L-MTZ", que usa la SD-WAN como puerto de entrada y la LAN como puerto de salida. Las subredes de origen son "L-S1",

"L-S2" y "MPLS", mientras que, la subred de destino es "L-MTZ". De esta manera, se establece la conexión desde la sucursal 1 y la sucursal 2 hacia la matriz.

La política "InterBranchTraffic_S1_S2" establece que la SD-WAN funciona tanto como puerto de entrada como puerto de salida. Las subredes de origen y destino involucradas son "L-S1", "L-S2" y "MPLS". Esta política permite la conexión bidireccional entre la sucursal 1 y 2, utilizando el Fortigate de la matriz como intermediario para el tráfico entre la sucursal 1 y la sucursal 2. Por ejemplo, si se cae el enlace de la sucursal 1 con la nube MPLS, el tráfico se dirigirá por el puerto 1.

Por último, en la figura 37 se presentan todas las políticas de la matriz, lo que proporciona una visión más clara y comprensible de todo lo descrito anteriormente.

Figura 37

Políticas de la matriz

| ID | Name | Source | Destination | Status |
|--|--------------------------|-----------------------|----------------------|---------|
| LAN-MTZ (port3) → virtual-wan-link 2 | | | | |
| 1 | Acceso a Internet | L-MTZ L-S1 MPLS | all | Enabled |
| 2 | To_L-MTZ | L-MTZ | L-S1 L-S2 | Enabled |
| virtual-wan-link → LAN-MTZ (port3) 1 | | | | |
| 3 | From_L-MTZ | L-S1 L-S2 MPLS | L-MTZ | Enabled |
| virtual-wan-link → virtual-wan-link 1 | | | | |
| 4 | InterBranchTraffic_S1_S2 | L-S1 L-S2 MPLS | L-S1 L-S2 MPLS | Enabled |
| Implicit 1 | | | | |
| 0 | Implicit Deny | all | all | |

Fuente: FortiOS v7.0.5

4.1.3.2. Políticas sucursal 1

Tanto en la sucursal 1 como en la matriz, se cuentan con 5 políticas: una de ellas es la denominada "Implicit Deny", mientras que las otras 4 fueron creadas para la gestión del tráfico. Estas políticas operan de manera similar a las de la matriz, pero se presta especial atención a los aspectos que han experimentado cambios.

La política denominada "Acceso a internet" establece que el puerto de entrada es el de la LAN, mientras que el puerto de salida corresponde a la SD-WAN de la sucursal 1. La única distinción aquí es que la subred de origen se asigna a "L-S1", y el destino sigue siendo "all" (todos). Esta política permite que todos los usuarios de la sucursal 1 puedan acceder a Internet y navegar libremente en la red.

La política denominada "To_L-MTZ_L-S2" en la sucursal 1 sigue la misma configuración que en la matriz, utilizando como puerto de entrada el puerto 3 y salida el puerto SD-WAN de la sucursal 1. En esta política, la subred de origen es "L-S1", y las subredes de destino son "L-MTZ" y "L-S2". Su objetivo es establecer una conexión unidireccional que va desde la sucursal 1 hacia la matriz y la sucursal 2. En cuanto a la política "From_L-MTZ_L-S2", esta opera en sentido contrario y emplea los mismos puertos de entrada y salida. Las subredes de origen en esta política son "L-MTZ", "MPLS" y "L-S2", mientras que la subred de destino es "L-S1". Su función es facilitar la conexión desde la matriz y la sucursal 2 hacia la sucursal 1, pudiendo utilizar la red MPLS para lograrlo.

La política "InterBranchTraffic_L-MTZ_L-S2" utiliza la SD-WAN como puerto de entrada y salida. Las subredes de origen incluyen "L-S2", "L-MTZ" y "MPLS", mientras que las subredes de destino son "L-MTZ" y "L-S2". Esta política posibilita el establecimiento de una conexión entre la sucursal 2 y la matriz, ya sea desde una hacia la otra o viceversa, pero mediante un enrutamiento a través de la sucursal 1. Es decir, el FortiGate ubicado en la sucursal 1 funciona como intermediario. Por último, es posible observar todas las políticas de la sucursal 1 en la figura 38.

Figura 38*Políticas de la sucursal 1*

| ID | Name | Source | Destination | Status |
|---------------------------------------|-------------------------------|-----------------------|---------------|---------|
| LAN-S1 (port3) → virtual-wan-link 2 | | | | |
| 1 | Acceso a internet | L-S1 | all | Enabled |
| 2 | To_L-MTZ_L-S2 | L-S1 | L-MTZ L-S2 | Enabled |
| virtual-wan-link → LAN-S1 (port3) 1 | | | | |
| 3 | From_L-MTZ_L-S2 | L-MTZ L-S2 MPLS | L-S1 | Enabled |
| virtual-wan-link → virtual-wan-link 1 | | | | |
| 4 | InterBranchTraffic_L-MTZ_L-S2 | L-MTZ L-S2 MPLS | L-MTZ L-S2 | Enabled |
| Implicit 1 | | | | |

Fuente: FortiOS v7.0.5

4.1.3.3. Políticas sucursal 2

La sucursal 2 se distingue de la matriz y sucursal 1 al ser una oficina remota más simplificada. En esta ubicación, se han establecido tres políticas, además de la política "Implicit Deny".

La política "Acceso a Internet" en la sucursal 2 tiene la configuración de usar la LAN como puerto de entrada y el puerto 1 de la sucursal 2 como puerto de salida. La subred de origen asignada es "L-S2", y el destino es "all" (todos). Esta política habilita el acceso a Internet para los usuarios presentes en la sucursal.

La política "To_L-MTZ_L-S1" presenta el puerto de entrada el de la LAN y de salida el puerto SD-WAN de la sucursal 2 y utiliza la misma subred de origen. La diferencia radica en la subred de destino, que corresponde a las subredes "L-MTTZ y L-S1". Esta política establece una conexión unidireccional desde la sucursal 2 hacia la sucursal 1 y la matriz. Por otro lado, la política "From_L-MTZ" emplea la SD-WAN como puerto de entrada y la LAN como puerto de salida. Las subredes de origen son "L-MTZ", "MPLS" y "L-S1", mientras que la subred de destino es "L-S2". Su propósito es establecer la conexión desde la matriz y sucursal

1 hacia la sucursal 2. Por último, todas las políticas de la sucursal 2 pueden ser apreciadas en la figura 39.

Figura 39

Políticas de la sucursal 2

| ID | Name | Source | Destination | Status |
|--|-------------------|-----------------------|---------------|---------|
| LAN-S2 (port3) → virtual-wan-link 2 | | | | |
| 1 | Acceso a Internet | L-S2 | all | Enabled |
| 2 | To_L-MTZ_L-S1 | L-S2 | L-MTZ L-S1 | Enabled |
| virtual-wan-link → LAN-S2 (port3) 1 | | | | |
| 3 | From_L-MTZ | L-MTZ L-S1 MPLS | L-S2 | Enabled |
| Implicit 1 | | | | |

Fuente: FortiOS v7.0.5

4.1.4. Reglas SD-WAN

Siguiendo las directrices de la red, se procede a establecer las pautas que caracterizan el funcionamiento de la SD-WAN. Estas pautas habilitan una mayor inteligencia en la red y permiten que tome decisiones de enrutamiento de manera automática, considerando factores como la latencia, el ancho de banda, entre otros. A continuación, se explica cómo funcionan las reglas SD-WAN en la matriz, sucursal 1 y 2.

4.1.4.1. Reglas de la matriz

Dentro de la matriz, se han establecido 3 reglas, siendo la primera denominada "To-L-S1". Su función principal es dirigir el tráfico que proviene tanto de la matriz como de la sucursal 2 hacia la sucursal 1. Con consideración de que las opciones de ruta disponibles son la "MPLS", la SD-WAN tomará la decisión de forma automática, seleccionando la mejor ruta en función del parámetro de latencia. En situaciones donde se presente un aumento inesperado en la demora, la SD-WAN se encargará de elegir la ruta óptima para el tráfico.

La segunda regla, denominada "To-L-S2", tiene la finalidad de dirigir el tráfico desde la matriz o sucursal 1 hacia la sucursal 2 utilizando la ruta óptima, según el mismo parámetro de latencia. Es relevante destacar que dicho parámetro puede ser ajustado a discreción del

administrador o del cliente, lo que permite considerar otras variables como el ancho de banda, pérdida de paquetes, SLA, entre otras. De esta manera, se ofrece flexibilidad para adaptar el comportamiento de la red según las necesidades específicas y preferencias del usuario.

A continuación, se presenta la regla denominada "Acceso a internet," la cual desempeña la función de equilibrar el tráfico que permite que tanto la matriz como la sucursal 1 accedan a Internet. Se Incluyó la sucursal 1 debido a que, en caso de que su enlace de conexión a Internet presente problemas, se ha determinado que haga uso de uno de los enlaces disponibles en la matriz. Para esta tarea, la SD-WAN selecciona la mejor de las conexiones disponibles. Si se producen múltiples sesiones simultáneas, se realizará una distribución equitativa de la carga de tráfico, asegurándose de que todas las conexiones participen en el proceso, todo esto basado en un Acuerdo de Nivel de Servicio (SLA). Finalmente, todas las reglas establecidas para la matriz se muestran en la figura 40.

Figura 40

Reglas de la matriz

| ID | Name | Source | Destination | Criteria | Members |
|-------------------|-------------------|---------------|-------------|-----------|-------------------------|
| IPv4 3 | | | | | |
| 1 | To-L-S1 | L-MTZ L-S2 | L-S1 | Latency | MTZ-R3 (port2) port1 |
| 2 | To-L-S2 | L-MTZ L-S1 | L-S2 | Latency | MTZ-R3 (port2) port1 |
| 3 | Acceso_a_internet | L-MTZ L-S1 | all | SLA | MTZ-R3 (port2) port1 |
| Implicit 1 | | | | | |
| | sd-wan | all | all | Source IP | any |

Fuente: FortiOS v7.0.5

4.1.4.2. Reglas sucursal 1

Asimismo, en la sucursal 1, se han establecido 3 reglas SD-WAN, siendo una de ellas denominada "To-L-MTZ". Esta regla tiene la responsabilidad de seleccionar la ruta óptima entre la sucursal 1 y la matriz, tomando como criterio fundamental el parámetro de latencia.

