Análisis de factibilidad técnica y económica para la implementación de Sdwan considerando su eficiencia operacional frente al servicio de Mpls en la empresa Puntonet

Arévalo García, Ricardo Xavier

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Maestría en Gerencia de Sistemas

Trabajo de titulación, previo a la obtención del título de Magíster en Gerencia de sistemas

Msc. Campaña Ortega, Eduardo Mauricio

10 de diciembre del 2020

URKUND

Document Information

Analyzed document	Tesis Ricardo Arévalo..pdf (D93582393)
Submitted	1/25/2021 11:40:00 PM
Submitted by	CAMPAÑA ORTEGA EDUARDO MAURICIO
Submitter email	emcampania@espe.edu.ec
Similarity	6%
Analysis address	emcampania.espe@analysis.urkund.com

EDUARDO MAURICIO
CAMPAÑA ORTEGA

Firma

Msc. Campaña Ortega, Eduardo Mauricio
C.C.: 1708856701

VICERRECTORADO DE INVESTIGACIÓN,
INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA
CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Análisis de factibilidad técnica y económica para la implementación de Sdwan considerando su eficiencia operacional frente al servicio de Mpls en la empresa Puntonet",** fue realizado por el señor **Arévalo García, Ricardo Xavier** 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 las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 16 de Noviembre del 2020

Msc. Campaña Ortega, Eduardo Mauricio
C.C.: 1708856701

VICERRECTORADO DE INVESTIGACIÓN,

INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Yo, **Arévalo García, Ricardo Xavier** con cédula de ciudadanía n° 1720736477 declaro que el contenido, ideas y criterios del trabajo de titulación: **Análisis de factibilidad técnica y económica para la implementación de Sdwan considerando su eficiencia operacional frente al servicio de Mpls en la empresa Puntonet",** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolqui, 16 de Noviembre de 2020

Firma

.....

Arévalo García, Ricardo Xavier
C.C.: 1720736477

VICERRECTORADO DE INVESTIGACIÓN,
INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA
CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Yo, **Arévalo García, Ricardo Xavier,** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: "**Análisis de factibilidad técnica y económica para la implementación de Sdwan considerando su eficiencia operacional frente al servicio de Mpls en la empresa Puntonet",** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 16 de Noviembre del 2020

Firma

.....

Arévalo García, Ricardo Xavier
C.C.: 1720736477

DEDICATORIA

A mis Padres Jaime Arévalo y Esther García quien con su guía, apoyo y amor me incentivaron para nunca rendirme, luchar por mis sueños, ser perseverante, siempre poniendo todo en manos de Dios, y con su ejemplo he ido superándome cada día.

A mis Hermas Liveth Arévalo y Gissel Arévalo que siempre me han animado en todo momento.

Ricardo Xavier Arévalo García

AGRADECIMIENTO

Agradezco a mis Padres quien siempre han estado a mi lado apoyándome y motivándome para nunca rendirme frente a una adversidad y a mi tutor de tesis Msc.Mauricio Campaña quien me ha orientado para el desarrollo del presente proyecto.

Ricardo Xavier Arévalo García

Tabla de contenidos

Agradecimiento 7
Índice de tablas 11
Índice de figuras 11
Abstract 14
Capítulo 1 15
Antecedentes 15
Planteamiento del problema 17
Justificación 18
Objetivos 19
Objetivo Generales 19
Objetivos específicos 19
Hipótesis de investigación 19
Marco teórico referencial 20
Capitulo II. Análisis de la red MPLS y SDWAN 22
Introducción 22
Arquitectura MPLS 23
LER (Label Edge Router), Enrutador de borde, de entrada o salida 23
LSR (Label Switch Router), Enrutador de conmutación de etiquetas 24
LSP (Label Switched Path), Ruta de cambio de etiqueta 24
Componentes de la arquitectura MPLS 24
Plano de Control 24
Plano de Datos 25
Etiquetas MPLS 26
Funcionamiento de una red MPLS 28
Protocolos principales en MPLS 29
Aplicaciones MPLS 32
Calidad de Servicio (QoS) 32
Ingeniería de tráfico 32
Beneficios de MPLS en ingeniería de tráfico (TE) 33
Limitaciones de la ingeniería de tráfico 35
VPN……. 36
Enrutamiento VPN MPLS 37
SDWAN 38
Funcionamiento de SD-WAN 40
Beneficios de SD-WAN 40
Seguridad en SD-WAN 41

Características de SD-WAN..... 42
Estructura actual de la red MPLS en Puntonet 44
Equipos perimetrales de una red MPLS..... 48
Enrutadores 49
Switch……..... 54
Firewall…..... 55
Palo Ato……..... 57
Fortinet…….. 58
Check Point 59
Elección del proveedor de seguridad perimetral 60
Requerimientos para la implementación de SDWAN en Puntonet..... 61
SD-WAN Edge..... 62
Controlador SD-WAN..... 63
SD-WAN Gateway 63
Orquestador de servicios 63
Portal Web de suscripción 64
Diseño de red SDWAN..... 64
Elección del proveedor de SD-WAN 65
VMware 66
Silver Peak 66
Fortinet 67
Cisco 68
Meraki 69
Viptela……..... 69
Capitulo III. Comparación entre SDWAN Y MPLS 71
Configuración de SD-WAN en Cisco Meraki..... 71
Direccionamiento IP..... 73
Selección de la capa de acceso y direccionamiento LAN 73
Balanceo de Carga 75
Traffic Shaping 76
Políticas de tráfico 77
VPN tipo Hub..... 78
Firewall... 79
Configuraciones en MPS..... 80
Configuraciones en el CE 80
Configuración en el PE 82
Ventajas 83
Desventajas..... 83
Factibilidad de implementación de SDWAN en Puntonet..... 84

Análisis Financiero operacional de la red SDWAN en Puntonet *85*
Factibilidad financiera *85*
Tir……..... *87*
Van…. *88*
Resultados *88*
Capítulo V..... *94*
Conclusiones..... *94*
Recomendaciones..... *95*
Referencias..... *96*

Índice de tablas

Tabla 1. Características del router Cisco ASR-920 49
Tabla 2. Características del router Cisco ASR-9010 51
Tabla 3. Características del router Cisco NCS-5001 52
Tabla 4. Comparación de firewalls aplicados a ISPs 60
Tabla 5. Tabla comparativa según posicionamiento de Gartner 65
Tabla 6. Tabla comparativa entre Cisco Sdwan, Meraki y Viptela 70
Tabla 7. Tabla comparativa entre Sdwan y Mpls 84
Tabla 8. Costo de implementar Sdwan 86
Tabla 9. Costo de implementar Mpls 86
Tabla 10. Ingresos anuales 87
Tabla 11. Cálculo del Jitter 89

Índice de figuras

Figura 1. Elementos de una red Mpls 23
Figura 2. Esquema del plano de control 25
Figura 3. Esquema del plano de datos 26
Figura 4. Etiqueta Mpls 27
Figura 5.Comparación entre IGP con ingeniería de tráfico 33
Figura 6. Esquema Mpls con Vpn 37
Figura 7. Esquema de Sdwan accediendo a la nube 39
Figura 8. Esquema de Mpls accediendo a la nube 39
Figura 9. Esquema de la red Mpls 46
Figura 10. Esquema de seguridad con redundancia 48
Figura 11. Router ASR920 49
Figura 12. Router ASR9010 50
Figura 13. Router NCS-5001 52
Figura 14. Router 76706-S 53
Figura 15. Switch ME-3600X 54
Figura 16. Cuadrante de Gartner en Firewalls 56
Figura 17. Firewall de Palo Alto 58

Figura 18. Firewall de Fortinet *59*
Figura 19. Firewall de CheckPoint 26000 ..... *59*
Figura 20. Componentes de una red Sdwan *62*
Figura 21.Tendencias de Infraestructura Sdwan *64*
Figura 22. Arquitectura de VMware Sdwan *66*
Figura 23. Arquitectura de Silver Peak Sdwan..... *67*
Figura 24. Arquitectura de Fortinet Sdwan *68*
Figura 25. Cisco Meraki Mr33..... *72*
Figura 26. Ubicación de redes en Sdwan *72*
Figura 27. Dirección MACs de los equipos en cada sede..... *73*
Figura 28. Direccionamiento IP *73*
Figura 29. Selección del modo de trabajo de Meraki *74*
Figura 30. Configuración de la LAN..... *74*
Figura 31. Monitoreo de las aplicaciones..... *75*
Figura 32. Habilitación del balanceador..... *76*
Figura 33. Traffic Shapping *77*
Figura 34. Políticas de tráfico *77*
Figura 35. Definición de reglas..... *78*
Figura 36. Tipo de Vpn..... *79*
Figura 37. Redes aprendidas *79*
Figura 38. Control de reglas Firewall..... *80*
Figura 39. Monitoreo del tráfico *90*
Figura 40. Prueba de latencia Sdwan..... *90*
Figura 41. Información de estado de la red *91*
Figura 42. Throughput..... *91*
Figura 43. Detección de Amenazas frecuentes *92*
Figura 44. Filtrado de aplicaciones..... *92*

Resumen

En el presente proyecto se ha realizado un análisis técnico, económico y de viabilidad para la implementación de la tecnología SD-WAN en la empresa Puntonet, considerando su arquitectura por medio de MPLS con la arquitectura que se tendría en base a SD-WAN.

Este análisis comprende una descripción de los requerimientos y componentes que son necesarios para la implementación de SD-WAN, comparados con los que se requiere para la red tradicional de MPLS, describiendo además los protocolos de red que intervienen, sus características y la optimización de las aplicaciones de una tecnología frente a la otra.

Para el diseño de la red SD-WAN, se menciona los equipos necesarios para su funcionamiento, realizando una comparación con MPLS, en la cual se observa la tecnología más adecuada y rápida para la implementación en cualquier ambiente.

Además, en el estudio se hace un análisis de los proveedores que cumplen con los requerimientos de SD-WAN, para luego evaluar económicamente si es factible o no dar el servicio de SD-WAN a futuros clientes que busquen incorporar esta tecnología en sus empresas.

- Palabras Clave:
    - **REDES HIBRIDAS**
    - **RED DEFINIDA POR SOFTWARE SD-WAN**
    - **TOPOLOGÍA DE RED**
    - **DISEÑO DE SD-WAN**
    - **MPLS**

Abstract

In this project, I have carried out a technical, economic and feasibility analysis for the implementation of SD-WAN technology in the Puntonet company, considering its architecture through MPLS with the architecture that should be based on SD-WAN.

The analysis describes the requirements and components that are necessary for the implementation of SD-WAN, compared with those required for the traditional MPLS network, also describing the network protocols involved, their characteristics and the optimization of the applications. of one technology versus the other.

For the design of the SD-WAN network, mention is made of the equipment necessary for its operation, as well as a comparison with MPLS, in which it is observed which technology is more efficient and faster for its implementation in any environment.

In addition, the study makes an analysis of the providers that comply with the SD-WAN requirements, to later evaluate economically whether or not it is feasible to provide the SD-WAN service to future customers who seek to incorporate this technology into their companies.

- Keywords:
    - **HYBRID NETWORKS**
    - **SD-WAN SOFTWARE DEFINED NETWORK**
    - **NETWORK TOPOLOGY**
    - **SD-WAN DESIGN**
    - **MPLS**

Capítulo 1

Antecedentes

De acuerdo al reporte sobre tendencias globales en redes de CISCO (Cisco, 2020), el mundo actual se ha vuelto más diverso y digitalizado, anhelando una tecnología con un mejor rendimiento y desempeño, lo que ha impulsado el crecimiento continuo de la red. Para el año 2023 se pronostica que 48.900 millones de dispositivos estarán conectados al internet en el mundo(IDC, 2019), con un consumo promedio de datos de 60GB por computador al mes(Cisco, 2018b), lo que demanda a las grandes empresas de telecomunicaciones, buscar alternativas para incrementar su capacidad de respuesta ante el continuo crecimiento tecnológico, y a la vez, ofrecer soluciones de interconexiones más óptimas.

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

Para el año 2023, más del 60% de las empresas a nivel mundial, según Gartner, prevén el uso del networking como un rol estratégico en el giro de sus negocios(Dennis Smith, Mayo 2019), siendo de vital importancia la asignación de recursos para el área de TI.

El tiempo es un factor muy importante, especialmente cuando el rol de negocios de una empresa es por medio del acceso al internet. TI debe garantizar que la red esté disponible todo el tiempo a más de que la información llegue y sea entregada oportunamente manteniendo su confiabilidad y confidencialidad. SD-WAN cumple los requisitos, cuando un enlace no está disponible, se puede enviar todo el tráfico a

través de otra red o ISP e incluso a través de una red de hogar de forma automática, permitiendo cumplir con las necesidades de las empresas(Naggi & Srivastava, 2018). En la actualidad, los aplicativos están siendo desarrollados para montarlos en la nube, lo cual permite el acceso desde cualquier parte del mundo; la comunidad científica indica que mediante SD-WAN se logrará tener una red más confiable que la tradicional por mpls.(Wood, 2017)

Un análisis técnico y económico de SD-WAN y MPLS, permitirá tener una mejor visión y selección de la tecnología aplicable a un proyecto de telecomunicaciones, para el aumento de la productividad de la empresa, así como también, aportando al administrador de red, una guía para determinar si renueva su tecnología de red tradicional MPLS por la actual SD-WAN.

El volumen de información que se maneja en la actualidad es mucho mayor al que se disponía hace 10 años, debido al creciente consumo de datos provenientes de diferentes equipos tecnológicos conectados al internet.

El consultor especializado en Big data Bernard Marr, estima que cada persona para el 2020 cada persona utilizará 1.7 megabyte de información por segundo, debido a que no solo generará tráfico mediante el uso del celular, sino mediante la televisión por internet, netflix, equipos de domótica, llamadas a través del internet, entre otras. Toda esta información circulando por la red demanda que nuevas tecnologías y soluciones permitan garantizar la seguridad no solo en redes corporativas sino también en redes privadas del hogar.

SD-WAN nace como solución a la problemática de una infraestructura decadente, que no brinda una fácil visibilidad de las aplicaciones en tiempo real, además por la deficiente experiencia que tiene el usuario al navegar en la internet por

medio de una conexión baja, alta latencia que resume en pérdida de tiempo y en consecuencia pérdida de dinero por el tiempo de espera.

La administración de redes WAN ha sido uno de los factores más caros en una empresa, pero con el avance tecnológico ha evolucionado en redes basadas en SD-WAN que simplifican el trabajo en su administración, realizando un análisis de forma automática para elección de la mejor vía, mejor ruta, con lo cual se gestiona de mejor manera el rendimiento de la red por medio de su capa de software que maximiza la calidad y aseguramiento de la información.(Marr.B, 2019)

Gartner señala que, a partir del 2020, el mercado de SD-WAN va atravesar un crecimiento exponencial del 76,2%, hasta alcanzar los 1.240 millones de dólares. Gartner estima que, para el año 2020, más del 50% de las iniciativas de actualización de las infraestructuras perimetrales de las redes wan estarán basadas en tecnología sd-wan y no en routers tradicionales, frente a la cifra actual, inferior al 2%. (Gordeychik & Kolegov, 2018)

Planteamiento del problema

La constante evolución a nivel global y la necesidad de disponer de conexiones de internet mucho más rápidas y con mayor ancho de banda, ha hecho que se busquen nuevas soluciones tecnológicas. Las redes SDWAN surgen de esa necesidad, pero se requiere conocer si tanto técnicamente como económicamente es rentable o no frente a las redes tradiciones de mpls.

Muchas empresas a nivel global no incorporan la red SDWAN, debido a la incertidumbre y desconocimiento de esta nueva tecnología sin saber los beneficios que obtendrían al implementarla.

El creciente desempleo y la falta de liquidez ha hecho que muchas empresas en Quito sean liquidadas, día a día negocios buscan la manera de cómo ahorrar dinero, pero a la vez demandan más el uso de internet, SDWAN plantea una alternativa al no requerir equipos costosos ni estar ligados a enlaces empresariales de gran valor económico.

Puntonet al dar servicio de internet, debe estar a la vanguardia tecnológica y la satisfacción del cliente, al dar un servicio más eficiente y a la vez más económico, lo cual permitiría obtener una mayor captación de clientes, por tal motivo se requiere conocer cuáles son las ventajas económicas y su rentabilidad al brindar al cliente tecnología SDWAN, como también ver la rentabilidad que obtendrá Puntonet al incorporar esta tecnología.

Justificación

Puntonet, como empresa de Telecomunicaciones está buscando constantemente mejorar el servicio que brinda al cliente, es por eso que requiere el desarrollo tecnológico mejorando su infraestructura, con el fin de brindar al cliente una alternativa de ahorro con SDWAN, e incidir positivamente en la liquidez que presentan varias de empresas que se han visto en la necesidad de reducir sus gastos, por el uso de tecnologías de telecomunicaciones más costosas.

Se realizará un análisis técnico y económico que permitirá conocer si es rentable o no para el cliente y para la empresa el implementar SDWAN frente a la infraestructura tradicional MPLS.

Mediante el estudio planteado, se pretende dar un aporte a los administradores de red o a nivel de gerencia de una empresa de Ecuador, para la toma de decisión en compatibilidad de infraestructura de SDWAN.

Objetivos

Objetivo Generales

Determinar la viabilidad técnica y económica del servicio de red SDWAN tanto para el proveedor como para el cliente final, en comparación con el servicio de red tradicional MPLS.

Objetivos específicos

- Analizar las ventajas y desventajas que Puntonet obtendrá al brindar el servicio de red SDWAN.
- Analizar las ventajas de rendimiento, velocidad, ancho de banda, de SDWAN frente a la red MPLS.
- Analizar el beneficio económico en la implementación del servicio de SDWAN tanto para el cliente como para el ISP.

Hipótesis de investigación

- Con SDWAN los tiempos de respuesta bajarían al no tener circuitos mpls de por medio, asignando la mejor ruta y SDWAN no requiere de equipos intermedios como un router, por lo que no se necesita el mantenimiento y administración de esos equipos.

- Se tiene un beneficio económico y técnico, teniendo una mayor velocidad, optimización del ancho de banda, monitoreo centralizado, mayor seguridad.

- Como proveedor de SDWAN, Puntonet, lograría captar más clientes empresariales que busquen mejorar su servicio en cuanto a rendimiento, costo, seguridad.

- La calidad de servicio en SDWAN al trabajar a nivel de túneles IPSEC de extremo a extremo.

Marco teórico referencial

De acuerdo a un estudio relacionado de Kable Global ICT Customer Insight, en los próximos dos años un 58,5 % de las empresas de todo el mundo planearán adoptar la tecnología SD-WAN. A su vez, se prevé que los ingresos globales de SD-WAN van a superar los US$ 6 mil millones en 2020, con una tasa de crecimiento anual superior al 90%. (Bau, 2016)

Según el estudio realizado por la empresa Española IDC, en España el mercado SD-WAN llegará a los 288 millones de euros entre 2018-2022 con un crecimiento del 60% (CAGR) entre 2016 - 2022. (Castellote, 2018)

SD-WAN estimula el crecimiento comercial, proporcionando una automatización y mayor eficiencia en aplicaciones basadas en la nube.

