Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Maestría en Telecomunicaciones

Comparativa de la calidad de servicio en redes de datos: MPLS vs. SD-WAN.

Trabajo de Titulación previa a la obtención del título de Magíster en Telecomunicaciones

AUTOR:

Ing. Diego Enrique Chala Folleco

DIRECTOR:

Ing. Marco Augusto Suing Ochoa, Mg. Sc.

Loja – Ecuador

2024

Certificación

Loja, 14 de agosto de 2024

Ing. Marco Augusto Suing Ochoa Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del trabajo de Investigación: **Comparativa de la Calidad de Servicio en Redes de Datos: MPLS vs. SD-WAN** de autoría del estudiante **Diego Enrique Chala Folleco** previo a la obtención del título de **Magíster en Telecomunicaciones**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Firmado electrónicamente por:
MARCO AUGUSTO SUING OCHOA

Ing. Marco Augusto Suing Ochoa Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

Autoría

Yo, **Diego Enrique Chala Folleco**, declaro ser autor del trabajo de titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido de este. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación del trabajo de titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

DIEGO ENRIQUE CHALA FOLLECO

Firmado digitalmente por DIEGO ENRIQUE CHALA FOLLECO
Fecha: 2024.08.16 09:13:03 -05'00'

Firma:

Autor: Diego Enrique Chala Folleco

Cédula de Identidad: 1715755474

Fecha: 14 de agosto 2024.

Correo electrónico: diego.chala@unl.edu.ec; diegochala1@hotmail.com

Teléfono: 0961294125

Carta de autorización por parte del autor para la consulta, reproducción parcial o total y /o publicación electrónica del texto completo del de trabajo de titulación.

Yo, **Diego Enrique Chala Folleco**, declaro ser autor del trabajo de Titulación denominado**: Comparativa de la Calidad de Servicio en Redes de Datos: MPLS vs. SD-WAN**, como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, suscribo, en la ciudad de Loja, a los catorce días del mes de agosto del de dos mil veinticuatro.

DIEGO ENRIQUE CHALA FOLLECO

Firmado digitalmente por DIEGO ENRIQUE CHALA FOLLECO
Fecha: 2024.08.16 09:13:33 -05'00'

Firma:

Autor: Diego Enrique Chala Folleco

Cédula: 1715755474

Dirección: Av. Maldonado e 3-44 y Joaquin Gutierrez Quito-Ecuador

Correo Electrónico: diego.chala@unl.edu.ec; diegochala1@hotmail.com

Teléfono: 0961294125

DATOS COMPLEMENTARIOS:

Director de trabajo de Titulación : Ing. Marco Augusto Suing Ochoa Mg. Sc.

Dedicatoria

En primer lugar, a Dios Todopoderoso, fuente de mi fortaleza y guía en cada paso de mi camino.

A mi Madre Amada, Folleco, por su amor incondicional y apoyo constante, y a Blanca Caviedes, que desde el cielo me da la fuerza necesaria para seguir adelante.

A mi querida esposa Marjorie y a mis tres hijos, quienes son mi razón de ser y mi mayor inspiración. Sin su amor y apoyo, no habría podido lograr todo lo que hoy celebro.

Quiero rendir un homenaje especial a las tres personas que he perdido este año y que siempre vivirán en mi corazón: Mi hermano Leo y mis tíos Mike y Chevy, aunque ya no estén físicamente conmigo, su recuerdo y su legado me impulsan a continuar con determinación y esperanza.

Diego Enrique Chala Folleco

Agradecimiento

Mi profundo agradecimiento a la Universidad Nacional de Loja, a la Facultada de Energía, las Industrias y los Recursos Naturales no Renovables, a todos los profesores quienes con las enseñanzas de sus conocimientos han hecho posible mi crecimiento profesional, gracias a cada uno de ustedes por su dedicación, apoyo y amistad.

Expreso mi más sincero agradecimiento al Ing. Marco Augusto Suing Ochoa Mg. Sc., por su dedicación, enseñanza y acertados consejos que ha permitido el desarrollo y exitosa culminación del presente trabajo de investigación.

Finalmente agradezco el apoyo de mis familiares, amigos y compañeros de maestría, quienes en el transcurso de estos estudios han contribuido con conocimientos, colaboración y su sincera amistad.

Diego Enrique Chala Folleco

Índice de Contenidos

Índice de Tablas:

Índice de Figuras

Índice de Anexos:

1. Título

Comparativa de la calidad de servicio en redes de datos: MPLS vs. SD-WAN

2. Resumen

La transformación del entorno digital ha puesto un enfoque particular en la administración de la Calidad de Experiencia (QoE) en redes de datos, sin lugar a duda una parte muy importante en el desempeño empresarial, hoy en día el desarrollo de Multiprotocol Label Switching (MPLS) y Software-Defined Wide Area Network (SD-WAN) se concentra en aspectos como escalabilidad, arquitectura, funcionalidad y sobre todo costos.

De forma muy específica MPLS prioriza el tráfico crítico a través de la etiquetación de paquetes y rutas, con su inflexibilidad los costos asociados pueden limitar su capacidad de adaptación, en cambio SD-WAN mejora la entrega de servicios reduciendo los costos mediante flexibilidad y gestión dinámica del tráfico gracias a la utilización de múltiples enlaces de red su arquitectura basada en software.

Teniendo en cuenta que ambas tecnologías se ocupan del ancho de banda y la gestión de recursos, hay una falta de conocimiento en su aplicación comparativa y práctica en ambientes empresariales reales donde destaca la escasez de estudios exhaustivos sobre adaptabilidad y eficacia, esto genera incertidumbre respecto al desempeño en entornos dinámicos apuntando a la conectividad con la nube y comunicación entre sucursales.

Para sustentar esta falta de información, importante y necesario realizar una investigación que evalúe su rendimiento en situaciones reales y analizar una implementación de QoS en cada una de las tecnologías en diversos escenarios ya sean simulados o en ambientes reales empresariales.

La pregunta fundamental consiste en identificar la tecnología más efectiva para implementar QoS en redes de datos: ¿MPLS o SD-WAN?.

Palabras clave: redes de datos, MPLS, SD-WAN, Adaptabilidad, Tráfico.

Abstract

The transformation of the digital environment certainly placed a particular focus on the management of Quality of Experience (QoE) in data networks, a very important part of business performance. Nowadays, the development of Multiprotocol Label Switching (MPLS) and Software-Defined Wide Area Network (SD-WAN) focuses on aspects such as scalability, architecture, functionality and, above all, costs.

Specifically, MPLS prioritizes critical traffic through packet and route labeling, but its inflexibility and associated costs can limit its adaptability, while SD-WAN improves service delivery by reducing costs through flexibility and dynamic traffic management using multiple network links and its software-based architecture.

Considering that both technologies deal with bandwidth and resource management; there is a lack of knowledge in their comparative and practical application in real business environments where the scarcity of exhaustive studies on adaptability and efficiency stands out; this generates uncertainty regarding performance in dynamic environments aiming at cloud connectivity and inter-branch communication.

To support this lack of information, it is important and necessary to conduct research to evaluate their performance in real situations, and to analyze a QoS implementation in each of the technologies in various scenarios, either simulated or in real business environments. The fundamental question is to identify the most effective technology for implementing QoS in data networks: MPLS or SD-WAN

Keywords: Data networks, MPLS, SD-WAN, Adaptability, Traffic.

3. Introducción

Hoy en día la conectividad y el intercambio de información son una parte esencial en el funcionamiento de las entidades, una decisión entre tecnologías como MPLS y SD-WAN genera un efecto directo en la calidad de servicio, eficacia y especialmente en la experiencia del usuario.

Generar un análisis es muy importante, debido a las actuales demandas de usuarios y organizaciones en cuanto al desempeño de la red y la velocidad de transformación tecnológica. Este estudio promoverá el progreso del conocimiento al realizar una evaluación comparativa de dos tecnologías, cubriendo áreas donde falta información y ofreciendo perspectivas valiosas sobre la elección estratégica entre MPLS y SD-WAN.

La contribución de este análisis ayuda al progreso del conocimiento centrándose en la creación de una base de datos sustancial sobre las mejores prácticas de cada tecnología también en las capacidades y restricciones, esto no solo será útil para los expertos en administración de redes o en tecnología de la información, sino muy importante para las personas encargadas de tomar decisiones en organizaciones que buscan mejorar sus infraestructuras de transmisión de datos.

El análisis exhaustivo de cómo MPLS y SD-WAN enfrentan los desafíos específicos relacionados con la gestión de la calidad de servicio en redes de datos, identificarán los puntos fuertes y las limitaciones en cada tecnología, esto permitirá tomar decisiones fundamentadas para solventar necesidades y superar obstáculos específicos.

Este análisis está en consonancia con el impulso para la eficacia en la administración tecnológica, uno de los objetivos es incentivar el crecimiento económico y la competitividad, también es importante respaldar las políticas gubernamentales e institucionales que fomentan la innovación tecnológica y mejoran la calidad de servicio.

Para la adecuada implementación en este análisis, previamente se han establecido tres objetivos específicos, detallados a continuación:

Comparación de Arquitectura y Funcionalidad: Examinar y verificar detalladamente cómo MPLS y SD-WAN manejan la calidad de servicio con la clasificación y priorización de tráfico, control y garantía de entrega de datos de manera confiable.

Evaluación de Costos y Escalabilidad: Compara los costos iniciales y a largo plazo entre MPLS y SD-WAN, y analiza cómo cada una de estas tecnologías puede crecer junto a tu negocio.

- **Pruebas de Rendimiento y Casos de Uso:** Se corren pruebas de rendimiento en un entorno simulado con herramientas y aplicaciones específicas con las cuales se puede analizar el caso de uso de conexión entre oficinas o el acceso a servicios en la nube, ayudándonos a encontrar los puntos claves y las limitaciones de cada tecnología en situaciones reales.

Objetivos

Objetivo General

El objetivo principal de este proyecto de investigación es realizar un análisis comparativo de dos tecnologías importantes en el manejo de la calidad de servicio en redes de datos, es el caso de: Multiprotocol Label Switching y Software-Defined Wide Area Network, teniendo en cuenta la QoS como un factor fundamental, debido a que se encarga de garantizar el funcionamiento correcto de las aplicaciones y servicios de red y ambas tecnologías buscan cumplir dicho objetivo dándole una solución diferente.

Objetivos Específicos:

- **Comparación de Arquitectura y Funcionalidad**: Analizar y comparar en detalle cómo MPLS y SD-WAN gestionan la QoS en términos de clasificación y priorización de tráfico, gestión de congestión y entrega.
- **Evaluación de Costos y Escalabilidad:** Evaluar y comparar los costos iniciales y operativos a largo plazo de la implementación de MPLS y SD-WAN, así como la capacidad de escalabilidad de ambas soluciones.
- **Pruebas de Rendimiento y Casos de Uso:** Realizar pruebas de rendimiento en un entorno simulado y analizar casos de uso específicos, como conectividad a la nube e interconexión de sucursales, para identificar fortalezas y debilidades de cada tecnología en escenarios prácticos.

4. Marco teórico

4.1. Contexto de Investigación.

El crecimiento masivo de Internet define al protocolo IP (Protocolo de Internet) como la base de las redes de telecomunicaciones actuales, transportando más del 80% del tráfico total, con una versión principal de IP, conocida como IPv4 y definida en la RFC 791, está en uso desde 1980, este protocolo está ubicado en la capa de red (Capa 3 OSI), genera los procedimientos en la distribución y enrutamiento de paquetes en redes de manera no confiable y sin conexión, está orientado exclusivamente hacia la conexión y la transferencia de datos y suele combinarse con TCP (Protocolo de Control de Transmisión) (Capa 4 OSI) para garantizar la entrega de paquetes (Black, Uyless D., 2000).

Desde el año 1995 hay un aumento con las expectativas de los clientes con respecto a los ISP (Proveedores de Servicios de Internet) para la necesidad de aplicaciones multimedia de mucha demanda de ancho de banda y una calidad de servicio (QoS) asegurada, esto llevó a la implementación de ATM (Modo de Transferencia Asincrónica) en la capa de enlace (Capa 2 OSI) de sus redes (Fernández, 2014).

El modelo de IP sobre ATM fue suficiente para satisfacer los requisitos de nuevas aplicaciones utilizando un enrutamiento de nivel 3 de los router en la red de acceso, para aumentar el ancho de banda y el rendimiento aprovechando la alta velocidad de los switches de capa 2 con circuitos virtuales permanentes ATM en la red principal, esta arquitectura presentaba ciertas limitaciones, como dificultad de operación e integración con una red basada en dos tecnologías completamente diferentes, debido a la aparición de switches IP y ATM en las redes principales, y la mayor capacidad de transmisión ofrecida por SDH/SONET (Jerarquía Digital Sincrónica / Red Óptica Sincrónica) y DWDM (Multiplexación por División de Longitud de Onda Densa) en comparación con ATM (Fernández, 2014).

En 1996, se generan nuevas soluciones para conmutación de nivel 2 concentradas en el núcleo de Internet, integraban la conmutación ATM con el enrutamiento IP, especialmente Aggregate Route-Based IP Switching de IBM o Tag Switching de Cisco, algunas de estas tecnologías compartían la característica para adoptar el software de control de un router IP, unirlo con el

rendimiento y reenvío con cambio de etiqueta de un switch ATM para crear un router extremadamente rápido y eficaz en términos de costos (Black, Uyless D., 2000), con la integración en esta arquitectura más profunda, y se utilizaban protocolos IP propietarios para distribuir y asignar los identificadores de conexión de ATM como etiquetas; sin embargo, estos protocolos no son interoperables y requerían infraestructura ATM (Black, 2001).

En 1997, se estableció el grupo de trabajo MPLS (Conmutación de Etiquetas de Multiprotocolo) por el IETF (Fuerza de Trabajo de Internet) al elaborar un estándar que unifica soluciones de conmutación de nivel 2, dando como resultado con la definición del estándar conocido como MPLS en 1998, el cual fue registrado en la RFC 3031, de esta forma la red MPLS proporciona los beneficios de la ingeniería de tráfico del modelo de IP sobre ATM, también una operación y diseño de red más sencillos y una mayor escalabilidad (Tejedor, 2012).

MPLS está diseñado para operar sobre cualquier tecnología en el nivel de enlace esto la diferencia de muchas soluciones patentadas, simplificando la migración a las redes ópticas de próxima generación basadas en infraestructuras SDH/SONET y DWDM.

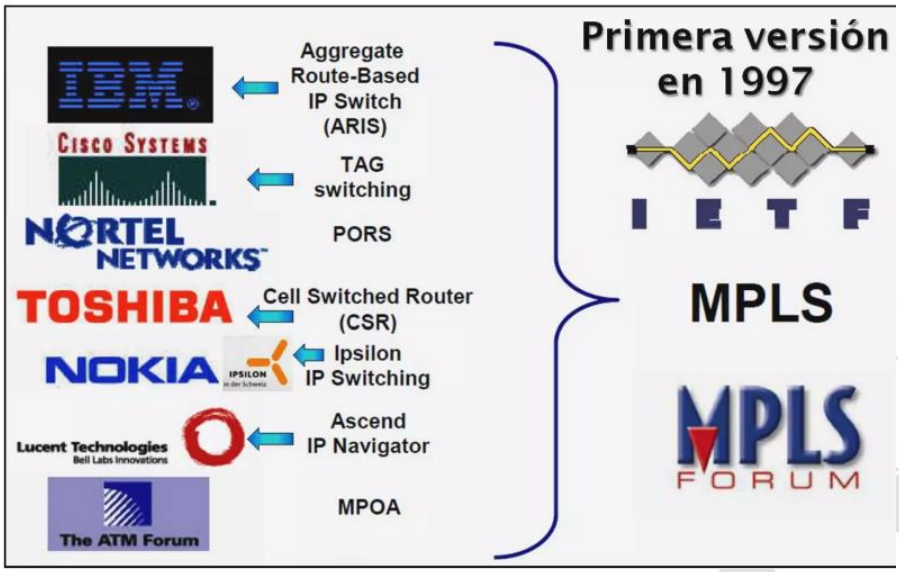

Figura 1 Origen de la red MPLS(Edison Coímbra, 2017)

4.1.1. ¿Qué es una red MPLS?

Una red de infraestructura MPLS (Multiprotocol Label Switching), está determinada mediante una tecnología de comunicación para garantizar conectividad y seguridad en la transmisión de

datos desde y hacia diferentes ubicaciones al ser como una Red Privada Virtual (VPN) eficiente y confiable, para ser empleada en el sector de las telecomunicaciones.

La MPLS no constituye un servicio en sí mismo, sino una técnica de transferencia de datos capaz de facilitar diversos servicios en telecomunicaciones, desde una VPN IP hasta una simple Internet Metropolitana, su aplicabilidad se destaca especialmente en servicios de redes de área extensa (WAN) y soluciones de privacidad como las VPN.

El núcleo de la MPLS es la conmutación de etiquetas multiprotocolo, esto es importante para la transferencia de datos con distintas etiquetas ya que se asegura la agrupación de varios tipos de datos transmitidos a través de una misma red, y facilitar el envío de paquetes de información (Citelia, 2021).

En el marco de las redes de comunicación, las etiquetas por conmutación de etiquetas multiprotocolo (MPLS) son un enfoque avanzado que opera en dos niveles fundamentales: la capa física y la transmisión de datos.

Desde el punto de vista físico, la red MPLS se basa en principios computacionales que se apoyan en teorías matemáticas para transformar la información de manera eficiente y confiable.

Al adentrarnos en el análisis del funcionamiento de una red MPLS, es esencial explorar cómo esta tecnología conecta dos sistemas de datos que pueden encontrarse en ubicaciones geográficas diferentes donde lo más importante es comprender minuciosamente cómo la capa de transmisión de datos facilita la transferencia segura y fluida de información desde su punto de origen hasta su destino final mediante un proceso de dividir la información en paquetes de datos que pueden contener una variedad de tipos de datos, como voz, texto o video, también se establecen rutas óptimas para estos paquetes, asegurando así su entrega eficiente y oportuna (Valdivia & Peña, s. f.).

En el ámbito de la transmisión de datos en una red MPLS, se utilizan dos enfoques principales: circuitos virtuales y datagramas como mecanismos que garantizan un intercambio preciso y confiable de paquetes de datos a lo largo de la red, contribuyendo a una comunicación fluida y sin problemas entre los dispositivos conectados (O. Ergun, s. f)

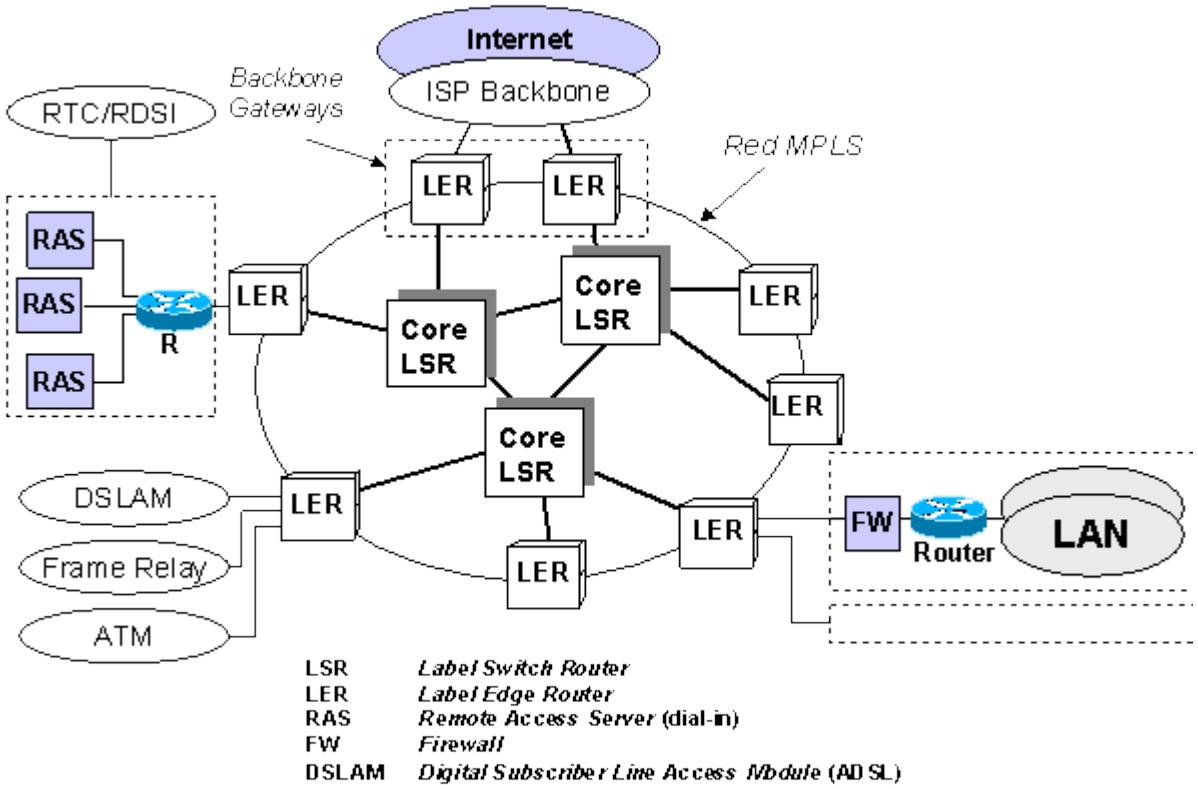

Figura 2 Diagrama de funcionamiento red MPLS (Ramón Millán, 2022)

Los datagramas permiten dirigir cada paquete de información de manera independiente, garantizando mayor velocidad en comparación con otros sistemas donde el origen y el destino deben comunicarse previamente, ralentizando el proceso.

Los datagramas y los circuitos virtuales son elementos clave en el funcionamiento de MPLS. Los datagramas permiten dirigir cada paquete de información de manera independiente, mejorando la velocidad de transmisión(Valdivia & Peña, s. f.).

4.1.2. ¿Cómo funciona una red MPLS?

Una infraestructura de red MPLS utiliza routers con etiquetas detalladas específicamente para cada tipo de datos, y se establece la posibilidad de una transferencia completa de información a lo largo de una ruta de baja latencia y alta velocidad (Citelia, 2021).

Cada router en la red establece una tabla señalando el manejo de paquetes de un tipo específico de FEC (Forwarding Equivalence Class). Cuando el paquete ingresa en la red, no se analiza el encabezado, pero si se emplea la etiqueta de índice en la tabla con una nueva FEC con ese paquete.

En una red MPLS sus etiquetas añaden información adicional a los paquetes, esta información es un dato añadido a lo que cada dispositivo posee para habilitar la gestión de paquetes de manera uniforme, asignando rutas de baja latencia para el tráfico en tiempo real ya sea telefonía o streaming, muy difícil seria realizarlo en el enrutamiento tradicional. (Chiradeep, 2022)

MPLS se sitúa en la capa "2,5" del modelo OSI, justo encima de la capa de enlace de datos (capa 2) y debajo de la capa de red (capa 3)(Ramón Millan, 2022)

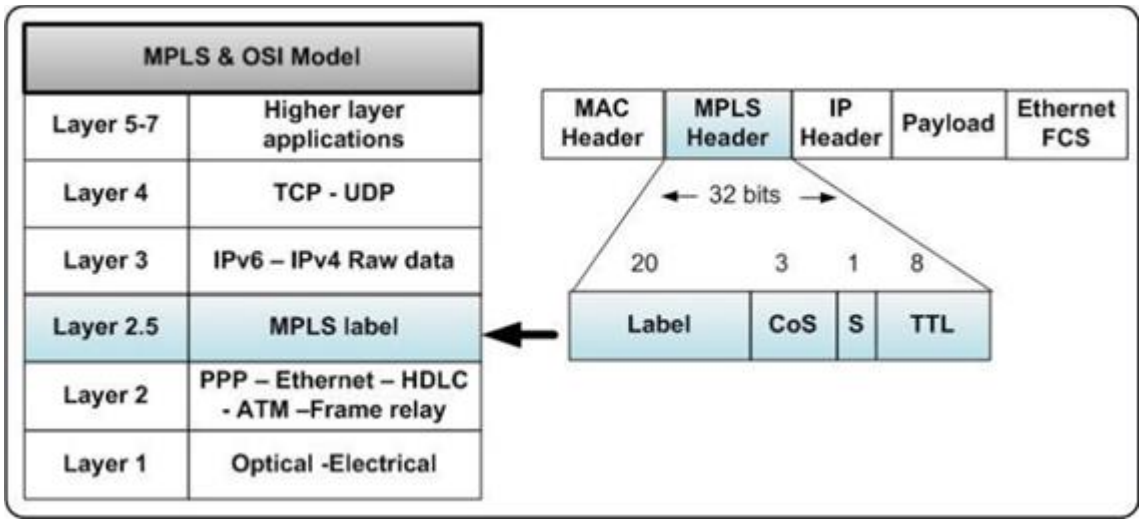

Figura 3 Ubicación de la MPLS en modelo OSI (Angel .H 2018)

En la MPLS no se verifica el encabezado IP lo importante es enviar el paquete en base al valor de la etiqueta (Barberá, 2007)

Un router IP verifica el encabezado y lo compara con la tabla de enrutamiento y asi define el siguiente salto este análisis de paquetes al realizar un recorrido más extenso genera mayor procesamiento y uso de memoria de los dispositivos (Morales, 2007).

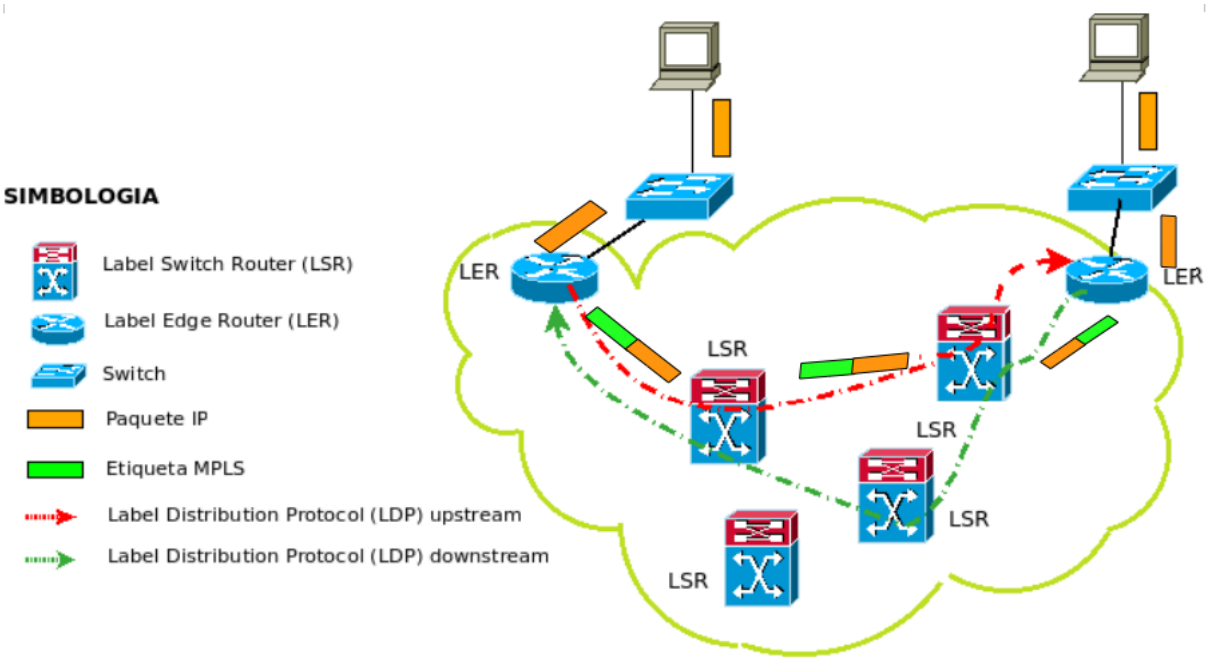

Figura 4 Esquema de distribución de etiquetas MPLS (Ramón Millán, 2022)

4.1.3. Beneficios y Limitaciones al tener una red MPLS

4.1.3.1. Beneficios

- La red puede recibir paquetes mediante un punto de entrada especifico o desde un dispositivo en este caso un router sin tener MPLS configurado.
- La transferencia de datos es mediante la relación que tienen las etiquitas definiendo los valores en sus tablas para el siguiente salto.
- Se puede recibir datos desde ubicaciones finales con condiciones diferentes de encaminamiento (FRC), es decir etiquetas diferentes serán reenviadas por diferentes rutas en cada LSR con esto existe tráfico diferente dentro de una misma red.

4.1.3.2. Limitaciones.

Al existir nuevos equipos como "Routers Gigabit", encontramos que existe una pérdida de relevancia en los equipos MPLS.

Si tomamos en cuenta la ventaja de juntar varias etiquetas, esto también puede causar bajo rendimiento en la infraestructura.

Si verificamos la calidad de servicio a través de etiquetas muchas veces no podría ser satisfactorio, muchas veces las aplicaciones específicas nos ayudan con el aseguramiento de la calidad.

4.1.4. MPLS y su Arquitectura

Los componentes Esenciales que se encuentran interconectados desempeñan una función muy importante en la red a continuación se detallan:

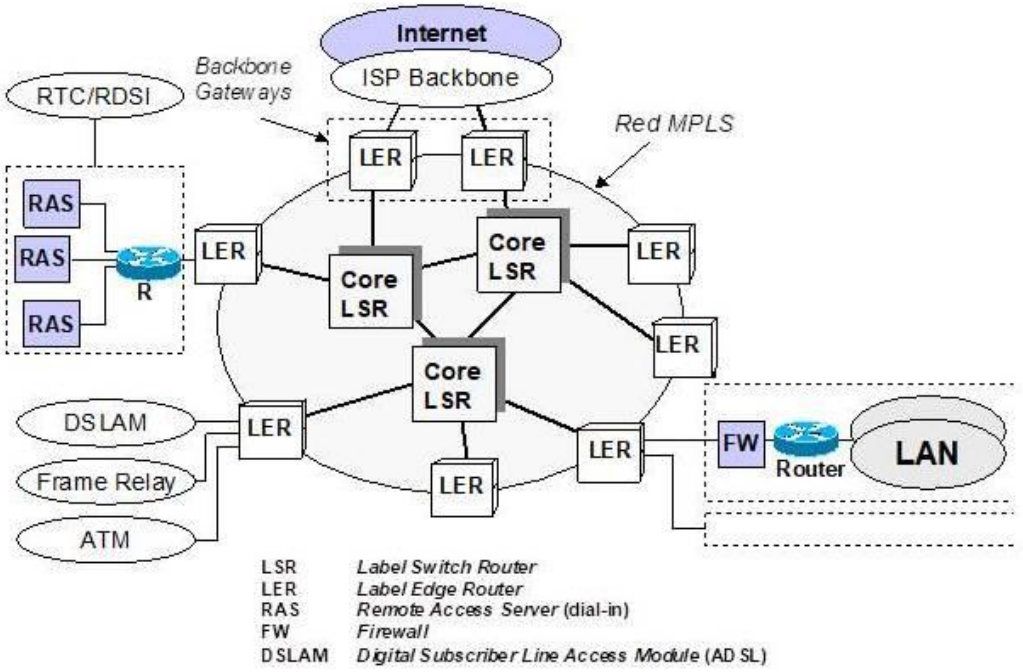

Figura 5 Componentes de una MPLS (Ramón Millán, 2022)

4.1.4.1. LSR Label Switch Router (LSR).

Su función principal es reenviar paquetes de datos utilizando etiquetas en lugar de direcciones IP tradicionales para el enrutamiento.

Cuando un paquete llega a un LSR, este examina la etiqueta adjunta al paquete y utiliza dicha información para determinar hacia dónde debe dirigirse el paquete, luego, el LSR elimina la etiqueta antigua y aplica una nueva etiqueta antes de enviar el paquete al próximo LRS en la ruta hacia su destino final, de esta forma no se verifica el paquete IP. (Ergun, 2021)

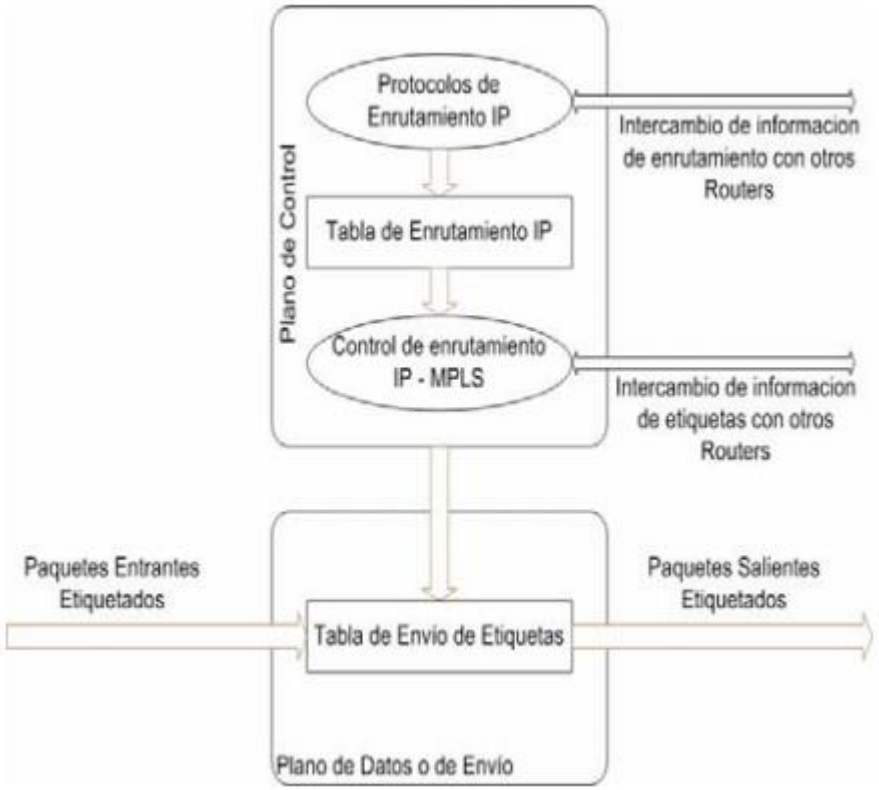

Figura 6 Diagrama LSR (Gracia et al., 2007)

4.1.4.2. LER Label Edge Router (LER).

Actúa como punto de entrada y salida de la red MPLS, donde los paquetes ingresan y salen de la red etiquetada.

El LER es uno de los equipos de borde en la red MPLS, es responsable de agregar o quitar las etiquetas MPLS a los paquetes de datos según su entrada o salida, cuando un paquete entra a la red MPLS, el LER agrega una etiqueta MPLS al paquete para indicar su ruta dentro de la red, y cuando un paquete sale de la red MPLS hacia una red externa, el LER elimina la etiqueta MPLS antes de que el paquete abandone la red MPLS. (Ergun, 2021)

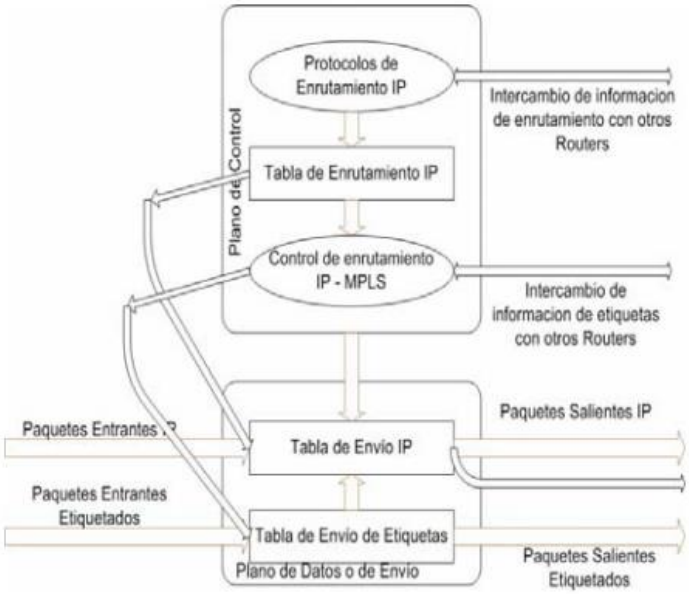

Figura 7 Diagrama LER (Gracia et al., 2007)

4.1.4.3. Label Etiqueta:

Es el número que se asigna a un paquete de datos, con esto se puede definir la ruta a seguir del mismo, son añadidas al ingresar a la red MPLS, están asociadas con una tabla de reenvío del router, esto permite la toma de decisiones rápidas en los router MPLS para el reenvío de paquetes evitando la revisión de todo el encabezado de estos.