Seguidamente, se realizó la regla denominada "To-L-S2," cuyo propósito es seleccionar la mejor ruta disponible para dirigir el tráfico desde la sucursal 1 y matriz hacia la sucursal 2. Al igual que las reglas previas, esta decisión se fundamenta en el parámetro de latencia.

Después, se encuentra una regla denominada "Acceso a internet" cuyo objetivo es seleccionar la mejor ruta basada en la latencia para permitir que los usuarios de la sucursal 1 accedan a Internet. En este contexto, la regla tiene la opción de elegir entre su única conexión de banda ancha o, alternativamente, utilizar el FortiGate de la matriz como intermediario para acceder a Internet. La representación visual de todas las reglas de la sucursal 1 se encuentra en la figura 41.

Figura 41

Reglas sucursal 1

| ID | Name | Source | Destination | Criteria | Members |
|-------------------|-------------------|---------------|-------------|-----------|--------------------------|
| IPv4 3 | | | | | |
| 1 | To-L-MTZ | L-S1 | L-MTZ | Latency | S1-MPLS (port2) port1 |
| 2 | To-L-S2 | L-MTZ L-S1 | L-S2 | Latency | S1-MPLS (port2) port1 |
| 3 | Acceso_a_internet | L-S1 | all | Latency | S1-MPLS (port2) port1 |
| Implicit 1 | | | | | |
| | sd-wan | all | all | Source IP | any |

Fuente: FortiOS v7.0.5

4.1.4.3. Reglas sucursal 2

En el caso de la sucursal 2, se han establecido 3 reglas SD-WAN, siendo la primera denominada "To-L-MTZ", cuya función principal es seleccionar la mejor ruta para dirigir el tráfico desde la sucursal 2 hacia la matriz. Para esta elección, cuenta con las opciones de ruta "MPLS" y "SD-WAN", y tomará la decisión basándose en la latencia, escogiendo así el camino óptimo para el tráfico.

La regla "To-L-S1" opera con el mismo mecanismo, pero tiene un destino diferente, es decir, su propósito es dirigir el tráfico desde la sucursal 2 hacia la sucursal 1.

Por último, se tiene la regla "Acceso a internet", la cual habilita a los usuarios para acceder a Internet utilizando la ruta más adecuada. En esta situación, se disponen únicamente de dos enlaces de banda ancha, como se ilustra en la figura 42. Por consiguiente, en caso de un alto tráfico, se aplica un balanceo de carga, similar al que se realiza en la matriz. De esta manera, se asegura un aprovechamiento óptimo de los enlaces disponibles para el acceso a Internet.

Figura 42

Reglas sucursal 2

| ID | Name | Source | Destination | Criteria | Members |
|-------------------|-------------------|--------|-------------|-----------|--------------------------|
| IPv4 3 | | | | | |
| 1 | To-L-MTZ | L-S2 | L-MTZ | Latency | S2-MPLS (port2) port1 |
| 2 | To-L-S1 | L-S2 | L-S1 | Latency | S2-MPLS (port2) port1 |
| 3 | Acceso_a_internet | L-S2 | all | SLA | S2-MPLS (port2) port1 |
| Implicit 1 | | | | | |
| | sd-wan | all | all | Source IP | any |

Fuente: FortiOS v7.0.5

4.2. Monitoreo de la red SD-WAN

Esta sección facilita la monitorización del desempeño de los enlaces pertenecientes a SD-WAN a través de señales de sondeo dirigidas a un servidor. De este modo, se evaluó la latencia, el jitter y la pérdida de paquetes de cada enlace, lo que está estrechamente vinculado con la Calidad de Servicio (QoS). Para llevar a cabo esta supervisión de los enlaces de manera efectiva, es imprescindible contar con la dirección IP de un servidor en el destino.

En la figura 43 se muestran los enlaces que se supervisaron desde la matriz. En primer lugar, encontramos el enlace denominado "QoS_L-S2", el cual se refiere a las rutas dirigidas hacia la sucursal 2. A continuación, aparece el enlace "Google", encargado de las conexiones a Internet. Por último, se visualiza el enlace "QoS_L-S1", el cual monitoriza las rutas dirigidas hacia la sucursal 1.

Figura 43*Monitoreo de enlaces matriz*

| Name | Detect Server | Packet Loss | Latency | Jitter |
|----------|---------------|-------------------------------|-------------------------------|-------------------------------|
| Google | 8.8.8.8 | port1: ? MTZ-R3 (port2): ? | port1: ? MTZ-R3 (port2): ? | port1: ? MTZ-R3 (port2): ? |
| QoS_L_S1 | 192.168.32.1 | port1: ? MTZ-R3 (port2): ? | port1: ? MTZ-R3 (port2): ? | port1: ? MTZ-R3 (port2): ? |
| QoS_L_S2 | 192.168.33.1 | port1: ? MTZ-R3 (port2): ? | port1: ? MTZ-R3 (port2): ? | port1: ? MTZ-R3 (port2): ? |

Fuente: FortiOS v7.0.5

Con relación a la sucursal 1, su función consiste en supervisar los enlaces dirigidos hacia Internet mediante el uso de "Google", así como los enlaces dirigidos hacia la matriz a través de "QoS_MPLS" y los enlaces que se dirigen hacia la sucursal 2 mediante "QoS_L-S2", como se ilustra en la figura 44.

Figura 44*Monitoreo de enlaces sucursal 1*

| Name | Detect Server | Packet Loss | Latency | Jitter |
|----------|---------------|--------------------------------|--------------------------------|--------------------------------|
| Google | 8.8.8.8 | port1: ? S1-MPLS (port2): ? | port1: ? S1-MPLS (port2): ? | port1: ? S1-MPLS (port2): ? |
| QoS_L_S2 | 192.168.33.1 | port1: ? S1-MPLS (port2): ? | port1: ? S1-MPLS (port2): ? | port1: ? S1-MPLS (port2): ? |
| QoS_MPLS | 192.168.31.1 | port1: ? S1-MPLS (port2): ? | port1: ? S1-MPLS (port2): ? | port1: ? S1-MPLS (port2): ? |

Fuente: FortiOS v7.0.5

Por último, la sucursal 2 opera de manera semejante a la matriz y a la sucursal 1, encargándose de supervisar las conexiones dirigidas hacia la sucursal 1 utilizando el "QoS_L-S1", desde la matriz mediante el "QoS_L-MTZ", y hacia Internet a través del "Google". Esta información se representa visualmente en la figura 45, que muestra los enlaces bajo monitorización.

Figura 45*Monitoreo de enlaces sucursal 2*

| Name | Detect Server | Packet Loss | Latency | Jitter |
|-----------|---------------|--------------------------------|--------------------------------|--------------------------------|
| Google | 8.8.8.8 | port1: ? S2-MPLS (port2): ↓ | port1: ? S2-MPLS (port2): ↓ | port1: ? S2-MPLS (port2): ↓ |
| QoS_L_MTZ | 192.168.31.1 | port1: ? S2-MPLS (port2): ↓ | port1: ? S2-MPLS (port2): ↓ | port1: ? S2-MPLS (port2): ↓ |
| QoS_L_S1 | 192.168.32.1 | port1: ? S2-MPLS (port2): ↓ | port1: ? S2-MPLS (port2): ↓ | port1: ? S2-MPLS (port2): ↓ |

Fuente: FortiOS v7.0.5

4.2.1. Conectividad

Al igual que en el monitoreo de la red WAN primero se realizaron pruebas de conectividad con la ayuda del protocolo ICMP (ping), con el fin de probar la conexión entre 1 o varios hosts. En la figura 46 se puede observar la conexión entre el router de administración “MATRIZ” y el router “SUCURSAL-1”.

Figura 46*Conectividad entre matriz y sucursal 1*

```

MATRIZ # execute ping 172.16.32.1
PING 172.16.32.1 (172.16.32.1): 56 data bytes
64 bytes from 172.16.32.1: icmp_seq=0 ttl=254 time=5.5 ms
64 bytes from 172.16.32.1: icmp_seq=1 ttl=254 time=4.0 ms
64 bytes from 172.16.32.1: icmp_seq=2 ttl=254 time=2.4 ms
64 bytes from 172.16.32.1: icmp_seq=3 ttl=254 time=3.5 ms
64 bytes from 172.16.32.1: icmp_seq=4 ttl=254 time=2.4 ms

--- 172.16.32.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.4/3.5/5.5 ms

