Diseño e implementación de una red Hub and Spoke sobre tecnología SD-WAN

Ruano Chulde, Dayana Lizbeth

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Trabajo de titulación, previo a la obtención del título de Ingeniera en Electrónica y Telecomunicaciones

Ing. Aguilar Salazar, Darwin Leonidas Msc.

29 de febrero del 2024

Copyleaks

Plagiarism and AI Content Detection Report

04_Trabajo_Titulación_Ruano_Chulde_...

Scan details

Scan time:	Total Pages:	Total Words:
March 4th, 2024 at 14:52 UTC	49	12115

Plagiarism Detection

Types of plagiarism		Words
Identical	0%	6
Minor Changes	0%	5
Paraphrased	1.9%	225
Omitted Words	0%	0

AI Content Detection

Text coverage		Words
AI text	1.9%	228
Human text	98.1%	11887

Learn more

Plagiarism Results: (9)

¿Sabes qué es una VPN y cómo funciona? - Redes Sociales 0.5%

https://www.redes-sociales.com/sabes-que-vpn-como-funciona/

Ir al contenido Quiénes somos Publicidad Contacto Mkt Online Redes Sociales Altern...

T.3298.pdf?sequence=1&isAllowed=y 0.5%

https://repositorio.umsa.bo/bitstream/handle/123456789/12631/t.3298.pdf?sequence=1&isallowed=y

UNIVERSIDAD MAYOR DE SAN ANDRÉS FACULTAD DE CIENCIAS PURAS Y NATURALES CARRERA DE INFORMÁTICA PROYECTO DE GRADO "IMPLEMENTACIÓN DE UNA R...

UNIVERSIDAD MAYOR DE SAN ANDRÉS FACULTAD DE CIENCIAS PURAS Y N... 0.5%

https://docplayer.es/88405470-universidad-mayor-de-san-andres-facultad-de-ciencias-puras-y-naturales-carr...

Iniciar la sesión ...

Redes basadas en Software (SDN) 0.4%

https://informatica.ucm.es/data/cont/media/www/pag-103596/transparencias/redes-por-software-sdn.pdf

Ingrid Lerida Ccoyllo Sulca

IV Semana de la Informática 2018 Redes definidas por Software (SDN) Mg. Ing. Ingrid Ccoyllo Sulca CCSI CCNA Índice • • • • • Introducc...

DARWIN LEONIDAS AGUILAR SALAZAR

Firmado digitalmente por DARWIN LEONIDAS AGUILAR SALAZAR
Fecha: 2024.03.05 09:55:23 -05'00'

ING. DARWIN AGUILAR SALAZAR MGRT
DOCENTE TITULAR DEEL TC
DOCENTE TUTOR

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Certificación

Certifico que el trabajo de titulación: "**Diseño e implementación de una red Hub and Spoke sobre tecnología SD-WAN**" fue realizado por la señorita **Ruano Chulde, Dayana Lizbeth;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 29 de febrero del 2024

DARWIN LEONIDAS AGUILAR SALAZAR

Firmado digitalmente por DARWIN LEONIDAS AGUILAR SALAZAR
Fecha: 2024.02.29 15:17:28 -05'00'

Ing. Aguilar Salazar, Darwin Leonidas, Msc.

C. C 1103036826

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Responsabilidad de Autoría

Yo, **Ruano Chulde, Dayana Lizbeth**, con cédula de ciudadanía n° 0401856216, declaro/declaramos que el contenido, ideas y criterios del trabajo de titulación: "**Diseño e implementación de una red Hub and Spoke sobre tecnología SD-WAN**" es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 29 de febrero de 2024

.....

Ruano Chulde, Dayana Lizbeth

C.C.: 0401856216

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Autorización de Publicación

Yo **Ruano Chulde, Dayana Lizbeth**, con cédula de ciudadanía n° 0401856216, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: "**Diseño e implementación de una red Hub and Spoke sobre tecnología SD-WAN**" en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 29 de febrero de 2024

Ruano Chulde, Dayana Lizbeth

C.C.: 0401856216

Dedicatorias

Este trabajo está dedicado a la niña que se ha convertido en mujer, a la mujer que ganó una batalla contra sí misma, a la mujer que quiere volver a volar y soñar, a la mujer que hoy vence sus miedos, deja su pasado atrás y pinta una nueva historia. Con mucho amor y admiración por mí y para mí.

Ruano Chulde Dayana Lizbeth

Agradecimiento

Agradezco principalmente a Dios, para él toda honra y gloria, por ser guía y compañía, enseñarme el significado del amor, servicio y sacrificio.

A mi madre Marcela Chulde y mi padre Joffre Ruano, quienes, con su apoyo incondicional, amor, trabajo y comprensión han estado conmigo en cada etapa de mi vida. A mis hermanas Alexandra y Leydi por ser ejemplo de valentía y lucha constante. A mi hermano Alejandro por animarme y confiar en mí. A mis sobrinos Joselyn, David y J. Alberto que llenan mi vida de sonrisas y esperanza, como también a J. Francisco que ahora desde el cielo se ha convertido en mi angelito y me ha permitido valorar cada instante. A mi tía Rocío y mis primos Diana, Johana y Said por brindarme apoyo, compañía y un segundo hogar.