Según el estudio de mercado realizado por Emilio Castellote, las compañías están cambiando su manera de hacer negocio, incluyéndose en la era tecnológica de (movilidad, Big Data y redes sociales), con el fin de mejorar su competitividad frente a un mercado tan exigente.(Castellote, 2018)

La enorme ventaja que aporta la SD-WAN es la posibilidad de consolidar en una única infraestructura todos sus recursos, tanto antiguos como nuevos, y de extender el control sobre todos ellos hasta la periferia de la red, por medio de técnicas como el enrutado con subdivisión de rutas o el control dinámico de rutas; la SD-WAN permite unificar en un único dominio común varias wan diferentes.

En la actualidad, las organizaciones se encuentran en un proceso de transformación digital, que afecta a las redes WAN en dos aspectos diferentes, ya que es evidente que las redes son el sistema nervioso de cualquier organización. En primer lugar, por el distanciamiento geográfico que exige que las empresas busquen alternativas que permitan interconectar sus puntos entre diferentes localidades o países. En segundo lugar, el modo de acceso a la información y a las aplicaciones que cada vez pasa más por el acceso a servicios de terceros que se prestan desde la nube, a la que acceden de forma directa todas las oficinas, por lo que el tráfico corporativo deja de ser estrella como ha venido siendo tradicionalmente, y los enlaces corporativos dejan de tener sentido. Este contexto provoca que la arquitectura WAN tradicional se quede obsoleta frente a un nuevo modelo más ágil y menos costoso.(Teldat, 2017)

Capitulo II. Análisis de la red MPLS y SDWAN

Introducción

La red MPLS es una tecnología mayormente implementada en isps a nivel mundial, debido a la capacidad de enrutamiento ip, convergencia y escalabilidad de la red, lo que permite transportar distintos tipos de paquetes, como datos o voz, con la posibilidad de utilizar calidad de servicio.

MPLS está ubicado entre la capa de enlace y red del modelo OSI, nació con el objetivo de llevar datos a alta velocidad y voz en una misma conexión, proporcionando fiabilidad y mayor rendimiento en la comunicación, lo que hace una solución idónea para centrales telefónicas VoIP porque permite priorizar el tráfico de voz, además que soporta múltiples protocolos de enrutamiento.

La tecnología MPLS utiliza etiquetas para el reenvío de paquetes, de esta forma se diferencia de un paquete al de otro paquete, cuando al ingresar al dominio, las etiquetas son añadidas y este es reenviado dentro del dominio MPLS, generalmente las etiquetes son añadidas de acuerdo a las direcciones de destino de capa 3, dirección fuente, etc. (Garcia, Nossa, & Telemática)

La etiqueta que se agrega a la entrada, se la usa como un distintivo que permite la elección de una etiqueta de salida identificando al dispositivo que será el próximo salto, estas etiquetas que son examinadas y comparadas en la base de datos son almacenadas.

Arquitectura MPLS

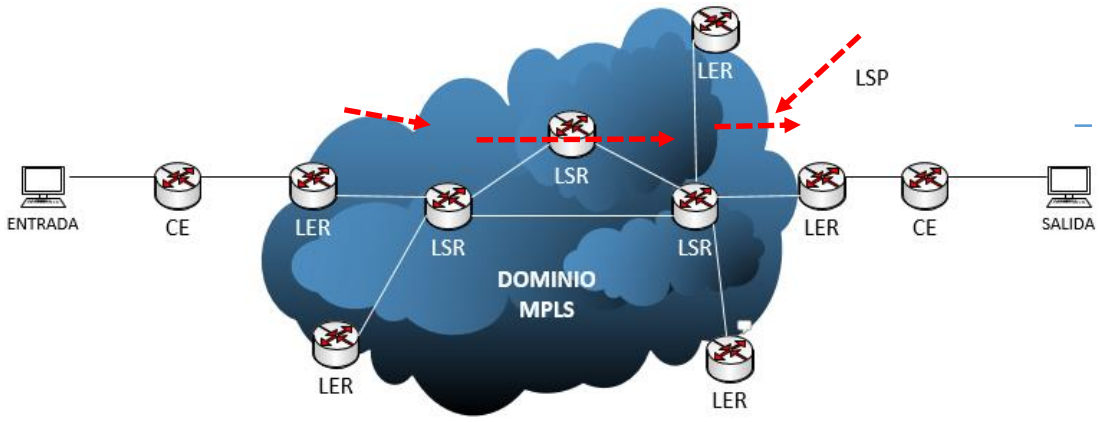
La arquitectura MPLS está comprendida de 3 elementos fundamentales que deben ser incluidos para su diseño, el primero es el enrutador de conmutación de etiquetas “LSR”, trayectoria de conmutación de etiquetas “LSP” y paquetes etiquetados “LP”. Un sistema simple de MPLS se podría decir que es un conjunto de LSR que realizan el envío de paquetes etiquetados a través de los LSP.

La red MPLS está compuesta por dos nodos principales, el enrutador de etiquetas de border ”LER” y enrutador de conmutación de etiquetas “LSR”, estos dos son físicamente un mismo dispositivo, un switch o un router de red troncal, el administrador realiza la configuración para elegir el modo de trabajo. (Jiménez Vázquez, 2010)

En la figura 1 se puede observar cómo es la estructura de una red MPLS, con sus principales elementos.

Figura 1

Elementos de una red MPLS



LER (Label Edge Router), Enrutador de borde, de entrada o salida

Es un enrutador que funciona en los bordes de una red MPLS. Un LER determina y aplica las etiquetas apropiadas y reenvía los paquetes etiquetados al MPLS dominio. (Smith, Mullooly, Jaeger, & Scholl, 2011)

El LER determina la ruta a seguir del paquete mediante la colocación de una etiqueta y de la misma forma al salir el paquete la etiqueta es eliminada.

LSR (Label Switch Router), Enrutador de conmutación de etiquetas

El LSR es el centro de la red MPLS porque realiza el enrutamiento de los paquetes a través de rutas de conmutación de etiquetas “LSP” o rutas predeterminadas. El proceso de enrutamiento es rápido porque las etiquetas ya tienen instrucciones de qué camino seguir, sin tener que revisar en las tablas o realizar cálculos de enrutamiento. (Guichard, Pepelnjak, & Apcar, 2003)

LSP (Label Switched Path), Ruta de cambio de etiqueta

Una ruta a través de una red MPLS, definida por un protocolo de señalización como LDP o el Border Gateway Protocol (BGP). La ruta se configura según los criterios de clase de equivalencia de reenvío (FEC).(Le Faucheur et al., 2002)

Componentes de la arquitectura MPLS

La arquitectura de MPLS está conformada de dos componentes, los cuales son:

- Plano de Control
- Plano de Datos

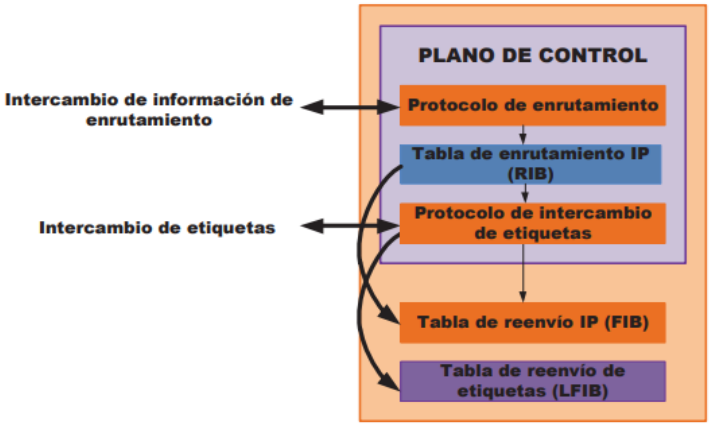
Plano de Control

Es aquel que determina la disponibilidad de acceso hacia una red destino, almacena la información de enrutamiento de la capa 3 permitiendo intercambiar información entre protocolos de enrutamiento y asigna el valor que llevan las etiquetas. Además, utiliza un protocolo de intercambio de etiquetas para crear,

mantener e intercambiar las etiquetas con otros dispositivos. Los protocolos de intercambio como LDP, TDP, BGP y RSVP, permiten que las etiquetas se unan a las redes aprendidas por medio de un protocolo de enrutamiento tal como OSPF, IGRP, IS-IS, RRIP, BGP.(Garcia et al.)

Figura 2

Esquema del plano de control



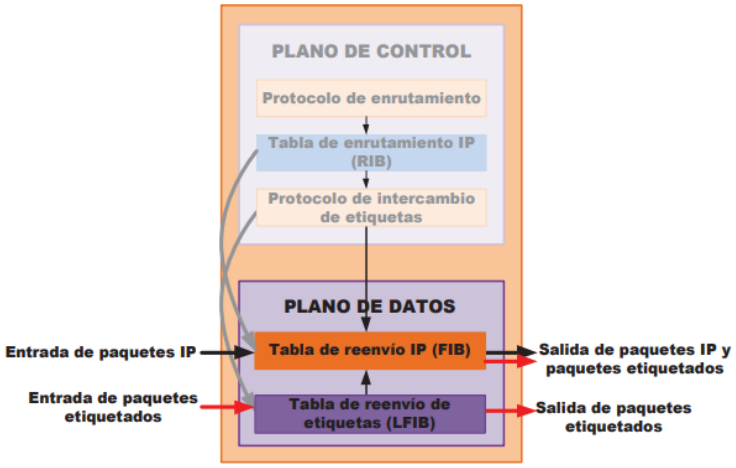
Tomado de *Oña Piña, 2016*

Plano de Datos

El plano de datos o plano de envío es el sé que encarga de conmutar los paquetes y construye las tablas de envío de etiquetas, las cuales son almacenadas en la LFIB y FIB, usando la información del plano del control para luego realizar el envío de los paquetes.(Garcia et al.)

Figura 3

Esquema del plano de datos



Tomado de *Oña Piña, 2016*

Etiquetas MPLS

La etiqueta MPLS es un identificador de 4 octetos (32 bits), longitud fija y significado local, que es utilizado para identificar la trayectoria que irá a seguir un paquete por el dominio MPLS e identifica al FEC al cual el paquete ha sido asignado.

La FEC es un conjunto de paquetes IP con características similares que pueden reenviarse de la misma manera, sobre la misma ruta; es decir, pueden estar vinculados a la misma etiqueta MPLS. Por ejemplo una FEC puede ser constituida por todo el tráfico con determinado valor de prioridad de IP.(Cisco, 2016a)

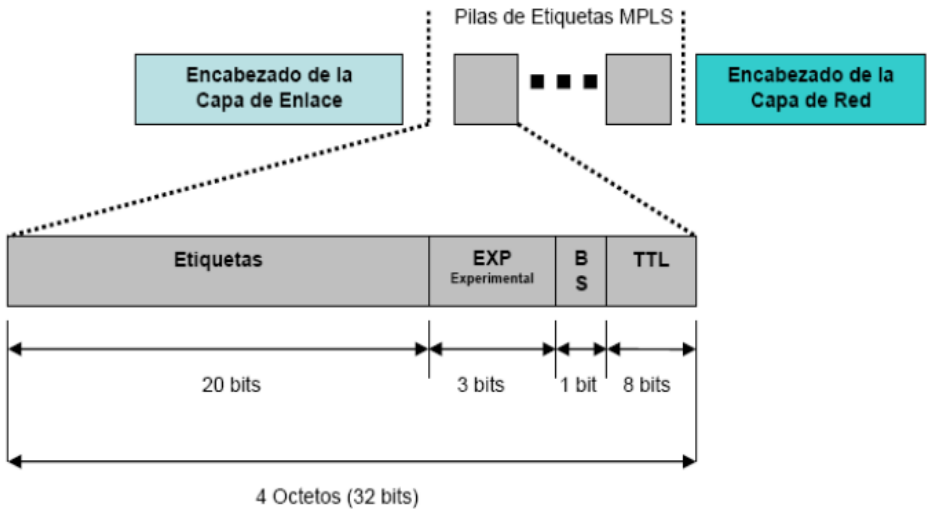
Las etiquetas especifican el destino, pero también pueden definir el nivel de servicio. Los dispositivos de frontera LSR que pertenecen en su mayoría a los ISP, agregan las etiquetes a los paquetes.

Una de las características que poseen las etiquetes MPLS es que proveen un mecanismo que permite ordenar los paquetes en varios FEC sin requerir examinar la cabecera de capa 3. En la figura 4, se describe el esquema de frame mode MPLS, el cual es un mecanismo que permite insertar la etiqueta entre la cabecera de capa 2 y

cabecera de capa 3, dicha etiqueta es utilizada por cada LSP a lo largo del camino para tomar decisiones de envío para cada paquete.

Figura 4

Etiqueta MPLS



Tomado de *Black, 2002*

- **Etiquetas:** Este campo corresponde a la Label o etiqueta de 20 bits**,** su valor puede ir desde 0 a 1048575**,** pero de 0 al 15 son valores reservados, al momento de ingresar un paquete en el dominio MPLS, una etiqueta es asignada, la cual llevará hasta el fin de su destino por medio de la red MPLS.

- **Experimental (EXP):** Es el campo que se utiliza para identificar la clase de servicio, conocidos también como bits experimentales, afecta directamente al encolado y descarte de paquetes y en consideraciones de calidad de servicio (QoS).

- **B (Bottom of Stack):** Este campo está conformado de 1 bit, agrupa etiquetas de forma jerárquica, permitiendo que múltiples etiquetas sean insertadas.

- **TTL:** Su función es evitar que se forme un bucle indefinido de paquetes, cuando atraviesa un router su valor es decrementado en 1 y al llegar a 0 es descartado el paquete. (Black, 2002)

Funcionamiento de una red MPLS

Luego de explicar cómo es la estructura de una red MPLS, ahora se mostrará cómo es su funcionamiento. Varios nodos llamados LSRs conforman un dominio, el cual está encargado de realizar la conmutación y envío de los paquetes en base a una etiqueta que ha sido añadida a cada paquete. Las etiquetas definen el camino de los paquetes entre dos puntos. Luego para cada FEC se puntualiza un camino especifico que seguirá por medio de la red de LSRs. Cuando el paquete ha llegado a un LER, examina la información entrante y asocia la calidad de servicio que requiere asignando al paquete una etiqueta. En la salida de la red MPLS, ocurre lo contrario, la etiqueta que fue agregada al inicio es removida para entregar al paquete de la misma forma en la cual fue recibido. De esta forma, los equipos ruteadores de frontera que realizan la etiquetación pueden convertir paquetes IP en paquetes MPLS y viceversa. Después de que se ha realizado la etiquetación de paquetes por el LER, dichos paquetes empiezan el viaje en la red MPLS y en el camino se encontrarán con los LSRs, los cuales tienen la función de dirigir el tráfico en el interior de la red de acuerdo con la etiqueta que ha sido asignada. Cuando un LSR recibe el paquete, este examina su etiqueta y la utiliza como un índice en una tabla propia que define el siguiente salto y asigna una nueva etiqueta, de esta manera el LSR intercambia esta etiqueta por la que contenía el paquete y lo envía hacia el siguiente ruteador. La ruta a seguir por el paquete entre dos nodos es llamada LSP. Los LSP son unidireccionales, que quiere decir que el tráfico de regreso utilizará un distinto LSP. El proceso es más rápido que otras tecnologías debido a que los LSRs no requieren examinar la cabecera IP, sino

que se basan simplemente en el valor de su etiqueta para el envío de cada paquete. (Duda, 2015)

Protocolos principales en MPLS

La arquitectura MPLS permite varios protocolos para distribuir las etiquetas entre LSRs los cuales son de enrutamiento y señalización, el uso y administración depende de cómo esté conformando la estructura del ISP.

- **Protocolo de Distribución de Etiquetas LDP**

- LDP proporciona los medios para que los LSR soliciten, distribuyan y publiquen información de enlace de prefijo de etiqueta a enrutadores pares en una red, está definido en la RFC 3036.
- LDP permite a los LSR descubrir posibles pares y establecer sesiones de LDP con esos pares con el fin de intercambiar información de enlace de etiquetas.
- También permite que un LSR informe a otro LSR de los enlaces de etiquetas que ha realizado. Una vez que un par de enrutadores comunican los parámetros LDP, establecen una ruta de cambio de etiqueta (LSP). permite que los LSR distribuyan etiquetas a lo largo de rutas normalmente enrutadas para admitir el reenvío de MPLS. Este método de distribución de etiquetas también se denomina reenvío salto por salto. Con el reenvío de IP, cuando un paquete llega a un enrutador, el enrutador busca la dirección de destino en el encabezado de IP, realiza una búsqueda de ruta y reenvía el paquete al siguiente salto. Con el reenvío de MPLS, cuando un paquete llega a un enrutador, el enrutador mira la etiqueta entrante, busca la etiqueta en una tabla y luego reenvía el paquete al siguiente salto. Este protocolo es útil para

aplicaciones que requieren reenvío salto por salto, como las VPN MPLS. (Cisco, 2008)

- **Protocolo de compuerta Interior IGP**

Se utiliza para enrutar dentro de un sistema autónomo (AS), el cual intercambia información de enrutamiento entre routers. También se lo describe como enrutamiento intra-AS. Las empresas, organizaciones e incluso proveedores de servicios usan un IGP en sus redes internas. Los IGP incluyen RIP, EIGRP, OSPF e IS-IS. Este protocolo calcula la ruta más corta.(Cisco, 2014b)

- **Protocolo de reservación de recursos (RSVP)**

Es un protocolo que especifica requerimientos de anchos de banda, su función es indicar los requerimientos de calidad de servicio QoS que demanda una aplicación, su particularidad es que funciona sobre cualquier protocolo de enrutamiento. (Cisco, 2016b)

- **Protocolo de Distribución de Etiquetas con Ruta Restringida (CR-LDP)**

Permite incrementar las funcionalidades de LDP, lo cual hace factible la configuración de trayectoria mucho más de lo que permiten los protocolos de enrutamiento. (Xiao, Hannan, Bailey, & Ni, 2000)

- **Protocolo de Reservación de Recursos con Ingeniería de Tráfico (RSVP-TE)**

Se utiliza para establecer los LSP de transporte MPLS cuando existen requisitos de ingeniería de tráfico. Se utiliza principalmente para proporcionar QoS y equilibrio de carga en el núcleo de la red.

RSVP permite el uso de enrutamiento de origen donde el enrutador de ingreso determina la ruta completa a través de la red. El enrutador de ingreso puede calcular primero la ruta más corta restringida (CSPF) para determinar una ruta hacia el destino, asegurando que se cumplan los requisitos de QoS. La ruta resultante se utiliza para establecer el LSP.(Networks, 2020b)

- **Protocolo de sistema intermedio (IS-IS)**

Es un protocolo de enrutamiento IP, su función es enviar información del enrutamiento IP por medio de un solo Sistema Autónomo (AS), intercambiando información de la topología con los vecinos más cercanos.(Networks, 2020a)

- **Protocolo de ruta más corta (OSPF)**

Está definido en RFC 2328, es un protocolo de puerta de enlace interior utilizado para distribuir información de enrutamiento dentro de un único sistema autónomo, comúnmente utilizado en grandes redes empresariales. Su característica es que tiene una convergencia rápida con un alto grado de escalabilidad, haciendo un uso eficaz del ancho de banda.