```

Fuente: FortiOS v7.0.5

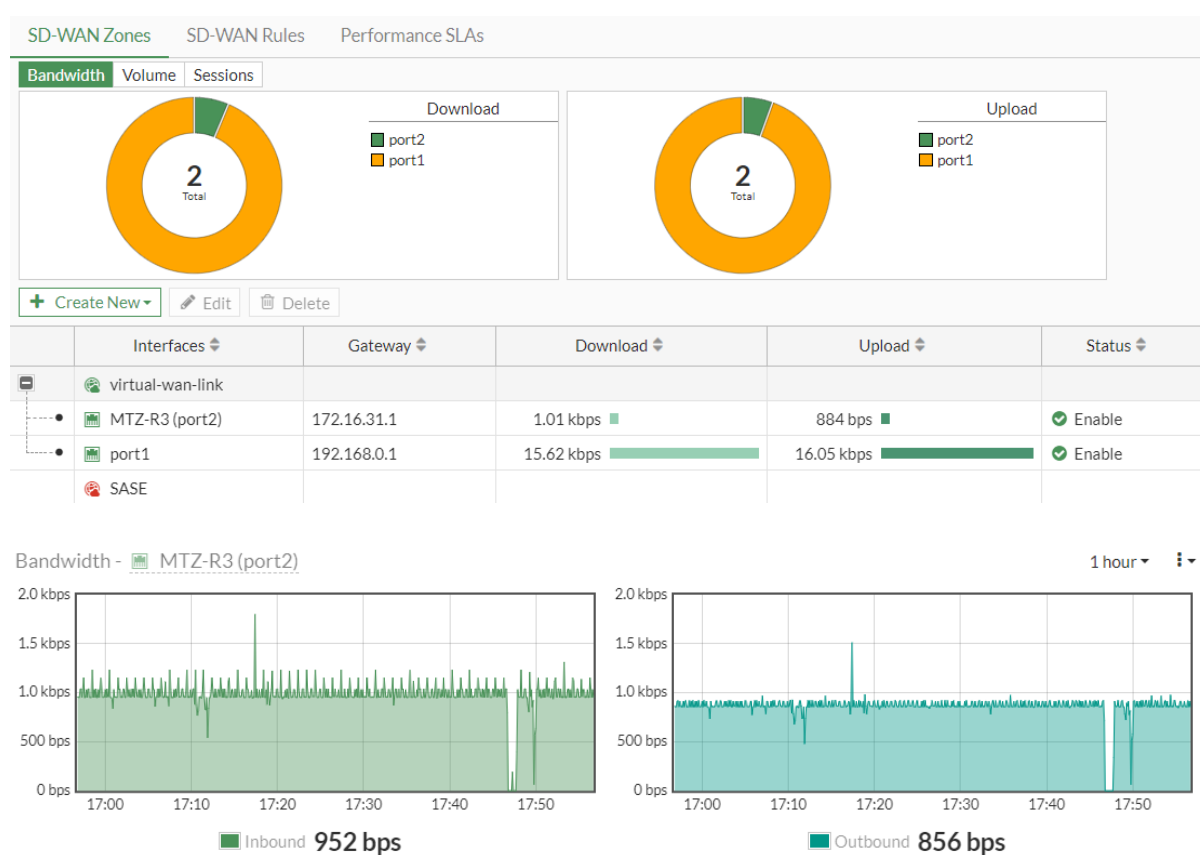
4.2.2. Ancho de banda

Se realizó una exhaustiva medición de ancho de banda en la red SD-WAN. Esta medición se llevó a cabo utilizando herramientas de monitoreo incluidas en los dispositivos

Fortigate que permitieron evaluar el rendimiento de la red en las interfaces que pertenecen a SD-WAN. Los resultados de la medición de ancho de banda confirman que la red es confiable, escalable y capaz de satisfacer las demandas de un entorno empresarial en constante evolución. Cuyos resultados son expuestos en la comparativa que se presenta más adelante en el apartado de análisis de resultados. En la figura 47, se presenta una gráfica de la medición de ancho de banda de los puertos pertenecientes a la SD-WAN.

Figura 47

Medición ancho de banda enlaces SD-WAN matriz



Fuente: FortiOS v7.0.5

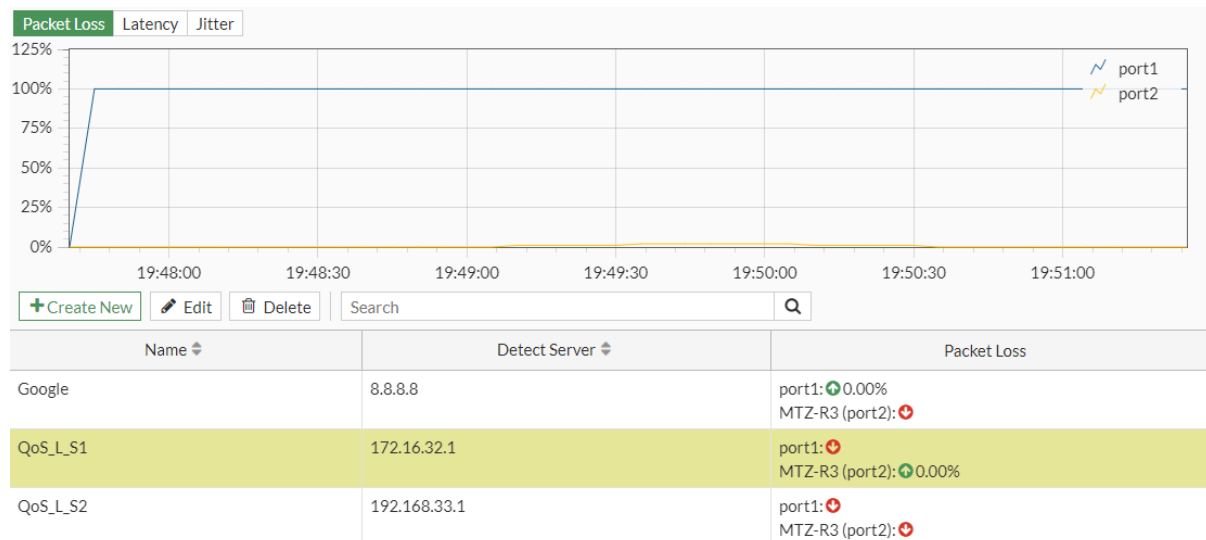
4.2.3. Perdida de paquetes

En la figura 48 se presenta la medición de pérdida de paquetes la red SD-WAN perteneciente a la matriz. Donde se ha demostrado una excelente estabilidad y confiabilidad, lo que ha resultado una transmisión de datos fluida y sin interrupciones al presentar ausencia

de pérdida de paquetes en el enlace asegurando una comunicación eficiente y proporcionando una experiencia de usuario excepcional, lo que se traduce en un entorno de trabajo óptimo.

Figura 48

Medición perdida de paquetes enlace SD-WAN matriz



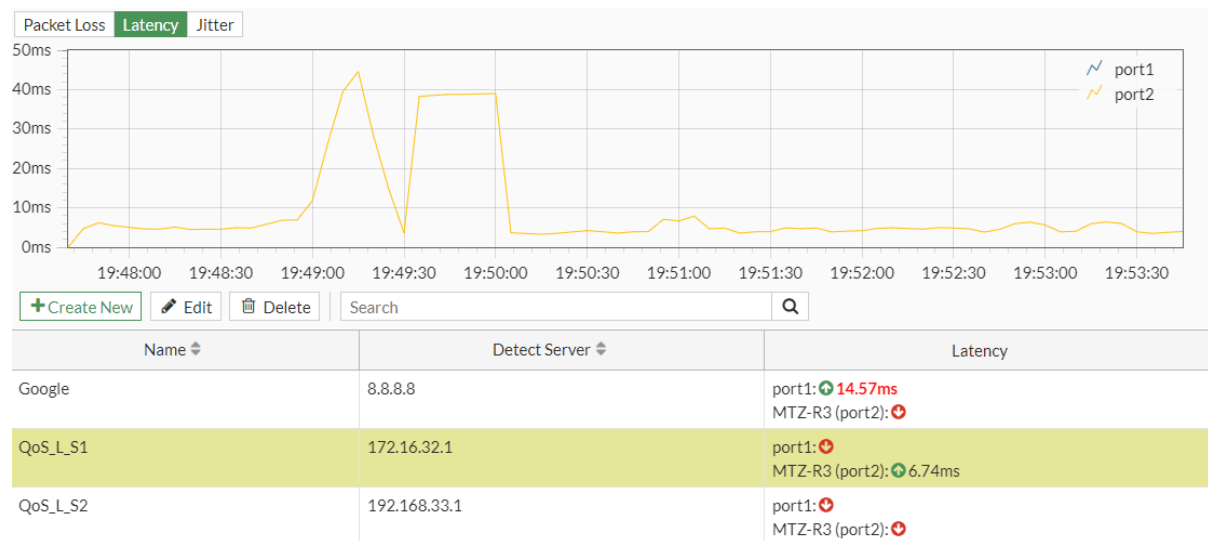
Fuente: FortiOS v7.0.5

4.2.4. Latencia

Se realizó exhaustivas pruebas de latencia en la red SD-WAN para evaluar su rendimiento y eficiencia. Estas pruebas han proporcionado una clara visión de los tiempos de respuesta entre diferentes puntos de la red, permitiendo identificar las métricas pertenecientes a cada enlace. Los resultados obtenidos serán evaluados más adelante en el apartado de análisis de resultados. En la figura 49 se muestra las pruebas de latencia del enlace SD-WAN de la matriz.

Figura 49

Medición latencia enlace SD-WAN matriz



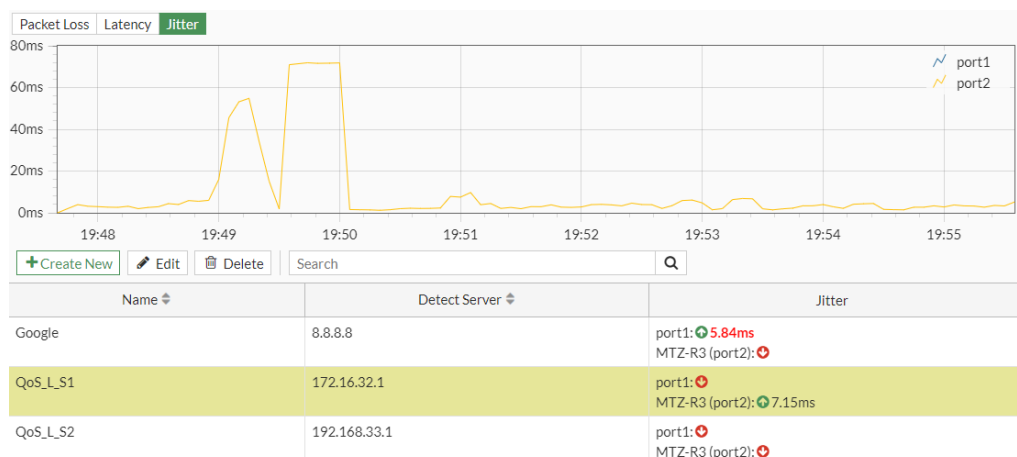
Fuente: FortiOS v7.0.5

4.2.5. Jitter

La medición de jitter en el enlace SD-WAN se realizó con la ayuda de las herramientas que brinda Fortigate en sus dispositivos, al igual que los parámetros anteriores, en este caso la figura 50 refiere a la evaluación de la variabilidad en los tiempos de llegada de los paquetes de datos a lo largo del enlace de red SD-WAN de la matriz. En otras palabras, en la gráfica se muestra la fluctuación en la latencia de la conexión.

