COMPARACIÓN DE ASPECTOS OPERATIVOS Y ECONÓMICOS ENTRE SD-WAN Y MPLS PARA ESTABLECER LA MEJOR OPCIÓN DE UNA EMPRESA CORPORATIVA A NIVEL NACIONAL E INTERNACIONAL

SANDRA MILENA MORENO ALAYÓN

UNIVERSIDAD SANTO TOMÁS DE AQUINO
FACULTAD DE INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C
2021

COMPARACIÓN DE ASPECTOS OPERATIVOS Y ECONÓMICOS ENTRE SD-WAN Y MPLS PARA ESTABLECER LA MEJOR OPCIÓN DE UNA EMPRESA CORPORATIVA A NIVEL NACIONAL E INTERNACIONAL

Presentado por:
SANDRA MILENA MORENO ALAYÓN
CÓDIGO: 2201446

Trabajo opción de grado Pasantías en la Empresa ORANGE S.A.

Director:
Juliana Alejandra Arevalo Herrera

MAGÍSTER EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD SANTO TOMÁS DE AQUINO
FACULTAD DE INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C
2021

RECTOR GENERAL
Padre José Gabriel Mesa Angulo, O.P.

VICERRECTOR ADMINISTRATIVO Y FINANCIERO GENERAL
Padre, Wilson Mendoza Rivera, O.P.

VICERRECTOR ACADÉMICO GENERAL
P. Eduardo Gonzáles Gil, O.P

SECRETARIA GENERAL
Ingrid Lorena Campos Vargas

SECRETARIA DE DIVISIÓN
E. C. Luz Patricia Rocha Caicedo

DECANO FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
Ingeniero Germán Macías Muñoz

Nota de Aceptación.

_____
_____
_____
_____

_____
Firma Ingeniera Juliana Arévalo Herrera
Tutor Asignado

_____
Firma del Jurado

_____
Firma del Jurado

_____
Fecha

Resumen

En la sociedad actual es necesario que las organizaciones se adapten a los cambios y busquen formas de estar a la vanguardia tecnológica con el fin de prestar un alto nivel de servicios. Los nichos del mercado en algunas ocasiones se deben arriesgar en la implementación de nuevas tecnologías, eso sí, con estudios previos sobre los beneficios y /o riesgos que se corren.

Se conoce que MPLS es una tecnología que lleva un tiempo considerable en el mercado, generando confianza ante su efectividad y eficiencia, pero a un alto costo. Con la situación de aislamiento, confinamiento y trabajo remoto, las organizaciones se han tenido que adaptar a los cambios que generan los nuevos requerimientos para satisfacer las necesidades de los usuarios, donde se ha evidenciado que el trabajo remoto requiere de mayor disponibilidad y Ancho de banda a nivel de red, además, la economía se ha visto afectada con la pandemia, obligando a las organizaciones a mitigar riesgos haciendo recortes de personal y/o reduciendo costos sin afectar el nivel de servicio. Un claro ejemplo para este sería la implementación de la tecnología SD-WAN sobre MPLS.

En este documento se identifica la Tecnología MPLS y SD-WAN con sus respectivas ventajas y desventajas, benéficos, aplicaciones y movimiento en el mercado, para identificar la mejor opción para una compañía de nivel mundial.

Palabras claves: SD-WAN, MPLS, Red, trabajo remoto, ancho de banda, economía, aplicaciones, nivel mundial.

Tabla de Contenidos

Lista de Diagramas

Lista de Tablas

Lista de Figuras

Glosario

AC ("*Attachment Circuits*" Circuito de Conexión): Interfaz vinculada a una instancia de conmutador virtual (VSI), AC lleva el tráfico de clientes en su forma nativa, es decir las tramas Ethernet con o sin la VLAN que marca con etiqueta dependiendo de si estamos creando un Pseudowire basado VLAN o Pseudowire basado los Ethernet. Para que funcione un servicio PW se tienen dos AC, uno en cada extremo conectado a un PW. (Cisco, 2007)

AS ("Autonomous System"): Es un grupo de uno o más prefijos de IP (listas de direcciones IP accesibles en una red) ejecutadas por uno o más operadores de red que mantienen una política de enrutamiento única y claramente definida. Los operadores de red necesitan números de sistema autónomo (ASN) para controlar el enrutamiento dentro de sus redes e intercambiar información de enrutamiento con otros proveedores de servicios de Internet (ISP). (Foro Huawei, 2020)

ATM ("*Asynchronous Transfer Mode*" Modo de transferencia asincrónica): Protocolo que transporta datagramas IP y otro tráfico sin conexión entre hosts, enrutadores, puentes y otros dispositivos de red. Existe una capa 5 de la adaptación ATM (AAL5) que envía los paquetes en una longitud variable sobre la red. (RFC2684, s.f.)

BGP ("*Border Gateway Protocol*" Protocolo de puerta de enlace fronteriza): Protocolo de Vector-Ruta que hace la cooperación entre enrutadores permitiendo un intercambio de información de ruteo entre diferentes Sistemas Autónomos (SA) para la internet, asegurando confiabilidad en la transmisión de datos. (RFC4271-IETF, 2006)

CE (“*Provider Edge*”): Router de borde del proveedor

EIGRP (“*Enhanced interior gateway routing protocol*” Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado: Protocolo de enrutamiento rápido que combina enrutamiento por estado de enlace y vector de distancia, aprende de manera dinámica a reconocer nuevas rutas que se unen a la red e identifica enrutadores inalcanzables e inoperantes. (Albrightson, 1994)

EVPN (“Ethernet VPN”): Es una solución de próxima generación que proporciona servicios multipunto Ethernet a través de redes MPLS. Existe debido a su uso de aprendizaje MAC basado en el plano de control sobre el núcleo tecnologías EVPN, que abarca soluciones L2VPN Ethernet de próxima generación que utilizan el Border Gateway Protocol (BGP) como plano de control para la señalización / aprendizaje de direcciones MAC en el núcleo, así como para la topología de acceso y el descubrimiento de puntos de conexión VPN. (Cisco, s.f.)

FEC-MPLS (“*Forwarding Equivalence Class*” Clase equivalente de reenvío): Corrección de errores en recepción (sin canal de retorno) (ITU, 1997), Es el conjunto de paquetes o flujos de información a los cuales tras ingresar a la red MPLS se le añade una cabecera que hace que todos sean tratados de la misma forma, independiente de que sean paquetes de distinto tipo de tráfico. (Garcia, 2008)

FEC(“*Forward error correction*” Corrección de errores en recepción): Sin canal de retorno. Es el conjunto de paquetes que agregan redundancia o bits de paridad a

los datos transmitidos para garantizar que el receptor detecte y corrija los errores por intermitencia del enlace de acceso a internet, recuperando el paquete inicial. (ITU, 1997)

GMPLS("*Generalized MultiProtocol Label Switching*" Conmutación generalizada de etiquetas multiprotocolo): Es la versión mejorada en la parte lógica de MPLS, ya que soporta tanto la conmutación de paquetes, como la conmutación en longitud de onda, la conmutación en el tiempo y la conmutación de fibras ópticas. (Tejedor, 2002)

GRE ("*Generic Router Encapsultion*"Encapsulación de enrutador genérico): Protocolo de enrutamiento que proporciona un mecanismo más simple que reduce la encapsulación de varios protocolos de capa de red de punto a punto mediante una red pública.(RFC2784, 2000). También es llamado protocolo de túnel, desarrollado por Cisco que encapsula varios protocolos punto a punto como Internet.(Tapia, 2016)

HDLC ("*High-level Data Link Control*" Control de enlace de datos de alto nivel): Reúne protocolos de conexión remota que opera a nivel de enlace de datos ofreciendo una comunicación confiable al proporcionar recuperación de errores en pérdidas de paquetes de datos. Se basa en la ISO 3309 (Manuel Freire Medina, s.f.)

IETF ("*Internet Engineering Task Force*") Es una compañía estadounidense que se encarga de regular los estándares y propuestas de internet (RFC).

IPLS ("*IP-only LAN Service*" Servicio LAN solo de IP): Es un tipo simplificado de VPLS donde el mantenimiento de las tablas de reenvío MAC se realiza

Mediante señalización y un dispositivo (PE) implementa conectividad LAN multipunto para tráfico IP. (RFC 7436, 2015)

IPSec (“*Internet Protocol security*” Seguridad del protocolo de internet): Protocolo apoyado en los estándares de la IETF que incorpora servicios de seguridad sobre la capa del protocolo de internet (IP) permitiendo un nivel de seguridad común y homogénea para todas las aplicaciones. (Rico Bautista, Medina Cárdenas, & Santos Jaimes, 2008)

LAP.B (“*Link Access Procedure Balanced*” Procedimiento Balanceado de Acceso al Enlace): Estándar de la ITU-T para redes WAN con conmutación de paquetes conocido como un protocolo de enlace de la norma X.25. Elemento que deriva de HDLC dando acceso a la capa de enlace de datos y sirve para el intercambio de datos por múltiples circuitos físicos. El X.25 ha sido reemplazado por Frame Relay. (UIT-T X.25, s.f)

LAB.F (“*Link Access Procedure for Framed*“Procedimiento de acceso al enlace para *Frame Relay*): Protocolo de conmutación rápida de paquetes que transporta información a través de redes privadas y públicas mediante retransmisión de tramas, una buena opción para transmisión de una alta cantidad de datos. Principalmente controla el enlace de datos de una red en la versión de control y núcleo (core). (Parra, 1996)

LAPM (“*Link Access Protocol for Modems*”): Protocolo basado en HDLC denominado procedimiento de acceso de enlace para módems definido en la recomendación T-REC-V.42. (UIT-T, T-REC-V.42, s.f.)

LDP (“*Label Distribution Protocol*”): Es el protocolo que permite que los enrutadores del switch de etiquetas del mismo nivel “*Label Switching Route*r” (LSR) en una red MPLS intercambien la información de enlace de etiquetas para soportar el reenvío salto por salto en una red MPLS**.** (Cisco, 2008)

LLC (*“Logical Link Control”* Subcapa de control de enlace lógico): Es una de las dos subcapas de la capa de enlace, administra la comunicación entre dispositivos sobre un solo enlace de red. ((IEEE 802.2, s.f.)

LSR (“*Label Switching Router*” Router de conmutación de etiquetas): Es el enrutador que asigna una clase FEC a cada uno de los paquetes, los clasifica y agrega etiquetas. (Cisco, 2008)

LSP (“*Label Switched Path”*): Cuando los enrutadores ya han establecido las sesiones LDP y se comunican entre ellos, se establece una ruta conmutada por etiquetas o LSP. (Cisco, 2008)

L1, L2 y L3: Capa1, 2 y 3

MAC (“Media Access Control” Control de Acceso al medio): Dirección Física de un dispositivo que ofrece posibilidades de control a acceso al medio.

MPLS (“*Multi Protocol Label Switching*” Conmutación de paquetes multi protocolo): Es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. (Millan, 2002).

NE (Nodo o Elemento de red)

OSPF (“*Open Shortest Path First*” Abrir el camino más corto primero): OSPF es un Protocolo de ruteo dinámico. Detecta rápidamente los cambios topológicos en el Sistema Autónomo (tal como fallas de la interfaz del enrutador) y calcula las nuevas rutas loop-free después de un período de convergencia. Este período de convergencia es corto e implica un mínimo de tráfico de ruteo. (RFC2328, 1998)

PE (“*Customer Edge*”): Router de borde del cliente

PPP (“P*oint to Point Protocol*” Protocolo punto a punto): PPP proporciona un método estandarizado para transportar datagramas multiprotocolo sobre enlaces punto a punto. Este tiene tres componentes principales: El método de encapsulamiento de datagramas multiprotocolo, el protocolo de control de enlace (LCP) y la familia de protocolos de control de red para enlazar diferentes protocolos de capa de red. (RFC1661, 1994)

PW (“Pseudowires” Pseudo cables) se utiliza para proporcionar los servicios de extremo a extremo a través de una red MPLS. Son los bloques de construcción básica que pueden proporcionar un servicio Point-toPoint así como un servicio de múltiples puntos tal como VPL, que está prácticamente una malla de PWs creaba el dominio de Bridge a través del cual los paquetes fluyen. (Guatavo, 2019)

QoS (“*Quality of Service*”Calidad de servicio): Efecto global de las características de servicio que determina el grado de satisfacción del usuario de un servicio. Se caracteriza por los aspectos combinados de los factores de comportamiento aplicables a todos los servicios. (ITU, 1997)

SaaS (“*Software as a Service*” Software como Servicio): El software como servicio (SaaS) permite a los usuarios conectarse a aplicaciones basadas en la nube a través de Internet y usarlas. Algunos ejemplos comunes son el correo electrónico, los calendarios y las herramientas ofimáticas (como Microsoft Office 365). SaaS permite que una organización se ponga en marcha y pueda ejecutar aplicaciones con un costo inicial mínimo. (Azure,s.f.)