A mis amigos de la universidad Andrés, Jonathan y compañeros que logré conocer en el baloncesto, quienes me brindaron su amistad durante todos estos años. En especial a Andrés quien se convirtió en mi enamorado y es un pilar fundamental en mi vida. A mis amigas Alejandra, Melani y Stefy quienes a pesar de los años continúan con su amistad sincera. A mis compañeros de trabajo que me apoyaron para poder finalizar esta etapa universitaria.

A mi tutor Darwin Aguilar, quien con su guía, confianza y apoyo me ha brindado la oportunidad de finalizar este trabajo de titulación, como también brindar su amistad, conocimiento y consejos en el trayecto estudiantil como profesional. Agradezco a todos los compañeros y docentes de la Universidad de las Fuerzas Armadas ESPE por formar parte de este desarrollo profesional de nuevos profesionales en el mundo.

Ruano Chulde Dayana Lizbeth

Contenido

Índice De Tablas

Índice De Figuras

Resumen

En la actualidad, el crecimiento de las redes corporativas a nivel mundial es inevitable debido al aumento de dispositivos y el procesamiento de grandes cantidades de datos, lo cual ha demandado mayores recursos de almacenamiento y ancho de banda, entre otras características. Por ello, han surgido paradigmas para la gestión centralizada de los componentes de una red mediante plataformas tecnológicas administrables, centralizadas y dinámicas, como es SD-WAN (Red de área amplia definida por software). La utilización de SD-WAN simplifica la operación y gestión de una red de área amplia (WAN) al separar el mecanismo de control del hardware de la red, lo que a su vez mejora la gestión y operación de los centros de datos. Una de las principales ventajas de SD-WAN es su capacidad para permitir a las empresas construir WAN de alto rendimiento utilizando un acceso a Internet rentable, brindando así la oportunidad de reemplazar costosas tecnologías de conexión como MPLS, ya sea parcial o totalmente. Por tal motivo, el objetivo de este proyecto es, mediante el diseño e implementación de una red Hub and Spoke utilizando la tecnología de SD-WAN con equipamiento Cisco para un cliente corporativo, mejorar la conectividad de Internet en cada sucursal mediante el control del tráfico entre ubicaciones en función de los requisitos establecidos por el cliente y la disponibilidad de la WAN. Con el diseño e implementación de esta red, se obtendrá valores de los siguientes indicadores: latencia, seguridad, costo y QoS con el objetivo de realizar un análisis del desempeño de la tecnología SD-WAN y presentar su resultado para proponer su empleo en futuros diseños de red para clientes corporativos de proveedores de servicios de internet corporativo.

Palabras Clave: Red de área amplia definida por software, multiprotocolo de conmutación de etiquetas, Topología de concentrador y radios.

Abstract

Currently, the growth of corporate networks worldwide is inevitable due to the increase in devices and the processing of large amounts of data, which has demanded greater storage resources and bandwidth, among other characteristics. For this reason, paradigms have emerged for the centralized management of network components through manageable, centralized and dynamic technological platforms, such as SD-WAN (Software Defined Wide Area Network). By dismantling the control mechanism of network hardware, SD-WAN streamlines the management and operation of data centers, resulting in a simplified wide area network (WAN). A key benefit of SD-WAN is its ability to facilitate the creation of high-performance WANs using cost-effective Internet access, presenting businesses with the option of replacing expensive connection technologies such as MPLS, either partially or entirely. For this reason, the objective of this project is, through the design and implementation of a Hub and Spoke network using SD-WAN technology with Cisco equipment for a corporate client, to improve Internet connectivity in each branch by controlling traffic between locations based on customer-established requirements and WAN availability. With the design and implementation of this network, values of the following indicators will be obtained: latency, security, cost and QoS with the objective of carrying out an analysis of the performance of the SD-WAN technology and presenting its results to propose its use in future designs network for corporate clients of corporate internet service providers.

Keywords: Software defined wide area network, multiprotocol label switching, Hub and spoke topology

Capítulo I: Introducción

Las redes definidas por software SDN (Software Defined Network) permiten el control inteligente de la red dentro de esta arquitectura, asegurando una gestión constante e integral de la red, independientemente del acceso o medio disponible en cada punto remoto.

Una de las redes más extendidas, definidas por un software es (SD-WAN), que permite la simplificación de las redes, mejorando el rendimiento de las aplicaciones que utilicen internet, desvinculando los servicios del software que se basan en un hardware subyacente gestionando el funcionamiento de aplicaciones programables, de redes configuradas de forma remota en su automatización del enrutamiento, menorando el gasto operativo, rendimiento de red, servicio, y enlaces de internet.