Si hay varios enrutadores en una red, OSPF crea una tabla (o topografía) de las conexiones del enrutador. Cuando los datos se envían de una ubicación a otra, el algoritmo OSPF compara las opciones disponibles y elige la forma más eficiente de enviar los datos. Esto limita retrasos innecesarios en la transmisión de datos y evita bucles infinitos. (Murphy & Badger, 1996)

Aplicaciones MPLS

MPLS presenta varias aplicaciones, entre las cuales se tiene:

- Calidad de Servicio (QoS)
- Ingeniería de tráfico
- VPN

Calidad de Servicio (QoS)

La calidad de servicio QoS, permite delimitar cierto ancho de banda para diferentes aplicaciones que requieran un mayor ancho de banda o una mejor ruta, como por ejemplo la voz y el video que son muy susceptibles a variaciones y requieren un tratamiento especial, por lo que mediante QoS se garantiza que el servicio no se verá afectado por el uso constante de la red.

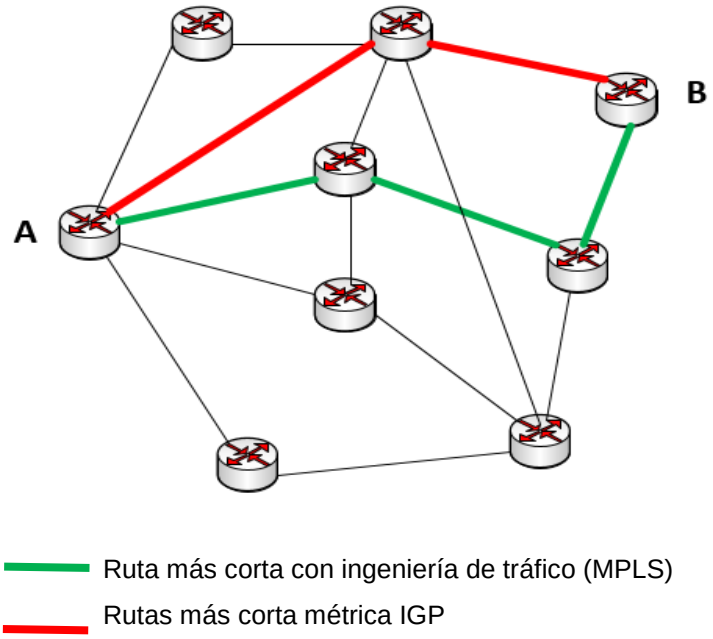
Ingeniería de tráfico

La ingeniería de tráfico se refiere al proceso de selección de rutas LS elegidas por el tráfico de datos para equilibrar la carga en varios enlaces, enrutadores y

conmutadores en la red. Esto es más importante en redes donde hay múltiples rutas paralelas o alternativas disponibles. El objetivo de Traffic Engineering es facilitar operaciones de red IP eficientes y confiables al tiempo que optimiza la utilización de recursos y el rendimiento de la red.

Figura 5

Comparación entre IGP con ingeniería de tráfico



Beneficios de MPLS en ingeniería de tráfico (TE)

La ingeniería de tráfico en MPLS implica la técnica de dirigir el tráfico que fluye dentro de una red. Varios procedimientos de enrutamiento implementan el reenvío de paquetes para una transmisión segura. Las siguientes ventajas mejoran la ingeniería de tráfico:

- **Minimiza la congestión de la red:** una red MPLS puede implementar TE para reducir el bloqueo de la red y aumentar el rendimiento. Todas las técnicas de enrutamiento en uso se modifican para asignar datos de paquetes a recursos de red. Tal proceso de mapeo puede manejar cuellos de botella de hacinamiento de paquetes con supresión de latencia, fluctuación de fase y factores de pérdida. MPLS TE permite la explotación del ancho de banda en uso en lugar de asignar nuevo ancho de banda para operar la ingeniería de tráfico. Los túneles dirigen el tráfico desde la ruta congestionada a la ruta subutilizada disponible para aliviar la congestión del tráfico.

- **MPLS Fast Reroute para falla de enlace / nodo:** la funcionalidad MPLS Fast Reroute maneja fallas de enlace o nodo al dirigir el tráfico encapsulado a una ruta secundaria preconfigurada cuando falla la primaria. Esto no es posible en el caso de redes IP, ya que el mecanismo de redireccionamiento no es aplicable aquí. Lo más destacado es que MPLS asegura la más alta confiabilidad y tiempo de actividad de la red con mecanismos apropiados para recuperarse de la congestión de la red y otros cuellos de botella.

- **Flexibilidad de implementación:** un sistema TE es eficiente incluso cuando la implementación de la red MPLS está subdesarrollada. Cualquier combinación de circuitos con T1, T3, portadores ópticos o Ethernet se puede asimilar en una configuración MPLS. Las oficinas con múltiples sucursales en todo el mundo aprovechan al máximo esta flexibilidad de implementación con diferentes combinaciones de conexiones. Es flexible durante situaciones en las que los paquetes desbordados de los enlaces se transfieren a los enlaces disponibles. Los túneles MPLS también pueden implementar ingeniería de tráfico sin LDP.

- **Clase de servicio (CoS):** este campo de 3 bits determina el valor de CoS, en función del cual se utiliza el tráfico en su cola de prioridad para la transmisión. En el borde de ingreso, el paquete IP que llega se marca con el valor CoS y se codifican para referencia en el encabezado MPLS. Esto proporciona una transmisión rápida de paquetes entre nodos para evitar la congestión de la red. Las funciones de CoS son la tasa de acceso comprometida (CAR), la detección temprana aleatoria ponderada (WRED) y la cola equitativa ponderada (WFQ). Cada clase de servicio implementa la ingeniería de tráfico clasificando el tráfico en función del ancho de banda disponible en los enlaces, gestiona el desbordamiento de paquetes en los enrutadores de borde, la probabilidad de caída y el control del tráfico de red utilizando algoritmos (como round-robin).

- **Identificación del tráfico del cliente:** la ingeniería de tráfico MPLS clasifica el tráfico del cliente en función del proveedor de servicios utilizado en la red MPLS. Esto se debe únicamente a la función CoS de la tecnología que realiza la categorización del tráfico.(solutions, 2020)

Limitaciones de la ingeniería de tráfico

Entre las limitaciones de ingeniería de tráfico, se tiene:

- **Uso excesivo de enlaces secundarios:** en los casos de fallas de enlaces, Fast Reroute de MPLS TE utiliza túneles de respaldo para redirigir el tráfico a través del enlace secundario. Si bien esta es una configuración para la recuperación, el rendimiento se completa solo si esos túneles comprenden suficiente ancho de banda. Un nivel satisfactorio de capacidad libre es necesario para un buen funcionamiento. A pesar de este método de respaldo,

las fallas frecuentes de los nodos de la red conducirán a una congestión de tráfico constante en rutas alternativas, reduciendo su eficiencia en general.

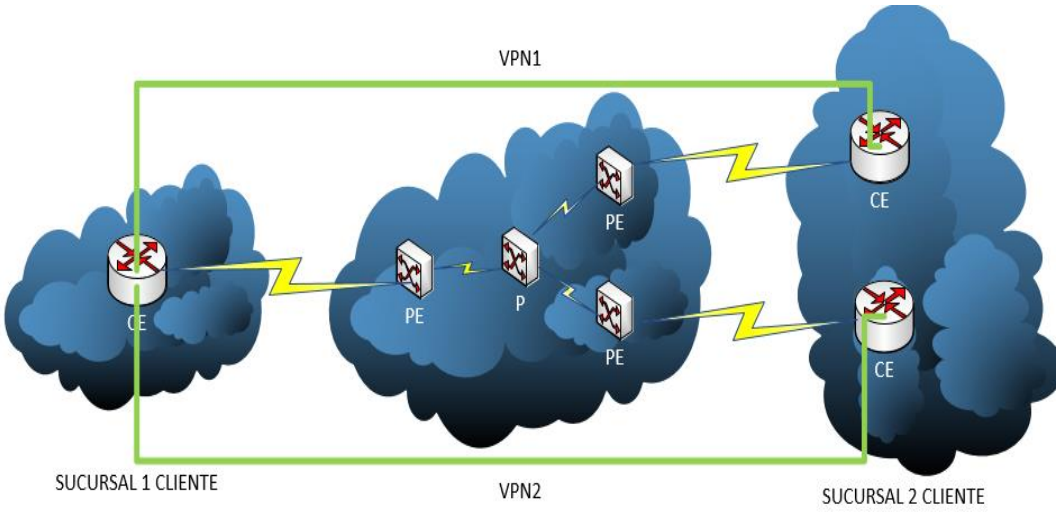
- **Configuración de ruta manual:** para implementar la ingeniería de tráfico, las rutas requieren una configuración manual independientemente de la presencia del Protocolo de Internet para el enrutamiento de paquetes. El cálculo de la ruta física es posible al denotar los saltos consecutivos que ocurren desde la ruta de origen a la de destino. Sin embargo, esta configuración manual necesita proveedores de soluciones profesionales para poner en práctica la configuración de ruta manual. Además, si los nodos intermedios no se configuran manualmente, el tráfico MPLS TE no gana importancia y se trata del mismo modo que el tráfico IP o MPLS regular.(solutions, 2020)

VPN

Las redes privadas virtuales (VPN) son redes privadas que usan una red pública para conectar dos o más sitios remotos. En lugar de conexiones dedicadas entre redes, las VPN utilizan conexiones virtuales enrutadas (tunelizadas) a través de redes públicas que generalmente son redes de proveedores de servicios. Las VPN son una alternativa rentable a las costosas líneas dedicadas. El tipo de VPN está determinado por las conexiones que utiliza y si la red del cliente o la red del proveedor realiza el túnel virtual.

Figura 6

Esquema MPLS con VPN



Enrutamiento VPN MPLS

Las VPN canalizan el tráfico de un sitio del cliente a otro, utilizando una red pública como red de tránsito, cuando se cumplen ciertos requisitos:

- El tráfico se reenvía mediante el reenvío de IP desde los enrutadores CE a los enrutadores PE.
- Los enrutadores PE establecen un LSP a través de la red del proveedor.
- El enrutador PE entrante recibe tráfico y realiza una búsqueda de ruta. La búsqueda produce un siguiente salto de LSP, y el tráfico se reenvía a lo largo del LSP.
- El tráfico llega al enrutador PE de salida, y el enrutador PE muestra la etiqueta MPLS y reenvía el tráfico con enrutamiento IP estándar.(J. Networks, 2019)

SDWAN

Es una red definida por software, tiene una arquitectura WAN virtualizada que permite a las empresas usar distintos tipos de planes de internet, ya sea empresariales o de hogar para transportar distinto tipo de tráfico y conectar de manera segura a los usuarios con las aplicaciones.

Una SD-WAN dirige el tráfico de forma segura e inteligente por medio de la WAN mediante una función de control centralizada, con el propósito de mejorar el rendimiento de las aplicaciones, presentando una mayor productividad, reducción de costos y a su vez una mayor experiencia para el usuario.

Las WAN tradicionales tienen un pequeño retraso por el tiempo que toma en ir un paquete desde una sucursal de una empresa y atravesar toda la circuitería de enrutamiento del data center de un ISP para llegar a su destino, ocasionando una deficiente experiencia para el usuario.

En la actualidad muchos aplicativos están alojados en la nube, en la arquitectura MPLS, todo está centralizado en un enrutador, mientras que el diseño de SD-WAN es enfocado para admitir aplicaciones alojadas en ISP, nubes, con niveles muy altos de rendimiento.

En una red MPLS la latencia afecta el rendimiento de una aplicación alojada en la nube por el tráfico que existe entre cada enrutador, SD-WAN simplifica esa tarea, con una mayor eficiencia de ancho de banda, lo que hace que las aplicaciones en la nube sean más dinámicas y ágiles sin dejar a un lado la seguridad y privacidad de datos. (Peak, 2019b)

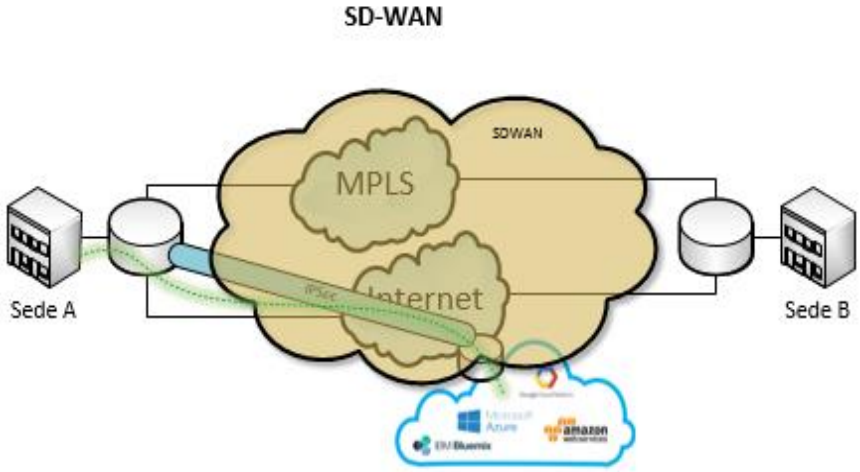
La tecnología SD-WAN se está volviendo rápidamente muy popular en las redes empresariales. SD-WAN admite servicios de seguridad, como firewalls, VPN.

Los proveedores prometen "agilidad sobre la marcha, simplicidad, seguridad y automatización "y muchos otros beneficios.(Gordeychik, Kolegov, & Nikolaev, 2018)

En la Fig 6 y FIg 7, se puede observar cómo sería un esquema para el uso de aplicaciones en la nube. SD-WAN se puede conectar de manera directa, mientras que en MPLS debe pasar por una seria de ruteadores.

Figura 7

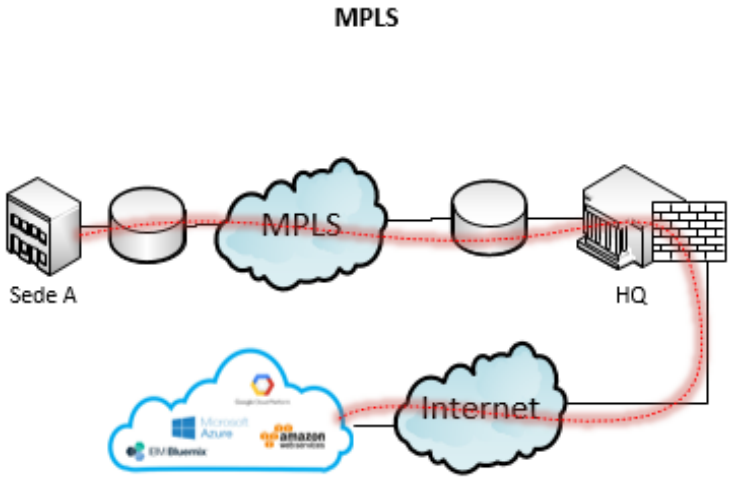
Esquema de SD-WAN accediendo a la nube



Tomado de *Netblogrk, 2018*

Figura 8

Esquema de MPS accediendo a la nube



Tomado de *Netblogrk, 2018*

Funcionamiento de SD-WAN

EL punto de operación de SD-WAN está centralizado, frecuentemente está situado en una aplicación SaaS que se ejecuta en una nube pública. El control se desacopla del hardware para simplificar la administración de la red y mejorar la entrega de servicios. Los dispositivos SD-WAN (y los dispositivos virtuales) siguen las reglas operativas transmitidas desde el punto de operación SD-WAN central. Esto reduce o elimina en gran medida la necesidad de administrar puertas de enlace y enrutadores de forma individual.

SD-WAN permite tener un mayor control de redes muy amplias y complejas, se enfoque en centralizar toda su administración desde un equipo principal, incorporando políticas, reglas para según sea las necesidades del ambiente del negocio. (Technology, 2020)

Beneficios de SD-WAN

El rendimiento del internet es un factor clave para la elección de la WAN, según la ruta que siga todo el tráfico, puede ocasionar latencia según los saltos que se tengan hasta llegar a su destino.

Otro factor importante es el cuello de botella que se forme como resultado de una sola ruta, limitando el ancho el ancho de banda, es por eso que se establecen conexiones redundantes para evitar este tipo de inconvenientes.

SD-WAN vigila constantemente el estado de cada enlace y puede determinar que ruta es la más óptima para redirigir el tráfico. Según las políticas configuradas SD-WAN puede discriminará el ancho de banda por aplicaciones como VoIP, reservando

un porcentaje del ancho de banda y el tráfico de menor prioridad dejarlo en cola o hacia otra ruta menos confiable.(Technology, 2020)

Seguridad en SD-WAN

SD-WAN brinda una mejora en la seguridad de la red encriptándola, permitiendo su visualización de una manera más amigable para el usuario y a su vez optimizando el rendimiento por la segmentación de la red.

Una ventaja aparente de seguridad de MPLS es que proporciona un enlace seguro y administrado entre las sucursales y el centro de datos a través de la red troncal interna del proveedor de servicios. Las conexiones públicas a Internet no proporcionan de forma nativa el mismo nivel de protección.

Pero esta comparación es engañosa. MPLS no proporciona ningún tipo de análisis de los datos que entrega. Esa sigue siendo responsabilidad del cliente MPLS. Incluso cuando atraviesa una conexión MPLS, el tráfico aún debe ser inspeccionado para detectar malware u otras vulnerabilidades, lo que requiere implementar un firewall y cualquier función de seguridad adicional en un extremo de la conexión o en el otro como mínimo.

Muchas soluciones SD-WAN, sin embargo, tienen el mismo problema. Además de algunas funciones de seguridad básicas, la mayoría de las soluciones SD-WAN aún requieren que se agregue seguridad como una solución de superposición. Y para aquellas organizaciones que intentan agregar seguridad a sus complejas conexiones SD-WAN como una ocurrencia tardía, el desafío es a menudo más de lo que esperaban.

Fortinet presenta una solución para la seguridad de SD-WAN, es diferente porque la conectividad se implementa como una función integrada dentro de un dispositivo NGFW, por lo que cada conexión incluye automáticamente capacidades VPN de malla dinámica para proteger los datos en tránsito, combinado con una inspección profunda de ese tráfico utilizando la amplia gama de herramientas de seguridad - Incluyendo IPS, firewall, WAF, filtrado web, antivirus y antimalware, que ya son parte de cada solución FortiGate NGFW que admite SD-WAN. Esto incluye la inspección de alta velocidad de las conexiones SSL e IPsec VPN, una función especialmente importante hoy en día, ya que casi el 70% de todo el tráfico de Internet hoy está encriptado, y muchos países encriptan hasta el 85% de todas las páginas web visitadas.(Fortinet, 2020)

Características de SD-WAN

- Las puertas de enlace SD-WAN admiten WAN híbrida, lo que implica que cada puerta de enlace puede tener múltiples conexiones utilizando diferentes transportes: MPLS, Internet de banda ancha, LTE, etc. Por lo general, se configura una red privada virtual (VPN) en cada conexión WAN por seguridad. En consecuencia, la SD-WAN puede ser una superposición que abarca una infraestructura de comunicaciones diversa.