Figura 50

Medición jitter enlace SD-WAN matriz



Fuente: FortiOS v7.0.5

4.3. Análisis de resultados

En este apartado se examinan los resultados logrados al emular la SD-WAN, junto con las ventajas destacadas del programa GNS3. De esta forma, se verificará el rendimiento de la red y se confirmarán los conceptos y características mencionadas en el marco teórico, específicamente en el apartado 2.4.

4.3.1. Emulación

En este segmento se verifica la correcta operatividad de la SD-WAN, analizando detalladamente los diversos parámetros que hacen posible su funcionamiento, como el control centralizado, la selección dinámica de ruta, monitorización en tiempo real, entre otros aspectos. En el anexo D se presenta la topología completa de la SD-WAN, junto con todas las redes locales y extendidas.

4.3.2. Transporte múltiple

En esta sección se verifica la capacidad de la SD-WAN para gestionar múltiples rutas, es decir, su habilidad para utilizar la red MPLS y la infraestructura pública de Internet como medios de transporte para dirigir el tráfico hacia Internet u oficinas remotas. Con el fin de comprobar su funcionamiento, se realiza un ping desde la matriz hacia la sucursal 1, de manera que el tráfico puede llegar a través de la red MPLS o el túnel IPsec que utiliza el enlace de banda ancha de Internet. El objetivo es observar cómo la red MPLS y las conexiones de Internet trabajan en conjunto para validar el enrutamiento múltiple de la SD-WAN. Dado que muchas empresas actualmente cuentan con infraestructura MPLS y desean mantenerla, esta se incluye en la emulación y se combina con los diversos transportes de la SD-WAN para lograr una configuración de SD-WAN Híbrida.

En la figura 51 se muestra la ejecución de un ping desde la matriz hacia la sucursal 1, empleando la interfaz de salida "MTZ-R3", que corresponde a uno de los enlaces conectados a

la red MPLS. Se efectúa un traceroute para identificar la ruta que los paquetes siguen hacia su destino.

Figura 51

Ping entre host matriz y host sucursal 1 por medio de MPLS

```

HOST-MATRIZ> ping 192.168.32.2
84 bytes from 192.168.32.2 icmp_seq=1 ttl=61 time=7.769 ms
84 bytes from 192.168.32.2 icmp_seq=2 ttl=61 time=4.972 ms
84 bytes from 192.168.32.2 icmp_seq=3 ttl=61 time=9.338 ms
84 bytes from 192.168.32.2 icmp_seq=4 ttl=61 time=9.991 ms
84 bytes from 192.168.32.2 icmp_seq=5 ttl=61 time=22.326 ms

HOST-MATRIZ> tracer 192.168.32.2
trace to 192.168.32.2, 8 hops max, press Ctrl+C to stop
 1  192.168.31.1    4.932 ms  6.034 ms  4.148 ms
 2  172.16.31.2    5.697 ms  5.924 ms  4.722 ms
 3  172.16.32.1    8.753 ms  6.249 ms  7.862 ms

```

Fuente: Solar-Putty (4.0.0.47)

Si se desea utilizar una red de transporte diferente para enviar los mismos paquetes a la sucursal 1, la tecnología SD-WAN proporciona una ruta a través de la red de internet. Se creó un túnel Isec llamado “M-S1” para la conexión entre la matriz y sucursal 1 por medio de internet. De manera similar, se ejecuta un traceroute que muestra en la figura 52 todos los saltos realizados, los cuales corresponden a la ruta tomada por este medio. La dirección 192.168.0.108 que corresponde al túnel Isec.

Figura 52

Ping entre host matriz y host sucursal 1 por medio de tunel Isec

```

HOST-MATRIZ> ping 192.168.32.2
84 bytes from 192.168.32.2 icmp_seq=1 ttl=62 time=11.425 ms
84 bytes from 192.168.32.2 icmp_seq=2 ttl=62 time=17.259 ms
84 bytes from 192.168.32.2 icmp_seq=3 ttl=62 time=8.071 ms
84 bytes from 192.168.32.2 icmp_seq=4 ttl=62 time=10.036 ms
84 bytes from 192.168.32.2 icmp_seq=5 ttl=62 time=12.793 ms

HOST-MATRIZ> tracer 192.168.32.2
trace to 192.168.32.2, 8 hops max, press Ctrl+C to stop
 1  192.168.31.1    1.814 ms  1.714 ms  2.247 ms
 2  192.168.0.108  5.824 ms  5.170 ms  5.868 ms

```

Fuente: Solar-Putty (4.0.0.47)

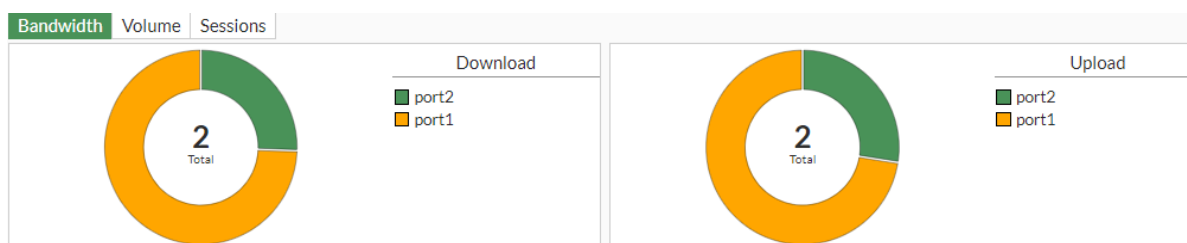
Por último, es posible observar cómo la red MPLS interactúa con los túneles IPsec o Internet, lo que significa que la SD-WAN Híbrida es capaz de soportar y controlar diferentes tipos de conexiones. En un entorno real, se requerirían las direcciones IP públicas proporcionadas por los proveedores de servicios de Internet en lugar de las direcciones privadas utilizadas en la emulación. El objetivo es comprender cómo la SD-WAN funciona como una red de múltiples transportes, ya que el intercambio entre direcciones públicas y privadas es sencillo.

4.3.3. Monitoreo uso de enlaces SD-WAN

La monitorización del uso de enlaces SD-WAN en un dispositivo FortiGate es esencial para garantizar el rendimiento y la eficiencia del tráfico en la red. Con la funcionalidad de SD-WAN, se pueden gestionar múltiples enlaces de conectividad, como líneas de Internet, líneas privadas y conexiones de banda ancha, y optimizar su uso para mejorar la experiencia del usuario y reducir los costos. En la figura 53 se observa la monitorización del uso de enlaces SD-WAN de la matriz a través de un panel de control unificado y amigable. Este panel proporciona una visión general del tráfico de los enlaces, que incluye información detallada sobre el ancho de banda utilizado, el volumen de datos transmitidos y el número de sesiones activas en cada enlace.

Figura 53

Monitoreo enlaces sd-wan de la matriz



Fuente: FortiOS v7.0.5

El ancho de banda utilizado muestra la cantidad de capacidad de red que está siendo aprovechada en tiempo real, permitiendo identificar si algún enlace está operando cerca de su

límite y si es necesario redirigir parte del tráfico a otros enlaces menos utilizados para evitar cuellos de botella.

El volumen de datos transmitidos representa la cantidad total de datos enviados y recibidos a través de cada enlace, lo que ayuda a entender la distribución del tráfico y posibles patrones de uso.

Por último, el número de sesiones activas indica la cantidad de conexiones de red establecidas en cada enlace en un momento dado. Esto puede ayudar a identificar aplicaciones o servicios que generan una gran cantidad de sesiones y que podrían estar afectando el rendimiento general de la red.

Además de proporcionar información en tiempo real, la monitorización del uso de enlaces SD-WAN en FortiGate también ofrece la posibilidad de generar informes históricos que permiten analizar tendencias y comportamientos a lo largo del tiempo. Con estos datos, los administradores de red pueden tomar decisiones informadas sobre cómo equilibrar la carga de tráfico en los enlaces, optimizar la configuración de SD-WAN y garantizar un rendimiento óptimo de la red en general.

4.3.4. Monitoreo calidad de enlaces SD-WAN

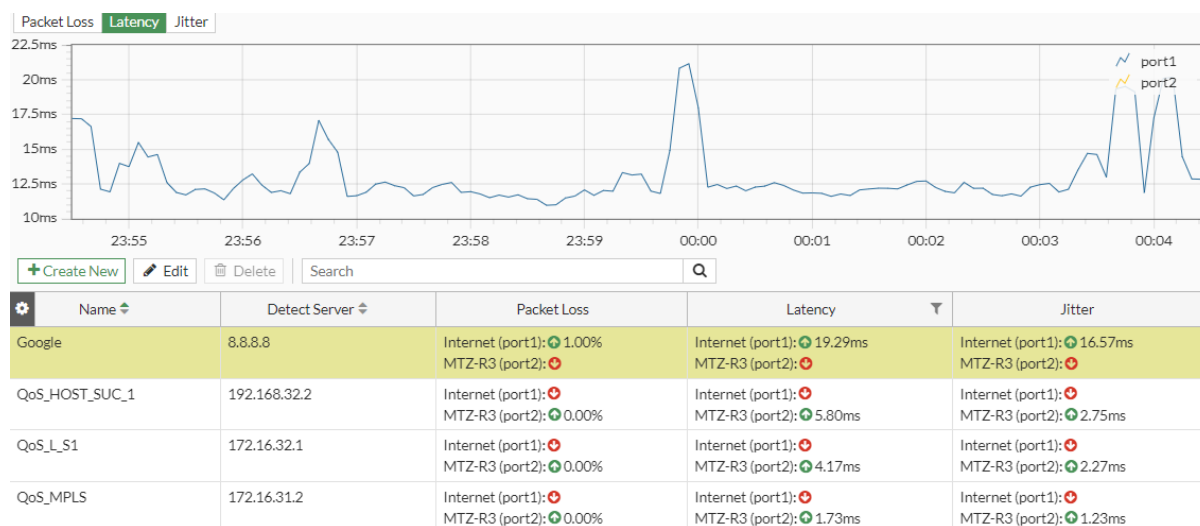
Esta sección se enfoca en llevar a cabo una monitorización inteligente de la Calidad de Servicio (QoS) en la SD-WAN mediante un análisis en tiempo real del rendimiento de los enlaces. Para lograr esto, se utilizó tres parámetros clave: la pérdida de paquetes, la latencia y el jitter, e incluso un Acuerdo de Nivel de Servicio (SLA). Esto brindó a la SD-WAN un mayor entendimiento de la condición de sus enlaces, lo que le permitió tomar decisiones informadas para seleccionar la ruta óptima y eficiente.