Antecedentes

Actualmente cada vez más la sociedad es más consciente de la importancia de mantener una conectividad online eficaz, segura y fiable, para una correcta comunicación y accesibilidad a información. En este sentido, puede que para las empresas la interconectividad resulte primordial, sobre todo entre sucursales y la matriz, sin límites de ubicación. En el mundo de la tecnología se han desarrollado múltiples formas para mantener conectados a las empresas descentralizadas por oficinas.

La conectividad en redes de área Amplia (WAN) ha evolucionado con el objeto de obtener una funcionalidad más sencilla y segura, pues, ahora el Internet es un medio común para unir sectores empresariales distantes. Pero con todo ello y las nuevas exigencias ha quedado rezagado con el aparecimiento de la nube, pues, ya no resulta eficiente, dado que pernoctan nuevas necesidades de almacenaje, transformación digital y servicios debido a la proliferación de aparatos móviles que buscan acceder a las redes (Zheng , 2017).

Las redes de datos han evolucionado vertiginosamente, muchas de las aplicaciones se pueden trasladar directamente a la nube, aumentando de forma exponencial los servicios que demandan de un ancho de banda eficaz, lo que conlleva a redes complejas, haciendo difícil la definición de una infraestructura y la gestión de estos. “E*n este contexto, es importante agregar que actualmente el mercado demanda una mayor agilidad, flexibilidad y control de los servicios de red, sin olvidarse de la seguridad y la reducción de costos*” (Jiménez, 2020).

Frente a esta dinámica de comportamiento y exigencias tecnológicas, parte la necesidad de generar nuevas tecnologías en el ámbito de sistemas y redes comunicacionales que reemplacen redes tradicionales como es la WAN. Es así como nace la tecnología SD-WAN (Software Defined – Wide Area Network), plataforma que admite la tenencia de varios servicios, conectividad como datos, Internet y red MPLS tradicional. La SD-WAN aísla el centro de control de datos, lo que implica que los servicios pueden seguir operando sin problema, a pesar de no contar con una conexión con la plataforma, creando una experiencia única y valor al usuario. Este se puede administrar de forma centralizada a través de un software para solucionar cualquier problemática de forma rápida y sencilla (Romero & Cuenca, 2020).

“Por el contrario, implementar una arquitectura de red de área amplia (WAN) a través de un servicio en la nube ofrece ahorros sustanciales de tiempo y costos, estableciendo un marco confiable para utilizar aplicaciones corporativas y garantizando una infraestructura de seguridad sólida” (Netec, 2019).

Graaff (2021) manifiesta que por medio de la SDN "Redes definidas por software" se puede configurar y ejecutar una amplia gama de configuraciones para la red de forma centralizada, es decir, lo que antes se realizaba a través de componentes de hardware, la WAN se controla mediante software. Haciendo posible el desarrollo de aplicaciones o uso de tipologías que permitan el uso eficaz y eficiencia para dar respuesta rápida a necesidades de control, centralización, sobre todo respuesta segura y confiable de datos e información.

Como se mencionó anteriormente, SD-WAN es una plataforma que posibilita la configuración mediante un software, por lo que tomando en cuenta los requerimientos de los clientes corporativos de agilizar proceso de transferencia de datos y otros, se plantea el diseño e implementación de una de las topologías WAN, de red estrella *Hub and Spoke* denominado a si en referencia a la rueda de una bicicleta donde Hub es el eje central de la rueda y spoke los radios que salen desde el centro de los ejes. *“Esta es una versión que permite que un sitio central se interconecte con sitios de sucursal utilizando enlaces punto a punto. Lo que implica que, los sitios de sucursal no pueden transferir o intercambiar datos con otros sitios de sucursal sin pasar por el sitio centra*l” (CCNA, 2019).

Planteamiento del problema

La globalización tecnológica y cambios continuos ha propiciado ambientes que han obligado a las empresas a trabajar bajo interconexión con las sucursales, oficinas u otros sitios desconcentrados ubicados en diferentes partes del país o lugar del mundo por medio de una solución SD-WAN; todo esto debido al alto uso de servicios en la nube, nuevos hábitos de subsistencia de los usuarios como el teletrabajo y aumento de requisitos de ancho de banda que necesitan de topologías de red revolucionarias, frente a lo cual es importante la implementación de una solución SD-WAN.

Por medio del sistema SD-WAN se puede controlar la WAN de forma centralizada, o "programada", mediante aplicaciones software. A pesar de ello, actualmente no se encuentran de forma estándar, pues, dependiendo del desarrollador o fabricante de la solución se crea una aplicación (Netec, 2019).

Por otra parte, el cliente corporativo de la empresa PuntoNet S. A., presenta problemas de administración de los requisitos de comunicación y seguridad, así también en la centralización de servicios, haciendo que no se pueda compartir entre diferentes cargas de

trabajo, además de operar con una conexión de red privada entre varios sitios con múltiples circuitos donde cada punto requiere una propia interfaz de hardware este a la vez demanda de múltiples routers con tarjetas de interfaz WAN, lo cual es muy costoso para la organización. A esto se suma, los frecuentes inconvenientes por corte de red de comunicación de cualquier sucursal que opera en el país, lo que provoca retratos en procesos de atención al usuario que termina en reclamos o denuncias.