- Otra característica de SD-WAN es la selección de ruta dinámica: que es la capacidad de enrutar el tráfico de forma automática y selectiva a un enlace WAN u otro, según las condiciones de la red o las características del tráfico. Los paquetes pueden dirigirse a un enlace en particular porque otro enlace está inactivo o no funciona muy bien, o para equilibrar el tráfico de red en todos los enlaces disponibles. SD-WAN también puede identificar paquetes por

aplicación, usuario, origen / destino, etc. y enviarlos por una ruta u otra según esas características.

- La gestión basada en políticas es lo que determina dónde la selección de ruta dinámica dirigirá el tráfico y qué nivel de prioridad (calidad de servicio o QoS) se le otorga. Las intenciones comerciales se pueden implementar como políticas a través de la consola de administración central. Las políticas nuevas y actualizadas se traducen en reglas operativas y se descargan a todas las puertas de enlace y enrutadores SD-WAN bajo control.

- Se puede crear una política, por ejemplo, para garantizar el mejor rendimiento para VoIP y conferencias web interactivas al dar prioridad a la transmisión de sus paquetes y enrutarlos en rutas de baja latencia. Los ahorros de costos se pueden realizar enviando copias de seguridad de archivos a través de una conexión a Internet de banda ancha. El tráfico WAN que requiere un alto nivel de seguridad puede restringirse a conexiones privadas (por ejemplo, MPLS) entre sitios y debe pasar por una sólida pila de seguridad al ingresar a la empresa.

- Una característica adicional de SD-WAN es la capacidad de encadenarla junto con otros servicios de red. La optimización de WAN a menudo se combina con SD-WAN para mejorar el rendimiento de la red y las aplicaciones. El tráfico de Internet que sale y entra a una sucursal puede enrutarse a través de una VPN a un servicio de seguridad basado en la nube para lograr un equilibrio entre rendimiento, seguridad y costo.(Technology, 2020)

Estructura actual de la red MPLS en Puntonet

Puntonet como ISP, es una empresa de servicios de telecomunicaciones y tecnologías de la información, tiene como objetivo brindar soluciones empresariales de calidad. Cuenta con 20 años de experiencia en el ámbito de las telecomunicaciones, innovando sus redes, siempre enfocados a las necesidades de sus clientes. Es por eso que desde el año 2011 al 2013 migro su tecnología a MPLS por los beneficios que presenta, como robustez y escalabilidad.

Puntonet como ISP tiene un centro de datos redundante bajo normas TIER III en las ciudades de Quito y Guayaquil. Su red MPLS está constituida por equipos robustos que garanticen la operatividad de todos sus clientes hacia la internet. Cuenta con varios proveedores de salida internacional, cuando falla uno se envía el tráfico hacia el proveedor más adecuado o se hace un balanceo de carga entre los diferentes proveedores, brindando al cliente una experiencia en las conexiones.

La red MPLS de Puntonet mediante sus enlaces redundantes entre Quito y Guayaquil permite optimizar de una mejor manera los niveles de tiempo de respuesta, garantizando la operatividad del servicio. El flujo de datos es constantemente monitoreado por personal de TI para tomar una decisión oportuna y rápida frente a una posible pérdida entre sus interconexiones por posibles errores lógicos o físicos o por saturamiento de la misma. Cuando se detecta una saturación por un alto tráfico de datos en una interconexión, el área encargada de su administración puede aplicar políticas de seguridad y enviar los datos a través de otras rutas que estén menos congestionadas, este trabajo es muy recurrente en los ISPs en donde se centraliza todo el tráfico en los data centers propios o arrendados.

Una ventaja de contar con normas TIER III es que a más de disponer equipos capaces para enfrentar los requerimientos que se presentan día a día por parte de los

usuarios, es dar una respuesta inmediata ante aplicaciones mayormente utilizadas por parte de los clientes, como es el caso de Netflix, google, los cuales están alojados en servidores propios del ISP para que la búsqueda sea más rápida y llegue de forma inmediata al usuario, sin importar de qué localidad del Ecuador se esté solicitando adquirir ese contenido.

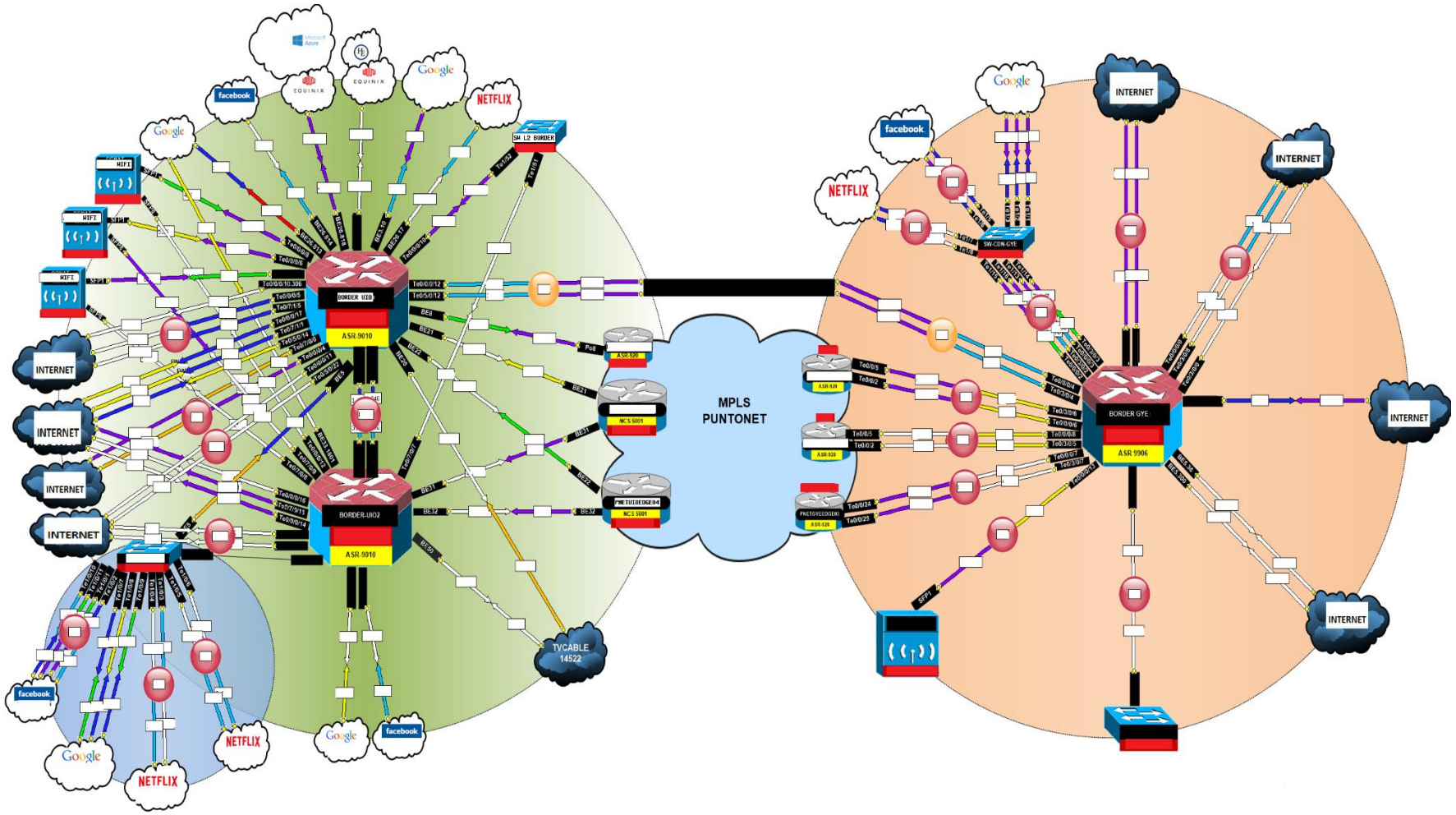
La integración de MPLS a la red de Puntonet en el año 2011 permitió hoy en día cumplir con los estándares requeridos a nivel mundial, pero de acuerdo a Gartner, para el año 2022 se estima un incremento considerable de acceso al internet por las nuevas generaciones, que demandarán un mayor ancho de banda, mayor velocidad, porque cada usuario contará con más de un dispositivo inteligente como celulares, televisores Smart, juegos en línea, entre otros, que hará que sea necesario buscar una tecnología superior como SD-WAN a la que actualmente es usada como MPLS. (Gartner, 2018)

En la Fig 9, se puede observar más claramente cómo está diseñada la red MPS, qué equipos son los mayormente usados y cómo está compuesta su infraestructura para brindar un servicio los 365 días del año por la redundancia en la red, para este caso se presenta un ejemplo de cómo sería la arquitectura MPLS entre 2 ciudades muy distantes, con diferentes salidas hacia al internet con más de un proveedor internacional.

.

Figura 9

Esquema de la red MPLS



La red MPLS de Puntonet no solo está conformada por los equipos mostrados en la Fig 9, sino que por detrás hay una ingeniería de tráfico muy robusta, cada equipo cuenta con configuraciones avanzadas de enrutamiento, políticas de seguridad, filtrado de paquetes, entre otros, que permiten el correcto funcionamiento de la red MPLS en un ISP. Esta tecnología ya se encuentra operativa 9 años, con actualizaciones de equipos a medida de la demanda de nuevos clientes y aplicaciones que se requieran, como el caso de aplicaciones en la nube, servidores, firewalls, máquinas virtuales.

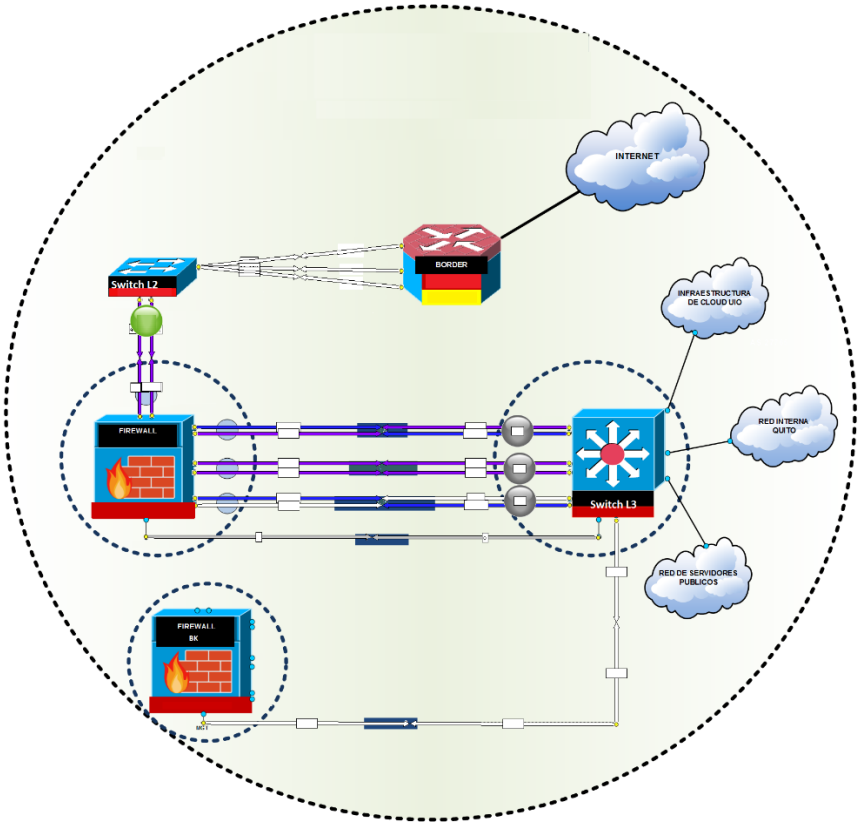
Esta tecnología hoy por hoy permite el dinamismo y fluido del tráfico hacia el internet a pesar de la complejidad de la red, por cada equipo de border o router principal, existen cientos de configuraciones, las cuales son añadidas por el administrador de la red, lo que representa una posible falla si una línea de comando estuvo incorrectamente ingresada, esa falla puede ser mínima que no sea perceptible por el cliente o puede tener un muy alto grado de impacto que ocasione una falla en la conexión hacia el internet, es por esa razón que en un futuro, cuando la demanda de acceso al internet aumente, este proceso de configuración ya no sería tan factible, por el tiempo que tomaría, la movilidad de los técnicos para reparar o cambiar un equipo principal, lo que representa un costo para la empresa; y, en el caso de que no se disponga del router de border correcto se debería importarlo.

Una ventaja de elegir a Puntonet como proveedor de servicios de internet, datos, o aplicaciones en la nube, es que dispone de una tecnología actualizada a las necesidades actuales de los clientes ecuatorianos. Su experiencia permitirá solventar cualquier requerimiento de empresas o de hogar, cuenta con servicios de fibra óptica, radio enlace e internet satelital, la seguridad es un punto clave para que la información llegue a su destino sin ser alterada, es por ese motivo que Putonet es una buena opción a la hora de elegir un ISP.

En la Fig 10, se puede ver un esquema de la seguridad que un ISP contaría para proteger el acceso interno y externo hacia el internet, como también así asegurar la información que es enviada por las distintas rutas e interconexiones físicas y hacia la nube, sin descuidar la redundancia de firewalls perimetrales que es muy importante, si un equipo falla el otro de reemplazo lo respalda, estas configuraciones son realizadas bajo líneas de comando en ruteadores, switches, servidores mediante protocolos de enrutamiento MPLS.

Figura 10

Esquema de seguridad con redundancia



Equipos perimetrales de una red MPLS

Cada ISP tiene una arquitectura diferente, de acuerdo a las necesidades requeridas y el enfoque de servicios que esté brindando, como puede ser además de internet, televisión por cable, telefonía celular.

Entre los equipos que se usan mayormente en un ISP enfocado al servicio de internet, datos y cloud, se tienen los siguientes:

Enrutadores

- **ASR-920**

El enrutador Cisco ASR 920 admite el acceso de banda ancha para ofrecer servicios "de reproducción" (voz, video, datos y movilidad) a miles de suscriptores, con calidad de servicio (QoS) en el enrutador Cisco ASR 920 capaz de escalar hasta gran cantidad de colas por dispositivo. La gran cantidad de colas, combinadas con el algoritmo de QoS jerárquico de tres niveles, da como resultado una experiencia de usuario de banda ancha mejorada. Este conmutador de capa 2 con todas las funciones y enrutador de capa 3 admite una variedad de aplicaciones de banda ancha, incluyendo IPTV y video a pedido (VoD), mejorando y extendiendo la arquitectura de la red programable evolucionada de Cisco.

Figura 11

Router ASR920

Tomado de *(Cisco, 2018a)*

Características

Tabla 1

Características del router Cisco ASR-920

Modelo	El ASR-920-4SZ
Ranuras por Chasis	Fijo
Tamaño del rack	1 RU

Máxima capacidad	64Gbps
1G Puertos	El ASR-920-4SZ: 2
	(Dos puertos de cobre 1G)
10G puertos	4 dual 1G / 10
Talla (H x W x D)	1.72 X 15.5 X 9.6 en. (43.7 X 393.7 X 243.8 mm)
Peso	7.0 lb (3.2kg)
Poder	2 x fijo, Max 105W, Típico: 75W
Los despliegues de destino	enrutador de red de acceso para Carrier Ethernet, backhaul móvil, y servicios de FTTH / FTTB
Precio	$2,689.11

Tomado de *(Ycict, 2018)*

- **ASR-9010**

Los enrutadores Cisco de la serie ASR 9010 ofrece un enrutamiento de núcleo y borde, tiene una escalabilidad alta, diseño amigable con el medio ambiente, adaptación increíble y un buen precio vs rendimiento. La serie Cisco ASR 9000 ofrece también una entrega de video optimizada y soporte móvil.

Figura 12

Router ASR9010

Tomado de *(Cisco, 2019a)*

Características

Tabla 2

Características del router Cisco ASR-9010

Modelo	ASR-9010
Descripción	Cisco ASR 9010 Chassis, ASR-9010-AC, ASR-9010 AC Chassis
Slots	8 Line Cards 2 RSPs
Tamaño Rack	21 RU
Bandwidth Por Slot	880 Gbps
Max Capacidad	14 Tbps
Tamaño (H x W x D)	36.75 in. x 17.5 in x 28.65 in
Alimentación	AC: 6 kW or 3 kW power modules DC: 4.4 kW or 2.1 kW or 1.5 kW power modules Note: Mixing of AC and DC modules is not supported
Software	IOS XR
Precio	$6,655

Tomado de *(Cisco, 2019a)*

- **NCS-5001**

La serie de Cisco NCS 5000 permite a los proveedores de internet y arquitecturas de ISP por medio de MPLS, dar soluciones elásticas con agilidad y operaciones simplificadas para ofrecer servicios móviles, de video y en la nube con un gran ancho de banda. También se lo puede usar como un estante de extensión por medio de tecnología de virtualización.(Cisco, 2017)

Figura 13

Router NCS-5001

Tomado de *(Cisco, 2017)*

Características

Tabla 3

Características del router Cisco NCS-5001

Descripción	Cisco NCS-5001
Interface integrada	40 puertos de 1/10 Gigabit Ethernet (GE) y 4 puertos 100 GE (NCS 5001) 80 puertos de 1/10 GE y 4 puertos 100 GE (NCS 5002)
Rendimiento	Hasta 1.2Tbps de rendimiento con 1.4 Bpps
Procesador de ruta integrado con 16 GB de RAM	Ejecuta el software Cisco IOS XR
Virtualización de red (nV)	La tecnología nV de Cisco reduce drásticamente los costos operativos y simplifica la red mediante el uso del plano de control distribuido de la serie Cisco ASR 9000
Puertos de gestión	Proporciona fácil acceso a la consola del sistema.
Usb externa	Ayuda a simplificar la gestión de imágenes y archivos.
Almacenamiento USB incorporado (eUSB) (32 GB)	Dispositivos de memoria flash para imagen de software, configuración, registro y recuperación.

Descripción	Cisco NCS-5001
Precio	$23,755

Tomado de *(Cisco, 2017)*

- **7606-S**

Es un enrutador mediano de alto rendimiento diseñado de 6 ranuras que permite ser implementado en el borde de la red, donde se necesitan un rendimiento sólido y servicios de conmutación de etiquetas multiprotocolo (MPLS) para satisfacer con las necesidades de tanto empresas como ISPS. Permite a los proveedores de servicios de Carrier Ethernet implementar una infraestructura de red avanzada que admite una variedad de aplicaciones de sistemas de video IP y triple play (voz, video y datos) en los mercados de servicios residenciales y comerciales. El Cisco 7606-S también ofrece soluciones de redes WAN y redes de área metropolitana (MAN) en el borde empresarial.