En la figura 54 se muestra la supervisión de los enlaces de la matriz. En esta representación gráfica se identifican tres destinos distintos: la sucursal 1, la sucursal 2 y la

conexión a Internet. Cada uno de estos destinos está asociado con los enlaces específicos que son utilizados por la matriz para alcanzarlos.

Figura 54

Monitoreo QoS enlaces sd-wan de la matriz



Fuente: FortiOS v7.0.5

En la visualización se puede apreciar que los enlaces "MPLS" e "Internet" se encuentran activos y habilitados para su uso. La gráfica muestra la evolución de la latencia a lo largo del tiempo, y se puede observar que el enlace "Internet" presenta un promedio de latencia de 19.29 ms.

En contraste, en la figura 55 se muestra un comando "ping" ejecutado en la interfaz de línea de comandos (CLI) hacia el host de la sucursal 1 utilizando. El propósito de este "ping" es verificar la precisión y efectividad del monitoreo realizado por FORTINET. En consecuencia, el promedio de latencia obtenido en la figura anterior debería ser cercano al promedio del "ping" realizado desde una computadora hacia la matriz.

Figura 55*Latencia del ping MTZ a L-SI*

```

MATRIZ # execute ping 192.168.32.2
PING 192.168.32.2 (192.168.32.2): 56 data bytes
64 bytes from 192.168.32.2: icmp_seq=0 ttl=62 time=6.1 ms
64 bytes from 192.168.32.2: icmp_seq=1 ttl=62 time=3.6 ms
64 bytes from 192.168.32.2: icmp_seq=2 ttl=62 time=3.8 ms
64 bytes from 192.168.32.2: icmp_seq=3 ttl=62 time=12.3 ms
64 bytes from 192.168.32.2: icmp_seq=4 ttl=62 time=13.8 ms

--- 192.168.32.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.6/7.9/13.8 ms

```

Fuente: FortiOS v7.0.5

El cálculo del promedio de los tiempos de latencia da como resultado un valor de 7.9 ms, el cual es cercano al valor expuesto en la figura 55 de 5.80 ms. Esto confirma que la monitorización está operando correctamente. Se sigue un enfoque similar con los otros enlaces y destinos, utilizando la latencia como parámetro clave, ya que las reglas de la SD-WAN se basan en esta métrica. No obstante, también es posible emplear otros parámetros como la pérdida de paquetes, el jitter o un SLA, en caso de estar disponible, tal como se ilustra en la figura 56.

Figura 56*Monitoreo en base a SLA*

The screenshot shows the 'Edit Performance SLA' configuration interface. The 'Name' is 'Google'. The 'Probe mode' is set to 'Active'. The 'Protocol' is 'Ping'. The 'Server' is '8.8.8.8'. The 'Participants' are 'All SD-WAN Members'. The 'SLA Target' section is highlighted with a red box and contains the following settings:

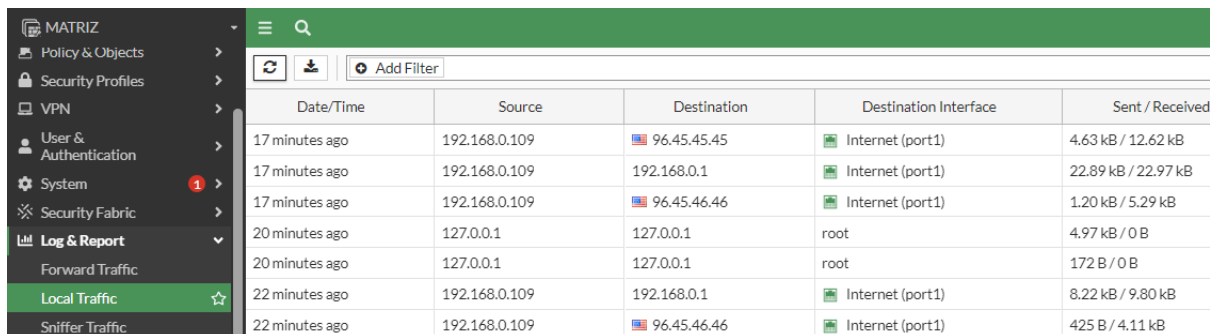
| SLA Target | Value | Unit |
|-----------------------|-------|------|
| Latency threshold | 20 | ms |
| Jitter threshold | 20 | ms |
| Packet Loss threshold | 5 | % |

Fuente: FortiOS v7.0.5

En conclusión, la SD-WAN proporciona un mecanismo de monitorización altamente eficiente que permite al administrador de red estar al tanto del estado de los enlaces en cualquier momento. Incluso, es posible verificar si se cumple el Acuerdo de Nivel de Servicio (SLA) establecido entre el cliente y el proveedor de servicios de Internet (ISP). Basándose en esta información sobre el estado de los enlaces, la SD-WAN toma decisiones de manera inteligente y automatizada, optimizando el enrutamiento del tráfico para garantizar un rendimiento óptimo y una experiencia de red mejorada.

4.3.5. Verificación de enrutamiento del tráfico SD-WAN

La verificación del tráfico de enrutamiento puede llevarse a cabo a través de dos métodos principales: el análisis de registros de tráfico y el uso de herramientas de captura de paquetes. Los registros de tráfico proporcionan información detallada sobre el flujo de datos a través de una red, registrando eventos, estadísticas y problemas potenciales. Estos registros permiten a los administradores de red identificar patrones de tráfico, diagnósticos de errores y optimizar el rendimiento general. Por otro lado, las herramientas de captura de paquetes, como Wireshark, permiten la observación en tiempo real y el análisis exhaustivo de cada paquete que circula en la red. Esto proporciona una visión detallada de la comunicación entre dispositivos, revelando información crucial sobre la ruta de enrutamiento, los protocolos utilizados y posibles problemas de congestión o seguridad. Ambos enfoques son complementarios y esencialmente brindan a los profesionales de redes herramientas valiosas para garantizar un enrutamiento eficiente y confiable en entornos de red. La figura 57 muestra el tráfico generado en el router SD-WAN de la matriz.

Figura 57*Monitoreo trafico local matriz*


| Date/Time | Source | Destination | Destination Interface | Sent / Received |
|----------------|---------------|-------------|-----------------------|---------------------|
| 17 minutes ago | 192.168.0.109 | 96.45.45.45 | Internet (port1) | 4.63 kB / 12.62 kB |
| 17 minutes ago | 192.168.0.109 | 192.168.0.1 | Internet (port1) | 22.89 kB / 22.97 kB |
| 17 minutes ago | 192.168.0.109 | 96.45.46.46 | Internet (port1) | 1.20 kB / 5.29 kB |
| 20 minutes ago | 127.0.0.1 | 127.0.0.1 | root | 4.97 kB / 0 B |
| 20 minutes ago | 127.0.0.1 | 127.0.0.1 | root | 172 B / 0 B |
| 22 minutes ago | 192.168.0.109 | 192.168.0.1 | Internet (port1) | 8.22 kB / 9.80 kB |
| 22 minutes ago | 192.168.0.109 | 96.45.46.46 | Internet (port1) | 425 B / 4.11 kB |

Fuente: FortiOS v7.0.5

En conclusión, el plan de migración de la red MPLS tradicional a una infraestructura SD-WAN ha resultado una transformación verdaderamente positiva ya que se ha demostrado una optimización significativa del tráfico, brindando una mayor agilidad y flexibilidad en la gestión de la red. La capacidad de aprovechar múltiples conexiones y utilizar rutas más eficientes mejoró la experiencia del usuario, garantizando una conectividad más rápida y confiable. Además, la disminución notable de la carga operativa en la administración de la red mediante una variedad de características y capacidades, donde, destacan la integración de funciones de seguridad avanzada lo que significa que las políticas de seguridad, como el firewall, prevención de intrusos y la protección contra malware, se puede gestionar de manera centralizada. Esta consolidación simplificó la administración y garantizó la seguridad de la red sin necesidad de desplegar dispositivos adicionales. La interfaz de gestión centralizada proporcionó una vista unificada de toda la red, donde se pudo configurar y gestionar políticas de tráfico, supervisar el rendimiento de la red y realizar actualizaciones de manera eficiente reduciendo la complejidad operativa. La automatización y la orquestación es otro punto positivo, al optimizar e implementar cambios de manera rápida y consistente, además de facilitar la coordinación de políticas y servicios en toda la infraestructura. Adicional, se pudo apreciar herramientas avanzadas de monitoreo y análisis de tráfico que permitió la visibilidad completa de la red posibilitando identificar y abordar proactivamente problemas de

rendimiento. Finalmente se pudo evidenciar la optimización de recursos ya que SD-WAN permitió la utilización eficiente de múltiples enlaces y caminos para el tráfico de red lo que permite dirigir el tráfico por las rutas más eficientes y disponibles, reduciendo latencia y mejorando la velocidad de aplicaciones. En resumen, la transición a SD-WAN no solo ha mejorado la eficiencia y la confiabilidad de la red, sino que también simplifico la administración de la red al proporcionar una plataforma integral que combina funciones de seguridad, gestión centralizada, automatización y visibilidad avanzada. Esta integración ayuda a administrar la red de manera más eficiente y responder de manera ágil las demandas cambiantes de la misma.