Justificación

"*En la actualidad, las redes han experimentado un crecimiento exponencial tanto en tamaño como en su complejidad, llevando a las arquitecturas de red tradicionales a su límite, generando problemas en los aspectos de control y organización en los recursos tecnológicos*" (Guanoluisa, 2019). Además, con el desarrollo constante de las tecnologías de la información y la comunicación (TIC) permite la creación de aplicaciones y servicios que requieren la implementación automatizada e individualizada de recursos en la red. "*Sin embargo, la infraestructura tradicional o heredada presenta dificultades de innovación como consecuencia del costo que implicaría su adaptación, por lo tanto, es necesario encontrar alternativas que administren eficientemente los recursos existentes*" (Mora, et al., 2019).

Por otro lado, "En el panorama empresarial actual, la conectividad corporativa sigue siendo crucial para las empresas, ya que la transformación digital y el auge de las tecnologías en la nube dan lugar a nuevas demandas relacionadas con los servicios de conectividad de redes de área amplia (WAN)" (Olmo, 2019). Los requisitos de conectividad dentro del panorama empresarial corporativo han progresado hasta un punto en el que los administradores de redes ya no pueden satisfacer estas demandas únicamente mediante el uso de servicios privados MPLS WAN para vincular oficinas remotas o centros de datos (Rodríguez, 2019).

“Para satisfacer las necesidades tecnológicas de los clientes, las redes corporativas deben sufrir una transformación hacia una tecnología más dinámica que ofrezca mayor agilidad y flexibilidad. Esto incluye integrar una visibilidad mejorada, una plataforma de gestión centralizada y garantizar la seguridad manteniendo la rentabilidad” (Romero I. , 2017). A raíz de estas necesidades, “El concepto de Redes Definidas por Software (SDN) ha dado lugar a diversos paradigmas, como SD-WAN y SD, que permiten la gestión centralizada de los componentes de la red a través de plataformas tecnológicas dinámicas y totalmente gestionables*”* (Barrera, et al., 2019).

Las empresas que buscan una solución rentable y optimizada para sus sedes están recurriendo a SD-WAN. Esta innovadora tecnología utiliza herramientas basadas en la nube para enrutar eficientemente el tráfico entre dispositivos en una WAN multiservicio o multiproveedor. Con control centralizado, los administradores de red pueden configurar fácilmente el tráfico en función de políticas y reglas de seguridad, lo que reduce la inversión de capital y simplifica las operaciones (Rohyans, et al., 2017).

Cisco es uno de los proveedores líderes de tecnología SD-WAN y ofrece una solución basada en software que incluye una única superposición que conecta el centro de datos, la nube y las sucursales de la empresa. Esta solución enruta de manera eficiente el tráfico físico y virtual, brinda visibilidad integral de la red y garantiza una experiencia de usuario consistente, segura y de alta calidad en todas las ubicaciones. Conocido como Cisco Meraki SD-WAN, sus principales ventajas incluyen ahorros de costos para la empresa y el potencial de mejorar las operaciones comerciales al brindar servicios superiores (Datacom, 2018).

Consecuentemente, “*el desarrollo de este proyecto es importante debido a que este diseño de red sirve para mejorar el rendimiento de las redes corporativas actuales, además, se analizan nuevos conceptos, los cuales aportan al entendimiento de un nuevo tipo de arquitectura*” (Datacom, 2018). Con el estudio de redes WAN definidas por software se puede

solucionar las limitaciones que hoy en día presentan las redes de datos. Además, en Ecuador son pocas las empresas que tienen implementada esta nueva tecnología de redes definidas por software, con el proyecto propuesto se diseña e implementa un Software-Definition Networking in a wide área network (SD-WAN) en la red de un cliente corporativo de un proveedor de servicios de internet (ISP), para demostrar su funcionalidad, viabilidad y el bajo costo de implementación que presenta para futuras aplicaciones en el país.

Alcance

La presente investigación tiene como alcance proponer un proyecto tecnológico que satisfaga los requerimientos del cliente corporativo de la empresa proveedora de servicios de internet, para lo cual se realiza el diseño e implementación de una red Hub&spoke sobre SD-WAN, esto comprende desde la presentación de aspectos teóricos hasta un análisis de la red SD-WAN implementada a fin de validar sus beneficios.

Objetivos

Objetivo general

Diseñar e implementar una red Hub and Spoke sobre SD-WAN para un cliente corporativo de la empresa proveedora de servicios de internet nacional.

Objetivos específicos

- Realizar un estudio previo sobre la red WAN definida por software (SD-WAN), red Multiprotocol label switch (MPLS) y red privada virtual (VPN).
- Diseñar la red Hub and Spoke sobre SD-WAN cumpliendo con los requisitos del cliente corporativo de una empresa proveedora de servicios de internet nacional.
- Implementar el diseño de la red Hub and Spoke sobre SD-WAN utilizando como hardware equipos Cisco.