Las etiquetas MPLS se insertan entre el encabezado de la capa 2 y el encabezado de la capa 3 del paquete, ayuda a compartir espacio con los protocolos de red ya sean IPv4 o IPv6, con el beneficio de que no es necesario modificar protocolos en capas superiores y asi optimizar el rendimiento de la infraestructura de red. (Ergun, 2021)

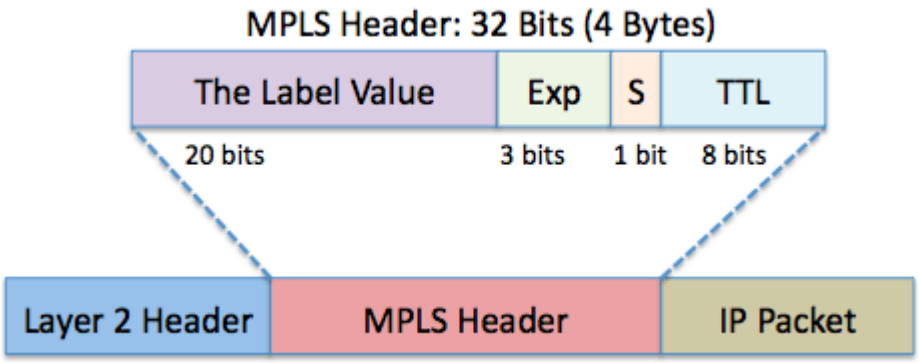

Figura 8 Segmentación de una etiqueta (Gracia et al., 2007)

4.1.4.4. FEC Forwarding Equivalence Class

Es un conjunto de paquetes que se tratan de la misma manera en un router MPLS, esto significa que todos los paquetes dentro de una FEC recibirán el mismo tratamiento de enrutamiento en la red MPLS. Específicamente una FEC se determina mediante un conjunto de criterios, como la dirección de destino IP, los valores de QoS (Quality of Service), o cualquier otra característica que sea relevante para el enrutamiento de los paquetes.

Las FEC se asignan a una o más etiquetas MPLS, donde los paquetes pertenecientes a la misma FEC se reenvían en la misma ruta en la red MPLS, permitiendo a los routers MPLS realicen un reenvío eficiente de paquetes, y no es necesario realizar búsquedas individuales para cada paquete solamente reenviar todos los paquetes de una FEC de manera colectiva.

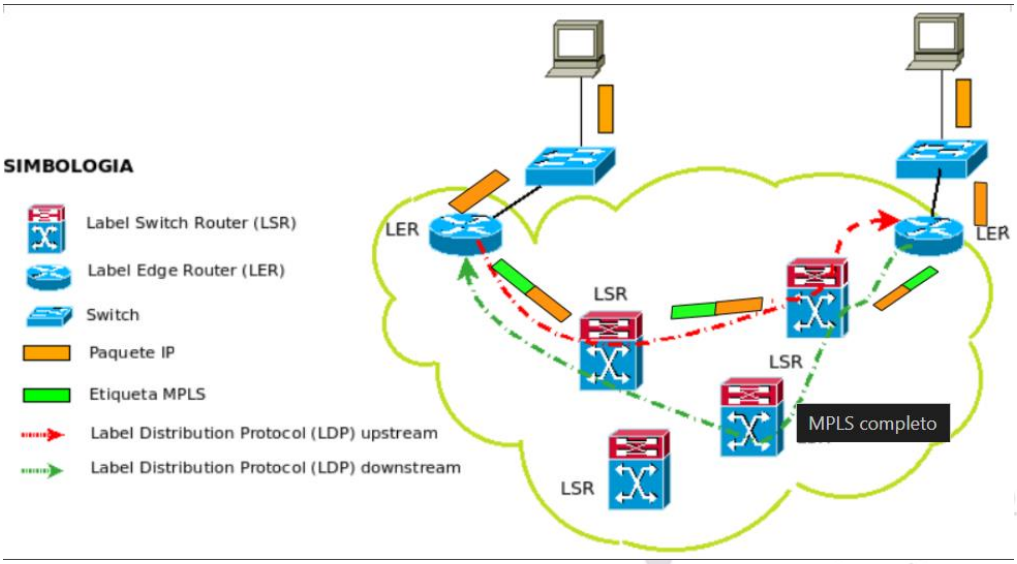

Figura 9 Diagrama distribución FEC(edualejo77, 2011)

4.1.5. Distribución de Etiquetas

Para mejorar la gestión del tráfico utilizando etiquetas tanto en la dirección ascendente (upstream) como en la descendente (downstream) entre los LSRs, se asigna una etiqueta específica, en este caso L1, a la FEC en los paquetes que van desde el Router1 al Router2. En este escenario, se identifica que el Router1 actúa como el LSR upstream y el Router2 como el LSR downstream en función de esta asociación y así cuando la etiqueta representa una FEC de upstream a downstream, se considera como una etiqueta local, aunque no es necesario que todos los paquetes de esa FEC sigan el mismo proceso. (Salviat, 2005).

MPLS no se limita solo a métodos como la señalización de etiquetas, sino que también se ha integrado con protocolos existentes, como el ampliamente utilizado BGP, agregando etiquetas a sus mensajes. También cabe recalcar una parte crucial a considerar es el Protocolo de Distribución de Etiquetas (LDP, por sus siglas en inglés), que permite un manejo y una señalización explícitos del espacio de etiquetas facilitando la asignación y el intercambio de etiquetas entre los dispositivos en la red MPLS, lo que contribuye a una gestión eficiente del tráfico y una mejor calidad de servicio (Rodríguez, 2008).

Existen diversas extensiones que se han desarrollado para mejorar el protocolo LDP en base a las cuales permiten marcar rutas específicas para definir la calidad de servicio (QoS) y la clase de servicio (COS) y se enfocan principalmente en el protocolo de Distribución de Etiquetas Basado en Restricciones (CR-LDP).

Los protocolos principales que se utilizan en este contexto y sus características más destacadas son:

LDP (Protocolo de Distribución de Etiquetas): Es el protocolo base que se utiliza para establecer caminos de enrutamiento en redes MPLS.

RSVP (Protocolo de Reserva de Recursos): Permite reservar recursos de red para flujos de datos específicos ayudando a garantizar la calidad de servicio.

CR-LDP (Protocolo de Distribución de Etiquetas Basado en Restricciones): Una mejora de LDP con capacidades adicionales para establecer rutas basadas en restricciones específicas de calidad de servicio.

PIM (Protocolo de Multidifusión Independiente del Protocolo): Utilizado para administrar el tráfico de multidifusión en redes MPLS.

BGP (Protocolo de Puerta de Enlace de Borde): Empleado especialmente en el contexto de redes privadas virtuales (VPN) para establecer y gestionar conexiones entre diferentes redes. (Salviat, 2005).

4.1.5.1. Distribución de Etiquetas Downstream (no solicitada) – DOU: En este enfoque, un LSR puede asignar etiquetas a LSRs que no las han solicitado. (Barberá, 2007)

4.1.5.2. Distribución de Etiquetas Downstream bajo Demanda (solicitada) – DOD: Permite que un LSR solicite explícitamente al siguiente salto de una FEC específica una asignación de etiquetas para dicha FEC. (Barberá, 2007)

La fusión para los flujos de tráfico entrante a un enrutador desde diversas interfaces puede ser combinados y dirigidos utilizando una etiqueta compartida, únicamente si están dirigidos hacia un mismo destino. (Barberá, 2007)

4.1.6. MPLS VPN

Una red privada virtual (VPN, por sus siglas en inglés) es una tecnología que establece una conexión segura y cifrada entre dos puntos o varios sitios a través de una infraestructura compartida. Ya que es muy importante entender el funcionamiento de una VPN, se debe tener muy en cuenta como es el funcionamiento de una VPN convencional con el fin de entender el funcionamiento en una VPN MPLS.

Una conexión VPN crea un túnel virtual que permite que los datos viajen de forma segura entre dos puntos, como si estuvieran conectados directamente en una red privada física destacando como una de las principales funciones el proteger la privacidad y seguridad de la información transmitida a través de redes públicas, permitiendo a los usuarios acceder a recursos de red de manera remota como si estuvieran físicamente presentes en la red privada.

Una VPN básica conecta directamente a un servidor con uno o más clientes estableciendo una ruta dinámica sobre una red pública o privada, todo esto garantiza una conexión segura debido a que los datos transmitidos entre estos equipos están codificados a manera de encriptación y se enrutan a través de una conexión segura previamente establecida. (Pepelnjak & Guichard, 2002)

Es muy importante tomar en cuenta las políticas y protocolos de seguridad en el proceso de implementación de una VPN, una de las maneras más adecuadas en la gestión de servidores de acceso y autenticación que garanticen la confiabilidad del intercambio de datos, aplicaciones o recursos, manteniendo la integridad de la información.

La conexión VPN se establece mediante un servidor que siempre está a la espera de peticiones de conexión normalmente es un hardware local, aunque en la actualidad se realizan mediante máquinas virtuales o con servicios montados en la nube, los clientes realizan una petición o

llamada donde se procede con el proceso de autorización y autenticación , y así establecer un túnel de comunicación VPN entre los dispositivos sobre la red pública(Pepelnjak & Guichard, 2002)

4.1.7. Conexiones VPN mediante protocolos

Existen varios protocolos de red utilizados para las VPN, los cuales tienen como objetivo principal garantizar altos niveles de seguridad para los datos transmitidos.

- **Protocolo de túnel punto a punto (PPTP**): PPTP establece un túnel de comunicación seguro entre un cliente y un servidor VPN, aunque es comúnmente asociada con Microsoft debido a que Windows ofrece soporte para este protocolo, este túnel encapsula los datos transmitidos, lo que significa que los datos originales se envuelven en un paquete protegido antes de ser transmitidos a través de la red con la capacidad adicional de admitir protocolos no IP proporcionando privacidad y seguridad a la información transmitida, dificultando a terceros acceder o interceptar los datos, también son referidos como servidores de Red Privada Virtual por Marcación (VPDN). (Pepelnjak & Guichard, 2002)

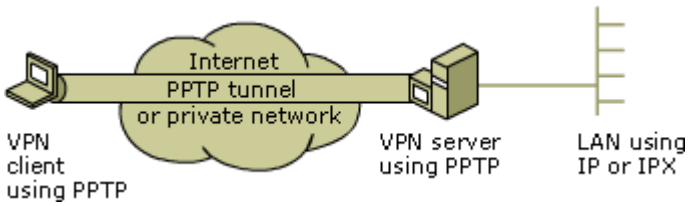

Figura 10 Protocolo de túnel punto a punto (PPTP): (L2TP) (rayh014, 2016)

- Protocolo de túnel de capa dos (L2TP): Combina las características del Protocolo de Túnel Punto a Punto (PPTP) y el Protocolo de Seguridad de Capa de Internet (IPsec) para proporcionar un método robusto y seguro de comunicación en redes no seguras este protocolo opera en el nivel de enlace de datos del modelo OSI y, al igual que PPTP, admite clientes no IP, sin embargo se evidencia que enfrentan desafíos al establecer un estándar para encriptación.(Pepelnjak & Guichard, 2002)

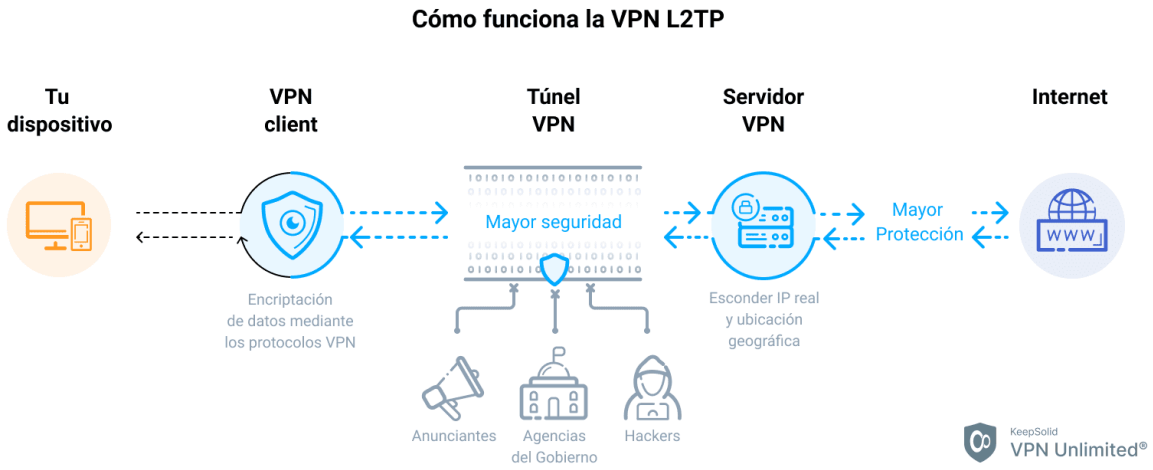

Figura 11 Protocolo de túnel de capa dos (L2TP)(KeepSolid Inc, 2024)

- Seguridad del Protocolo de Internet (IPsec): Es un conjunto de múltiples protocolos relacionados que se usa para el aseguramiento de las conexiones en todos los ambientes ya sean públicos o privados, se lo utiliza como un complemento y una solución completa de protocolo VPN mediante un esquema de encriptación para L2TP o PPTP.

  Puede operar en dos modos principales: modo túnel y modo transporte. En el modo túnel, todo el paquete IP original se encapsula dentro de otro paquete IP protegido por IPsec, lo que permite proteger todo el tráfico de red entre dos puntos.

  En el modo transporte, solo el payload (carga útil) del paquete IP se protege con IPsec, lo que permite asegurar las comunicaciones de host a host. (Pepelnjak & Guichard, 2002)

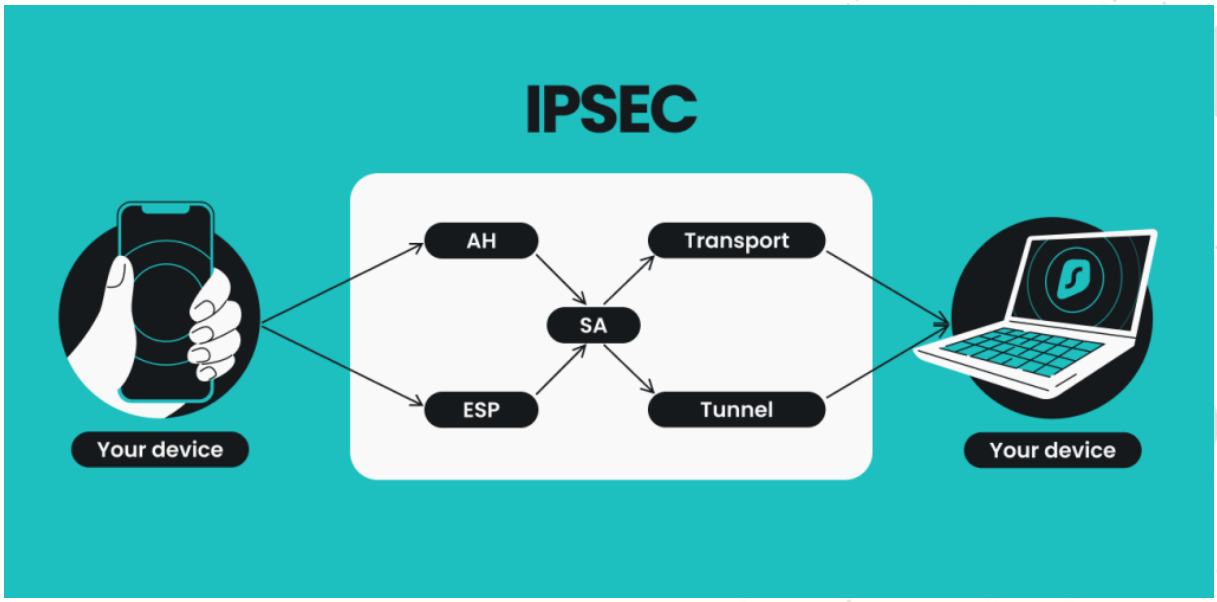

Figura 12 Seguridad del Protocolo de Internet (IPsec) (Antanas Rimeikis,2023)

4.1.8. VPN en MPLS

Para establecer una VPN en una red MPLS, es importante comprender la terminología asociada con los dispositivos involucrados:

- **P y PE:** Representan los routers dentro de la infraestructura del proveedor de servicios en este caso un P es un router interno, mientras que PE es un router fronterizo que se conecta con los clientes.
- **CE:** Se refiere al router del cliente, donde se necesita el servicio de VPN.
- **Site:** Son las redes internas de los clientes, que están separadas por ubicaciones físicas y se conectarán a través de la VPN.

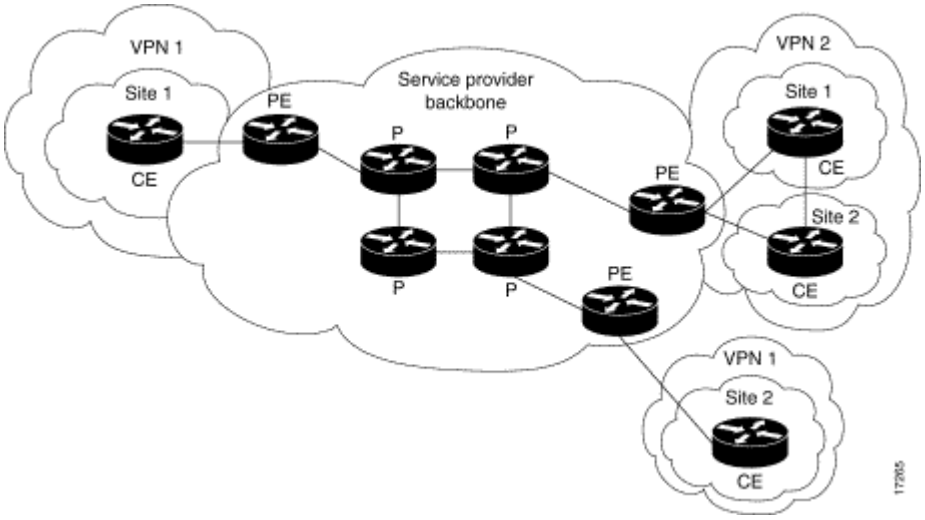

Figura 13 VPN en MPLS (Cisco,2022)

En el contexto de las VPNs, se asocia una VRF (Virtual Routing and Forwarding) que actúa como un contenedor virtual que mantiene separadas las rutas y las tablas de enrutamiento de diferentes redes dentro de VPNs, donde cada VRF tiene su propia tabla de enrutamiento IP y tabla CEF (Forwarding Information Base), junto con las interfaces asignadas para su uso específico, es aquí donde las VRFs distribuyen las rutas dentro de las VPNs, permitiendo que cada red sea distribuida de manera independiente dentro de cada VPN. (Julio J, 2022)

La ruta de una VPN comienza desde el router CE del cliente, se agrega al protocolo BGP (Border Gateway Protocol) y se anuncia su ruta objetivo, que se obtiene de la lista de rutas seleccionadas en la VRF es aquí donde se definen los atributos que una comunidad extendida debe tener para ser importada.

Los routers PE reciben los prefijos IPv4 de los routers CE del cliente mediante protocolos de enrutamiento o rutas estáticas, después el router CE convierte estos prefijos en prefijos VPN_IPv4 y les agrega un identificador de ruta o route distinguer (RD) para identificar al cliente.

La información sobre la capacidad de alcance de los prefijos VPN_IPv4 se obtiene a través de BGP, ya sea internamente (iBGP) entre routers PE o externamente (eBGP) a través de sesiones PE-CE aquí también se puede aplicar a la información de IPv6 o IPX mediante la extensión de sesiones BGP. (Julio J, 2022)

Para reenviar los paquetes, es esencial consultar las tablas almacenadas en la VRF, ya que serán utilizadas por los routers PE para agregar las etiquetas a cada prefijo obtenido de los routers CE, similar a la función de los LER y LSR.

Cuando un paquete proviene de un router CE hacia el PE, se le agrega una etiqueta y se envía, aquí los paquetes que atraviesan el backbone llevan dos etiquetas: la primera indica la dirección del router PE, y la segunda indica cómo el router PE debe reenviar el paquete al router CE, después el router PE recibe el paquete, lee la primera etiqueta, la elimina y reenvía el paquete al destino indicado en la segunda etiqueta. (Julio J, 2022)

4.1.9. QOS en MPLS

MPLS no crea una nueva arquitectura de QoS, simplemente basa en los modelos de la IETF para redes IP ya que estos modelos permiten a los proveedores ofrecer distintos niveles de QoS de extremo a extremo en un entorno IP.

En el modelo de Servicios Integrados, MPLS utiliza RSVP para reservar tráfico agregado de esta forma se asigna etiquetas a los flujos con reservas RSVP y se los agrupa en FECs, evitando analizar las cabeceras IP y de transporte; también al asignar todos los paquetes de una FEC a un LSP, un único LSP puede brindar garantías de QoS a múltiples flujos de tráfico.

MPLS tiene dos objetos RSVP específicos:

- **LABEL_REQUEST:** permite la solicitud de etiquetas downstream en mensajes PATH y RESV.
- **LABEL:** transporta la etiqueta asignada por el router de salida.

El modelo de Clasificación de la IETF clasifica los paquetes en 8 clases según los bits de Precedencia IP, se descartan en congestión según su nivel de precedencia, priorizando los de mayor nivel. Se ha evidenciado que existen varias limitaciones de consenso en la implementación entre fabricantes y de interoperabilidad para QoS de extremo a extremo. (Ghanwani et al., 2000).

En cuanto a los Servicios Diferenciados (DiffServ), el estándar RFC 3270 define dos métodos para la señalización del nivel de QoS:

- EXP-LSP o E-LSP:
    - Los nodos determinan el proceso y tratamiento de QoS (clase y nivel de descarte) del paquete MPLS solo de los bits EXP en la cabecera MPLS.
    - Permite multiplexar varias clases de tráfico dentro de un único LSP.
    - Los datos IP en los ingresos DSCP son enviados al campo EXP en los equipod de borde.
    - No se puede implementar en ATM-LSR.

En el contexto de las redes MPLS, se emplean diversos mecanismos para garantizar la calidad de servicio (QoS), adaptándose a las necesidades específicas de cada red para la selección del modelo adecuado depende de factores como la complejidad, la escalabilidad y los requisitos de QoS (Ghanwani et al., 2000).

El modelo E-LSP se destaca por su eficiencia en comparación con el L-LSP, debido a que limita el número total de LSP (Label Switched Paths), lo que permite conservar etiquetas, un recurso valioso en algunos dispositivos de red (Ghanwani et al., 2000).

El estándar RFC 3270 establece la asignación de un Differentiated Services Code Point (DSCP) a los paquetes, indicando la prioridad y el tratamiento de QoS que deben recibir, el Per-Hop Behavior (PHB) también está definido en base a este estándar, determinando cómo se manejará y tratará el paquete en cada salto de la red.

Durante el establecimiento de las etiquetas MPLS, se establece una asignación entre el valor del encabezado MPLS (EXP para E-LSP o los valores de CLP o DE para L-LSP) y el PHB

correspondiente, para garantizar que los paquetes se gestionen correctamente según su prioridad y tipo de servicio, siguiendo las pautas preconfiguradas y los valores estándar establecidos.

Datos Preconfigurados y Valores por Defecto: Esta asignación puede basarse en datos preconfigurados por el administrador de red, siempre y cuando sean consistentes para todos los LSP (Label Switched Paths, caminos conmutados por etiquetas).El contexto del servicio DiffServ para cada etiqueta, que incluye el tipo de LSP (E-LSP o L-LSP), los PHBs soportados y el mapeo de encapsulado a PHBs para etiquetas entrantes o de PHBs a encapsulados (marcación) para etiquetas salientes, se almacena en la ILM (Incoming Label Map) o en la FTN (FEC-to-NHLFE) durante el establecimiento del LSP. (Ghanwani et al., 2000)

4.1.9.1. Calidad de Servicio en Redes MPLS con VPN

La calidad de servicio (QoS) en una red privada virtual (VPN) se asegura aplicando diferentes políticas de gestión, específicamente en los routers de borde para cada VPN en particular, denotando que, una vez que el tráfico entra al núcleo de la red MPLS, no hay discriminación basada en VPN debido a que no se crean colas ni se descarta tráfico específico de VPN en el núcleo de la red proporcionando una solución escalable de QoS, independientemente de la cantidad de VPN en uso.

4.2. Modelos de QoS:

Los modelos más usados para implementar las garantías de QOS entre dos puntos en una VPN:

4.2.1. Modelo de Tubería (Pipe):

En este enfoque, el proveedor de servicios ofrece al usuario de la VPN garantías específicas de calidad de servicio para flujos de tráfico particulares entre dos routers CE (Customer Edge) dentro de la misma VPN y dentro de los PE (Provider Edge), en los extremos del túnel se definen los flujos de tráfico que pueden utilizarla es un modelo unidireccional y permite asimetrías en los patrones de tráfico, pueden convivir varios túneles que se originen desde un router CE.

Para implementar este modelo de manera efectiva:

- Se emplean caminos de conmutación de etiquetas (LSP) con anchos de banda garantizados para respaldar el modelo, y mejora la escalabilidad de la gestión de calidad de servicio de la VPN MPLS.
- El usuario debe conocer muy bien el comportamiento de su tráfico y realizar un análisis exhaustivo del mismo utilizando herramientas de planificación adecuadas.

4.2.2. Modelo de Manguera (Hose):

En este modelo, el proveedor de servicios ofrece al usuario garantías específicas sobre el tráfico que un router CE en particular enviará o recibirá de otros routers CE dentro de la misma VPN, para realizar esta implementación no es necesario un análisis minucioso del comportamiento del tráfico o una planificación muy detallada.

Dentro del modelo de manguera se definen dos parámetros principales:

- **Tasa de Ingreso Comprometida (ICR):** La velocidad a la que los routers CE en la VPN pueden recibir datos de la red.
- **Tasa de Egreso Comprometida (ECR):** La velocidad a la que pueden enviar datos hacia la red.

4.3. Qué es una red SDWAN

La tecnología de Red definida por Software(SD-WAN) es una herramienta clave para la interconexión de lugares o sitios remotos, con dispositivos específicos y capacidades de software avanzadas, es muy importante entender, que a diferencia de las redes privadas que dependen de circuitos centralizados para el acceso a la nube publica y tienen una conmutación multiprotocolo como la MPLS, presentan inconvenientes a medida que los clientes crecen en infraestructura ya sea en sucursales o sitios remotos, con este contexto la SD-WAN simplifica la interconexión virtualizando la infraestructura de red, con el cambio de circuitos privados como MPLS, por una RED superior controlada directamente por software, donde toda la comunicación como el enrutamiento, se implementa mediante funciones de red virtualizadas(VNF), y se instalaría normalmente 1 servidor por sucursal, esto ayuda a que los sites accedan directamente a las aplicaciones de la nube publica e internet, esto ayuda

enormemente a eliminar la dependencia de estar conectado a un centro de Datos central.(Prensario, 2023).

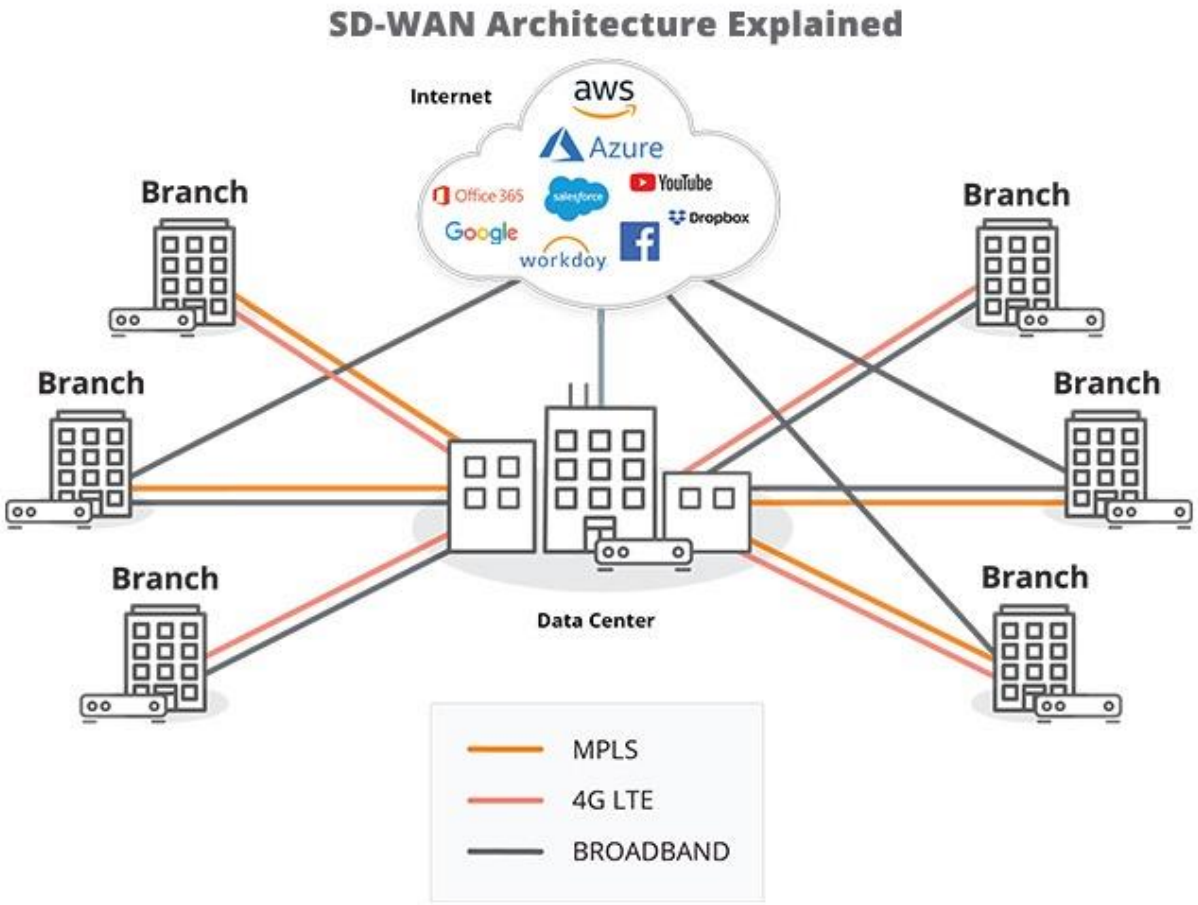

Figura 14 Arquitectura SDWAN (Andrés Cuevas, 2020)

Una red SD-WAN simplifica las configuraciones al ejecutarse en un solo servidor por sucursal, reduciendo la complejidad y los costos asociados, la flexibilidad es otro aspecto crucial de la SD-WAN, a diferencia de las redes privadas heredadas que dependen de proveedores de servicios específicos y conexiones costosas, la SD-WAN permite el uso de acceso de banda ancha, redes inalámbricas y otros servicios, brindando a las empresas una gama más amplia de opciones para implementar sus propias SD-WAN (bxavier, 2023),

Desde la década de 1980 y en la época actual, las redes de área amplia (WAN) han estado mayormente basadas en TDM (Multiplexación por División de Tiempo), utilizadas para servicios de voz y datos, a principios de los años 90, las empresas comenzaron a implementar redes basadas en paquetes para las WAN, con la tecnología Frame Relay predominando en ese momento, durante esa misma década, surgió la tecnología ATM (Modo de Transferencia Asincrónica), adoptada por numerosas organizaciones de telecomunicaciones y finalmente, a partir del año 2000, se inició el auge de MPLS, convirtiéndose en la nueva tecnología dominante para las WAN (Heredia, 2019).

La arquitectura actual de las redes WAN está principalmente orientada a empresas, sus sucursales y centros de datos tomado en cuenta que, cuando una empresa utiliza aplicaciones alojadas en la nube, como Software as a Service (SAAS), las redes WAN pueden experimentar un exceso de tráfico, lo que provoca problemas significativos en su rendimiento y conlleva costos elevados de mantenimiento debido a la necesidad de canales dedicados y redundantes.

Uno de los principales desafíos es facilitar la conexión de múltiples usuarios a diversos tipos de dispositivos dispersos en distintos entornos de la nube.(K. Yang et al., 2019)

La tecnología SD-WAN proporciona una solución integral de enrutamiento entre los diversos equipos y dispositivos de la red, facilitando una comunicación eficiente y sin problemas ya que también incluye medidas avanzadas de protección contra una amplia variedad de amenazas cibernéticas, para garantizar la seguridad de los datos y la continuidad operativa de la empresa.

SD-WAN tiene la capacidad optimizar el uso de los canales dedicados de la red para permitir una distribución más eficiente del tráfico y una utilización más efectiva de los recursos disponibles, esta optimización contribuye a mejorar el rendimiento general de la red y a reducir los tiempos de respuesta.

Una de las partes importantes de SD-WAN es facilitar la gestión eficaz de la red WAN, permitiendo a los administradores monitorear y controlar de manera centralizada el tráfico de datos, así como implementar políticas de seguridad y priorización de aplicaciones de forma ágil y sencilla, esto se traduce en una mayor disponibilidad de todas las aplicaciones empresariales, asignando recursos de manera dinámica según las necesidades del negocio.

Con una Red SD-WAN el gasto operativo (OpEX) asociado con la infraestructura de red, reemplaza los costosos servicios de conmutación a comparación con las tecnologías tradicionales como MPLS, con una conectividad de banda ancha más económica y flexible.

En cuanto a la seguridad, SD-WAN ofrece una protección integral al cifrar la información de extremo a extremo y al proporcionar un control de acceso en tiempo real para los usuarios, la tecnología SD-WAN permite distribuir de manera efectiva las medidas de seguridad a las sucursales y puntos de acceso remotos de la organización, mediante el uso de Firewalls de Próxima Generación (NGFW), Antivirus de Próxima Generación (NGAV) y seguridad basada en DNS.(Alwasel et al., 2020).

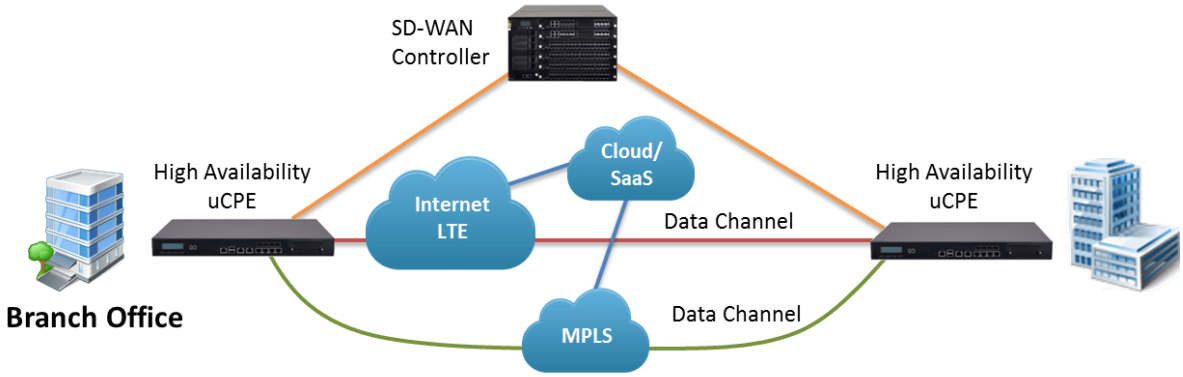

Figura 15 Seguridad SDWAN (Andrés Cuevas, 2020)

4.3.1. ¿Cómo funcionan las SD-WAN?

Las tecnologías de redes definidas por software (SD-WAN) operan mediante la separación del plano de control del plano de datos, en contexto de redes, el plano de control abarca todos los elementos encargados de dirigir y gestionar el flujo de datos a través de la red, mientras que el plano de datos se encarga de la transferencia física de esos datos según las indicaciones recibidas del plano de control.

Tradicionalmente, en las arquitecturas de red convencionales, el plano de control y el plano de datos estaban íntimamente vinculados y se ejecutaban en dispositivos de hardware específicos proporcionados por los proveedores de equipos de red, hoy en día, con la

evolución hacia las SD-WAN, se ha adoptado un enfoque diferente desacoplando el plano de control, que opera a través de software, del plano de datos, que sigue basándose en hardware.