SLA (“Service-Level Assurance”Acuerdo de nivel de servicio): Es un protocolo de medición de rendimiento que ofrece un amplio conjunto de tipos de mensajes de medición. Los tipos de medición se pueden clasificar como los que prueban la conectividad (como ping) proporcionando medidas de latencia de ida y vuelta o unidireccionales, y los que proporcionan un conjunto más rico de estadísticas, incluido el Jitter de red y la pérdida de paquetes o tramas. SLA mide los parámetros del nivel de servicio tales como latencia de red, variación del retardo, y pérdida del paquete/de la trama. (RFC6812, 2013)

TCP/ IP (*“Transmission Control Protocol/Internet Protocol”)*: Es el conjunto de protocolos que son el fundamento de Internet y proporciona una conectividad universal a través de la red con reconocimiento de extremo a extremo. (SCI, s.f.)

TCP /IP es el lenguaje que permite la comunicación entre ordenadores y es denominado como un protocolo que separa TCP o protocolos orientados a la conexión e IP. IP se encarga de enviar paquetes tanto a nivel local como en toda la red.

TE (“*Traffic Engineering*” Ingenieria de trafico): Identifica las capacidades funcionales necesarias para implementar directivas que faciliten las operaciones de red

eficientes y confiables en un dominio MPLS. Estas capacidades se pueden utilizar para optimizar la utilización de los recursos de red y para mejorar las características de rendimiento orientadas al tráfico. (rfc2702, 1999)

UCS (Servicios de Conectividad Subyacente): Servicio de conectividad pública o privada, proporciona la conectividad entre una o más ubicaciones del suscriptor a donde se entrega el servicio de SD-WAN. Es responsabilidad del proveedor de servicio de SD-WAN acordar con el suscriptor la cantidad y el tipo de conectividad sobre los que se proveerá el servicio de SD-WAN. En el servicio *underlay* o subyacente, el proveedor de servicio controla y es dueño de la UCS a diferencia del servicio *overlay*, lo que es aceptable en el mundo de la libre transmisión (OTT, "*Over the Top*", por sus siglas en inglés) donde a las aplicaciones no les «importa» sobre qué corren. El UCS es compatible con los servicios de Ethernet, servicios IP, servicios de conectividad L1 y los servicios de acceso público a Internet, ofreciendo a SD-WAN un plano de reenvío amplio desde lo óptico hasta lo IP. (Mef 70, 2019).

VLAN ("*Virtual LAN*" LAN virtual): Es un mecanismo utilizado para permitir que los usuarios reciban direcciones IP de la misma subred, incluso si no pueden estar conectados al mismo enrutador o conmutador. Las VLANs simplifican la asignación de direcciones entre diferentes unidades administrativas y permiten que los usuarios físicamente dispares sean tratados como una unidad. (Prashant Garimella, s.f.)

VPLS ("*Virtual Private LAN Services*" Servicio de LAN privada virtual): Proporciona conectividad entre sitios de clientes geográficamente dispersos a través de

MAN y WAN, como si estuvieran conectados mediante una LAN. (RFC4762 -IETF, 2007)

VPN (“*Virtual private network*” Red privada virtual) Configuración de un sistema donde el abonado puede construir una red privada mediante conexiones con diferentes conmutadores de red que pueden incluir capacidades de red privada. (ITU, 1997)

VPWS (“*Virtual Private Wire Service*“Servicio de cable privado virtual): Servicio formado por Peseudowires, es un circuito lógico punto a punto (enlace) conectado a dos dispositivos Customer Edge. (RFC 4026, 2005).

VRF (“*Virtual Routing and Forwarding”*): Router de reenvío virtual usado en los enrutadores físicos como el PE y CE para crear múltiples enrutadores virtuales. La VRF sobre una PE asegura que el tráfico que pasa sobre una VPN no se direccione a otras VPN. Los VRF funcionan en la Capa tres de forma muy similar a cómo funcionan las VLAN en la Capa dos, mediante la asignación de interfaces a un dominio virtual aislado de otros dominios virtuales en la misma capa. “separa el tráfico de diferentes servicios, de algunas aplicaciones críticas para el negocio, o simplemente para separar el tráfico de datos, voz y video” (Davila, s.f.)

VSI (“*Virtual Switch Instance*” Instancia de conmutador virtual): Switch virtual que permite hacer un mapeo entre los AC y PW interconectando las LAN para que funcione como una sola red. (Guatavo, 2019).

Introducción

Gracias a la necesidad de interconectar y comunicar ordenadores entre sí, surge lo que hoy se reconoce como “Redes”, clasificadas de acuerdo a su capacidad de extensión (LAN, WAN, MAN, inalámbricas y de internet…), su forma de transmisión (punto a punto, Broadcast) y según la cantidad de datos que soporta en cada transmisión (redes de transmisión simple, half-duplex y full-duplex). La red WAN se crea para interconectar dispositivos con una extensión más amplia a la de una red de área local (LAN) o una red de área metropolitana (MAN). Sin embargo, al ver la necesidad de unificar los tipos de datos transmitidos sin afectar la velocidad de los mismos en una WAN, se implementa una forma de transferencia de datos llamada Multiprotocol Label Switching (MPLS) a finales del año 1990.

Así como MPLS optimizó otro tipo de tecnologías antes utilizadas como Frame Relay y ATM disminuyendo la complejidad de mapeo de direcciones IP; en el año 2012, surge lo que hoy se denomina SD-WAN en Cisco (Tori, 2020), una tecnología que pretende revolucionar el uso de las redes tradicionales, encaminando a los proveedores de servicios y compañías a un mundo tecnológico evolucionado en la nube.

En la actualidad las tecnologías permiten a las compañías mejorar los servicios y procesos generando optimización de los recursos según (Greenfield,s.f.) Andrew Lerner. Pronostica que el 1% de empresas que cuenta con la Tecnología SD-WAN en sus sucursales, pasará a ser un 30% en el 2019, para finalmente crecer en el mercado con un 59% anual y generando ingresos para el 2020 de más de $1.3 mil millones según el blog referente Gartner. Es evidente la necesidad de las empresas para optimizar y mantener

las redes a la vanguardia tecnológica, sin embargo, salen a relucir algunos interrogantes frente a este tema ¿una tecnología como MPLS que se ha usado y se usa ofreciendo un nivel de estabilidad y seguridad alto, podrá ser reemplazada por una tecnología inédita como lo es SD-WAN? ¿Qué tan segura puede ser una red basada SDN que centraliza la gestión de las WAN? ¿Qué nivel de seguridad se puede garantizar de los servicios basados en "internet" o "Cloud"?. En este proyecto se pretende hacer una breve comparación entre estas dos tecnologías y definir cuál es la más viable para una empresa que necesita especialmente una considerable reducción en sus gastos por servicios.

Contextualización del proyecto

Planteamiento Del Problema

La emergencia sanitaria ha generado nuevas necesidades tecnológicas en las organizaciones por el incremento en el uso de recursos digitales a través de Internet, el cloud computing y de modelos de software como servicio (SaaS) a nivel mundial; llevando a las empresas a reconsiderar la forma en que se une e interconecta la red.

La privacidad de los datos y la gestión eficaz de información, son prioridad para abordar tanto las obligaciones de una empresa como para llenar las expectativas de los clientes. Sin embargo, se ha generado un incremento de gastos en mantenimiento, infraestructura, proveedores, personal y procesos de TI insostenible durante la pandemia en la sede de Bogotá. Las empresas creen que la raíz del problema es el uso de tecnologías de transporte de alto costo como MPLS y por la falta de implementación de una tecnología como SD-WAN. ¿Cuál tecnología (SD-WAN o MPLS) reduce los gastos

operativos y de infraestructura, de las compañías que se caracterizan por usar mecanismos de transporte de datos con cambio de etiquetas multiprotocolo en Bogotá?

Justificación

En la actualidad las empresas requieren adoptar nuevas soluciones tecnológicas en vista de las necesidades y demanda actual (Mayor ancho de banda, calidad de servicio, agilidad, otros) y el mercado muestra un alto interés en la implementación SD-WAN, sin embargo, MPLS lleva mayor tiempo en el mercado, generando un mayor nivel de confianza en su efectividad y seguridad. Para Seleccionar la mejor implementación o solución para una compañía a nivel internacional e internacional, es necesario reconocer las tecnologías (SD-WAN y MPLS).

Objetivo General

Definir cuál tecnología entre SD-WAN y MPLS reduce los gastos operativos y de infraestructura, de las compañías que usan mecanismos de transporte de datos con cambio de etiquetas multiprotocolo en Bogotá.

Objetivos Específicos

- Reconocer la tecnología SD-WAN y MPLS para observar las ventajas y desventajas que ofrecen a la red.
- Comparar las tecnologías teniendo en cuenta los principales elementos para una comunicación corporativa.
- Determinar la tecnología más apropiada, entre las dos estudiadas, según los requerimientos definidos para la compañía.

Capítulo 1
Reconocimiento de MPLS y SD-WAN

Multi-Protocol Label Switching (MPLS)

MPLS es un protocolo que permite implementar redes inteligentes sobre una misma infraestructura ofreciendo servicios IP de extremo a extremo, se caracteriza por permitir la unión de los bordes MPLS a cualquier tipo de tecnología de acceso ya existente como Ethernet, IP, ATM y Frame Relay, ya que esta es totalmente independiente de los tipos de enlace de acceso.

El estándar MPLS es apto para cualquier protocolo de capa de red y evita principalmente el retardo ocasionado en los enrutadores de una red convencional al hacer un reenvío de capa de red. Es decir, en la red convencional es usual que cada uno de los enrutadores que recibe un paquete, deba hacer un análisis de su encabezado de la capa de red, asignarlo a una *Forward error correction* (FEC) y definir el siguiente salto, finalmente, en cada salto el enrutador debe volver a hacer ese reproceso. Según la RFC 3031 (2001), MPLS no asigna una nueva FEC en cada salto, sino que lo asigna una única vez, al identificar el ingreso del paquete a la red. La FEC se codifica en un código corto denominado “Etiqueta”, que permitirá identificar el paquete a lo largo de la red.

La etiqueta especifica el siguiente salto y una nueva etiqueta, con el fin de reemplazar la antigua etiqueta por la nueva en cada salto hasta llegar a su destino. Lo anterior, ofrece algunas ventajas frente al enrutamiento IP convencional, ya que en una red convencional internet no acepta aplicaciones para video conferencia, apps en tiempo real y otros, ahora

con MPLS se logra integrar los niveles de enlace de datos (capa 2) con la rápida conmutación y el nivel de red (capa 3) con el control de enrutamiento.

MPLS usa el Label Distribution Protocol (LDP) para ofrecer a la red los medios para enviar y dar acceso a la información de enlace de etiquetas entre los enrutadores LSR, los enrutador establecen las seciones LDP con su par potencial y finalmente, definen una ruta de conmutacion LSP logrando el intercambio de conmutacion de etiquetas y enviando el paquete a su destino.

