VICERRECTORADO DE INVESTIGACIÓN,

INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

MAESTRÍA EN GERENCIA DE SISTEMAS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN GERENCIA DE SISTEMAS

TEMA: Análisis de Factibilidad Técnico y Económico entre una red MPLS Traffic Engineering (TE) con Ipsec y una red Sd-Wan moderna.

AUTOR: Bustos Sánchez, Cristian Santiago

DIRECTOR: Mg. Phd (C) Ing. Salazar Chacón, Gustavo David

Sangolquí - 2019

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICADO DEL DIRECTOR

Certifico que el trabajo de titulación, "***ANÁLISIS DE FACTIBILIDAD TÉCNICO Y ECONÓMICO ENTRE UNA RED MPLS TRAFFIC ENGINEERING (TE) CON IPSEC Y UNA RED SD-WAN MODERNA.***" fue realizado por el señor ***Bustos Sánchez, Cristian Santiago*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 10 de Diciembre de 2018

Firma:

.....

Ing. Gustavo Salazar, Mg. PhD (c)

C.C.: 171610479-7

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIA DE RESPONSABILIDAD

Yo, ***Bustos Sánchez, Cristian Santiago***, con cédula de ciudadanía n° 150086311-1, declaro que el contenido, ideas y criterios del trabajo de titulación: ***ANÁLISIS DE FACTIBILIDAD TÉCNICO Y ECONÓMICO ENTRE UNA RED MPLS TRAFFIC ENGINEERING (TE) CON IPSEC Y UNA RED SD-WAN MODERNA*** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 10 de Diciembre de 2018

Firma

.....

Cristian Santiago Bustos Sánchez

C.C.: 150086311-1

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN

Yo, ***Bustos Sánchez, Cristian Santiago*** *autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación:* ***ANÁLISIS DE FACTIBILIDAD TÉCNICO Y ECONÓMICO ENTRE UNA RED MPLS TRAFFIC ENGINEERING (TE) CON IPSEC Y UNA RED SD-WAN MODERNA*** *en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.*

Sangolquí, 10 de diciembre de 2018

Firma

.....

Cristian Santiago Bustos Sánchez

C.C.: 150086311-1

DEDICATORIA

A mi madre y hermanos porque creyeron en mí, me han dado ejemplos de superación y entrega para llegar a cumplir mis metas sean académicas o personales, siempre estuvieron impulsándome en los momentos que más necesitaba de ellos.

Cristian Santiago Bustos Sánchez

AGRADECIMIENTO

Agradezco a mi madre y hermanas, que han sido las personas que me han dado fortaleza y apoyado de manera incondicional en todo momento.

Al Ing. Gustavo Salazar, Mg. PhD (c), quien me han orientado en todo momento en la realización de este proyecto que es un escalón importante para cumplir mis objetivos y metas.

Cristian Santiago Bustos Sánchez

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

En el presente proyecto se diseñará e implementará de mantra experimental una red de transporte Multiprotol Label Switching (MPLS) con las siguientes características y equipamiento: Provider Router (P), Provider Edge (PE), Customer Edge (CE), Router Reflector con sistemas autónomos e IPv4 privadas, enrutamiento dinámico con Open Shortest Path First (OSPF) y Border Gateway Protocol (BGP); en la misma que se configurará dos tecnologías como Traffic Engineering (TE) y seguridad de la información (IPSec), de similar forma se configura una red Software-defined networking in a Wide Área Network (SD-WAN) sobre MPLS, posterior a esto se obtendrá valores de los siguientes indicadores: jitter, latencia, seguridad, ancho de banda y QoS con el propósito de realizar un análisis comparativo del desempeño de las tecnologías mencionadas y plasmar el resultado en un informe gerencial para proponer el empleo de la mejor red de transporte a los Proveedores de Servicio de Internet (ISP), también se realiza un análisis económico en base al costo total de propiedad (TCO), valor actual neto (VAN) y tasa interna de retorno (TIR) de las tecnologías de estudio.

***Palabras Clave*:** **Redes definidas por software**
Ingeniería de tráfico
Protocolo de seguridad de internet
Multiprotocolo de conmutación de etiquetas
Redes

ABSTRACT

In the present project, an MPLS multiprotol label change will be designed and implemented with the following features and equipment: provider router (P), provider edge (PE), customer edge (CE), route reflector with autonomous systems and IPv4 private, dynamic routing with the shortest open path (OSPF) and the border gateway protocol (BGP) in the same configuration that configures two technologies such as traffic engineering (TE) and information security (IPSec), in a similar way configures in the network MPLS software defined in the wire are SD-WAN network, later values of the following indicators are found: jitter, latency, security, bandwidth and QoS with the purpose of performing a comparative analysis of the performance of the technologies of the consultation and translate the result into a management report to propose the use of the best transport network to the Internet Service Providers (ISP), also performs an economic analysis based on the total cost of ownership (TCO), net present value (NPV) and internal rate of return (IRR) of the study technologies.

***Keywords*:** **Software defined networking**
Traffic Engineering
Internet protocol security
Multiprotocol label switching
Networking

CAPÍTULO I. Planteamiento del problema de investigación

Tema: Análisis de factibilidad técnico y económico entre una red MPLS Traffic Engineering (TE) con IPSec y una red SD-WAN moderna.

1.1 Antecedentes

Hoy en día, los departamentos de TI están bajo presión para hacer más con menos; es decir, administrar más sitios y clientes con presupuestos limitados y un equipo relativamente pequeño, todo sin reducir la confiabilidad y la seguridad. El alto costo de la conectividad WAN empresarial, el soporte y el personal, combinados con el crecimiento de aplicaciones de transmisión de datos con gran ancho de banda y servicios basados en la nube, está obligando a muchos administradores de red a buscar soluciones alternativas.

1.2 Problema Macro

En la actualidad, los Proveedores de Servicio de Internet (ISP) que tienen implementada una red Multiprotocol label switch (MPLS) no realizan encriptación de extremo a extremo para los servicios de transporte que brindan a sus clientes y no aprovechan el canal de respaldo establecido entre los terminales de la red, esto debido al desconocimiento de las tecnologías como Internet Protocol Security (IPSec) y Traffic Engineering (TE) que se pueden emplear de manera estructurada dentro de la red MPLS. En Ecuador no se tiene implementada la nueva tecnología de redes definidas por software (LAN, WAN y WLAN), con el proyecto se configura Software-Definition Networking in a wide área network (SD-WAN) para demostrar

su funcionalidad en una red MPLS y demostrar la viabilidad al implementarla en un ISP en el país.

1.3 Objetivo General

- Analizar el desempeño de una red MPLS con IPSec, Traffic Engineering (TE) y una red MPLS con SD-WAN, para que los ISP a nivel nacional y mundial tomen la mejor opción técnica y económica.

1.4 Objetivos Específicos

- Diseñar y simular una red experimental MPLS con todos sus componentes Provider Router (P), Provider Edge Router (PE), Customer Edge Router (CE) y protocolos de enrutamiento dinámico.
- Configurar sobre la red MPLS tecnología como Traffic Engineering (TE), seguridad de internet IPSec y SD-WAN.
- Contrastar los indicadores técnicos y económicos de las dos tecnologías.

CAPÍTULO II. Marco Teórico

2.1 Redes de Transporte

Las redes de transporte, o también llamadas redes de telecomunicaciones, permiten trasladar información mediante redes de transporte de información dependiendo del servicio que emite el transmisor y el receptor, las mismas que son diferentes.

2.1.1 Protocolo X.25

El protocolo X.25 fue creado en 1970, como un estándar internacional de telecomunicaciones (ITU-T), debido a la necesidad de contar con un protocolo de Wide Área Network (WAN) que conceptualice la comunicación entre un equipo terminal y de red. La red X.25 tiene tres elementos básicos como son: Equipo terminal de datos (DTE), equipo de circuito de datos (DCE) e intercambio de paquetes de conmutación (PSE).

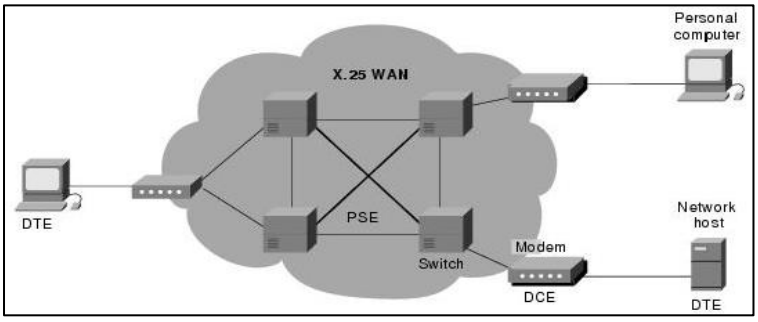

Figura 1. **Elementos de una red X.25**
Fuente (Baylon, 2017)

En la operación de X.25, se emplean los siguientes elementos:

- El ensamblaje y de samblaje de paquetes (PAD) está ubicado entre el DCE y el DTE, para tener un buffer de conmutación.
- El establecimiento de sesión entre los DTE son full-dúplex.
- Los circuitos virtuales, son de conmutación de circuitos virtuales (SCV) y conmutación de paquetes (PVC).

En X.25 tiene tres capas con las siguientes funciones:

1. Packet Layer Protocol (PLP) funciona en cinco modos distintos: configuración de llamada, transferencia de datos, inactivo, liberación de llamadas y reinicio.
2. Link Access Procedure Balanced (LAPB), las tramas de LAPB tienen información, supervisión y no números.
3. La capa X.21bits, define el medio físico eléctrico y electromecánico que se emplea. (Cisco, X.25, 2012)

2.1.2 NoBroadcast MultiAccess networks NBMA, ATM y Frame Relay

Asynchronous Transfer Mode Switching (ATM) es un estándar de la ITU-T orientado a la conexión para transmitir múltiples servicios como: datos, voz y video. Una red ATM consta de los siguientes elementos: Interfaz de red de usuario (UNI), interfaz de red pública en el nodo (P-NNI), emulación de la LAN (LANE) y multiprotocolo sobre ATM.

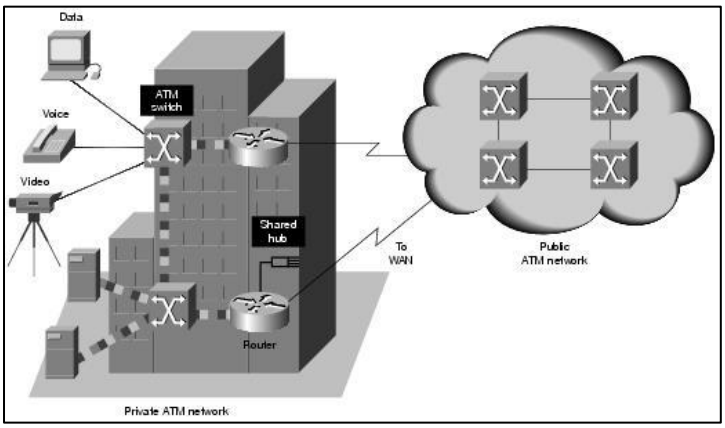

***Figura 2*. Redes ATM con datos, voz y video.**
Fuente (Emagister Servicios de Formación, s.f.)

Un paquete ATM tiene una trama de 53 bytes y los divide en cinco bytes de cabecera (Control de tráfico, identificador de camino virtual VPI, identificador de canal virtual VCI, priorización y control de errores) y 48 bytes de payload para los servicios (circuito virtual permanente PVC, circuito virtual conmutado SVC y servicios sin conexión SMDS). ATM tiene las capas con referencia al modelo OSI, con las siguientes funciones:

1. Capa física.- Convertir el flujo en bits, control de transmisión y recepción de bits, rastrear y empaquetado de celdas.
2. Capa ATM.- Comparte los circuitos virtuales por el medio físico, es decir, multiplexación y retransmisión de celdas con ayuda del VPI y VCI.
3. Capa de adaptación ATM.- Separa las funciones de la capa superior de los ATM, convierte los datos de usuario en celdas y segmentos. (Cisco, ATM, 2012)

Frame Relay, con estándar ITU-T y ANSI, fue diseñado para redes integradas de servicios digítales. Es una versión mejorada de X.25 y de similar forma opera en la WAN con mayor confiabilidad, rendimiento y eficiencia por operar en capa dos; emplea mecanismos para descongestionar la red, los cuales son: Notificación de congestión hacia adelante-explícita (FECN) y Notificación de congestión hacia atrás-explícita (BECN). El modo de operación de Frame Relay es por conmutación de circuitos virtuales y circuitos virtuales permanente, se puede observar los componentes de una red Frame Relay. (Figura. 3) (Cisco, Frame Relay, 2012)

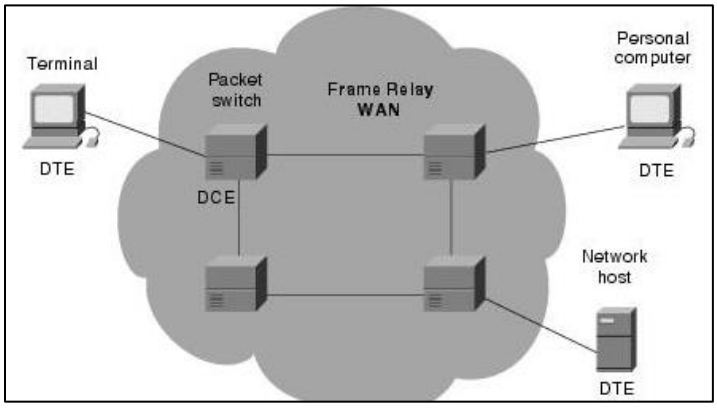

Figura 3. Red Frame Relay
Fuente (Gonzalez, 2009)

2.1.3 Metro Ethernet

Las redes Metro Ethernet están basadas en el estándar de Ethernet 802.3, son las que se encuentran en áreas metropolitanas o en el segmento WAN de una red, se podría decir que es una red de banda ancha que transporta los servicios de redes privadas, se considera a internet como un ejemplo de una red Metro Ethernet.

Dichas redes se emplean en capa 2 y 3, utilizan distintos medios de transmisión como par trenzado de cobre y fibra óptica, llegan a velocidades de 10 Mbps-10Base-T Ethernet, 100 Mbps-Fast Ethernet, 1000 Mbps-Gigabit Ethernet o un 1-Gigabit Ethernet con el estándar 802.ac. Los equipos terminales o de red son router y switch. En este tipo de redes se cuenta con diferentes tipo de topología como: bus, anillo, estrella o malla. Los principales componentes de una red Metro Ethernet son: Equipo de usuario (CE), Metro Ethernet Network (MEN) y una interfaz de usuario (UNIs).

2.1.4 MultiProtocol Label Switching (MPLS)

Multi Protocol Label Switching (MPLS) se inicia en los años 90, el mismo avanza en el mercado de manera exponencial y es adoptada por diversos proveedores a nivel mundial para sus redes de backbone debido a la necesidad de incrementar la capacidad de sus enlaces, luego de siete años de su creación se realizaron técnicas de conmutación de diferentes capas o también llamadas multinivel logrando el estándar actual.

MPLS está fundamentada por dos mecanismos esenciales como son: separación entre las funciones de control (routing) y de envío (forwarding), también se empleó las etiquetas para identificar los circuitos virtuales a lo largo de la red y así poder aplicar calidad de servicio. Es una red de nueva generación debido a que soporta multiservicios. En la actualidad, está desplazando a la tecnología IP/ATM,

por su técnica de enrutamiento acelerado de paquetes, debido que agrupa la característica de un switch como es la rápidez y la de un router que es la inteligencia.

2.1.5 Redes definidas por software SDN

SD-WAN utiliza un software y una infraestructura en la nube con el objetivo de garantizar la conectividad a los destinos remotos. Con el sotfware virtualizado que se aplica para el funcionamiento de la red permite a los encargados de TI tener una administración centralizada, segura, rápida, fiabilidad y calidad, que a su vez genera menores costos de TI y mayores beneficios. Estas conexiones se pueden emplear canales de internet con diferentes niveles de compartición y sin la necesidad de administración de direcciones públicas. Se ha visualizado y reflejado que en la actualidad las la nuevas aplicaciones y base de datos requieren un mayor consumo de ancho de banda al igual que tienen que ser distribuida por los diferentes canales de uplink.

2.2 Multi Protocol Label Switch MPLS

2.2.1 Características MPLS

Entre las características más importantes de la red MPLS se tienen:

- Opera entre la capa enlace y red del modelo OSI.
- Utiliza etiquetas para el marcado de los paquetes y enrutamiento.
- La calidad de servicio que se brinda depende del etiquetado del paquete.

- Soporta múltiples protocolos como unicast, multicast, ingeniería de tráfico, VPN, etc.
- Permite introducir QoS en redes IP.
- La unidad máxima de transferencia (MTU) soportada es mayor a 1500.
- En su implementación soporta diferentes tipos de redes como IP, ATM, Frame Relay, etc.
- Los servicios de MPLS se subdividen según la capa de uso, como es el caso capa 2 se tiene uvpls, l2vpn y en capa 3 con el l3vpls

2.2.2 Label Distribution Protocol (LDP)

MPLS es un mecanismo que permite el reenvío de paquetes que utiliza etiquetas añadidas en cada paquete IP. Para la asignación de etiquetas y su correspondiente distribución se la considera de la siguiente manera:

Para iniciar se emplea el protocolo de distribución de etiquetas LDP, el cual se encarga de establecer vecindades entre LSRs al remitir de forma continua mensajes de HELLO a las interfaces que se comunican con MPLS, las interfaces que han recibido el HELLO responden el mismo, permiten establecer adyacencias entre los routers y de esta manera son difundidos en la red con la dirección multicast 224.0.0.2, utilizan el puerto 646 tanto en TCP y UDP.