Con una velocidad de reenvío de hasta 240 Mpps distribuidos y 480 Gbps de rendimiento total, el Cisco 7606-S ofrece rendimiento y confiabilidad con opciones para procesadores de ruta redundantes y fuentes de alimentación.(Cisco, 2014a)

Figura 14

Router 76706-S

Tomado de *(Cisco, 2014a)*

Características

- Mecanismos de conmutación por error mejorados en el hardware, que cuando se combina con la imagen de software Cisco IOS adecuada, puede lograr una conmutación por error de 100 ms.

- Capacidad para ofrecer una mayor potencia de hasta 750 W por ranura

- Módulo de bandeja de ventilador de alta velocidad con cinco velocidades en un diseño de flujo de aire de lado a lado.

- **Precio:** $2,709.00

Switch

- **ME-3600X**

Mediante el Switch de la serie Cisco ME 3600X se simplifican las operaciones de red mediante la convergencia de servicios inalámbricos y alámbricos con los switches de acceso Ethernet. Extiende la velocidad de transporte a 10 Gbps en la capa de acceso para aplicaciones empresariales y móviles, también permite a los proveedores de servicios iniciar servicios VPN basados en conmutación de etiquetas multiprotocolo (MPLS) desde la capa de acceso.(Cisco, 2010)

Figura 15

Switch ME-3600X

Tomado de *(Cisco, 2010)*

Características

- Proporciona una velocidad de transporte de 10 Gbps en la capa de acceso para aplicaciones empresariales y móviles

- Ayuda a iniciar servicios VPN basados en MPLS desde la capa de acceso

- Facilite servicios premium con capacidades mejoradas de acuerdo de nivel de servicio (SLA)

- **Precio:** $1,750.00

Firewall

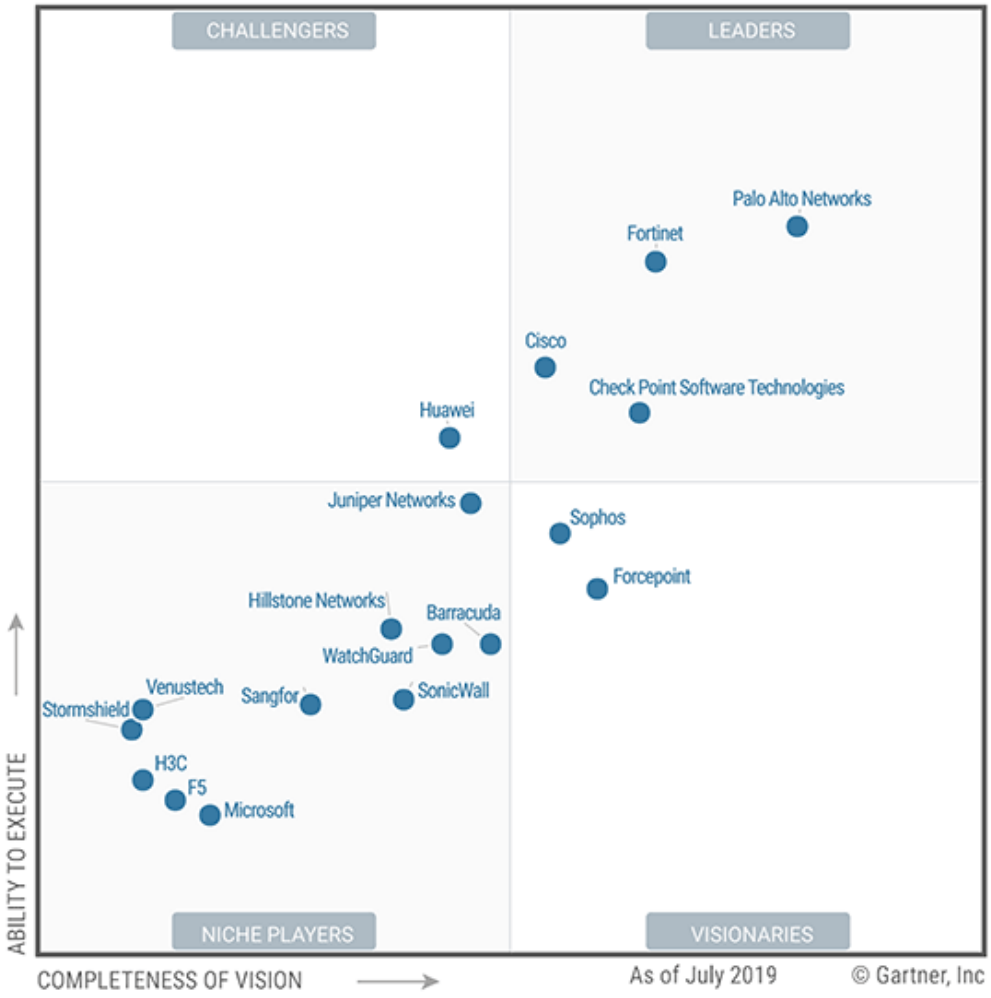
Puntonet cuenta con equipos perimetrales de seguridad a la vanguardia de la tecnología, capaces de cumplir con normas internacionales para mitigar y proteger toda la información que día a día está siendo constantemente atacada por ciber atacantes que intentan sacar provecho de una falla en la seguridad, con el fin de obtener una remuneración a cambio de no divulgar o no alterar los datos si lograrían penetrar dentro de la red.

Muchos ISP años atrás protegían su infraestructura mediante servidores Centos, Linux, pero no contaban con la suficiente protección que en la actualidad se requiere, es por eso que empresas enfocadas a la seguridad brindan soluciones empresariales capaces de afrontar esa problemática.

De acuerdo al cuadrante de Gartner actualizado hasta septiembre 2019, los líderes en soluciones empresariales de seguridad son los que se pueden en la ver la Fig 16.

Figura 16

Cuadrante de Gartner en Firewalls



Tomado del *(Gartner, 2019a)*

Tomando en consideración el cuadrante de Gartner se analizarán los Firewalls más utilizados en una infraestructura ISP, Palo Alto, Fortinet y Check Point.

Palo Ato

Palo Alto es un pionero en seguridad de la red con una plataforma innovadora que permite proteger la red y habilitar de forma segura un número de aplicaciones cada vez más complejo y en rápido crecimiento. El núcleo de esta plataforma es el firewall de próxima generación, que ofrece visibilidad y control sobre las aplicaciones, los usuarios y el contenido dentro del firewall utilizando una arquitectura de hardware y software altamente optimizada.

Características:

- App-ID: Hace un escaneo continuo de todas las aplicaciones por todos los puertos independientemente del cifrado (SSL o SSH) para evadir una detección de un posible atacante.

- ID de usuario: Vincula sus usuarios y grupos a políticas específicas, independientemente del tipo de dispositivo.

- Content-ID: Hace un control minucioso de la navegación web de los usuarios, así como también previene la transferencia de información no autorizada.

- WildFire: Identifica, analiza y genera automáticamente protección para cualquier tipo de malware.

- Global Protect: Protege a todos los usuarios mediante políticas de seguridad, independientemente de su ubicación o dispositivos.

- Panorama: Desde una ubicación centralizada, configura, administra e implementa sus políticas en varios firewalls de Palo Alto.

Figura 17

Firewall de Palo Alto

Tomado de *(P. a. networks, 2019)*

Fortinet

Los firewalls de Fortinet son de próxima generación, filtran el tráfico de red para proteger a una organización de amenazas externas. Al mantener las funciones de los firewalls con estado, como el filtrado de paquetes, el soporte de VPN, la supervisión de la red y las funciones de mapeo de IP, los NGFW también poseen capacidades de inspección más profundas que les brindan una capacidad superior para identificar ataques, malware y otras amenazas. Los firewalls de próxima generación brindan a las organizaciones control de aplicaciones, prevención de intrusiones y visibilidad avanzada en toda la red. A medida que el panorama de amenazas continúa desarrollándose rápidamente, los firewalls tradicionales se quedan atrás y ponen en riesgo a la organización. Los NGFW no solo bloquean el malware, sino que también incluyen rutas para futuras actualizaciones, dándoles la flexibilidad de evolucionar con el paisaje y mantener la red segura a medida que surgen nuevas amenazas.

FortiGate permite la creación de redes basadas en la seguridad y consolida las capacidades de seguridad, como el sistema de prevención de intrusiones (IPS), el filtrado web, la inspección de la capa de sockets seguros (SSL) y la protección automatizada contra amenazas. Los NGFW de Fortinet satisfacen las necesidades de

rendimiento de arquitecturas de TI híbridas altamente escalables, lo que permite a las organizaciones reducir la complejidad y administrar los riesgos de seguridad.(Fortinet, 2019)

Figura 18

Firewall de Fortinet

Tomado de *(Fortinet, 2019)*

Check Point

Es un líder del mercado en los mercados de firewall empresarial, firewall personal y VPN a nivel mundial. A través de su plataforma NGX, ofrece una amplia gama de soluciones en cuanto a la seguridad requerida, de perímetro, red local, ciberespacio y de punto final que aseguran las comunicaciones y recursos comerciales para redes y aplicaciones corporativas, empleados remotos y sucursales. La línea de productos ZoneAlarm de la compañía es la suite de seguridad para computadoras personales mejor calificada, compuesta por soluciones de seguridad de punto final galardonadas que protegen a millones de PC de piratas informáticos, spyware y robo de datos. Las soluciones de Check Point son vendidas, integradas y atendidas por una red de más de 2,200 socios de Check Point en 88 países y sus clientes incluyen el 100% de las compañías Fortune 100 y decenas de miles de empresas y organizaciones de todos los tamaños. (CheckPoint, 2019)

Figura 19

Firewall de CheckPoint 26000

Tomado de *(CheckPoint, 2019)*

Elección del proveedor de seguridad perimetral

Se presentará una comparación entre los tres tipos de proveedores de seguridad perimetral descritos anteriormente, por su ubicación de líderes del mercado según el cuadrante de Garnet, tanto en precios como en características, los equipos son enfocados para pequeños como grandes ISP, entre los que se tiene:

Tabla 4
Comparación de firewalls aplicados a ISPs

	Palo Alto	Fortinet	Check Point
	Serie 5280	Serie 6300F	Serie 23800
Prevención de amenazas / Rendimiento	68Gbps	60Gbps	10.5Gbps
Rendimiento de inspección SSL	6.5 Gbps	90 Gbps	5 Gbps
New Sessions/Sec	462,000	2 millones	319,000
Rendimiento VPN IPsec	24 Gbps	96 Gbps	28 Gbps
Firewall + IPS + Antivirus + filtrado URL	Si	Si	Si
Interfaz gráfica	Si	Si	SI
Incluye QoS	Si	Si	Si
Soporte	Si	Si	Si
Seguridad Cloud	Si	Si	Si
COSTO	$199,500.00	$180,000.00	$148,953.99

En base a la tabla 4 y a los análisis efectuados para cada proveedor de firewalls, se puede decir que Palo Alto es más orientado a empresas grandes, presenta soluciones empresariales que brindan una mayor seguridad, filtrado de paquetes, análisis de aplicaciones, soluciones SD-WAN y de acuerdo al cuadrante de Gartner está en primero lugar de los proveedores se seguridad perimetral.

El precio no lo es todo, más prima el nivel y experiencia que tengan frente a ataques de ciber delincuentes; y, otro punto a favor del por qué Palo Alto es mayormente preferido es por el soporte que brindan, disponibilidad inmediata, atención personalizada, la implementación requiere menor tiempo y por la administración de los equipos, el cual tiene un ambiente más amigable para el usuario.

Fortinet y Check Point son más orientados para empresas de tamaño medio y pequeño, en el cual se requiera un nivel menor de seguridad y del enfoque del negocio porque hay soluciones que presentan las 2 empresas que las hacen muy competitivas en el mercado de firewalls y las han colocado como líderes en el primer cuadrante de Gartner.

Requerimientos para la implementación de SDWAN en Puntonet

Puntonet cuenta con una red MPLS, bajo este esquema puede trabajar SD-WAN, pero con la vertiginosa demanda de una tecnología cada vez mejor y el requerimiento de aplicaciones en la nube sea mayor, se deberá pensar en un cambio de tecnología para tener una red sobre SD-WAN, para este cambio se plantea los componentes a requerir:

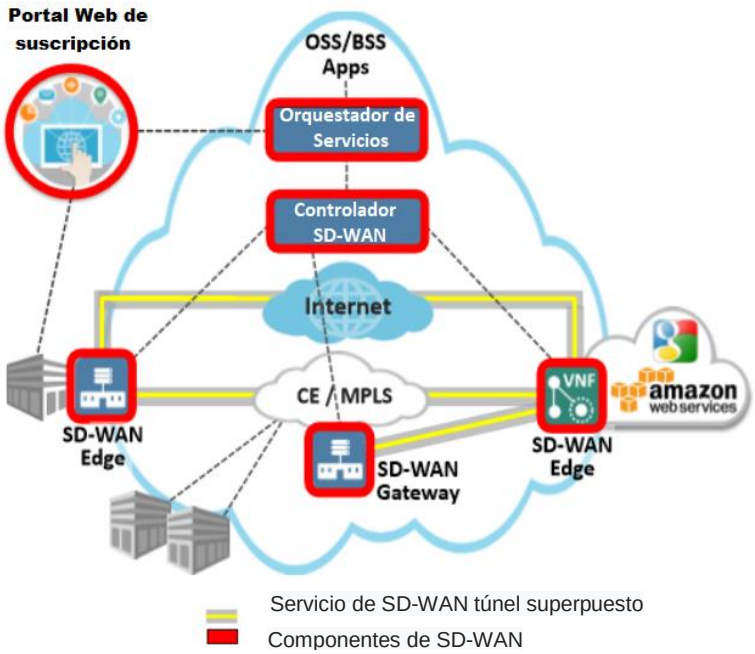
- SD-WAN Edge

- Controlador SD-WAN
- Orquestador de servicios
- SD-WAN Gateway
- Portal Web de suscripción

En la Fig 17 se puede observar, cuál sería la estructura para implementar una red SD-WAN en Puntonet con todos sus componentes e incluso interconectar con una red de MPLS.

Figura 20

Componentes de una red SD-WAN



Tomado de *(Lacnic, 2017)*

SD-WAN Edge

En este dispositivo es en donde el túnel SD-WAN es inicializado o finalizado y provee servicios de demarcación, además de crear túneles seguros (encriptados) sobre diferentes tipos de redes como fibra óptica, redes inalámbricas, mpls.

Permite también realizar QoS mediante políticas de seguridad, reenvío de aplicaciones por medio de una o más conexiones WAN y según el rendimiento que presenten selecciona la ruta más óptima.

Otra característica del SD-WAN Edge es que hace una optimización de la WAN, reordenando paquetes, compresión de datos y corrección de errores.

Controlador SD-WAN

El controlador SD-WAN proporciona gestión física o virtual de todos los dispositivos de SD-WAN Edge y SDWAN Gateway asociadas con el controlador. El controlador SD-WAN mantiene conexiones con todos los SD-WAN Edge y SD-WAN Gateway para identificar el estado operativo de los túneles a través de diferentes WAN y recuperar métricas de QoS para cada túnel. Estas métricas son utilizadas por los servicios del orquestador.

Aquí radica la inteligencia de la red, señalando las políticas a todos los elementos descritos.(Mef, 2017)

SD-WAN Gateway

Proporcionan la ruta más óptima a todas las aplicaciones, sucursales y centros de datos junto con la capacidad de entregar servicios de red alojados en la nube, además de permitir una interconexión entre SD-WAN con otro tipo de VPSs como las VPNs sobre MPLS.

Orquestador de servicios

Proporciona el servicio de gestión del ciclo de vida del servicio SD-WAN, incluyendo el cumplimiento de los servicios de, control, aseguramiento, análisis, seguridad y políticas.

También modifica o crea nuevas redes, políticas y servicios para maximizar los recursos disponibles.

Portal Web de suscripción

Permite crear o modificar el servicio del cliente.(Mef, 2017)

Diseño de red SDWAN

Para el diseño de red SD-WAN, debemos primeramente elegir el proveedor adecuado que nos brinde una solución acorde a nuestras necesidades, en el mercado internacional existen varias empresas que disponen este servicio, según el cuadrante de Gartner de acuerdo al último informe de noviembre 2019, se tiene a VMware y Silver Peak como líderes de SD-WAN, seguidos por Cisco, Fortinet, Huawei y Citrix.

Figura 21

Tendencias de Infraestructura SD-WAN

Tomado de *(Gartner, 2019b)*

Elección del proveedor de SD-WAN

Los proveedores más pequeños no cuentan con un sistema completo para la gestión de WAN y no suelen contar con la experiencia requerida. Un proveedor adecuado sabrá reconocer y resolver los puntos débiles, liderando en el mercado WAN. Esto garantizará el cumplimiento de todos los requerimientos presentes y futuros para el desarrollo de proyecto SD-WAN y cualquier otro.

En consideración a lo descrito anteriormente del cuadrante Gartner, se analizarán los siguientes proveedores de SD-WAN según la tabla.