Básicamente una red MPLS segura y funcional, requiere de:

1. Interconectar los enrutadores por medio de cables o Wireless (capa 2)
2. Un protocolo de enrutamiento junto con el protocolo LDP para sincronizar los enrutadores con capa 2 y capa 3
3. Un túnel VPLS
4. La unión lógica de la interfaz física con el túnel VPLS y lo que se reconoce como un puente “BRIDGE”

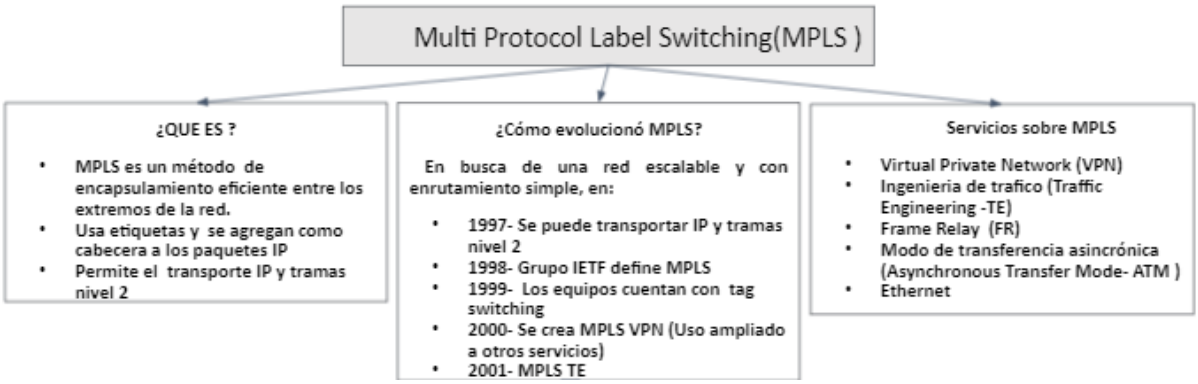

Diagrama 1. Generalidades MPLS modificados de: https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro_MPLS.pdf

Servicios que puede ofrecer MPLS

MPLS crea una red escalable y segura con garantía sobre el nivel de calidad del servicio, apoyado en componentes como VPN de capa 2 y capa 3 del modelo OSI, ingeniería de tráfico (TE), QoS, IPv6, GMPLS y otros. Principalmente este apartado se enfocará en los servicios VPN capa 1 y 2 e ingeniería de tráfico.

Servicio De Red Privada Virtual (Virtual Private Network - VPN) -(RFC 4026)

La VPN o red privada virtual, permite que una red compartida sea segura. Su función principal es cifrar la información que pasa entre el cliente y el servidor para anticiparse a ataques, lectura de datos y detección de paquetes. La red MPLS podrá compartir elementos e infraestructura con los clientes, sin embargo, estas serán redes totalmente independientes a la red principal.

"Cuando se utiliza con MPLS, la función VPN permite que varios sitios se interconecten de forma transparente a través de la red de un proveedor de servicios. Una red de proveedor de servicios puede admitir varias VPN IP diferentes. Cada uno de estos aparece para sus usuarios como una red privada, separada de todas las demás redes. Dentro de una VPN, cada sitio puede enviar paquetes IP a cualquier otro sitio en la misma VPN" (Cisco, 2020)

VPN es una red basada en IP, comunica varios sitios formando una red privada que puede pasar a través de toda una infraestructura pública sin afectar su efectividad y seguridad.

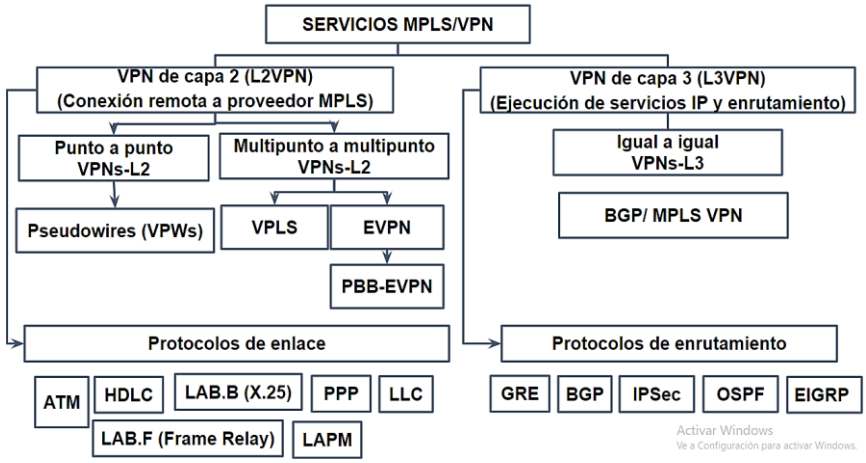

Diagrama 2.MPLS/VPN capa 2 y capa 3 (Cisco, 2018)

El L2VPN hace un enlace en los servicios de datos con el fin de generar efectividad en los procesos y herramientas para satisfacer al proveedor donde MPLS/VPN reenvía datos por la conmutación de etiqueta y no por búsqueda de IP. Según Cisco Community (2016) “MPLS/VPN hace un reenvío de datos al proveedor de servicios basado en la conmutación de etiquetas y no en la búsquedas de IP, donde L2VPN proporciona servicios de enlace de datos con Ethernet,Frame Relay, VLAN, ATM, punto a multipunto, entre otros. Con L3VPN el proveedor de servicios puede ofrecer servicios de red y enrutamiento (IP, IPv6 y otros)”

MPLS L2VPN (VPN capa 2)

L2VPN representa el uso de VPNs sobre MPLS e IP con conexiones de protocolos de enlace y/o circuitos heterogéneos (Ethernet a Ethernet, PPP a PPP, HDLC, etc) reconocidos como AC, su finalidad, es interconectar las redes punto a punto, traducir los datos encapsulados en capa 2 y conectar los equipos del cliente final a una VPN.

Para Gustavo, H (2019) L2-VPN permite que los proveedores de servicios trabajen sobre una sola infraestructura de red y ofrece al cliente su propio encaminamiento cumpliendo con los niveles de seguridad y calidad de servicio. La L2-VPNs está definida por la IETF que requiere de una conexión punto a punto con un servicio de cable privado virtual (Pseudowires - VPWS) en L2 y una simulación de red LAN en una WAN con un servicio VPLS. La sociedad ha ido implementando en las organizaciones redes privadas virtuales donde mejoran los servicios y procesos para mitigar riesgos e innovar en los servicios y/o productos que se prestan.

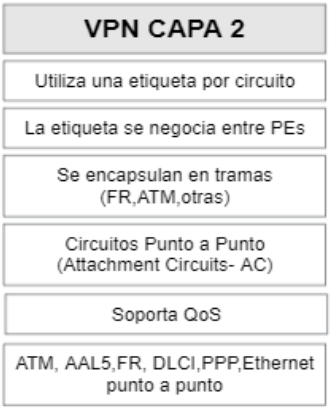

Figura 1. Características de VPN capa 2 modificado de:https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro_MPLS.pdf

Servicio de LAN privada virtual (Virtual Private Lan Service -VPLS):

VPLS es un servicio reconocido, el cual brinda una funcionalidad completa a una red interconectando segmentos; Como una tecnología usada por MPLS para crear redes LAN virtuales. VPLS ofrece servicios LAN sobre una WAN. Según Andersson, L (2015) “Un VPLS es un servicio de proveedor que emula la funcionalidad completa de una red de área local (LAN) tradicional. Un VPLS permite interconectar varios segmentos de

LAN a través de una red de conmutación de paquetes (PSN) y hace que los segmentos de LAN remotos se comporten como una sola LAN”

Al unir VPLS de capa 2 con MPLS que interconecta la capa 2 y 3 del modelo OSI, se garantiza la seguridad y accesibilidad de las LAN a cada una de las sedes o cliente, esto sucede a través de la interfaz de un proveedor de servicios.

El VPLS se basa en comunicaciones Ethernet multipunto a multipunto y es usualmente utilizada para dar acceso a dos o más sedes a internet seguro. Esto quiere decir, que el proveedor de servicio tendrá un único dominio de enrutador para crear y dar acceso a una LAN compartida con cada una de las sedes de la empresa. VPLS sustituye las líneas dedicadas por túneles seguros y controlables.

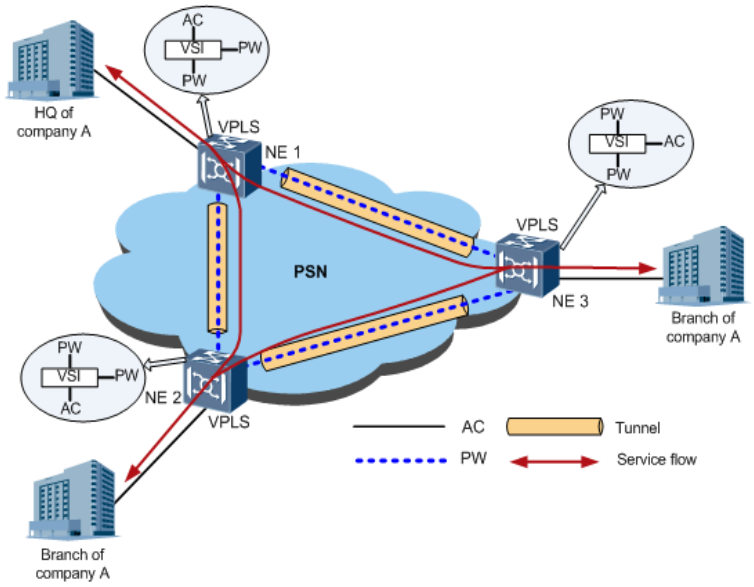

Diagrama 3. Aplicación de VPLS tomada de:https://forum.huawei.com/enterprise/es/%C2%BFcu%C3%A1l-es-la-diferencia-entre-vpls-y-vpws/thread/506873-100237 .

Según Gustavo, H (2019) En la figura anterior se evidencia el uso de la Tecnología VPLS basada en VPNs de capa 2, donde los nodos NE aíslan el segmento

LAN, dividen el tráfico de capa 2 mediante una instancia de conmutador virtual (VSI) y configuran una única interfaz lógica para representar varias VLAN existentes. El VSI permite hacer un mapeo entre la interfaz AC y PW interconectando las LAN para que funcione como una sola red

Tabla 1. Ventajas y desventajas de VPLS (Modificada de: https://mum.mikrotik.com/presentations/EC17/presentation_4477_1500865514.pdf

VPLS	
Ventajas	**Desventajas**
•No hay overhead (bit adicionales de control) y consigo no hay menor ancho de banda. •El servicio es apto para desplazarse por toda la red MPLS incluyendo a la red propia y clientes. •Ahorro en costos: Las empresas de gran tamaño podrán rentar el servicio VPLS.	• El túnel VPLS al tener un método de difusión broadcast requiere de cuidado y control. • Red expuesta a posibles bucles de encaminamiento o Routing loop, donde las tramas de datos se quedan en un bucle infinito en la red y gastando un ancho de banda innecesario. • Requiere de profesionales y de conocimiento calificado para implementar este tipo de servicio. • Requiere de una dirección de Loopback y de no activar el NAT para garantizar la conectividad VPLS

Al tener la red MPLS el servicio VPLS permite atravesar de forma transparente las tramas ethernet de un punto a otro de esta red, por medio de un portal compuesto de “Pseudo Cables (PWs)” que unen de forma lógica una interfaz VPLS con una interfaz física.

Para prestar un servicio VPLS el proveedor de servicio forma un puente o bridge de aprendizaje donde el reenvío de paquetes se hace en función de las direcciones MAC y las etiquetas VLAN. Este Puente se reconoce como VPWS.

Servicio de Cable Privado Virtual (VPWS)

En la red MPLS se encuentran los Pseudo cables o Pseudowire (PW) interconectando los circuitos de conexión ACs, los PW forman una malla reconocida como un puente o Bridge denominado VPWS definida por la RFC 4026 como:

"VPWS es un circuito punto a punto (enlace) conectando a dos dispositivos Customer Edge. El enlace está establecido de forma lógica a través de una red de conmutación de paquetes. El enrutador (CE) en La red del cliente está conectada a un enrutador PE en la red del proveedor a través de un Circuito de conexión" (RFC 4026,2005)

Es decir, que el VPWS como tecnología de VPN ofrece un servicio de transmisión punto a punto de paquetes en capa 2 y se encarga de hacer un mapeo entre las interfaces ACs y los PW, formando un circuito virtual y garantizando el flujo de paquetes de forma transparente entre clientes. El uso de varios VPWS formar una red L2VPN de múltiples sitios (Cisco, 2017)

Pseudo Cable (Pseudowire - PW)

Principalmente un Pseudo cable separa la parte IP de la parte de etiquetas MPLS como método de control de borde a borde. Es decir, en una red de conmutación de paquetes (PSN) el enrutador de MPLS diferenciará entre información de control de borde PW e información IP.

El transporte de múltiples servicios sobre una Red de conmutación virtual o PSN se logra al encontrar un formato intermedio común entre paquetes (IP, Ethernet, MPLS, otros) proporcionada por los PWs.