Los protocolos de enrutamiento (OSPF, EIGRP, IS-IS, etc.) generan la tabla de enrutamiento IP, a cada ruta es asignada una etiqueta, la asignación y anuncios de las etiquetas es realizada por los LSR, que tienen su propia base LIB, LFIB y FIB en donde se localizan todas las bases de las etiquetas que son intercambiadas entre LSR.

Posterior, se intercambian las etiquetas de entrada por las de salida, de dicho proceso se encargan los LSR, basándose en la LFIB de cada router.

Para finalizar, en la salida de los router LSR mueven la etiqueta y analizan la información de enrutamiento para el envío del paquete IP.

2.2.3 Ventajas MPLS

- Generan que la red sea escalable, es decir, es multiservicio.
- Permite calidad de servicio QoS.
- Posibilita la creación de clases de servicios.
- En el router de borde el ruteo es rápido
- Es una red de nueva generación.
- Garantiza un MTU mayor a 1500.
- Mejor desempeño en el reenvío de paquetes.
- No permite lazos en la red.

2.2.4 Calidad de Servicio en MPLS (QoS)

La calidad de servicio se encuentra considerada en la trama de etiquetas de MPLS, para lo cual se tiene un campo experimental con tres bits que permite ocho posibilidades al tener en cuenta los Time to Live (TTL).

Por defecto los tres bits del campo Differentiated Services Code Point (DSCP) (IP Precedence) de la cabecera IP son copiados al campo EXP de MPLS.

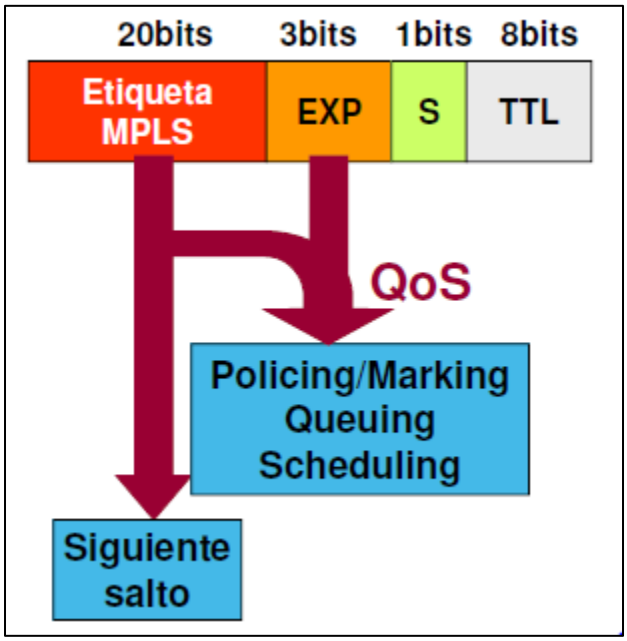

Figura 4. **Etiqueta QoS en MPLS**
Fuente (Piñeiro, 2015)

Los protocolos de distribución de etiquetas LDP identifican los lazos, los cuales son utilizados por los protocolos de Gateway interior que sirven para identificar los lazos (loops) que se utilizan para determinar el camino, en el caso de que existiera configuraciones erróneas podrían generarse lazos, por lo que en estos casos se

considera el campo TTL el cual sirve para controlar los lazos infinitos para esto se asigna el valor inicial de 255 en el campo TTL de la etiqueta, también se puede deshabilitar la propagación del TTL entre los routers de core en el dominio MPLS de manera inmediata se forma nuevas tablas de LFIB y FIB, basándose en la información que se encuentra en la base de datos de las etiquetas LIB.

2.2.5 Virtual Routing Forwarding VRF

Las VRF son empleadas para enrutamiento y envío de información de un grupo de subredes con idénticos requerimientos de conectividad. Están relacionados de forma habitual por un Router Distinguisher (RD) y los Router Target (RT) de import y export, estas VRF son asignadas a las interfaces físicas, loopback, subinterfaces y lógicas.

Es importante conocer que cada interfaz soporta una sola VRF, la misma que puede estar configurada en varias interfaces, a su vez una interfaz puede no pertenecer a ninguna VRF, pero puede recibir y enviar tráfico correspondiente a múltiples VPNs por la misma interfaz, esto se llama VRF selection usando PBR.

2.2.6 Router Distinguishers

El RD se utiliza para evitar duplicidad de direcciones de subred de los clientes, el cual se encarga de divulgar los prefijos IP de cada dirección y consigue un único prefijo identificable que convierte en exclusivas a las direcciones IP de cada cliente.

Los prefijos están formados de 64 bits obteniendo de esta manera una dirección IPv4 única de 96 bits, que es la suma de los 32 bits de una dirección IPv4 y los 64 bits de prefijo.

La dirección IP obtenida es la dirección VPNv4 que es intercambiada entre los PE routers mediante el protocolo BGP, que soporta otras familias de direcciones adicionales a las direcciones IPv4 y es llamado Multiprotocol IBGP (MP-BGP). MPLS VPN es usado dentro de un mismo sistema autónomo por lo que la sesión BGP entre los PE routers es siempre la sesión IBGP.

El RD, al ser configurado en el router, lleva la información del sistema autónomo y el número que diferencia las rutas.

Los router PE y LER son de border debido que están a los extremos de la red y ambos realizan etiquetado de los paquetes.

2.2.7 Route-target RT

Se presentan casos en que la función de los router distinguishers no es suficiente por lo que se utiliza el *route target* que permite usarse en más de una red privada virtual y soporta topologías complejas.

Los RT son propiedades adicionales anexas a las rutas BGP VPNv4 para indicar la participación de una VPN, dentro de BGP se utilizan las comunidades extendidas para codificar estos atributos, cualquier número de RTs pueden ser añadidos a una simple ruta.

Los prefijos del RT son de importación y exportación y cumplen las siguientes funciones:

Export RTs:

- Reconoce la intervención de cada red privada virtual
- Añade rutas al convertirse en prefijos VPNv4

Import RTs:

- Inscritos en cada tabla de enrutamiento virtual
- Adopta las rutas que se van a establecer en tabla de enrutamiento virtual

2.3 Software Definition Networking SD-WAN

2.3.1 Características de SD-WAN

En las redes SD-WAN se permite tener diferentes tipos de servicios y conexiones como datos, internet y LTE o de una red MPLS tradicional.

SD-WAN separa el plano de control del de datos, es decir, si pierde conexión a su plataforma de control los servicios siguen funcionando sin ningún inconveniente, añadiendo una sensación de mejora al usuario final.

Tiene una administración centralizada y mediante software, que permite la resolución de problemas de manera sencilla. (Networkworld, s.f.)

2.3.2 Funcionamiento SD-WAN

Las redes SD-WAN centralizan en el CE de manera física múltiples enlaces de diferentes tecnologías y servicios con el objetivo de ser visto como un único enlace lógico, producto de la suma del ancho de banda de los mismos. Con la concentración de canales permite garantizar el funcionamiento de las aplicaciones independiente que se presente delay, intermitencias o jitter altos en uno de los enlaces, debido a que los paquetes son enviados de manera automática por el mejor canal, para lo cual se consideran los siguientes parámetros: latencia de WAN a WAN, verifica el throughput y la calidad del enlace. Con el conocimiento adquirido de la red se puede tomar decisiones para priorizar el tráfico.

2.3.3 Ventajas SD-WAN

- Rápido instalación.- Se puede realizar la activación plug and play, debido a que se carga la configuración centralizada y con cambios remotos.
- Menor ancho de banda.- No se requiere canales dedicados de datos, se puede emplear con canales de internet compartidos y suma el ancho de banda de cada canal.
- Seguridad.- Garantiza seguridad de extremo a extremo, debido que implementa el protocolo de IPsec en la Virtual Protocol Network VPN.
- Redes Hîbridas.- Tiene diferentes métodos de integración de la VPN para no afectar la infraestructura actual y puede funcionar detrás de un firewall de nueva generación con enlaces de banda ancha.
- Calidad de servicio.- Con la administración de un canal agregado se puede tomar decisiones acogidas a las necesidades de la empresa. (Citrix, s.f.)

2.4 Internet protocol Security (IPsec)

IPSec (Internet Protocol Security) está definido por un conjunto de protocolos que buscan garantizar la seguridad en las comunicaciones sobre la capa de red a través de la autenticación y encriptación de los paquetes IP.

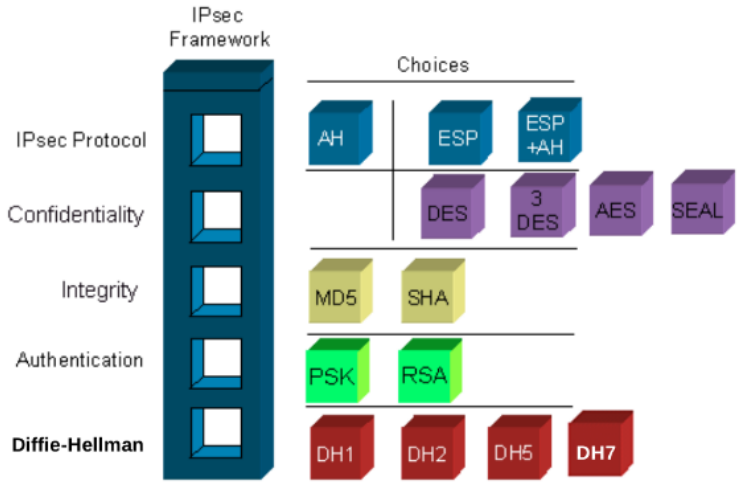

Figura 5. **IPsec Framework**
Fuente (Waas, 2017)

2.4.1 Características IPSec

IPsec ofrece las siguientes características:

- Confidencialidad, al utilizar algoritmos para cifrar la información antes de ser transmitida.
- Integridad, garantiza que la información no sea alterada durante la transmisión.
- Autenticación, verifica la identidad del origen y confiabilidad de los datos.

2.4.2 Funcionamiento IPSec

IPSec establece una comunicación segura entre dos pares a través de túneles, se define previamente los paquetes considerados sensibles y los parámetros que serán usados para protegerlos. Dichas especificaciones de seguridad, conocidas como asociaciones de seguridad (SA), son un conjunto de protocolos y algoritmos

que se aplican de forma unidireccional a un paquete IP y para un único protocolo (AH o ESP).

Para determinar el tráfico que será protegido es necesario configurar listas de acceso aplicadas a las interfaces mediante conjuntos de mapas criptográficos, lo cual permitirá establecer la conexión IPSec y definirá qué tráfico será permitido o dropeado entre los pares.

En caso de no existir una adecuada asociación de seguridad, se emplea el protocolo Internet Key Exchange Protocol (IKE) para negociar con los pares de IPSec las políticas necesarias para asegurar el circuito (algoritmos, protocolos, tiempo de vida).

Una vez finalizada la fase IKE1, se negocia el tipo de algoritmos criptográficos y material de claves para el intercambio de los datos en la fase IKE2.

Posterior a establecer la comunicación entre los pares IPSec, al concluir con el intercambio de paquetes los hosts descartan las llaves que se emplearon en las asociaciones de seguridad.

2.4.3 Modo de operación

- Transporte: Usado para la comunicación entre dos hosts, se encarga de cifrar o autenticar únicamente la carga útil del paquete IP conservando la cabecera IP intacta.
- Túnel: Se emplea para comunicaciones entre equipos que sirven como puerta de enlace en la red, es decir, comunicación host a host, host hacia una subred, o desde una subred hacia otra. En este modo de operación se cifra o autentica todo el paquete IP y se garantiza mayor seguridad en la comunicación.

2.5 Ingeniería de tráfico TE

La TE permite adaptar flujos de tráfico a recursos físicos de la red con el objetivo de evitar cuellos de botella cuando se tengan otros recursos que no se encuentren muy utilizados, en las redes IP convencionales los paquetes suelen seguir el camino más corto, esto suele provocar que algunos enlaces se saturen mientras otros están subutilizados, es decir, se requiere minimizar la congestión.

TE es una tecnología que permite utilizar los canales pasivos y tener control del tráfico que circula por cada uno de los enlaces que se interconectan en la red, para lograr el objetivo de desviar el tráfico se requiere un protocolo de Gateway interior para aplicar los nuevos caminos con su respectivo next-hot, que representaría un mejor camino tomando en consideración todas las métricas.(Adrián Delfino, 2000)

2.5.1 Características TE

Las características se las detalla por la orientación de minimización de performance.

- Orientada a tráfico.- Mejorar los indicadores de transporte de datos (minimizar perdida, minimizar retardo, maximizar rendimiento)
- Orientada a recursos.- Optimización de recurso de red (ancho de banda)Las dos características tienen como principal propósito descongestionar la red, debido que el congestionamiento de la red se evidencia de manera clara en las aplicaciones del cliente final y si no se aplica las opciones de TE o QoS llega a generar pérdidas económicas a las organizaciones, a nivel de red el congestionamiento presenta tiempos altos de latencia y jitter diverso.

2.5.2 Funcionamiento TE

1. Inicia con la identificación de los caminos primarios alrededor de conocidos puntos de congestionamiento en la red.
2. Análizar o verificar los segmentos de la red que se encuentren saturados con flujo de tráfico y conmutar el tráfico por otros enlaces de la red que se encuentran como backup pasivos o sin utilización.
3. Mejorar la utilización de todos los segmentos de la infraestructura de la red, con el objetivo de mejorar el performance de las aplicaciones y de los canales de comunicación que presenta un valor monetario a la organización.

4. Minimizar o eliminar si es el caso la saturación de los canales de comunicaciones y que se refleje en baja latencia a la de extremo a extremo.
5. Contar con un control del flujo que se desplaza por los distintos segmentos de la red y tener la capacidad de conmutar el tráfico de manera dinámica.

2.5.3 Desventajas TE

- Identifica y estructura metas y prioridades en términos de mejora de la calidad de servicio que se brinde a los usuarios de los servicios de red.
- Ayuda en la medición y análisis del cumplimiento de éstas metas.
- Adapta los flujos de tráfico a los recursos físicos de la red.

2.5.4 Componentes TE

La ingeniería de tráfico utiliza cuatro componentes.

- Packet fowarding
- Distribución de información
- Selección de camino
- Componente de señalización

2.5.4.1 Packet Fowarding

El packet forwarding es el primer componente, en una red MPLS los paquetes o subredes se convierten en prefijos o label, los mismos que son transmitidos o

intercambiados entre nodos por label switched path (LSP), cada uno de estas rutas se envía por label switching router LSR.

2.5.4.2 Distribución de Información

La distribución de información hace referencia a la base de datos de rutas que cada router tiene en su tabla obtenida del protocolo de Gateway internet IGP, para poder establecer TE por una ruta alterna que no se encuentre en la tabla de ruta y seleccionar un camino por otro enlaces.

2.5.4.3 Selección de caminos

Para la selección del camino en los LSP se considera la tabla de ruteo del IGP y el camino de TE que se ha desarrollado, en primer lugar el túnel se indica las prioridades que se va seguir.

2.5.4.4 Señalización

En la señalización hace referencia al LSP que estable el intercambio entre los terminales del segmento de la red, en MPLS maneja dos protocolos para la señalización como es RSPV y LDP.

CAPÍTULO III. Diseño de la red

3.1 Diseño de la red MPLS

En el capítulo anterior se describió los componentes de una red MPLS, que serán considerados en el diseño del presente proyecto y podrá ser empleado como bosquejo para fines de estudio o para proveedores de servicio de internet ISP.

3.1.1 Topología

En la topología de la Figura. 6, está conformado por cuatro Router Provider (P) de modelo cisco ASR920 interconectados entre sí y conforman un anillo de redundancia, por ocho Router Provider Edge (PE) cisco ASR901 que tienen dos conexiones WAN a diferentes P con el objetivo de tener redundancia en las conexiones de última milla de los PE, además dos Router Reflector (RR) cisco ASR920 que se conectan de similar forma que los PEs al P. Los equipos antes mencionados son el core o el backbone de la red MPLS, en sus extremos se tiene dos Router Customer Edge (CE) que se conectan con diferente última milla a distintos PE para ofrecer el esquema de dual PE.