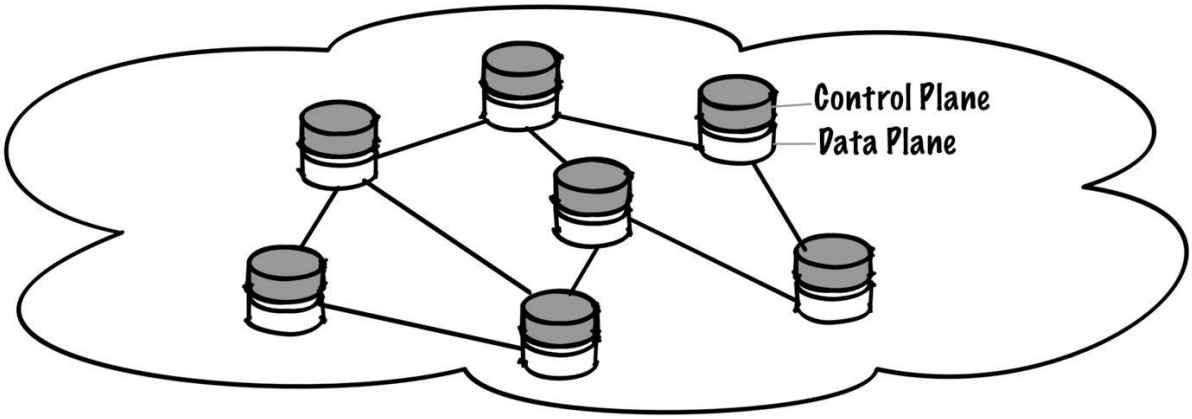

Figura 16 WAN Tradicional (Juniper Networks, 2024)

Esta separación permite que las funciones de enrutamiento y gestión de la red se implementen de manera más flexible y eficiente, de esta forma ya no depende únicamente de dispositivos de hardware especializados para llevar a cabo las tareas de enrutamiento, las SD-WAN permiten que el enrutamiento se realice en el software que se ejecuta en hardware estándar o básico, para brindar una mayor flexibilidad y escalabilidad a la hora de gestionar el tráfico de la red.(Juniper Networks, 2024)

Al separar el plano de control del plano de datos, las SD-WAN facilitan la implementación de políticas de gestión de tráfico más dinámicas y adaptativas y las empresas pueden ajustar y optimizar continuamente el rendimiento de su red según las necesidades cambiantes del negocio y las condiciones del entorno.(Juniper Networks, 2024)

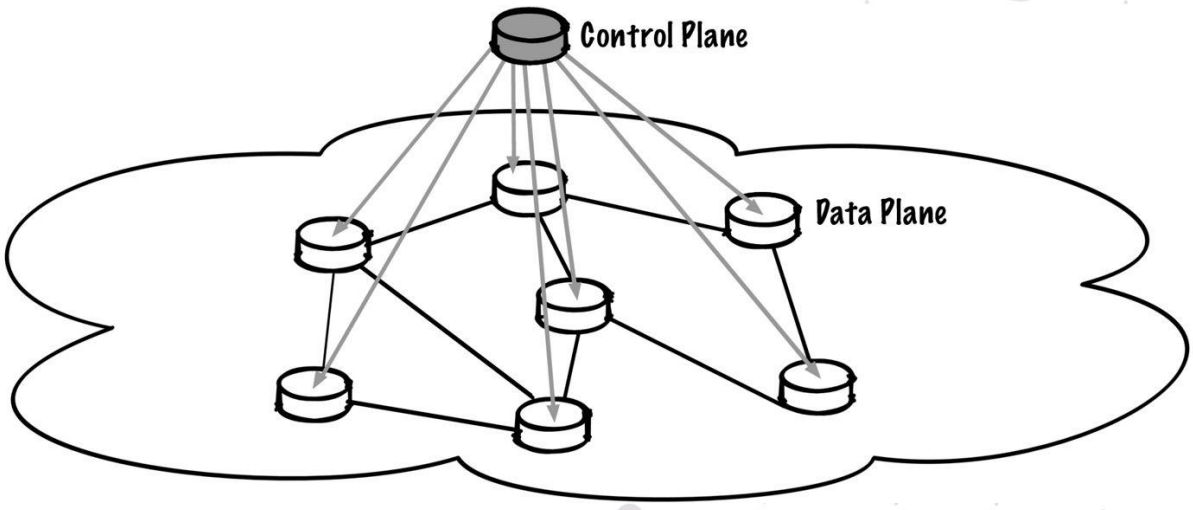

Figura 17 SD-WAN definida por software(Juniper Networks, 2024)

4.3.2. Ventajas y limitaciones de una red SDWAN:

4.3.2.1. Ventajas

- **Bajo costo debido a la naturaleza basada en software**: SD-WAN se basa en software, debido a que puede implementarse en hardware estándar o básico en lugar de requerir dispositivos de red especializados y costosos, reduciendo significativamente los costos de hardware y licencias, haciendo que la solución sea más accesible para una variedad de organizaciones.(cloudflare, 2024)
- **Facilidad de configuración y adaptación a las configuraciones:** La naturaleza basada en software de SD-WAN facilita su configuración y personalización ya que se pueden adaptar fácilmente las configuraciones según las necesidades específicas de la organización, permitiendo una implementación más rápida y una respuesta más ágil a los cambios en los requisitos de la red. (cloudflare, 2024)
- **Control centralizado:** SD-WAN ofrece un control centralizado sobre toda la red, para simplificar la gestión y la monitorización de los recursos, mediante un único panel de control, facilitando la supervisión y gestión en todos los aspectos de la red, desde la asignación de ancho de banda hasta la implementación de políticas de seguridad.(Cloudflare, 2024)
- **Programabilidad para adaptarse a las condiciones cambiantes del tráfico:** Los algoritmos de enrutamiento inteligente pueden ajustarse dinámicamente para optimizar el tráfico en función de las condiciones de la red y las necesidades del negocio. Por ejemplo, SD-WAN puede priorizar automáticamente el tráfico crítico para las aplicaciones empresariales en momentos de congestión de la red, garantizando un rendimiento óptimo en todo momento.(Cloudflare, 2024)

4.3.2.2. Limitaciones

- **Entrega el control del ancho de banda dedicado al ISP:** Aunque SD-WAN proporciona herramientas para priorizar y gestionar el tráfico de red, algunas implementaciones pueden requerir que el proveedor de servicios de internet (ISP) tenga cierto control

sobre el ancho de banda dedicado, limitando la flexibilidad y autonomía del usuario sobre la gestión del ancho de banda(cloudflare, 2024).

- **Entrega el control de las medidas de seguridad al ISP:** En algunas configuraciones de SD-WAN, especialmente en implementaciones gestionadas por el proveedor de servicios, el control sobre las medidas de seguridad puede recaer en el ISP, se dependería estrictamente de las políticas de seguridad, como los cortafuegos y la detección de intrusiones y pueden ser gestionadas por el ISP en lugar de ser administradas directamente por el usuario una de las rezones que genera preocupaciones sobre la confidencialidad y la privacidad de los datos, así como sobre la capacidad del ISP para proteger eficazmente la red del cliente. (cloudflare, 2024).
- **Dependencia del firmware del dispositivo y su seguridad:** La seguridad de una red SD-WAN puede estar sujeta a la calidad y la fiabilidad del firmware del dispositivo utilizado. Si el firmware no está actualizado o no es seguro, la red podría estar expuesta a vulnerabilidades de seguridad, incluyendo ataques de malware o piratería.(Cloudflare, 2024)
- **Eficiencia decreciente con la distancia para aplicaciones no optimizadas para la web:** Si bien SD-WAN ofrece una optimización del tráfico de red para aplicaciones basadas en la web, su eficacia puede disminuir significativamente con la distancia para aplicaciones que no están diseñadas o no son compatibles con la optimización web. Teniendo como resultado una posible degradación del rendimiento y una menor calidad de experiencia para los usuarios finales, especialmente en entornos distribuidos geográficamente o con conexiones de larga distancia.(cloudflare, 2024)

4.3.3. Arquitectura de la Red SDWAN:

La infraestructura convencional de las redes de área amplia ya no es suficiente para afrontar el creciente dinamismo de las tendencias en redes y el uso cada vez más intensivo de aplicaciones. Además, las demandas de calidad de servicio por parte de los usuarios han alcanzado niveles más exigentes que requieren soluciones más avanzadas y flexibles.

En este contexto, las redes de área amplia definidas por software (SD-WAN) emergen como una alternativa innovadora y altamente eficiente, estas redes tienen como objetivo fundamental simplificar el diseño y la gestión de las infraestructuras de red, reducir la complejidad operativa, optimizar el rendimiento y, sobre todo, introducir un nivel de flexibilidad y adaptabilidad que las redes tradicionales no pueden igualar.

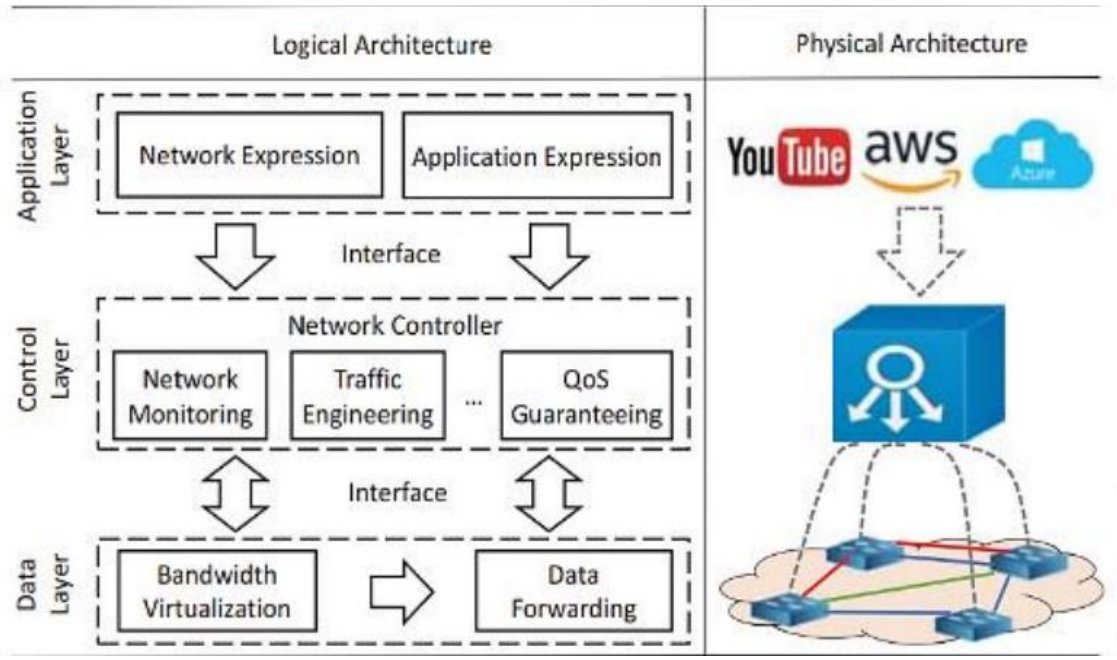

Figura 18 arquitectura lógica y física SDWAN(Z. Yang et al., 2019a)

Al permitir la programación y la gestión centralizada a través de software, las SD-WAN ofrecen un enfoque más ágil y dinámico para la configuración y el despliegue de la red. (Z. Yang et al., 2019)

Las SD-WAN están diseñadas para ofrecer una mayor eficiencia en el uso de los recursos de red, permitiendo una distribución más inteligente del tráfico y una mejor optimización de la conectividad, se evidencia un rendimiento más consistente y una experiencia de usuario mejorada, incluso en entornos con una alta demanda de ancho de banda y recursos compartidos. (Z. Yang et al., 2019)

4.3.3.1. Arquitectura lógica:

En la red de área amplia definida por software (SD-WAN), se distinguen tres capas que se organizan de abajo hacia arriba, estas capas comprenden la capa de software, la capa de control y la capa de aplicación, como se ilustra en la figura 14 del documento.

- Capa de Datos: Esta capa se divide en virtualización de ancho de banda y reenvío de datos, la virtualización combina múltiples enlaces de red para aprovechar plenamente los recursos de ancho de banda, proporcionando una ubicación centralizada de recursos disponibles para todos los servicios y aplicaciones, el reenvío de datos implica el uso de elementos de red distribuidos para reenviar paquetes utilizando el ancho de banda proporcionado por la virtualización. (Z. Yang et al., 2019)
- Capa de Control: Considerada la capa más crítica dentro de la arquitectura SD-WAN, se encarga de funciones como centralizar las aplicaciones, visualizar la estructura de red y configurar cada nodo de red en rutas específicas para el envío y recepción de tráfico, esta capa selecciona el mejor camino y toma decisiones de enrutamiento de tráfico para la red.(Bannour et al., 2018)
- Capa de Aplicación: Esta capa representa el nivel más alto y se encarga de establecer aplicaciones de manera centralizada, implementando configuraciones, aprovisionando y extendiendo nuevos servicios en la red, la comunicación entre la capa de aplicación y la capa de control se lleva a cabo mediante una API, que proporciona información sobre el estado general de la red y ayuda a mejorar la transmisión de datos para aplicaciones específicas.(Guanoluisa Jaramillo, 2019)

4.3.3.2. Arquitectura física:

En la capa de datos de la infraestructura SDN (Redes Definidas por Software), se establece un conjunto interconectado de controladores, los cuales son esenciales para la gestión y el control de los dispositivos de red, estos controladores se comunican entre sí mediante enlaces físicos, formando una red de control distribuida que abarca toda la infraestructura.

La función principal de cada controlador de red es supervisar y coordinar el funcionamiento de los dispositivos de red bajo su control, se pueden incluir conmutadores, routers y otros elementos de red que conforman la infraestructura SDN.

Cada controlador asume la responsabilidad de gestionar un conjunto específico de dispositivos, asegurando su correcto funcionamiento y optimizando su rendimiento según las necesidades del sistema. (Z. Yang et al., 2019)

En términos de implementación, los controladores de red suelen desplegarse como servidores dedicados o como clústeres de servidores, dependiendo de la escala y la complejidad permitiendo adaptar la capacidad y los recursos del controlador a las demandas particulares de la infraestructura SDN.

Un aspecto importante para considerar es la redundancia y la tolerancia a fallos en la arquitectura de control de la red, para garantizar la disponibilidad y la fiabilidad del sistema, es común implementar múltiples controladores distribuidos en diferentes ubicaciones geográficas, donde se designa un controlador como principal y los demás actúan como controladores de respaldo, de ser así cuándo ocurra una falla en el controlador principal, los controladores de respaldo automáticamente toman el control y continúan gestionando la red sin interrupciones significativas. (Z. Yang et al., 2019).

4.3.4. Distribuciones de SDWAN

Con el aumento de la digitalización empresarial, existe una creciente demanda de profesionales y empresas de SD-WAN para proporcionar soluciones. SD-WAN, las empresas dependen de las redes de área amplia, o redes caracterizadas por grupos de computadoras que están geográficamente distantes entre sí, para comunicarse de diversas formas, especialmente entre la oficina central y las sucursales, el soporte de SD-WAN implica asegurarse de que la red misma pueda ajustarse dinámicamente a los cambios en las condiciones, sin tener que depender de asistencia manual.

En general, el nivel de soporte que recibe una organización para SD-WAN depende de su tamaño, las grandes empresas tienden a realizar la mayoría de sus actividades relacionadas con SD-WAN internamente, confiando en su propio personal de ingeniería, las empresas de tamaño mediano a menudo adoptan un enfoque híbrido, subcontratando algunas operaciones a proveedores externos mientras mantienen otras ellas mismas, las organizaciones más pequeñas a menudo carecen de la experiencia para gestionar SD-WAN por sí mismas, por lo que frecuentemente contratan empresas de SD-WAN para que se hagan cargo del proceso por ellas.

Figura 19 Top 15 empresas desarrollo SDWAN(Field Engineer, 2024)

- Cisco Meraki SD-WAN

Cisco Meraki es una empresa de soluciones de software en la nube con sede en California, cuenta con una amplia experiencia en soluciones de redes gestionadas en la nube, incluido el mantenimiento y despliegue de SD-WAN, ofrece a las empresas soluciones empresariales escalables de SD-WAN y proporciona a los clientes una variedad de herramientas basadas en la nube para gestionar sus productos.(Field Engineer, 2024)

- Riverbed SD-WAN

Riverbed es una empresa de redes en la nube especializada en SD-WAN. La empresa asegura que puede superponer nuevos y mejorados sistemas de SD-WAN sobre la infraestructura de red existente, reduciendo las interrupciones durante el despliegue. También afirma que sus productos tienen una curva de aprendizaje sorprendentemente suave debido a sus herramientas de software intuitivas. (Field Engineer, 2024)

- Nuage SD-WAN

Nuage es una división de la antigua empresa líder en telefonía móvil, Nokia. La empresa comenzó a diversificarse en diferentes áreas de negocio y se convirtió en uno de los primeros líderes en el espacio de SD-WAN. A diferencia de muchos otros proveedores de la industria, Nuage cree que es mejor ser primero receptivo a las necesidades de las aplicaciones, en lugar de optimizar los anchos de banda y el nivel de sucursal después del hecho. (Field Engineer, 2024)

- Velocloud SD-WAN

Velocloud, antes llamada Velocloud Networks, es un servicio de redes basado en la nube que ofrece una cartera de productos, incluido SD-WAN entregado en la nube. Fundada en 2012, la empresa se ha ganado una reputación por poder ofrecer soluciones de software de clase empresarial para gestionar flujos de datos entre sucursales y centros de datos. (Field Engineer, 2024)

- Versa SD-WAN

Versa promete cambiar el pensamiento corporativo tradicional. En lugar de preguntar qué puede hacer la empresa basándose en lo que IT puede entregar, Versa quiere permitir que IT cumpla con lo que el negocio necesita. La empresa ofrece una gama de productos de SD-WAN gestionados, ayudando tanto en el despliegue como en el monitoreo de las WAN. (Field Engineer, 2024)

- Aryaka SD-WAN

Aryaka es uno de los proveedores de servicios empresariales de SD-WAN más valorados en el mundo, gracias a su combinación única de tecnologías. Aryaka ofrece a las empresas redes privadas en conjunto con técnicas de aceleración, interoperabilidad con plataformas en la nube y soluciones de servicios de SD-WAN listas para usar en toda la red. (Field Engineer, 2024)

- Barracuda SD-WAN

Barracuda entiende que las organizaciones no solo desean SD-WAN eficientes y altamente optimizados, sino también redes seguras, afirmando que sus tecnologías pueden ayudar a superar las limitaciones tradicionales del firewall y proporcionar seguridad en la nube de

próxima generación para organizaciones que transfieren datos sensibles a través de redes. (Field Engineer, 2024)

- Juniper SD-WAN

El producto SD-WAN de CloudGenix es una solución completa de SD-WAN, que ofrece todas las características críticas que las organizaciones podrían necesitar. CloudGenix, al igual que muchos otros proveedores, está feliz de ofrecer un enfoque híbrido, con algunas funciones mantenidas internamente y otras llevadas a cabo por sus ingenieros. (Field Engineer, 2024)

- Big Leaf SD-WAN

Big Leaf se especializa en el desarrollo e implementación de SD-WAN basado en la nube para las empresas en crecimiento de hoy. La empresa afirma que su tecnología SD-WAN puede eliminar problemas de rendimiento y ayudar a las empresas a cambiar a organizaciones centradas en la nube. La empresa, con sede en Beaverton, Oregón, se constituyó en 2012 y ofrece una gama de soluciones de conectividad a Internet y de red. (Field Engineer, 2024)

- Talari SD-WAN

Talari se especializa en ayudar a reducir los costos de SD-WAN a medida que las empresas crecen. El proveedor afirma que, a través de su plataforma, los clientes obtienen no solo una red ágil que responde en tiempo real, sino también una que se expande sin que haya una penalización de precio. El SD-WAN de Talari, según el proveedor, tiene una fiabilidad líder en su clase y un mejor rendimiento de aplicaciones que la competencia. (Field Engineer, 2024)

- Cato SD-WAN

Cato es uno de los líderes del mercado en lo que ellos llaman "SD-WAN 3.0" - o SD-WAN gestionado y operado en la nube, la empresa se especializa en la implementación en la nube de SD-WAN y proporciona conectividad segura tanto a usuarios móviles como a centros de datos en la nube, oficinas remotas y cualquier otra ubicación donde un interesado pueda acceder a Internet. (Field Engineer, 2024)

- Cisco Viptela SD-WAN

Una de las tecnologías empleadas para la creación de redes SD-WAN es conocida como Cisco-Viptela, esta tecnología se basa en la capacidad de independizarse completamente del entorno

físico de manera automática y segura, lo que permite obtener una visibilidad en tiempo real de todos los cambios que ocurren dentro de la red. Este enfoque tiene como objetivo optimizar las decisiones que impactan en el entorno de manera más rápida y efectiva.

En el caso de una organización que utiliza tecnología de acceso MPLS y también cuenta con otro acceso a Internet, Cisco-Viptela dirigirá automáticamente el tráfico de la red hacia uno u otro acceso en función de las latencias que se presenten en ese momento. Esta capacidad de adaptación dinámica permite ofrecer una arquitectura WAN desde un servicio en la nube, lo que resulta en una notable reducción de costos y tiempos durante el despliegue de la red. Además, proporciona una arquitectura de seguridad más sólida para proteger los datos transmitidos a través de la red. (Field Engineer, 2024)

Cisco-Viptela está compuesto por cuatro componentes, cada uno de los cuales se enfoca en distintos aspectos.

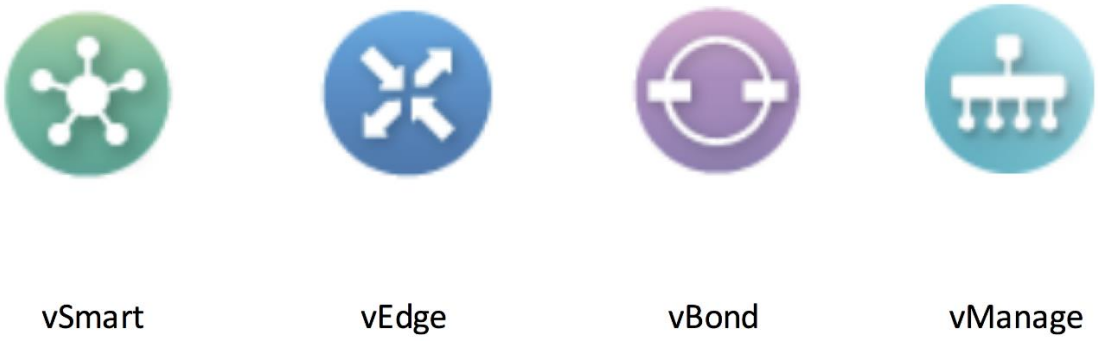

Figura 20 Componentes Cisco Viptela (fuente: autor)

- vEdge: Centrado en el plano de datos, es esencialmente el router ubicado en las oficinas, no solo se conecta de manera segura con otros componentes de la red, sino que también desempeña un papel crucial al establecer sesiones IPSec con otros dispositivos vEdge en la red WAN, esta capacidad de conexión da lugar a diferentes topologías, como completamente malladas, parcialmente malladas, punto a punto y de concentrador y radios.(DCLessons, 2020)

  La última de estas topologías se usa comúnmente para VPN de datos, mientras que las completamente malladas son preferidas para VPN de voz y permite una segmentación

segura del tráfico en una misma infraestructura física, lo que brinda flexibilidad y robustez a la red.

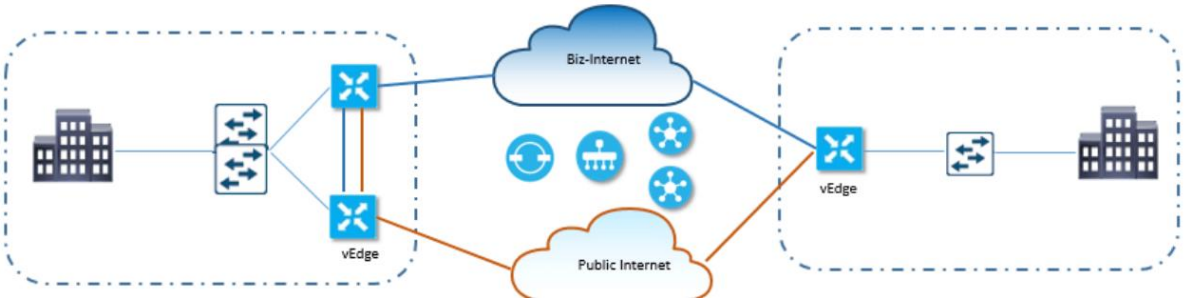

Figura 21 vEdge diagrama(DCLessons, 2020)

- vSmart: Facilita todas las conexiones mediante Secure Sockets Layer (SSL), que encriptan el tráfico entre navegadores web y sitios web, así como entre servidores, protegiendo la conexión con los demás elementos dentro de la red SD-WAN de Cisco-Viptela mediante el protocolo Overlay Management Protocol (OMP), se determina todas las políticas relacionadas con el enrutamiento de la información, así como la seguridad y el control de todos los accesos definidos de manera centralizada, para entender mejor el funcionamiento de este dispositivo, se puede comparar con un reflector de rutas del Protocolo de Puerta de Enlace Fronteriza (BGP), lo que permite la presencia de múltiples dispositivos vSmart dentro de la red de la organización. (DCLessons, 2020)

  El protocolo OMP es responsable de establecer y mantener el plano de control en una red SD-WAN. Ofrece servicios esenciales, como la conectividad en toda la red, la distribución de rutas de enrutamiento a nivel de servicio y la gestión de los distintos parámetros de seguridad, además, controla y distribuye las políticas de enrutamiento, regulando así el flujo de tráfico entre los dispositivos vSmart y vEdge. (Liu et al., 2020)

  Algunas de las características clave de este protocolo son las siguientes:

  - Basado en el protocolo Transmission Control Protocol (TCP).
  - Funciona eficazmente en mallas completas.
  - Realiza segmentación de Redes Privadas Virtuales (VPN).
  - Ofrece accesibilidad y seguridad.
  - Proporciona rutas de servicio.

- Establece políticas de enrutamiento de datos en toda la red.

- vManage: opera a través de un panel centralizado que facilita la configuración, gestión y supervisión integral de toda la red SD-WAN implementada mediante Cisco-Viptela. Esto implica que permite monitorear la red en tiempo real y tomar decisiones óptimas respecto al enrutamiento y la transferencia de información entre diferentes medios. Es importante destacar que, si bien este dispositivo es fundamental en la red, depende de otros dispositivos para recopilar toda la información disponible; específicamente, depende de los equipos vEdge para presentar los resultados a nivel de aplicación. (DCLessons, 2020)

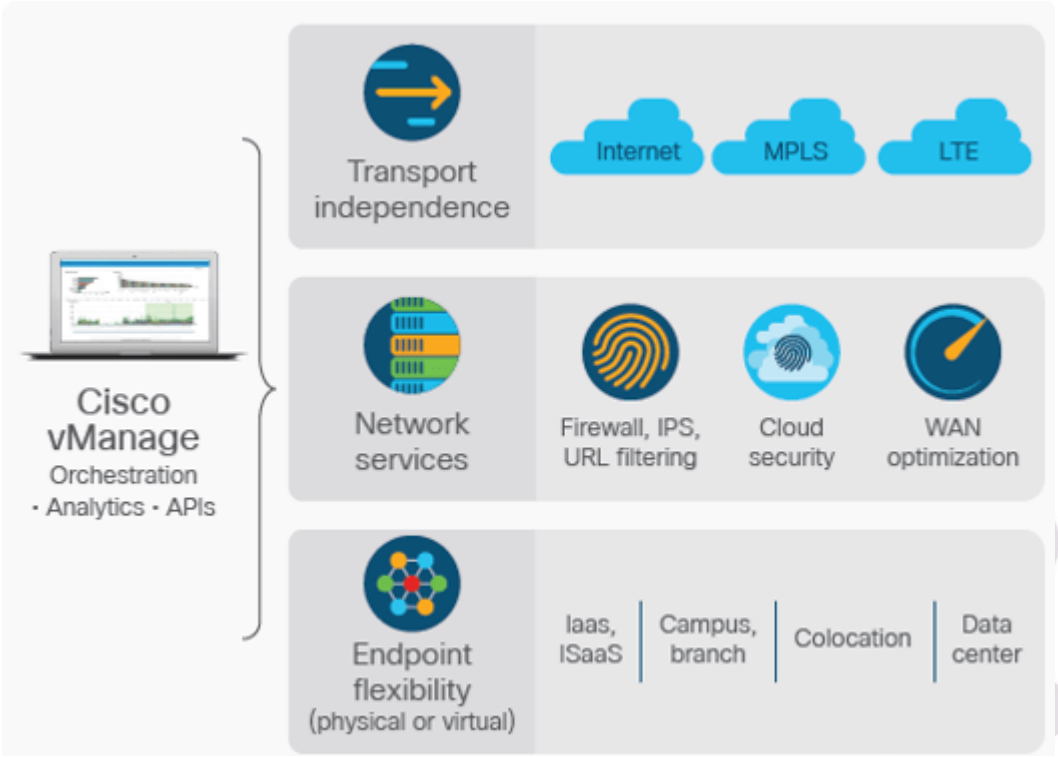

Figura 22 vManage diagrama (DCLessons, 2020)

- vBond: Es un componente crucial que lleva a cabo el despliegue inicial de la red, ejecutando las tareas de autenticación y autorización de todos los elementos en la infraestructura. Su función es fundamental, ya que proporciona la información necesaria sobre cómo deben conectarse entre sí cada uno de los componentes de la red.(DCLessons, 2020)

4.3.5. QOS en SDWAN

Una de las practicas más importantes es el uso común de las políticas de datos habilitando QOS en las interfaces de los dispositivos borde vEdge, esto con el fin de clasificar la información de los datos según la importancia de ellos, clasificándolos de múltiples formas según la necesidad del usuario. Esto se lo puede definir en múltiples colas de salida en las interfaces, adicional a la programación de la tasa de transmisión que se envía cada clase de tráfico.

El avance en las tasas de transmisión mediante internet, cada vez es más amplio en este tiempo es aproximadamente de 10/40 Gigabit en toda la red de área local ya sea en los sitios principales, como en remotos; sin embargo los enlaces WAN, todavía son limitados esto genera un cuello de botella en la parte de los enrutadores al gestionar la conexión con los recursos de red y mucho más al manejar por igual todos los paquetes, esto se debe a que no existe un mecanismo que haga diferencia y determine qué importancia existe en los flujos de tráfico. Los paquetes son almacenados en memoria y enviados al azar, por ende, la perdida de paquetes es constante. (NetworkAcademy, 2023)

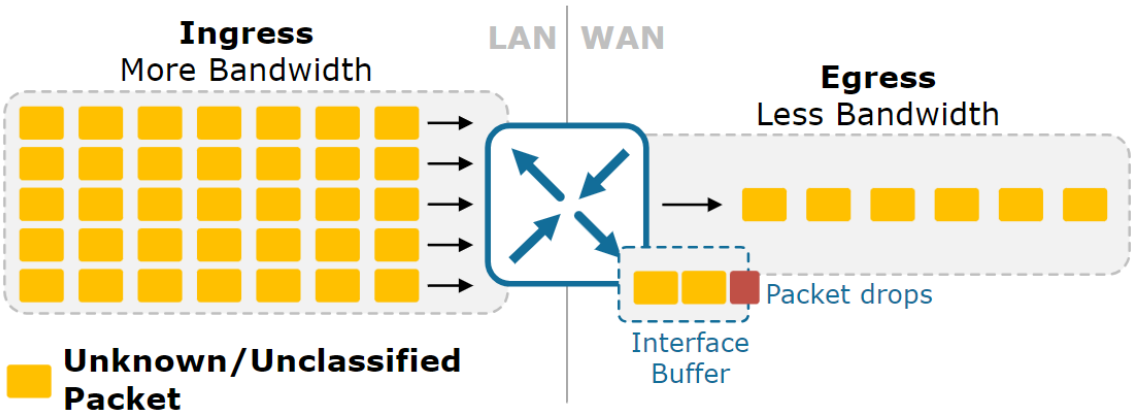

Figura 23 Por que es importante QOS (Network Academy,2023)

El objetivo principal para implementar QOS es maximizar la calidad de la experiencia (AppQoE) gestionando los recursos de la red WAN y diferenciando los flujos de tráfico Dependiendo de la actividad de la empresa u organización el tráfico será clasificado en base a su criticidad. (NetworkAcademy, 2023)

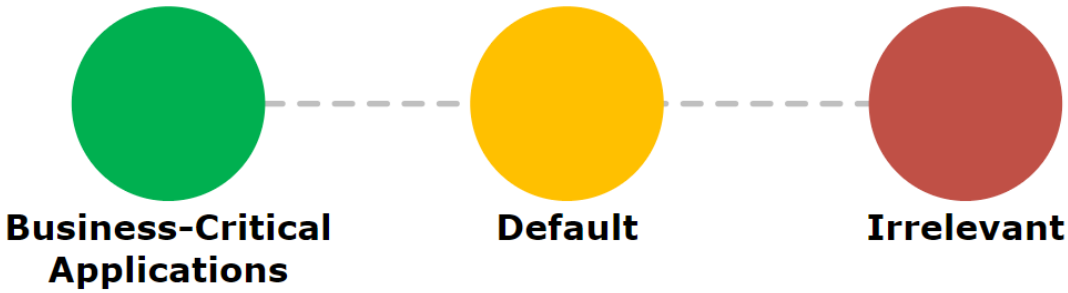

Figura 24 importancia del tráfico (Network Academy,2023)

- Aplicaciones de Negocio Critico:

Aplicaciones que soportan directamente el negocio Deberían ser clasificados por mercado y tratados en consecuencia.

- Por defecto

Estas aplicaciones son usadas recurrentemente, pero no son de suma importancia para el negocio, ej: Email, Navegación por internet etc, Pueden ser tratadas con el mejor esfuerzo.

- Irrelevantes

Estas aplicaciones no soportan directamente el negocio, son orientadas al consumo, estas puedes ser tratadas bajo el mejor esfuerzo. (NetworkAcademy, 2023)

4.3.6. El Framework de QOS

Qos en SD-WAN no es solo una característica o una herramienta, es un framework que para tener QOS optimo utiliza múltiples herramientas:

- Clasificación y Marcado: Esta etapa implica identificar y categorizar los distintos tipos de tráfico que fluyen a través de la red, debido a que el tráfico es marcado con una etiqueta que indica su nivel de prioridad o importancia para la organización en este caso como ejemplo, el tráfico de voz puede ser marcado como prioritario sobre el tráfico de correo electrónico. (NetworkAcademy, 2023)
- Control de Tráfico, Modelado y Descarte: En esta etapa, se aplican políticas para controlar el flujo de tráfico garantizando que se cumpla con los requisitos de calidad de

servicio. Se puede usar técnicas basadas en limitación de velocidad (policing), la regulación del flujo (shaping) y el descarte selectivo de paquetes en caso de congestión.

- Gestión de Congestión: Aquí se maneja la mejora de los periodos de congestión en la red ya que se incluye el uso de algoritmos de programación de colas para priorizar ciertos tipos de tráfico sobre otros, se implementa políticas de equidad para garantizar que todos los usuarios tengan un acceso justo a los recursos de red.
- Herramientas Específicas de Plataforma/Interfaz: Se trata de incluir características y funcionalidades específicas proporcionadas directamente por el proveedor de SD-WAN para optimizar el rendimiento y la calidad de servicio en su plataforma, se puede incluir técnicas como el enrutamiento basado en cada aplicación, la selección dinámica de enlaces y la optimización del tráfico, sin embargo la configuración de QoS en Cisco SD-WAN no siempre se realiza siguiendo el orden en el que las diversas herramientas y capacidades interactúan.. (NetworkAcademy, 2023)

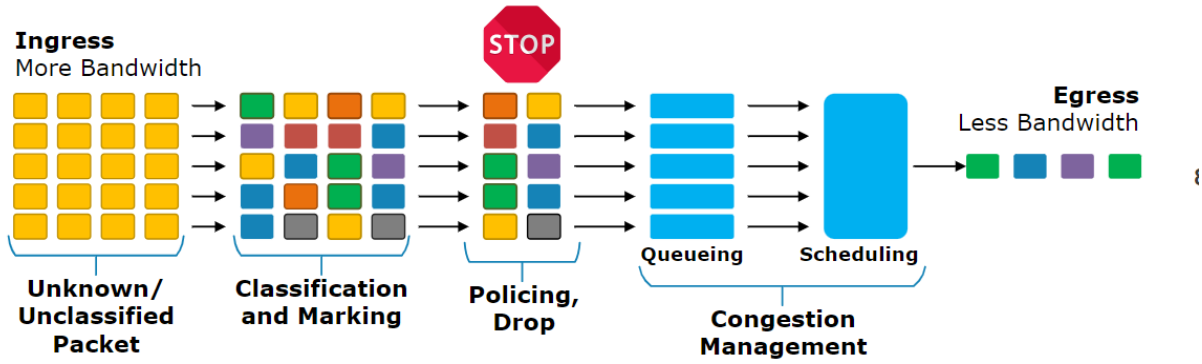

Figura 25 El Framework de QOS (NetworkAcademy, 2023)

4.4. Comparación de arquitecturas y soluciones WAN

La arquitectura de red empresarial ha dependido históricamente de tecnologías como Multiprotocol Label Switching (MPLS) para construir redes de área amplia, utilizando conexiones privadas y conmutación de capas multiprotocolo, sin embargo, la aparición de las redes de área amplia definidas por software (SD-WAN) plantea un desafío significativo a este enfoque tradicional (Prensario, 2023)

El MPLS ha sido un estándar de la industria para mantener y supervisar los recursos de red, ofreciendo conexiones sólidas y confiables, sin embargo, las empresas están explorando la funcionalidad de SD-WAN, que permite la agregación de múltiples circuitos para ejecutar

aplicaciones y servicios de manera confiable y segura a través de conexiones públicas a Internet y la necesidad constante de más ancho de banda y capacidad impulsa esta transición, ya que adquirir tecnología MPLS puede resultar lento y costoso (Prensario, 2023).

En algunos casos, SD-WAN no reemplaza completamente a MPLS de inmediato ya que las empresas pueden adoptar SD-WAN de manera incremental, comenzando con la implementación de recursos como conectividad complementaria para sucursales más pequeñas, posteriormente, pueden aumentar su inversión en SD-WAN, equilibrando gradualmente el entorno hacia la nube, y el enrutamiento basado en aplicaciones permite un control flexible del tráfico, utilizando tanto SD-WAN como WAN tradicional para contribuir a la red general (Prensario, 2023).

La adopción de SD-WAN aporta beneficios significativos a las redes empresariales, la ventaja clave radica en la capacidad de agregar nuevos dispositivos perimetrales y aplicaciones a la red de manera más rápida y económica en comparación con las redes WAN tradicionales ofreciendo la ventajas para un control centralizado de la red, permitiendo la administración eficiente de cada aplicación y conexión desde un único panel con una significativa mejora en el rendimiento de las aplicaciones, la mayor supervisión del uso de datos y la posibilidad de ofrecer una red más segura son ventajas adicionales asociadas con SD-WAN (Prensario, 2023).