Para el buen funcionamiento de un PW, se debe saber que MPLS no cuenta con un protocolo de encapsulamiento estándar y que un paquete PW no debe tener por ningún motivo una etiqueta en el LSR (paquete IP) que inicie por 4 o 6 (IPv4, IPv6) como lo afirma la (RFC 4385,2006), dado a que el objetivo de PW se perdería al enrutar paquetes IP y no paquetes de control de borde.

Según la RFC 4385 (2006) "Un pseudowire es una conexión punto a punto emulada a través de una red de conmutación de paquetes que permite la interconexión de dos nodos con cualquier tecnología L2. El PW comparte algunos de los componentes básicos y construcciones arquitectónicas con las soluciones punto a multipunto"

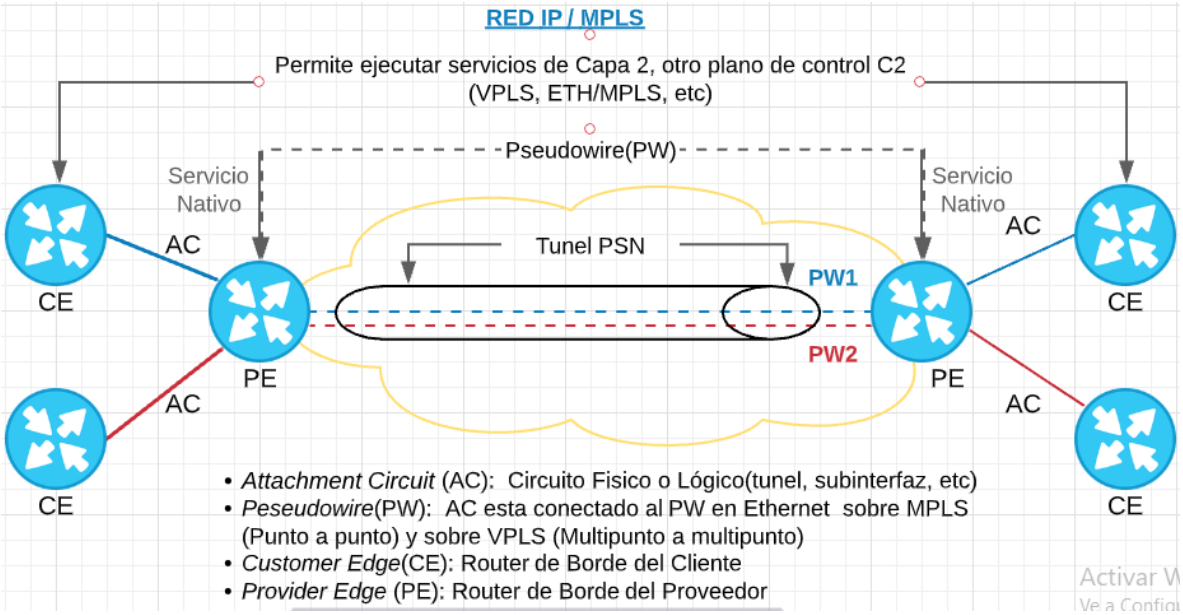

Diagrama 4.Topología MPLS capa 2 con PW diagrama modificado de: https://orhanergun.net/what-is-attachment-circuit-in-mpls-vpn/

En MPLS los datos recibidos por un enrutador PE se encapsulan y se envían a través del Pseudowire hasta llegar al otro enrutador PE, donde se quita nuevamente el encapsulamiento de datos.

Se debe tener en cuenta que en VPLS los Provider Edge (CE) pueden representar enrutadores, hosts o conmutadores a diferencia de una IPLS que transporta solo paquetes IP o de soporte. Donde los CE son conocidos como enrutadores o host, no como conmutadores.

MPLS L3VPN (VPN capa 3)

L3VPN o el modelo VPN de capa 3 para MPLS se basa en la RFC 4364, L3VPN usa un medio de transmisión de igual a igual (peer to peer) junto con el protocolo de puerta de enlace fronteriza (BGP). Este modelo de igual a igual permite el intercambio de datos de enrutamiento en la capa 3 entre el proveedor de servicios y los clientes, es decir que el proveedor puede hacer uso de las redes troncales para prestar servicios IP a sus clientes. (Cisco, s.f)

L3VPN en MPLS evita el cambio de infraestructura y enrutadores ante la necesidad de añadir un nuevo sitio a la red, puesto que, solo se debe actualizar el enrutador de borde del proveedor de servicios.

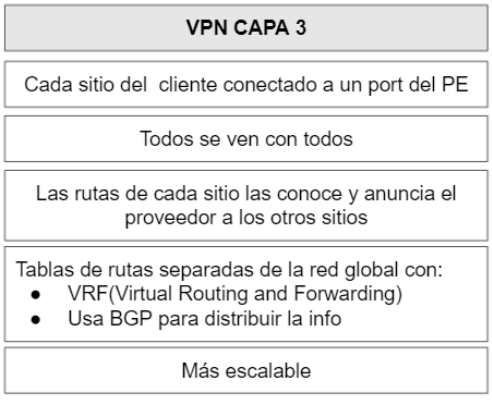

Figura 2. VPN Capa 3
Modificada de: https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro_MPLS.pdf

Ingeniería de tráfico (TE)

La ingeniería de tráfico adapta flujos de tráfico a recursos físicos, generando un equilibrio entre estas y evitando los llamados cuellos de botella (Recursos excesivamente utilizados). Es decir que el objetivo principal de TE es minimizar la congestión.

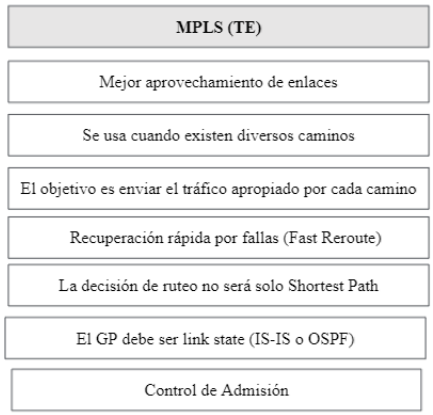

Figura 3.Ingeniería de tráfico modificado de:https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro_MPLS.pdf

La TE puede actuar en función de:

- **Tráfico** (minimiza pérdidas, minimiza retardos y mejora el rendimiento), también puede actuar
- **Los recursos** (optimiza el ancho de banda o recursos en general).

Calidad de servicio (Quality of Service-QoS)

QoS hace referencia a los parámetros básicos de calidad de un servicio, estos parámetros de control generan modificaciones para el cumplimento del nivel de servicio requerido.

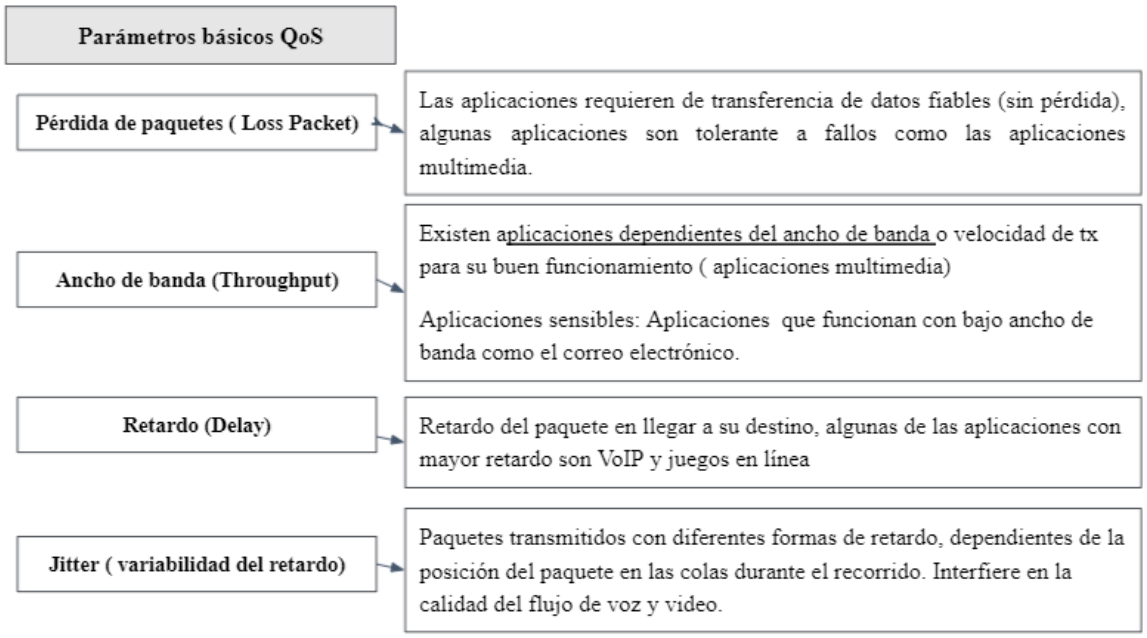

Diagrama 5. Parámetros básicos de calidad servicios realizados por: Sandra Moreno

De lo anterior, se puede afirmar que MPLS cuenta con un sistema seguro, confiable y de calidad alta, ya establecido en el mercado.

Software-Defined Networking in a Wide Area Network (SD-WAN)

SD-WAN es una red definida por software creada principalmente para facilitar la implementación y gestión de una red de área amplia (WAN). Se caracteriza por ofrecer un control centralizado, mayor tráfico de datos en la nube, mayor rendimiento en tiempo real, facilidad en la automatización de procesos, seguridad de la información y visibilidad de aplicaciones e infraestructura; ideal para las empresas que buscan una transformación digital a un costo asequible y funcional.

“Un servicio SD-WAN proporciona una red de superposición virtual que permite la aplicación de políticas, Conectividad impulsada y orquestada entre las interfaces de red de usuario SD-WAN, y proporciona la construcción lógica de una red privada virtual enrutada L3 para el suscriptor que transmite IP Paquetes entre sitios de suscriptores”

(MEF 70,2019, pág.6). SD-WAN permite aplicar políticas, mejora la conectividad proporcionando una construcción lógica de la red.

Capacidades principales de SD-WAN

Según los resultados plasmados por IBM y las encuestas realizadas por AvidThink en el 2018, las capacidades encontradas con mayor frecuencia en las soluciones de SD-WAN se evidencian en el siguiente gráfico.

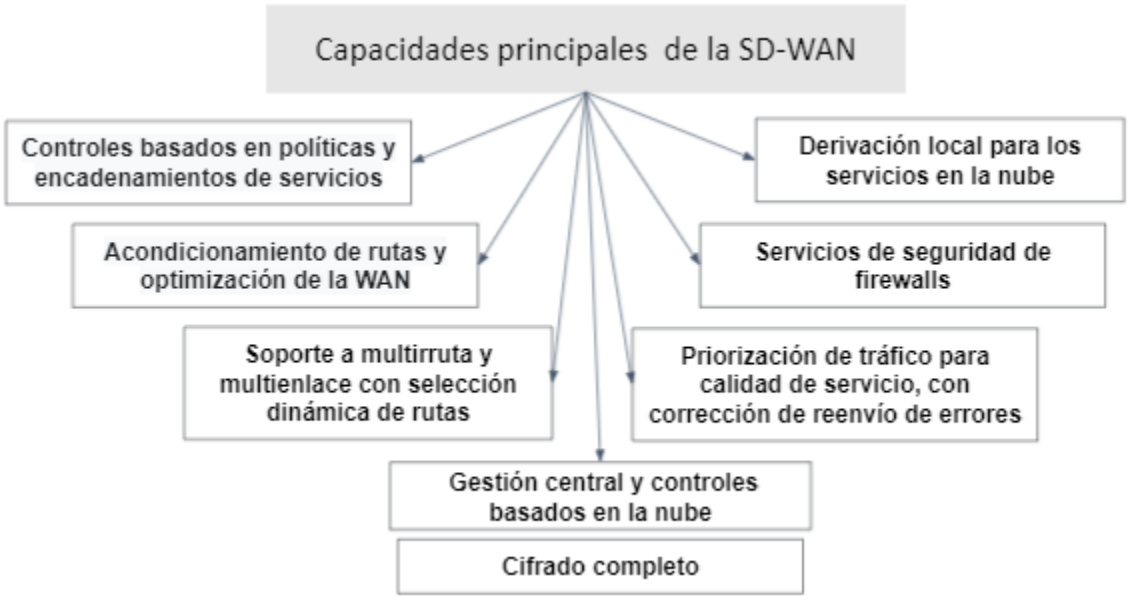

Diagrama 6. Principales capacidades de la solución SD-WAN datos tomados de: https://www.ibm.com/downloads/cas/3AW5O9OR

SD-WAN reúne un conjunto de herramientas que se adaptan al incremento del uso de aplicaciones y servicios basados en la nube (Office 365, Workday, Azure, AWS, otros), el incremento del tráfico y la necesidad de un mayor ancho de banda, para finalmente ofrecer una solución completa a la industria.