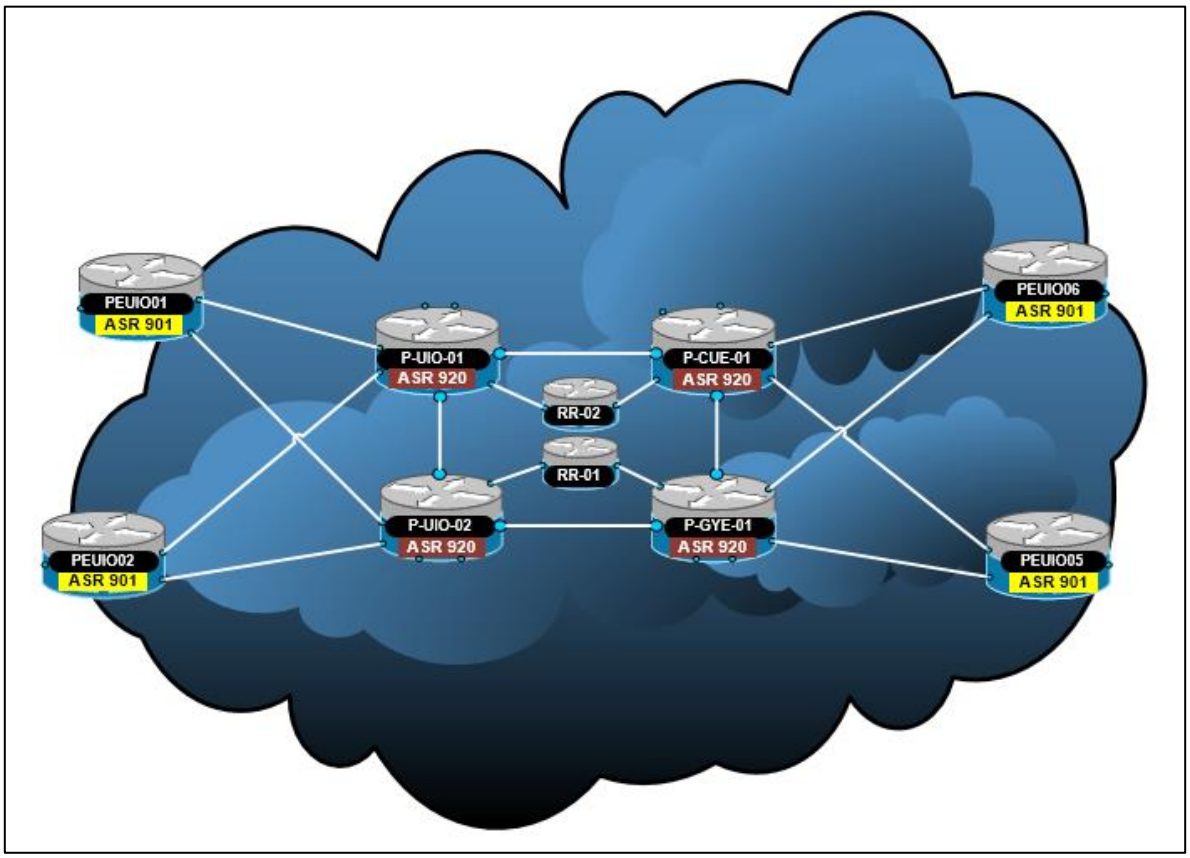

Figura 6. **Red MPLS de backbone**

3.1.2 Direccionamiento

Una de las características de la red MPLS es la seguridad intrínseca que tiene de extremo a extremo, al poseer un direccionamiento privado en la red de backbone.

En el presente proyecto se diseñó un direccionamiento con una subred privada clase B 172.16.0.0/16 subneteada con máscara de 30 bits, debido a que son conexiones punto a punto entre el P-P, P-PE, P-RR y PE-CE.

Tabla 1.
Subred en la red de backbone MPLS.

Punto a Punto		
Origen	Destino	Subred
P-UIO-01	P-CUE-01	172.16.0.0/30
P-UIO-01	P-UIO-02	172.16.0.4/30
P-UIO-01	RR-02	172.16.0.8/30
P-UIO-01	PE-UIO-01	172.16.0.12/30
P-UIO-01	PE-UIO-02	172.16.0.16/30
P-UIO-02	P-GYE-01	172.16.0.20/30
P-UIO-02	RR-01	172.16.0.24/30
P-UIO-02	PE-UIO-01	172.16.0.28/30
P-UIO-02	PE-UIO-02	172.16.0.32/30
P-CUE-01	P-GYE-01	172.16.0.36/30
P-CUE-01	RR-02	172.16.0.40/30
P-CUE-01	PE-CUE-01	172.16.0.44/30
P-CUE-01	PE-CUE-02	172.16.0.48/30
P-GYE-01	RR-01	172.16.0.52/30
P-GYE-01	PE-CUE-01	172.16.0.56/30
P-GYE-01	PE-CUE-02	172.16.0.64/30

Cada uno de los equipos de core cuenta con una subred de loopback de 32 bits, esta IP se utiliza como identificativo del equipo dentro de la red y realiza actualizaciones de los protocolos de enrutamiento.

Tabla 2.
IPs de loopback equipos de core

Equipo	IP Loopback
P-UIO-01	10.1.1.1/32
P-UIO-02	10.2.2.2/32
P-GYE-01	10.3.3.3/32
P-CUE-01	10.4.4.4/32
PE-UIO-01	172.32.0.1/32
PE-UIO-02	172.32.0.2/32
PE-CUE-01	172.32.0.3/32
PE-CUE-02	172.32.0.4/32
RR-01	10.5.5.5/32
RR-02	10.6.6.6/32

3.1.3 Enrutamiento

En la red de backbone MPLS se requiere emplear dos tipos de protocolos de enrutamiento, el primero es un protocolo de gateway interior (IGP) que será Open Shortest Path First (OSPF) configurado entre el P-PE, P-P y P-RR. El protocolo OSPF en área 0 ayuda a designar el enlace principal y el backup y es considerado para el control de las conexiones, como se ilustra en la siguiente tabla.

Tabla 3.
Sesión OSPF de la red backbone MPLS.

OSPF AS 100 Área 0			
Origen	Destino	Estado	Métrica
P-UIO-01	P-CUE-01	Principal	200
P-UIO-01	P-UIO-02	Backup	20000
P-UIO-02	P-GYE-01	Principal	200
P-UIO-01	P-UIO-01	Backup	20000
P-CUE-01	P-UIO-01	Principal	200
P-CUE-01	P-GYE-01	Backup	20000
P-GYE-01	P-UIO-02	Principal	200
P-GYE-01	P-CUE-01	Backup	20000
PE-UIO-01	P-UIO-01	Principal	200
PE-UIO-01	P-UIO-02	Backup	20000
PE-UIO-02	P-UIO-01	Principal	200
PE-UIO-02	P-UIO-02	Backup	20000
PE-CUE-01	P-CUE-01	Principal	200
PE-CUE-01	P-GYE-01	Backup	20000
PE-CUE-02	P-CUE-01	Principal	200
PE-CUE-02	P-GYE-01	Backup	20000
RR-01	P-UIO-01	Principal	200
RR-01	P-CUE-01	Backup	20000
RR-02	P-UIO-02	Principal	200
RR-02	P-GYE-01	Backup	20000

Para el intercambio de prefijos o etiquetas entre los PEs con el RR se utilizará un protocolo de gateway (BGP), para establecer las sesiones de BGP en L3VPN se utiliza el address-family vpnv4 y la comunicación entre el PE-CE emplea el address-family ipv4, estos intercambios de prefijos son designados con MP-BGP. En la tabla 4 se define los protocolos establecidos entre los elementos de la red MPLS.

Tabla 4.
Sesión MP-BGP de la red MPLS

IBGP 6300 vpnv4				
Origen	Destino	Estado	Métrica in	Métrica out
PE-UIO-01	RR-02	Principal	1000	6300
PE-UIO-01	RR-01	Backup	100	6300 6300 6300
PE-UIO-02	RR-02	Principal	1000	6300
PE-UIO-02	RR-01	Backup	100	6300 6300 6300
PE-CUE-01	RR-02	Principal	1000	6300
PE-CUE-01	RR-01	Backup	100	6300 6300 6300
PE-CUE-02	RR-02	Principal	1000	6300
PE-CUE-02	RR-01	Backup	100	6300 6300 6300

3.1.4 Equipos

La red MPLS diseñada y simulada en GNS3 con router de sistema operativo IOS Cisco, como se detalla en la tabla 5.

***Tabla 5*.**
Router de la red de backbone

Equipo	Modelo	Descripción
P-UIO-01	ASR920	Provider uno en Quito
P-UIO-02	ASR920	Provider dos en Quito

CONTINUA

P-CUE-01	ASR920	Provider en Cuenca
P-GYE-01	ASR920	Provider en Guayaquil
PE-UIO-01	ASR901	Provider edge uno en Quito
PE-UIO-02	ASR901	Provider edge dos en Quto
PE-CUE-01	ASR901	Provider edge uno en Cuenca
PE-CUE-02	ASR901	Provider edge dos en Cuenca
RR-01	ASR920	Route reflector uno
RR-02	ASR920	Route reflecto dos

3.2 IPsec

3.2.1 Topología

Se asegura la transmisión de la información de extremo a extremo, como se tiene dos última millas se agrega un CPE para tener una solo WAN y LAN definidas de manera clara el momento de levantar la IPsec.

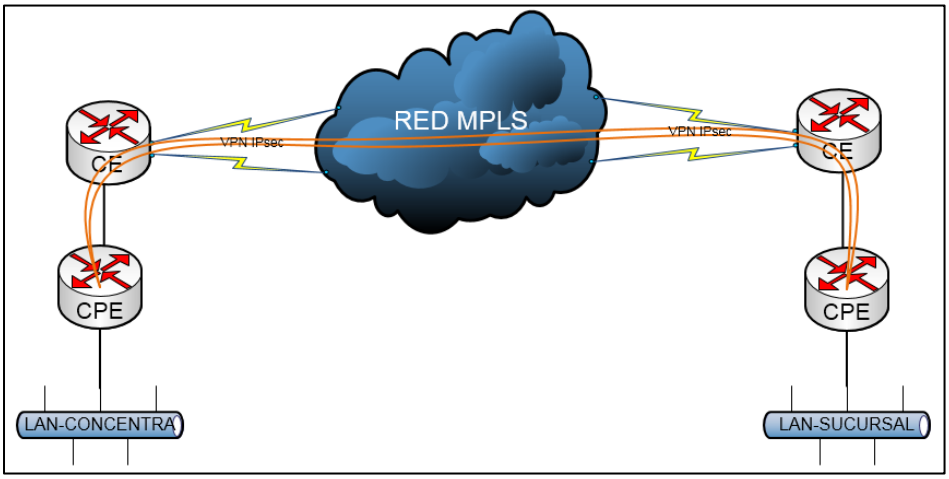

Figura 7. **IPsec entre el concentrador y la sucursal**

3.2.2 Direccionamiento

La siguiente tabla detalla las subredes utilizadas entre el PE-CE y CE-CPE.

Tabla 6.
Subredes de la WAN

Punto a Punto		
Origen	Destino	Subred
PE-UIO-01	CE-Concentrador	172.16.0.0/30
PE-UIO-02	CE-Concentrador	172.16.0.4/30
PE-CUE-01	CE-Sucursal	172.16.0.8/30
PE-CUE-02	CE-Sucursal	172.16.0.12/30
CE-Concentrador	CPE-Concentrador	172.16.0.16/30
CE-Sucursal	CE-Sucursal	172.16.0.20/30

Para aplicar calidad de servicio en la LAN, se divide los servicios en vlan y subred como se presenta en la tabla.

Tabla 7.
Subredes de la LAN

Sucursal	Servicio	Vlan	Subred
CE-Concentrador	Datos	10	192.168.1.0/24
CE-Concentrador	Video	20	192.168.2.0/24
CE-Concentrador	Voz	30	192.168.3.0/24
CE-Sucursal	Datos	10	192.168.10.0/24
CE-Sucursal	Video	20	192.168.11.0/24
CE-Sucursal	Voz	30	192.168.12.0/24

3.2.3 Enrutamiento

El PE y CE tienen dos conexiones para redundancia, la conexión principal tiene mejores métricas de BGP como se muestra en la siguiente tabla.

Tabla 8.
Sesión BGP entre PE y CE

EBGP 6300/6200 ipv4				
Origen	Destino	Estado	Métrica in	Métrica out
PE-UIO-01	CE-Concentrador	Principal	1000	6300
PE-UIO-02	CE-Concentrador	Backup	100	6300 6300 6300
PE-CUE-01	CE-Sucursal	Principal	1000	6300
PE-CUE-02	CE-Sucursal	Backup	100	6300 6300 6300

Las rutas entre el CE y CPE son estáticas y se las detalla en la tabla 9 siguiente:

Tabla 9.
Subred anunciada desde CE y CPE

Enlace	Network	Máscara
CE-Concentrador	192.168.1.0	255.255.255.0
CE-Concentrador	192.168.2.0	255.255.255.0
CE-Concentrador	192.168.3.0	255.255.255.0
CE-Sucursal	192.168.10.0	255.255.255.0
CE-Sucursal	192.168.11.0	255.255.255.0
CE-Sucursal	192.168.12.0	255.255.255.0

3.3 Traffic Enginerring (TE)

3.3.1 Topología

En la red de backbone MPLS se tiene redundancia de P y PE, si las conexiones principales PE-UIO-01, P-UIO-01, P-CUE-01, PE-CUE-01 están saturadas o desea utilizar otra ruta como la PE-UIO-01, P-UIO-02, P-GYE-01, PE-CUE-01, con el objetivo de aprovechar de mejor manera los enlaces.

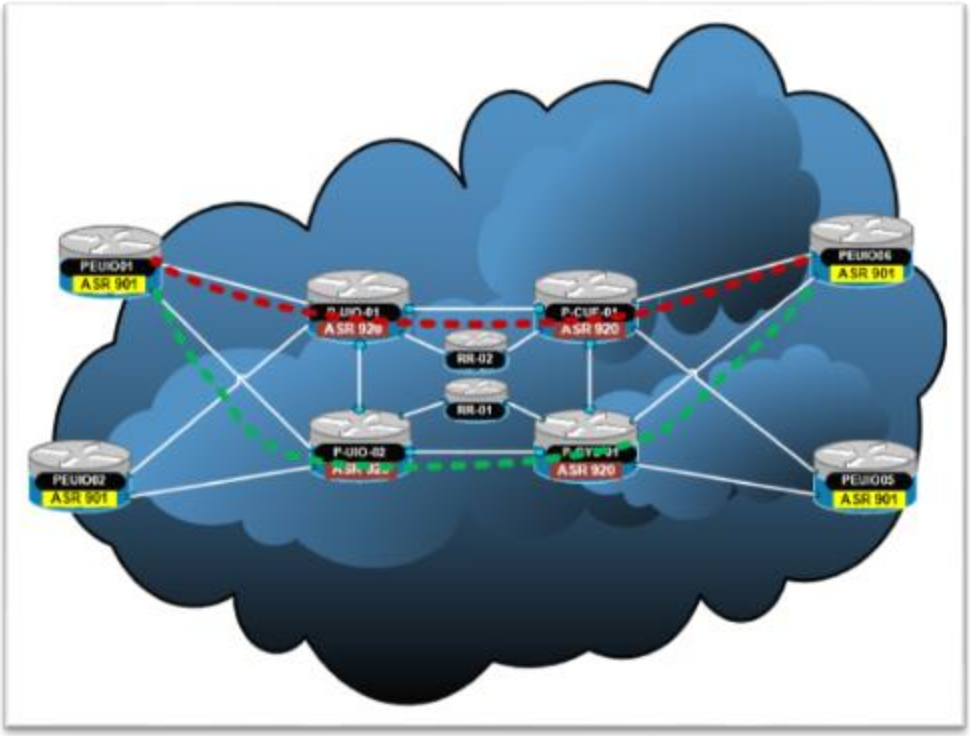

Figura 8. **Ingeniería de tráfico**

3.3.2 Direccionamiento y enrutamiento

En la siguiente tabla 10 se verifica las IPs por el enlace principal y por el alterno que se genera con ingeniería de tráfico.

Tabla 10.
Ruta principal y alterna TE

Principal	P o PE	Alterna	P o PE
172.16.0.14	PE-UIO-01	172.16.0.30	PE-UIO-01
172.16.0.13	P-UIO-01	172.16.0.29	P-UIO-02
172.16.0.2	P-UIO-01	172.16.0.21	P-UIO-02
172.16.0.1	P-CUE-01	172.16.0.22	P-GYE-01
172.16.0.45	P-CUE-01	172.16.0.57	P-GYE-01
172.16.0.46	PE-CUE-01	172.16.0.58	PE-CUE-01

3.4 Diseño SD-WAN

3.4.1 Topología

La red SD-WAN tiene un enlace de internet y datos, los dos enlaces son conexiones WAN que se concentran en el CE y se interconectan a nubes diferentes de MPLS e internet, además la conexión de red interna.