- Analizar y verificar métricas de QoS (Calidad de Servicio) y seguridad con el fin de comenzar a implementar la tecnología de SD-WAN en futuras redes.

Resumen de contenidos

Primer Capítulo

En este capítulo, brindaremos una descripción general concisa de la importancia y la lógica detrás de este proyecto, junto con el contexto y los esfuerzos relevantes que se han llevado a cabo. Profundizaremos en los objetivos específicos descritos anteriormente y proporcionaremos un desglose completo de los propósitos que pretenden cumplir.

Segundo Capítulo

El capítulo II, presenta una recopilación de teoría e información sobre todo lo relacionado con las redes definidas por WAN (SD-WAN), redes WAN, redes SDN. Se describirá las características de la tecnología SD-WAN y comparación con otras tecnologías como MPLS y VPN.

Tercer Capítulo

En este capítulo se describe los antecedente y requisitos de la red del cliente corporativo para poder desarrollar el diseño de la red hub and spoke sobre la tecnología SD-WAN, como también la selección del equipamiento para la implementación del diseño y se describe el proceso para la implementación.

Cuarto Capítulo

El cuarto capítulo, abarca la descripción de la funcionalidad del diseño e implementación de la red hub and spoke bajo la tecnología SD-WAN, como los resultados de las pruebas para verificar el control de tráfico, latencia y seguridad de la red.

Quinto Capítulo

El quinto capítulo concluye con un análisis integral de los resultados, acompañado de la formulación de conclusiones en base a los objetivos establecidos. Además, se presentan recomendaciones para asegurar el progreso continuo del proyecto.

Capítulo II: Marco Teórico

Las redes de telecomunicaciones desempeñan un papel fundamental como el motor de la conectividad global en la era digital, permitiendo la transmisión eficiente de datos, voz y video a través de diversas tecnologías. Han experimentado una evolución constante que redefine la forma en que las personas, empresas y dispositivos se comunican.

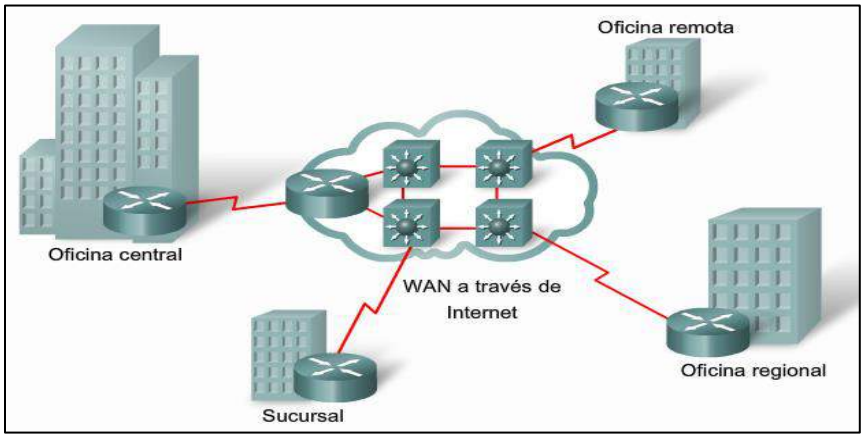
Redes WAN

De acuerdo con Cabarcas y Marrugo (2008), las redes WAN, que en sus siglas en ingles se escribe como *Wide Área Network* o red de área amplia, es una fuente de traspaso de datos hacia zonas geográficas extensas. Estas redes desempeñan un papel crucial en la interconexión de sucursales, oficinas remotas y centro de datos para lo cual se vale de LANs (redes de área local), permitiendo la comunicación eficiente y la transmisión de datos a nivel global.

Por otra parte, Suárez (2020) agrega que, esta red usa enlaces, posee una capacidad que puede cubrir una distancia de 1.000km, utilizan las redes privadas virtuales (VPN), inalámbricas, *Multiprotocol Label Switching* (MPLS) e Internet para tener una conectividad. Por lo que es una red de mayor banda ancha tanto en el público como en el privado, con soporte para voz y datos. En la siguiente **Figura 1**, se puede observar la arquitectura:

Figura 1

Arquitectura de una Red WAN



Nota. El gráfico muestra la arquitectura de una Red WAN. Tomado de "*Introducción a las redes WAN*", (De la Fuente, 2011)

Según De la Fuente (2011), las redes WAN tienen las siguientes características:

- Tiene varios hosts conectados con subredes.
- Se utilizan equipos de potencia alta para alcanzar una conectividad eficaz.
- Los conmutadores, transmisores y enrutadores se encuentran fragmentados.
- Posee routers.
- Facilita el intercambio de datos.
- Se utilizan la fibra óptica o equipo satelital.
- Basado en software y con alta tecnología de equipos de telecomunicación.

Elementos de interconexión

Los elementos de interconexión entre redes son los que se utilizan para la transportar datos de un punto a otro garantizando la seguridad. Por lo que, se constituyen en equipos que se encargan de transformar la información y enviar a diferentes lugares. Estos se utilizan dependiendo de la aplicación que se va a emplear. Los equipos de transmisión de información se enlistan a continuación:

- Equipo de Fibra óptica tanto en redes privadas y públicas
- Cobre para red pública.
- Transferencia de datos vía inalámbrica.
- Transmisión de datos vía satélite.