Estándar MEF 70 - Atributos y servicios SD-WAN

El *Metro Ethernet Forum* (MEF) es un foro global de la industria de redes, nube y tecnología. Su objetivo principal es establecer servicios seguros, dinámicos y certificados que permitan la transformación digital de las empresas, además, MEF está comprometido con estandarizar y establecer una terminología común ante el mercado. Este foro aprueba MEF 70, el primer estándar global de la industria que define y establece los atributos y servicios característicos de SD-WAN (tynmagazine, 2019). En la siguiente tabla se evidencian los componentes establecidos para SD-WAN.

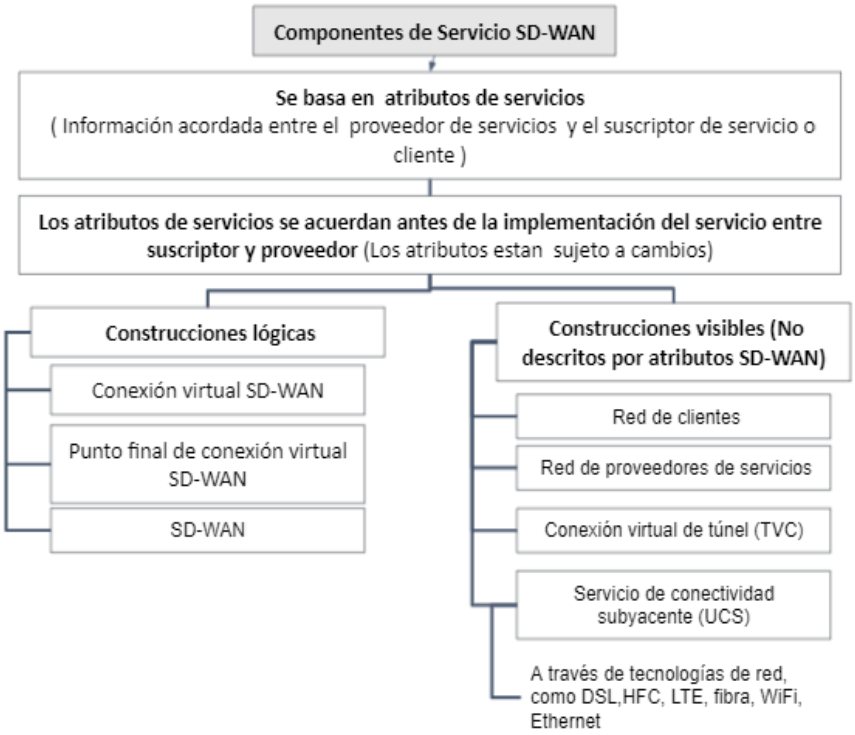

Diagrama. 7. Atributos y Componentes de Servicios SD-WAN Información tomada de https://www.mef.net/wp-content/uploads/2019/07/MEF-70.pdf(pag .9)

Los componentes del servicio SD-WAN son definidos según los atributos de servicios que se establecen entre el proveedor y cliente. Antes de la implementación del

servicio se deben aclarar los atributos en cuanto a la construcción lógica de la red. Sin embargo, hay aspectos de infraestructura y conectividad visible que se deben tener presentes. Una de ellas es el Servicio de Conectividad Subyacente (UCS) que el proveedor de servicios ofrece además de los servicios SD-WAN, otorgando a aquellos clientes que no cuentan con un nivel de conexión requerido para implementar SD-WAN. El UCS cuenta con algunas características que definen el flujo de aplicaciones y que es proporcionado por el proveedor de servicios SD-WAN por su propia red o por medio de un operador de red junto con internet.

Servicio de Conectividad Subyacente (UCS)

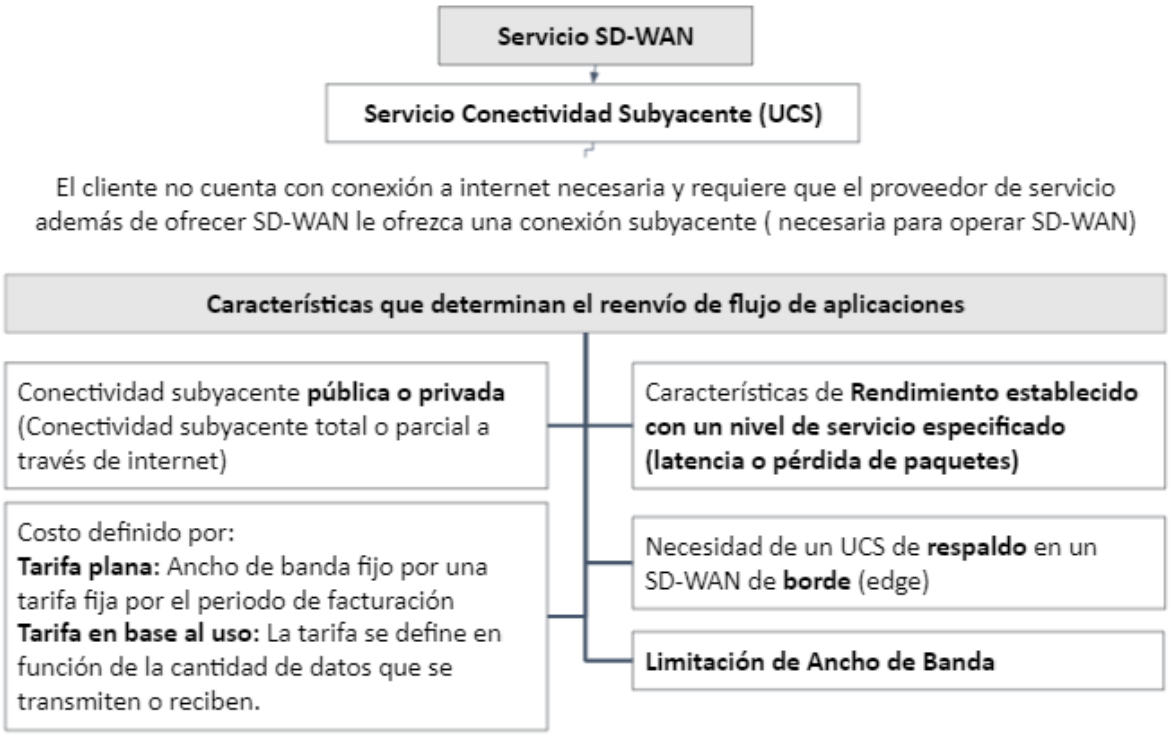

Diagrama 8. Características de un Servicio de Conectividad Subyacente (UCS)

En la implementación de SD-WAN usualmente se requieren Múltiples capas de conectividad subyacentes con diferente rendimiento y costo (IP VPN sobre red MPLS) o (Túnel IPsec sobre la red de Internet). El beneficio que ofrece en este caso SD-WAN es un diferenciador de transporte y menor costo.

Túnel Virtual de Conexión (TVC)

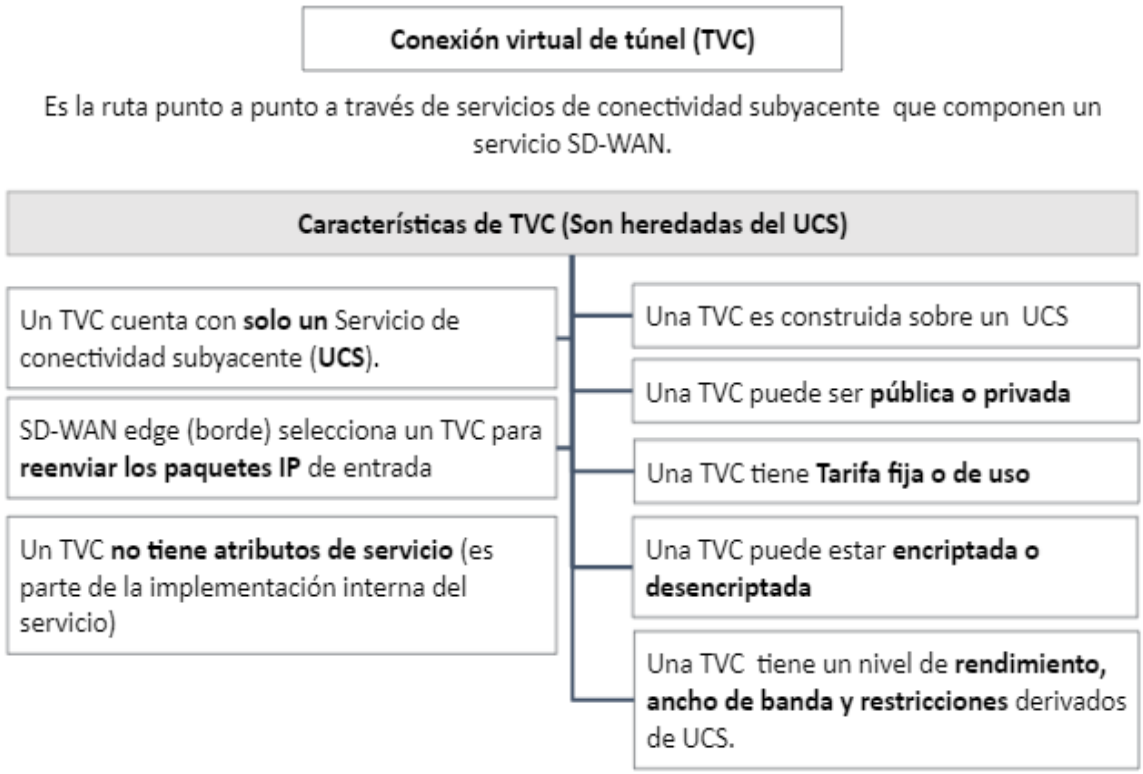

Diagrama 9. Túnel de Conexión Virtual l (TVC)

Al ser creado el túnel virtual, se crear junto él toda una topología virtual superpuesta y diferenciada de la topología física. Permitiendo una conectividad de malla

completa independientemente de si se conecta la sede con los clientes, pero no entre clientes.

Conexión Virtual SD-WAN y Punto Final (SWVC)

SD-WAN cuenta con una conexión virtual unidad a los puntos finales de conexión virtual ubicada en la interfaz de red del usuario. El Punto Final (SWVC) asocia los paquetes IP de forma lógica, aplicándoles una política de reenvío y decisión.

Ruptura de INTERNET

SD-WAN con la ruptura de internet logra evitar el envío de algunos paquetes por la interfaz de usuario o por el Túnel de Conexión virtual, debido al posible envío del paquete directamente al destino conectado a internet.

Los Parámetros de internet que debe tener en cuenta el cliente y proveedor: 1. Ancho de Banda, 2. La disponibilidad funcional de NAT/PAT y 3. Direccionamiento IP.

Según lo anterior, se puede evidenciar que SD-WAN cuenta con parámetros de conectividad, calidad y componentes de servicio básicos que deben ser establecidos entre el proveedor del servicio y el suscriptor antes de la implementación a fin de evitar inconvenientes futuros.

Ventajas y Desventajas de MPLS y SD-WAN

Tabla 1.Ventajas y desventajas de MPLS y SD-WAN

	Ventajas	Desventajas
MPLS	- MPLS puede tener varios tipos de enlaces de acceso, evitando cambios en la infraestructura actual de la compañía o proveedor de servicio - Eficiente, segura y escalable - Confiabilidad en la entrega de paquetes. - Uso de aplicaciones en tiempo real ofreciendo un nivel de calidad de servicio para equipo remoto, VoIP, video, entre otros contenidos multimedia. - Red más fiable y óptima al garantizar mayor control de la red. - Posibilidad de priorizar el tráfico y retener paquetes - Garantiza la privacidad de los datos.	- Requiere capacidad de banda ancha - Costo elevado - Usa una red tradicional, no es escalable - Posible fallo en la configuración tradicional genera un nivel alto de Inseguridad sobre la red - Manejo complejo - Requiere piezas dedicadas de Hardware para cada oficina remota y para el centro de datos (Enrutadores) - Cuenta con enrutadores con tecnología patentada y con administración requerida equipo por quipo.
SD-WAN	- Evoluciona la arquitectura tradicional (LAN, MAN y WAN) - Mayor rendimiento al garantizar mayor ancho de banda - Disponibilidad para hacer actualizaciones - Escalable - Simplifica el manejo y gestión del flujo de datos - Conexiones de red más flexibles - Interconexiones unificadas o centralizadas a un menor costo.	- Disminuye la confiabilidad en la entrega de paquetes. - Disminuye el control directo del tráfico por el uso de redes públicas aumentando la probabilidad de pérdida de paquetes y de latencia. - No es conveniente para compañías con multitud de aplicaciones imprescindibles o vitales en tiempo real.