CONCLUSIONES

La ejecución de este proyecto se logró a través de la herramienta GNS3, la cual proporcionó una perspectiva realista en el diseño de red, presentando una simulación compleja y completa tanto en la red tradicional como en la red SD-WAN, permitiendo realizar pruebas de rendimiento y gestión que posibilitó obtener resultados adecuados, evidenciando de forma positiva las ventajas que tiene una infraestructura sobre la otra.

SD-WAN demostró ser una solución avanzada, adaptativa y escalable para las necesidades de un ISP, presentando una serie de beneficios tales como, eficiencia, flexibilidad, reducción de costos y seguridad, además de presentar una mejora notable en la calidad y velocidad de conexión.

La metodología de PMBOK fue de gran ayuda en la organización y ejecución del proyecto al permitir desarrollar la misma por medio de etapas, iniciando desde lo más elemental que es la creación de una base sólida de fuentes bibliográficas, para posteriormente proceder con la planificación del diseño de red donde se detalló los requerimientos que debe tener una red, así como también las etapas del plan de migración, la ejecución se centró en el desarrollo de la simulación de las redes, posteriormente, en la etapa de desempeño se realizó las pruebas de rendimiento y administración para finalizar con las conclusiones.

La red SD-WAN mostró tener ventajas significativas en la carga operativa de la red, presentando disminución de costos operativos gracias a la automatización y simplificación de configuraciones, así como también, la gestión centralizada y consolidación de funciones que simplifican la administración de la red.

SD-WAN demostró ser una solución robusta y confiable en comparación con la red tradicional, al presentar mejorías en la optimización del tráfico al permitir utilizar múltiples enlaces que, en caso de condiciones adversas, permite la continuidad del servicio mediante la diversificación de rutas y la capacidad de respuesta de fallos de manera automática.

La implementación de SD-WAN no solo representa una evolución en la gestión de redes, sino también un salto hacia la preparación para tecnologías emergentes. La arquitectura flexible y escalable de SD-WAN permite a las organizaciones adaptarse de manera ágil a las tendencias tecnológicas en constante cambio. Al proporcionar una infraestructura de red que puede evolucionar rápidamente, SD-WAN no solo satisface las necesidades actuales de conectividad y rendimiento, sino que también actúa como un cimiento sólido para la integración sin problemas de tecnologías emergentes, como la inteligencia artificial, el Internet de las cosas y la computación en la nube, impulsando así la innovación continua en el panorama empresarial.

RECOMENDACIONES

Antes de iniciar la migración, es fundamental llevar a cabo una evaluación exhaustiva de los requisitos de la organización. Esto implica identificar las aplicaciones críticas, el tráfico de red, la ubicación de los sitios y las necesidades de ancho de banda. Una comprensión sólida de estos factores garantizará una implementación exitosa de la SD-WAN que cumpla con las expectativas.

La elección del proveedor y la plataforma de SD-WAN es crítica. Se deben considerar factores como la flexibilidad, el soporte técnico, la interoperabilidad con la infraestructura existente y las capacidades de gestión centralizada. Realizar una evaluación exhaustiva de los proveedores y sus soluciones es esencial antes de tomar una decisión.

La SD-WAN permite una gestión más granular del tráfico. Se recomienda diseñar políticas de tráfico bien definidas para priorizar las aplicaciones críticas y asignar recursos de red de manera eficiente. Esto garantizará un rendimiento óptimo de las aplicaciones y una experiencia de usuario positiva.

En lugar de realizar una migración abrupta, se considera una implementación gradual. Esto implica iniciar con un conjunto de ubicaciones o sucursales piloto para evaluar y ajustar la configuración antes de ampliar la migración a toda la red. Esta estrategia reduce el riesgo de problemas inesperados.

Una vez que la SD-WAN esté en funcionamiento, es fundamental establecer un proceso de monitoreo constante. Esto permitirá detectar y abordar posibles problemas de rendimiento, así como optimizar la configuración a medida que cambien las necesidades de la red.

Hay que asegurar que el personal esté debidamente capacitado en la gestión y operación de la SD-WAN. Esto incluye comprender las políticas de tráfico, la resolución de problemas y la seguridad. Una fuerza laboral bien entrenada es esencial para aprovechar al máximo los beneficios de la SD-WAN.

En resumen, una migración exitosa de una red MPLS a una SD-WAN requiere una planificación meticulosa, una selección cuidadosa de proveedores y plataformas, una gestión eficiente del tráfico y una capacitación adecuada del personal. Además, la implementación gradual y el monitoreo continuo son prácticas recomendadas para garantizar un despliegue exitoso y un rendimiento óptimo de la red.

BIBLIOGRAFÍA

- 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/>
- Amazon. (2023). ¿Qué es la latencia de red? Amazon Web Services.
<https://aws.amazon.com/es/what-is/latency/>
- Arias, P. (2011). Diseño de una red LAN/WAN segura para el Tribunal Constitucional aplicando la metodología de 3 capas de CISCO. Pontificia Universidad Católica del Ecuador.
- aruba. (2022). ¿Qué es SD-WAN? Arubanetworks.Com.
<https://www.arubanetworks.com/es/faq/que-es-sd-wan/>
- Avance Digital. (2023). Tecnologías de acceso. Digitalización e Inteligencia Artificial.
<https://avancedigital.mineco.gob.es/banda-ancha/tecnologias/Paginas/tecnologias-acceso.aspx>
- BCM. (2023). Top 3 SD-WAN Architecture Types. Bcmone.Com.
<https://www.bcmone.com/blog/the-three-different-types-of-sd-wan/>
- CISCO. (2018). FUNDAMENTOS DE MPLS.
<https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKCQEA4/introducci%C3%B3n-a-mpls>
- CUAED. (2017). Administración de la Red. Unidad de Apoyo Para El Aprendizaje.
https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/931/mod_resource/content/4/contenido/index.html

- 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/>
- Forti One. (2023). 6 razones para elegir SD WAN Fortinet. Forti1.Com. <https://forti1.com/es/sd-wan-por-que-elegir-un-fortinet/>
- FORTINET. (2023a). Ciberseguridad, dondequiera que la necesite. Fortinet.Com. <https://www.fortinet.com/lat/corporate/about-us/about-us>
- FORTINET. (2023b). Fortimanager. FORTINET. https://docs.google.com/document/d/10Yq2iOC6Xumi819TDFJoJsyhtsER_asj/edit
- FORTINET. (2023c). Fortinet es nombrado un líder en el Cuadrante Mágico™ de Gartner® 2022 para SD-WAN. Fortinet.Com. <https://www.fortinet.com/lat/solutions/gartner-wan-edge>
- FORTINET. (2023d). Secure SD-WAN. Fortinet.Com. <https://www.fortinet.com/lat/products/sd-wan>
- FORTINET. (2023e). What Is SD-WAN Architecture? Fortinet. <https://www.fortinet.com/resources/cyberglossary/sd-wan-architecture>
- FS | community. (2022). SD-WAN vs MPLS: Ventajas y desventajas. <https://community.fs.com/es/blog/sd-wan-vs-mpls-pros-and-cons.html>
- GNS3. (2023). Primeros pasos con GNS3. Docs.Gns3.Com. <https://docs.gns3.com/docs/>
- Huidobro, J., & Millán, R. (2002). MPLS Multi Protocol Label. <https://www.ramonmillan.com/tutoriales/mpls.php#elementosredmpls>
- IDT. (2023). ¿Qué es el jitter? Causas típicas y formas de reducirlo. IDT EXPRESS. <https://www.idtexpress.com/es/blog/what-is-jitter-typical-causes-ways-to-reduce->

it/#:~:text=Jitter%20es%20una%20variaci%C3%B3n%20o,mide%20en%20mili segundos%20(ms).

Juniper Networks. (2020). SD-WAN: Todo lo que hay que saber. Juniper.Net.

<https://www.juniper.net/mx/es/research-topics/sd-wan-explained.html>

LANNER. (2020, April 30). La SD-WAN mitiga el reto del teletrabajo para asegurar la

continuidad comercial. La SD-WAN Mitiga El Reto Del Teletrabajo Para

Asegurar La Continuidad Comercial. [https://www.lanner-america.com/es/sin-](https://www.lanner-america.com/es/sin-categorizar/la-sd-wan-mitiga-el-reto-del-teletrabajo-para-asegurar-la-continuidad-comercial/)

[categorizar/la-sd-wan-mitiga-el-reto-del-teletrabajo-para-asegurar-la-](https://www.lanner-america.com/es/sin-categorizar/la-sd-wan-mitiga-el-reto-del-teletrabajo-para-asegurar-la-continuidad-comercial/)

[continuidad-comercial/](https://www.lanner-america.com/es/sin-categorizar/la-sd-wan-mitiga-el-reto-del-teletrabajo-para-asegurar-la-continuidad-comercial/)

Layots. (2022). SD-WAN over MPLS: Explained. Layots.Com. [https://layots.com/sd-](https://layots.com/sd-wan-over-mpls-explained/)

[wan-over-mpls-explained/](https://layots.com/sd-wan-over-mpls-explained/)

Lemus, J. (2020, February 19). Qué es Fortinet y cómo funciona. Vertical-Iberica.Com.

<https://vertical-iberica.com/que-es-fortinet-y-como-funciona/>

López, J. (2020). EMULACIÓN DE UNA RED SD-WAN (SOFTWARE-DEFINED WIDE AREA NETWORK) UTILIZANDO TECNOLOGÍA FORTINET Y EL SOFTWARE GNS3. ESCUELA POLITÉCNICA NACIONAL.

Machado, J., Ramos, A., & Cuéllar, J. (2014). Implementación de OpenFlow sobre

NetFPGA. Revista de Ingeniería y Región.

Maya, J. (2021). VENTAJAS Y DESVENTAJAS DEL PARADIGMA DE LAS

REDES DEFINIDAS POR SOFTWARE (SDN). Universidad Técnica de

Babahoyo.