Estas opciones ofrecen diferente velocidades y capacidades para adaptarse a las necesidades específicas de conectividad de cada organización.

Topologías físicas WAN

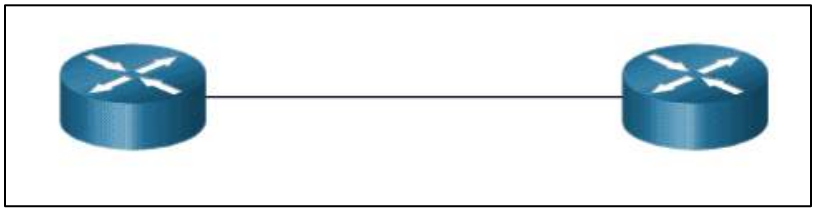
La topología de una red refiere a la relación existente entre los dispositivos de red y las interconexiones (CCNA, 2019). Existen 2 tipos que se utilizan en redes WAN: las lógicas y físicas. Por una parte, la topología física muestras las conexiones físicas y las interconexiones con dispositivos finales e intermedios, como son los routers, switches, puntos inalámbricos y otros.

- **Punto a Punto**

Es una topología WAN simple, la más utilizada. Esta se encuentra enlazada de forma permanente entre dos puntos finales, como se muestra en la siguiente **Figura 2**:

Figura 2

Topología punto a punto de una WAN



Nota. Tomado de (CCNA, 2019)

- **Hub and Spoke**

Es un modelo de red que operan como el centro (el concentrador), trabaja interactuando con aplicaciones, por medio de conversaciones (o spokes). Través de este se reducen o

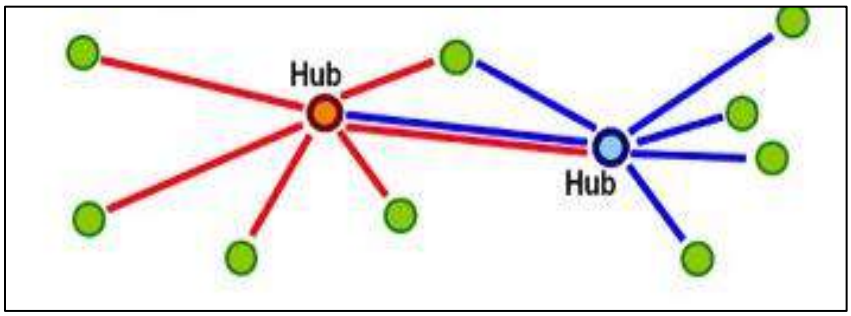
eliminan circuitos. Muchos sitios de web, o los radios, se conectan a una sede central o concentradores, sin conexión entre ellos. Para evitar fallos de conexión, el hub-and-spoke en ocasiones se extiende a una topología redundante hub-and-spoke (CCNA, 2019).

Es un modelo futuro para una oficina que operará bajo el hub-and-spoke; donde los hub vienen a ser las oficinas centrales, ubicados en una ciudad o localidad matriz, y los spokes pueden estar en cualquier lugar del país, pero conectados por un mismo sistema tecnológico (OptimaFacility, 2020).

Lo anterior expuesto se indica en la **Figura 3**, donde los hub están representados por las centrales y los spoke de color verde:

Figura 3

Topología Hub and Spoke



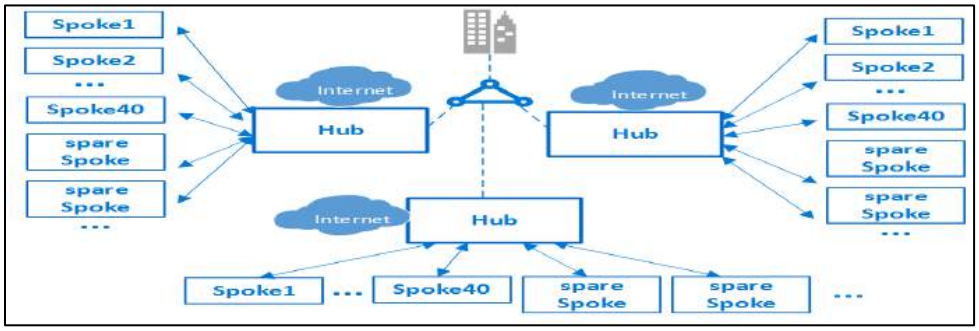
Nota. Tomado de (Universidad Politécnica de Valencia , 2013)

Se trata de una versión WAN tipo estrella donde a través de un sitio central se interconecta con sitios de sucursal usando enlaces punto a punto. En el caso de los sitios de sucursal, estos no pueden intercambiar datos o información con otros sitios de sucursal, puesto que primero deben pasar por el sitio central. Como se muestra en la siguiente figura los hubs son las centrales y los spoke´s conversaciones o sucursales (ORACLE, 2018) (Carrillo & Roncansio, 2020).