Capítulo2.
Mejor opción entre SD-WAN y MPLS según los requerimientos de la empresa.

Breve estudio de mercado (adopción de SD-WAN)

La empresa estadounidense SDxCentral dentro de sus análisis de mercado tecnológico, evalúa la realidad de las empresas que están interesadas en implementar SD-WAN o a las que ya la adoptaron.

"El 55% de los encuestados tienen desplegada WAN híbrida o SD-WAN; el 27% solo tienen MPLS y otra línea privada, mientras que el 18% solo tienen Internet de banda ancha" IBM (2018).

Dado al notable incremento del uso de SD-WAN, se genera cierto interés y curiosidad por parte de los expectantes por conocer y reconocer esta tecnología más a fondo.

Según IBM (2018) los requerimientos principales para que una empresa adopte SD-WAN son: La reducción de costos, Agilidad de la red y las herramientas de gestión (automatización), este último ofrecería a la empresa un nivel de ahorro en capital y en la parte operativa.

Si SD-WAN ofrece un buen nivel de servicio y cumple con un nivel alto de las necesidades actuales del mercado ¿Qué sucede con las empresas que aún no implementan SD-WAN?, pues según IBM (2018) no hay confiabilidad en los proveedores de servicio TI pues no hay garantía de obtener un TI calificado, por el número de proveedores posibles para contratar (son todo un desafío) y finalmente, porque no se tiene clara la solución más apropiada. El desconocimiento en el costo estimado y tiempo de la

implementación se suma a los miedos que evitan la implantación de SD-WAN en las redes existentes.

Se podría afirmar que todos los obstáculos antes mencionados se pueden solucionar empapándose en este tema y haciendo una buena elección, sin embargo, es cierto que no todo lo que esperan las compañías al implementar SD-WAN se hace realidad, pues, el nivel de mejora en el rendimiento de la red fue de menos del 10% para la mayoría de las empresas con SD-WAN encuestadas. Tristemente, la red tiene la posibilidad de no cumplir con las expectativas del suscriptor y pondría en duda el nivel de rendimiento de la red en futuras ocasiones.

Frente a la duda que genera SD-WAN en cuanto al posible mal rendimiento de la red, se hace un contraste con los beneficios indudables que ofrece, como la reducción de costos, ya que, se obtuvo un 52% de ahorro en costos de ancho de banda y un 42% de ahorro en costos operativos y de gestión, como resultado de las compañías que implementaron red Hibrida o SD-WAN. Devolviendo un porcentaje de la inversión.

Requerimientos de la empresa:

Los requerimientos de la empresa se establecieron según nivel de prioridad para la situación actual.

1. Reducción de costos y/o gastos: La empresa requiere un mayor ancho de banda, operatividad y gestión centralizada a un menor valor.
2. Distribución dinámica del tráfico: Es necesario garantizar la Agilidad de la red y la supervisión en la pérdida, latencia y QoS de los paquetes y/o servicios.

3. Aplicaciones y estabilidad del servicio con VPN (Internet, VoIP, Centro de datos y otros)
4. Seguridad

Además, es necesaria la conectividad de:

1. Localidades remotas y sucursales
2. Localidades de oficinas centrales y locales
3. Centros de datos privados (Nube privada)
4. Acceso a internet
    - Varias conexiones WAN
    - Varios proveedores de servicios

Comparación entre MPLS y SD-WAN según los requerimientos

Los requerimientos clave para una red según Gartner en (2020):

1. Debe soportar múltiples tipos de conexión (MPLS, Internet, LTE, otros)
2. Selecciona rutas dinámicas (Permite compartir cargas a través de conexiones WAN)
3. Provee una interfaz simple para manejar WAN (El proceso de instalación de infraestructura TI o aprovisionamiento se podrá hacer sin contacto a una sucursal con fácil configuración)
4. Debe soportar VPNs (Ofrece servicios adicionales)
    - Optimización de la WAN
    - Controladores
    - Firewalls

- Gateways web

5. Costo y/o gastos convenientes.

A continuación, se tienen en cuenta los requerimientos de la empresa y se comparan las dos tecnologías MPLS y SD-WAN. Esta comparación entre tecnologías está basada en uno de los segmentos de From The Guys in Orange junto a Pat Herron (Fastmetrics,s.f.).

Proveedor de Servicio (Internet)

La red MPLS requiere de un proveedor de servicios en un circuito a través de una red privada de nivel de operador con su respectivo acuerdo de nivel de servicio típico.

A diferencia de SD-WAN que requiere de dos circuitos de Internet.

Mejor entrega de paquetes

MPLS ofrece una entrega del 99,9% de los paquetes (1 de 1000 paquetes en tránsito se pierden) gracias al acuerdo de nivel de servicio. Esto representa dinero para la empresa.

SD-WAN puede tener pérdidas del 1% o más (más de uno de 100 paquetes se puede perder). Al tener dos o más conexiones a internet prevé que el nivel de servicio ofrecido por el proveedor de banda ancha sea menos significativo para la pérdida de paquetes en casos de congestión de la red.

Las pérdidas generadas por errores e intermitencia en los enlaces de acceso a internet, SD-WAN se mitigan con la corrección de errores de reenvío (Forward Error Correction -FEC) agregando redundancia o bits de paridad a los datos transmitidos para

finalmente dar los datos necesarios a el receptor para detecta la pérdida y recuperar el paquete inicial.

Mejor rendimiento de las aplicaciones y priorización de servicios

MPLS ofrece mayores garantías de rendimiento que SD-WAN pues tiene la posibilidad de asignar 2,4 o hasta 7 colas o niveles de prioridad a las aplicaciones. La asignación la hace el administrador de la red al identificarlas, etiquetarlas y mapearlas en la cola indicada (abordada como QoS) este proceso es engorroso pero confiable.

A diferencia de MPLS, SD-WAN ofrece docenas de colas o niveles de priorización de las aplicaciones por medio de una herramienta para el seguimiento y control, simplificando la asignación de Apps a las colas, sin embargo, esta priorización no es garantizada al ser transmitidas a través de internet, con un posible desorden de paquetes al llegar de un extremo al otro. Al tener una red de datos privada puede priorizar las aplicaciones que fluirán sobre los recursos compartidos y agregar herramientas para mejorar la priorización.

Fiabilidad

MPLS hace copias de seguridad de la red por medio de BGP y una VPN en internet como una solución de conmutación de error, a espera de recuperar el acceso a la red privada. El costo de estas copias de seguridad las cubre la empresa y no son tan efectivas por posibles interrupciones en servicios (Telefonía) en caso de un error.

SD-WAN tiene múltiples enlaces a internet, múltiples enlaces a internet no será más seguro que solo uno, lo que degrada finalmente la calidad del circuito. Sin embargo, SD-WAN reconoce las Apps prioritarias y las envía por el mejor canal incluso en caso de

un fallo en un enlace de acceso. La confiabilidad de las Apps depende de la solución SD-WAN ofrecida dando la oportunidad de mejorar la confiabilidad de las apps de forma simple, rápida y eficaz.

Seguridad

En MPLS el contenido de los paquetes solo puede ser visto por los nodos MPLS que tienen la etiqueta destinada al mismo nodo. Luego, el paquete es enviado a un proveedor de servicio de confianza.

SD-WAN cuenta con un túnel seguro permitiendo el desplazamiento de los paquetes sobre la red de forma transparente con protocolos como IPSec y una conexión VPN.

SD-WAN permite adicionar y superponer servicios de seguridad de red. (Firewalls). Al ser una tecnología con tantos caminos posibles para llevar el tráfico y con una buena distribución la interceptación de paquetes se hace casi imposible.

Tabla 2.*Comparación entre MPLS y SD-WAN*

	MPLS	**SD-WAN**
Proveedor de Servicio (Internet)	1. Servicio de Internet dedicado de nivel de operador	1. Servicio de Internet dedicado de nivel de operador 2. servicio de Internet de banda ancha del proveedor de cable.
Mejor entrega de paquetes	**A Nivel De Operador**: MPLS pierde menos del 0.1% de paquetes con acuerdo de nivel de servicio (SLA) con garantía real.	**A Través De Internet:** SD-WAN pierde un 1.0% de los paquetes con un acuerdo de nivel de servicio (SLA) con garantía nominal. Por lo tanto, SD-WAN requiere 2 o más conexiones a internet.

Mejor rendimiento y priorización de las aplicaciones	MPLS ofrece mayores garantías de rendimiento que SD-WAN. MPLS ofrece calidad de servicio y priorización de extremo a extremo con un etiquetado y mapeo engorroso pero muy confiable.	No se garantiza la priorización de Apps en SD-WAN al ser transmitidas a través de internet. Sin embargo, la priorización de aplicaciones se caracteriza por tener un acceso a cambios y configuración simple. SD-WAN ofrece más herramientas de seguimiento y control que MPLS junto con una visibilidad del rendimiento de las Apps al ingeniero de TI.
Fiabilidad	MPLS usa la conmutación de error basada en (BGP) y VPN para conectarse a MPLS, las conexiones de respaldo no funcionan como deben y su tiempo de conmutación por error es prolongado.	• SD-WAN utiliza múltiples enlaces • Usa un mecanismo de conmutación autoconsciente • Usa enrutamiento de aplicaciones de forma prioritaria sobre la mejor conexión • Sus aplicaciones son basadas en sesiones ininterrumpidas
Seguridad	MPLS es considerado seguro aún con recursos de red compartida con: - Direccionamiento de paquetes privados - Un proveedor de servicios único	SD-WAN se considera seguro en un nivel aceptable aún al funcionar a través de internet, ya que, permite adicionar servicios de seguridad a menor costo y de forma sencilla. Cuenta con un Túnel seguro basado VPN (IPsec) y Varias rutas activas que aumentan la seguridad.

Capítulo 3.
Mejor opción para una empresa corporativa a nivel nacional e internacional según sus Requerimiento

Al hacer el análisis de las dos tecnologías e identificar sus desventajas, sus ventajas e infraestructura, se define SD-WAN como la tecnología más apropiada para esta compañía según sus necesidades.

MPLS es mucho más confiable, segura y con una mayor experiencia en el mercado, sin embargo, SD-WAN es una tecnología más flexible y adaptable a las necesidades actuales. SD- WAN se elige sobre MPLS por los siguientes motivos:

- **Conexiones de internet:** SD-WAN ofrece conexiones a internet y un mejor nivel de servicio a un menor costo.

- **Configuración de la red:** MPLS requiere de configuraciones complejas para los dispositivos de red

- **Oficinas remotas internacionales:** MPLS no ofrece conectividad directa a internet para las oficinas remotas y SD-WAN sí.

- **Cambios y flexibilidad sobre la red:** MPLS es una red estática que toma decisiones en base a direccionamiento IP, los cambios y despliegue de la red son demorados, mientras que el negocio del cliente se basa en aplicaciones en la nube.

- **Reducción de costos y gastos:** MPLS tiene un alto costo del ancho de banda, usualmente los proveedores deben asociarse con otros servicios que ayudan a tener la cobertura global, por lo que los precios aumentan aún más.

  Actualmente los usuarios consumen contenido multimedia, realidad aumentada, realidad virtual a un alto costo, la demanda puede afectar el presupuesto de una empresa y SD-WAN reduce este alto factor, al ser una tecnología que se complementa con enlaces de internet públicos (banda ancha, 4G, LTE). Hoy en

día son más accesibles.

El principal beneficio que brinda SD-WAN es el nivel económico que ofrece a la industria, por tal motivo a continuación se especifican los gastos por servicio que debe costear una compañía en Bogotá con MPLS frente a la implementación de SD-WAN.

Diferencia en gastos por servicios e infraestructura

En este capítulo se muestra la topología MPLS y SD-WAN, junto con los valores mensuales que **debe costear** el cliente por el servicio que le presta la compañía de TI según cada una de las tecnologías, para finalmente diferenciar la infraestructura y gastos por servicios.