Moncada, I. (2020). Labores de un administrador de telecomunicaciones y sus cambios

en época de pandemia. Universidad Piloto de Colombia.

Moreno Alayón Sandra Milena. (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.

- 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.
- ONF. (2023). SDN OVERVIEW. Opennetworking.Org.
<https://opennetworking.org/sdn-definition/>
- Palo Alto Networks. (2023). MPLS | ¿Qué es la conmutación de etiquetas multiprotocolo? PRISMA. <https://www.paloaltonetworks.com/cyberpedia/mpls-what-is-multiprotocol-label-switching>
- Parra, D. (2020). SD-WAN Vs MPLS: Los Pros, Los Contras. BiTS.
<https://www.bits.com.mx/sd-wan-vs-mpls/>
- Rejón, J. (2019, May 14). Simulador de red GNS3. Mundotelematico.Com.
<https://www.mundotelematico.com/simulador-de-red-gns3/>
- Smith, M. (2017). The 3 types of SD-WAN architecture. NETWORKWORLD.
<https://www.networkworld.com/article/3219653/the-3-types-of-sd-wan-architecture.html>
- SPTel. (2021). MPLS Advantages & Disadvantages: Explained in 5 Simple Steps.
<https://sptel.com/mpls-advantages-and-disadvantages>
- Tapia, J. (2022). TESTBED PARA EL ESTUDIO DE LA TECNOLOGÍA DE REDES DEFINIDAS POR SOFTWARE PARA LA CARRERA DE TELECOMUNICACIONES DE LA UNIVERSIDAD TÉCNICA DEL NORTE. Universidad Técnica del Norte.

- Technopedia. (2023). What is Access Networks & Its General Architecture?
Technopediastite. <https://www.technopediastite.com/2018/12/what-is-access-networks-its-general.html>
- TELDAT. (2021). SD-WAN y la revolución digital en tiempos del Covid-19. TELDAT Blog.
- Telectrónica. (2018, April 29). GNS3 Guía Introductoria: Características y Requerimientos Mínimos. Telectronika.Com.
<https://www.telectronika.com/articulos/ti/que-es-gns3/>
- Thomas, J. (2019, May 2). Las ventajas y desventajas de las WAN. Purple.
<https://purple.ai/es/blogs/las-ventajas-y-desventajas-de-las-wan/#:~:text=Al%20igual%20que%20con%20cualquier,y%20los%20problemas%20de%20mantenimiento.>
- Todos hacemos TIC. (2015, July 9). GNS3: SOFTWARE DE SIMULACIÓN DE REDES PARA LAS CERTIFICACIONES DE CISCO Y JUNIPER.
Diocesanos.Es. <https://diocesanos.es/blogs/equipotic/2015/07/09/gns3-software-de-simulacion-de-redes-para-las-certificaciones-de-cisco-y-juniper/>
- Valencia, B., & Santacruz, S. (2015). PROTOTIPO DE REDES IPV6 DEFINIDAS POR SOFTWARE MEDIANTE MININET. Universidad Católica de Pereira.
- Versa Networks. (2022). ¿Qué es la SD-WAN (WAN definida por el software)?
<https://versa-networks.com/es/sd-wan/>
- 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/>

ANEXOS

ANEXO A. Configuración de direccionamiento ip

```
[admin@SUCURSAL-1] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS           NETWORK             INTERFACE
0   172.16.32.1/30      172.16.32.0        ether1
1   192.168.32.1/24     192.168.32.0       ether2
2   10.5.33.1/30        10.5.33.0          ether3
```

Ilustración 1. Direccionamiento ip router (SUCURSAL-1)

```
[admin@SUCURSAL-2] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS           NETWORK             INTERFACE
0   172.16.33.2/30      172.16.33.0        ether3
1   192.168.33.1/24     192.168.33.0       ether1
2   10.5.33.1/30        10.5.33.0          ether2
```

Ilustración 2. Direccionamiento ip router (SUCURSAL-2)

```
[admin@R1] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS           NETWORK             INTERFACE
0   172.16.32.2/30      172.16.32.0        ether1
1   172.16.34.1/30      172.16.34.0        ether2
2   3.3.3.3/32          3.3.3.3             Loopback 30
```

Ilustración 3. Direccionamiento ip router (R1)

```
[admin@R2] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS           NETWORK             INTERFACE
0   172.16.34.2/30      172.16.34.0        ether1
1   172.16.35.1/30      172.16.35.0        ether2
2   172.16.36.1/30      172.16.36.0        ether3
3   2.2.2.2/32          2.2.2.2             Loopback 20
```

Ilustración 4. Direccionamiento ip router (R2)

```
[admin@R3] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS           NETWORK             INTERFACE
0   172.16.31.2/30      172.16.31.0        ether3
1   172.16.35.2/30      172.16.35.0        ether1
2   172.16.37.2/30      172.16.37.0        ether2
3   1.1.1.1/32          1.1.1.1             Loopback 10
```

Ilustración 5. Direccionamiento ip router (R3)

```
[admin@R4] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK          INTERFACE
0   172.16.39.2/30     172.16.39.0     ether1
1   172.16.33.1/30     172.16.33.0     ether2
2   6.6.6.6/32         6.6.6.6         Loopback 60
```

Ilustración 6. Direccionamiento ip router (R4)

```
[admin@R5] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK          INTERFACE
0   172.16.37.1/30     172.16.37.0     ether2
1   172.16.38.2/30     172.16.38.0     ether1
2   172.16.39.1/30     172.16.39.0     ether3
3   5.5.5.5/32         5.5.5.5         Loopback 50
```

Ilustración 7. Direccionamiento ip router (R5)

```
[admin@R6] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK          INTERFACE
0   172.16.36.2/30     172.16.36.0     ether1
1   172.16.38.1/30     172.16.38.0     ether2
2   4.4.4.4/32         4.4.4.4         Loopback 40
```

Ilustración 8. Direccionamiento ip router (R6)

ANEXO B. Configuración OSPF y MPLS

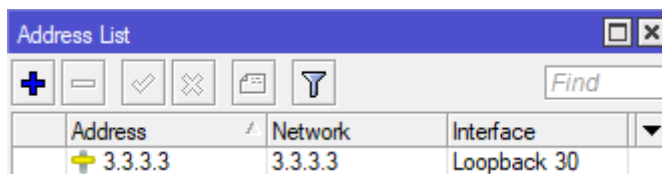


Ilustración 9. Configuración loopback (R1)

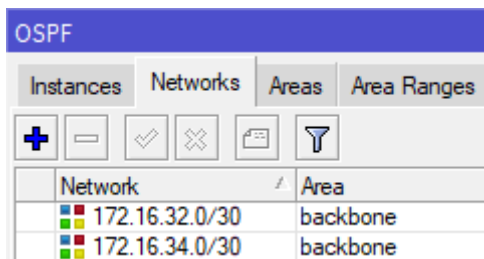


Ilustración 10. Configuración OSPF(R1)

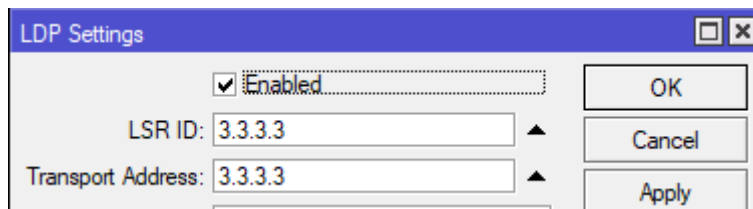


Ilustración 11. Configuración LDP (R1)

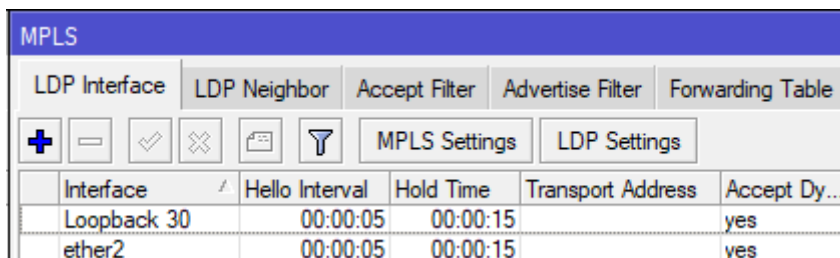


Ilustración 12. Interfaz LDP (R1)

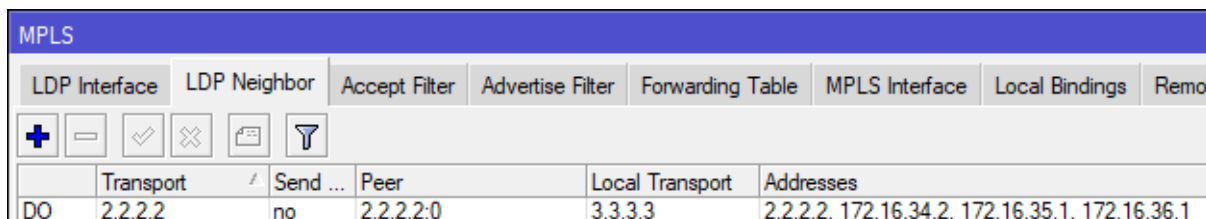


Ilustración 13. LDP Neighbor (R1)

| Address | Network | Interface |
|---------|---------|-------------|
| 2.2.2.2 | 2.2.2.2 | Loopback 20 |

Ilustración 14. Configuración loopback (R2)

| Network | Area |
|----------------|----------|
| 172.16.34.0/30 | backbone |
| 172.16.35.0/30 | backbone |
| 172.16.36.0/30 | backbone |

Ilustración 15. Configuración OSPF(R2)

Enabled
 LSR ID: 2.2.2.2
 Transport Address: 2.2.2.2

Ilustración 16. Configuración LDP (R2)

| Interface | Hello Interval | Hold Time | Transport Address | Accept Dy... |
|-------------|----------------|-----------|-------------------|--------------|
| Loopback 20 | 00:00:05 | 00:00:15 | | yes |
| ether1 | 00:00:05 | 00:00:15 | | yes |
| ether2 | 00:00:05 | 00:00:15 | | yes |
| ether3 | 00:00:05 | 00:00:15 | | yes |