Tabla 5

Tabla comparativa según posicionamiento de Gartner

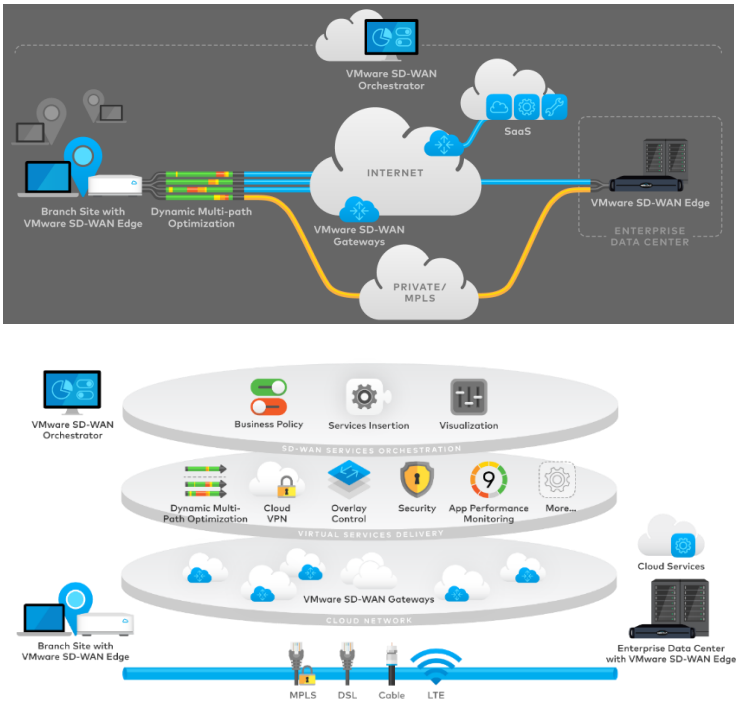
Posicionamiento	Proveedor	Estimación clientes a nivel mundial
1	VMware	5.500
2	Silver Peak	3000
3	Fortinet	21.000
4	Cisco	100.000
5	Citrix	1200
6	Huawei	50.000
7	HPE (Aruba)	250
8	Nauge Networks	1400
9	Teldat	1000

VMware

La SD-WAN de VMware permite el acceso hacia el Internet por cable o inalámbrico con o sin MPLS tradicional para crear redes de área amplia de grado empresarial con mayor ancho de banda, acceso de alto rendimiento a la nube, inserción de servicios y amplia visibilidad de red y una capa de orquestación impulsada por el negocio para la automatización y la inserción de servicios virtuales.(velocloud, 2020)

Figura 22

Arquitectura de VMware SD-WAN



Tomado de *(velocloud, 2020)*

Silver Peak

Silver Peak es una solución SD-WAN completa y de alto rendimiento. Permite a los proveedores de servicios llevar al mercado servicios SD-WAN nuevos,

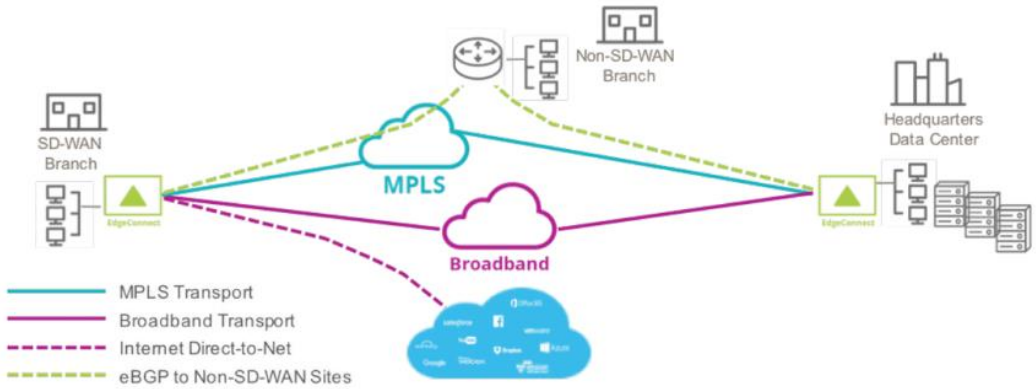
diferenciados y administrados de manera rápida y rentable para impulsar nuevas fuentes de ingresos, ampliar el alcance del mercado y entregar SLA dentro y fuera de la región.

La solución Silver Peak SD-WAN consta de dispositivos físicos y virtuales de toque cero, y un orquestador de múltiples inquilinos, Unity OrchestratorSP, para optimizar la gestión de servicios para miles de clientes. (peak, 2019a)

La arquitectura que presenta Silver Peeak es la que se puede ver en la Fig 23, en la cual está basada netamente en una solución SD-WAN pero que además permite interconexiones por medio de la red tradicional MPLS.

Figura 23

Arquitectura de Silver Peak SD-WAN



Tomado de *(peak, 2019a)*

Fortinet

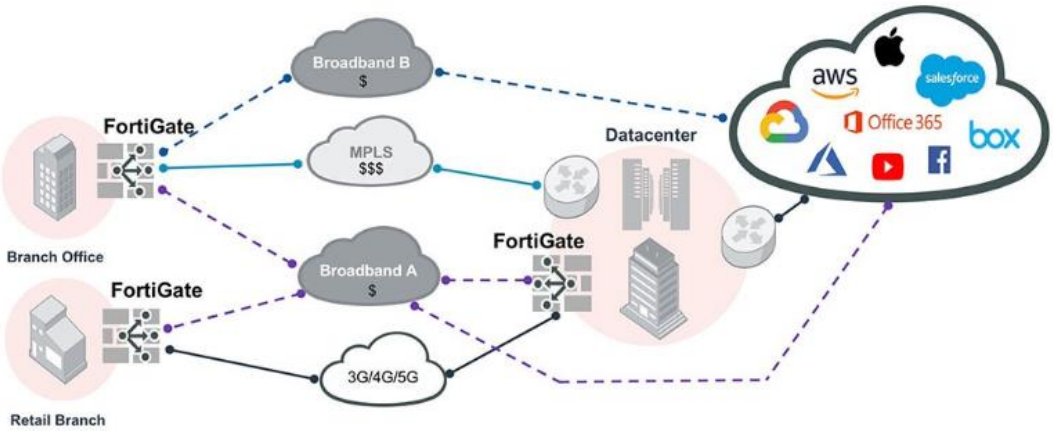
Bajo el esquema de SD-WAN de Fortinet, ofrece las mejores capacidades SD-WAN y de NGFW para ayudar a las empresas a reducir costos, mejorar la experiencia de las aplicaciones, simplificar las operaciones y habilitar una postura de alta

seguridad, también dispone de herramientas de corrección de errores para una mejor experiencia de usuario.(Gartner, 2019b)

En la Fig.24, podemos observar la arquitectura que tiene Fortinet en cuanto a soluciones SD-WAN, en la cual no requiere de una red MPLS para poder trabajar si no que se usa para balancear el tráfico y proceder a enviar los paquetes más susceptibles a latencia por el canal más adecuado.

Figura 24

Arquitectura de Fortinet SD-WAN



Tomado de *(Gartner, 2019b)*

Cisco

SD-WAN de Cisco, brinda una arquitectura segura y escalable. A través de la consola de Cisco vManage, se puede conectar centros de datos, puntos remotos, e ISPs para ampliar la velocidad, seguridad y eficiencia de la red.

Además, cuenta con una administración centralizada segura, políticas en las aplicaciones y optimización en la conectividad hacia la nube.

La red Cisco SD-WAN hace un control riguroso de las amenazas y protección de datos dentro de la misma infraestructura, de tal forma la información no debe pasar por otros equipos de seguridad o ir aun data center para ser protegida.

Cisco presenta dos tecnologías de SD-WAN, Meraki y Viptela.

Meraki

Cisco Meraki SD-WAN es una excelente opción para proveedores de soluciones que tienen pequeñas empresas o clientes con WAN que buscan una mayor flexibilidad de red.

El panel de Meraki permite que un administrador pueda ver el consumo de ancho de banda y uso de aplicaciones para impulsar políticas de bloqueo, o incluir en listas blancas para optimizar la experiencia del usuario. La visibilidad y el control profundos proporcionan información real desde cualquier dispositivo con acceso a Internet.

Viptela

Esta solución de Cisco es orientada para organizaciones de gran tamaño, con sedes en varios países.

Separa la orquestación, el control, el reenvío y la administración en componentes discretos y unifica su funcionalidad bajo una sola estructura. Esto le da a la solución la capacidad de escalar a miles de sitios, automatizar los cambios de configuración en minutos y diseñar el tráfico para una conectividad óptima. Toda esta funcionalidad se combina con una arquitectura altamente resistente y altamente disponible. (Cisco, 2019b)

En la Tabla 6 se ha realizado una comparación de las características más importantes entre las dos tecnologías, como se había mencionado la elección dependerá del tamaño y servicio el cual está enfocada la empresa.

Tabla 6

Tabla comparativa entre Cisco SD-WAN, Meraki y Viptela

MERAKI MX	VIPTELA
Gestion Simple y Multifuncional	Altamente Flexible y Personalizable
Soporte de dos UPLINKS WAN	Soporte de 3 a 7 UPLINKS WAN
Panel único de gestión de Infraestructura completa (seguridad, WAN, conmutación, inalámbrico, y más)	Servicio de relacionamiento de L4 a L7
Proteccion con AMP (Advanced Malware Protection)	Optimización TCP y aceleración WAN
Cisco Snort IPS	Segmentación altamente flexible y personalizable, topologías en base VRF
URL filtering Integrado	Soporte de Multicast sobre WAN
firewalling basado en Geo IP	Capacidades de VNF
Configuración y monitoreo intuitivos basados en GUI	Soporte de IPv6
Gestion en Nube	Gestion On premises y en Nube
CAPACIDADES COMPARTIDAS	
Desarrollo Layer 3 VPN overlay para hub and spoke	
Políticas de enrutamiento en L3 a L7 basadas en Rendimineto	
Independencia de transporte a través de una variedad de tipos de conexión	
Despliegue Zero touch y plantillas de Configuración	

Altamente escalable (más de 10,000 sitios)
Integración con Plataformas virtuales para AWS / Azure
Gestión de la nube pública

Capitulo III. Comparación entre SDWAN Y MPLS

Las dos tecnologías han evolucionado por la necesidad de disponer mejores servicios y conexiones. MPLS ha venido desempeñando un trabajo predominante y eficaz acorde a los requerimientos que los usuarios han demandado, es por eso que los ISPs están paulatinamente mejorando su infraestructura con el fin de ser competitivos frente a otras empresas que dan el mismo servicio y dependiendo del fabricante los equipos de border tienen una vida útil de entre 5 a 8 años, garantizando el posible crecimiento de ancho banda, velocidad, que se requerirá a futuro.

El acceso al internet es más demandado, pero con la aparición de aplicaciones en la nube, se está buscando como mejorar la red MPLS porque presenta latencia, lo que ocasiona una demora en la entrega de la información. Es por esto que SD-WAN soluciona este problema, siendo enfocado principalmente para aplicaciones alojadas en la nube.

En el presente proyecto se ha realizado pruebas para evidenciar el tiempo de respuesta que se toma en enviar un paquete por medio de una red MPLS y mediante la plataforma Meraki de Cisco, con ello se pudo evidenciar la ventaja que se tiene una tecnología con respecto de la otra, el análisis se presenta a continuación:

Configuración de SD-WAN en Cisco Meraki

Para realizar el análisis de SD-WAN, se ha utilizado el equipo Meraki MR33, como prueba se agregaron los nombres “Espe Latacunga” y “Espe Sangolquí”, que

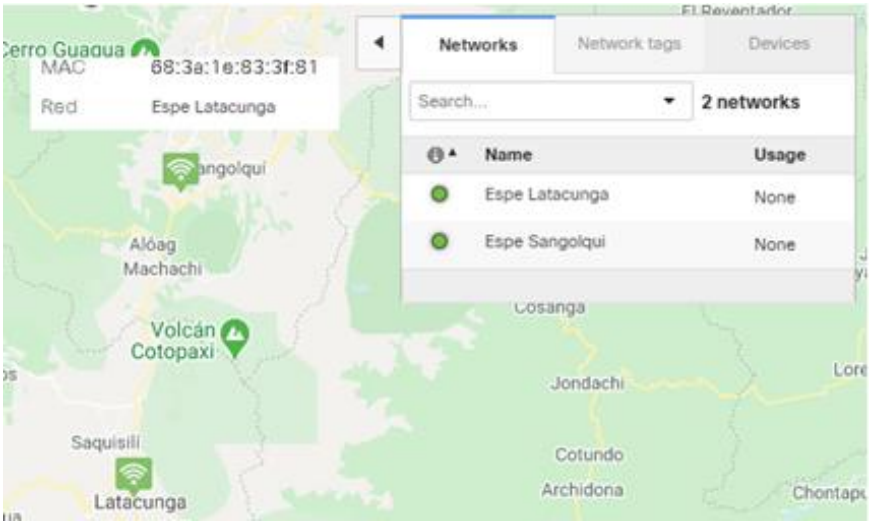
representan dos sucursales. Una característica de la plataforma Meraki es que nos muestra la ubicación de las dos redes en el mapa, para tener un mejor control y administración, tal como podemos apreciar en la Figura 25.

Figura 25

Cisco Meraki Mr33

Figura 26

Ubicación de redes en SD-WAN



Una vez agregado nuestros dispositivos por la serie de cada uno, veremos agregados en el dashboard de Meraki, tal como como se puede observar en la Figura26.

Figura 27

Dirección MACs de los equipos en cada sede

Dirección MAC	Modelo
68:3a:1e:83:3f:81	MR33
68:3a:1e:83:45:11	MR33

Direccionamiento IP

Configuramos el direccionamiento de nuestros equipos de forma estática dentro de la consola gráfica de Meraki (dashboar).

Figura 28

Direccionamiento IP

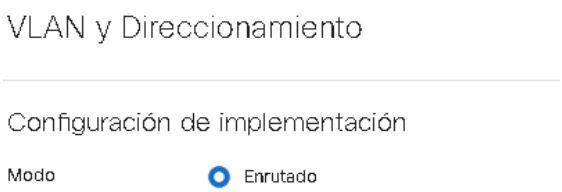
Selección de la capa de acceso y direccionamiento LAN

Una vez configurado el direccionamiento IP de la WAN procedemos a configurar la LAN, para ello vamos a la opción “Seguridad y SD-WAN” y dentro de las opciones seleccionamos “VLAN y direccionamiento”, en esta opción Figura 29,

elegimos “Modo Enrutado” para que el dispositivo trabaje en capa 3 y pueda traducir las direcciones a IP.

Figura 29

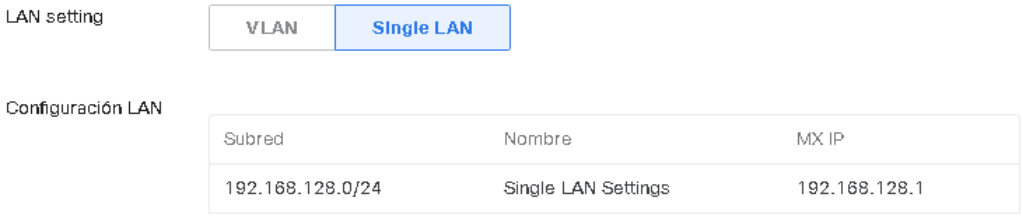
Selección del modo de trabajo de Meraki



Dentro de la misma ventana para nuestro caso se configuró la LAN en modo acceso sin definir una vlan, como se puede observar en la Figura 30.

Figura 30

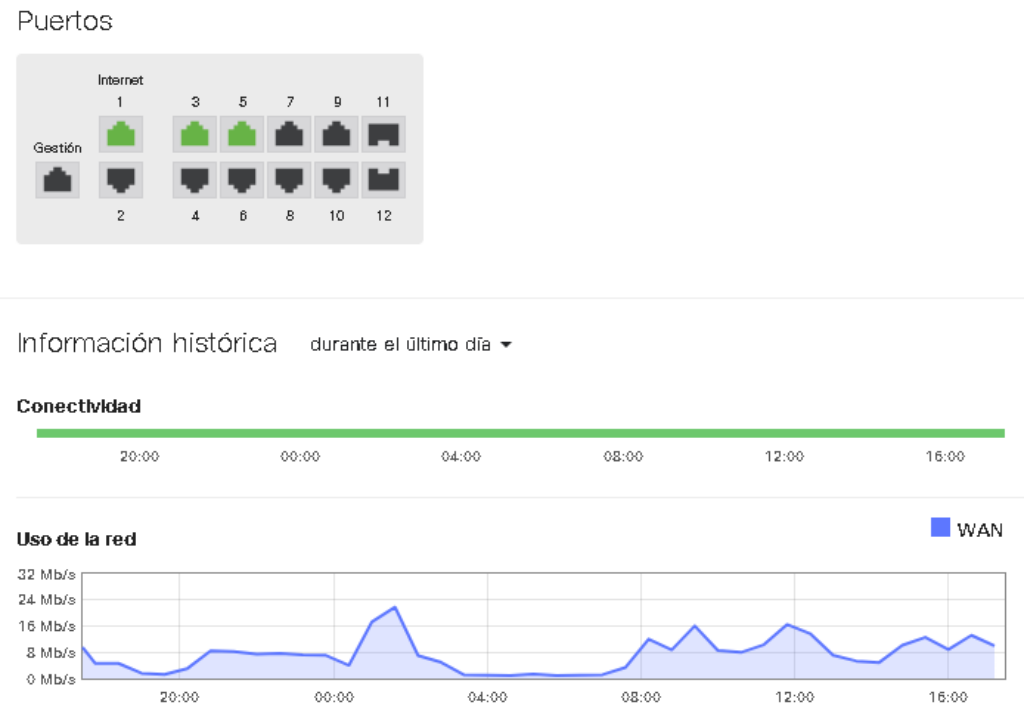
Configuración de la LAN



Al momento de terminar con la configuración del direccionamiento, los puertos se habilitan y el tráfico presentado lo podemos de manera gráfica Figura 31, sin requerir una aplicación adicional, esa es una venta de la plataforma SD-WAN de Cisco.

Figura 31

Monitoreo de las aplicaciones



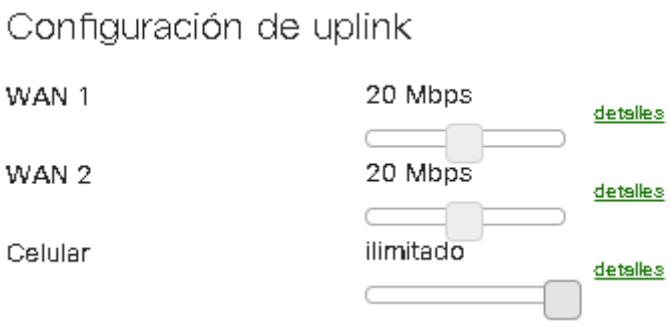
Balanceo de Carga

En la opción de direccionamiento IP, agregamos otra IP pública similar a lo indicado anteriormente, habilitando la WAN 2, para el proyecto se hizo uso de la red Movistar a través de un modem 3G con puerto Rj45.

Ingresamos a la opción de seguridad y SD-WAN para seguidamente seleccionar SD-WAN y modelado de tráfico, en donde limitamos el ancho de banda de las interfaces WAN 1 y WAN 2 a 20Mbps.

Figura 27

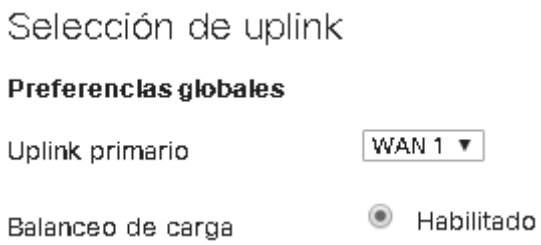
Balaceo de carga



Se procede a habilitar el balanceador de carga, para que el tráfico se extienda a través de ambos uplinks en la proporción configurada de 20Mbps.

Figura 32

Habilitación del balanceador

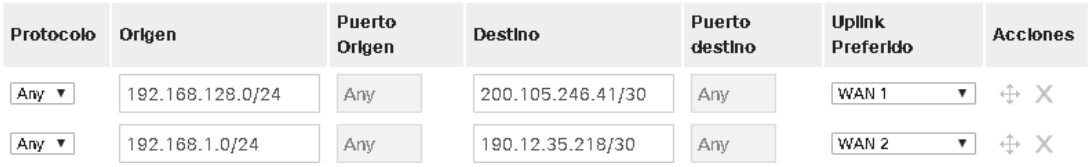


Traffic Shaping

Se configura la red de origen con el protocolo (TCP, UDP o cualquier) y destino para el puerto requerido que sea reenviado a través de la WAN especificada, logrando de esta manera redistribuir el tráfico deseado.