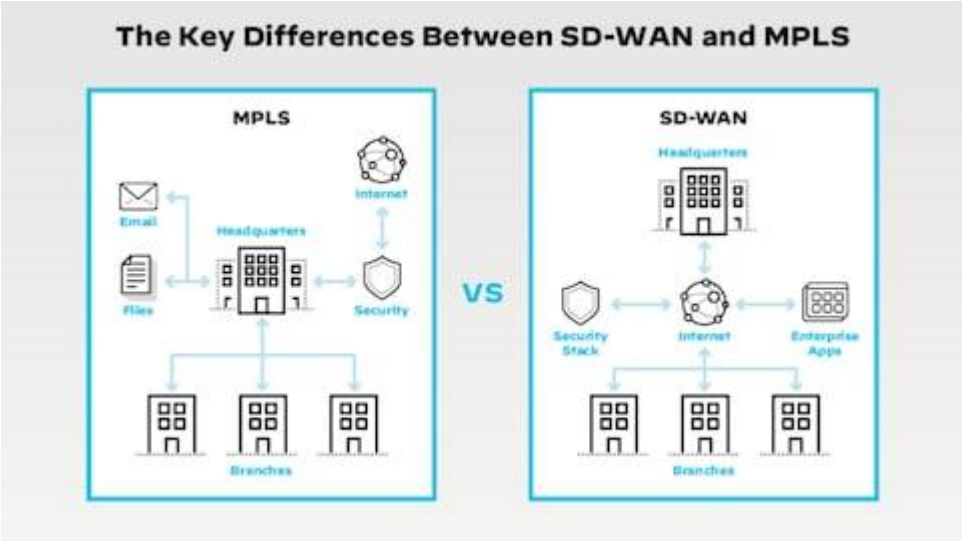

Figura 26 MPLS vs SDWAN (Prensario, 2023).

La importancia de SD-WAN para las empresas actuales radica en su capacidad para mirar hacia el futuro y adaptarse a un entorno empresarial en constante evolución tomando muy en

cuenta la agilidad para agregar nuevos servicios y ubicaciones de manera rentable es fundamental para el crecimiento, y la compatibilidad con implementaciones SaaS respalda la creciente importancia de la nube con una baja inversión operativa requerida en comparación con las conexiones de red privadas tradicionales, SD-WAN ofrece un riesgo bajo y una recompensa potencialmente alta, la elección del proveedor adecuado es crucial, y soluciones como la red SD-WAN totalmente administrada, de esta forma están diseñadas para maximizar la eficiencia de la red y cumplir con las necesidades en constante cambio de las empresas (Prensario, 2023).

4.5. Herramientas de simulación

Los simuladores de red son herramientas informáticas diseñadas para recrear entornos de redes informáticas de manera virtual, los cuales cuentan con una gran gama de características, a continuación, las más destacadas:

- **Práctica sin riesgos:** Los simuladores permiten a los usuarios experimentar con configuraciones de red sin correr el riesgo de dañar equipos o afectar redes reales.
- **Aprendizaje interactivo:** Los simuladores proporcionan un entorno interactivo donde los usuarios pueden experimentar con diferentes configuraciones de red, protocolos y tecnologías.
- **Costo-efectividad:** La implementación de una red de prueba en un entorno físico puede ser costosa y requerir hardware adicional.
- **Disponibilidad de recursos:** Los simuladores a menudo incluyen una amplia gama de dispositivos de red y tecnologías que pueden ser difíciles o costosas de obtener en un entorno físico.

Existen varios programas gratuitos que podemos instalar en nuestras computadoras nos permiten crear redes complejas y simular su funcionamiento como si fuera en el mundo real. Sin embargo, es importante tener en cuenta que, al ser gratuitos, algunas características especiales pueden estar limitadas o no estar disponibles en su totalidad.

También, con el uso de ciertos dispositivos o funcionalidades avanzadas, es posible que necesitemos adquirir licencias de pago. Aunque con varias restricciones, estas herramientas

siguen siendo muy importantes para detectar y corregir problemas potenciales antes de implementar nuestras configuraciones en entornos de producción, a continuación, algunas de las más usadas:

4.5.1. Cisco Packet Tracer

Es uno de los simuladores de redes más populares y completos disponibles, lo desarrollo Cisco, es muy utilizado y recomendado por la misma empresa para realizar pruebas con sus productos, como routers, switches, hubs y servidores, es fácil de usar y gratuita, esto que lo hace accesible para una amplia gama de usuarios.

Este programa se centra en el estudio y la comprensión del switching y routing en el sistema operativo Cisco IOS, utilizado en los routers de Cisco, esta herramienta es ideal para usuarios que están comenzando en el mundo de las redes y desean familiarizarse con los conceptos básicos de la configuración de dispositivos de red. Sin embargo, para configuraciones más avanzadas como MPLS o superiores, Packet Tracer no cuenta realmente con la capacidad de desarrollo, ya que carece de algunas opciones de configuración avanzadas que ofrecen otros simuladores más completos.(Javier Jiménez, 2024)

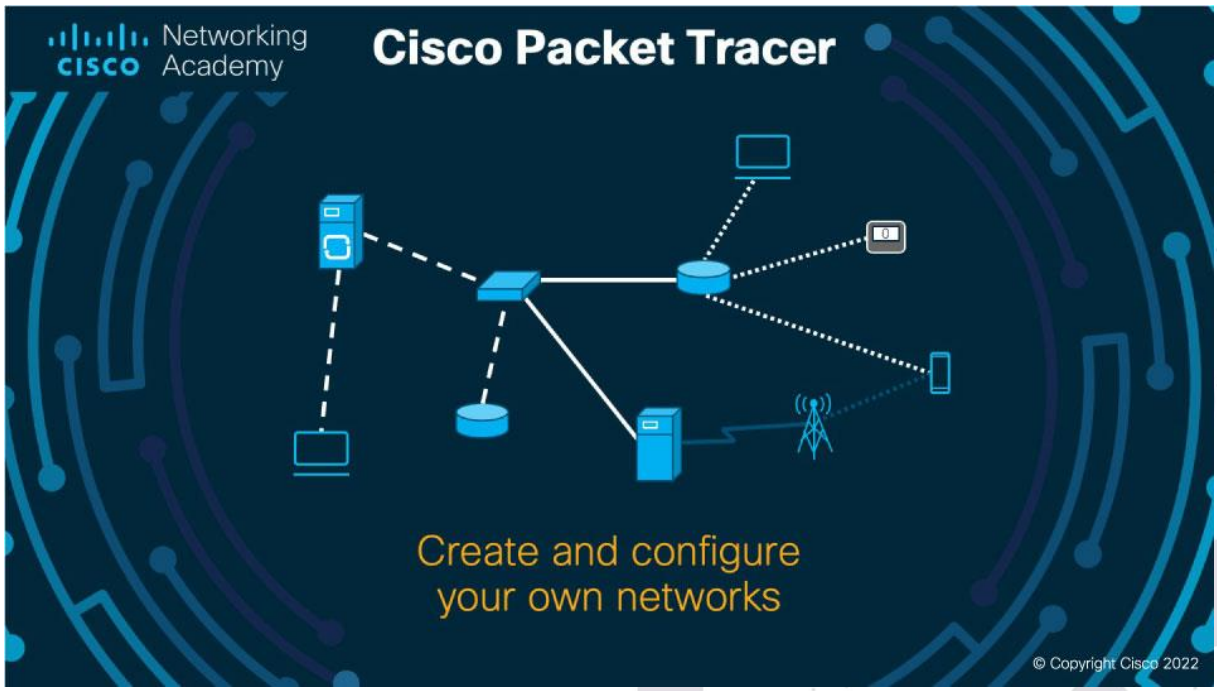

Figura 27 Cisco Packet Tracer (Cisco Netacad, 2020)

4.5.2. GNS3

Una herramienta de simulación de código abierto la cual está diseñada para crear entornos de red más avanzados de manera fácil y precisa.

GNS3 utiliza módulos como Dynamips, VirtualBox y Qemu para ofrecer una experiencia realista con diferentes sistemas operativos de routers y dispositivos de red, una de las ventajas es que es compatible con sistemas operativos Windows, Linux y macOS, lo que lo hace accesible para una amplia variedad de usuarios. (Javier Jiménez, 2024)

Aunque GNS3 puede ser más complicado de configurar que otras herramientas como Cisco Packet Tracer, ofrece funcionalidades avanzadas que lo hacen muy atractivo.

Para simular una red MPLS con GNS3, podemos cargar las imágenes binarias del sistema operativo de Cisco y ejecutarlas de forma emulada. Además, podemos interactuar conectando GNS3 a las tarjetas de red un equipo real para una mayor interacción y realismo.

No es posible la configuración de equipos Cisco Viptela, ya que es una solución de SD-WAN de Cisco que generalmente se implementa en hardware específico de Cisco o en la nube utilizando la plataforma Cisco SD-WAN vManage. (Javier Jiménez, 2024)

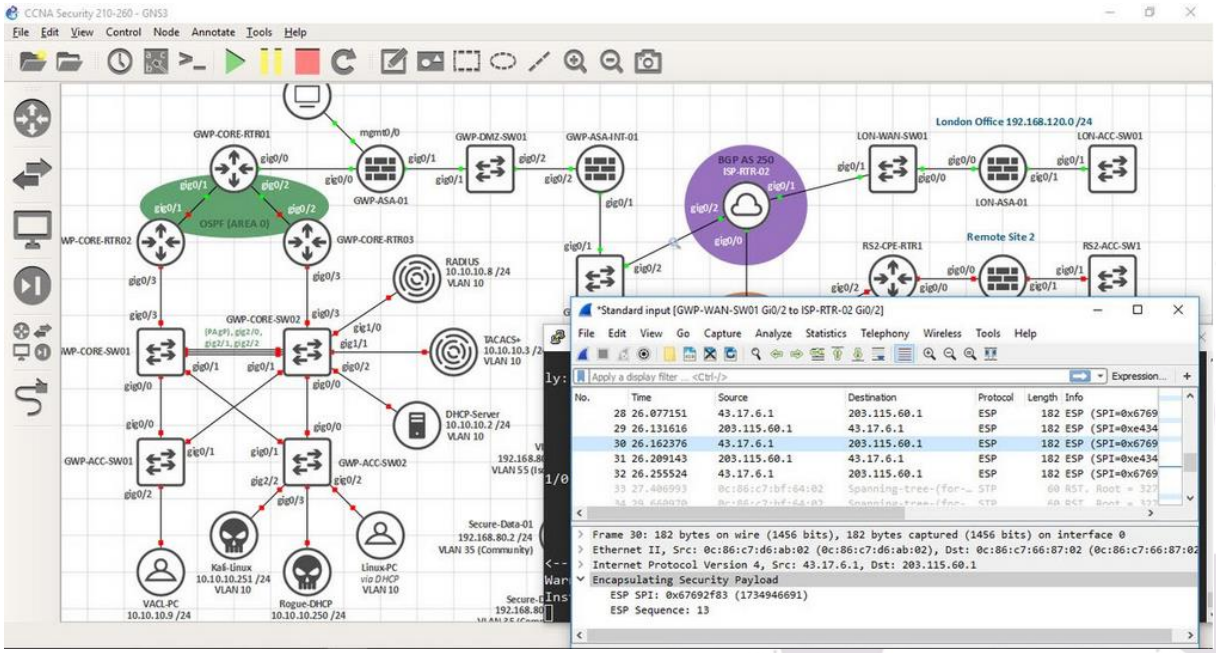

Figura 28 Pantalla Principal GNS3(Javier Jiménez, 2024)

4.5.3. EVE-NG

También conocido como Emulated Virtual Environment Next Generation, dieseñada para emular entornos virtuales de múltiples dispositivos.

A diferencia de otras opciones, Eve-NG ofrece una edición gratuita llamada "Community Edition", así como una versión profesional de pago anual.

Para simular una red MPLS con EVE-NG, es necesario cargar las imágenes binarias del sistema operativo de Cisco y ejecutarlas de forma emulada.

Esta aplicación es compatible con una amplia gama de fabricantes de equipos de red, entre sus características destacadas se incluye el aumento de capacidades de hardware con KVM para un mejor rendimiento, una interfaz HTML5 completa, capacidad para usuarios múltiples que pueden acceder simultáneamente a un mismo proyecto, la posibilidad de importar redes reales para pruebas y la opción de crear imágenes personalizadas con Visio para su integración en Eve-NG.

En una simulación de redes MPLS y Cisco SD-WAN Viptela, Eve-NG ofrece un entorno virtual donde se pueden configurar y probar los dispositivos y protocolos necesarios. Permitiendo diseñar topologías complejas de red, implementar y ajustar configuraciones específicas de MPLS y SD-WAN, y realizar pruebas de conectividad y rendimiento antes de implementar los cambios en un entorno de producción.(Javier Jiménez, 2024)

Figura 29 Pantalla principal EVE-NG (eve-ng.com)

4.5.4. Equipos simulados para MPLS

4.5.4.1. IOURC

Los equipos IOU nos permiten emular dispositivos Cisco con sistemas operativos IOS (Internetwork Operating System) en entornos basados en Unix, de esta forma se realizará una simulación precisa de la funcionalidad y el comportamiento de los dispositivos Cisco en una red MPLS.

- **Emulación de routers y switches:** Con los equipos IOU, se puede emular routers como switches Cisco. En una topología de red MPLS nos permite diseñar redes complejas que incluyan dispositivos como enrutadores PE (Provider Edge), P (Provider), CE (Customer Edge), así como switches de capa de acceso y distribución.(*Community | eveng*, s. f.)
- **Configuración de protocolos MPLS:** Los equipos IOU admiten la configuración de protocolos MPLS como LDP (Label Distribution Protocol), RSVP-TE (Resource Reservation Protocol - Traffic Engineering) y MP-BGP (Multiprotocol Border Gateway Protocol), estos protocolos en los dispositivos emulados son necesarios para establecer la conmutación de etiquetas y la ingeniería de tráfico en la red MPLS. (*Community | eveng*, s. f.)
- **Pruebas de funcionalidad y desempeño**: realizaremos pruebas exhaustivas de la funcionalidad y el rendimiento de una red MPLS simulada donde configuraremos escenarios de prueba para evaluar el comportamiento de la red bajo diferentes condiciones y cargas de tráfico, permitiendo identificar y aplicar reglas y funciones de Calidad de servicio dentro de las VPNs creadas. ((*Community | eveng*, s. f.)
- **Compatibilidad con otros dispositivos:** Se puede interactuar con otros dispositivos emulados, como equipos de monitoreo de red, sistemas de gestión y servidores, con esto realizaremos el diseño de la topología de red MPLS completa y realista incluyendo todos los componentes necesarios para su funcionamiento. (*Community | eveng*, s. f.)

4.5.4.2. Tipos de dispositivos IOU

- **IOU L2 (Layer 2):** Están diseñados para emular switches Cisco en la capa 2 del modelo OSI, de esta forma permiten la emulación de características y protocolos de

conmutación de capa 2, como VLANs, STP (Spanning Tree Protocol), EtherChannel, troncalización de enlaces. A su vez se puede simular la configuración y el funcionamiento de switches Cisco Catalyst y otros dispositivos de conmutación de capa 2 en EVE-NG , además son útiles para diseñar y probar topologías de red que incluyan segmentación de VLAN, configuración de troncales, configuración de VLAN nativa, y otras funcionalidades específicas de conmutación de capa 2.(Cisco Admin, 2020)

- **IOU L3 (Layer 3):** Estas imágenes de IOU están diseñadas para emular routers Cisco en la capa 3 del modelo OSI, Permiten la emulación de características y protocolos de enrutamiento de capa 3, como OSPF, EIGRP, BGP, RIP, IPv4 e IPv6, y muchas otras características de enrutamiento. Se puede simular la configuración y el funcionamiento de routers Cisco ISR (Integrated Services Routers) y otros dispositivos de enrutamiento de capa 3 en EVE-NG , serán ampliamente útiles para diseñar y probar topologías de red que incluyan configuraciones de enrutamiento complejas, configuración de políticas de enrutamiento, configuración de VPN, y otras funcionalidades específicas de enrutamiento de capa 3. (Cisco Admin, 2020).

5. Metodología

Para el desarrollo de este proyecto de titulación, partimos inicialmente con la profundización de los temas de calidad de servicio y cómo se implementaría. Se ha realizado el estudio de varios trabajos desarrollados en base a la implementación de calidad de servicio en redes MPLS, calidad de servicio en SD-WAN y calidad de servicio en VPNs y así, se ha desarrollado de forma teórica una gran metodología para implementar QoS en dichas redes, además de valorar mucho los estándares de Internet detallando las limitaciones, requerimientos y ventajas cuando QoS se aplique en cada una de las redes y clases de servicios.

La metodología aplicada en este proyecto se fundamenta en dos partes fundamentales: la cuantitativa, que se emplea para verificar el comportamiento de cada una de las redes y clases de servicios al implementar QoS utilizando los equipos proporcionados, de esta forma se permite recopilar datos estadísticos en tiempo real, junto con el monitoreo de las redes simuladas y su posterior análisis.

También se emplea una metodología exploratoria para llevar a cabo un estudio exhaustivo de cada una de las redes y, de esta manera, identificar las mejores prácticas para optimizar y mejorar el rendimiento de dichas redes de esta forma se proporcionará una visión más completa del comportamiento de las redes de área extensa MPLS y SD-WAN, con el propósito de mejorar una topología establecida y garantizar un uso efectivo de las políticas de QoS.

Este documento puede servir como un manual detallado, donde se describe paso a paso cada uno de los procesos para implementar una red MPLS y sus VPNs, o una red SD-WAN utilizando simuladores que abarquen la demanda de uso para poder aprovisionar los mecanismos de QoS. Hemos estructurado el trabajo de la siguiente manera:

- **Sección 5.1:** proporciona una explicación de las herramientas a utilizar en este caso la simulación donde se realizará la configuración e implementación de una red MPLS.
- **Sección 5.2:** proporciona una guía metodológica para la implementación de una red MPLS en EVE-NG.
- **Sección 5.2**: ofrece una guía metodológica para la implementación de servicios con diferentes niveles de calidad dentro de una red MPLS y sus VPNs.
- **Sección 5.3:** presenta una guía metodológica para la implementación de una red SD-WAN.

- **Sección 5.4:** detalla una guía metodológica para la implementación de servicios con diferentes niveles de calidad dentro de una red SD-WAN.

5.1. Tabla comparativa de Herramientas de simulación

Tabla 1 Comparativa herramientas de simulación (fuente: Autor)

Aspecto	Packet Tracer	GNS3	EVE-NG	VIRL	NetSim
Versiones Pagas	No	Sí (GNS3 WorkBench)	Sí (EVE-NG Professional)	Sí (Cisco Modeling Labs)	Sí (Boson NetSim)
Versiones Gratuitas	Sí	Sí	Sí	No	No
Uso de Recursos	Bajo	Alto	Alto	Alto	Medio a Alto
Configuración de Equipos MPLS	Básica	Completa	Completa	Completa	Básica
Configuración de Equipos Cisco Viptela	No	No	No	No	No

Se ha decidido usar la herramienta de simulación de redes **EVE-NG** debido a las siguientes ventajas sobre los otros simuladores

Flexibilidad: EVE-NG permite una mayor flexibilidad en la configuración de redes, con la interacción de los usuarios al tener más control sobre cómo diseñan y despliegan sus redes MPLS Y SD-WAN.(Rejón, 2019)

Amplia compatibilidad: EVE-NG es compatible con una amplia gama de dispositivos y sistemas operativos, especialmente Cisco Viptela, donde se puede integrar dispositivos y tecnologías de diferentes fabricantes en una sola red simulada, este punto es muy importante para la implementación de redes MPLS y SD-WAN, debido a que se involucra una variedad de equipos de red. (Rejón, 2019)

Personalización avanzada: EVE-NG ofrece opciones avanzadas de personalización y configuración, permitiendo ajustar y optimizar las redes MPLS y SD-WAN de acuerdo con las necesidades específicas. (Rejón, 2019)

Comunidad activa: EVE-NG cuenta con una comunidad activa de usuarios y desarrolladores que comparten recursos, consejos y soluciones para configurar redes MPLS y SD-WAN y resolver problemas comunes.

Escalabilidad: EVE-NG es altamente escalable para manejar redes grandes y complejas, una herramienta ideal para simular redes MPLS -SD-WAN a gran escala con múltiples dispositivos y enlaces. (Rejón, 2019)

5.2. Implementación de dispositivos IOU en EVE-NG

5.2.1. Requisitos previos:

Descargar las imágenes de IOU necesarias se debe tener en cuenta que las imágenes no se distribuyen de manera gratuita y deben ser obtenidas legalmente a través de Cisco.

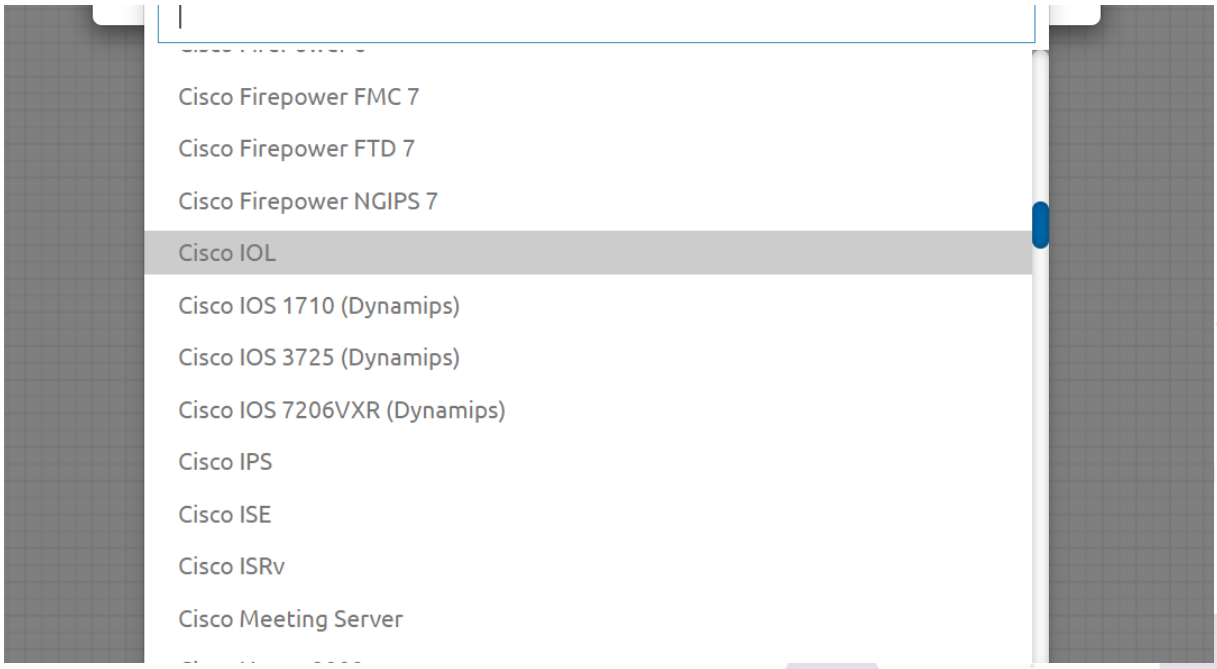

Figura 30 Equipos de EVE-NG (Autor,2024)

- Convertir la imagen a formato compatible con EVE-NG debido a que las imágenes de IOU generalmente vienen en formatos que no son compatibles directamente con EVE-NG.

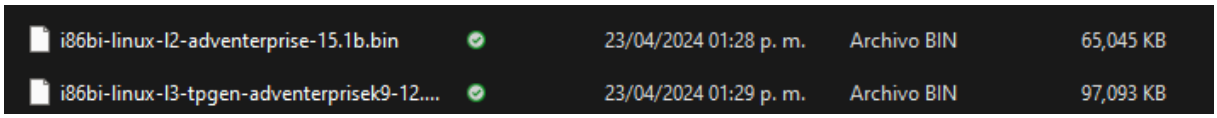

Figura 31 Archivos de IOU con formato original (Autor,2024)

- Subir la imagen a EVE-NG: Una vez que se tenga la imagen en el formato adecuado, se puede subir al servidor EVE-NG esto puede ser mediante un traspaso FTP.

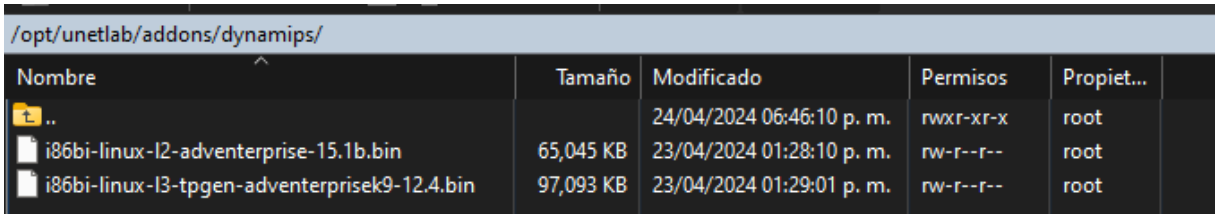

Figura 32 Archivo de IOS dentro del servidor EVE-NG(Fuente: Autor)

- Permisos de uso de los dispositivos en EVE-NG

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

Figura 33 Permiso de uso de dispositivos (Fuente: Autor)

- Se Debe licenciar cada nodo IOU, con la licencia gratuita generada en la máquina virtual

```
**************************************************************************
Create the license file $HOME/.iourc with this command:
 echo -e '[license]\neve-ng = 972f30267ef51616;' | tee $HOME/.iourc

The command adds the following text to $HOME/.iourc:
[license]
eve-ng = 972f30267ef51616;
```

Figura 34 Licenciamiento de nodos (Fuente: Autor)

- **Crear un nodo en EVE-NG utilizando la imagen IOU**: Después de que la imagen haya sido cargada con éxito, se puede crear nodos en la topología de red utilizando las imágenes cargadas ingresando a la sección de diseño de red en EVE-NG, seleccionamos la imagen IOU.

Figura 35 Carga de Dispositivos (Fuente: Autor)

5.3. Implementación de una red MPLS con VPNs en EVE-NG

Como parte fundamental de este proyecto es muy importante tomar en cuenta la seguridad de la comunicación dentro de la red MPLS, por ende, es muy importante generar redes privadas virtuales. Dentro de la sección 4.1.6 se contempló y se detalló el cómo funciona una VPN dentro de una red MPLS, aquí se detallara la configuración para tráfico de paquetes, en equipos Cisco y para ello nos basaremos en los ejemplos desarrollados en el libro *"MPLS Implementation Status Advanced MPLS VPNs"*(Tomsu, 2001) ya que se ha tomado en cuenta los requisitos mínimos como software IP,software ATM MPE(WAN DTE) ya que este configura LANs sobre ATM.

En el caso de Cisco, por ser la tecnología de los equipos que vamos a utilizar en los equipos de borde, y en los equipos del núcleo de la red, es obligatorio ejecutar los protocolos MPLS y CEF (Cisco Express Forwarding), de la misma forma el protocolo BGP para proporcionar los servicios de VPN.

5.3.1. Diagrama de implementación

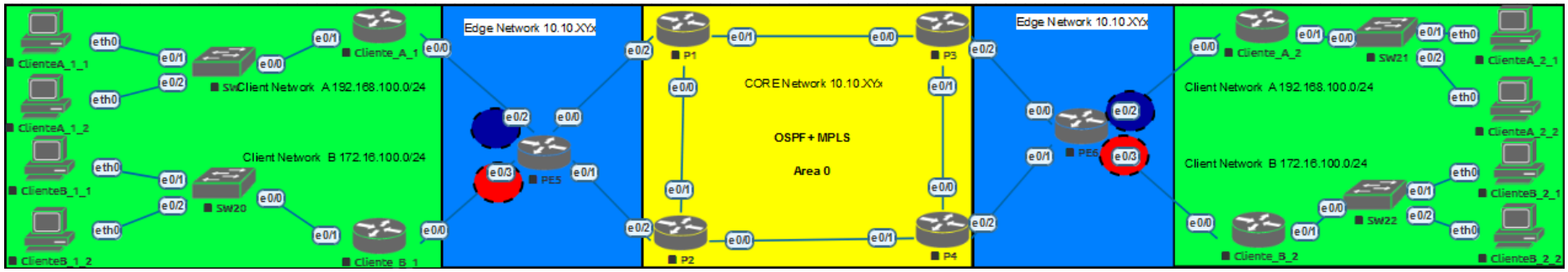

Figura 36 Diagrama de Red (Fuente: Autor)

5.3.2. Configuración y Verificación

5.3.2.1. Dispositivos

Se utilizarán Routers marca Cisco modelo IOU L3 con el ***firmware i86bi-linux-l3-tpgen-adventerprisek9-12.4,*** los cuales tendrán los siguientes nombres:

- Router #1(core): **P1**
- Router #2(core): **P2**
- Router #3(core): **P3**
- Router #4(core): **P4**
- Router #5(Borde): **PE5**
- Router #6(Borde): **PE6**
- Router #7(Cliente): **Cliente A_1**
- Router #8(Cliente): **Cliente B_1**
- Router #9(Cliente): **Cliente A_2**
- Router #10(Cliente): **Cliente B_2**
- Host # 1: **Cliente A_1_1**
- Host # 2: **Cliente A_1_2**
- Host # 3: **Cliente A_2_1**
- Host # 4: **Cliente A_2_2**
- Host # 5: **Cliente B_1_1**
- Host # 6: **Cliente B_1_2**
- Host # 7: **Cliente B_2_1**
- Host # 8: **Cliente B_2_2**

5.3.2.2. Conexiones Físicas

En el diagrama actual, se encuentran 4 routers de CORE, que constituyen una red en forma de anillo, cada router está equipado con tres conexiones Ethernet.

- Conexión A entre P1, P2 y P3
- Conexión B entre P2, P1 y P4
- Conexión C entre P3, P1 y P4

- Conexión D entre P4, P2 y P3

Se cuenta con 2 equipos de borde conectados hacia los P con un cable Ethernet.

- Conexión E entre PE5, P1 y P2
- Conexión F entre PE6, P3 y P4

Se cuenta con 4 routers de cliente que estarán conectados hacia los routers de borde con un cable Ethernet

- Conexión G entre PE5 y CA1
- Conexión H entre PE5 y CB1
- Conexión I entre PE6 y CA2
- Conexión J entre PE6 y CB2

Se conectan 2 host a cada equipo Cliente para la interconexión de las VPNs

- Conexión K entre CA1 y Cliente A_1_1
- Conexión L entre CA1 y Cliente A_1_2
- Conexión M entre CB1 y Cliente B_1_1
- Conexión N entre CB1 y Cliente B_1_2
- Conexión O entre CA2 y Cliente A_2_1
- Conexión P entre CA2 y Cliente A_2_2
- Conexión Q entre CB2 y Cliente B_2_1
- Conexión R entre CB2 y Cliente B_2_2

5.3.2.3. Redes

Para garantizar cierta independencia, hemos configurado redes diferentes para las conexiones entre routers y las conexiones en la red local detalladamente todas las interfaces utilizarán máscaras de 24 bits 192.168.xy.x/24 donde 'x' representa el número asignado al router y y al enlace, aunque en el caso de las conexiones entre equipos de CORE no serían necesarias tantas direcciones 10.10.10.xy , Además, configuraremos en cada router P y PE una interfaz virtual con la dirección 10.10.xy.z, donde 'x' representa el número asignado al router de origen

y 'y' al router de destino siempre el router con el número más bajo será el origen y z será el octeto final del enlace, estas interfaces tendrán máscaras de 32 bits (rutas de host).

- Redes Virtuales (loopback 0)
    - **P1:** IP 1.1.1.1/32
    - **P2:** IP 2.2.2.2/32
    - **P3:** IP 3.3.3.3/32
    - **P4:** IP 4.4.4.4/32
    - **PE5:** IP 5.5.5.5/32
    - **PE6:** IP 6.6.6.6/32
- Redes de Conexión punto a punto
    - Redes P1: 10.10.12.0/30,10.10.13.0/30,10.10.15.0/30
    - Redes P2: 10.10.12.0/30,10.10.24.0/30,10.10.25.0/30
    - Redes P3: 10.10.13.0/30,10.10.34.0/30-10.10.36.0/30
    - Redes P4: 10.10.24.0/30,10.10.34.0/30,10.10.46.0/30
    - Redes P5: 10.10.15.0/30,10.10.25.0/30,192.168.15.0/24,172.16.15.0/24
    - Redes P6: 10.10.36.0/30,10.10.46.0/30,192.168.16.0/24-172.16.16.0/24
    - Red Clientes_A: 192.168.100.0/24
    - Red Clientes_B: 172.16.100.0/24

5.3.2.4. Protocolos

- **Ip cef:** Para funcionamiento de MPLS
- **OSPF:** Enrutamiento en redes de Core y borde
- **MPLS:** Habilitar en las interfaces P-PE
- **iBGP:** Enrutamiento PE-PE
- **Ebgp:** Enrutamiento PE-Clientes

5.3.2.5. VPNs

Cada router cliente conectado a los Router PE se asocia con una VRF asignada en los routers PE.