Ilustración 17. Interfaz LDP (R2)

| Transport | Send ... | Peer | Local Transport | Addresses |
|------------|----------|-----------|-----------------|--|
| DO 1.1.1.1 | no | 1.1.1.1:0 | 2.2.2.2 | 1.1.1.1, 172.16.31.2, 172.16.35.2, 172.16.37.2 |
| DO 3.3.3.3 | no | 3.3.3.3:0 | 2.2.2.2 | 3.3.3.3, 172.16.32.2, 172.16.34.1 |
| DO 4.4.4.4 | no | 4.4.4.4:0 | 2.2.2.2 | 4.4.4.4, 172.16.36.2, 172.16.38.1 |

Ilustración 18. LDP Neighbor (R2)

| Address | Network | Interface |
|---------|---------|-------------|
| 6.6.6.6 | 6.6.6.6 | Loopback 60 |

Ilustración 19. Configuración loopback (R4)

| Network | Area |
|----------------|----------|
| 172.16.39.0/30 | backbone |

Ilustración 20. Configuración OSPF(R4)

Enabled
 LSR ID: 6.6.6.6
 Transport Address: 6.6.6.6

Ilustración 21. Configuración LDP (R4)

| Interface | Hello Interval | Hold Time | Transport Address | Accept Dy... |
|-------------|----------------|-----------|-------------------|--------------|
| Loopback 60 | 00:00:05 | 00:00:15 | | yes |
| ether1 | 00:00:05 | 00:00:15 | | yes |

Ilustración 22. Interfaz LDP (R4)

| Transport | Send ... | Peer | Local Transport | Addresses |
|------------|----------|-----------|-----------------|--|
| DO 5.5.5.5 | no | 5.5.5.5:0 | 6.6.6.6 | 5.5.5.5, 172.16.37.1, 172.16.38.2, 172.16.39.1 |

Ilustración 23. LDP Neighbor (R4)

| Address | Network | Interface |
|---------|---------|-------------|
| 5.5.5.5 | 5.5.5.5 | Loopback 50 |

Ilustración 24. Configuración loopback (R5)

| Network | Area |
|----------------|----------|
| 172.16.37.0/30 | backbone |
| 172.16.38.0/30 | backbone |
| 172.16.39.0/30 | backbone |

Ilustración 25. Configuración OSPF(R5)

Enabled
 LSR ID: 5.5.5.5
 Transport Address: 5.5.5.5

Ilustración 26. Configuración LDP (R5)

| Interface | Hello Interval | Hold Time | Transport Address | Accept Dy... |
|-------------|----------------|-----------|-------------------|--------------|
| Loopback 50 | 00:00:05 | 00:00:15 | | yes |
| ether1 | 00:00:05 | 00:00:15 | | yes |
| ether2 | 00:00:05 | 00:00:15 | | yes |
| ether3 | 00:00:05 | 00:00:15 | | yes |

Ilustración 27. Interfaz LDP (R5)

| Transport | Send ... | Peer | Local Transport | Addresses |
|------------|----------|-----------|-----------------|--|
| DO 1.1.1.1 | no | 1.1.1.1:0 | 5.5.5.5 | 1.1.1.1, 172.16.31.2, 172.16.35.2, 172.16.37.2 |
| DO 4.4.4.4 | no | 4.4.4.4:0 | 5.5.5.5 | 4.4.4.4, 172.16.36.2, 172.16.38.1 |
| DO 6.6.6.6 | no | 6.6.6.6:0 | 5.5.5.5 | 6.6.6.6, 172.16.33.1, 172.16.39.2 |

Ilustración 28. LDP Neighbor (R5)

| Address | Network | Interface |
|---------|---------|-------------|
| 4.4.4.4 | 4.4.4.4 | Loopback 40 |

Ilustración 29. Configuración loopback (R6)

| Network | Area |
|----------------|----------|
| 172.16.36.0/30 | backbone |
| 172.16.38.0/30 | backbone |

Ilustración 30. Configuración OSPF(R6)

Enabled
 LSR ID: 4.4.4.4
 Transport Address: 4.4.4.4

OK Cancel Apply

Ilustración 31. Configuración LDP (R6)

| Interface | Hello Interval | Hold Time | Transport Address | Accept Dy... |
|-------------|----------------|-----------|-------------------|--------------|
| Loopback 40 | 00:00:05 | 00:00:15 | | yes |
| ether1 | 00:00:05 | 00:00:15 | | yes |
| ether2 | 00:00:05 | 00:00:15 | | yes |

Ilustración 32. Interfaz LDP (R6)

| Transport | Send ... | Peer | Local Transport | Addresses |
|------------|----------|-----------|-----------------|--|
| DO 2.2.2.2 | no | 2.2.2.2:0 | 4.4.4.4 | 2.2.2.2, 172.16.34.2, 172.16.35.1, 172.16.36.1 |
| DO 5.5.5.5 | no | 5.5.5.5:0 | 4.4.4.4 | 5.5.5.5, 172.16.37.1, 172.16.38.2, 172.16.39.1 |

Ilustración 33. LDP Neighbor (R6)

ANEXO C. Configuración miembros SD-WAN de la sucursal 1 y 2.

The screenshot displays the configuration for an SD-WAN member in Sucursal-1. The interface includes a sidebar with navigation options and a main configuration area. The configuration details are as follows:

| Interfaces | Gateway | Cost |
|------------------|-------------|------|
| virtual-wan-link | | |
| S1-MPLS (port2) | 172.16.32.1 | 0 |

Ilustración 34. Configuración miembros SD-WAN sucursal-1

The screenshot displays the configuration for an SD-WAN member in Sucursal-2. The interface includes a sidebar with navigation options and a main configuration area. The configuration details are as follows:

| Interfaces | Gateway | Cost |
|------------------|-------------|------|
| virtual-wan-link | | |
| S2-MPLS (port2) | 172.16.33.2 | 0 |

Ilustración 35. Configuración miembros SD-WAN sucursal-2

ANEXO D. Topología completa de red SD-WAN.

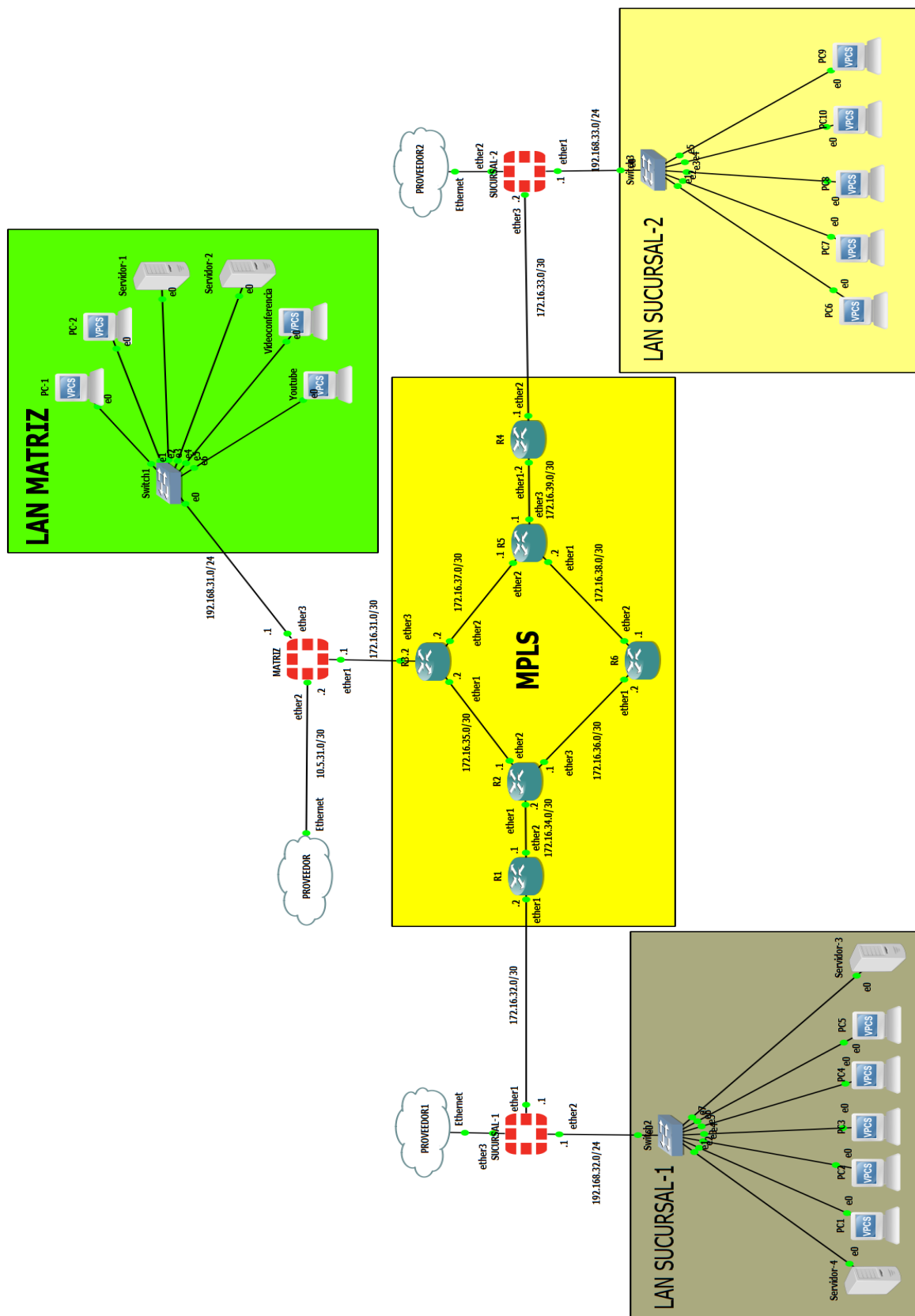


Ilustración 36. Topología completa red SD-WAN