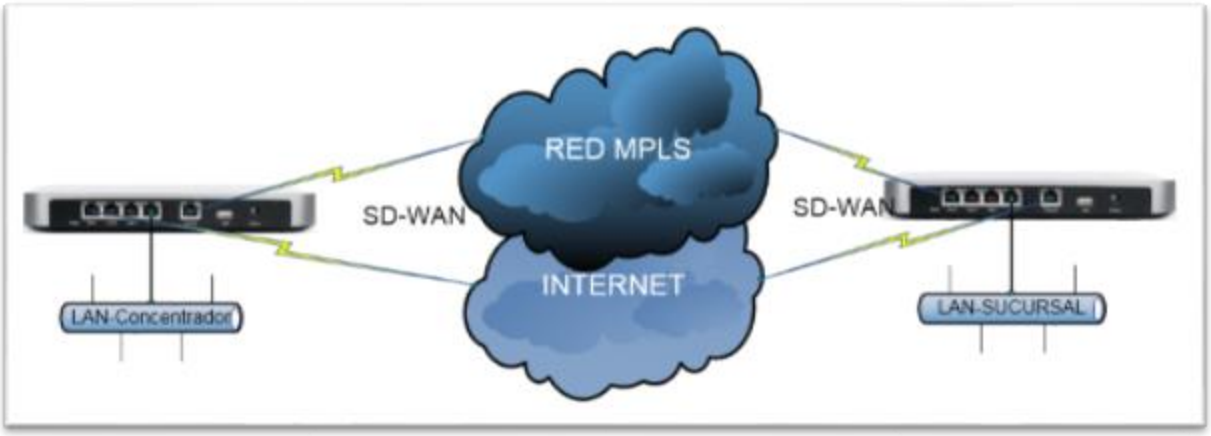

Figura 9. Red SD-WAN

3.5.2 Direccionamiento

La WAN del CE tiene dos direcciones IP una pública de internet y otra IP pública dentro de la red MPLS, y se incluyen las subredes LAN con su respectiva VLAN asignada a los servicios en matriz y sucursal, que se detalla en la tabla 11.

Tabla 11.
Direcciones WAN SD-WAN

	Punto a Punto	
Origen	Destino	Subred
PE-UIO-01	CE-Concentrador	200.105.251.136/30
PE-UIO-02	CE-Concentrador	190.57.150.124/30
PE-CUE-01	CE-Sucursal	190.12.54.156/30
PE-CUE-02	CE-Sucursal	200.105.239.132/30

Tabla 12.
Direcciones LAN SD-WAN

Sucursal	Servicio	Vlan	Subred
CE-Concentrador	Datos	1	192.168.0.0/24
CE-Concentrador	Video	20	192.168.2.0/24
CE-Concentrador	Voz	30	192.168.3.0/24
CE-Sucursal	Datos	1	192.168.100.0/24
CE-Sucursal	Video	20	192.168.11.0/24
CE-Sucursal	Voz	30	192.168.12.0/24

3.4.2 Enrutamiento

En SD-WAN no requiere tener un protocolo de enrutamiento entre el PE y CE, solo configurar el Gateway en cada interfaz del CE, la ruta por defecto se instala de manera automática por cada WAN y selecciona las subredes de la LAN que van a formar parte de la VPN. El dashboard de Cisco-Meraki con un clip genera el balanceo de la carga con las dos interfaces WAN.

3.4.3 Equipos

En SD-WAN se requiere en el concentrador un router Cisco Meraki modelo MX64 que tiene un puerto WAN de capa 3, un puerto USB y 4 puertos LAN de capa 2.

Figura 10. **Cisco Meraki MX64**
Fuente (CISCO, 2018)

CAPÍTULO IV. Implementación

4.1 RED MPLS

La red MPLS está diseñado en GNS3 2.1.3 con respaldo en Vmware Workstation Pro 14 en Linux con IOS de i86bi-linux-l3-adventerprisek9-15.4.2T.bin, router de 8 interfaces seriales y 8 ethernet.

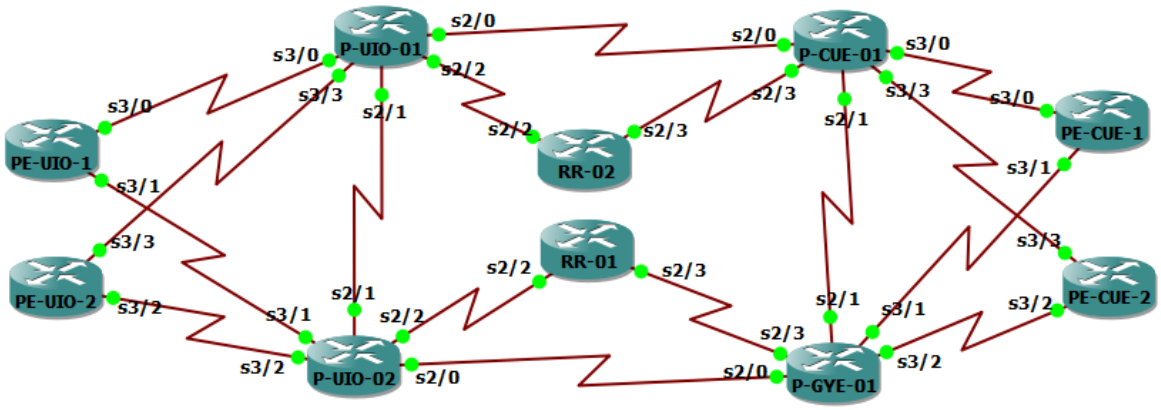

Figura 11. **Red MPLS en GNS3**

4.1.1 Direccionamiento

Todos los equipos de la red backbone de MPLS tienen asignado un nombre y desactivada la búsqueda recurrente de nombres de dominios.

```
P-UIO-01(config)#hostname P-UIO-01  ¨ Nombre del router ¨
P-UIO-01(config)#no ip domain lookup ¨Desactivar búsqueda recurrente¨
```

Los cuatro Ps se configura las interfaces seriales con la subred que se asignó en el anterior capítulo, se activa la interfaz y una descripción con respecto al equipo que se conecta de manera directa.

```
P-UIO-01(config)#interface serial 2/0
P-UIO-01(config-if)# ip address 172.16.0.1 255.255.255.252
P-UIO-01(config-if)#no shutdown
```

Las interfaces del P quedan configuradas con las siguientes IPs, también se comprueba el status y el protocolo esta ¨up¨

```
P-UIO-01#sh ip interface brief | inc 172.16.0
Interface              IP-Address      OK? Method Status                Protocol
Serial2/0              172.16.0.1      YES manual up                    up
Serial2/1              172.16.0.5      YES manual up                    up
Serial2/2              172.16.0.9      YES manual up                    up
Serial3/0              172.16.0.13     YES manual up                    up
Serial3/3              172.16.0.17     YES manual up                    up
```

En cada una de las interfaces tiene una descripción de conexión.

```
P-UIO-01#sh interfaces description | inc TO
Interface                      Status         Protocol Description
Se2/0                          up             up       TO P-CUE-01
Se2/1                          up             up       TO P-UIO-02
Se2/2                          up             up       TO RR-02
Se3/0                          up             up       TO PE-UIO-01
Se3/3                          up             up       TO PE-UIO-02
```

Un proceso similar se realiza en el resto de P, PE y RR de la red MPLS, con lo que se puede probar la conectividad punto a punto de los enlaces, con el protocolo icmp ¨ping¨ cómo se detalla a continuación:

```
P-UIO-01#ping 172.16.0.2 source 172.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.2, timeout is 2 seconds:
Packet sent with a source address of 172.16.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/10/12 ms
```

Se configura una interfaz virtual a los equipos de la red MPLS como identificativo IP y para realizar actualizaciones de las sesiones de enrutamiento dinámico.

```
P-UIO-01(config)#interface loopback 10
P-UIO-01(config-if)#ip address 10.1.1.1 255.255.255.255
P-UIO-01(config-if)#description *** P-UIO-01 ***
```

La configuración se visualiza de la siguiente manera:

```
P-UIO-01#show run | begin interface Loopback10
interface Loopback10
 description *** P-UIO-01 ***
 ip address 10.1.1.1 255.255.255.255

P-UIO-01#show run interface serial 2/0
Building configuration...
Current configuration : 174 bytes
!
interface Serial2/0
```

```
 description TO P-CUE-01
 ip address 172.16.0.1 255.255.255.252
serial restart-delay 0
end
```

4.1.2 Enrutamiento IGP (OSPF)

La sesión OSPF se establece entre los P to P, PE to P y RR con el P, con el objetivo de indicar cuál es el enlace principal y backup, con las prioridades de costo (200 enlace principal y 20000 backup) que se asignó en el capítulo anterior, también es necesario especificar que las redes son punto a punto.

```
P-UIO-01(config)#interface serial 2/0
P-UIO-01(config-if)#ip ospf network point-to-point
P-UIO-01(config-if)#ip ospf cost 200
```

El sistema autónomo utilizado para la sesión OSPF es el 100 en área 0, además se incluye un identificador para la sesión, que en este caso es la IP de la interfaz de loopback, y se especifica como una interfaz pasiva el momento que anuncia las subredes propias.

```
P-UIO-01(config)#router ospf 100
P-UIO-01(config-router)#router-id 10.1.1.1
P-UIO-01(config-router)#passive-interface loopback 10
P-UIO-01(config-router)#network 10.1.1.1 0.0.0.0 area 0
P-UIO-01(config-router)#network 172.16.0.0 0.0.0.3 area 0
P-UIO-01(config-router)#network 172.16.0.4 0.0.0.3 area 0
```

```
P-UIO-01(config-router)#network  172.16.0.8 0.0.0.3 area 0
P-UIO-01(config-router)#network  172.16.0.12 0.0.0.3 area 0
P-UIO-01(config-router)#network  172.16.0.16 0.0.0.3 area 0
```

Similares configuraciones se realiza en el resto de equipos de la red de backbone de MPLS, el método para comprobar que las mencionadas configuraciones son correctas es el comando ¨show ip ospf neighbor¨ que refleja un estado sesión ¨FULL¨.

```
P-UIO-01#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.32.0.2        0   FULL/  -        00:00:35    172.16.0.18     Serial3/3
172.32.0.1        0   FULL/  -        00:00:36    172.16.0.14     Serial3/0
10.6.6.6          0   FULL/  -        00:00:39    172.16.0.10     Serial2/2
10.2.2.2          0   FULL/  -        00:00:36    172.16.0.6      Serial2/1
10.4.4.4          0   FULL/  -        00:00:31    172.16.0.2      Serial2/0
```

4.1.3 Configuración de LDP

Las interfaces de los Ps, PEs se tienen que habilitar MPLS, para el intercambio de LDP de la red de backbone.

```
P-UIO-01(config)#interface serial 2/0
P-UIO-01(config-if)#mpls ip
```

Se visualiza los peer que se encuentran configurado MPLS y detalles como identidad, puertos de conexión, mensajes enviados, recibidos, tiempo de vecindad, interfaz y la IP de que se conecta.

```
P-UIO-01#show mpls ldp neighbor
    Peer LDP Ident: 10.6.6.6:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.6.6.6.21665 - 10.1.1.1.646
        State: Oper; Msgs sent/rcvd: 148/147; Downstream
        Up time: 01:45:05
        LDP discovery sources:
          Serial2/2, Src IP addr: 172.16.0.10
        Addresses bound to peer LDP Ident:
          172.16.0.10     10.6.6.6        172.16.0.42
```

```
P-UIO-01#show mpls ldp neighbor | inc Peer LDP Ident:
    Peer LDP Ident: 10.6.6.6:0; Local LDP Ident 10.1.1.1:0
    Peer LDP Ident: 172.32.0.1:0; Local LDP Ident 10.1.1.1:0
    Peer LDP Ident: 10.2.2.2:0; Local LDP Ident 10.1.1.1:0
    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
    Peer LDP Ident: 172.32.0.2:0; Local LDP Ident 10.1.1.1:0
```

Se recomienda que primero se pruebe la conectividad entre los PEs y RR, con el objetivo que no exista problemas el momento de levantar la sesión MP-BGP.

```
PE-UIO-1#ping 10.6.6.6 source 172.32.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 172.32.0.1
!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 18/19/21 ms



RR-02#ping 172.32.0.1 source 10.6.6.6
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.32.0.1, timeout is 2 seconds:
Packet sent with  a source address of 10.6.6.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/19/20 ms
```

También se sincroniza los LDP con la sesión OSPF en los PE y RR.

```
PE-UIO-1(config)#router ospf 100
PE-UIO-1(config-router)#mpls ldp sync
```

4.1.4 Enrutamiento MP-BGP (vpnv4)

Se configura las sesiones iBGP entre los PE y RR en el address-family vpnv4 con las interfaces de loopback con sistema autónomo AS de 63001, las siguientes configuraciones pertenecen al PE-UIO-01.

```
PE-UIO-1(config)#router bgp 63001
PE-UIO-1(config-router)#bgp router-id 172.32.0.1
PE-UIO-1(config-router)#bgp log-neighbor-changes
PE-UIO-1(config-router)#no bgp default ipv4-unicast
PE-UIO-1(config-router)#neighbor 10.5.5.5 remote-as 63001
PE-UIO-1(config-router)#neighbor 10.5.5.5 description TO RR-01
PE-UIO-1(config-router)#neighbor 10.6.6.6 remote-as 63001
PE-UIO-1(config-router)#neighbor 10.6.6.6 description TO RR-02
```

```
PE-UIO-1(config-router)#address-family vpnv4
PE-UIO-1(config-router-af)#neighbor 10.5.5.5 activate
PE-UIO-1(config-router-af)#neighbor 10.5.5.5 send-community both
PE-UIO-1(config-router-af)#neighbor 10.6.6.6 activate
```

PE-UIO-1(config-router-af)#neighbor 10.6.6.6 send-community both

Con parámetros similares se configura las sesiones iBGP RR-02 con el resto de Pes, pero se añade el comando que indica que es un route reflector tipo cliente.

```
RR-02(config)#router bgp 63001
RR-02(config-router)# bgp router-id 10.6.6.6
RR-02(config-router)# bgp log-neighbor-changes
RR-02(config-router)# no bgp default ipv4-unicast
RR-02(config-router)# neighbor 172.32.0.1 remote-as 63001
RR-02(config-router)# neighbor 172.32.0.1 description TO PE-UIO-01
RR-02(config-router)# neighbor 172.32.0.1 update-source Loopback10
RR-02(config-router)# neighbor 172.32.0.2 remote-as 63001
RR-02(config-router)# neighbor 172.32.0.2 description TO PE-UIO-02
RR-02(config-router)# neighbor 172.32.0.2 update-source Loopback10
RR-02(config-router)# neighbor 172.32.0.3 remote-as 63001
RR-02(config-router)# neighbor 172.32.0.3 description TO PE-CUE-01
RR-02(config-router)# neighbor 172.32.0.3 update-source Loopback10
RR-02(config-router)# neighbor 172.32.0.4 remote-as 63001
RR-02(config-router)# neighbor 172.32.0.4 description TO PE-CUE-02
RR-02(config-router)# neighbor 172.32.0.4 update-source Loopback10
RR-02(config-router)# address-family vpnv4
RR-02(config-router-af)#  neighbor 172.32.0.1 activate
RR-02(config-router-af)#  neighbor 172.32.0.1 send-community both
 RR-02(config-router-af)#  neighbor 172.32.0.1 route-reflector-client
RR-02(config-router-af)#  neighbor 172.32.0.2 activate
RR-02(config-router-af)#  neighbor 172.32.0.2 send-community both
RR-02(config-router-af)#  neighbor 172.32.0.2 route-reflector-client
RR-02(config-router-af)#  neighbor 172.32.0.3 activate
RR-02(config-router-af)#  neighbor 172.32.0.3 send-community both
```

```
RR-02(config-router-af)#  neighbor 172.32.0.3 route-reflector-client
RR-02(config-router-af)#  neighbor 172.32.0.4 activate
RR-02(config-router-af)#  neighbor 172.32.0.4 send-community both
RR-02(config-router-af)#  neighbor 172.32.0.4 route-reflector-client
```

4.1.5 Enrutamiento MP-BGP (IPv4 - VRF)

Se integra a la red de backbone los CE, que tiene dos conexiones la principal y backup, como se evidencia en la figura 12.

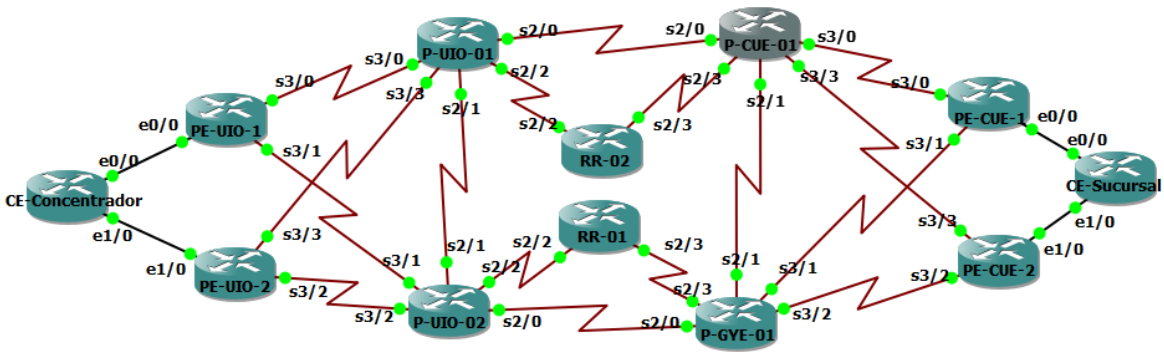

Figura 12. **Red MPLS con CE-Concentrador y CE-Sucursal**

En los 4 PE de la red MPLS se procede a crear la vrf con el nombre de datos, el rd 63001:100 e importar y exporta los prefijos del mismo route distinguer.

```
PE-UIO-1(config)#ip vrf datos
PE-UIO-1(config-vrf)# rd 63001:100
PE-UIO-1(config-vrf)# route-target export 63001:100
PE-UIO-1(config-vrf)# route-target import 63001:100
```

En el PE se configura la interfaz que tiene una descripción, la vrf que pertenece y la dirección como se indica a continuación.

```
PE-UIO-1(config)#interface Ethernet0/0
PE-UIO-1(config-if)# description *** CE-CONCENTRADOR-PRINCIPAL ***
PE-UIO-1(config-if)# ip vrf forwarding datos
PE-UIO-1(config-if)# ip address 172.16.0.1 255.255.255.252
```

En el PE y CE se establece una sesión EBGP con address family ipv4, el CE tiene un AS de 63600 y se redistribuye las conexiones directas.

```
router bgp 63001
 !
 address-family ipv4 vrf datos
  redistribute connected
  neighbor 172.16.0.2 remote-as 63600
  neighbor 172.16.0.2 description *** CONCENTRADOR PRINCIPAL ***
  neighbor 172.16.0.2 activate
  neighbor 172.16.0.2 as-override
 exit-address-family
```

Para poder identificar en la sesión entre el enlace principal y backup se modifica las métricas de BGP como es local preference y el as-path.