- **VRF CLIENTE_A**: Red Clientes_A

- VRF CLIENTE_B: Red Clientes_B

Se configuran tablas de enrutamiento para cada VPN con un *Route distinguisher* (RD) y un *Route target (RD).*

- VRF CLIENTE_A: rd 100:1 rt 100:1
- VRF CLIENTE_B: rd 100:2 rt 100:2

5.3.3. Scripts de configuración

5.3.3.1. Las siguientes configuraciones son creadas por el autor.

- Configuración Router P1

```
enable
configure terminal
hostname P1
no ip domain-lookup
ip cef
mpls ip
interface loopback 0
ip address 1.1.1.1 255.255.255.255
no shutdown
interface ethernet 0/0
ip address 10.10.12.1 255.255.255.252
no shutdown
interface ethernet 0/1
ip address 10.10.13.1 255.255.255.252
no shutdown
interface ethernet 0/2
ip address 10.10.15.1 255.255.255.252
no shutdown

mpls ldp router-id loopback 0

Router ospf 1
router-id 1.1.1.1
network 1.1.1.1 0.0.0.0 area 0
network 10.10.12.0 0.0.0.3 area 0
network 10.10.13.0 0.0.0.3 area 0
network 10.10.15.0 0.0.0.3 area 0
mpls ldp autoconfig
```

- Configuración Router P2

```
enable
configure terminal
hostname P2
no ip domain-lookup
ip cef
mpls ip
interface loopback 0
ip address 2.2.2.2 255.255.255.255
no shutdown
interface ethernet 0/0
ip address 10.10.24.1 255.255.255.252

no shutdown
interface ethernet 0/1
ip address 10.10.12.2 255.255.255.252

no shutdown
interface ethernet 0/2
ip address 10.10.25.1 255.255.255.252
no shutdown


mpls ldp router-id loopback 0
Router ospf 1
router-id 2.2.2.2
network 2.2.2.2 0.0.0.0 area 0
network 10.10.12.0 0.0.0.3 area 0
network 10.10.24.0 0.0.0.3 area 0
network 10.10.25.0 0.0.0.3 area 0
mpls ldp autoconfig
```

- Configuración Router P3

```
enable
configure terminal
hostname P3
no ip domain-lookup
ip cef
mpls ip
interface loopback 0
ip address 3.3.3.3 255.255.255.255
no shutdown
interface ethernet 0/0
ip address 10.10.13.2 255.255.255.252
```

```
no shutdown
interface ethernet 0/1
ip address 10.10.34.1 255.255.255.252

no shutdown
interface ethernet 0/2
ip address 10.10.36.1 255.255.255.252
no shutdown

mpls ldp router-id loopback 0
Router ospf 1
router-id 3.3.3.3
network 3.3.3.3 0.0.0.0 area 0
network 10.10.13.0 0.0.0.3 area 0
network 10.10.34.0 0.0.0.3 area 0
network 10.10.36.0 0.0.0.3 area 0
mpls ldp autoconfig
```

- Configuración Router P4

```
enable
configure terminal
hostname P4
no ip domain-lookup
ip cef
mpls ip
interface loopback 0
ip address 4.4.4.4 255.255.255.255
no shutdown
interface ethernet 0/0
ip address 10.10.34.2 255.255.255.252

no shutdown
interface ethernet 0/1
ip address 10.10.24.2 255.255.255.252

no shutdown
interface ethernet 0/2
ip address 10.10.46.1 255.255.255.252
no shutdown

mpls ldp router-id loopback 0
Router ospf 1
router-id 4.4.4.4
network 4.4.4.4 0.0.0.0 area 0
network 10.10.24.0 0.0.0.3 area 0
network 10.10.34.0 0.0.0.3 area 0
```

```
network 10.10.46.0 0.0.0.3 area 0
mpls ldp autoconfig
```

- Configuración Router PE5

```
enable
configure terminal
hostname PE5
no ip domain-lookup
ip cef
interface loopback 0
ip address 5.5.5.5 255.255.255.255
no shutdown
interface ethernet 0/0
ip address 10.10.15.2 255.255.255.252

no shutdown
interface ethernet 0/1
ip address 10.10.25.2 255.255.255.252

no shutdown


mpls ldp router-id loopback 0
Router ospf 1
network 5.5.5.5 0.0.0.0 area 0
network 10.10.15.0 0.0.0.3 area 0
network 10.10.25.0 0.0.0.3 area 0
mpls ldp autoconfig


vrf definition Cliente_1
address-family ipv4
 rd 65200:1
 route-target export 65200:1
 route-target import 65200:2
!
!
vrf definition Cliente_2
address-family ipv4
 rd 65300:1
 route-target export 65300:1
 route-target import 65300:2
!
!
router bgp 65100
 no synchronization
 bgp router-id 5.5.5.5
 bgp log-neighbor-changes
```

```
 neighbor 6.6.6.6 remote-as 65100
 neighbor 6.6.6.6 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 6.6.6.6 activate
  neighbor 6.6.6.6 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf Cliente_1
  no synchronization
  neighbor 192.168.15.2 remote-as 65200
  neighbor 192.168.15.2 activate
 exit-address-family
 !
 address-family ipv4 vrf Cliente_2
  no synchronization
  neighbor 172.16.15.2 remote-as 65300
  neighbor 172.16.15.2 activate
 exit-address-family
!

interface ethernet 0/2
vrf forwarding Cliente_1
ip address 192.168.15.1 255.255.255.252
no shutdown

interface ethernet 0/3
vrf forwarding Cliente_2
ip address 172.16.15.1 255.255.255.252
no shutdown
```

- Configuración Router PE6

```
enable
configure terminal
hostname PE6
no ip domain-lookup
ip cef

interface loopback 0
ip address 6.6.6.6 255.255.255.255
no shutdown
interface ethernet 0/0
ip address 10.10.36.2 255.255.255.252

no shutdown
```

```
interface ethernet 0/1
ip address 10.10.46.2 255.255.255.252


no shutdown
mpls ip
mpls ldp router-id loopback 0

Router ospf 1

network 6.6.6.6 0.0.0.0 area 0
network 10.10.36.0 0.0.0.3 area 0
network 10.10.46.0 0.0.0.3 area 0
mpls ldp autoconfig

show ip ospf database
show ip ldp neig
traceroute 6.6.6.6 source lo0

vrf definition Cliente_1
address-family ipv4
 rd 65200:2
 route-target export 65200:2
 route-target import 65200:1
!
!
vrf definition Cliente_2
address-family ipv4
 rd 65300:2
 route-target export 65300:2
 route-target import 65300:1
!
!


router bgp 65100
 no synchronization
 bgp router-id 6.6.6.6
 bgp log-neighbor-changes
 neighbor 5.5.5.5 remote-as 65100
 neighbor 5.5.5.5 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf Cliente_1
```

```
  no synchronization
  neighbor 192.168.16.2 remote-as 65200
  neighbor 192.168.16.2 activate
 exit-address-family
 !
 address-family ipv4 vrf Cliente_2
  no synchronization
  neighbor 172.16.16.2 remote-as 65300
  neighbor 172.16.16.2 activate
 exit-address-family
!

interface Ethernet0/2
 vrf forwarding Cliente_1
 ip address 192.168.16.1 255.255.255.252

interface Ethernet0/3
 vrf forwarding Cliente_2
 ip address 172.16.16.1 255.255.255.252
```

- Configuración Router Cliente_A1

```
enable
configure terminal
hostname Cliente_A1
no ip domain-lookup

interface ethernet 0/0
ip address 192.168.15.2 255.255.255.252
no shutdown

interface Ethernet0/1.100
 encapsulation dot1Q 100
 ip address 192.168.100.1 255.255.255.0

router bgp 65200
neighbor 192.168.15.1 remote-as 65100
network 192.168.100.0 mask  255.255.255.0

!
```

- Configuración Router Cliente_A2

```
enable
configure terminal
hostname Cliente_A2
no ip domain-lookup

interface ethernet 0/0
ip address 192.168.16.2 255.255.255.252
no shutdown

interface Ethernet0/1.200
 encapsulation dot1Q 200
 ip address 192.168.200.1 255.255.255.0

router bgp 65200
neighbor 192.168.16.1 remote-as 65100
network 192.168.200.0 mask  255.255.255.0
```

- Configuración Router Cliente_B1

```
enable
configure terminal
hostname Cliente_B1
no ip domain-lookup

interface ethernet 0/0
ip address 172.16.15.2 255.255.255.252
no shutdown

interface Ethernet0/1.100
 encapsulation dot1Q 100
 ip address 172.16.100.1 255.255.255.0


router bgp 65300
neighbor 172.16.15.1 remote-as 65100
network 172.16.100.0 mask  255.255.255.0
```

- Configuración Router Cliente_B2

```
enable
configure terminal
hostname Cliente_B2
no ip domain-lookup
```

```
interface ethernet 0/0
ip address 172.16.16.2 255.255.255.252
no shutdown

interface Ethernet0/1.200
 encapsulation dot1Q 200
 ip address 172.16.200.1 255.255.255.0


router bgp 65300
neighbor 172.16.16.1 remote-as 65100
network 172.16.200.0 mask  255.255.255.0
```

5.3.4. Configuración de técnicas QOS en red MPLS

Las empresas tienen como uno de sus principales objetivos la implementación de políticas de negocio, especialmente en lo que respecta al uso del ancho de banda abarcando dispositivos como firewalls, enrutadores en VPN y almacenamiento, con el fin de respaldar decisiones específicas:

- **Clasificación de usuarios según su jerarquía en la red:** Se establecen distintos niveles de acceso y privilegios para usuarios basados en su posición dentro de la estructura de la empresa.
- **Gestión de aplicaciones críticas:** Se asignan niveles de prioridad a las aplicaciones fundamentales para el funcionamiento del negocio, garantizando que reciban la mayor parte del ancho de banda disponible.
- **Asignación de ancho de banda según necesidades individuales:** Se delimita el uso de ancho de banda de acuerdo con los requerimientos específicos de cada usuario, adaptándose a sus demandas particulares.
- **Gestión del tráfico de voz, video y datos:** Se administra el flujo de tráfico en las redes WAN y LAN, asegurando un rendimiento óptimo para cada tipo de datos y comunicación.
- **Control del flujo de tráfico interno y externo:** Se establecen políticas para regular el tráfico que circula tanto dentro como fuera de la red empresarial, evitando congestiones y garantizando un funcionamiento fluido de las comunicaciones.

Para lograr estos objetivos, es importante configurar la red con políticas que regulen el tráfico entrante, permitiendo programar la transmisión de este según los servicios requeridos asegurando un control efectivo del flujo de datos y evitando la degradación de la calidad de las comunicaciones.

En el contexto de una topología de red configurada para una VPN, se pueden implementar diversas políticas de Calidad de Servicio (QoS) con el fin de clasificar adecuadamente los paquetes de datos según la aplicación correspondiente garantizando que los niveles de servicio sean establecidos y mantenidos correctamente, incluso cuando las condiciones de la red varíen.

Es importante identificar los puntos de acceso donde se concentra el mayor consumo de ancho de banda, categorizándolo por aplicación y en base a este análisis crear políticas por grupos de usuarios y horarios, lo que asegura una gestión eficiente de la congestión de datos y garantizar el cumplimiento de los Acuerdos de Nivel de Servicio (SLA), mediante la clasificación de paquetes utilizando etiquetas MPLS y PBH, diferenciando las etiquetas según el tipo de servicio requerido.

Las políticas generadas se basarán en:

Para garantizar un flujo de datos eficiente y prevenir la congestión en la red, se implementan varias estrategias:

- **Clasificación del tráfico:** Se clasifica el tráfico según la cabecera IPv4 o la interfaz, basándose en los Acuerdos de Nivel de Servicio (SLA) y las cabeceras de capa 3, 4 o 7 del paquete analizado.
- **Configuración de colas de salida:** En cada interfaz, se establecen colas de salida para organizar el flujo de datos.
- **Implementación de esquemas de encolamiento:** Se utilizan esquemas como CBWFQ (Class-Based Weighted Fair Queuing), WFQ (Weighted Fair Queuing) y WRR (Weighted Round Robin) para determinar el orden de transmisión de los paquetes en función de la cola de salida.
- **Monitoreo y gestión de colas de salida:** Se monitorean las colas de salida y se implementa el algoritmo RED (Random Early Detection) para anticipar problemas de

congestión descartando paquetes de forma anticipada, evitando la congestión antes de que ocurra y proporcionando una solución proactiva.

5.3.5. Marcación y Clasificación de paquetes:

Según lo descrito en el marco teórico, se establece que la clasificación de paquetes es la parte más importante en las políticas de QOS, por lo cual se ha establecido la siguiente tabla:

Tabla 2 Mapeo DSCP para QOS y niveles de servicio (fuente Autor)

DSCP DiffServ	QOS política de nivel	Clase de servicio
EF	6	Premium
AF11-AF12-AF13	5	Platinum
AF21-AF22-AF23	4	Gold
AF31-AF32-AF33	3	Silver
AF41-AF42-AF43	2	Bronze
DE (Discard Elegible)	1	Standard

Después de marcar y clasificar el tráfico, procedemos a marcar los 6 bits del byte DSCP, implementándolo en los equipos de borde junto con la clasificación en los bits EXP de las etiquetas MPLS (E-LSP) o dentro de cada nueva etiqueta (L-LSP), de igual forma el campo EXP y la política de servicio para las VPN del cliente_A:

- Garantizaremos un ancho de banda de 250 Mbps a todo el tráfico de la VPN de presentarse congestión.
- Una cola de máximo 50 paquetes antes de descartar los paquetes siguientes.
- Se asigna un valor de 4 al campo MPLS EXP si los paquetes cumplen los requerimientos de la clase de tráfico asociada.
- En los valores por defecto se incluyen 64 colas para el tráfico que no cumple la regla de la VPN y un tráfico de hasta 30 paquetes en cada cola para descartar los siguientes.

```
class-map match-all Cliente_A
!
policy-map Cliente_A_Policy
 class Cliente_A
    bandwidth 250000
    queue-limit 50 packets
  set mpls experimental 4
 class class-default
    fair-queue 64
    queue-limit 30 packets
```

En los dispositivos del Core P, configuramos el Per-Hop Behavior (PHB) para los bits EXP en las etiquetas MPLS, directamente estableceremos una clase2 que corresponde al valor EXP 4 para asegurar que cualquier tráfico que coincida con esta clase tenga garantizado un ancho de banda mínimo de 250 Mbps.

Reservaremos una cola con capacidad para almacenar hasta 70 paquetes antes de comenzar a descartar los paquetes adicionales que lleguen, definiendo que cuando la cola alcanza su límite de 70 paquetes, los paquetes posteriores serán descartados si no hay suficiente capacidad disponible para manejarlos.

```
class-map match-all Clase2
 match mpls experimental topmost 4
!
policy-map clase_Politica_PHB
 class Clase2
    bandwidth 250000
    queue-limit 70 packets
!
```

Cuando configuramos el redireccionamiento, la tabla asignará el comportamiento por salto apropiado a los paquetes entrantes, así también marcará el paquete saliente según el comportamiento por salto que le corresponda y lo enviará al siguiente salto requerido.

Los mapeos según la tabla 1 para esta configuración serían los siguientes:

Tabla 3 PHB aplicado a EXP (Fuente Autor)

AF1		AF2		AF3	
EXP	PHB	EXP	PHB	EXP	PHB
001	AF11	100	AF21	111	AF31
010	AF12	101	AF22	-	-
011	AF13	110	AF23	-	-

- **Con Expedited Forwarding (EF**) de 5 normalmente usado se garantiza baja latencia, baja pérdida de paquetes y baja variabilidad en el tiempo de tránsito (jitter) lo utilizaremos en aplicaciones sensibles al tiempo, como la voz sobre IP (VoIP) y el video en tiempo real.
- **Con Assured Forwarding (AF)** en base a la tabla 3 en seria AF-21 realizaremos un control más detallado al manejar el tráfico bajo condiciones de congestión.

5.3.6. Control y administración del flujo de datos

Según el ancho de banda asignado y la configuración definida, se restringe el tráfico en diferentes áreas utilizando filtros dentro de cada política, asegurando que el tráfico crítico tenga acceso ilimitado a los recursos de red.

Cada política contiene la información E-LSP o L-LSP para conducir los paquetes a la cola establecida en base al mapeo configurado en el nivel de QOS a continuación base a la tabla se configura los siguiente:

Determinar que cola ingresa primero según el nivel de transmisión y también configuramos la oportunidad de retransmisión de paquetes para cada cola.

Tabla 4 Qos para las clases de servicio (fuente:Autor)

Clase	Nivel	Nivel de retransmisión	Porcentaje en peso
Premium	6	40	100%
Platinum	5	20	40%
Gold	4	16	30%
Silver	3	10	20%
Bronze	2	4	16%
Standard	1	2	5%

5.3.7. Aplicación en dispositivos

- Configuración Routers Cliente

Para configurar QoS en el router Cliente_A1, se definen clases de tráfico basadas en la precedencia IP, priorizando voz, video, navegación web y aplicaciones empresariales para la configuración específica, se crean class-maps para clasificar el tráfico.

```
class-map match-all VOICE
 match ip precedence 5
!
class-map match-all VIDEO
 match ip precedence 4
!
class-map match-all WEB
 match ip precedence 3
!
class-map match-all ENTERPRISE_APP
 match ip precedence 6
```

- Configuración Routers PE

En la configuración actual, notamos que los clientes A y B están conectados a los routers de borde PE5 y PE6, donde cada uno recibe servicios QoS adaptados a diferentes tipos de tráfico, vemos que el cliente A utiliza la interfaz Ethernet 0/2, mientras que el cliente B utiliza la interfaz Ethernet 0/3, estos enlaces con políticas específicas para gestionar su tráfico saliente. Además, hemos etiquetado los paquetes como pertenecientes a Cliente_A y Cliente_B respectivamente.

Por otro lado, el Cliente B tiene una política interna de QoS que se basa en los bits ToS, donde cada uno de estos paquetes también se asignan con los bits EXP de MPLS en los dispositivos Core y de Borde de la red con lo cual empleamos el comando 'match-all' para asegurarnos de que los paquetes que cumplan con los criterios de Cliente_B sean correctamente gestionados.

```
!
class-map match-all Cliente_B
 match input-interface Ethernet0/3
 class-map match-all Cliente_A
 match input-interface Ethernet0/2
!
!
```

- Configuración Routers P:

En los equipos de núcleo, se pueden manejar hasta 7 clases de tráfico utilizando los 3 bits EXP en la etiqueta MPLS en la configuración establecida definiremos 5 clases, seleccionadas en función del valor de EXP, determinando así los recursos requeridos para cada flujo de tráfico.

```
class-map match-all clase1
 match mpls experimental topmost 5
class-map match-all clase2
 match mpls experimental topmost 4
class-map match-all clase3
 match mpls experimental topmost 3
```

```
class-map match-all clase4
 match mpls experimental topmost 2
class-map match-all clase5
 match mpls experimental topmost 1
```

- Políticas de Servicio para QOS en los Router Cliente

Se crea un policy-map para asignar ancho de banda y establecer prioridades: 30% para voz, 20% para video, 10% para navegación y 35% para aplicaciones empresariales, detallando directamente sobre el policy-map que incluye fair-queue para el tráfico por defecto.

```
policy-map QoS_POLICY
 class VOICE
  priority percent 30
  set ip precedence 5
 class VIDEO
  bandwidth percent 20
  set ip precedence 4
 class WEB
  bandwidth percent 10
  set ip precedence 3
 class ENTERPRISE_APP
  bandwidth percent 35
  set ip precedence 6
 class class-default
  fair-queue
```

- Políticas de Servicio para VPN_Cliente_A

Para las políticas de servicio en la VPN_Cliente_A en los switches PE, especificamos que se garantizará un mínimo de ancho de banda de 256 Megabytes en caso de congestión, con el tráfico de la VPN Cliente_A, la cola de esta clase puede contener hasta 50 paquetes antes de comenzar a descartar.

Basándonos en la Clase 4, asignamos un valor de 4 a los bits EXP en la etiqueta MPLS para cumplir con las políticas de esta clase de tráfico.

También configuraremos una política para la clase por defecto, incluida dentro del policy-map Cliente_A_Policy, la cual en dicha clase tiene configuradas 64 colas para el tráfico que no cumpla con los criterios de conformidad y las clases asociadas al policy map y asi cada cola podrá contener un máximo de 30 paquetes antes de que se empiece a descartar paquetes por el mecanismo normal.

```
class-map match-all Cliente_A
!
policy-map Cliente_A_Policy
 class Cliente_A
    bandwidth 2500
    queue-limit 50 packets
  set mpls experimental 4
 class class-default
    fair-queue 64
    queue-limit 30 packets
```

- Políticas de Servicio para VPN_Cliente_B

Para las políticas de servicio en la VPN_Cliente_B en los switches PE, especificamos que se garantizará un mínimo de ancho de banda de 128 Megabytes en caso de congestión, con el tráfico de la VPN Cliente_B, la cola de esta clase puede contener hasta 50 paquetes antes de comenzar a descartar.

Basándonos en la Clase 3, asignamos un valor de 3 a los bits EXP en la etiqueta MPLS para cumplir con las políticas de esta clase de tráfico.

También configuraremos una política para la clase por defecto, incluida dentro del policy-map Cliente_A_Policy, la cual en dicha clase tiene configuradas 64 colas para el tráfico que no cumpla con los criterios de conformidad y las clases asociadas al policy map y asi cada cola podrá contener un máximo de 30 paquetes antes de que se empiece a descartar paquetes por el mecanismo normal.

```
policy-map Cliente_B_Policy
 class Cliente_A
    bandwidth 1280
    queue-limit 50 packets
  set mpls experimental 3
 class class-default
    fair-queue 64
    queue-limit 30 packets
```

- Políticas de Servicio para los dispositivos P

Se configuran las políticas de servicio para las clases de tráfico establecidas.

Para la Clase1, se garantiza un mínimo de ancho de banda de 512 Mbps, y la cola reservada para este tráfico puede contener hasta 80 paquetes antes de iniciar el descarte de igual forma, la clase por defecto tendrá 64 colas hash configuradas, con una capacidad máxima de 40 paquetes por cola antes de comenzar a descartarlos.

Para la Clase2, se garantiza un mínimo de ancho de banda de 256 Mbps, y la cola reservada para este tráfico puede contener hasta 60 paquetes antes de iniciar el descarte de igual forma, la clase por defecto tendrá 64 colas hash configuradas, con una capacidad máxima de 40 paquetes por cola antes de comenzar a descartarlos.

Para la Clase3, se garantiza un mínimo de ancho de banda de 128 Mbps, y la cola reservada para este tráfico puede contener hasta 40 paquetes antes de iniciar el descarte de igual forma, la clase por defecto tendrá 64 colas hash configuradas, con una capacidad máxima de 40 paquetes por cola antes de comenzar a descartarlos.

Para la Clase4, se garantiza un mínimo de ancho de banda de 64 Mbps, y la cola reservada para este tráfico puede contener hasta 30 paquetes antes de iniciar el descarte de igual forma, la clase por defecto tendrá 64 colas hash configuradas, con una capacidad máxima de 40 paquetes por cola antes de comenzar a descartarlos.

Para la Clase5, se garantiza un mínimo de ancho de banda de 64 Mbps, y la cola reservada para este tráfico puede contener hasta 20 paquetes antes de iniciar el descarte de igual forma, la clase por defecto tendrá 64 colas hash configuradas, con una capacidad máxima de 40 paquetes por cola antes de comenzar a descartarlos.

```
policy-map clase_PHB_Policy
 class clase1
    bandwidth 5120
    fair-queue
    queue-limit 80 packets
 class clase2
    bandwidth 2560
    fair-queue
    queue-limit 60 packets
 class clase3
    bandwidth 1280
    fair-queue
    queue-limit 40 packets
 class clase4
    bandwidth 640
    fair-queue
    queue-limit 40 packets
 class clase5
    bandwidth 320
    fair-queue
    queue-limit 40 packets
!
```

- Implementación de políticas de QOS

Las interfaces específicas asignadas en los routers Cliente: Ethernet0/0 y Ethernet0/1.100, son interfaces de salida, la política de QoS se aplica a estas interfaces para asegurar que el tráfico saliente crítico reciba el tratamiento adecuado, mejorando la calidad del servicio.

```
interface Ethernet0/0
 service-policy output QoS_POLICY
!
interface Ethernet0/1.100
 service-policy output QoS_POLICY
```

Las interfaces específicas asignadas en los routers PE: Ethernet0/2 para cliente_A y Ethernet0/3 para cliente_B, son interfaces de salida, la política de QoS se aplica a estas interfaces para asegurar que el tráfico saliente crítico reciba el tratamiento adecuado, mejorando la calidad del servicio MPLS.

```
interface Ethernet0/2
 service-policy output Cliente_A_Policy
!
interface Ethernet0/3
 service-policy output Cliente_B_Policy
```

Las interfaces específicas asignadas en los routers P: Ethernet0/2, son interfaces de salida, la política de QoS se aplica a estas interfaces para asegurar que el tráfico saliente crítico reciba el tratamiento adecuado, mejorando la calidad del servicio MPLS.

```
interface Ethernet0/2
 service-policy output clase_PHB_Policy
```

5.3.8. Implementación de dispositivos SDWAN-Viptela en EVE-NG

5.3.8.1. Requisitos previos:

- Descarga las imágenes de SD-WAN necesarias se debe tener en cuenta que las imágenes no se distribuyen de manera gratuita y deben ser obtenidas legalmente a través de Cisco.

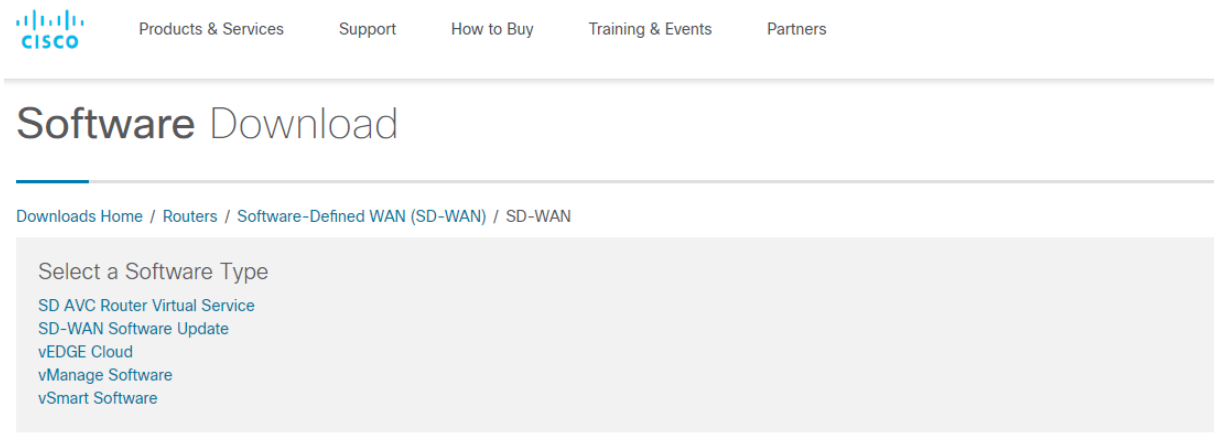

Figura 37 Pagina de descarga Cisco (Cisco, 2024)

- Convertir la imagen a formato compatible con EVE-NG debido a que las imágenes de SD-WAN generalmente vienen en formatos que no son compatibles directamente con EVE-NG.

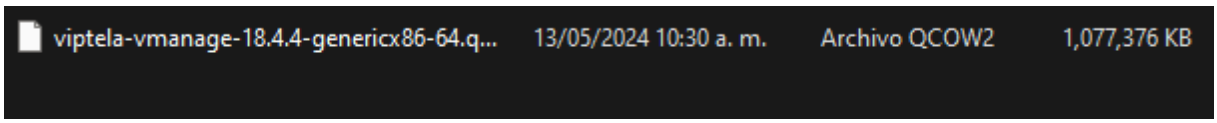

Figura 38 Archivos de Viptela con formato original (Autor,2024)

- Subir la imagen a EVE-NG: Una vez que se tenga la imagen en el formato adecuado, se puede subir al servidor EVE-NG esto puede ser mediante un traspaso FTP

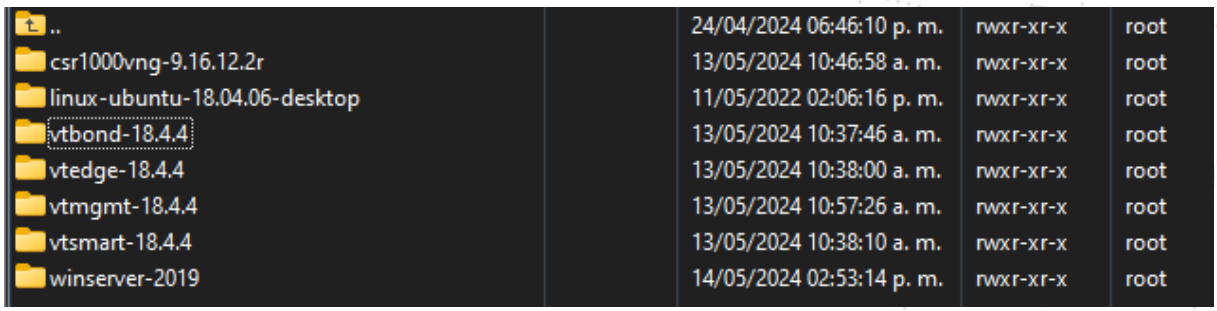

Figura 39 Archivo de SD-WAN Viptela dentro del servidor EVE-NG(Fuente: Autor)

- Permisos de uso de los dispositivos en EVE-NG

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

Figura 40 Permiso de uso de dispositivos (Fuente: Autor)

- Se Debe renombrar cada equipo viptela dentro del servidor

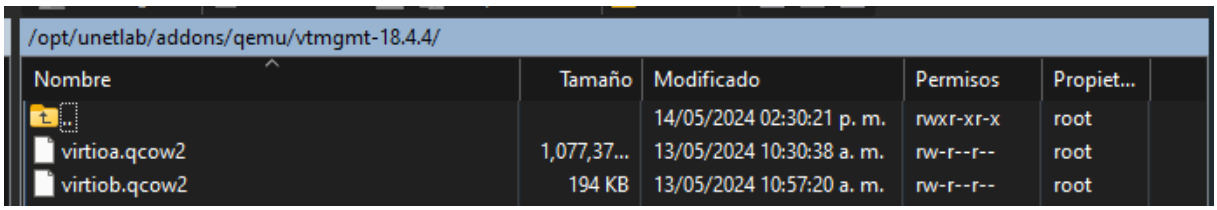

Figura 41 Archivos de disco de los equipos SD-WAN de nodos (Fuente: Autor)

- Se verifican los archivos transformados en disco para los nodos en EVE-NG

```
root@eve-ng:/opt/unetlab/addons/qemu# ls
arubacx-10.13.1000              vtbond-18.4.4  vtsmart-18.4.4
csr1000vng-9.16.12.2r           vtedge-18.4.4  winserver-2019
linux-ubuntu-18.04.06-desktop   vtmgmt-18.4.4
root@eve-ng:/opt/unetlab/addons/qemu# cd vtbond-18.4.4/
root@eve-ng:/opt/unetlab/addons/qemu/vtbond-18.4.4# ls
virtioa.qcow2
root@eve-ng:/opt/unetlab/addons/qemu/vtbond-18.4.4#
```

Figura 42 Archivos de Nodos transformados a disco(autor,2014)

- **Crear un nodo en EVE-NG utilizando la imagen SD-WAN Viptela**: Después de que la imagen haya sido cargada con éxito, se puede crear nodos en la topología de red utilizando las imágenes cargadas ingresando a la sección de diseño de red en EVE-NG, seleccionamos la imagen deseada.

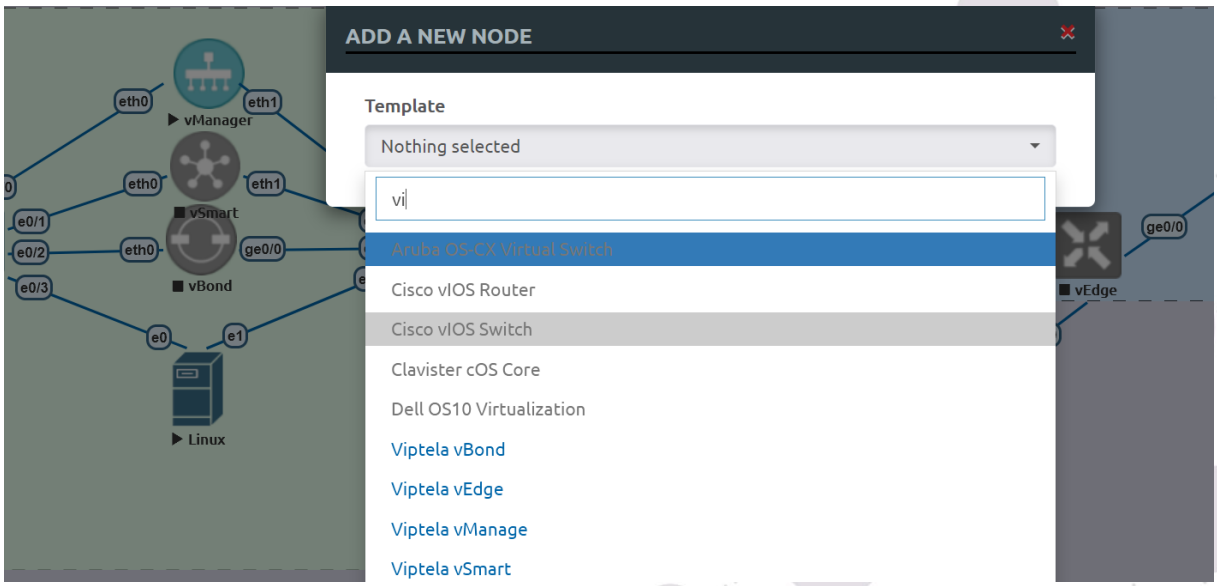

Figura 43 Carga de Dispositivos Viptela (Fuente: Autor)

5.4. Implementación de una red SD-WAN en EVE-NG

La red SD-WAN con Viptela interconecta varios sitios utilizando MPLS y redes WAN Ethernet para garantizar una conectividad eficiente y confiable, debido a que la tecnología SD-WAN de Viptela optimiza el enrutamiento del tráfico, se asegura que los datos se envíen por la ruta más adecuada en función de las condiciones de la red en tiempo real.

En la siguiente configuración, los enlaces MPLS proporcionaran una conectividad segura y de alta velocidad, mientras que las redes WAN de internet generan una conectividad rentable y de alto rendimiento, con la combinación de estos dos tipos de enlaces permite a la red SD-WAN adaptarse a las necesidades específicas de cada aplicación y optimizar el rendimiento de la red en general.

5.4.1. Diagrama de implementación

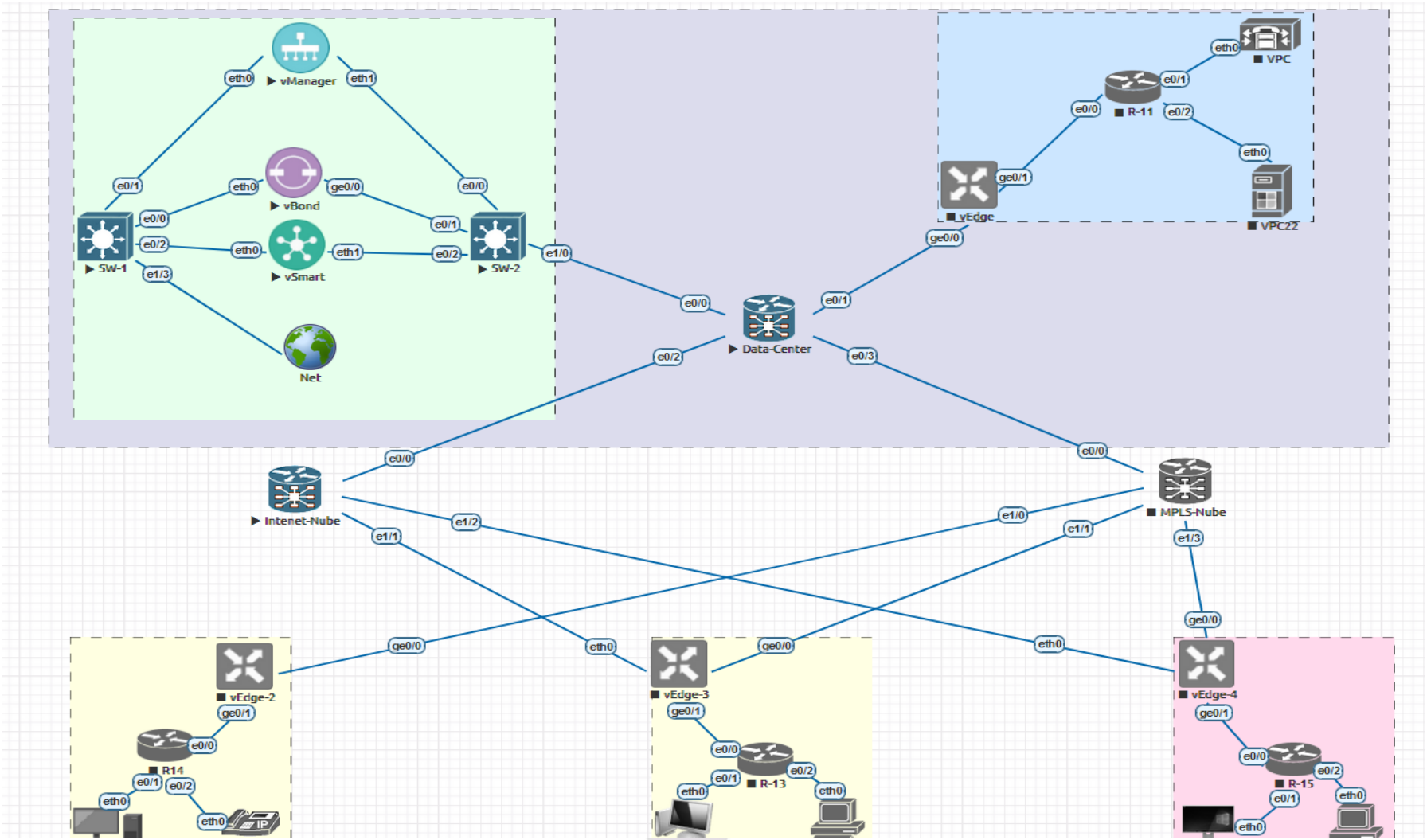

Figura 44 Diagrama de Red SD-WAN (Fuente: Autor)

5.4.2. Configuración y Verificación

5.4.2.1. Dispositivos

Para la simulación de la conectividad WAN y MPLS se utilizarán Routers marca Cisco modelo IOU L3 con el ***firmware i86bi-linux-l3-tpgen-adventerprisek9-12.4.***

Para la simulación de la conectividad de la red interna del Data Center y los dispositivos de administración de RED-SDWNA se utilizarán switchs marca Cisco modelo IOU L2 con el ***firmware i86bi-linux-l2-adventerprise-15.1b.bin.***

Para la simulación de la conectividad de la red de dispositivos finales se utilizarán Routers marca Cisco modelo IOU L3 con el ***firmware i86bi-linux-l3-tpgen-adventerprisek9-12.4.***

- Vmanage (DC): **Vmanage**
- vSmart(DC): **vSmart**
- vBond (DC): **vBond**
- Switch1 (DC): **SW-1**
- Switch2 (DC): **SW-2**
- Server Linux (DC): **Windows server 2019**
- vEdge1(Sitio 1): vEdge1
- vEdge2(Sitio 2): vEdge1
- vEdge3(Sitio 3): vEdge1
- CSR(Sitio 4): CSR_1
- Router 1(DC): Router_DC
- Router 2(Nube de Internet): **Internet-Nube**
- Router 3(Red MPLS): **MPLS-Nube**
- Router #4(Sitio 1): **site-1**
- Router #5(Sitio 2): **site-2**
- Router #6(Sitio 3): **site-3**
- Router #7(Sitio 4): **site-4**
- Router #8(Sitio 5): **site-5**
- Host # 1: **Cliente site-1**
- Host # 2: **Cliente site-2**
- Host # 3: **Cliente site-3**

- Host # 4: **Cliente site-4**
- Host # 5: **Cliente site-5**

5.4.2.2. Conexiones Físicas

En el diagrama actual dentro del Data Center para la conexión LAN y administración de los dispositivos SD-WAN, se encuentran 2 switch de CORE, que constituyen una red ende administración, cada switch está equipado con cuatro conexiones Ethernet.

- Conexión A1 entre Sw-1, vManager
- Conexión B2 entre Sw-2, vManager
- Conexión A2 entre Sw-1, vSmart
- Conexión B2 entre Sw-2, vSmart
- Conexión A3 entre Sw-1, vBond
- Conexión B3 entre Sw-2, vBond
- Conexión A4 entre Sw-1, Servidor de Datos
- Conexión B4 entre Sw-2, Servidor de Datos

En el diagrama actual, se encuentran 3 routers para Interconexión **WAN**, que constituyen una externa para la conexión con los equipos de borde, cada router está equipado con cuatro conexiones Ethernet.