Figura 33

Traffic Shapping

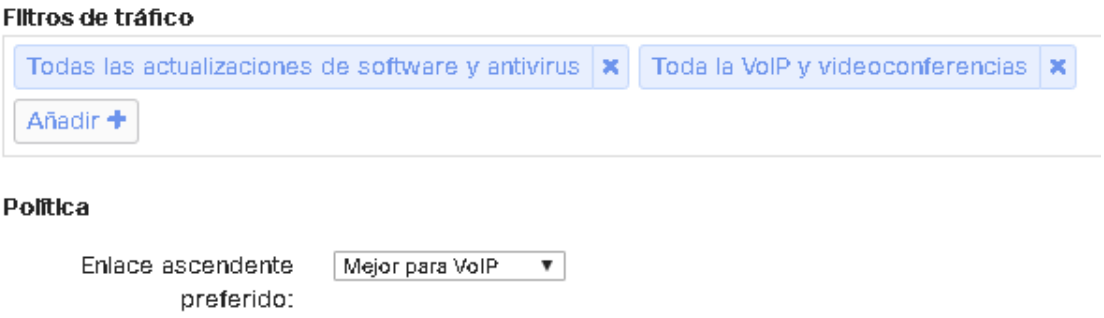


Políticas de tráfico

Se filtran los paquetes de acuerdo a la creación de políticas, para priorizar el ancho de banda, en especial atención para VoIP.

Figura 34

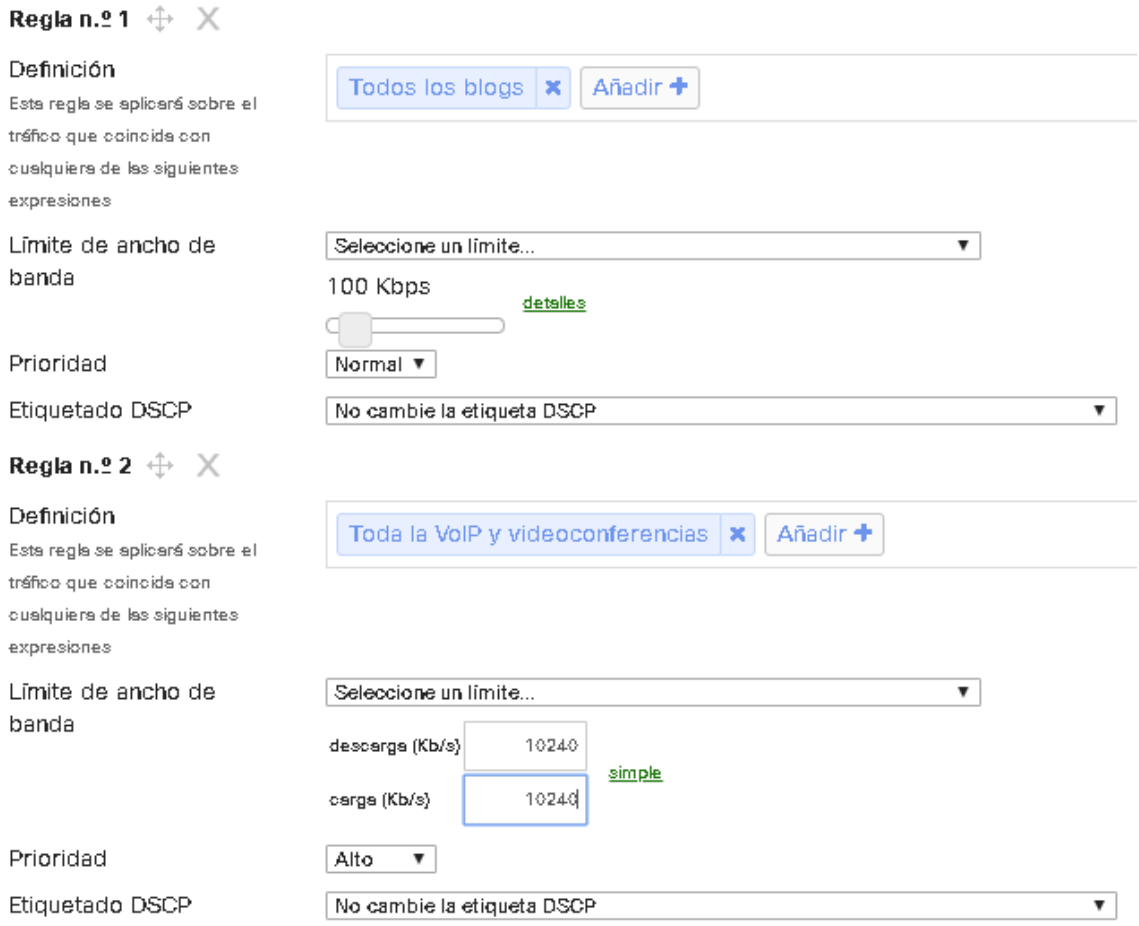
Políticas de tráfico



Se crean reglas para limitar el tráfico según la importancia, característica importante para priorizar la voz y el video, lo paquetes tendrán un ancho de banda mayor para ese servicio.

Figura 35

Definición de reglas



VPN

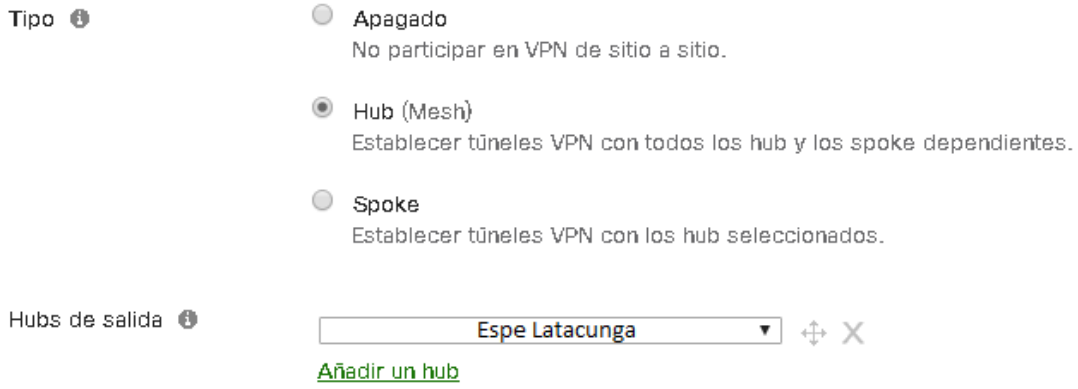
Para implementar una VPN en SD-WAN, ingresamos a Seguridad y SD-WAN, luego se selecciona VPN de sitio a sitio, en la cual se tiene 2 tipos de VPN y el Hub de salida que se muestra con el nombre de “Espe Latacunga” porque se tiene configurada esta función en dicha sede.

VPN tipo Hub

Para el presente proyecto se ha seleccionado tipo Hub, en el caso que se tuviera más sucursales y se haya activado dicha función, nos mostrará de forma automática para elegir la sede con su nombre distintivo que fue configurado.

Figura 36

Tipo de VPN



Al elegir tipo hub y la sede con dicha función previamente activada, se mostrará las redes de esa sede y ya se tendrá configurada la VPN.

Figura 37

Redes aprendidas

Firewall

Para la implementación de un control de seguridad ingresamos a Seguridad y SD-WAN, Firewall, se controla el tráfico de origen y saliente de los puertos de correos y se agrega una regla para bloquear el acceso de la red de invitados a la red interna.

Figura 38

Control de reglas Firewall

Configuraciones en MPS

Para verificar el comportamiento que tiene una red MPLS, se hará uso de routers cisco, mediante una red con enlace principal y redundante para Matriz y sus sucursales en Quito y Guayaquil.

Configuraciones en el CE

Se configura la interfaz a la cual se la asignará de WAN con su descripción referente si es principal o de respaldo.

```
interface FastEthernet0
 description ENLACE F.O.
 ip address 10.1.36.2 255.255.255.252
 duplex auto
 speed auto
```

Para el caso del respaldo en el caso que el canal principal no esté disponible, se configura otra interfaz con su ip.

```
interface FastEthernet1
 description ENLACE RADIO BK
 ip address 10.1.36.6 255.255.255.252
 duplex auto
 speed auto
```

Se configura una VLAN para anunciar la red LAN y asignamos a los puertos del router que tendrán acceso para la LAN.

```
interface Vlan10
 description LAN CLIENTE
 ip address 192.168.1.1 255.255.255.0
```

```
interface FastEthernet2
 switchport access vlan 10
!
interface FastEthernet3
 switchport access vlan 10
!
interface FastEthernet4
 switchport access vlan 10
!
interface FastEthernet5
 switchport access vlan 10
!
interface FastEthernet6
 switchport access vlan 10
!
interface FastEthernet7
 switchport access vlan 10
!
interface FastEthernet8
 switchport access vlan 10
!
interface FastEthernet9
 switchport access vlan 10
```

Se configura mediante el protocolo BGP y un sistema autónomo (AS) para este caso de 64600 y los parámetros para identificar las redes del enlace principal y de backup.

```
router bgp 64600
 bgp router-id 10.1.36.2
 bgp log-neighbor-changes
 neighbor 10.1.36.1 remote-as 65001
 neighbor 10.1.36.1 description Principal
 neighbor 10.1.36.5 remote-as 65001
 neighbor 10.1.36.5 description BackUp
 !
 address-family ipv4
 redistribute static
 neighbor 10.1.36.1 activate
 neighbor 10.1.36.1 route-map PRINCIPAL-IN in
 neighbor 10.1.36.5 activate
 neighbor 10.1.36.5 route-map BACKUP-IN in
 neighbor 10.1.36.5 route-map BACKUP-OUT-DATOS out
 no auto-summary
 no synchronization
 network 192.168.1.0
 exit-address-family
```

```
route-map BACKUP-OUT-DATOS permit 10
 set as-path prepend 64600 64600 64600
!
route-map BACKUP-OUT-DATOS deny 200
!
route-map BACKUP-IN permit 10
 set local-preference 200
!
route-map BACKUP-IN deny 200
!
route-map PRINCIPAL-IN permit 10
 set local-preference 2000
!
route-map PRINCIPAL-IN deny 200
```

Para poder monitorear el tráfico por medio de una aplicación como STG, se configura la comunidad, la que es específica para la ip de ese enlace.

```
snmp-server community PRUEBA RO
```

Configuración en el PE

En el PE se crea una VLAN y una vrf que es la etiqueta única dentro del PE, la vrf se mantendrá la misma en los PE para que todas las sucursales tengan comunicación una con otra, la VLAN si puede variar. La IP 10.1.36.1 es la red a la que pertenece la IP configurada en la interfaz FastEthernet 0 en el router cliente o CE inicialmente.

```
interface Vlan1020
 description Matriz Principal
 ip vrf forwarding dat1036
 ip address 10.1.36.1 255.255.255.252
```

En el PE cada red de la LAN de todas las sucursales se las configura mediante una ruta estática, indicando su máscara y Gateway del router CE en el cual se encuentra creada, si pertenece al mismo PE, caso contrario se coloca la IP al cual corresponde.

```
B     192.168.0.0/24 [200/0] via 172.29.0.22, 6w1d
B     192.168.1.0/24 [20/0] via 10.1.36.2, 7w0d
B     192.168.2.0/24 [200/0] via 172.29.0.64, 7w0d
```

Las configuraciones descritas son realizas en todos los CE y dependiendo del servicio que se requiere se puede agregar muchas más configuraciones como acl. QoS mediante línea de comando.

Ventajas

- SD-WAN presenta mayor agilidad
- El tiempo reducido en las instalaciones por medio soluciones SD-WAN
- El tiempo en diseño y configuración de equipos es mucho más rápido con SD-WAN
- Fácil implementación por medio de SD-WAN
- Mejora el rendimiento de la aplicación hacia la nube
- Eficiencia por parte del área del TI por medio de soluciones SD-WAN
- Registro de nuevos equipos sin enviar una especialista de red en SD-WAN

Desventajas

- Conexiones MPLS tienden a ser rígidas
- No se puede realizar un reconocimiento de aplicaciones directamente por los equipos router CE ni PE en MPLS
- Susceptibilidad a fallas por el ingreso de una línea errónea de comando
- Se deben hacer ajustes para restringir el tráfico

En el siguiente cuadro se hace un resumen comparativo de las ventajas y desventajas más relevante de las tecnologías SD-WAN vs MPLS.

Tabla 7

Tabla comparativa entre SD-WAN y MPLS

	SD-WAN	MPLS
Costo	Consolidación de servicios, su administración es centralizada basada en políticas.	El mantenimiento es costoso, un técnico especializado debe ir al lugar.
Escalabilidad	Permite aumentar fácilmente la capacidad según sea necesario.	Se requiere de un análisis para aumentar la capacidad lo que lleva más tiempo.
Rendimiento	Permite monitorear el estado del enlace y redirigir el tráfico según sea necesario directamente desde la plataforma.	MPLS presenta latencia dependiendo del número de saltos que requiera y para el monitoreo se requiere de otras aplicaciones.
Agilidad	Respuesta rápida a las solicitudes de nuevos servicios WAN.	La respuesta requiere tiempo para ofrecer un producto de acorde a lo solicitado.

Factibilidad de implementación de SDWAN en Puntonet

De acuerdo al estudio realizado, la red MPLS de Puntonet cuenta con una infraestructura adecuada, con equipos robustos, bajo normas TIER III con sistemas redundantes, lo que le permite ser unas de las empresas de internet con mayor aceptación en el mercado, entregando a los clientes un servicio de calidad a un costo muy asequible.

Los routers principales y de border de la red MPLS de Puntonet, permiten que redes SD-WAN trabajen conjuntamente bajo el mismo esquema sin hacer modificaciones, la diferencia es que, al trabajar bajo los mismos parámetros, no se aprovecharía al 100% de la nueva tecnología de SD-WAN, debido a que, si existe problemas de hardware o una línea mal configurada en un PE, la red se vería afectada drásticamente dependiendo del nivel de fallo que pueda presentar. Otro motivo es que de acuerdo al número de saltos que, de un paquete entre los PE hasta llegar a su destino, el tiempo de respuesta aumentaría y si la aplicación como el caso de voz o video demanda que la comunicación sea estable sin latencia, los paquetes llegarían en distintos tiempos, ocasionando que la voz se entre corte.

La implementación de SD-WAN en Puntonet es factible, se puede levantar una red SD-WAN a través de datos o internet sobre la red MPLS o independientemente a través de una red metro Ethernet entre diferentes ISP, todo va a depender del tipo de servicio que se vaya a ofrecer y cual sea su uso.

SD-WAN es factible implementar desde cualquier ámbito en Puntonet, por la tecnología que actualmente dispone, la cual fue descrita en el anterior capítulo, se puede tener una red híbrida entre las dos tecnologías o se puede implementar una red pura de SD-WAN.

Análisis Financiero operacional de la red SDWAN en Puntonet

Factibilidad financiera

En la siguiente tabla se presenta el costo que tendría en implementar la tecnología SD-WAN en comparación a la actual por MPLS, para ver si es rentable o no.

El análisis se ha hecho tomando en cuenta un enlace principal y de respaldo, con sus respectivos PE y CE.

En mano de obra para la solución SD-WAN se ha propuesto sin costo, debido a que la complejidad y tiempo que toma en montarlo es muy reducida en comparación a una implementación por MPLS.

Tabla 8

Costo de implementar SD-WAN

ÍTEM		PRECIO
1	Cisco Meraki MX65	$1314
2	Cisco Meraki MX65	$1314
3	Dashboard SD-WAN	$964
4	Licencia por un año	$350
5	Mano de obra / tiempo	
Costo		**3942**

Tabla 9

Costo de implementar MPLS

ÍTEM		PRECIO
1	Cisco 1811 CE	$200
2	Cisco 1811 CE	$200
3	Cisco ASR-920 PE	$2,689.11
4	Cisco ASR-920 PE, BK	$2,689.11
5	Mano de obra / tiempo	$300
Costo		**6078,22**

Como se puede apreciar en la tabla 8 y 9, la implementación de los equipos en referencia a costos es factible, se tiene que SD-WAN es un 64,87% más económico

que MPLS, porque no requiere routers ASR que son colocados dentro de la arquitectura MPLS en un ISP y además no se incluye el costo por establecer toda la ingeniería de tráfico presente en la tecnología tradicional.

Cabe mencionar que, si existe un error en una línea de comando en los CE, PE, el tiempo de detección del error y corrección influiría directamente al costo final, porque si los clientes tienen un SLA previamente establecido y se quedan sin servicio, van a requerir una compensación por ese tiempo y a pesar de disponer de un enlace redundante, se va a reflejar latencias.

Lo que no ocurrirá bajo un esquema SD-WAN, que se puede configurar una redundancia para que automáticamente si detecta problemas de latencia en una de las redes de transporte, proceda con el envío de los datos por la otra red.

Tir

La inversión inicial para el proyecto de implementación de SD-WAN es de $3942, a ese valor se suma costo por Mega, si se entrega 20Mb con compartición de 1 a 1 el valor mensual es de $220, con lo cual se tendrá un ingreso anual de:

Tabla 10

Ingresos anuales

Costo	Tiempo
$2640	Primer año
$2640	Segundo año
$2640	Tercer año

EL valor del TIR es del 45%, lo que quiere decir que el proyecto es rentable para la empresa, pero se debe mantener como mínimo al cliente 1 año y 3 meses para recuperar lo invertido.

Van

El valor del VAN lo calculamos en base al 16% de interés, con lo que obtenemos un resultado de $1.987,15, lo que nos refleja como resultado que mediante SD-WAN se logrará recuperar cartera y obtener ganancias.

Resultados

Al realizar un análisis entre las dos tecnologías MPLS y SD-WAN, se ha podido obtener varios datos que demuestran la eficacia que existe una de la otra y entender por qué el futuro de las redes se apunta a redes definidas por software.

Muchas empresas buscan la manera de reducir el costo operacional, pero a su vez como obtener mayores beneficios, es así que se presenta las siguientes pruebas:

Cálculos de rendimiento en la red MPLS

Se ha calculado varios parámetros para medir el rendimiento de la red por MPLS, los cuales son latencia, Jitter.

Se obtiene la latencia de 2 ms, midiendo el tiempo de retardo al hacer un ping entre el PE y una de las sucursales CE.

```
PNETUIOMTZPE04#ping vrf dat1036 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

De igual forma se hace una prueba desde el CE hacia el PE, obteniendo la latencia de 2ms.

```
Matriz#ping 10.1.36.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.36.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Calculamos el valor del Jitter realizando 6 prueba de ping desde el PE hacia el CE, con lo que se obtiene.