Route-map para el enlace principal de entrada

```
CE-Concentrador(config-route-map)#route-map principal-in permit 10
CE-Concentrador(config-route-map)# set local-preference 1000
CE-Concentrador(config-route-map)#route-map principal-in deny 20
```

Route-map para el enlace principal de salida con un AS de 63600

```
CE-Concentrador(config-route-map)#route-map principal-out permit 10
```

CE-Concentrador(config-route-map)# set as-path prepend 63600

CE-Concentrador(config-route-map)#route-map principal-out deny 20

Route-map para el enlace backup de entrada

```
CE-Sucursal(config)#route-map backup-in permit 10
CE-Sucursal(config-route-map)# set local-preference 100
CE-Sucursal(config-route-map)#route-map backup-in deny 20
```

Route-map para el enlace principal de salida con tres AS de 63600

```
CE-Concentrador(config-route-map)#route-map backup-out permit 10
CE-Concentrador(config-route-map)# set as-path prepend 63600 63600 63600
CE-Concentrador(config-route-map)#route-map backup-out deny 30
```

Se procede con la configuración de la sesión BGP entre el CE y PE

```
CE-Concentrador(config)#router bgp 63600
CE-Concentrador(config-router)# bgp router-id 172.16.0.2
CE-Concentrador(config-router)# no bgp log-neighbor-changes
CE-Concentrador(config-router)# neighbor 172.16.0.1 remote-as 63001
CE-Concentrador(config-router)# neighbor 172.16.0.1 description PRINCIPAL
CE-Concentrador(config-router)# neighbor 172.16.0.5 remote-as 63001
CE-Concentrador(config-router)# neighbor 172.16.0.5 description BACKUP
CE-Concentrador(config-router)# !
CE-Concentrador(config-router)# address-family ipv4
CE-Concentrador(config-router-af)#  redistribute connected
CE-Concentrador(config-router-af)#  redistribute static
CE-Concentrador(config-router-af)#  neighbor 172.16.0.1 activate
```

```
CE-Concentrador(config-router-af)#$172.16.0.1 route-map principal-in in
CE-Concentrador(config-router-af)#$172.16.0.1 route-map principal-out out
CE-Concentrador(config-router-af)# neighbor 172.16.0.5 activate
CE-Concentrador(config-router-af)#$172.16.0.5 route-map backup-in in
CE-Concentrador(config-router-af)#$172.16.0.5 route-map backup-out out
```

Se puede evidenciar con si la sesión BGP se encuentra activa y aprendiendo prefijos.

```
CE-Concentrador#sh ip bgp summary | inc 172.16.0.
BGP router identifier 172.16.0.2, local AS number 63600
172.16.0.1     4     63001     25     27     5     0     0 00:19:48     4
172.16.0.5     4     63001     26     31     5     0     0 00:19:48     4
```

De similar manera, se puede comprobar desde el PE

```
PE-UIO-1#sh ip bgp vpnv4 vrf datos summary | inc 172.16.0.2
172.16.0.2     4     63600     31     29     11     0     0 00:23:10     2
```

4.2 IPsec

4.2.1 CE Concentrador

En el CE se procede a crear la isakmp de fase 1, con encriptación 3DES, autenticación PRE-SHARE en un grupo 2 y un tiempo de vida de 86 400 ms.

```
CPE-Concentrador(config)#crypto isakmp policy 1
CPE-Concentrador(config-isakmp)#encryption 3des
CPE-Concentrador(config-isakmp)#authentication pre-share
```

```
CPE-Concentrador(config-isakmp)#group 2
```

```
CPE-Concentrador(config-isakmp)#lifetime 86400
```

Se crea la contraseña y la dirección IP de su destino.

```
CPE-Concentrador(config)#crypto isakmp key TeSiS2018 address 172.16.0.10
```

Se selecciona la subred origen y destino que van a ser transmitidas por IPsec, es decir el tráfico interesante de la VPN.

```
CPE-Concentrador(config)#ip access-list extended IPSEC-LAN
CPE-Concentrador(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.10.0 0.0.0.255
```

Se realiza una transformada con ESP-3DES y ESP-MD5-HMAC, este es el inicio de la Fase 2 de IKE (Internet Key Exchange)

```
CPE-Concentrador(config)#crypto ipsec transform-set TS-SUCURSAL esp-3des esp-md5-hmac
```

Se crea una crypto map para asociar el vecino, la transformada y la LAN que se emplea.

```
CPE-Concentrador(config)#crypto map CMAP-SUCURSAL 10 ipsec-isakmp
CPE-Concentrador(config-crypto-map)#set peer 172.16.0.10
CPE-Concentrador(config-crypto-map)#set transform-set TS-CONCENTRADOR
CPE-Concentrador(config-crypto-map)#match address IPSEC-LAN
```

Se aplica el cryto map en la WAN del enlace.

```
CPE-Concentrador(config)#interface eth0/0
CPE-Concentrador(config-if)#crypto map CMAP-SUCURSAL
```

Se desplegará un mensaje de iniciado la ISAKMP

```
*Nov 13 02:43:14.669: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Se puede verificar que la sesión IPsec y las subredes que intervienen están correctamente.

```
CE-Concentrador#show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 172.16.0.10 port 500
  Session ID: 0
  IKEv1 SA: local 172.16.0.2/500 remote 172.16.0.10/500 Active
  IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.10.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

4. 3 Ingeniería de tráfico TE

4.3.1 PE Concentrador

En el PE de UIO se habilita en la sesión OSPF para habilitar TE en la interfaz de loopback10 en área 0, además se agrega el camino alterno de la red MPLS para llegar al mismo destino.

```
PE-UIO-1(config)#router ospf 100
PE-UIO-1(config-router)#mpls traffic-eng router-id Loopback10
PE-UIO-1(config-router)#mpls traffic-eng area 0
PE-UIO-1(config)#ip explicit-path name PEUIO01_PUIO02_PGYE01_PECUE01



PE-UIO-1(cfg-ip-expl-path)#next-address 172.16.0.29
```

```
PE-UIO-1(cfg-ip-expl-path)#next-address 172.16.0.22
PE-UIO-1(cfg-ip-expl-path)#next-address 172.16.0.58
```

Se configura la interfaz tunnel de TE una descripción y se especifica que asigne la interfaz loopback 10 como ID del túnel, indica que es un túnel de TE, la ip destino, la prioridad, se garantiza el ancho de banda de banda y especifica el path.

```
PE-UIO-1(config)#interface tunnel 100
PE-UIO-1(config-if)#description *** TRAFFIC ENG - TO PE-CUE-01 ***
PE-UIO-1(config-if)#ip unnumbered loopback 10
PE-UIO-1(config-if)#tunnel mode mpls traffic-eng
PE-UIO-1(config-if)#tunnel destination 172.32.0.3
PE-UIO-1(config-if)#tunnel mpls traffic-eng priority 2 2
PE-UIO-1(config-if)#tunnel mpls traffic-eng bandwidth 20000
PE-UIO-1(config-if)#$tion 2 explicit name PEUIO01_PUIO02_PGYE01_PECUE01
PE-UIO-1(config-if)#tunnel mpls traffic-eng path-option 8 dynamic
```

Las configuraciones son similares en los PEs y Ps de la red L3MPLS.

4.4 SD-WAN

Con el fin de implementar SD-WAN se utilizaron equipos reales Cisco-Meraki con su correspondiente cloud.

Se integran los equipos al dashboard (visualización de cloud Meraki) con el objetivo de tener una administración centralizada, en el dashboard se añada cada MX64 con el número de serie y el nombre de la red TESIS-ESPE.

MAC address ▲	Serial number	Network	Model
0c:8d:db:df:de:00	Q2MN-77BH-RKG9	TESIS-ESPE - 2	MX64W
e0:cb:bc:2c:f0:48	Q2KN-LZ7R-EU4L	TESIS-ESPE - 1	MX64

Figura 13. **MX64 en el dashboard**

Se implementa la dirección geográfica de cada MX64.

Figura 14. **Ubicación geográfica MX64 Guayaquil**

4.4.1 Direccionamiento

Se configura dos direcciones IPs para las WANs desde el dashboard, en la WAN 1 se tiene una IP privada por DHCP.

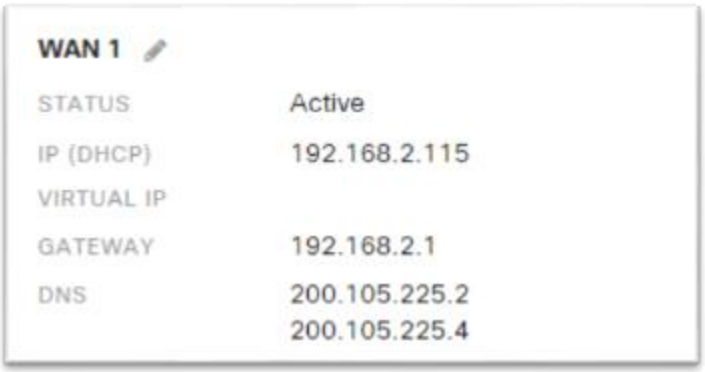

Figura 15. **WAN1 IPv4 privada DHCP**

La segunda WAN2 se configura una subred pública (IP, máscara y gateway), con sus respectivos DNS primario y secundario.

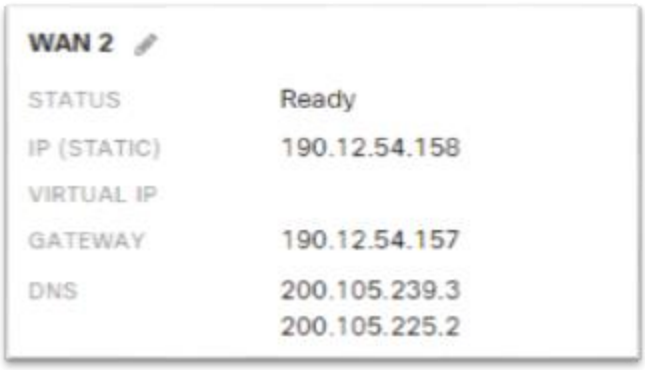

Figura 16. **WAN2 IPv4 pública estática**

Se habilita el modo de funcionamiento del MX, que se encuentra en el siguiente path *Security and SD--WAN--Configure--Addressing & VLANs*.

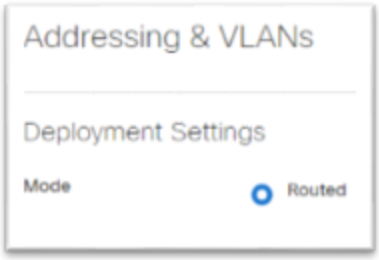

Figura 17. **Habilitar modo routed en el MX**

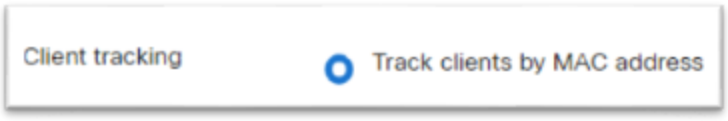

Figura 18. **Habilitar mismo subred**

Se configura una interfaz LAN en modo acceso con la subred IPv4 192.168.100.0/24, sin tag alguna en los puertos, cabe indicar que también permite configurar VLANs en modo trunk en cada uno de los puertos.

Figura 19. **Dirección IPv4 LAN remota**

Con las configuraciones que se detalla se tiene visibilidad de los equipos en el dashboard, para una administración centralizada y total.

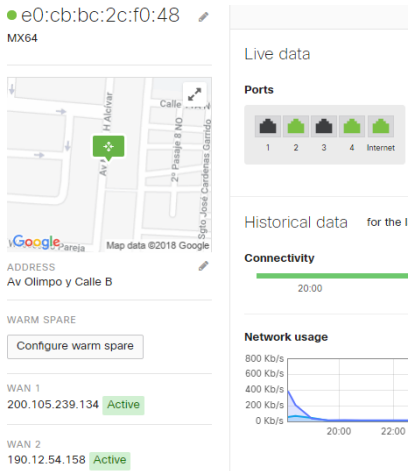

Figura 20. **Dashboard MX64 sucursal**

4.4.2 VPN HUB

Para la implementación de la VPN se ingresa a la pestaña *Secury&SD-WAN----Site-to-site-VPN,* para habilitar al concentrador el tipo de funcionamiento HUB y anunciar la subred LAN.

Figura 21. **Concentrador SD-WAN tipo HUB**

Si existe otros equipos en el dashboard que realicen la función de HUB se desplegarán de manera automático, en el presente proyecto se tiene un MX con dicha función.

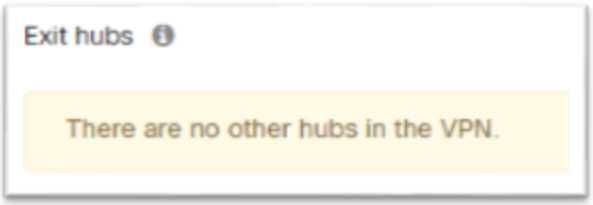

Figura 22**. Número de HUB MX**

Como se habilito la función de router también se especifica el tráfico interesante que va ser anunciado o intercambiado en la VPN.

Figura 23. **Tráfico interesante VPN HUB**

La VPN se tiene activado por defecto IPsec con las siguientes configuraciones de la fase 1 y fase 2.

Figura 24. **IPsec default SD-WAN**

Para aprender redes que se encuentren detrás de un router, se puede habilitar OSPF para facilitar el intercambio de información, además la opción de levantar VPN con equipos que sean de otro vendor.

4.4.3 VPN Spoke

Para la implementación de la VPN se ingresa a la pestaña Secury&SD-WAN----Site-to-site-VPN, para habilitar al equipo remoto el tipo de funcionamiento SPOKE y anunciar la subred LAN correspondiente.

Figura 25. **Tipo Remoto SD-WAN tipo SPOKE**

El remoto, con la funcionalidad de spoke, debe seleccionar el nombre del MX que fue designado como hub.

Figura 26. **Selección del nombre del Hub**

De similar forma que el MX tipo hub, se habilita la subred o tráfico interesante que se intercambia.

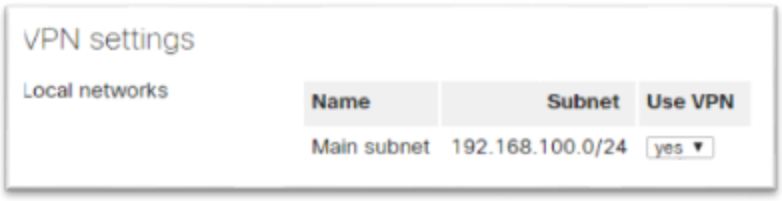

Figura 27. **Tráfico interesante VPN remoto**

4.4.4 Balanceo de tráfico

En la pestaña *Security&SD-WAN* se despliega la opción *SD-WAN&traffic-shaping* que se procede a seleccionar, en la nueva ventana se limita el ancho de banda de las interfaces WANs a 10 Mbps.

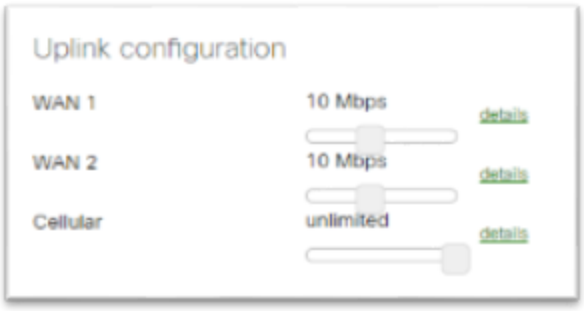

Figura 28. **Uplink 10 Mbps en las WANs**

En las dos interfaces se habilita balanceo de tráfico.

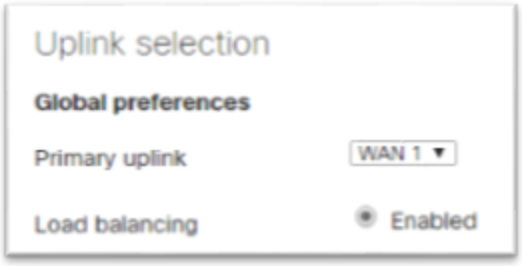

Figura 29 **Habilitar balanceo de las WANs**

4.4.5 Traffic Shaping QoS

Se crea tráfico de preferencias por las dos acceso a internet desde el MX, en las preferencia se configura el protocolo (TCP, UPD o ANY), la subred o host origen y destino, puertos de origen y destino, y la preferencia por la interfaz que requiere.