- Conexión C entre Router_DC, SW1, Internet_Nube, vEdge1 y MPLS-Cloud
- Conexión D entre Internet Cloud, vEdge2, vEdge3, CSR, vEdge4
- Conexión E entre MPLS Cloud, vEdge2, vEdge3, CSR, vEdge4

Se cuenta con 4 routers de cliente que estarán conectados hacia los vEdge de borde con un cable Ethernet

- Conexión F entre vEdge1 y Site_1
- Conexión G entre vEdge2 y Site_2
- Conexión H entre vEdge3 y Site_3
- Conexión I entre CSR y Site_4
- Conexión J entre vEdge4 y Site_5

5.4.2.3. Redes

Se ha realizado la configuración de interfaces en cada dispositivo

- Router_DC

Tabla 5 Configuración interfaces router DC(Fuente: Autor)

Interface	IP address	Mascara de Subred
E0/0	10.10.10.1	255.255.255.0
E0/1	20.10.10.2	255.255.255.252
E0/2	100.10.10.1	255.255.255.252
E0/3	200.10.10.1	255.255.255.252

- Router_MPLS

Tabla 6 Configuración interfaces router DC(Fuente: Autor)

Interface	IP address	Mascara de Subred
E0/0	200.10.10.2	255.255.255.252
E1/0	200.10.11.1	255.255.255.252
E1/1	200.10.12.1	255.255.255.252
E1/2	200.10.13.1	255.255.255.252
E1/3	200.10.14.1	255.255.255.252

- Router_Internet

Tabla 7 Configuración interfaces router Internet (Fuente: Autor)

Interface	IP address	Mascara de Subred
E0/0	100.10.10.1	255.255.255.252
E1/0	100.10.11.1	255.255.255.252
E1/1	100.10.12.1	255.255.255.252
E1/2	100.10.13.1	255.255.255.252
E1/3	100.10.14.1	255.255.255.252

- Configuración Router Data-Center

```
hostname Data-Center
!
interface Ethernet0/0
ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/1
ip address 20.10.10.2 255.255.255.252
!
interface Ethernet0/2
ip address 100.10.10.1 255.255.255.252
!
interface Ethernet0/3
ip address 200.10.10.1 255.255.255.252
!
router ospf 1
passive-interface default
no passive-interface Ethernet0/2
network 10.10.10.0 0.0.0.254 area 0
network 20.10.10.0 0.0.0.3 area 0
network 100.10.10.0 0.0.0.3 area 0
network 200.10.10.1 0.0.0.3 area 0
!
router bgp 65001
bgp log-neighbor-changes
redistribute ospf 1
neighbor 30.1.1.1 remote-as 65001
!
```

- Configuración Router MPLS

```
hostname MPLS
!
interface Ethernet0/0
ip address 200.10.10.2 255.255.255.252
!
interface Ethernet0/1
ip address 200.10.11.1 255.255.255.252
ip ospf network point-to-point
!
interface Ethernet0/2
ip address 200.10.12.1 255.255.255.252
ip ospf network point-to-point
!
interface Ethernet0/3
ip address 200.10.13.1 255.255.255.252
ip ospf network point-to-point
!
interface Ethernet1/0
ip address 200.10.11.1 255.255.255.252
ip ospf network point-to-point
!
router ospf 1
network 200.10.10.0 0.0.0.3 area 0
network 200.10.11.0 0.0.0.3 area 0
network 200.10.12.0 0.0.0.3 area 0
network 200.10.13.0 0.0.0.3 area 0
network 200.10.14.0 0.0.0.3 area 0
```

- Configuración Router MPLS

```
hostname Internet
!
no ip domain lookup
ip cef
!
interface Ethernet0/0
ip address 100.10.10.1 255.255.255.252
!
interface Ethernet0/1
ip address 100.10.11.1 255.255.255.252
!
interface Ethernet0/2
ip address 100.10.12.1 255.255.255.252
!
interface Ethernet0/3
ip address 100.10.13.1 255.255.255.252
!
interface Ethernet1/0
ip address 100.10.14.1 255.255.255.252
!
ip route 10.10.10.0 255.255.255.252 100.10.10.1
```

- Configuración de Vmanage

Se realiza la configuración de los siguientes parámetros:

- **Hostname**: vManage1
- **System-IP**: 10.10.10.12
- **SiteID**: 1
- **Organization**: "DCH sdwan""
- **Vbond Address:** 10.10.10.4
- **Timezone:** America/Guayaquil

```
      config
      !
      system
      host-name vManage1
      system-ip 10.10.10.12
      site-id 1
      organization-name "DCH sdwan"
      clock timezone America/Guayaquil
      vbond 10.10.10.4
      !
      commit
      !
      vpn 0
      no interface eth0
      interface eth1
      ip address 10.10.10.2/24
      tunnel-interface
      allow-service all
      allow-service netconf
      allow-service sshd
      no shut
      ip route 0.0.0.0/0 10.10.10.1
      !
      vpn 512
      interface eth0
      ip address 192.168.100.2/24
      no shut
      !
commit
```

- Ingreso Vmanage

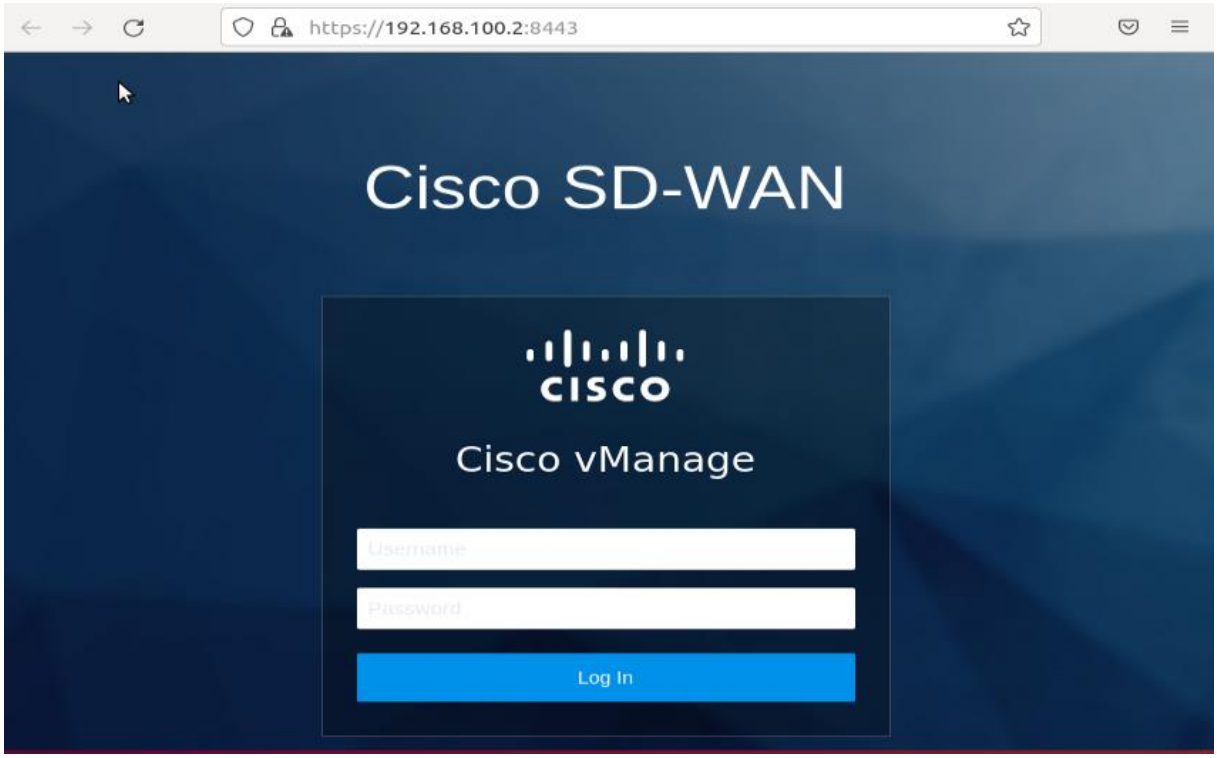

Figura 45 Ingreso Vmanage (fuente: Autor)

- Pantalla Principal Vmanage

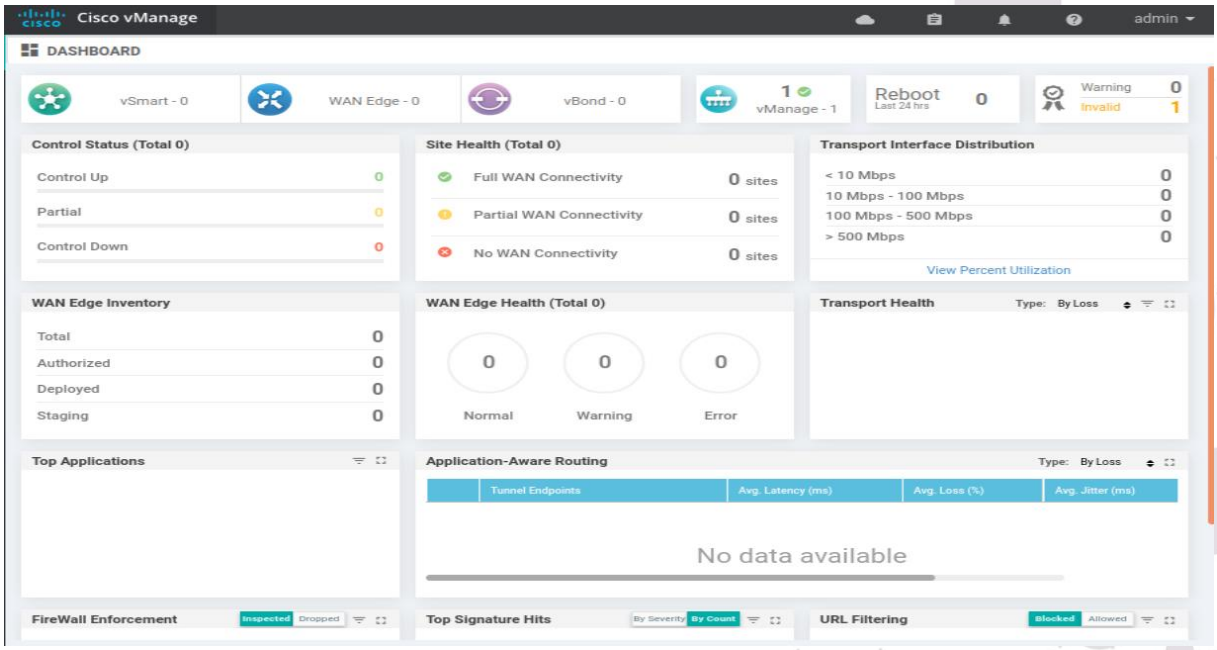

Figura 46 Ingreso pantalla principal Vmanage (fuente: Autor)

- Registro Vmanage

Al ser este la controladora principal se verifica que el dispositivo ya esta ingresado como Controladora.

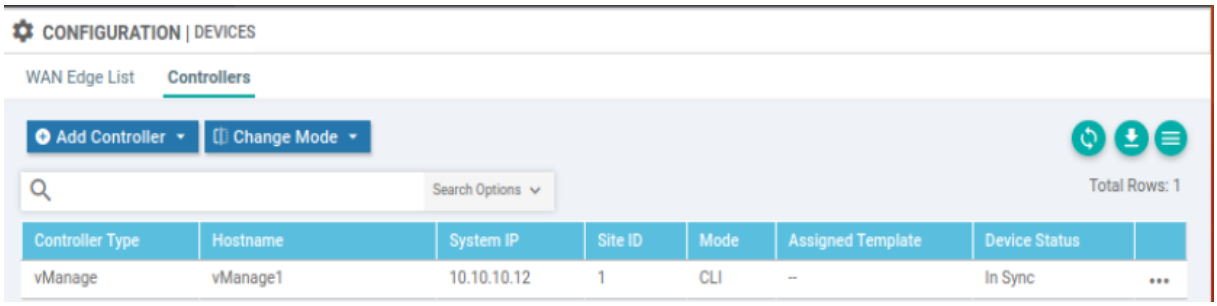

Figura 47 Registro de vManage (Fuente: Autor)

- Configuración de Vbond

Se realiza la configuración de los siguientes parámetros:

- **Hostname**: vBond1
- **System-IP**: 10.10.10.14
- **SiteID**: 1
- **Organization**: "DCH sdwan""
- **Vbond Address:** 10.10.10.4
- **Timezone:** America/Guayaquil

```
config
!
system
host-name vBond1
system-ip 10.10.10.14
site-id 1
organization-name "DCH sdwan"
clock timezone America/Guayaquil
vbond 10.10.10.4 local
```

```
!
vpn 0
no interface eth0
interface ge0/0
ip address 10.10.10.4/24
allow-service netconf
allow-service all
tunnel-interface encapsulation ipsec
allow-service sshd
no shut
ip route 0.0.0.0/0 10.10.10.1
!
vpn 512
interface eth0
ip address 192.168.100.4/24
no shut
!
commit
```

- Registro de Vbond

Se realiza el ingreso dentro de la controladora al Vbond

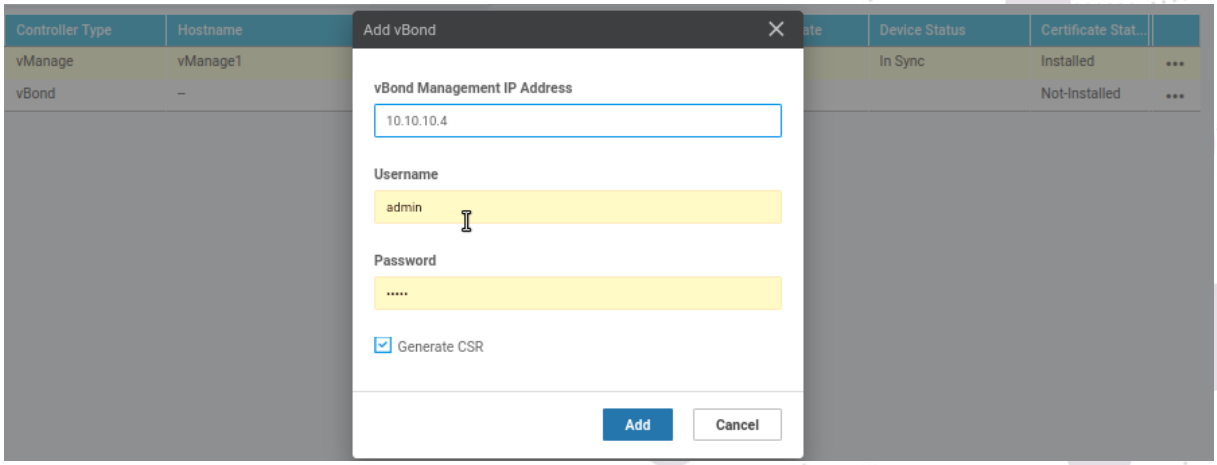

Figura 48 Registro de Vbond (Fuente: Autor)

- Configuración de Vsmart

Se realiza la configuración de los siguientes parámetros:

- **Hostname**: Vsmart1
- **System-IP**: 10.10.10.13
- **SiteID**: 1
- **Organization**: "DCH sdwan""
- **Vbond Address:** 10.10.10.4
- **Timezone:** America/Guayaquil

```
config
!
system
host-name vSmart1
system-ip 10.10.10.13
site-id 1
organization-name "DCH sdwan"
clock timezone America/Guayaquil
vbond 10.10.10.4
!
vpn 0
no interface eth0
interface ge0/0
ip address 10.10.10.3/24
allow-service netconf
allow-service all
tunnel-interface encapsulation ipsec
allow-service sshd
no shut
ip route 0.0.0.0/0 10.10.10.1
!
vpn 512
```

```
interface eth0
ip address 192.168.100.3/24
no shut
!
commit
```

- Registro de Vbond

Se realiza el ingreso de Vsmart dentro de la controladora

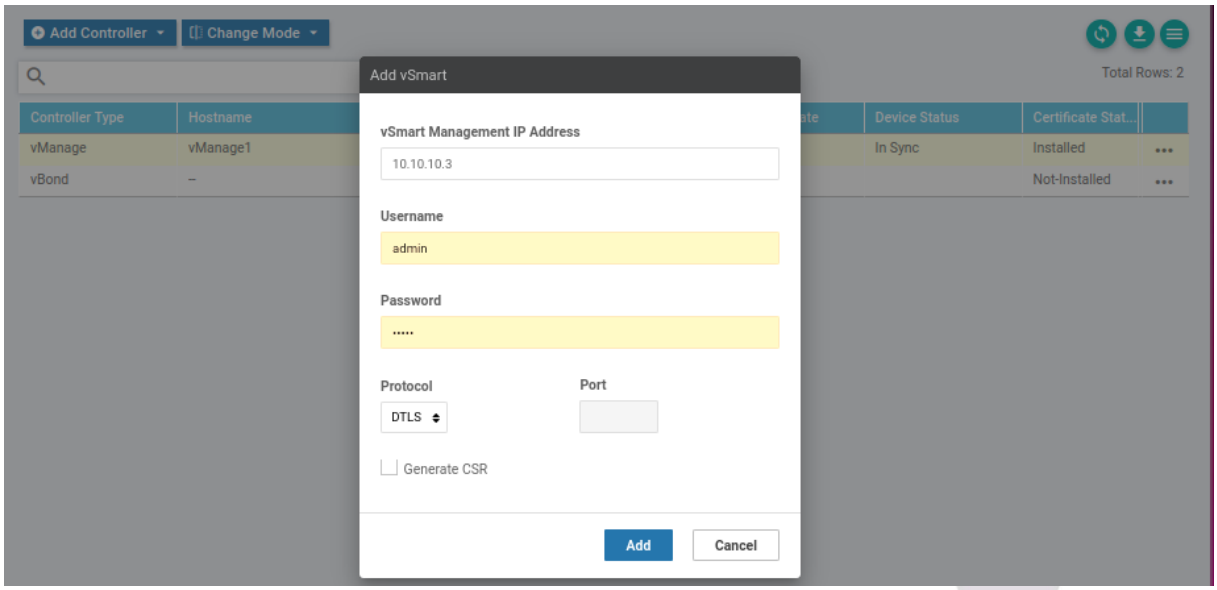

Figura 49 Ingreso Vsmart (Fuente: Autor)

- Configuración de vEdge1

Se realiza la configuración de los siguientes parámetros:

- **Hostname**: vEdge1
- **System-IP**: 20.10.10.2
- **SiteID**: 1
- **Organization**: "DCH sdwan""
- **Vbond Address:** 10.10.10.4
- **Timezone:** America/Guayaquil

```
config
system
host-name vEdge1
system-ip 20.10.10.1
site-id 1
organization-name "DCH sdwan"
clock timezone America/Guayaquil
vbond 10.10.10.4
!
vpn 0
interface ge0/0
ip address 20.10.10.1/24
tunnel-interface
encapsulation ipsec
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 20.10.10.2
vpn 512
interface eth0
ip dhcp-client
no shutdown
commit
```

- Ingreso de vEdge1
    - Se realiza el ingreso de Vedge1 dentro de la controladora para esto es necesario registrar y solicitar tokens directamente de una cuenta Smart de la página del proveedor.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	Assigned Template	
	CSR1000v	CSR-EEA17C51-1201-258B-CEF9-3495...	Token - f5fb4c62bab70...	--	--	--	CLI	--	...
	CSR1000v	CSR-CC450DF7-6AC2-D83B-3E5E-7525...	Token - 79f9c5e14683d...	--	--	--	CLI	--	...
	CSR1000v	CSR-FFEACA92-AD8A-7CC5-9C14-1B4...	Token - a1d593e8a05b...	--	--	--	CLI	--	...
	CSR1000v	CSR-253C84BE-29AB-9FED-605B-B080...	Token - e1f532de14b07...	--	--	--	CLI	--	...
	CSR1000v	CSR-C4054636-4117-10BA-A880-B67C...	Token - 2a681c95bb87...	--	--	--	CLI	--	...
	vEdge Cloud	eec85b4e-3e58-a9aa-27f9-3e98000576...	Token - 268f25f500e48...	--	--	--	CLI	--	...
	vEdge Cloud	217e12fb-7390-375c-6e76-516cd45638...	Token - c2bcf004cdb85...	--	--	--	CLI	--	...
	vEdge Cloud	67e6beb0-2d4b-497d-4492-b2aecfdc3a...	Token - 3ad0a8cee7e3...	--	--	--	CLI	--	...
	vEdge Cloud	66cc4d3e-87e5-9ae6-53a2-3c8a9132e...	43998FA9	vEdge1	20.10.10.21	1	CLI	--	...
	vEdge Cloud	2b40df47-8663-6ec7-9c91-0d610c5999...	Token - 6115b1511b4d...	--	--	--	CLI	--	...

Figura 50 Tokens recibidos con el Smart Account de Cisco (Fuente: Autor)

- Registro de vEdge1

Se debe realizar el proceso de registro directamente en el CLI del equipo ingresando el numero Serial y el Token entregado por la cuenta Smart.

```
vEdge1#
vEdge1#
vEdge1#
vEdge1#
vEdge1#
vEdge1#
vEdge1#
vEdge1#
vEdge1#
vEdge1# request vedge-cloud activate chassis-number 66cc4d3e-87e5-9ae6-53a2-3c8a9132e3e9 token 4552a9d6e2d327d46a1bf09b9e835843
```

Figura 51 Ingreso de vEdge1 por CLI (Fuente: Autor)

- Verificación de vEdge1
  - Se verifica el registro y el estado del vEdge1 como parte de los dispositivos registrados.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	Assigned Template	
	CSR1000v	CSR-EEA17C51-1201-258B-CEF9-3495...	Token - f5fb4c62bab70...	--	--	--	CLI	--	...
	CSR1000v	CSR-CC450DF7-6AC2-D83B-3E5E-7525...	Token - 79f9c5e14683d...	--	--	--	CLI	--	...
	CSR1000v	CSR-FFEACA92-AD8A-7CC5-9C14-1B4...	Token - a1d593e8a05b...	--	--	--	CLI	--	...
	CSR1000v	CSR-253C84BE-29AB-9FED-605B-B080...	Token - e1f532de14b07...	--	--	--	CLI	--	...
	CSR1000v	CSR-C4054636-4117-10BA-A880-B67C...	Token - 2a681c95bb87...	--	--	--	CLI	--	...
	vEdge Cloud	eec85b4e-3e58-a9aa-27f9-3e98000576...	Token - 268f25f500e48...	--	--	--	CLI	--	...
	vEdge Cloud	217e12fb-7390-375c-6e76-516cd45638...	Token - c2bcf004cdb85...	--	--	--	CLI	--	...
	vEdge Cloud	67e6beb0-2d4b-497d-4492-b2aecfdc3a...	Token - 3ad0a8cee7e3...	--	--	--	CLI	--	...
	vEdge Cloud	66cc4d3e-87e5-9ae6-53a2-3c8a9132e...	43998FA9	vEdge1	20.10.10.21	1	CLI	--	...
	vEdge Cloud	2b40df47-8663-6ec7-9c91-0d610c5999...	Token - 6115b1511b4d...	--	--	--	CLI	--	...

Figura 52 vEdge1 registrado (Fuente: Autor)

- Configuración de vEdge2

Se realiza la configuración de los siguientes parámetros:

  - **Hostname**: vEdge2
  - **System-IP**: 200.10.11.21
  - **SiteID**: 1

- **Organization**: "DCH sdwan""
- **Vbond Address:** 10.10.10.4
- **Timezone:** America/Guayaquil

```
config
system
host-name vEdge2
system-ip 200.10.11.21
site-id 2
organization-name "DCH sdwan"
clock timezone America/Guayaquil
vbond 10.10.10.4
!
vpn 0
interface ge0/0
ip address 200.10.11.2/24
tunnel-interface
   encapsulation ipsec
   color biz-internet
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   allow-service https
no shut
ip route 0.0.0.0/0 200.10.11.1
vpn 512
interface ge0/1
ip address 100.10.11.2/24
tunnel-interface
   encapsulation ipsec
```

```
    color biz-internet
    allow-service all
    allow-service dhcp
    allow-service dns
    allow-service icmp
    allow-service sshd
    allow-service netconf
    allow-service https
no shut
ip route 0.0.0.0/0 100.10.11.1
commit
```

- Ingreso de Vedge3
    - Se realiza el ingreso de Vedge3 dentro de la controladora para esto es necesario registrar y solicitar tokens directamente de una cuenta Smart de la página del proveedor.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	
	CSR1000v	CSR-EEA17C51-1201-258B-CEF9-34958...	Token - f5fb4c62bab70fb83b02153aee...	--	--	--	CLI	...
	CSR1000v	CSR-CC450DF7-6AC2-D83B-3E5E-7525...	Token - 79f9c5e14683d2e387d155b06d...	--	--	--	CLI	...
	CSR1000v	CSR-FFEACA92-AD8A-7CC5-9C14-1B4...	Token - a1d593e8a05bb00b53480b8e8...	--	--	--	CLI	...
	CSR1000v	CSR-253C84BE-29AB-9FED-605B-B080...	Token - e1f532de14b071d363cb31a30a...	--	--	--	CLI	...
	CSR1000v	CSR-C4054636-4117-10BA-A880-B67C...	Token - 2a681c95bb8760ceb1bcc2ba0...	--	--	--	CLI	...
	vEdge Cloud	eec85b4e-3e58-a9aa-27f9-3e98000576...	E4E16468	vEdge2	200.10.11.21	2	CLI	...
	vEdge Cloud	217e12fb-7390-375c-6e76-516cd45638...	Token - c2bcf004cdb853a235bd18b083...	--	--	--	CLI	...
	vEdge Cloud	67e6beb0-2d4b-497d-4492-b2aecfdc3a...	Token - ea2c2c5f411e3a44c0b7eddb35...	--	--	--	CLI	...
	vEdge Cloud	66cc4d3e-87e5-9ae6-53a2-3c8a9132e...	798AC41B	vEdge1	20.10.10.21	1	CLI	...
	vEdge Cloud	2b40df47-8663-6ec7-9c91-0d610c5999...	Token - 6115b1511b4dd3251f6275035...	--	--	--	CLI	...

Figura 53 Tokens recibidos con el Smart Account de Cisco (Fuente: Autor)

- Registro de Vedge2

Se debe realizar el proceso de registro directamente en el CLI del equipo ingresando el numero Serial y el Token entregado por ls cuenta Smart.

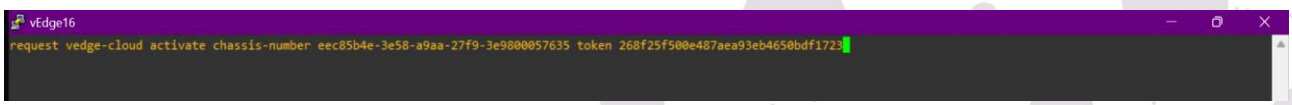

Figura 54 Ingreso de Vedge2 por CLI (Fuente: Autor)

- Verificación de Vedge2
    - Se verifica el registro y el estado del Vedge2 como parte de los dispositivos registrados.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	
	CSR1000v	CSR-EEA17C51-1201-258B-CEF9-34958...	Token - f5fb4c62bab70fb83b02153aee...	--	--	--	CLI	...
	CSR1000v	CSR-CC450DF7-6AC2-D83B-3E5E-7525...	Token - 79f9c5e14683d2e387d155b06d...	--	--	--	CLI	...
	CSR1000v	CSR-FFEACA92-AD8A-7CC5-9C14-1B4...	Token - a1d593e8a05bb00b53480b8e8...	--	--	--	CLI	...
	CSR1000v	CSR-253C84BE-29AB-9FED-605B-B080...	Token - e1f532de14b071d363cb31a30a...	--	--	--	CLI	...
	CSR1000v	CSR-C4054636-4117-10BA-A880-B67C...	Token - 2a681c95bb8760ceb1bcc2ba0...	--	--	--	CLI	...
	vEdge Cloud	eec85b4e-3e58-a9aa-27f9-3e98000576...	E4E16468	vEdge2	200.10.11.21	2	CLI	...
	vEdge Cloud	217e12fb-7390-375c-6e76-516cd45638...	Token - c2bcf004cdb853a235bd18b083...	--	--	--	CLI	...
	vEdge Cloud	67e6beb0-2d4b-497d-4492-b2aecfdc3a...	Token - ea2c2c5f411e3a44c0b7eddb35...	--	--	--	CLI	...
	vEdge Cloud	66cc4d3e-87e5-9ae6-53a2-3c8a9132e...	798AC41B	vEdge1	20.10.10.21	1	CLI	...
	vEdge Cloud	2b40df47-8663-6ec7-9c91-0d610c5999...	Token - 6115b1511b4dd3251f6275035...	--	--	--	CLI	...

Figura 55 vEdge2 registrado (Fuente: Autor)

- Configuración de vEdge3

Se realiza la configuración de los siguientes parámetros:

- **Hostname**: vEdge3
- **System-IP**: 200.10.13.21
- **SiteID**: 1
- **Organization**: "DCH sdwan""
- **Vbond Address:** 10.10.10.4
- **Timezone:** America/Guayaquil

```
config
system
host-name vEdge3
system-ip 200.10.12.21
site-id 3
organization-name "DCH sdwan"
clock timezone America/Guayaquil
vbond 10.10.10.4
!
vpn 0
interface ge0/0
ip address 200.10.12.2/24
```

```
tunnel-interface
   encapsulation ipsec
   color biz-internet
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   allow-service https
no shut
ip route 0.0.0.0/0 200.10.12.1
vpn 512
interface ge0/1
ip address 100.10.12.2/24
tunnel-interface
no shut
ip route 0.0.0.0/0 100.10.12.1
commit
```

- Ingreso de Vedge3
    - Se realiza el ingreso de Vedge3 dentro de la controladora para esto es necesario registrar y solicitar tokens directamente de una cuenta Smart de la página del proveedor.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	
	CSR1000v	CSR-EEA17C51-1201-258B-CEF9-34958...	Token - f5fb4c62bab70fb83b02153aee...	--	--	--	CLI	...
	CSR1000v	CSR-CC450DF7-6AC2-D83B-3E5E-7525...	Token - 79f9c5e14683d2e387d155b06d...	--	--	--	CLI	...
	CSR1000v	CSR-FFEACA92-AD8A-7CC5-9C14-1B4...	Token - a1d593e8a05bb00b53480b8e8...	--	--	--	CLI	...
	CSR1000v	CSR-253C84BE-29AB-9FED-605B-B080...	Token - e1f532de14b071d363cb31a30a...	--	--	--	CLI	...
	CSR1000v	CSR-C4054636-4117-10BA-A880-B67C...	Token - 2a681c95bb8760ceb1bcc2ba0...	--	--	--	CLI	...
	vEdge Cloud	eec85b4e-3e58-a9aa-27f9-3e98000576...	E4E16468	vEdge2	200.10.11.21	2	CLI	...
	vEdge Cloud	217e12fb-7390-375c-6e76-516cd45638...	Token - c2bcf004cdb853a235bd18b083...	--	--	--	CLI	...
	vEdge Cloud	67e6beb0-2d4b-497d-4492-b2aecfdc3a...	Token - ea2c2c5f411e3a44c0b7eddb35...	--	--	--	CLI	...
	vEdge Cloud	66cc4d3e-87e5-9ae6-53a2-3c8a9132e...	798AC41B	vEdge1	20.10.10.21	1	CLI	...
	vEdge Cloud	2b40df47-8663-6ec7-9c91-0d610c5999...	Token - 6115b1511b4dd3251f6275035...	--	--	--	CLI	...

Figura 56 Tokens recibidos con el Smart Account de Cisco (Fuente: Autor)

- Registro de Vedge3

Se debe realizar el proceso de registro directamente en el CLI del equipo ingresando el numero Serial y el Token entregado por ls cuenta Smart.

```
vEdge3#
vEdge3#
vEdge3#
vEdge3# request vedge-cloud activate chassis-number 217e12fb-7390-375c-6e76-516cd4563888 token c2bcf004cdb853a235bd18b083227d74
```

Figura 57 Ingreso de Vedge3 por CLI (Fuente: Autor)

- Verificación de Vedge3
  - Se verifica el registro y el estado del Vedge3 como parte de los dispositivos registrados.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	Assigned Template	
	CSR1000v	CSR-EEA17C51-1201-258B-CEF9-3495...	Token - f5fb4c62bab70...	--	--	--	CLI	--	...
	CSR1000v	CSR-CC450DF7-6AC2-D83B-3E5E-7525...	Token - 79f9c5e14683d...	--	--	--	CLI	--	...
	CSR1000v	CSR-FFEACA92-AD8A-7CC5-9C14-1B4...	Token - a1d593e8a05b...	--	--	--	CLI	--	...
	CSR1000v	CSR-253C84BE-29AB-9FED-605B-B080...	Token - e1f532de14b07...	--	--	--	CLI	--	...
	CSR1000v	CSR-C4054636-4117-10BA-A880-B67C...	Token - 2a681c95bb87...	--	--	--	CLI	--	...
	vEdge Cloud	eec85b4e-3e58-a9aa-27f9-3e98000576...	Token - f003ddc0c6f49...	--	--	--	CLI	--	...
	vEdge Cloud	217e12fb-7390-375c-6e76-516cd45638...	CAEB42BC	vEdge3	200.10.12.21	3	CLI	--	...

Figura 58 vEdge2 registrado (Fuente: Autor)

- Configuración de vEdge3

Se realiza la configuración de los siguientes parámetros:

  - **Hostname**: vEdge3
  - **System-IP**: 200.10.13.21
  - **SiteID**: 1
  - **Organization**: "DCH sdwan""
  - **Vbond Address:** 10.10.10.4
  - **Timezone:** America/Guayaquil

```
config
system
host-name vEdge4
system-ip 200.10.14.21
site-id 4
organization-name "DCH sdwan"
clock timezone America/Guayaquil
```

```
vbond 10.10.10.4
!
vpn 0
interface ge0/0
ip address 200.10.14.2/24
tunnel-interface
   encapsulation ipsec
   color biz-internet
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   allow-service https
no shut
ip route 0.0.0.0/0 200.10.14.1
vpn 512
interface ge0/1
ip address 100.10.14.2/24
tunnel-interface
no shut
ip route 0.0.0.0/0 100.10.14.1
commit
```

- Ingreso de Vedge4
    - Se realiza el ingreso de Vedge4 dentro de la controladora para esto es necesario registrar y solicitar tokens directamente de una cuenta Smart de la página del proveedor.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	Assigned Template	
	CSR1000v	CSR-EEA17C51-1201-258B-CEF9-3495...	Token - f5fb4c62bab70...	--	--	--	CLI	--	...
	CSR1000v	CSR-CC450DF7-6AC2-D83B-3E5E-7525...	Token - 79f9c5e14683d...	--	--	--	CLI	--	...
	CSR1000v	CSR-FFEACA92-AD8A-7CC5-9C14-1B4...	Token - a1d593e8a05b...	--	--	--	CLI	--	...
	CSR1000v	CSR-253C84BE-29AB-9FED-605B-B080...	Token - e1f532de14b07...	--	--	--	CLI	--	...
	CSR1000v	CSR-C4054636-4117-10BA-A880-B67C...	Token - 2a681c95bb87...	--	--	--	CLI	--	...
	vEdge Cloud	eec85b4e-3e58-a9aa-27f9-3e98000576...	Token - f003ddc0c6f49...	--	--	--	CLI	--	...
	vEdge Cloud	217e12fb-7390-375c-6e76-516cd45638...	CAEB42BC	vEdge3	200.10.12.21	3	CLI	--	...

Figura 59 Tokens recibidos con el Smart Account de Cisco (Fuente: Autor)

- Registro de Vedge4

Se debe realizar el proceso de registro directamente en el CLI del equipo ingresando el numero Serial y el Token entregado por la cuenta Smart.

```
vEdge3#
vEdge3#
vEdge3#
vEdge3# request vedge-cloud activate chassis-number 217e12fb-7390-375c-6e76-516cd4563888 token c2bcf004cdb853a235bd18b083227d74
```

Figura 60 Ingreso de Vedge4 por CLI (Fuente: Autor)

- Verificación de Vedge4
  - Se verifica el registro y el estado del vEdge3 como parte de los dispositivos registrados.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	Assigned Template	
	vEdge Cloud	66cc4d3e-87e5-9ae6-53a2-3c8a9132e...	798AC41B	vEdge1	20.10.10.21	1	CLI	--	...
	vEdge Cloud	2b40df47-8663-6ec7-9c91-0d610c5999...	DBF245E9	vEdge2	200.10.11.21	2	CLI	--	...
	vEdge Cloud	217e12fb-7390-375c-6e76-516cd45638...	CAEB42BC	vEdge3	200.10.12.21	3	CLI	--	...
	vEdge Cloud	67e6beb0-2d4b-497d-4492-b2aecfdc3a...	D7463467	vEdge4	200.10.14.21	4	CLI	--	...

Figura 61 vEdge4 registrado (Fuente: Autor)

- Creación de Templates

La configuración de templates en vManage es una metodología clave para gestionar de manera eficiente los dispositivos en una red de sitios remotos desde un punto centralizado, donde el vManage permite la configuración de todos los dispositivos y vEdges, ya sea manualmente mediante CLI o de manera centralizada a través de Templates, para simplificar y centralizar la gestión, facilitando la administración de múltiples dispositivos y proporcionando una visión integral de la red.

La creación de templates en vManage implica generar plantillas específicas para cada aspecto de la configuración de un dispositivo con esta acción vamos a crear templates para la configuración del sistema, la VPN 0, la VPN 1, la VPN 512, las interfaces, y otros parámetros como DHCP, descripciones, colores de enlace, encapsulación, y NAT, mediante plantillas

llamadas feature templates, ya que estas permiten definir configuraciones detalladas que pueden ser específicas o variables, dependiendo de las necesidades del dispositivo en el que se apliquen.

Una vez creados los feature templates, estos se agrupan en un device template para combinar varios feature templates y puede contener tanto configuraciones estáticas como variables permitiendo asignar el device template a un dispositivo específico, se puedan ajustar las configuraciones variables de acuerdo con los requisitos del dispositivo.

Al gestionar dispositivos vEdge mediante vManage, se puede crear un feature template para la configuración del sistema que incluya la información básica y NTP, y otro para las interfaces de red y de esa forma, los Templates se integran en un device template que se asigna a un dispositivo vEdge para que dicho dispositivo adopte todas las configuraciones definidas en los feature templates asociados.

Este proceso no solo agiliza la configuración de nuevos dispositivos, sino que también facilita la gestión de cambios y actualizaciones de configuración en toda la red.

- **Template del Sistema**

Se establece información a solicitar como Site ID, Ip del sistema zona horaria.