En la **Figura 4** se presenta la topología expuesta:

Figura 4

Topología Hub and spoke de una WAN



Nota. Tomado de (Carrillo & Roncansio, 2020)

Esta tipología se utiliza para diseñar soluciones de red creativas y potentes en la nube en los siguientes casos:

- Para configurar ecosistemas de desarrollo y producción independientes.
- Aislar cargas de trabajo de varios clientes, como son los suscriptores de un ISV (Proveedor de software independiente).
- Para suministrar servicios de TI compartidos: servidor de log, DNS o para compartir archivos desde una red central.

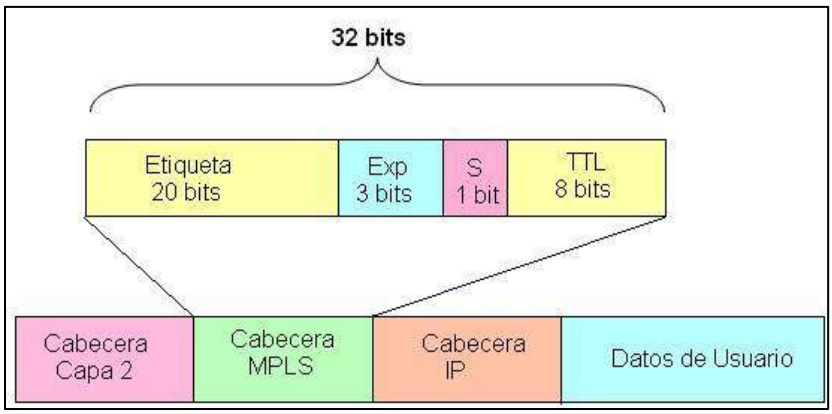
Redes WAN MPLS (Multiprotocol Label Switch)

Según Quintana y Tabares (2011) una MPLS es una solución voluble que nace con el fin de dar respuesta a problemáticas de redes, *"El objetivo principal de esta tecnología es establecer redes que sean flexibles, escalables y capaces de ofrecer alto rendimiento, estabilidad y calidad de servicio (QoS) a través de factores como la velocidad, la gestión del tráfico y la ingeniería"* (p.22), además integra la Ingeniería de Tráfico y soporte de VPNs, este provee (QoS) compuesto por diferentes tipos de servicio (CoS).

La estructura MPLS se compone de encabezados de 32 bits de longitud y divididos en cuatro secciones, cada una de las cuales tiene un propósito distinto, como se muestra en la **Figura 5**:

Figura 5

Cabeceras de una MPLS



Nota. Tomado de (Hinojosa, 2009)

- **Campo Label o Etiqueta:** Con este campo los *Label Switching Route* (LSR) pueden conmutarse. La etiqueta es asignada por el elemento que inicia o termina el túnel (Ingress LER o *Label Edge Route*), esto en base a los parámetros descritos en los anuncios de estado de enlace (LSA).
- **Campo Experimental EXP:** Debido a la creciente necesidad de priorización dentro del protocolo IP, la información de Servicios Diferenciados (DiffServ) se utiliza en el campo de uso experimental, específicamente para el transporte de dicha información, incluido el esquema Best Effort.
- **Campo Stacking:** "La clasificación de las etiquetas se puede lograr utilizando este campo. MPLS posee la capacidad de etiquetar el tráfico MPLS que se origina en una red vecina, creando una pila. A la primera entrada de la pila se le asigna un

valor de 1, mientras que a las entradas siguientes se les asigna un valor de 0*”* (Hinojosa, 2009).

- **Campo TTL Time to Live:** “El recuento de saltos sirve como mecanismo para evitar la formación de bucles al enviar paquetes etiquetados. Actúa como un reemplazo del TTL en el encabezado IP y disminuye en uno por cada nodo que atraviesa. Si llega a cero en un LSP particular, el paquete se descarta*”* (Hinojosa, 2009).