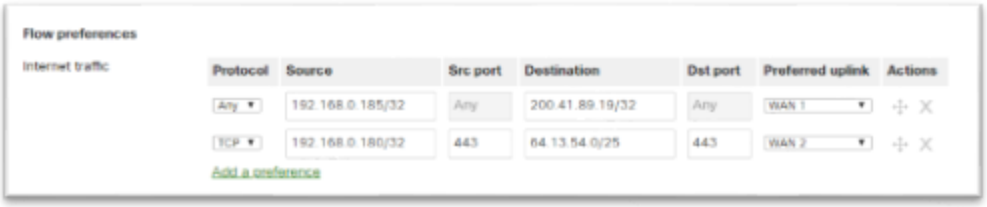

***Figura 30*. Preferencia de tráfico internet**

También se crea preferencia en el tráfico de SD-WAN interesante de la VPN, se prioriza el empleo de Skype que se direccione por la interfaz WAN1 y si presenta una baja performance conmute a la WAN2, con prioridad de tráfico de VoIP.

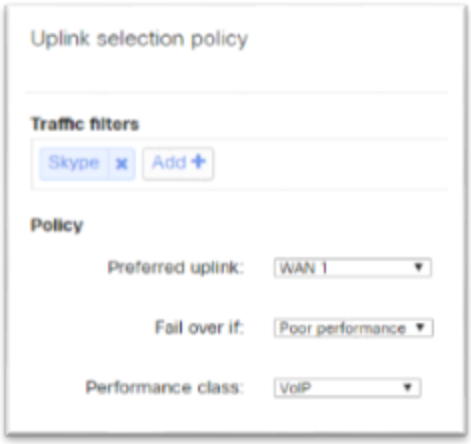

***Figura 31*. Priorizar el Skype por la WAN1**

Se puede personalizar el desempeño de la red, para aplicar en las políticas de priorización dependiendo de las necesidades del usuario final, en este caso se crea

una regla de nombre SERVER-SQL que hace referencia a los parámetros de latencia, jitter y paquetes perdidos.

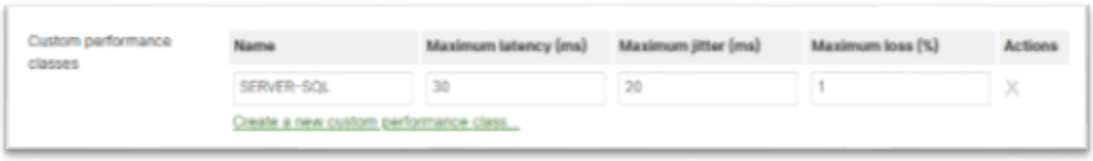

***Figura 32*. Personalizar latencia, jitter y pérdidas.**

En la nueva regla para servicio de iCloud y Backup de base de datos se aplica la política personalizada SERVER-SQL.

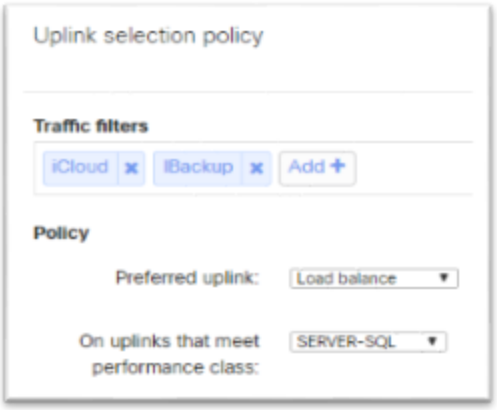

***Figura 33.* Regla iCloud con política personalizada.**

Se restringe que todos los usuarios de la red no pueden consumir un ancho de banda mayor a 2Mbps de bajada y 1Mbps de subida.

***Figura 34*. Restringir el ancho de banda a todos los usuarios.**

De similar forma se crea reglas con función en las aplicaciones, se limita el ancho de banda de su uso, el tipo de prioridad y el marcar, para ser categorizado en la red.

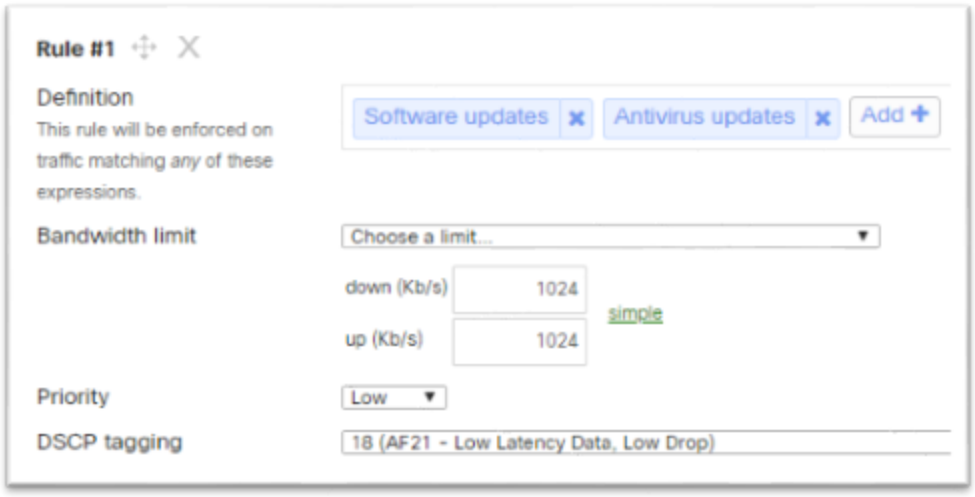

***Figura 35.* Regla de las aplicaciones**

CAPÍTULO V. Ejecución y Resultados

5.1 Pruebas de funcionamiento de la red MPLS

El escenario de la red MPLS que se desarrollaran las pruebas, es el mencionado en los capítulos anteriores de diseño e implementación, el mismo que fue simulado con la herramienta GNS3 que es open source y apoyado en una máquina virtual en Linux que trabaja como background con los IOS de los respectivos router utilizados.

Una red MPLS tipo L3VPN con cuatro P, cuatro PE, dos RR y dos CE, en los que encuentra configurados protocolos como OSPF, MP-BG, LDP, IPsec y TE. Para obtener las pruebas respectivas se ingresa por comand line interface CLI en cada uno de los equipos.

5.1.1 Conectividad de MPLS (Latencia, jitter y máximo unidad de transmisión)

Se verifica conectividad desde el CE concentrador hasta el CE remoto de LAN a LAN y se tiene una latencia promedia de 35 ms.

```
CE-Concentrador#ping 192.168.10.1 source 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 34/35/36 ms
```

Pruebas desde el CE concentrador hasta el CE remoto y se tiene una latencia similar de 35 ms.

```
CE-Concentrador#ping 192.168.10.1 source 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with  a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 34/35/36 ms
```

Para calcular el jitter, se da 6 pines desde el CE concentrador hasta el CE remoto y se tiene los siguientes valores:

```
Success rate is 100 percent (1/1), round-trip min/avg/max = 32/32/32 ms
Success rate is 100 percent (1/1), round-trip min/avg/max = 41/41/41 ms
Success rate is 100 percent (1/1), round-trip min/avg/max = 40/40/40 ms
Success rate is 100 percent (1/1), round-trip min/avg/max = 36/36/36 ms
Success rate is 100 percent (1/1), round-trip min/avg/max = 35/35/35 ms
Success rate is 100 percent (1/1), round-trip min/avg/max = 34/34/34 ms
```

Para obtener el jitter se resta entre los 6 valores de los ping de los enlaces.

Tabla 13.
Jitter del enlace

Repeticiones	Latencia	Cálculo	Jitter
1	32		
2	41	abs(41-32)	9
3	40	abs(40-41)	-1
4	36	abs(36-41)	-6
5	35	abs(35-36)	-1
6	34	abs(34-35)	-1

Se garantiza que la comunicación de LAN to LAN sea de 1500 de MTU.

```
CE-Concentrador#ping 192.168.10.1 source 192.168.1.1 size 1500 repeat 100
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 41/48/62 ms
```

5.1.2 Seguridad

Se puede verificar en el CE remoto que las subredes de origen y destino de datos están en la sesión de IPsec.

```
CPE-Sucursal#show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 172.16.0.2 port 500
  Session ID: 0
  IKEv1 SA: local 172.16.0.10/500 remote 172.16.0.2/500 Active
  IPSEC FLOW: permit ip 192.168.10.0/255.255.255.0 192.168.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

5.1.3 Convergencia de comunicación

El CE-Concentrador y CE-Remoto tienen comunicación full mesh con los elementos de la red L3MPLS, por lo que se procede a simular la caída en el PE-UIO-01 para garantizar la continuidad de comunicación de los equipos de la red, en la figura 36 se evidencia que se presentó una afectación en el PE-UIO-01 y se tiene 69 ping perdidos equivalente a 2 minutos con 17 segundos.

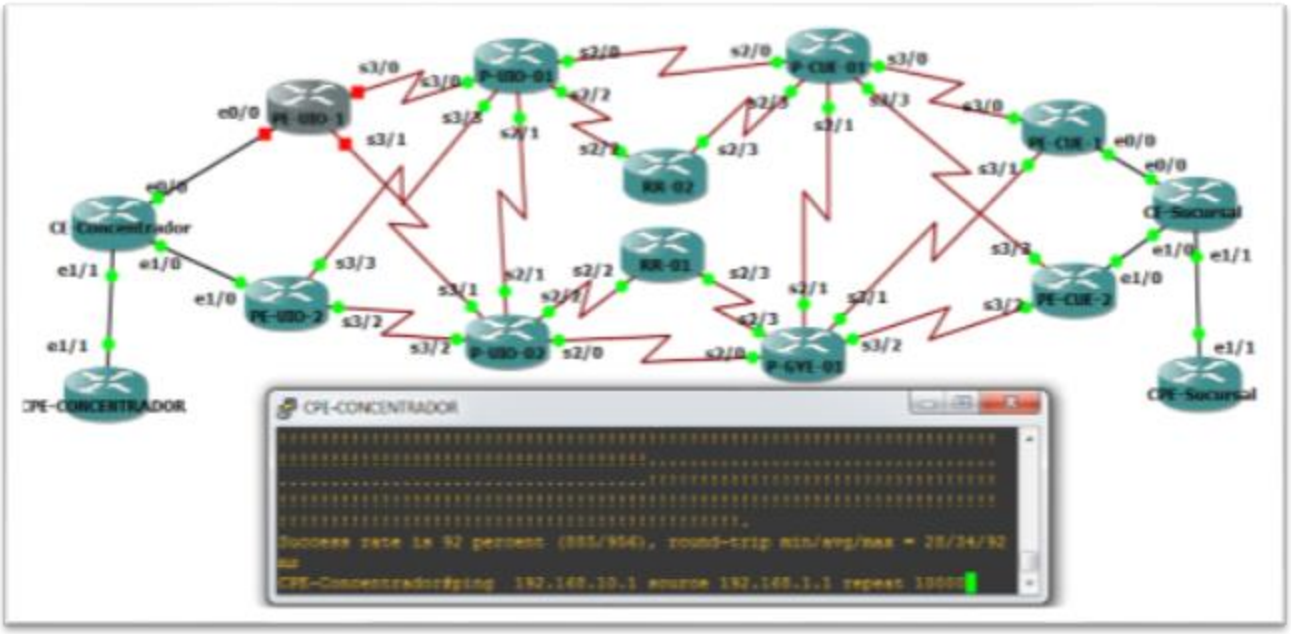

Figura 36. **Conmutación de red PE-UIO-01 down**

El traceroute desde el CE-Concentrador hasta el CE-Remoto de WAN a WAN por la ruta principal, se evidencia que el camino principal es de 7 pasos como se detalla en el camino que se genera en la IP 172.16.0.1 correspondiente al PE-UIO-01.

```
CPE-Concentrador#traceroute 172.16.0.22 source 172.16.0.18
Type escape sequence to abort.
Tracing the route to 172.16.0.22
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.0.17 3 msec 7 msec 6 msec
  2 172.16.0.1 5 msec 5 msec 6 msec
  3 172.16.0.13 [MPLS: Labels 38/40 Exp 0] 29 msec 29 msec 28 msec
  4 172.16.0.2 [MPLS: Labels 38/40 Exp 0] 28 msec 29 msec 28 msec
  5 172.16.0.9 [MPLS: Label 40 Exp 0] 29 msec 29 msec 28 msec
  6 172.16.0.10 26 msec 29 msec 23 msec
  7 172.16.0.22 30 msec 28 msec 29 msec
```

El momento que el PE-UIO-01 esta down se evidencia que el camino es por la IP 172.16.0.5 que está configurada en el PE-UIO-02.