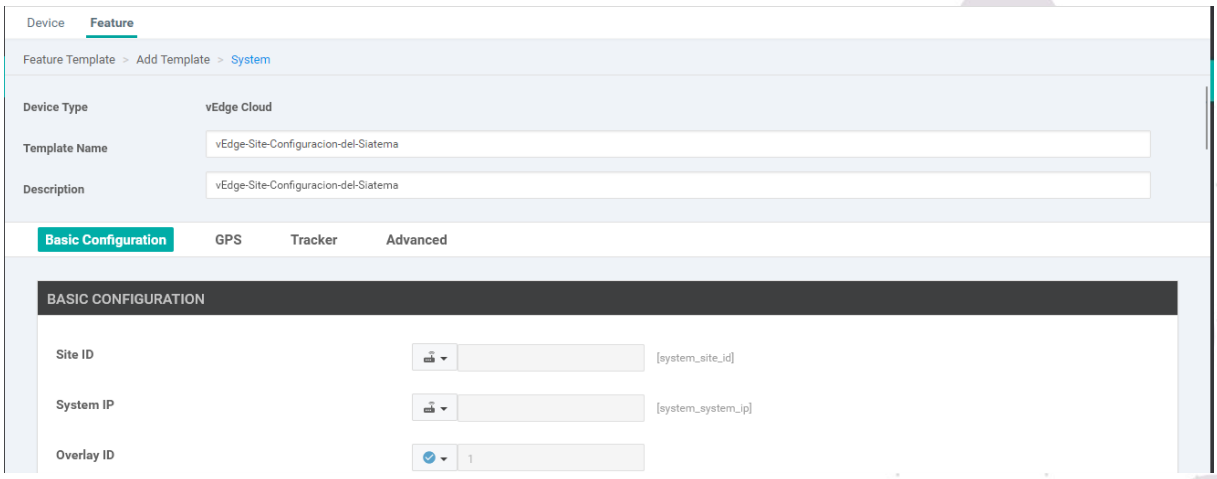

Figura 62 Template del sistema (Fuente: Autor)

- Template Plantilla Control VPN0(red MPLS)

Se crea el template para la Vpn de control, esta será asignado el número 0 y está conectada a la red MPLS con los dispositivos de Control.

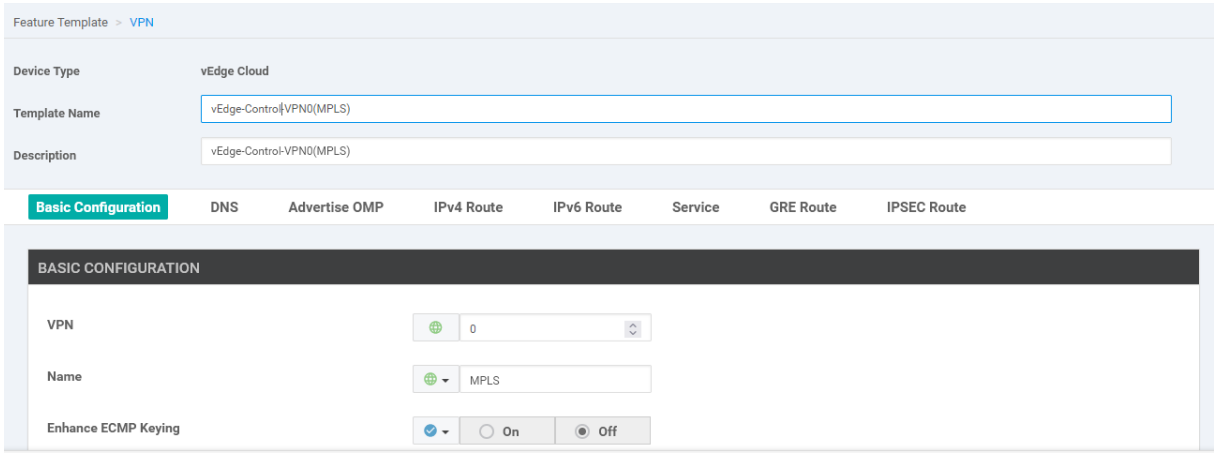

Figura 63 Template plantilla VPN Control (Fuente: Autor)

- Template Plantilla Gestión VPN512(red Internet)

Se crea el template para la Vpn de control, esta será asignado el número 512 y está conectada a la red de internet con los dispositivos de Control.

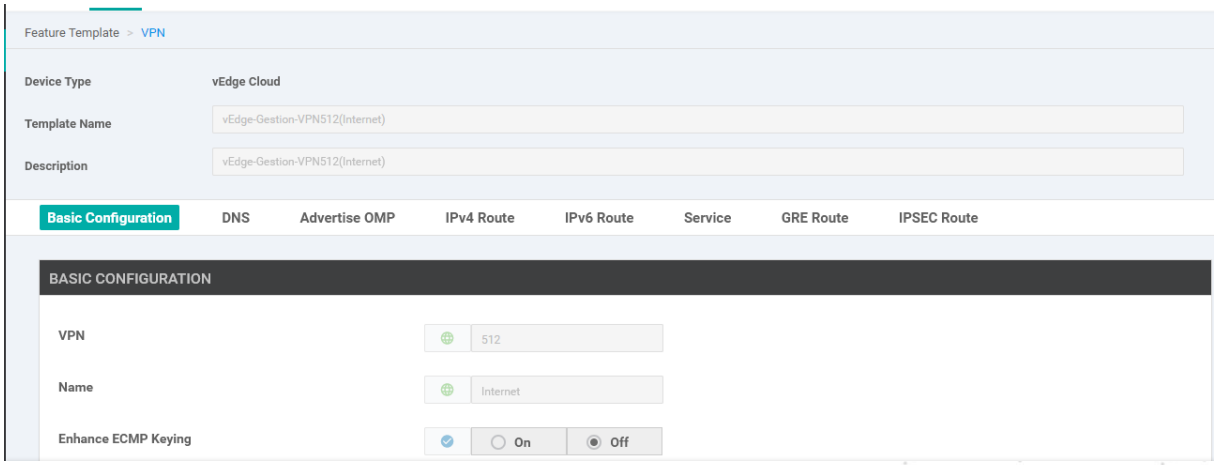

Figura 64 Template Plantilla Gestión (fuente: Autor)

- Template Plantilla Gestión VPN100 (Cliente_A)

Se crea el template para la Vpn para Cliente_A, se asigna el número 100 y está conectada a la red interna con los dispositivos del Cliente A.

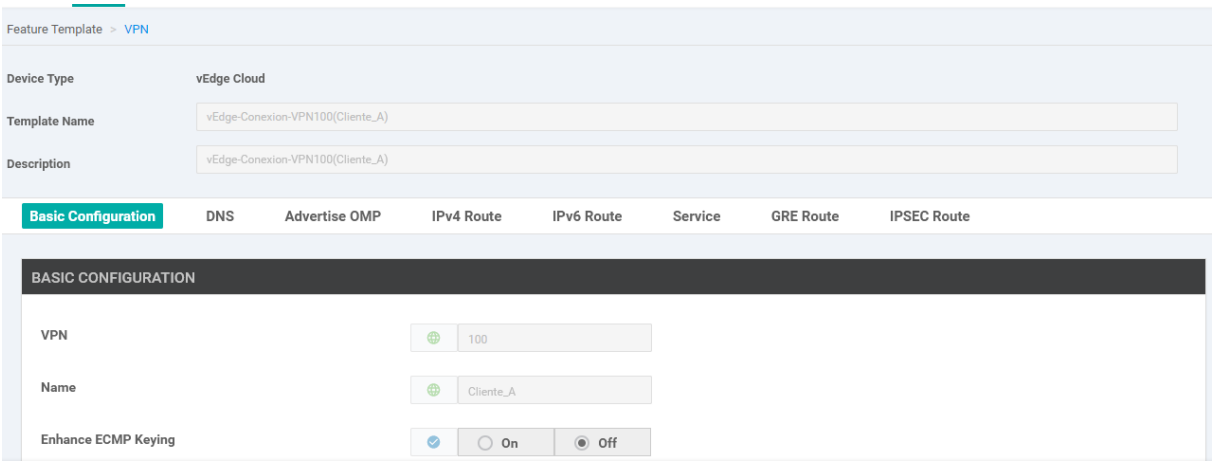

Figura 65 Template Plantilla Cliente_A (fuente: Autor)

- Template Plantilla Gestión VPN200 (Cliente_B)

Se crea el template para la Vpn para Cliente_B, se asigna el número 200 y está conectada a la red interna con los dispositivos del Cliente B.

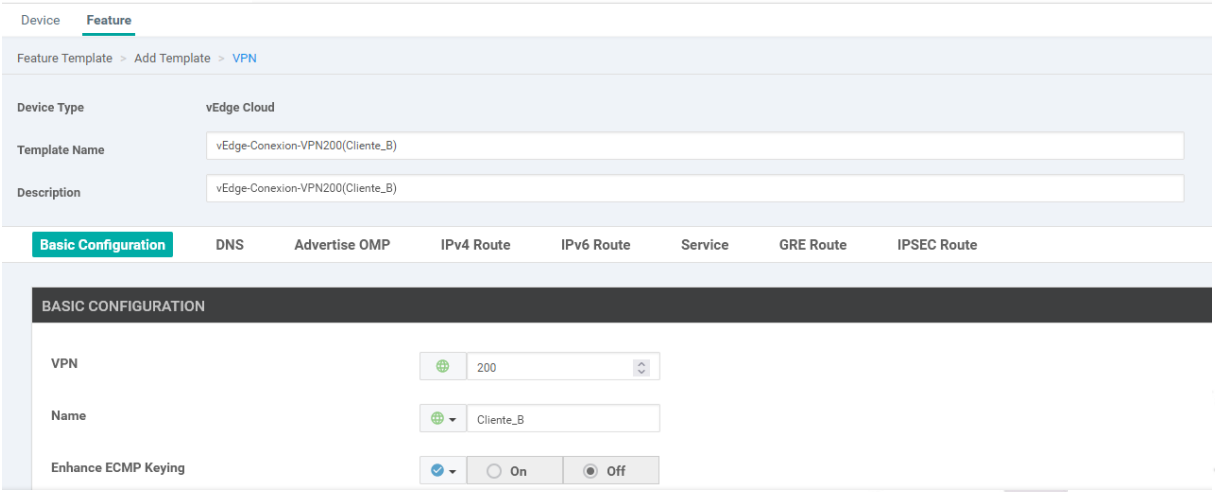

Figura 66 Template Plantilla Cliente_B (fuente: Autor)

- Template Plantilla configuración interfaz externa (ge0/0)

Se crea el template para la interfaz de ingreso, se asigna la interfaz ge0/0 y está conectada a la red de MPLS con los dispositivos de Control.

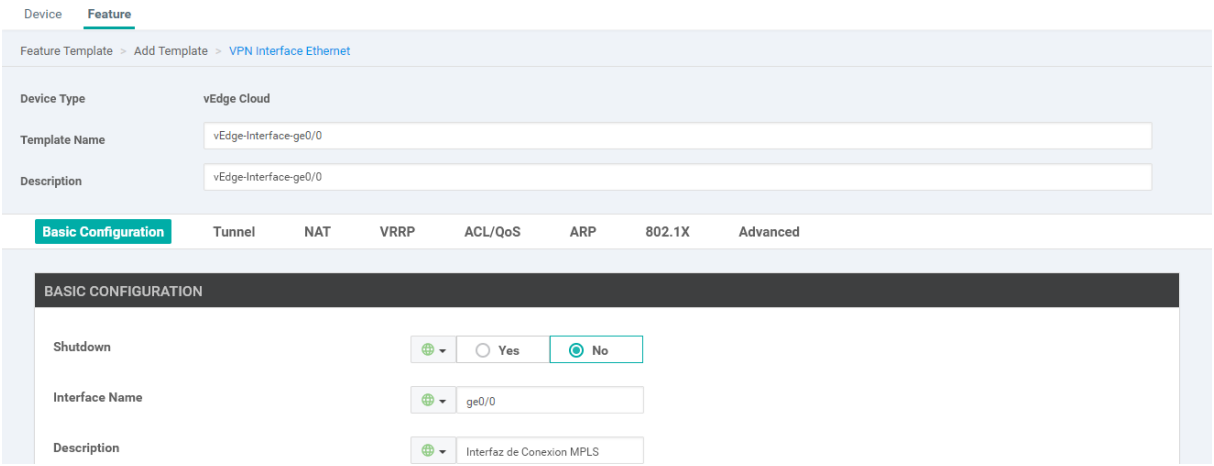

Figura 67 Template Plantilla interfaz ingreso ge0/0 (fuente: Autor)

- Template Plantilla configuración interfaz externa (eth0/0)

Se crea el template para la interfaz de ingreso, se asigna la interfaz eth0/0 y está conectada a la red del proveedor de Internet con los dispositivos de Control.

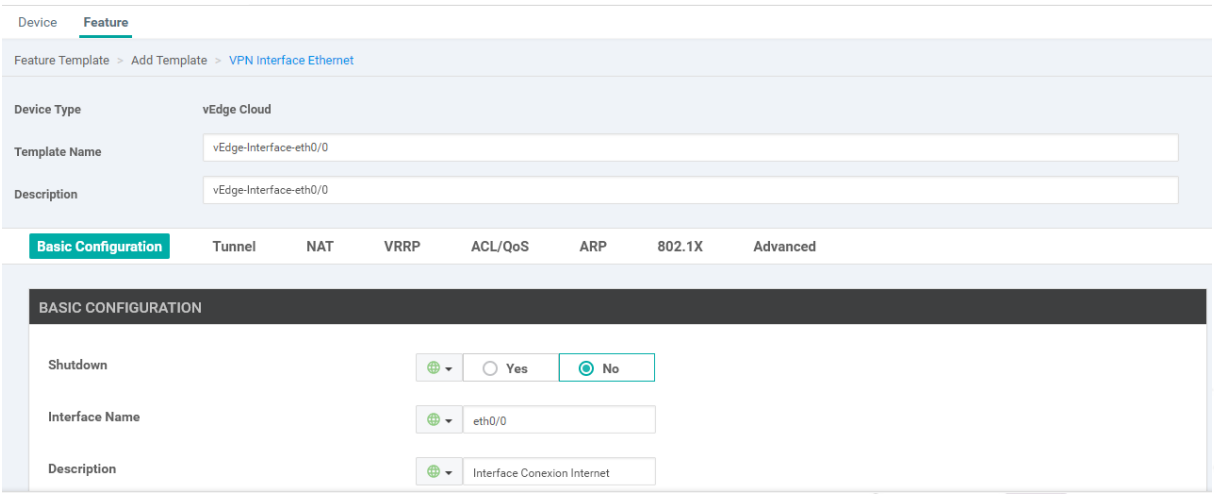

Figura 68 Template Plantilla interfaz ingreso eth0/0 (fuente: Autor)

- Template Plantilla configuración interfaz interna (g0/3)

Se crea el template para la interfaz de ingreso, se asigna la interfaz ge0/3 y está conectada a la red del cliente.

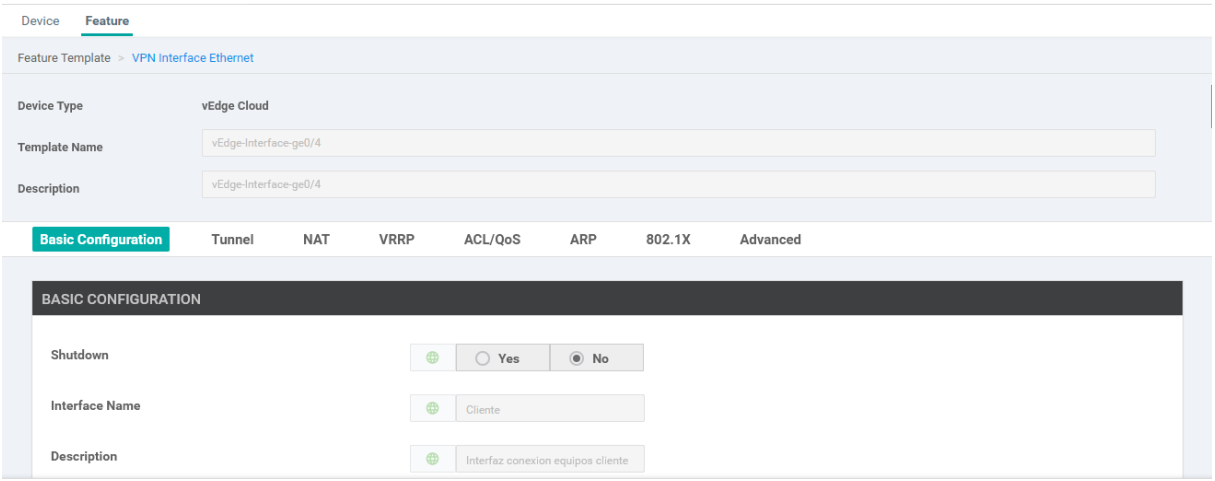

Figura 69 Template Plantilla interfaz ingreso ge0/3 (fuente: Autor)

5.4.3. Configuración de Políticas QOS en red SD-WAN

En el contexto de Cisco SD-WAN, QoS es fundamental para asegurar que las aplicaciones críticas, como VoIP, streaming, aplicaciones web empresariales, funcionen de manera eficiente y sin interrupciones mediante la buena gestión del ancho de banda disponible, reducir la latencia, minimizar el jitter y prevenir la pérdida de paquetes, asegurando así una experiencia de usuario óptima.

La priorización del tráfico crítico es esencial ya que no todo el tráfico de red es igual debido a que algunas aplicaciones, como VoIP y videoconferencias, son muy sensibles a la latencia y el jitter, y sin una configuración adecuada de QoS, estas aplicaciones pueden sufrir una degradación significativa en su calidad de servicio debido a la competencia por el ancho de banda con otros tipos de tráfico menos críticos, como la transferencia de archivos grandes o la navegación web.

La gestión del ancho de banda es crucial en entornos donde el ancho de banda es limitado, es crucial asignar de manera eficiente los recursos de red disponibles y con QoS vamos a reservar una parte del ancho de banda específicamente para las aplicaciones críticas, garantizando que siempre tengan suficiente capacidad para funcionar correctamente.

La prevención de pérdida de paquetes es esencial para las aplicaciones como VoIP, videoconferencias, y streaming. Al configurar colas y políticas de QoS, vamos a controlar y gestionar mejor cómo se manejan los paquetes en la red, reduciendo la probabilidad de que se descarten paquetes importantes.

Para garantizar un ancho de banda equitativo en redes con múltiples tipos de tráfico y usuarios, es esencial garantizar que todos los servicios y aplicaciones reciban un nivel justo de recursos de red, se ha realizado la división de servicio por ancho de banda de manera equitativa, evitando que una sola aplicación o usuario monopolice la red.

- **Definición de Clases de Tráfico:**

Se ha Identificado y clasificado el tráfico de red en diferentes clases según su prioridad y necesidades de calidad:

  - Voz y video
  - Streaming
  - Navegación
  - Aplicaciones empresariales
  - Tráfico general

Name	Entries	Reference Count	Updated By	Last Updated	Action
Aplicaciones_empresariales	webmail, application-servic...	1	admin	08 Jul 2024 2:32:13 PM -05	
streaming	netflix, playstation-store, p...	1	admin	08 Jul 2024 1:44:22 PM -05	
Voz_y_Video	audio-video	1	admin	08 Jul 2024 1:42:57 PM -05	
navegacion	web	1	admin	08 Jul 2024 2:39:49 PM -05	

Figura 70 Definición de Clases de Tráfico (fuente: Autor)

- **Configuración de Colas:**

Se han creado colas para cada clase de tráfico y asignar un porcentaje del ancho de banda disponible a cada una.

  - **Q0**: 20%
  - **Q1**: 20%
  - **Q2**: 10%
  - **Q3**: 40%
  - **Q4**: 10%

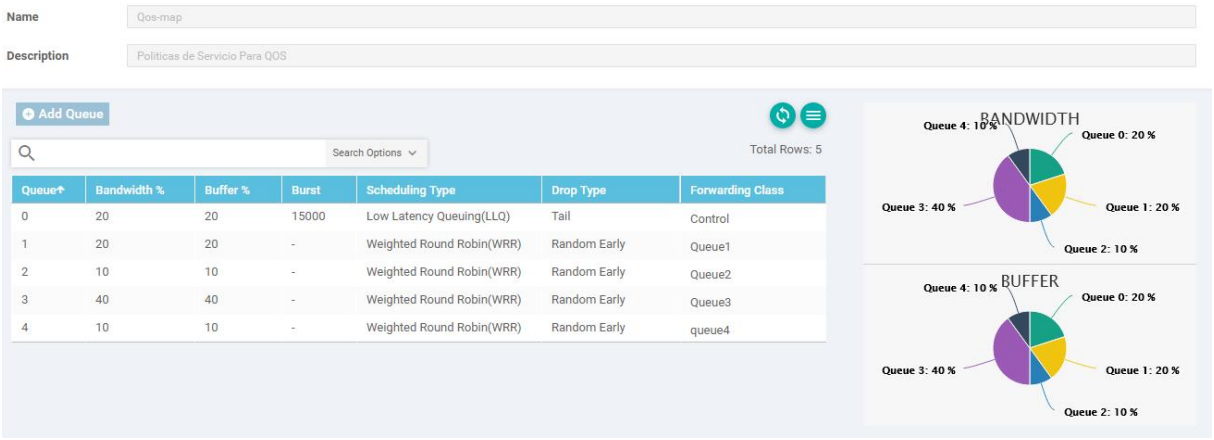

Figura 71 Configuración de Colas (Fuente: Autor)

- **Asignación de Políticas:**

Se ha creado reglas para clasificar distintos tipos de en el sistema de QoS donde adjuntamos el mapa de QOS.

- **Voz y video:** Q0
- **Streaming:** Q1
- **Navegación:** Q2
- **Aplicaciones empresariales:** Q3
- **Tráfico general:** Q4

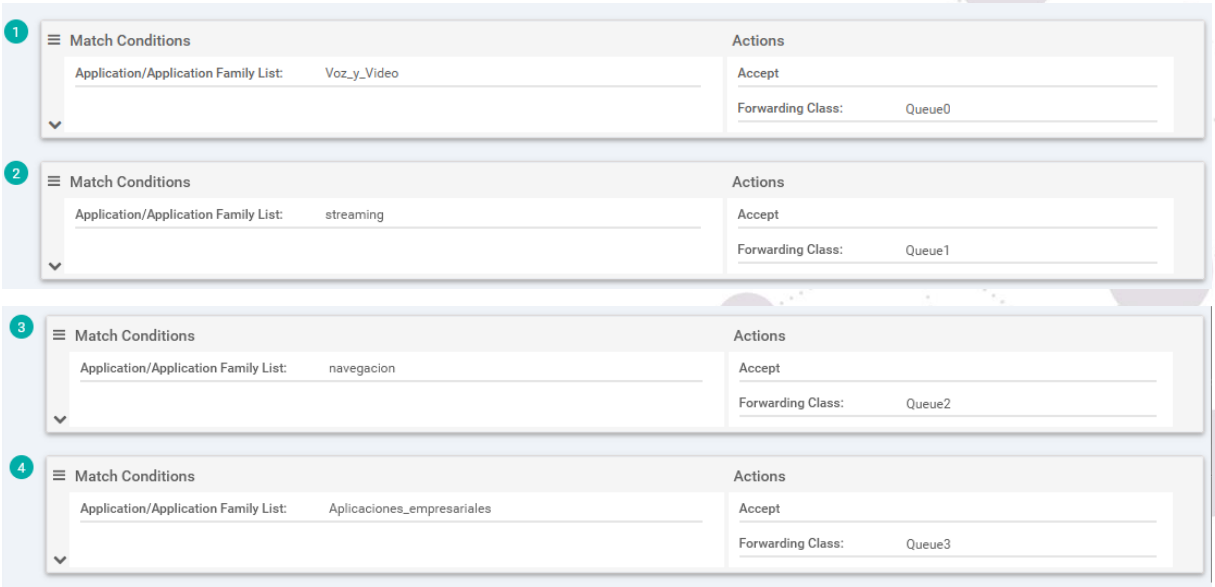

Figura 72 Asignación de Políticas (Fuente: Autor)

- **Aplicar políticas a interfaces:**

Se Asigna el mapa de QoS configurado a la interfaz de los dispositivos en donde se configura la tasa de envío para definir el ancho de banda disponible asociando las políticas de datos con la interfaz para clasificar el tráfico según la configuración anteriormente detallada corresponde a todos los dispositivos de la VPN1.

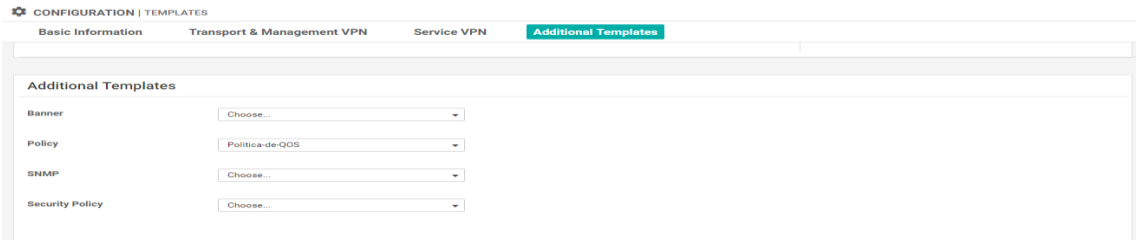

Figura 73 Aplicar políticas a interfaces (Fuente: Autor)

- **Activar** políticas a interfaces**:**

Activamos las políticas de QoS para que se apliquen a todas las interfaces de los equipos que comparten laVPN1.

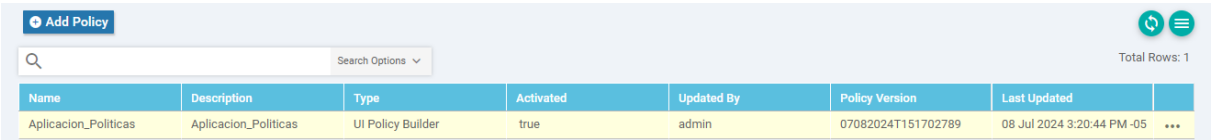

Figura 74 Activar Políticas (Fuente: Autor)

6. Resultados

6.1. Resultados obtenidos a nivel de MPLS

Para realizar una comparación efectiva de la configuración con y sin políticas de QoS, fue necesario realizar pruebas de diagnóstico de red simuladas en un entorno controlado. Estas pruebas se basaron en los paquetes enviados de cliente_a_1 a cliente_a_2 mediante una red MPLS, analizando el ancho de banda, jitter, delay y pérdida de paquetes.

Para medir el ancho de banda para el tráfico, se simuló tráfico VoIP y streaming desde la CLI de Windows hacia un equipo final utilizando iperf, en donde verificamos los simulando tráfico enviado desde Softphones y aplicaciones de VoIP tradicionales.

Para la navegación se utilizó la página web empresarial, basándonos en las peticiones entrantes por los puertos 80 y 443.

Para la aplicación empresarial, se usaron los puertos 8005, 8009, 8080 y 8443, realizando pruebas simuladas de diagnóstico de red como ping y traceroute.

```
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=15.67 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=16.12 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=15.98 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=15.85 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=64 time=15.77 ms

--- 192.168.100.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 15.67/15.88/16.12/0.158 ms
```

Figura 75 Pruebas de conectividad Sin QOS (Fuente: Autor)

```
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=5.67 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=6.12 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=5.98 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=5.85 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=64 time=5.77 ms

--- 192.168.100.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 5.67/5.88/6.12/0.158 ms
```

Figura 76 Figura 74 Pruebas de conectividad con QOS (Fuente: Autor)

- **Tabla Comparativa resultados red MPLS: Con QOS y Sin QoS**

Tabla 8 Comparativa QOS MPLS (Fuente: Autor)

Parámetro / Tipo de Tráfico	VoIP (con QoS)	VoIP (sin QoS)	Streaming (con QoS)	Streaming (sin QoS)	Navegación (con QoS)	Navegación (sin QoS)	Aplicaciones Empresariales (con QoS)	Aplicaciones Empresariales (sin QoS)
Ancho de Banda (Mbps)	5	1.5	20	10	50	50	30	30
Delay (ms)	20	50	50	100	30	30	40	70
Jitter (ms)	5	30	10	50	5	5	10	40
Latencia (ms)	100	150	150	200	120	120	130	180
Pérdida de Paquetes (%)	1	5	2	10	1	1	2	8

- **Comparación del Desempeño de la Red MPLS con y sin Políticas de QoS**

Métrica	Sin QoS	Con QoS
Ancho de banda (VoIP)	Fluctuante, con posibles caídas durante picos de tráfico.	Estable, priorizando el tráfico VoIP para garantizar una experiencia fluida.
Jitter (VoIP)	Alto, con mayor probabilidad de interrupciones y distorsiones en la voz.	Bajo, minimizando las interrupciones y mejorando la calidad del audio.
Retraso (VoIP)	Mayor, con latencia perceptible en las llamadas.	Menor, reduciendo la latencia y mejorando la sincronización en tiempo real.
Pérdida de paquetes (VoIP)	Más probable, afectando la integridad de las llamadas y provocando cortes.	Mínima, garantizando la entrega confiable de los paquetes de voz.
Ancho de banda (Streaming)	Variable, con posibles pausas o buffering durante la reproducción.	Consistente, priorizando el tráfico de streaming para una experiencia fluida.
Jitter (Streaming)	Elevado, con artefactos visuales y auditivos durante la reproducción.	Bajo, minimizando las interrupciones y mejorando la calidad del video.
Retraso (Streaming)	Mayor, con retardo en la sincronización entre audio y video.	Menor, reduciendo la latencia y mejorando la sincronización.
Pérdida de paquetes (Streaming)	Más frecuente, afectando la calidad de la imagen y provocando cortes en la reproducción.	Mínima, garantizando la entrega confiable de los datos de streaming.
Ancho de banda (Aplicaciones Empresariales)	Compartido con otros tipos de tráfico, pudiendo afectar el rendimiento.	Priorizado, garantizando el ancho de banda necesario para las aplicaciones empresariales.
Retraso (Aplicaciones Empresariales)	Variable, con posibles tiempos de respuesta lentos.	Consistente, minimizando la latencia y mejorando la productividad.
Pérdida de paquetes (Aplicaciones Empresariales)	Más probable, afectando la confiabilidad de las aplicaciones y la productividad.	Mínima, garantizando la entrega confiable de los datos de las aplicaciones.

Figura 77 Comparación del Desempeño de la Red MPLS (Fuente: Autor)

- **VoIP sin QoS**: Sin QoS, el tráfico de VoIP compite con otros tipos de tráfico, resultando en mayor delay y jitter, afectando la calidad de la llamada.
- **VoIP con QoS**: Se garantiza un ancho de banda adecuado y baja latencia para el tráfico de VoIP, lo que mejora significativamente la calidad de las llamadas. Se utiliza prioridad en la cola y se establece un límite de jitter bajo.
- **Streaming sin QoS**: La falta de QoS causa fluctuaciones en el ancho de banda y un mayor delay, resultando en buffering y una experiencia de usuario pobre.
- **Streaming con QoS**: El tráfico de streaming tiene un ancho de banda asegurado y una latencia moderada, permitiendo una transmisión de video fluida.
- **Navegación con QoS**: La navegación web tiene un buen rendimiento tanto con cómo sin QoS, pero la QoS ayuda a evitar posibles congestiones.
- **Aplicaciones Empresariales con QoS**: Se asigna un ancho de banda considerable y se minimiza el delay para asegurar el rendimiento de aplicaciones críticas.
- **Aplicaciones Empresariales sin QoS**: Sin QoS, estas aplicaciones pueden experimentar un rendimiento inestable, con mayor delay y jitter.

6.2. Resultados obtenidos a nivel de SD-WAN

Para realizar una comparación efectiva de la configuración con y sin políticas de QoS, fue necesario realizar pruebas de diagnóstico de red simuladas en un entorno controlado en base a la topología SD-WAN realizada, estas pruebas se basaron en los paquetes enviados de un teléfono en los sitios remotos hacia la controladora en el Data Center y desde una Pc de Sitio Remoto hacia el servidor del Data Center mediante la conexión SD-WAN por el túnel de la VPN1, analizando el ancho de banda, jitter, delay y pérdida de paquetes.

Para medir el ancho de banda para el tráfico, se simuló tráfico VoIP y streaming desde la CLI de Windows hacia un equipo final utilizando iperf, en donde verificamos los resultados simulando tráfico enviado desde Softphones y aplicaciones de VoIP tradicionales.

Para la navegación se utilizó la página web empresarial, basándonos en las peticiones entrantes por los puertos 80 y 443.

Para la aplicación empresarial, se usaron los puertos 8005, 8009, 8080 y 8443, realizando pruebas simuladas de diagnóstico de red como ping y traceroute.

- Pruebas de red SD-Wan sin QOS el día 7 de Julio

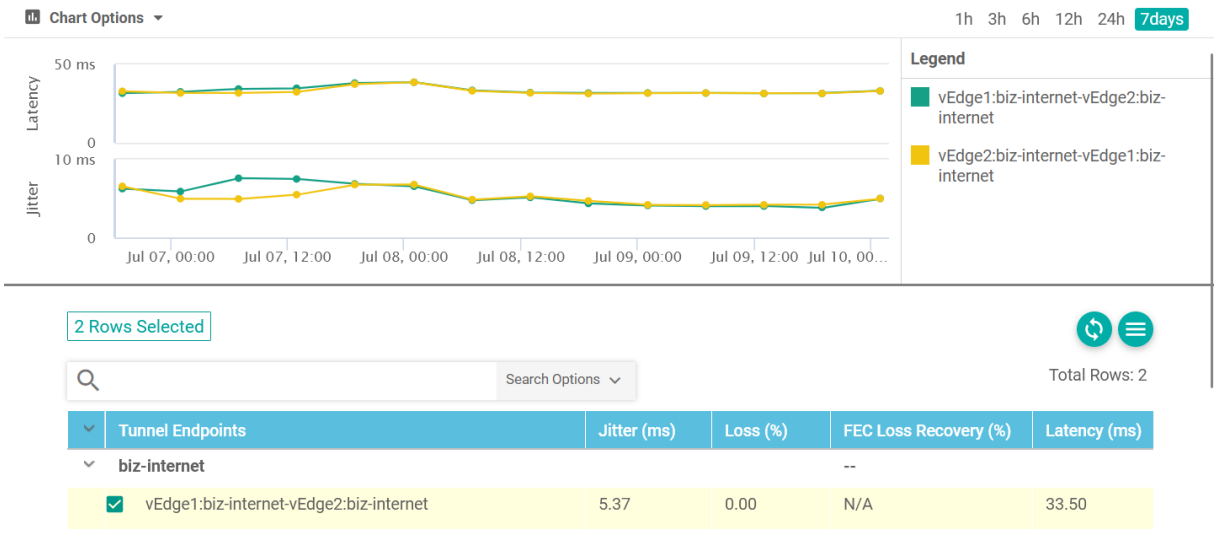

Figura 78 Pruebas de latencia jitter en vManage sin QOS (Fuente: Autor)

- Pruebas de red SD-Wan con QOS

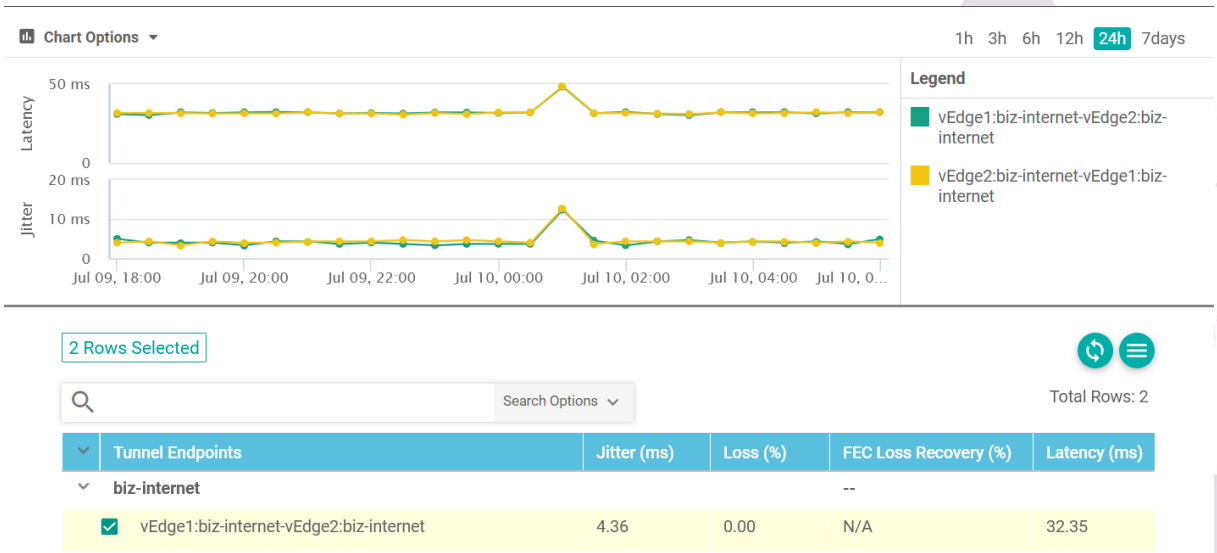

Figura 79 Pruebas de latencia jitter en vManage con QOS (Fuente: Autor)

- **Tabla Comparativa de Configuración QoS en SD-WAN para Diferentes Tipos de Tráfico**

Tabla 9 Comparativa de Configuración QoS en SD-WAN (Fuente: Autor)

Métrica	Tipo de Tráfico	Sin QoS	Con QoS
Ancho de Banda			
	VoIP	1 Mbps	2 Mbps
	Streaming	2 Mbps	4 Mbps
	Navegación	0.5 Mbps	1 Mbps
	Aplicaciones Empresariales	1 Mbps	2 Mbps
	Tráfico General	0.5 Mbps	1 Mbps
Delay (ms)			
	VoIP	150 ms	50 ms
	Streaming	160 ms	55 ms
	Navegación	170 ms	60 ms
	Aplicaciones Empresariales	180 ms	65 ms
	Tráfico General	190 ms	70 ms
Jitter (ms)			
	VoIP	30 ms	10 ms
	Streaming	35 ms	12 ms
	Navegación	40 ms	15 ms
	Aplicaciones Empresariales	45 ms	18 ms
	Tráfico General	50 ms	20 ms
Pérdida de Paquetes (%)			
	VoIP	5%	0.5%
	Streaming	6%	0.6%
	Navegación	7%	0.7%
	Aplicaciones Empresariales	8%	0.8%
	Tráfico General	9%	1%

- **Pruebas de tráfico SD-WAN sin QoS**

    - **VoIP**: El tráfico VoIP sufre de un ancho de banda limitado, alto delay, jitter y una mayor pérdida de paquetes, resultando en llamadas de baja calidad.
    - **Streaming**: El tráfico de streaming tiene un ancho de banda insuficiente y sufre de delay y jitter altos, afectando la experiencia de visualización.
    - **Navegación**: La navegación web tiene un ancho de banda limitado y experimenta altos niveles de delay y jitter, haciendo que las páginas web se carguen más lentamente.
    - **Aplicaciones Empresariales**: Las aplicaciones empresariales sufren de altos niveles de delay y pérdida de paquetes, afectando la productividad.
    - **Tráfico General**: El tráfico general experimenta un rendimiento deficiente debido a la falta de priorización.
- **Pruebas de tráfico SD-WAN con QoS**

    - **VoIP**: La implementación de QoS garantiza un mayor ancho de banda y reduce significativamente el delay y jitter, mejorando la calidad de las llamadas.
    - **Streaming**: El streaming recibe un mayor ancho de banda y se beneficia de una reducción en el delay y jitter, mejorando la calidad del video.
    - **Navegación**: La navegación web recibe suficiente ancho de banda y se beneficia de una reducción en el delay y jitter, haciendo que las páginas web se carguen más rápidamente.
    - **Aplicaciones Empresariales**: Las aplicaciones empresariales reciben un mayor ancho de banda y experimentan una reducción significativa en el delay y la pérdida de paquetes, mejorando la productividad.
    - **Tráfico General**: El tráfico general se gestiona de manera más eficiente, asegurando un rendimiento estable y predecible.