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/36 ms
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/16 ms
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/12 ms
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Tabla 11

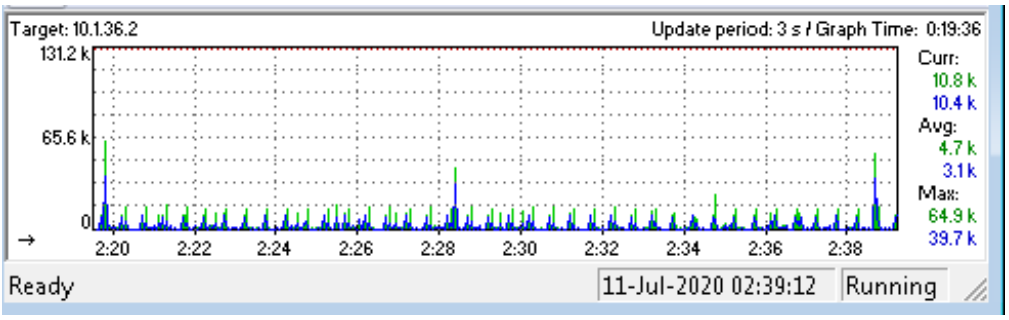
Cálculo del Jitter

PING	LATENCIA (ms)	JITTER
1	3	
2	9	6
3	5	-4
4	7	2
5	3	-4
6	2	-1

Para monitorear el tráfico se hace uso de la herramienta gratuita STG, en la cual permite además de ver el consumo del canal, ver las pérdidas de paquetes y si el enlace principal está activo o no por el tráfico existente.

Figura 39

Monitoreo del tráfico



Resultados de la red SD-WAN

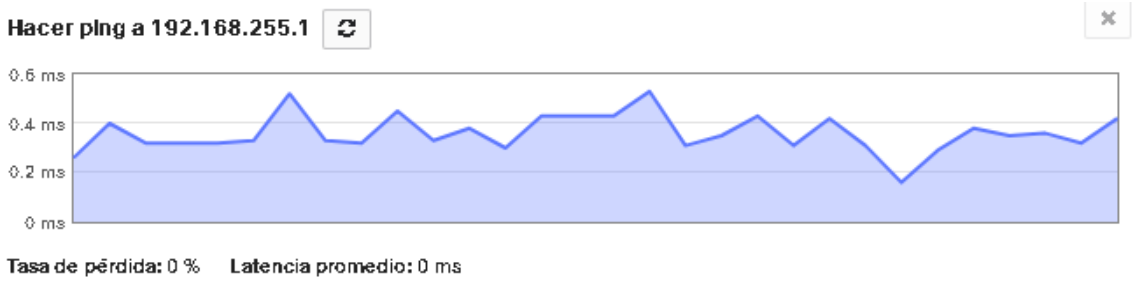
Las herramientas de SD-WAN son muy prácticas y sencillas de usar, como se lo ha visto en las pruebas realizadas para el proyecto presente.

Los resultados obtenidos de SD-WAN al hacer una prueba de latencia desde Matriz hacia la sucursal son muy bajos, alrededor de los 0.5ms, lo que demuestra que la red SD-WAN es mucho más óptima con una menor latencia que por MPLS.

Respondiendo a la pregunta de hipótesis, se ha comprobado que el tiempo de respuesta es mucho menor.

Figura 40

Prueba de latencia SD-WAN

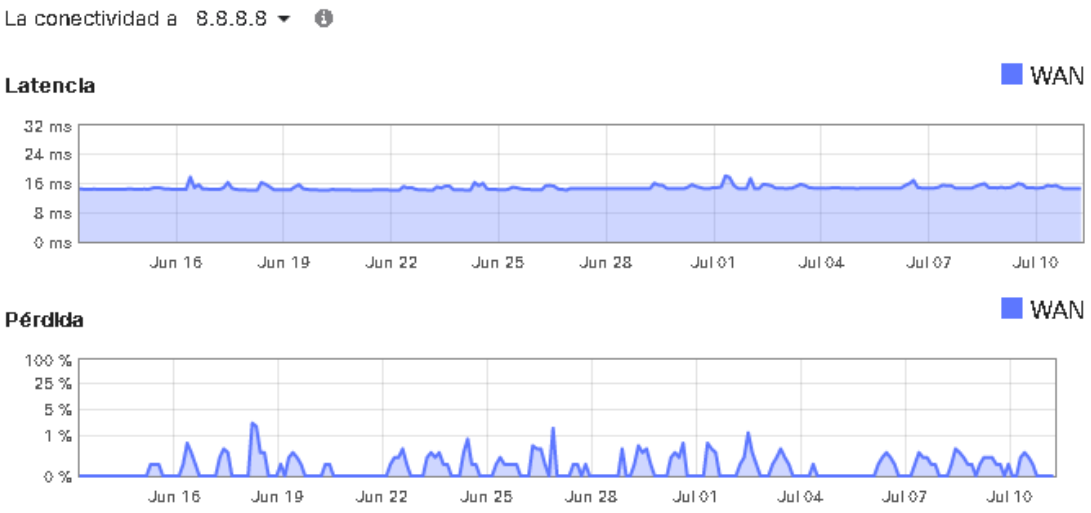


Una de las ventajas que tiene SD-WAN es que permite obtener un reporte de latencia y pérdidas de paquetes que se han presentado desde un período de tiempo,

con lo cual se puede saber el estado de la red en tiempo real y tomar decisiones en el acto.

Figura 41

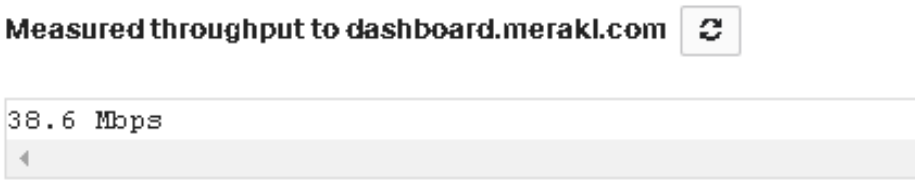
Información de estado de la red



El cálculo de la tasa real de trasferencia throughput para este ejemplo es de 38.6Mbps.

Figura 42

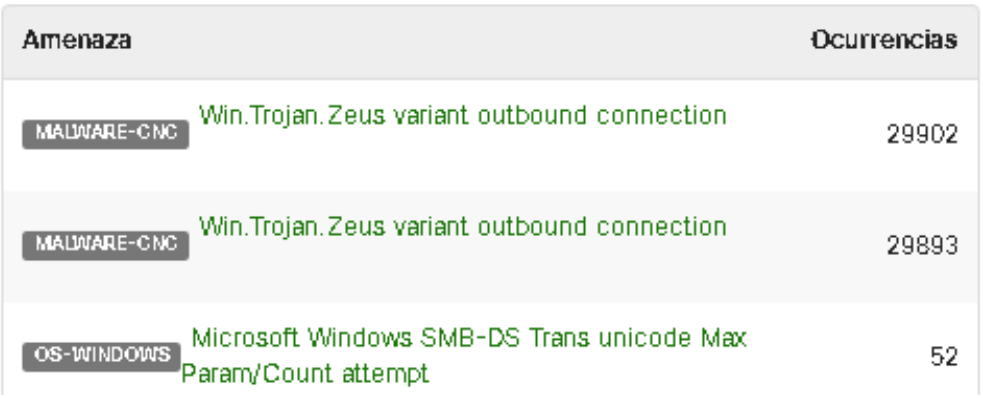
Throughput



En seguridad, el dashboard de SD-WAN presenta herramientas útiles para la detección de amenazas frecuentes con el número de ataques hacia la red, los equipos que han presentado mayor amenaza y control del spam sin requerir un firewall adicional.

Figura 43

Detección de Amenazas frecuentes

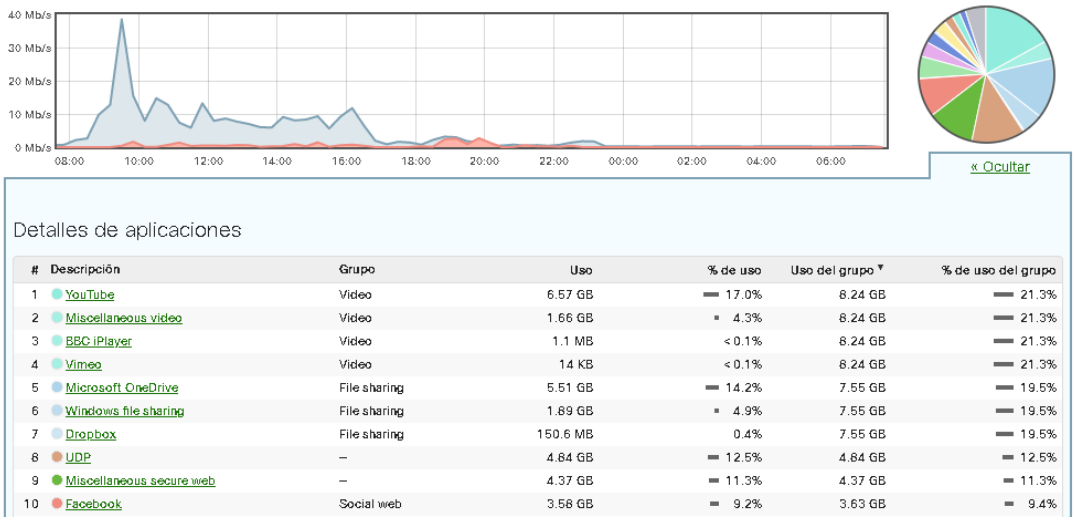


Amenaza	Ocurrencias
MALWARE-CNC Win.Trojan.Zeus variant outbound connection	29902
MALWARE-CNC Win.Trojan.Zeus variant outbound connection	29893
OS-WINDOWS Microsoft Windows SMB-DS Trans unicode Max Param/Count attempt	52

Con el filtrado de aplicaciones se puede determinar cuál es la que ha presentado una mayor demanda, por el cual se puede asignar un ancho de banda específico para esa aplicación si así se lo requiere.

Figura 44

Filtrado de aplicaciones



#	Descripción	Grupo	Uso	% de uso	Uso del grupo	% de uso del grupo
1	YouTube	Video	6.57 GB	17.0%	8.24 GB	21.3%
2	Miscellaneous video	Video	1.66 GB	4.3%	8.24 GB	21.3%
3	BBC iPlayer	Video	1.1 MB	< 0.1%	8.24 GB	21.3%
4	Vimeo	Video	14 KB	< 0.1%	8.24 GB	21.3%
5	Microsoft OneDrive	File sharing	5.51 GB	14.2%	7.55 GB	19.5%
6	Windows file sharing	File sharing	1.89 GB	4.9%	7.55 GB	19.5%
7	Dropbox	File sharing	150.6 MB	0.4%	7.55 GB	19.5%
8	UDP	–	4.84 GB	12.5%	4.84 GB	12.5%
9	Miscellaneous secure web	–	4.37 GB	11.3%	4.37 GB	11.3%
10	Facebook	Social web	3.58 GB	9.2%	3.63 GB	9.4%

En base al análisis realizado entre ambas tecnologías, se puede decir que MPLS es adecuado para clientes pequeños o de hogar, que no demanden de un filtrado de

paquetes más detallado, ni para aquellos en el cual su rol de negocio no se base en aplicaciones en la nube y el lapso de tiempo que pueden estar sin servicio no les afecte mayormente, como en el caso de una florícola que si requiere disponer del servicio de internet para poder ofertar sus productos vía video llamada y para el grupo de empresas que requieren tener un mayor control de la red, con baja latencia y el reemplazo de un equipo no demanda mayor tiempo que representa un costo, al trasladar al técnico a un lugar alejado para el cambio del equipo.

Otro punto a destacar es la facilidad para configurar un balanceador de cargar, a través de su dashboard, que de manera muy intuitiva se pueden ejecutar procesos para asignación de un límite de ancho de banda para cada interfaz WAN e incluso mediante una red 3G, lo que no ocurre con MPLS que el trabajo toma más tiempo, un mayor conocimiento de la red y para permitir la posibilidad de usar una red 3G para el balanceo, se requieren de equipos adicionales.

Capítulo V. Conclusiones y Recomendaciones

Conclusiones

Mientras en una red MPLS se genera un retardo en el tiempo por el circuito de enrutamiento del data center de un ISP para llega a su destino, el diseño SD-WAN simplifica esa tarea por una reducción o eliminación de enrutadores individuales, con una mayor eficiencia de ancho de banda, permitiendo que las aplicaciones en la nube sean más dinámicas y ágiles con seguridad y privacidad de dato, permitiendo niveles muy alto de rendimiento.

La configuración de enrutadores y puertas de enlace de forma individual, obliga al desplazamiento de personal a otros lugares para instalar nuevos equipos, en tanto que con el sistema de SD-WAN, el diseño, implementación y administración de nuevos equipos se lo hace desde una ubicación central, lo que incide en la eficiencia de la demanda comercial.

La incertidumbre por el desconocimiento de la tecnología SD-WAN se desvirtúa por la garantía del ancho de banda, por el control de la ruta diferenciada que toma el tráfico de red para cada transmisión más dinámica, y por la capacidad que tiene el sistema de seleccionar entre el tráfico de aplicaciones o usuarios según sea su prioridad, por ejemplo, entre el manejo de transacciones comerciales o aplicaciones para seguridad de archivos.

La tecnología incorporada por Puntonet y su historia en el servicio de internet, le garantizan la capacidad de cumplir con todos los requisitos actuales y fututos para el desarrollo del proyecto SD-WAN.

La capacidad de gestión basada en políticas y selección de rutas, permiten llegar a un equilibrio adecuado entre costo, confiabilidad y rendimiento para una mezcla diversa de tráfico de aplicaciones.

La administración centralizada, permite poner más o menos tráfico en enlaces de banda ancha en cualquier momento sin tener que reconfigurar enrutadores y puertas de enlace de forma individual.

El sistema de SD-WAN reduce costos en el mantenimiento continuo del sistema, pues los técnicos no tienen que desplazarse para implementaciones pudiendo hacerla desde la oficina.

SD-WAN reduce costos al proporcionar conectividad multi punto utilizando puntos de control y de intercambio de datos privados bridando acceso seguro y local a los usuarios desde la red o la nube.

Recomendaciones

A medida que la tecnología evoluciona y el requerimiento de aplicaciones en la nube sea mayor, exige un cambio de tecnología a SD-WAN que requiere de varios componentes: SD-WAN Edge, controlador SD-WAN, orquestador de servicios, SD-WAN Gateway, portal web, cada uno con sus características propias de aplicación que proporcionan seguridad, eficiencia del servicio y optimización de recursos.

Referencias

Bau, D. N. (2016). Evolución del mercado de SD-WAN. *Juniper*.

Black, U. D. (2002). *MPLS and label switching networks*: Prentice Hall PTR.

Castellote, E. (2018). El mercado SD-WAN y su potencialidad

en EMEA.

CheckPoint. (2019). Firewall CheckPoint.

Cisco. (2008). MPLS Label Distribution Protocol (LDP).

Cisco. (2010). Cisco ME 3600X Series Ethernet Access Switches.

Cisco. (2014a). CISCO 7606.

Cisco. (2014b). IGP and EGP Routing Protocols.

Cisco. (2016a). Multiprotocol label switching mpls.

Cisco. (2016b). Resource Reservation Protocol (RSVP).

Cisco. (2017). Cisco NCS 5000 Series.

Cisco. (2018a). Cisco ASR 920 Series Aggregation Services Router.

Cisco. (2018b). Pronóstico anuál de VNI (Visual Networking Index).

Cisco. (2019a). ASR-9010.

Cisco. (2019b). Cisco SD-WAN, Viptela.

Cisco. (2020). Reporte sobre tendencias globales en redes

del Olmo Bautista, J. (2019). Presente y futuro de las redes WAN: SD-WAN y NFV.

Dennis Smith, D. K., Lisa Pierce. (Mayo 2019). Invierta en redes para logar el éxito en el negocio digital, Gartner.

Duda, T. (2015). Quality of Service in IP Networks.

Fortinet. (2019). FortiGate NGFW: Enterprise Firewalls.

Fortinet. (2020). SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2020.

Garcia, L. G. Y., Nossa, L. P., & Telemática, I. MULTI PROTOCOL LABEL SWITCHING (MPLS).

Gartner. (2019a). Cuadrante de Gartner en Firewall.

Gartner. (2019b). Magic Quadrant for WAN Edge Infraestructure.

Gordeychik, S., & Kolegov, D. (2018). SD-WAN Threat Landscape. *arXiv preprint arXiv:1811.04583*.

Gordeychik, S., Kolegov, D., & Nikolaev, A. (2018). SD-WAN Internet Census. *arXiv preprint arXiv:1808.09027*.

Guichard, J., Pepelnjak, I., & Apcar, J. (2003). *MPLS and VPN architectures* (Vol. 2): Cisco Press.

IDC. (2019). Pronóstico de datos y dispositivos de Iot a nivel Mundial. *International Data Corporation*.

Jiménez Vázquez, Y. (2010). *Propuestas de mejora en la red MPLS de Cienfuegos.* Universidad Central" Marta Abreu" de Las Villas.

Lacnic. (2017). SD-WAN, Software Defined WAN.

Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., . . . Heinanen, J. (2002). *Multi-protocol label switching (MPLS) support of differentiated services*. Retrieved from

Marr.B, O. (2019). SD-WAN, Principales conceptos y modelo de funcionamiento. https://ostec.blog/es/seguridad-perimetral/sd-wan-conceptos-funcionamiento.

Mef. (2017). Understanding SD-WAN Managed Services.

Murphy, S. L., & Badger, M. R. (1996). *Digital signature protection of the OSPF routing protocol.* Paper presented at the Proceedings of Internet Society Symposium on Network and Distributed Systems Security.

Naggi, R., & Srivastava, R. (2018). SD-WAN The Networking Blueprint for Modern Businesses.

Netblogrk. (2018). Sd Wan, Conceptos Básicos Y Arquitectura.

Networks, J. (2019). MPLS VPN Overview.

Networks, M. (2020a). IS-IS.

Networks, M. (2020b). RSVP-TE.

networks, P. a. (2019). Firewalls.

Oña Piña, G. D. (2016). *Diseño y comparación de redes de acceso MPLS y Metro Ethernet integradas a un backbone MPLS para un proveedor de servicios y realización de un prototipo base.* Quito, 2016.

Orbit. (2019). Cuáles son las Los firewalls de Fortinet son de próxima generación, filtran el tráfico de red para proteger a una organización de amenazas externas. Al mantener las funciones de los firewalls con estado, como el filtrado de paquetes, el soporte de VPN, la supervisión de la red y las funciones de mapeo de IP, los NGFW también poseen capacidades de inspección más profundas que jas de una red SD-WAN. *Orbit*.

peak, S. (2019a). Architecting an Application-Driven WAN Edge.

Peak, S. (2019b). SD-WAN.

Smith, D., Mullooly, J., Jaeger, W., & Scholl, T. (2011). Label Edge Router Forwarding of IPv4 Option Packets *RFC 6178 (Proposed Standard)*: Internet Engineering Task Force.

solutions, B. n. (2020). MPLS Traffic Engineering.

Technology, R. (2020). What is SD-WAN.

Teldat. (2017). SD-WAN Solution.

USS. (2019). SDW-WAN Architecture. https://uss.com.ar/corporativo/sd-wan/.

velocloud. (2020). VMware SD-WAN.

Wood, M. (2017). How to make SD-WAN secure. *Network Security, 2017*(1), 12-14.

Xiao, X., Hannan, A., Bailey, B., & Ni, L. M. (2000). Traffic Engineering with MPLS in the Internet. *IEEE network, 14*(2), 28-33.

Ycict. (2018). Cisco ASR 920-4SZ A-Router.