```
CPE-Concentrador#traceroute 172.16.0.22 source 172.16.0.18
Type escape sequence to abort.
Tracing the route to 172.16.0.22
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.0.17 8 msec 9 msec 7 msec
  2 172.16.0.5 7 msec 5 msec 1 msec
  3 172.16.0.17 [MPLS: Labels 38/40 Exp 0] 30 msec 28 msec 31 msec
  4 172.16.0.2 [MPLS: Labels 38/40 Exp 0] 29 msec 27 msec 29 msec
  5 172.16.0.9 [MPLS: Label 40 Exp 0] 29 msec 28 msec 35 msec
  6 172.16.0.10 33 msec 25 msec 29 msec
  7 172.16.0.22 29 msec 31 msec 30 msec
```

5.2 Pruebas de funcionamiento de SD-WAN

El escenario de SD-WAN que se desarrollaran las pruebas, es el mencionado en los capítulos anteriores de diseño e implementación, sobre una red física ubicada en Guayaquil y otra en la ciudad de Quito interconectadas con equipos Cisco Meraki MX64, que tiene direccionamiento público en cada una de sus interfaces, aplicando políticas de navegación y reglas para las diferentes aplicaciones de la VPN. Mediante el dashboard de cisco meraki que se encuentra en la web permite administrar de manera centralizada los equipos y obtener las pruebas requeridas

5.2.1 Conectividad de MPLS (Latencia, throughput y MTU)

Desde el dashboard MX64 concentrador se procede a dar ping a la LAN del MX64 remoto, como se evidencia solo se ubica ingresa la dirección IP a la que deseo probar y se tiene una interfaz interactiva para analizar los resultados como la latencia de 10 ms.

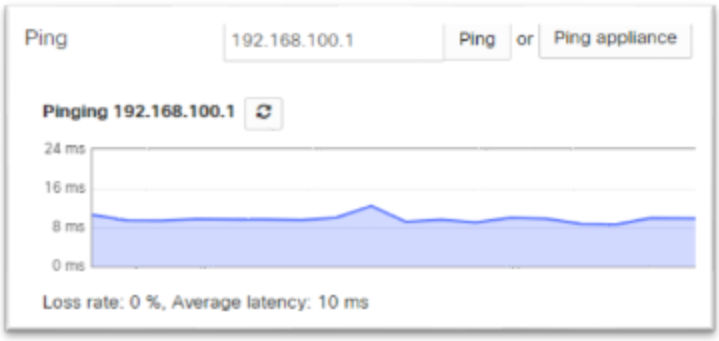

Figura 37. **Ping desde MX-Concentrador al MX-Remoto**

Se puede evidenciar en el dashboard la conectividad del MX en la red desde la fecha que inicio y si presenta cortes en la misma.

Figura 38. **Conectividad del MX en dashboard**

En la plataforma se visualiza el porcentaje de las pérdidas que se pueden generar en las interfaces WANs en fechas especificadas.

Figura 39. **Pérdidas de WANs desde el dashboard**

El tráfico que se genera en cada uno de las interfaces WANs.

Figura 40. **Tráfico de las interfaces WANs**

Se puede evidenciar el throughput que puede cruzar por el MX, dependiendo de las configuraciones que se realiza, si se realiza mayores configuraciones el throughput baja.

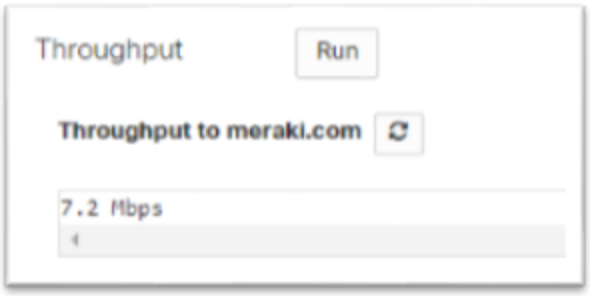

Figura 41. **Throughput del MX64**

5.2.2 Seguridad

En el dashboard se tiene un ambiente controlado con seguridad en cada uno de los host de la red, como: limitación de ancho de banda general, reglas de capa 3 y 7, y las políticas de tráfico para cada aplicación.

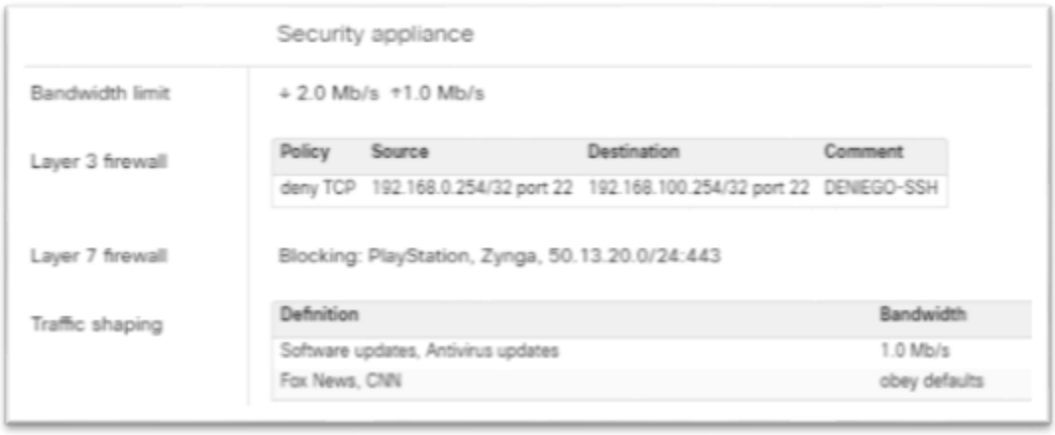

Figura 42. **Aplicación de seguridad en el MX**

En el propio dashboard se analiza el tráfico de input, output o forwarding en cada uno de las interfaces del Meraki, se puede exportar a un wireshark el tráfico que

requiera ser analizado con filtros de dirección IP, puerto, protocolo icmp y las interfaces.

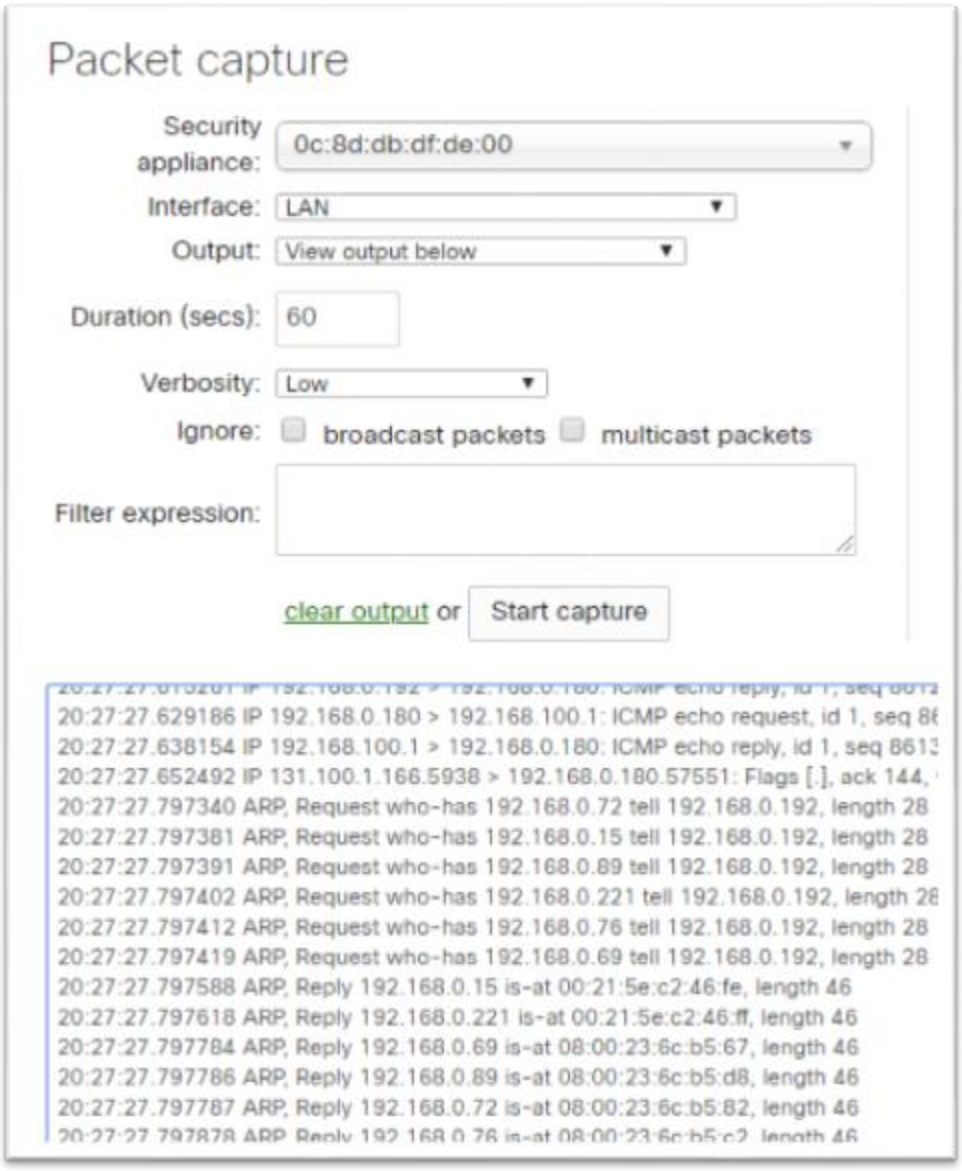

Figura 43. **Captura de tráfico de LAN.**

Otro aspecto de seguridad en los MX y otros vendors que integran la VPN está visible desde el dashboard, con esta característica se tiene un ambiente controlado de cada uno de los MX y subredes que participan en la VPN.

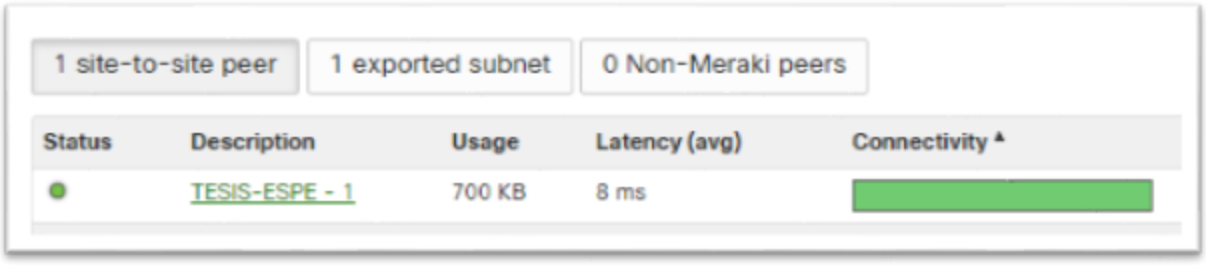

***Figura 44*. MX y subred conforman la VPN**

5.2.3 Convergencia de comunicación

Desde el MX-Concentrador se tiene conectividad al MX-remoto por la VPN que se estable entre los equipos, como se puede evidenciar en la figura 45 y 46, que se presenta el camino para llegar a su destino.

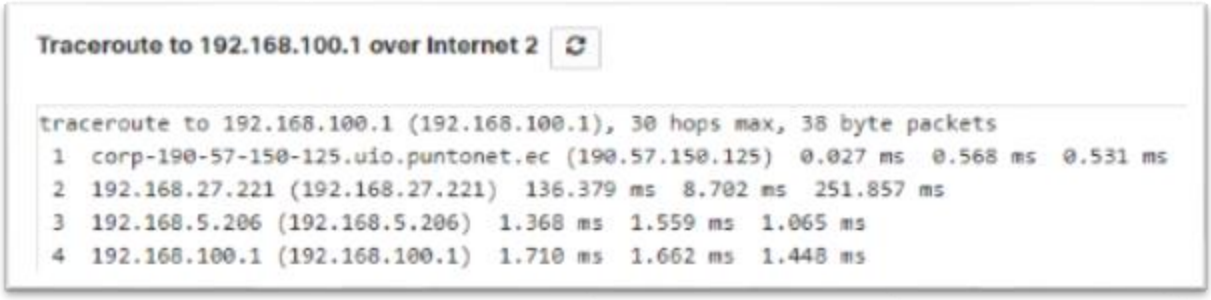

***Figura 45.* Comunicación VPN entre MX con origen Ethernet 2**

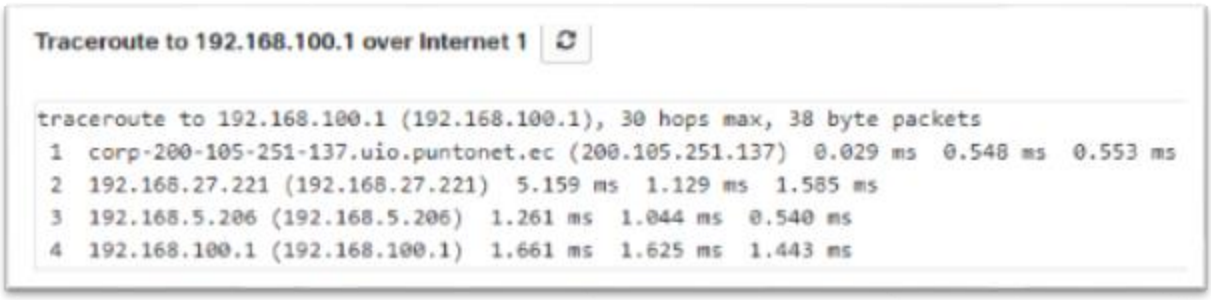

***Figura 46*. Comunicación VPN entre MX con origen Ethernet 1**

Cada uno de los MX tienen salida al internet directa por la pública que tienen configurada, es decir que los servicios de VPN y acceso a internet si se llega averiar uno de los enlaces no presenta afectación para el usuario final.

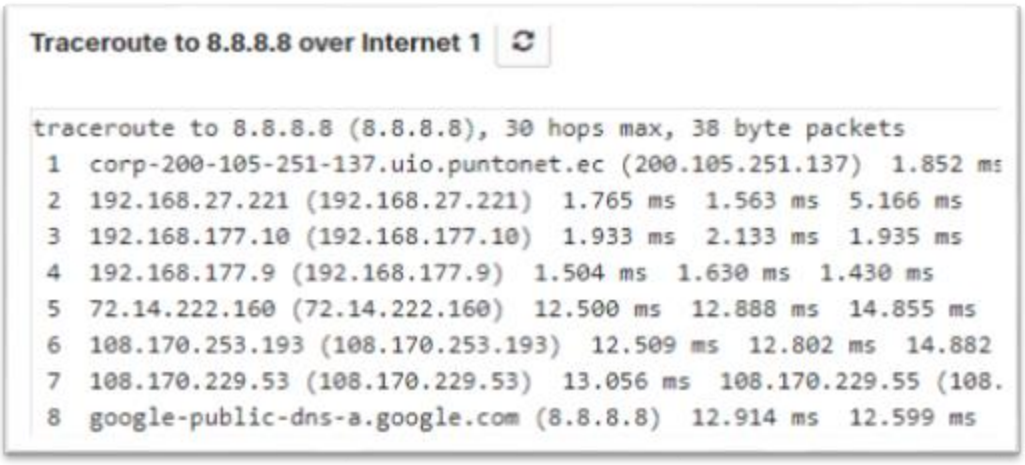

***Figura 47.* Acceso a internet por Ethernet 1**

Traceroute to 8.8.8.8 over Internet 2

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
 1  corp-190-57-150-125.uio.puntonet.ec (190.57.150.125)  0.705 ms  0.59
 2  192.168.27.221 (192.168.27.221)  2.229 ms  1.446 ms  5.244 ms
 3  192.168.177.10 (192.168.177.10)  1.891 ms  1.818 ms  1.884 ms
 4  192.168.177.9 (192.168.177.9)  2.579 ms  1.836 ms  1.952 ms
 5  72.14.222.160 (72.14.222.160)  12.802 ms  12.446 ms  12.681 ms
 6  108.170.253.209 (108.170.253.209)  12.833 ms  12.800 ms  12.938 ms
 7  108.170.229.61 (108.170.229.61)  12.710 ms  108.170.229.55 (108.170.
 8  google-public-dns-a.google.com (8.8.8.8)  12.471 ms  *  13.055 ms
```

Figura 48. **Acceso a internet por Ethernet 2**

5.2.4 Monitoreo Aplicaciones

En el dashboard con la administración centralizada, se analiza en un ambiente amigable cada una de las aplicaciones y el ancho de banda que emplean los usuarios.

Figura 49. **Consumo del enlace y aplicaciones**

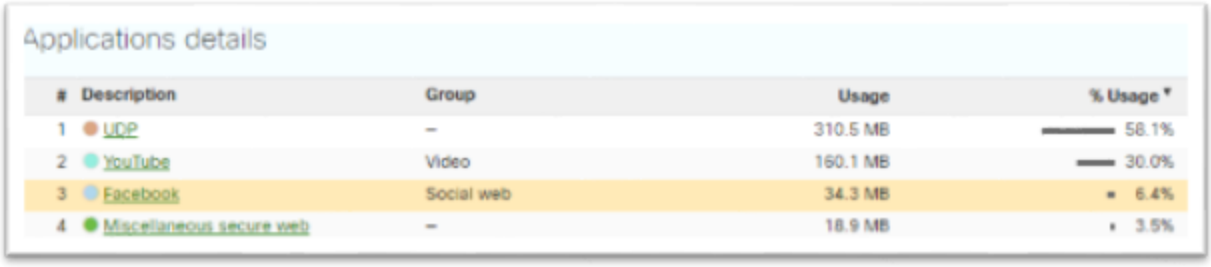

Figura 50. **Aplicaciones de mayor consumo**

	Status	Description	Last seen	Usage ▾	OS	IPv4 address
1		asistconta	Nov 25 16:26	540.0 MB	Windows 7	192.168.0.180
2		18:66:da:2d:6a:82	Nov 25 11:58	55 KB	Windows 10	192.168.0.185

Figura 51. **Host de la red de mayor consumo.**

5.3 Análisis Técnico y Económico

5.3.1 Análisis técnico de convergencia de la red

En el presente proyecto se tiene algunas características técnicas que deben ser analizadas para tener una visión clara de cuál es la mejor opción entre una red MPLS con IPSec y TE en comparación de una red SD-WAN. Entre las características se podrá mencionar diseño, implementación, número de equipos a emplear, configuraciones, tiempos de respuesta de extremo a extremo (latencia y jitter), funcionamiento de las aplicaciones MTU, políticas de restricción de ancho de banda, balanceo de enlaces y seguridad.

El diseño de una red MPLS para ofrecer las mismas funciones de una red SD-WAN se tiene considerar varios aspectos como: complejidad en la topología, direccionamiento a emplear y protocolos de enrutamiento, los mismos que para ser empleados se tiene que tener un alto nivel de conocimiento técnico para ejecutar en la red MPLS vía CLI, que lo contrario en una red SD-WAN es de manera amigable con el usuario debido a su administración centralizada y gráfica.

En una red MPLS tradicional se emplea mayor número de recursos como un CE y CPE en cada punto para establecer la comunicación, y en una SD-WAN solo un MX garantiza el funcionamiento. Una de las principales características o ventajas que se tiene con SD-WAN es la facilidad de configuración en su dashboard centralizada que permite integrar nuevos MX de forma plug-play.

Otro punto a considerar es la latencia y jitter, en la red MPLS siempre sigue el camino seleccionado según los router en la tabla de ruteo que se genera con la mejor métrica, causando que en determinadas ocasiones los tiempos se eleven por saturación en el canal y el jitter oscila entre 10 milisegundos; en la SD-WAN la latencia se puede elevar en un uplink pero mediante el software conmuta a otro uplink sin afectar los servicios, de esta maneja el jitter tiene una oscilación de 3 milisegundos.

En las dos redes se garantiza el MTU mayor a 1500 para el funcionamiento de las aplicaciones de capa siete en SD-WAN, en el caso de MPLS se comprobó con icmp de size 1500 que se tiene respuesta de extremo a extremo de los CPE, como se mencionó en SD-WAN se tiene el dahboard que permite aplicar y visualizar de modo gráfica las políticas, reglas y restricciones de ancho de banda en capa tres y capa siete; en el escenario de MPLS es más complejo lograr las metas mencionadas, debido que tiene que configurar por CLI access-list, clases, route-map e integrar a en la interfaz, recalcando que no se puede aplicar a nivel capa siete.

En el balanceo de tráfico en MPLS se implementó TE en la parte de backbone para tener una ruta alterna y en WAN se tiene BGP con sus métricas permite tener los dos enlaces activos-pasivo, en SD-WAN se emplea dos enlaces de uplink que se puede balancear el tráfico de internet como el de las VPN auto configuradas. La VPN en SD-WAN con Cisco Meraki MX se crea de manera dinámica auto VPN y no requiere un conocimiento avanzado de las dos fases de IPsec como en MPLS que se tiene que si la emplea a detalle además de incluir un CPE adicional debido que se requiere un solo WAN para establecer el túnel VPN.

Tabla 14.

Análisis técnico MPLS (IPSec – TE) y SD-WAN

Característica	***MPLS***	***SD-WAN***
Conomiento técnico	Alto	Bajo
Topología	Full-mesh	Full-mesh
Direccionamiento	Privado Público	Público
Enrutamiento	OSPF BGP MP-BPG	Estático
Administración	CLI	Gráfica
Equipamiento	CE CPE	MX
Configuración	Avanzado	Dashboard plug&play
Latencia	34 ms	24 ms
Jitter	10 ms	3 ms
MTU	>1500	>1500
Políticas	Capa 3	Capa 3 Capa 7
Seguridad	IPsec en dos fases	Auto VPN con IPsec

5.3.2 Análisis económico costo / beneficio

Para la realización del análisis económico de las tecnologías se revisan los siguientes ítems para la ejecución de las mismas

- Costos de instalación e implementación
    - Instalación de enlaces
    - Equipos de comunicación
    - Configuración de tecnologías (IpSec,TE vs. SDWAN)
    - Recurso humano

- Costos de mantenimiento y soporte
    - Recursos de comunicación (enlaces)
    - Recurso Humano

Tabla 15.