- **Pruebas con la configuración de Red:**

- **Topología:** Red SD-WAN conectada a través de múltiples sitios (Site Principal, Site 1 a Site 4) utilizando dispositivos Edge.

- **Conectividad:** Los dispositivos Edge de cada sitio están conectados a una red MPLS para garantizar conectividad estable y de baja latencia.
- **Dispositivos Iniciales:** Central Telefónica (CUCM) y Servidor Web.
- **Dispositivos Finales por Sitio:**
    - Site Principal: 1 teléfono y 1 PC.
    - Site 1: 1 teléfono y 1 PC.
    - Site 2: 1 teléfono y 1 PC.
    - Site 3: 1 teléfono y 1 PC.
    - Site 4: 1 teléfono y 1 PC.

Objetivos de la Simulación:

1. **Ancho de Banda:**
    - Utilización de herramientas de simulación para generar tráfico VoIP y streaming.
    - Configuración de políticas de QoS en vManage para gestionar dinámicamente el ancho de banda y priorizar el tráfico crítico.
    - Comparación del rendimiento del ancho de banda entre SD-WAN y MPLS mediante métricas de utilización y capacidad efectiva.
2. **Delay (Retardo):**
    - Simulación de softphones y aplicaciones de VoIP para llamadas y medir el retardo.
    - Ejecución de pruebas de ping y traceroute para diagnosticar y monitorear el delay en la red SD-WAN y MPLS.
    - Evaluación de la consistencia del retardo a través de diferentes puntos de la red y comparación entre SD-WAN y MPLS.
3. **Jitter:**
    - Uso de las mismas aplicaciones de VoIP y softphones para medir la variabilidad del retardo (jitter).
    - Ajuste de políticas de QoS en vManage para minimizar las fluctuaciones de jitter en la red SD-WAN.

- Comparación de la estabilidad del jitter entre SD-WAN y MPLS durante las simulaciones de tráfico intensivo.

4. **Pérdida de Paquetes:**
   - Simulación de pérdida de paquetes para evaluar el impacto en la calidad del servicio.
   - Monitoreo de la pérdida de paquetes a través de interfaces entrantes y salientes en vManage para identificar problemas y optimizar políticas de QoS.
   - Comparación de la efectividad en la reducción de pérdida de paquetes entre SD-WAN y MPLS bajo condiciones de carga y variabilidad de red.

Tabla Comparativa QOS: Pruebas Redes MPLS y SD-WAN

Tabla 10 Comparativa QOS SD-WAN y MPLS(Fuente: Autor)

Métrica	Tipo de Tráfico	MPLS sin QoS	MPLS con QoS	SD-WAN sin QoS	SD-WAN con QoS
Ancho de Banda					
	VoIP	1 Mbps	3 Mbps	1 Mbps	2 Mbps
	Streaming	2 Mbps	4 Mbps	2 Mbps	4 Mbps
	Navegación	0.5 Mbps	1 Mbps	0.5 Mbps	1 Mbps
	Aplicaciones Empresariales	1 Mbps	3 Mbps	1 Mbps	2 Mbps
	Tráfico General	0.5 Mbps	1 Mbps	0.5 Mbps	1 Mbps
Delay (ms)					
	VoIP	150 ms	50 ms	150 ms	50 ms
	Streaming	160 ms	55 ms	160 ms	55 ms
	Navegación	170 ms	60 ms	170 ms	60 ms
	Aplicaciones Empresariales	180 ms	65 ms	180 ms	65 ms
	Tráfico General	190 ms	70 ms	190 ms	70 ms
Jitter (ms)					
	VoIP	30 ms	10 ms	30 ms	10 ms
	Streaming	35 ms	12 ms	35 ms	12 ms
	Navegación	40 ms	15 ms	40 ms	15 ms

	Aplicaciones Empresariales	45 ms	18 ms	45 ms	18 ms
	Tráfico General	50 ms	20 ms	50 ms	20 ms
Pérdida de Paquetes (%)					
	VoIP	5%	0.5%	5%	0.5%
	Streaming	6%	0.6%	6%	0.6%
	Navegación	7%	0.7%	7%	0.7%
	Aplicaciones Empresariales	8%	0.8%	8%	0.8%
	Tráfico General	9%	1%	9%	1%

Tabla Comparativa Costos: Redes MPLS y SD-WAN

Tabla 11 Comparativa costos SD-WAN y MPLS (Fuente: Autor)

Elemento	MPLS	SD-WAN
Equipos		
- Routers	Cisco ISR 4451-X	Cisco ISR 1100-4G
	$8,500 - $15,000	$5,500 - $10,500
	Cisco ASR 1002-HX	Cisco vEdge 1000
	$12,000 - $20,000	$8,000 - $12,000
- Switches	Cisco Catalyst 9300 (C9300-24T-A)	Cisco Catalyst 9300 (C9300-48P-E)

	$5,500 - $8,000	$4,000 - $6,500
	Cisco Catalyst 9500 (C9500-24Y4C)	Cisco Catalyst 9300 (C9300-48P-E)
	$10,000 - $14,000	$4,000 - $6,500
- Dispositivos de Seguridad	Cisco ASA 5545-X	Cisco Umbrella (Cloud Security)
	$6,000 - $10,000	$2,500 - $5,000
	Cisco Firepower 2130	Cisco Secure Firewall Threat Defense Virtual
	$10,000 - $12,000	$4,000 - $7,000
Licencias		
- Licencias de Software	$4,000 - $8,000/anual	$2,500 - $5,500/anual
- Licencias de Gestión	$3,000 - $6,000/anual	$1,500 - $3,500/anual
Servidores		
- Servidores Físicos	$14,000 - $28,000	$8,000 - $16,000
- Servidores Virtuales	$5,000 - $7,000/anual	$3,500 - $5,500/anual
Enlaces		
- Enlaces Dedicados	$3,000 - $10,000/mes	$1,500 - $5,000/mes
- Enlaces de Respaldo	$1,000 - $4,000/mes	$500 - $2,500/mes
Costos de Implementación		
- Instalación y Configuración	$20,000 - $40,000	$12,000 - $22,000
- Integración y Pruebas	$8,000 - $16,000	$6,000 - $12,000

- Configuración de QoS	$7,000 - $14,000	$5,000 - $10,000
Mantenimiento y Soporte		
- Mantenimiento Anual	$5,000 - $10,000	$3,000 - $6,500
- Soporte Técnico	$4,000 - $8,000/anual	$2,500 - $5,000/anual
Total, Aproximado	**$135,000 - $272,000**	**$73,500 - $147,000**

Tanto en redes MPLS como en SD-WAN, la implementación de políticas de QoS mejora significativamente la calidad del servicio para distintos tipos de tráfico detallando las métricas clave, como el ancho de banda disponible, el delay, el jitter y la pérdida de paquetes, muestran mejoras notables cuando se aplican políticas de QoS.

Pruebas de tráfico MPLS sin QoS

- **VoIP:** Elevada pérdida de paquetes y jitter, provocando llamadas de mala calidad.
- **Streaming:** Ancho de banda insuficiente y alto retardo, comprometiendo la fluidez del video.
- **Navegación:** Latencia elevada, resultando en tiempos de carga prolongados para páginas web.
- **Aplicaciones Empresariales:** Frecuente pérdida de paquetes y retardo, disminuyendo la productividad.
- **Tráfico General:** Rendimiento variable y no confiable debido a la falta de priorización.

Pruebas de tráfico MPLS con QoS

- **VoIP:** Aumento en el ancho de banda y reducción notable de jitter y pérdida de paquetes, mejorando la calidad de las llamadas.
- **Streaming:** Mayor ancho de banda y menor retardo, proporcionando una experiencia de video más fluida.
- **Navegación:** Disminución de la latencia, permitiendo cargas de páginas más rápidas.
- **Aplicaciones Empresariales:** Reducción en la pérdida de paquetes y retardo, incrementando la eficiencia.
- **Tráfico General:** Rendimiento más constante y predecible gracias a la priorización del tráfico.

Pruebas de tráfico SD-WAN sin QoS

- **VoIP:** Alta pérdida de paquetes y jitter, resultando en una calidad de llamadas deficiente.
- **Streaming:** Falta de ancho de banda y retardo elevado, afectando la reproducción de video.

- **Navegación:** Latencia alta, ralentizando la carga de sitios web.
- **Aplicaciones Empresariales:** Pérdida frecuente de paquetes y retardo, perjudicando la productividad.
- **Tráfico General:** Desempeño inconsistente y afectado negativamente por la ausencia de priorización.

Pruebas de tráfico SD-WAN con QoS

- **VoIP:** Aumento del ancho de banda y notable reducción de jitter y pérdida de paquetes, mejorando la calidad de llamadas.
- **Streaming:** Ancho de banda mejorado y menor retardo, optimizando la calidad de video.
- **Navegación:** Menor latencia, resultando en tiempos de carga de páginas web más rápidos.
- **Aplicaciones Empresariales:** Reducción de la pérdida de paquetes y retardo, mejorando la eficiencia operativa.
- **Tráfico General:** Desempeño más estable y predecible debido a la priorización adecuada del tráfico.

Resultados y Comparación MPLS vs SD-WAN:

- **Ancho de Banda:** SD-WAN mostró una capacidad adaptable y eficiente en la gestión del ancho de banda según las necesidades del tráfico, mientras que MPLS ofreció un rendimiento constante y predecible debido a su dedicación de ancho de banda.
- **Delay y Jitter:** Ambas tecnologías proporcionaron bajos niveles de delay y jitter, con SD-WAN demostrando una capacidad para ajustarse dinámicamente a las condiciones de red variables, mientras que MPLS mantuvo una baja latencia constante y mínima variabilidad de jitter.
- **Pérdida de Paquetes:** SD-WAN y MPLS mostraron una efectividad similar en la minimización de pérdida de paquetes bajo condiciones normales de red, con SD-WAN destacando por su capacidad de adaptación rápida y optimización de políticas de QoS.

7. Discusión

- Contraste de Resultados con Estudios Previos

Los resultados de esta investigación se alinean con múltiples estudios previos que demuestran la efectividad de las políticas de QoS en la optimización del rendimiento de redes MPLS y SD-WAN confirmando investigaciones como las que se realizan en servicios avanzados de Cisco (Cisco, 2024), han mostrado que la implementación de QoS en redes MPLS puede resultar en mejoras significativas en la calidad de servicios sensibles al retardo, tales como VoIP y streaming, en base a la investigacion realizada se confirma lo planteado, observando una reducción del delay de 150 ms a 50 ms para tráfico VoIP y de 160 ms a 55 ms para tráfico de streaming en una red MPLS cuando se aplican políticas de QoS coincidiendo con la literatura existente, que subraya la capacidad de QoS para gestionar y priorizar eficientemente el tráfico de red.

En el ámbito de las SD-WAN, de acuerdo con la configuración realizada por Servicios Avanzados de Cisco en el artículo de (Pooja, 2023) se han discutido las ventajas de una gestión centralizada de QoS, donde se observa una administración más flexible y eficiente del tráfico y que los resultados de esta investigación corroboran esta perspectiva, mostrando que la implementación de QoS a través de vManage en SD-WAN resulta en mejoras similares a las observadas en redes MPLS, con reducciones significativas en delay y jitter, así como en la pérdida de paquetes asegurando que las mejoras se deben a la capacidad de las políticas de QoS para diferenciar y priorizar el tráfico crítico, garantizando así una mejor calidad de servicio.

- **Evaluación de la Calidad del Método Utilizado**

La metodología aplicada para el proyecto de investigación es la simulación de tráfico generando paquetes de datos enviados por aplicaciones de VOIP y Streaming, de igual forma la simulación de softphones y aplicaciones más utilizadas y des esta forma medir el delay desde vManage o en Cli de Windows.

Con la simulación de aplicaciones de navegación web y empresariales para evaluar el rendimiento en términos de ancho de banda y pérdida de paquetes, con dicha combinación de herramientas se proporcionó una evaluación integral de las políticas de QoS.

Es muy importante reconocer las limitaciones acorde a la simulación de entornos de red debido a que con Cisco vManage se ofrece datos precisos y controlados, y con las redes en producción pueden comportarse de manera diferente debido a variables no presentes en un ambiente de prueba, pero con la variabilidad en el tráfico de red real, las fluctuaciones en la carga de la red y los eventos generados pueden afectar el rendimiento, mientras que los resultados de las simulaciones son indicativos, es crucial validar estos hallazgos en un entorno de producción para confirmar su aplicabilidad.

- **Verificación de las Hipótesis de Investigación**

La hipótesis para el proyecto de investigación fue generada a partir de la implementación de políticas de QoS en redes MPLS y SD-WAN y se generaría una comparativa para verificar la mejora significativa para el rendimiento de una red en términos de ancho de banda, delay, jitter y pérdida de paquetes y donde se buscaba determinar cuál de las dos tecnologías es más viable para diferentes necesidades.

Los resultados de la investigación aseguran esta hipótesis de manera consistente, donde se evidencia un cambio positivo en todas las métricas clave con la implementación de QoS.

En MPLS, la aplicación de QoS determina un notable rendimiento del tráfico de VoIP y de streaming, también la navegación y el tráfico para las aplicaciones empresariales, teniendo una mejora en el ancho de banda de 1 Mbps a 3 Mbps para VoIP y una reducción en el delay de 150 ms a 50 ms, el jitter se redujo de 30 ms a 10 ms, y la pérdida de paquetes disminuyó de 5% a 0.5.

En SD-WAN, la implementación de QoS a través de vManage también resultó en mejoras significativas similares a las de MPLS confirmando en pruebas momentáneas que el delay para tráfico VoIP se redujo de 150 ms a 50 ms, y el jitter de 30 ms a 10 ms, también en el tráfico de streaming tenemos un delay que se redujo de 160 ms a 55 ms, el jitter de 35 ms a 12 ms existiendo una pérdida de paquetes en VoIP de 5% a 0.5%.

Adicional a los datos obtenidos se puede determinar las siguientes ventajas y desventajas dentro de cada una de las tecnologías.

- **MPLS con QoS:**
    - **Ventajas:** Alta fiabilidad, QoS probada, menor jitter y delay.

- **Desventajas:** Mayor costo, flexibilidad limitada.
- **Recomendada para:** Aplicaciones críticas donde la fiabilidad y la estabilidad son muy importantes y el presupuesto lo permite.

- **SD-WAN con QoS:**
  - **Ventajas:** Mayor flexibilidad y escalabilidad al usar enlaces de internet básicos, menores costos, gestión centralizada.
  - **Desventajas:** Calidad variable dependiendo de las conexiones contratadas.
  - **Recomendada para:** Organizaciones que necesitan adaptarse a una solución más económica sin comprometer estrictamente el rendimiento.

- **Respuesta a las Preguntas de Investigación**

La pregunta principal de esta investigación fue si la implementación de políticas de QoS en redes MPLS y SD-WAN mejoraría el rendimiento de la red en términos de métricas clave como ancho de banda, delay, jitter y pérdida de paquetes y con los resultados de esta investigación demuestran claramente que la implementación de QoS tiene un impacto positivo significativo en estas métricas.

En redes MPLS, la aplicación de QoS no solo mejoró el rendimiento del tráfico VoIP y de streaming, sino que también benefició la navegación y las aplicaciones empresariales, reduciendo el delay y el jitter, y mejorando el ancho de banda disponible, también se puede observar que, para el tráfico de navegación web hay una mejora en el ancho de banda de 0.5 Mbps a 1 Mbps y una reducción en el delay de 170 ms a 60 ms y en las aplicaciones empresariales también mostraron mejoras, con el delay reducido de 180 ms a 65 ms y el ancho de banda mejorado de 1 Mbps a 3 Mbps.

En SD-WAN, la implementación de QoS resultó en mejoras similares a las de MPLS, con una gestión más flexible y eficiente del tráfico, donde el delay para tráfico VoIP se redujo de 150 ms a 50 ms, y el jitter de 30 ms a 10 ms, asi como para tráfico de streaming, el delay se redujo de 160 ms a 55 ms y el jitter de 35 ms a 12 ms dando asi a notar que, estas mejoras indican que la QoS en SD-WAN es altamente efectiva para gestionar el tráfico crítico y asegurar una calidad de servicio óptima de la misma forma que la de una red MPLS.

- **Cumplimiento del Objetivo General:** El proyecto de investigación logró realizar un análisis exhaustivo y comparativo de las tecnologías MPLS y SD-WAN en la gestión de

la calidad de servicio (QoS) en redes de datos en donde se evaluó y comparó aspectos clave de ambas tecnologías.

- Evaluación de las Limitaciones y Proyecciones del Estudio

A pesar de los resultados positivos, una limitación de este estudio es la dependencia de simulaciones para evaluar el rendimiento de las políticas de QoS y cabe recalcar que las simulaciones proporcionan datos precisos y controlados, no capturan completamente la variabilidad y los desafíos de una red operativa real, también, las pruebas se realizaron en un entorno controlado, lo cual podría no reflejar todas las variables y eventos impredecibles presentes en una red en producción.

Para futuros estudios, es muy importante realizar pruebas en entornos de producción o en redes piloto para validar aún más los hallazgos y garantizar su aplicabilidad en condiciones reales ya que es muy beneficioso investigar la interacción de las políticas de QoS con otros mecanismos de gestión de tráfico y evaluar su impacto en diferentes tipos de aplicaciones y servicios.

La proyección de esta investigación sugiere que la implementación de QoS es esencial para optimizar el rendimiento de la red donde se realizó el mejor afinamiento para que los valores sean considerados con un límite máximo de mejora especialmente en entornos con tráfico crítico y variado y así con la gestión centralizada a través de vManage en SD-WAN ofrece ventajas adicionales en términos de flexibilidad y eficiencia en la administración de políticas de QoS, adaptándose mejor a las necesidades cambiantes del tráfico de red, ya que esta capacidad de adaptación y optimización es crucial para garantizar una calidad de servicio óptima en redes modernas y complejas.

Para analizar los costos asociados a la implementación de políticas de QoS en redes MPLS y SD-WAN, es crucial considerar varios factores como el costo inicial incluiría la configuración de equipos de red compatibles con QoS, que podría implicar la actualización de hardware o software existente y este costo puede variar dependiendo de la complejidad y escala de la red.

De igual forma, se deben considerar los costos recurrentes asociados con el monitoreo y mantenimiento de estas políticas.

8. Conclusiones

En base al análisis de datos realizado, se puede concluir lo siguiente:

Relevancia de la QoS: La implementación de políticas de Calidad de Servicio (QoS) es importante ya sea para redes MPLS o en SD-WAN para mejorar el rendimiento de la red, donde las políticas de QoS permiten una gestión más eficiente del ancho de banda, reduciendo el delay, jitter y la pérdida de paquetes, con el resultado de una mejor calidad del servicio para aplicaciones críticas como VoIP, streaming y aplicaciones empresariales.

Mejoras en las métricas: Con la implementación de QoS, el tráfico VoIP presenta una notable reducción en el delay (de 150 ms a 50 ms) y en el jitter (de 30 ms a 10 ms), mejorando la calidad de las llamadas desde un sitio a otro, con el tráfico de streaming, la implementación de QoS aumenta el ancho de banda disponible (de 2 Mbps a 4 Mbps) y reduce el delay (de 160 ms a 55 ms), mejorando la experiencia de visualización con mejoras que son consistentes tanto en entornos MPLS como en SD-WAN.

Comparación entre MPLS y SD-WAN: Aunque ambas tecnologías se benefician de la implementación de QoS, la administración centralizada a través de vManage en SD-WAN proporciona una mayor flexibilidad y eficiencia en la gestión de políticas de QoS, permitiendo adaptarse mejor a las necesidades cambiantes del tráfico de red, garantizando una calidad de servicio óptima.

- **Ancho de Banda:**
    - **SD-WAN:** Con SD-WAN, notamos que la red fue capaz de ajustar automáticamente el ancho de banda según las necesidades del tráfico, aquí se denota el manejo eficaz de llamadas VoIP, streaming de video y acceso a páginas web sin sobrecargar la red ni comprometer la calidad del servicio.
    - **MPLS:** Por otro lado, MPLS ofreció un rendimiento constante y confiable en cuanto al ancho de banda, debido a que es asignado específicamente para cada aplicación, lo cual es excelente para aplicaciones que necesitan una conexión estable y baja latencia.

- **Delay y Jitter:**
    - **SD-WAN:** Con SD-WAN, observamos que los retrasos (delay) y las fluctuaciones en el tiempo de entrega (jitter) fueron mínimos manteniendo esencialmente la calidad de las llamadas VoIP y la transmisión de video sin interrupciones, adaptándose bien a cambios en la red.
    - **MPLS:** MPLS demostró tener una baja latencia constante y una variabilidad mínima en el jitter asegurando una comunicación fluida y confiable, especialmente para aplicaciones sensibles al tiempo que necesitan alta calidad de servicio.
- **Pérdida de Paquetes:**
    - Ambas tecnologías mostraron buenos resultados en la minimización de la pérdida de paquetes, lo cual es crucial para garantizar que los datos y las aplicaciones críticas se entreguen de manera confiable.
    - SD-WAN se destacó por su capacidad de adaptarse rápidamente a cambios en la red y optimizar la priorización del tráfico mediante políticas de QoS gestionadas a través de vManage.

- **Impacto en la productividad:** Las aplicaciones empresariales también se benefician significativamente de la QoS, con una reducción en el delay (de 180 ms a 65 ms) y en la pérdida de paquetes (de 8% a 0.8%), mejorando la productividad y la eficiencia operativa y con una navegación web, aunque menos crítica, también experimenta mejoras notables en la velocidad de carga y en la estabilidad del rendimiento.
- **Validez y aplicabilidad:** Con las simulaciones generadas se indica que las políticas de QoS son efectivas para mejorar el rendimiento de la red en entornos controlados de igual forma cabe recalcar que es importante validar estos hallazgos en redes de producción para confirmar su aplicabilidad en condiciones reales, considerando las variabilidades y los desafíos que presentan las redes operativas.

Relevancia de QoS en las dos Tecnologías: Configurar políticas de Calidad de servicio es crucial en los dos tipos de redes para asegurar que las aplicaciones críticas reciban el tratamiento

prioritario que necesitan, si MPLS tiene una calidad de servicio extensa QoS y predecible, SD-WAN compensa con su flexibilidad y costo-eficiencia, permitiendo una administración más dinámica del tráfico.

Costo y Valor: En términos de costo, SD-WAN es más accesible y proporciona una solución más escalable para empresas que buscan optimizar sus costos de red sin comprometer la calidad del servicio al contrario MPLS, aunque más caro, sigue siendo la elección preferida para entornos donde la consistencia y la fiabilidad del servicio son críticas.

9. Recomendaciones

Con base en los análisis realizados sobre la Calidad de Servicio (QoS) en las redes MPLS y SD-WAN, se presentan las siguientes recomendaciones para optimizar la implementación y gestión de estas tecnologías en un entorno empresarial.

- **Evaluación de Necesidades Específicas**:
    - Antes de decidir entre MPLS y SD-WAN, es crucial realizar una evaluación exhaustiva de las necesidades específicas de la organización, considerando factores como el tipo de aplicaciones utilizadas, los requisitos de latencia y jitter, y la sensibilidad a la pérdida de paquetes.
- **Implementación de QoS**:
    - **MPLS**: Aprovechar las capacidades avanzadas de QoS inherentes a MPLS para aplicaciones críticas que requieren alta fiabilidad y consistencia para asegurar que las políticas de QoS estén bien definidas y alineadas con las prioridades del negocio.
    - **SD-WAN**: Configurar políticas de QoS flexibles y dinámicas a través de la plataforma vManage para adaptarse rápidamente a los cambios en el tráfico de red y garantizar un rendimiento óptimo.
- **Gestión Centralizada**:
    - Utilizar herramientas de gestión centralizada, especialmente en SD-WAN, para simplificar la administración y monitoreo de la red para permitir una configuración eficiente y una rápida adaptación a las necesidades cambiantes del tráfico de red.
- **Costos y Beneficios**:
    - **Análisis de Costos**: Realizar un análisis de costo-beneficio detallado para determinar la solución más económica sin comprometer la calidad del servicio en donde se debe considerar ya sea los costos iniciales de implementación como los costos operativos a largo plazo.

- **Optimización de Recursos**: Para empresas con presupuestos limitados, SD-WAN puede ofrecer una solución costo-eficiente aprovechando conexiones de Internet más económicas mientras mantiene un alto nivel de QoS.

- **Seguridad de la Red**:
  - **MPLS**: Aprovechar la naturaleza de red privada gestionada de MPLS para garantizar la seguridad de los datos, especialmente en industrias reguladas o con altos requisitos de seguridad.
  - **SD-WAN**: Implementar medidas de seguridad adicionales en SD-WAN para proteger las conexiones de Internet públicas, asegurando que las políticas de seguridad estén alineadas con los estándares corporativos.

- **Escalabilidad y Futuro Crecimiento**:
  - Considerar la escalabilidad de la solución elegida para soportar el crecimiento futuro de la empresa como tecnología actual se puede evidenciar que SD-WAN ofrece una mayor flexibilidad para escalar la red de manera eficiente en comparación con MPLS.

- **Elección Recomendada:**
  - **SD-WAN:** Recomendaría SD-WAN para infraestructuras donde se busca flexibilidad y eficiencia en el manejo del ancho de banda, especialmente si se necesita cambios frecuentes en las necesidades de la red o para optimizar costos operativos sin sacrificar el rendimiento.
  - **MPLS:** Por otro lado, MPLS sería la opción ideal para priorizar la estabilidad y la baja latencia para aplicaciones críticas como VoIP o sistemas de videoconferencia, donde la consistencia en el rendimiento es fundamental.

10. Bibliografía:

| Network, Academy. io. (2023, marzo 10). *LAB 5—Cisco SD-WAN QoS*. https://www.networkacademy.io/ccie-enterprise/sdwan/qos

Alwasel, K., Jha, D. N., Hernandez, E., Puthal, D., Barika, M., Varghese, B., Garg, S. K., James, P., Zomaya, A., Morgan, G., & Ranjan, R. (2020). IoTSim-SDWAN: A simulation framework for interconnecting distributed datacenters over Software-Defined Wide Area Network (SD-WAN). *Journal of Parallel and Distributed Computing*, *143*, 17-35. https://doi.org/10.1016/j.jpdc.2020.04.006

ANDRES, C. (2020, noviembre 12). *Qué es SD-WAN y cuáles son sus principales beneficios*. https://integracion.cube.net.ar/blog/sd-wan-beneficios

Bannour, F., Souihi, S., & Mellouk, A. (2018). Distributed SDN Control: Survey, Taxonomy, and Challenges. *IEEE Communications Surveys & Tutorials*, *20*(1), 333-354. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2017.2782482

bxavier. (2023, septiembre 1). Tecnologías SASE: El perímetro de servicio de acceso seguro. *Ikusi MX*. https://www.ikusi.com/mx/blog/tecnologias-para-sase/

Chiradeep, B. (2022, septiembre 8). *Understanding the Role of MPLS in Networking*. https://www.spiceworks.com/tech/networking/articles/what-is-mpls/

Cisco. (2024a). *Software Download—Cisco Systems*. https://software.cisco.com/download/home/286320995/type

Cisco Admin. (2020, febrero 13). *IOSvL2—More info (updated 10/2/15)*. https://learningnetwork.cisco.com/s/article/iosvl2-more-info-updated-10-2-15-x

Cisco Netacad. (2020, marzo 24). *Cisco Packet Tracer—Networking Simulation Tool*. Networking Academy. https://www.netacad.com/courses/packet-tracer

Cisco, S. A. (2024b). *Preguntas frecuentes sobre Calidad de servicio (QoS)*. Cisco. https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/22833-qos-faq.html

cloudflare. (2024). *Qué es SD WAN y cómo funciona | Administración de redes | Cloudflare*. https://www.cloudflare.com/es-es/learning/network-layer/what-is-an-sd-wan/

Community | GNS3. (s. f.). Recuperado 23 de abril de 2024, de https://www.gns3.com/community/featured

DCLessons. (2020). *Cisco Viptela Architecture | Cisco Viptela Design | Guide, Lab, Training & Certification*. DCLessons. https://www.dclessons.com/sd-wan-solution-overview-components

Edison Coimbra. (2017, mayo 11). *9.8 mpls*. SlideShare. https://es.slideshare.net/CristianTipanguano/98-mpls

edualejo77. (2011, agosto 16). VPN's y MPLS cuál es su relación??? *Edualejo77's Blog*. https://edualejo77.wordpress.com/2011/08/16/vpns-y-mpls-cual-es-su-relacion/

Ergun, R. (2021, enero). https://www.ietf.org/rfc/rfc3031.txt

Field Engineer. (2024). *Top 15 SD-WAN Vendors & Companies | Field Engineer*. https://www.fieldengineer.com/sd-wan/top-15-sd-wan-vendors

Ghanwani, A., Jamoussi, B., Fedyk, D., Ashwood-Smith, P., Li, L., & Feldman, N. (2000). Traffic engineering standards in IP-networks using MPLS. *Communications Magazine, IEEE*, *37*, 49-53. https://doi.org/10.1109/35.809384

Gracia, A. V. B., Jarrín, A. A. C., Gavilanes, L. M. V., & Moreno, I. I. M. (2007). *Diseño e Implementación Mediante el Simulador Dynamips de una Red MPLS para la Conexión WAN de una Empresa Mediana con sus Sucursales*.

Guanoluisa Jaramillo, E. D. (2019). *Diseño de la arquitectura de una red SDN mediante el protocolo Openflow con simulación en el software mininet para la infraestructura de una PYMES* [bachelorThesis, Quito: Universidad de las Américas, 2019]. http://dspace.udla.edu.ec/handle/33000/10884

Javier Jiménez. (2024, enero 7). *Qué simuladores de red utilizar para aprender redes con routers y switch*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/programas-simular-red/

Julio, J. (2022, noviembre 14). *Configuración de una red privada virtual (VPN) MPLS básica*. Cisco. https://www.cisco.com/c/es_mx/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html

Juniper Networks. (2024). *SD-WAN: Todo lo que hay que saber*. Juniper Networks. https://www.juniper.net/mx/es/research-topics/sd-wan-explained.html

KeepSolid Inc. (2024). *¿Qué es el protocolo VPN L2TP? | Disponible en VPN Unlimited*. https://www.vpnunlimited.com/es/help/vpn-protocols/l2tp-protocol

Liu, L., Chen, L., Xu, H., & Shao, H. (2020). Automated Traffic Engineering in SDWAN: Beyond Reinforcement Learning. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 430-435. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162994

Pepelnjak, I., & Guichard, J. (2002). *MPLS and VPN architectures* (CCIP ed). Cisco Press.

Pooja, K. (2023). *Implementación de QoS en Cisco SD-WAN*. Cisco. https://www.cisco.com/c/es_mx/support/docs/routers/vedge-router/213408-implement-qos-in-cisco-sd-wan.html

Prensario. (2023, octubre 30). SD-WAN Versus MPLS: Comparación de arquitecturas y soluciones WAN. *Prensario Tila*. https://prensariotila.com/sd-wan-versus-mpls-comparacion-de-arquitecturas-y-soluciones-wan/

Ramón Millan. (2022, junio 6). *Qué es... MPLS (MultiProtocol Label Switching)*. https://www.ramonmillan.com/tutoriales/mpls.php

Rejón, J. (2019, mayo 14). *Simulador de red GNS3 – mundotelematico.com*. https://www.mundotelematico.com/simulador-de-red-gns3/

Tomsu, P. (2001). *MPLS Implementation Status Advanced MPLS VPNs*.

Top 15 SD-WAN Vendors & Companies | Field Engineer. (s. f.). Recuperado 26 de marzo de 2024, de https://www.fieldengineer.com/sd-wan/top-15-sd-wan-vendors

Valdivia, J. R. G., & Peña, C. M. (s. f.). *MPLS Y SU APLICACIÓN EN REDES PRIVADAS VIRTUALES*. *83*.

Yang, K., Guo, D., Zhang, B., & Zhao, B. (2019). Multi-Controller Placement for Load Balancing in SDWAN. *IEEE Access*, *PP*, 1-1. https://doi.org/10.1109/ACCESS.2019.2953723

Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. (2019a). Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities. *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, 1-9. https://doi.org/10.1109/ICCCN.2019.8847124

Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. (2019b). Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities. *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, 1-9. https://doi.org/10.1109/ICCCN.2019.8847124

11. Anexos

Anexo 1: Hoja de Acrónimos

ATM: Modo de Transferencia Asincrónica

BGP: Protocolo de Puerta de Enlace de Borde (Border Gateway Protocol)

CE: Customer Edge

DSCP: Differentiated Services Code Point

DNS: Sistema de Nombres de Dominio

DWDM: Dense Wavelength Division Multiplexing

ECR: Tasa de Egreso Comprometida (Committed Information Rate)

E-LSP: Label Switched Path de Expresión

FEC: Forwarding Equivalence Class

ICR: Tasa de Ingreso Comprometida (Committed Information Rate)

IETF: Internet Engineering Task Force

IP: Protocolo de Internet (Internet Protocol)

IPsec: Protocolo de Seguridad de la Capa de Internet (Internet Protocol Security)

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

L2TP: Protocolo de Túnel de Capa Dos (Layer 2 Tunneling Protocol)

LER: Label Edge Router

L-LSP: Label Switched Path de Longitud Fija

LSR: Label Switch Router

MPLS: Multiprotocol Label Switching

NGAV: Antivirus de Próxima Generación

NGFW: Firewall de Próxima Generación

OSI: Open Systems Interconnection

PE: Provider Edge

PHB: Per-Hop Behavior

PPTP: Protocolo de Túnel Punto a Punto (Point-to-Point Tunneling Protocol)

QoE: Calidad de Experiencia (Quality of Experience)

QoS: Calidad de Servicio (Quality of Service)

RFC: Request for Comments

SAAS: Software como Servicio

SDH: Hierarchical Synchronous Digital Hierarchy

SD-WAN: Red Definida por Software

TCP: Protocolo de Control de Transmisión (Transmission Control Protocol)

TDM: Multiplexación por División de Tiempo

VRF: Virtual Routing and Forwarding

VPN: Red Privada Virtual (Virtual Private Network)

WAN: Red de Área Amplia (Wide Area Network)

Anexo 2: Certificación de traducción del resumen.

CERTIFICADO DE TRADUCCION

Andres Baldassari
MA.App.Lng

CERTIFICO:

Haber realizado la traducción de español a inglés de la tesis titulada: "Comparativa de la Calidad de Servicio en Redes de Datos: MPLS vs. SD-WAN." **de autoría** DIEGO ENRIQUE CHALA FOLLECO con cédula de identidad Nro: 1715755474, egresado de la Facultad de la Energía, las Industrias y los recursos no Renovables de la Universidad Nacional de Loja, trabajo que se encuentra bajo la dirección del Ingeniero Marco Augusto Suing Ochoa Mg. Sc. previo a la obtención del título de Magister en Telecomunicaciones.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado hacer uso del presente documento en lo que creyere conveniente.

Quito 15 de Agosto de 2024

Andres Roberto Baldassari Casquete
Certified Translator MDT-3104-CCL-259519
Celular: (593) 098 7030 511
Mail: andresbaldassari@hotmail.com