Infraestructura MPLS y gastos por servicio mensual

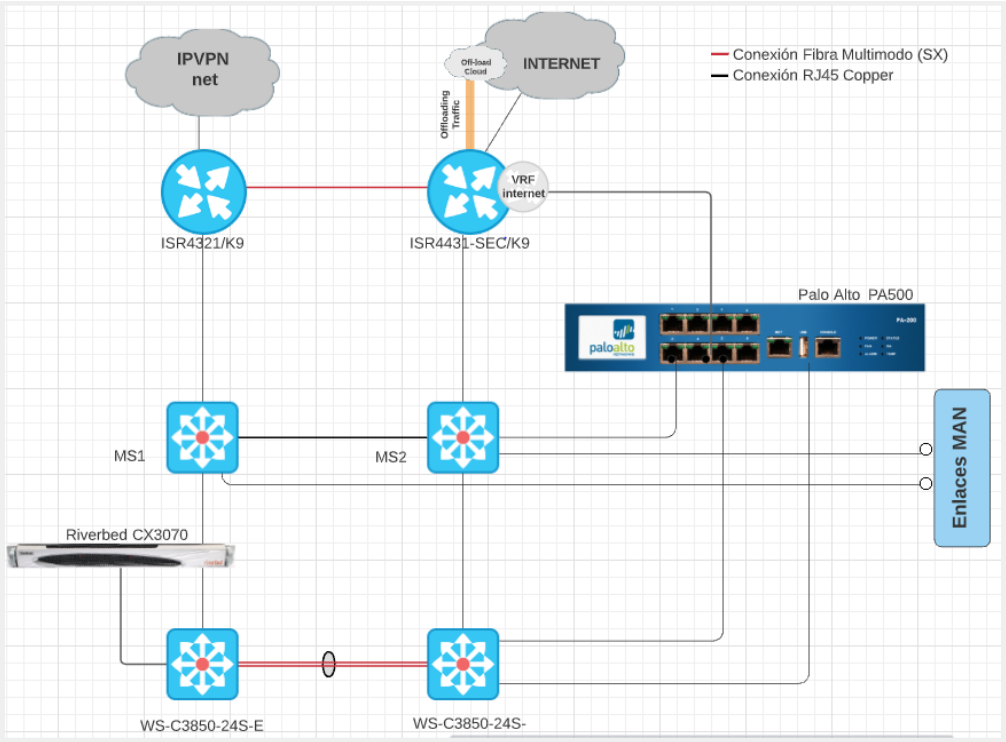

Diagrama 10.Topología MPLS Bogotá

Los equipos utilizados en la topología MPLS son:

- **Enrutador ISR4321 /K9:** Enrutador de servicios integrados para sucursales pequeñas entregando 50Mbps – 100 Mbps.
- **Enrutador ISR4431-SEC /K9:** Enrutador ISR4321 /K9 con paquete de seguridad que entrega de 500Mbps-1Gbps
- **Switch MS**
- **Acelerador de aplicaciones Riverbed CX3070:** Dispositivo de optimización WAN dedicado mejora el rendimiento de apps y transferencia de datos en este caso con un ancho de banda de 30 Megas.
- **Switch WS-C3850-2AS-E:** Conmutador con 24 puertos SFP, permite la conmutación de capa 2 a la 4 al comunicar la capa de acceso (1-2) con la capa de agregación.
- **Firewall de PALO ALTO PA500**: Protege la red de ciberamenazas y habilita el acceso a aplicaciones de forma segura.

Tabla 3. Gastos que incurre el cliente por el servicio de MPLS

Gastos que incurre el cliente por el servicio de MPLS			
No.	**Servicio**	**Especificación**	**Valor mensual**
1	**Conectividad MPLS**		$1,884.00
1.1.	**Internet**	Servicio principal, Acceso seguro a internet (SIA), Gestión de enrutamiento y garantía del nivel del servicio.	
2	**Gestión del servicio MPLS**		$7,373.00
2.1.	**Equipos**		
2.2	**Licencias**	Licencia DNA	

2.3	**SDN gateway**	SDN Gateway	
2.4	**Mantenimiento**	Mantenimiento de equipos	
2.5	**Servicio**	Mantenimiento punto final por equipo Servicio de mantenimiento por sitio	
3.	**Acelerador de BW**	Optimización de canal 30 Megas con Riverbed CX3070	$1,530.00
Servicio MPLS (mensual en USD)			**$10,787.00**
Servicio MPLS (mensual en COP)			**$ 39.631.438**

La compañía debe pagar mensualmente por el Servicio MPLS un valor de $10,787 dorares que incluye la optimización del canal de 30 Megas que ofrece Riverbed CX3070 con un valor de $1,530.00 USD mensual, la durabilidad del contrato de este servicio es de 36 Meses e incluye posibles renovaciones de contrato.

Infraestructura SD-WAN y gastos por servicio mensual

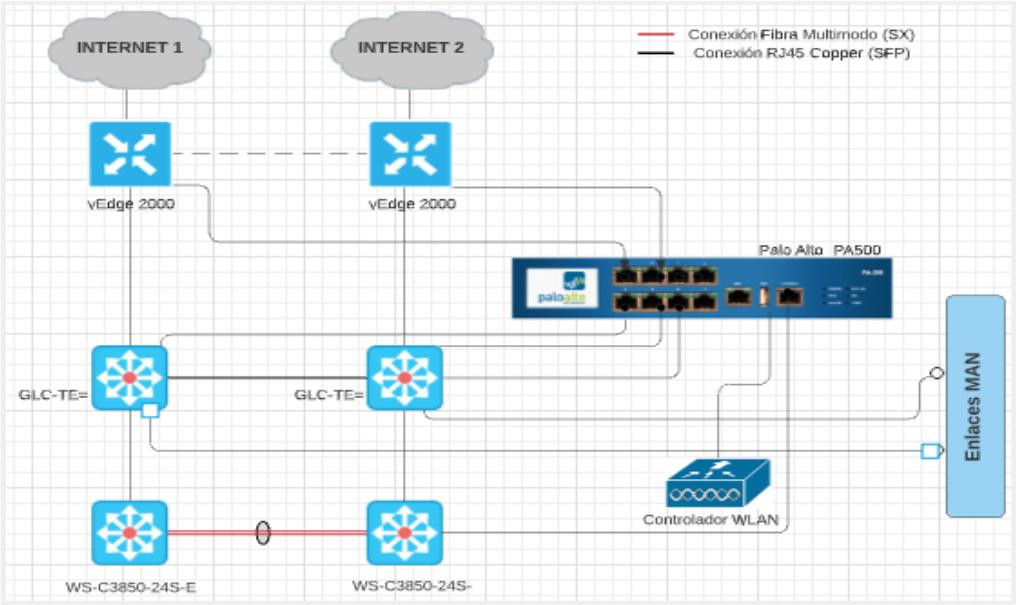

Diagrama 11. Topología SD-WAN Bogotá

Los equipos utilizados en la topología SD-WAN son:

- **VEdge-2000-AC-K9:** Enrutador que brinda la capacidad esencial de WAN, múltiples nubes y seguridad. Es indispensable para establecer una red de superposición virtual segura sobre cualquier transporte WAN. Puede ser un Software, Hardware, componentes virtuales o nube. VEdge-2000-AC-K9 es un enrutador físico (Hardware) con 2 módulos de interfaz (8 puertos de 1Geth y 2puertos de 10Geth), 4 SFP de 1Giga Etherner.
- **Switch con GLC-TE:** Conmutador con modulos SFPs fibra óptica
- **Switch WS-C3850-2AS-E:** Conmutador con 24 puertos SFP, permite la conmutación de capa 2 a la 4 al comunicar la capa de acceso (1-2) con la capa de agregación.
- **PALO ALTO PA500:** Protege la red de ciberamenazas y habilita el acceso a aplicaciones de forma segura.
- **Controlador WLAN:** Controlador virtual LAN con administrador central que facilita la configuración de firmware en un solo dispositivo. Despliegue de configuración automática, facilidad en nuevos puntos de acceso, posibilidad de paso de un dispositivo WLAN a otro sin pérdida de conexión (comunicación puntos de accesos y enrutadores) y alta disponibilidad de infraestructura WLAN

Para implementar SD-WAN, se trabaja sobre la red ya existente WAN (figura1), donde se reemplazan los enrutadores de la serie ISR 4000 por los vEdge 2000 de Cisco para crear canales de internet puro que serán alcanzables desde la zona de control de la red. La red LAN no se interviene con el fin de garantizar la seguridad y estabilidad de la

red. Además, se hace innecesario el uso del equipo Riverbed CX3070, conocido como acelerador de ancho de banda, ya que este se encarga de acelerar la transferencia de datos y aplicaciones entre las redes Cloud, sucursales, centros de datos y usuarios finales; función que ya cumple la infraestructura SD-WAN.

Sabiendo que hoy en día el ancho de banda de internet es más económico, se puede decir que al implementar SD-WAN y retirar el equipo Riverbed pasa de ofrecer un servicio MPLS con un ancho de banda de 30 Megas a ofrecer un Internet de 150 Megas, con una evidente reducción de gastos en equipos e infraestructura.

Tabla 4. Gastos que incurre el cliente por el servicio de SD-WAN

Gastos que incurre el cliente por el servicio de SD-WAN			
No.	**Servicio**	**Especificación**	**valor (USD)**
1	**Conectividad SD-WAN**		**$1,711.00**
1.1.	**Internet**	Internet 1 Internet 2	
2	**Gestión del servicio SD-WAN**		**$1,839.00**
2.1.	**Equipos**	VEDGE-2000-AC-K9 (2 unidades)	
2.2	**Licencias**	Licencia DNA	
2.3	**SDN Gateway**	SDN Gateway	
2.4	**Mantenimiento**	Mantenimiento de equipos	
2.5	**Servicio**	Mantenimiento punto final por equipo Servicio de mantenimiento por sitio	
Servicio SD-WAN (mensual en USD)			**$3,550.00**
Servicio SD-WAN (mensual en COP)			**$13.163.400**

Se ahorra un valor de $7,237.00 (USD) al retirar parcialmente el MPLS, poner un canal de internet con mayor ancho de banda y retirar el servicio que cumplía el Riverbed o el acelerador de Ancho de Banda.

MPLS	SD-WAN	Ahorro (67,09%)
10.787,00	3.550,00	7.237,00

La mejor opción para una empresa corporativa a nivel nacional e internacional según sus requerimientos, es la implementación de SD-WAN sobre MPLS, así se ofrece la calidad de servicio, ancho de banda, flexibilidad, acceso a la nube y reducción de gastos que ofrece SD-WAN y se mantienen los circuitos confiables que ofrece MPLS.

Conclusiones

- La red MPLS genera un alto nivel de confianza en el mercado por su trazabilidad a lo largo de los años. Sin embargo, obliga al sector a cubrir valores altos por una red inadaptable a cambios y al modelo de red actual.
- SD-WAN es una tecnología que ofrece soluciones basadas en la nube, un claro ejemplo es el servicio de correo electrónico con Office 365 o el servicio de gestión de recursos humanos con el software de planificación de recursos (ERP) desde Workday y Salesforce, aplicaciones ejecutadas principalmente en la nube, que hace innecesario el uso de servidores dedicados en el centro de datos. Estas facilidades no las brinda MPLS
- Según la comparación realizada entre MPLS y SD-WAN, se identificó que SD-WAN ofrece simplicidad operativa, control centralizado y con visibilidad de extremo a extremo de la red. La flexibilidad y la priorización de aplicaciones sin afectar el rendimiento de las mismas, es otra de las características propias de esta tecnología. SD-

WAN crea una red apta para evolucionar y adaptarse a la naturaleza de las aplicaciones, al incremento del tráfico, a los requerimientos del cliente y al uso de servicios en la nube. Por último, el beneficio que lleva a la industria a implementar SD-WAN, es el nivel de reducción gastos mensuales frente a MPLS. Según el estudio realizado se obtuvo una reducción de un 67,09% al pasar de MPLS a SD-WAN.

- SD-WAN tiene también sus puntos débiles y uno de ellos es el básico nivel de seguridad que ofrece por su constante interacción con la red pública, sin embargo, las empresas han optado por invertir un poco más en el ámbito de seguridad e integrarlas como una herramienta más a SD-WAN.
- SD-WAN es escogida como la solución más apropiada para la Compañía porque cumple su principal necesidad en bajo costo, su adaptabilidad a cambios, acceso a servicios sobre la nube (Administración centralizada) y por el nivel seguridad aceptable que ofrece.