Costos de instalación e implementación IpSec y Traffic Engineerer

Costo de instalación de enlaces			
Tipo de enlace	Velocidad / Compartición		Costo mensual
Datos CE-Concentrador Principal	10 MB / 1:1	$	200,00
Datos CE-Concentrador Back-up	10 MB / 1:1	$	200,00
Datos CE-Remoto Principal	10 MB / 1:1	$	200,00
Datos CE-Remoto Back - up	10 MB / 1:1	$	200,00

CONTINUA

Equipos de comunicación			
Tipo	Modelo		
Router	Cisco 2921	$	5.900,00
Router	Cisco 892	$	1.227,00
Servicios de configuración			
IPSec		$	50,00
Traffic Engineering		$	75,00
Recurso Humano			
Ingeniero de Soporte		$	1.500,00
Total instalación e implementación IPSec y Traffic Engineer		$	9.552,00

Tabla 16.

Costo de instalación e implementación de SD – WAN

Costo de instalación de enlaces			
Tipo de enlace	Velocidad / Compartición	Costo mensual	
Internet Principal	10 MB / 1:1	$	200,00
Internet Back – up	10 MB / 1:1	$	200,00
Internet Principal	10 MB / 2:1	$	200,00
Internet Back – up	10 MB / 2:1	$	200,00
Equipos de comunicación y/o licenciamiento			
Tipo	Modelo		
Router	Cisco Meraki MX64	$	945,00
Router	Cisco Meraki MX64	$	945,00
Licencia Meraki (anual)		$	1.000,00
Licencia Meraki (anual)		$	1.000,00
Licencia Dashboard (anual)		$	1.000,00
Recurso Humano			
Tecnólogo de soporte		$	800,00
Total instalación e implementación SD WAN		$	6.490,00

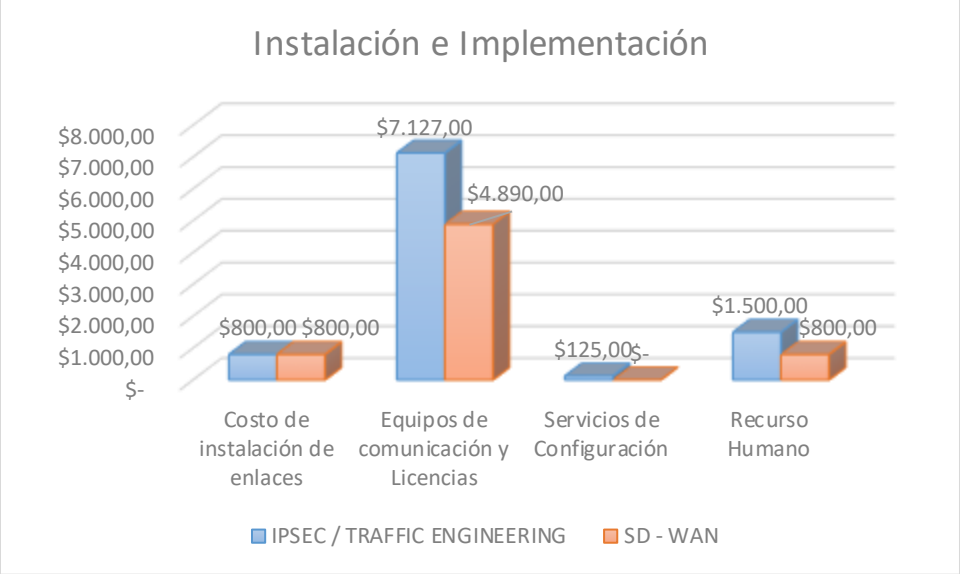

Figura 52. **Instalación e implementación**

Para lo cual al realizar el comparativo de instalación e implementación de tecnologías se tienen los siguientes resultados

Tabla 17.

Resultados de costos de instalación

Instalación e implementación	TOTAL
IPSec y Traffic Engineer	$ 9.552,00
SD WAN	$ 6.490,00

Se puede visualizar en la *Figura 53*., que la tecnología SD-WAN en cuanto a costos es viable con una diferencia de 32% respecto a la tecnología IPSec, uno de los ítems que marca la diferencia es el recurso humano; esto se muestra debido a

que los equipos de comunicación requeridos en la aplicación de tecnología SD-WAN son fáciles de utilizar debido al dashboard que se utiliza en la administración.

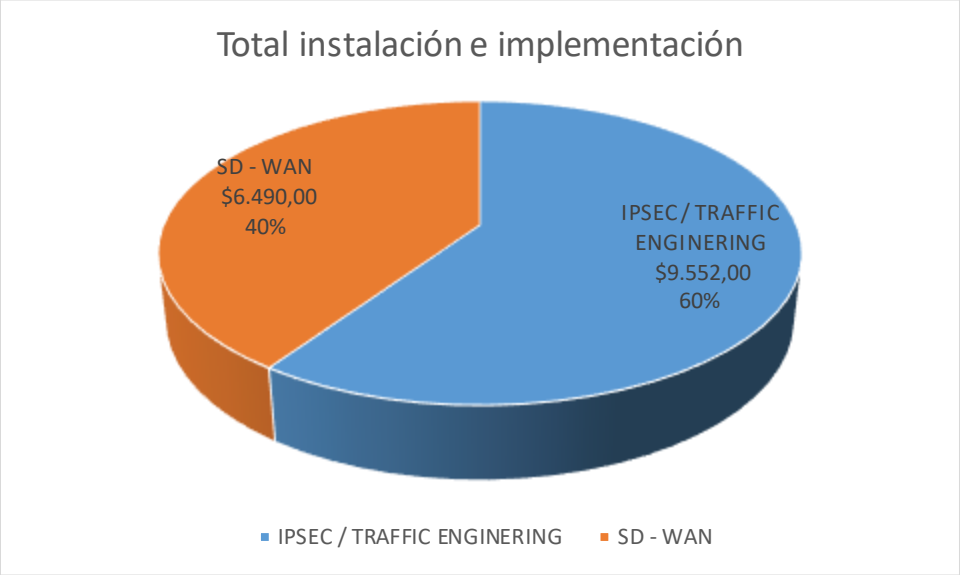

Figura 53. **Total de costos de instalación e implementación**

Adicional se debe tener en cuenta el soporte y mantenimiento que será un costo periodico para el uso de las tecnologías.

Tabla 18.

Mantenimiento y soporte IPSec y TE

Recurso de comunicación		
TIPO DE ENLACE	VELOCIDAD	COSTO
Datos CE-Concentrador Principal	10 MB / 1:1	$ 1.000,00
Datos CE-Concentrador Back-up	10 MB / 1:1	$ 1.000,00
Datos CE-Remoto Principal	10 MB / 1:1	$ 1.000,00
Datos CE-Remoto Back – up	10 MB / 1:1	$ 1.000,00
Recurso Humano		

Ingeniero de Soporte	$ 1.500,00

Tabla 19.

Mantenimiento y soporte SD-Wan

Recurso de comunicación		
TIPO DE ENLACE	VELOCIDAD	COSTO
Internet Principal	10 MB / 1:1	$ 500,00
Internet Back – up	10 MB / 1:1	$ 500,00
Internet Principal	10 MB / 2:1	$ 300,00
Internet Back – up	10 MB / 2:1	$ 300,00
Recurso Humano		
Tecnólogo de soporte		$ 800,00
TOTAL		$ 2.400,00

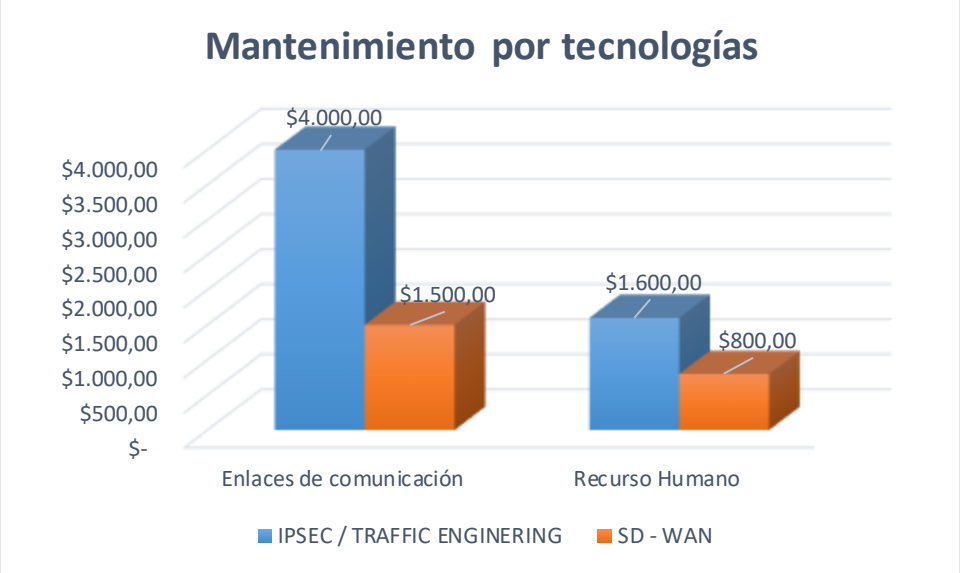

Figura 54. **Mantenimiento mensual por tecnologías**

En el mantenimiento y soporte que se muestra en las tablas 17 y 18, se evidencia los valores mensuales para el cliente que contrate los enlaces con las tecnologías presentadas.

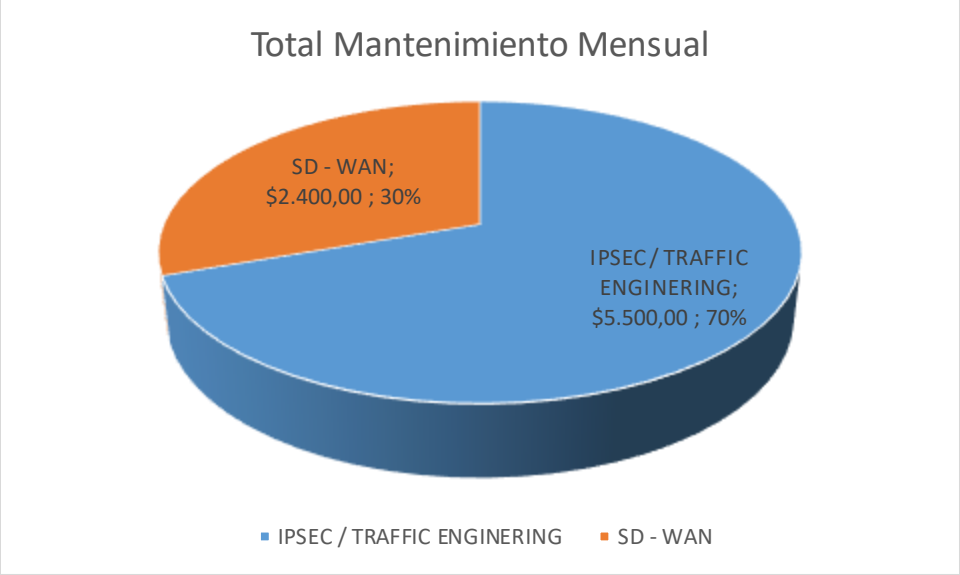

Figura 55. **Valor total de mantenimiento mensual**

Para el cálculo del costo total de propiedad TCO, se utilizará el costo de instalación e implementación que se mostraron en la tabla 14 y 15; el soporte y mantenimiento para cinco años, no se utiliza la tasa de incremento anual porque al firmar el contrato con el ISP se mantienen los costos desde la contratación del servicio.

Tabla 20.

Costo total de Propiedad

Tecnologías\Años	0	1	2	3	4	5	TCO
IPSec y TE	$ 9.552,00	$ 66.000,00	$ 66.000,00	$ 66.000,00	$ 66.000,00	$ 66.000,00	**$ 339.552,00**
SD- WAN	$ 6.490,00	$ 28.800,00	$ 28.800,00	$ 28.800,00	$ 28.800,00	$ 28.800,00	**$ 150.490,00**

Al obtener el valor del TCO se evidencia que el gasto que se genera al utilizar la tecnología SD-WAN es del 44.32% sobre el valor que se gastaría con la tecnología IPSec.

En cuanto al Valor actual Neto VAN no se muestra porque se tiene el análisis sobre el cliente que contrataría el servicio al ISP, y sus ingresos deben ser revisados de acuerdo al giro de negocio de la empresa contratante.

CAPÍTULO VI. Conclusiones y Recomendaciones

6.1 Conclusiones

Una red tradicional MPLS de capa 3 implementando las tecnologías IPsec y Traffic Engineering, al igual que una red SD-WAN moderna, ofrecen al cliente ventajas tales como: comunicación segura, balanceo de tráfico, calidad de servicio, convergencia de la red y alta disponibilidad, sean estos basados en enlaces Internet o canales de datos dedicados para la interconexiones de sus sedes empresariales, tal como se analizó en la fase teórica y práctica de la presente tesis. La diferencia entre ambas soluciones responde a la flexibilidad, administración centralizada, simplicidad y menores costes que puede ofrecer SD-WAN sobre MPLS tradicional.

La solución SD-WAN propone mejorar la conectividad mediante la entrega de servicios WAN basada en Internet o enlaces de datos (MPLS, Capa 2, etc.), de forma rápida, flexible, con calidad, seguridad y fiabilidad. Dado que se basa en la nube, ofrece una administración centralizada y simplificada desde una única plataforma de gestión en la cual fácilmente se puede aplicar configuraciones, políticas de seguridad y ejecutar diagnósticos, así como automatizar el despliegue

en sedes u oficinas remotas eliminando costos operativos y la necesidad de movilizar personal técnico a las localidades. Además, ofrece balanceo de carga entre los múltiples enlaces y control de ruta inteligente, lo que garantiza el rendimiento de las aplicaciones independiente de la demanda de ancho de banda y condiciones de la red (pérdida, latencia, inestabilidad, etc.).

Las redes de transporte actualmente están en un tiempo de transición hacia las redes definidas por software (SDN), una de las aplicaciones de esta nueva tendencia es SD WAN; debido a que tiene una curva de aprendizaje más rápida que la configuración bajo línea de comandos, la cual requiere de experiencia, capacitación y habilidades de troubleshooting muy avanzadas y las implementaciones de conexión entre sedes empresariales requieren de rapidez y visibilidad total, así como compatibilidad entre diferentes vendor; características que fueron comprobadas en la fase de implementación de la presente tesis.

6.2 Recomendaciones

Basándose en la experiencia y en la investigación realizada, se recomienda el uso de MPLS dentro de la nube del proveedor; debido a que MPLS ofrece confiabilidad en la comunicación, altos niveles de calidad de servicio, entre otras ventajas que ha desarrollado MPLS por la constante evolución, sin embargo la implementación de SD-WAN se podría darse a nivel de la WAN con el fin de facilitar

el despliegue de la conectividad de extremos a extremos de aplicaciones críticas para la organización y reducir gastos de operación de TI.

En la implementación de IPsec se debe configurar en el CPE que está más cercano a la red interna y está conectado de manera directa la subred LAN o tráfico interesante que interactúa en la VPN segura, si la implementado es realizada en equipos intermedios como CE con una topología de principal y backup se tiene que levantar un túnel IPsec por cada uno de las interfaces WANs, causando que determinadas sesiones estén en estatus down el momento que se llega a conmutar el tráfico por el enlace de backup.

Estudios futuros

Sería interesante que en un futuro se analice segment-routing (SR) como una nueva tendencia para mejorar en las redes MPLS, debido que remplaza el protocolo de distribución de etiquetas por SR (Salazar, 2018)

REFERENCIAS

[1] Adrián Delfino, S. R. (Marzo de 2000). *Traffic Engineering for IP Networks.* Obtenido de https://iie.fing.edu.uy/investigacion/grupos/artes-old/fce/net-te/Ingenieria_de_Trafico_en_Redes_MPLS.pdf

[2] Cisco. (2012). *ATM*. Obtenido de http://docwiki.cisco.com/wiki/Asynchronous_Transfer_Mode_Switching

[3] Cisco. (2012). *Frame Relay*. Obtenido de http://docwiki.cisco.com/wiki/Frame_Relay

[4] Cisco. (2012). *X.25*. Obtenido de http://docwiki.cisco.com/wiki/X.25

[5] CISCO. (2018). *Meraki Cisco System*. Obtenido de https://meraki.cisco.com/products/appliances/mx84

[6] Citrix. (s.f.). *SD-WAN*. Obtenido de https://www.citrix.com/content/dam/citrix/en_us/documents/solution-brief/sd-wan-the-answer-to-networking-demands-es.pdf

[7] Networkworld. (s.f.). *SD-WAN*. Obtenido de https://www.networkworld.es/networking/sdwan-que-es-y-por-que-lo-va-a-usar

[8] ORBCOOM. (2018). *Orbcoom*. Obtenido de https://store.orbcomm.com/product/6444_cisco_meraki_mx65_cloud_managed_security_appliance.htm