Lista de referencias

Albrightson, R.-L.-A. J. (1994). *EIGRP: un protocolo de enrutamiento rápido basado en vectores de distancia*. Obtenido de https://escholarship.org/content/qt9h48b8x2/qt9h48b8x2.pdf

Andersson y Madsen (2005). *Provider provisioned VPN Terminology*. RFC 4026. Recuperado de https://datatracker.ietf.org/doc/html/rfc4026#page-3

Andersson, L (2015). *Terminología de red privada virtual (VPN) aprovisionada por el proveedor.* Recuperado de https://datatracker.ietf.org/doc/html/rfc4026#section-6.1

Azure (s.f). *¿Qué es SaaS?.* Recuperado de: https://azure.microsoft.com/es-es/overview/what-is-saas/

Cisco. (s.f.). *Ethernet VPN (EVPN)* . Obtenido de https://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-series-aggregation-services-routers/whitepaper_c11-731864.html

Cisco (s.f). Layer 3 *VPNs (L3VPN).* Cisco. Recuperado de https://www.cisco.com/c/en/us/products/ios-nx-os-software/layer-3-vpns-l3vpn/index.html

Cisco. (2007). *Conceptos y troubleshooting de Pseudowire.* Obtenido de https://www.cisco.com/c/es_mx/support/docs/multiprotocol-label-switching-mpls/mpls/212007-Pseudowire-Concepts-and-troubleshooting.pdf

Cisco. (2008). *MPLS Label Distribution Protocol (LDP).* Obtenido de https://www.cisco.com/c/en/us/td/docs/ios/mpls/configuration/guide/12_2sr/mp_12_2sr_book/mp_ldp_overview.pdf

Cisco (2017). *Conceptos y thoubleshooting de pseudowire*. Recuperado de https://www.cisco.com/c/es_mx/support/docs/multiprotocol-label-switching-mpls/mpls/212007-Pseudowire-Concepts-and-troubleshooting.html

Cisco (2018). *MPLS L2VPN Pseudowire*. Cisco. Recuperado de https://www.cisco.com/c/es_mx/support/docs/multiprotocol-label-switching-mpls/mpls/213238-mpls-l2vpn-pseudowire.html

Cisco (2020). *Configuración de una VPN MPLS básic*a. Recuperado de https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html

Cisco Community (2016). *L2 VPN V/S L3 VPN*. Recuperado de https://community.cisco.com/t5/mpls/l2-vpn-v-s-l3-vpn/td-p/2898002

Davila, L. P. (s.f.). *VRF (Virtual Routing and Forwarding).* Obtenido de Cisco: https://community.cisco.com/t5/documentos-routing-y-switching/vrf-virtual-routing-and-forwarding/ta-p/3406835

https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html, C. (. (s.f.).

Fastmetrics (s.f). *SD-WAN vs MPLS*. Recuperado de https://www.fastmetrics.com/blog/tech/sd-wan-vs-mpls/

Foro Huawei (2020) *Sistema Autónomo (AS).* Recuperado de: https://forum.huawei.com/enterprise/es/sistema-aut%C3%B3nomo-as/thread/658833-100235

Gartner (2020). *SD-WAN ¿Qué es y porque le ahorrará más que dolores de cabeza? Blog bismark* Recuperado de https://bismark.net.co/sdwan-conceptos-y-ventajas-para-las-empresas/

Greenfield (s.f.). *Una historia de SD-Wan*. Recuperado de https://www.catonetworks.com/sd-wan/a-history-of-sd-wan/

Genovez, A (2017). *Tuneles VPLS sobre MPLS*. Recuperado de https://mum.mikrotik.com/presentations/EC17/presentation_4477_1500865514.pdf

IEEE802.2. (s.f.). *Logical Link Control (LLC).* Obtenido de http://www.networksorcery.com/enp/protocol/IEEE8022.htm

ITU. (1997). *VOCABULARIO DE TÉRMINOS DE LAS TELECOMUNICACIONES*. Obtenido de Rec. UIT-R M.1224: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1224-0-199702-S!!PDF-S.pdf

IBM (2018). *Implementación de SD-WAN*. Recuperado de https://www.ibm.com/downloads/cas/3AW5O9OR

Manuel Freire Medina, J. R. (s.f.). *Simulación de protocolos de comunicaciones* . Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/6696/1/SIMULACI%c3%93N%20DE%20PROTOCOLOS%20DE%20COMUNICACIONES.pdf

Millan, R. (2002). *MPLS (MultiProtocol Label Switching)*. Obtenido de https://www.ramonmillan.com/documentos/mpls.pdf

Mef 70 (2019). Mef 70 SD-WAN service attributes and services. Recuperado de https://www.mef.net/wp-content/uploads/2019/07/MEF-70.pdf

Para Guatavo, H (2019). *¿Cuál es la diferencia entre VPLS y VPWS?*. Huawei . Recuperado de https://forum.huawei.com/enterprise/es/%C2%BFcu%C3%A1l-es-la-diferencia-entre-vpls-y-vpws/thread/506873-100237

Parra, J. F. (1996). *DISEÑO E IMPLEMENTACIÓN DE REDES FRAME RELAY Y.* Obtenido de https://repositorio.tec.mx/bitstream/handle/11285/628635/CEM337086.pdf?sequence=1

Prashant Garimella, Y.-W. E. (s.f.). *Characterizing VLAN usage in an Operational Network.* Obtenido de https://dl.acm.org/doi/pdf/10.1145/1321753.1321772

RFC 3031 (2001). *MPLS Architecture*. Recuperado de https://datatracker.ietf.org/doc/html/rfc3031#page-3

RFC 4385 (2006). Provider provisioned VPN Terminology. Recuperado de https://datatracker.ietf.org/doc/html/rfc4026#page-3

RFC 4385 (2006). Pseudowire Emulation Edge-to-Edge (PWE3) control Word for Use over an MPLS PSN. Cisco Systems. Recuperado de https://datatracker.ietf.org/doc/html/rfc4385

Albrightson, R.-L.-A. J. (1994). *EIGRP: un protocolo de enrutamiento rápido basado en vectores de distancia*. Obtenido de https://escholarship.org/content/qt9h48b8x2/qt9h48b8x2.pdf

Cisco. (2007). *Conceptos y troubleshooting de Pseudowire.* Obtenido de https://www.cisco.com/c/es_mx/support/docs/multiprotocol-label-switching-mpls/mpls/212007-Pseudowire-Concepts-and-troubleshooting.pdf

Cisco. (2008). *MPLS Label Distribution Protocol (LDP).* Obtenido de https://www.cisco.com/c/en/us/td/docs/ios/mpls/configuration/guide/12_2sr/mp_12_2sr_book/mp_ldp_overview.pdf

Cisco. (s.f.). *Ethernet VPN (EVPN)* . Obtenido de https://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-series-aggregation-services-routers/whitepaper_c11-731864.html

Davila, L. P. (s.f.). *VRF (Virtual Routing and Forwarding).* Obtenido de Cisco: https://community.cisco.com/t5/documentos-routing-y-switching/vrf-virtual-routing-and-forwarding/ta-p/3406835

Foro Huawei. (30 de Septiembre de 2020). *Sistema Autónomo (AS).* Obtenido de https://forum.huawei.com/enterprise/es/sistema-aut%C3%B3nomo-as/thread/658833-100235

https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html, C. (. (s.f.).

IEEE802.2. (s.f.). *Logical Link Control (LLC).* Obtenido de http://www.networksorcery.com/enp/protocol/IEEE8022.htm

ITU. (1997). *VOCABULARIO DE TÉRMINOS DE LAS TELECOMUNICACIONES*. Obtenido de Rec. UIT-R M.1224: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1224-0-199702-S!!PDF-S.pdf

Manuel Freire Medina, J. R. (s.f.). *Simulación de protocolos de comunicaciones* . Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/6696/1/SIMULACI%c3%93N%20DE%20PROTOCOLOS%20DE%20COMUNICACIONES.pdf

Millan, R. (2002). *MPLS (MultiProtocol Label Switching)*. Obtenido de https://www.ramonmillan.com/documentos/mpls.pdf

Parra, J. F. (1996). *DISEÑO E IMPLEMENTACIÓN DE REDES FRAME RELAY Y.* Obtenido de https://repositorio.tec.mx/bitstream/handle/11285/628635/CEM337086.pdf?sequence=1

Prashant Garimella, Y.-W. E. (s.f.). *Characterizing VLAN usage in an Operational Network.* Obtenido de https://dl.acm.org/doi/pdf/10.1145/1321753.1321772

RFC1661. (1994). *The Point-to-Point Protocol (PPP).* Obtenido de https://dl.acm.org/doi/pdf/10.17487/RFC1661

RFC2328. (1998). *OSPF Version 2*. Obtenido de https://dl.acm.org/doi/pdf/10.17487/RFC2328

RFC2684. (s.f.). *Multiprotocol Encapsulation over ATM Adaptation Layer 5.* Obtenido de https://www.rfc-editor.org/rfc/rfc2684

rfc2702. (1999). *Requirements for Traffic Engineering Over MPLS.* Obtenido de https://datatracker.ietf.org/doc/html/rfc2702

RFC2784. (Marzo de 2000). *Generic Routing Encapsulation* . Obtenido de https://dl.acm.org/doi/pdf/10.17487/RFC2784

RFC4271, IETF. (2006). *BGP*. Obtenido de https://datatracker.ietf.org/doc/html/rfc4271#page-90

RFC4762 -IETF. (2007). *Virtual Private LAN Service over LDP*. Obtenido de VPLS: https://datatracker.ietf.org/doc/html/rfc4762

RFC6812. (2013). *Cisco Service-Level Assurance Protocol.* Obtenido de https://datatracker.ietf.org/doc/html/rfc6812

RFC7436. (2015). *IP-Only LAN Service (IPLS).* Obtenido de https://datatracker.ietf.org/doc/html/rfc7436

Rico Bautista, D. W., Medina Cárdenas, Y. C., & Santos Jaimes, L. M. (Septiembre de 2008). *IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA.* Obtenido de https://www.redalyc.org/pdf/849/84920503057.pdf

SCI. (s.f.). *El protocolo IP.* Obtenido de https://www.sci.uma.es/wwwscidoc/ip.pdf

Tapasco, G. M. (2008). *MPLS, El presente de las redes IP.* Obtenido de https://core.ac.uk/download/pdf/71395663.pdf#:~:text=FEC%3A%20%28%E2%80%9CForwarding%20equivalence%20Class%E2%80%9D%2C%20Clase%20de%20Env%C3%ADo%20Equivalente%29.,que%20sean%20paquetes%20de%20distinto%20tipo%20de%20tr%C3%A1fico.

Tapia, X. E. (Diciembre de 2016). *Universidad Politecnica Saleciana (UPS).* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/13702/1/UPS%20-%20ST002950.pdf

Tejedor, R. J. (2002). *Integración de redes ópticas e IP con GMPLS.* Obtenido de https://www.ramonmillan.com/tutoriales/gmpls.php

TyN Magazine.(Agosto de 2019). *MEF publica el primer estándar SD-WAN de la industria.* Obtenido de https://www.tynmagazine.com/mef-publica-el-primer-estandar-sd-wan-de-la-industria/

Tori, G. (12 de 08 de 2020). *Blog Cisco Latinoamérica*. Obtenido de Cico: https://gblogs.cisco.com/la/por-que-sd-wan-4-factores-a-considerar-para-la-evolucion-de-su-red-de-sucursal/

UIT-T, T-REC-V.42. (s.f.). *DATA COMMUNICATION OVER THE TELEPHONE NETWORK* . Obtenido de https://www.itu.int/rec/T-REC-V.42-199303-S/es

vmware. (s.f.). *La tecnología MPLS: un breve análisis*. Obtenido de https://www.vmware.com/mx/solutions/sd-wan/mpls.html#:~:text=Seg%C3%BAn%20la%20definici%C3%B3n%20de%20IETF%20RFC%203031%2C%20MPLS,la%20red%20MPLS%20elimina%20de%20nuevo%20la%20etiqueta.

X.25, U.-T. (s.f). *SERIE X: REDES DE DATOS Y COMUNICACIÓN.* Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.25-199610-I!!PDF-S&type=items