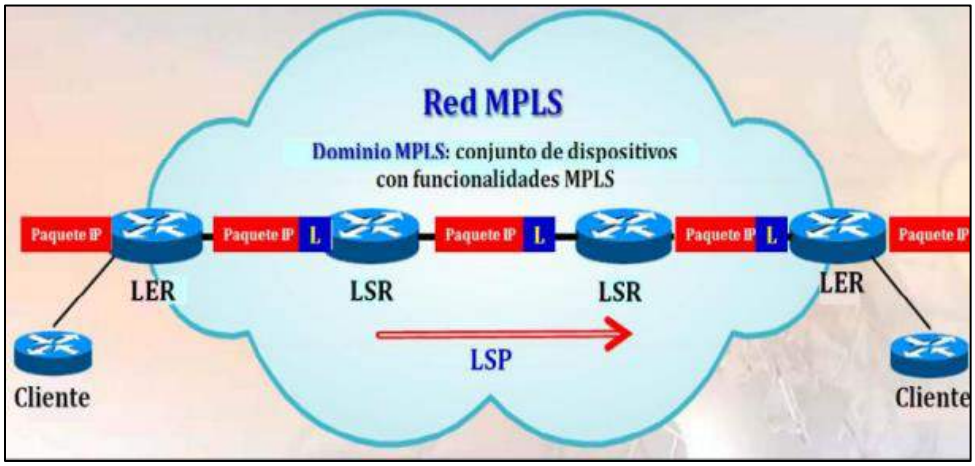
Elementos de una MPLS

Mediante el uso del LDP, además de descubrirse entre sí, los nodos MPLS tienen la capacidad de establecer una comunicación significativa y comprender el significado y el uso previsto de las etiquetas en los enlaces vecinos*. Es decir, a través de un LDP con la que se crea el camino por medio de una red MPLS*” (ComputerWorld, 2018).

Dentro de la estructura de una red MPLS, existen dos componentes esenciales conocidos como nodos: el LER y el LSR. Estos nodos, que pueden adoptar la forma de enrutadores o conmutadores troncales con software MPLS integrado, poseen un parecido físico. El intercambio de información de topología de red entre nodos MPLS se ve facilitado por los protocolos de enrutamiento OSPF ampliamente utilizados, que son responsables de calcular la ruta más corta. Los componentes antes descritos se exponen en la **Figura 6**:

Figura 6

Elementos de una Red MPLS



Nota. Tomado de (Quintana & Tabares, 2011)

Una vez que se tiene estas tablas se establecen las etiquetas MPLS, por tanto, las LSP que guían los paquetes. “En esencia, el LER determina la ruta completa que debe atravesar el paquete y, una vez que se elige MPLS, el LER reenvía el paquete a un LSR ubicado dentro del núcleo de la red MPLS. Luego, el LSR emplea un enrutamiento eficiente basado en conmutación de etiquetas, limitado al nivel 2”. (Imagar, 2021).

“Al llegar a la interfaz LSR, se examina la etiqueta de entrada del encabezado MPLS y se consulta la tabla de conmutación para determinar la etiqueta de salida y la interfaz. Posteriormente, el paquete se dirige a lo largo de la ruta predeterminada y al mismo tiempo se agrega un nuevo encabezado” (Imagar, 2021).

Redes Virtuales Privadas (VPN)

Las VPN (Virtual Private Network) o Redes Privadas Virtuales crean redes locales sin necesidad de que los usuarios estén físicamente conectados, es decir únicamente comparten dados e información a través del internet. Para ello es necesario un enrutador o módem, para

conectar el lugar con el proveedor de Internet, usando un cable o inalámbricamente (Stackscale, 2021).

Las VPNs ocultan las direcciones IP, con ello las actividades que se realizan vía online no se pueden rastrear, manteniendo la información de forma confidencial y privada. Los usos más frecuentes de esta red son por las siguientes razones:

- Se utilizan porque permite el acceso a recursos restringidos de una empresa.
- Se usan para acceder a la red del trabajo cuando estén fuera de la oficina.
- Permite el acceso a la red del hogar mientras se está fuera de casa.
- Ocultar los datos de navegación.
- Evitar la censura en Internet. (Stackscale, 2021)

Funcionamiento

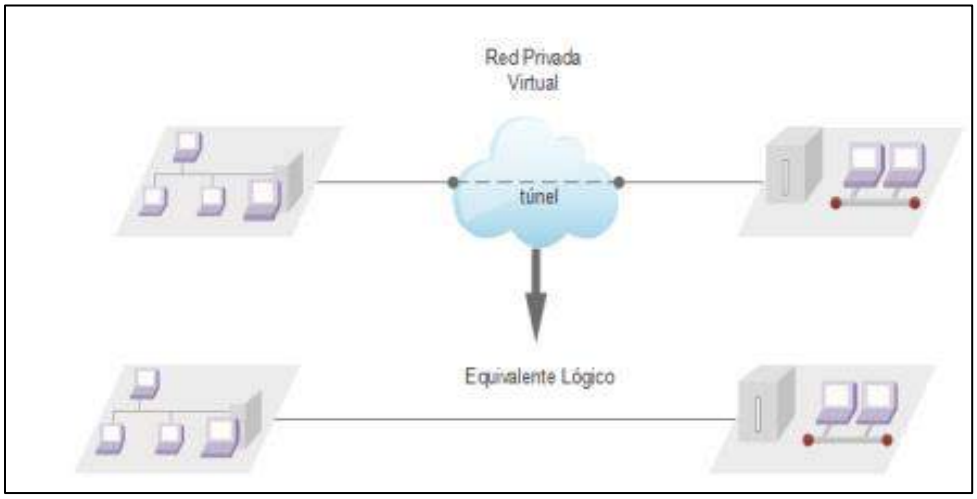
Según Quezada (2016), una red privada virtual opera mediante el protocolo de túnel, el cual se encarga de cifrar los datos transmitidos desde un lado de la VPN hacia el otro lado de esta, cuyo funcionamiento se muestra en la **Figura 7**.

Dentro de las funciones que realiza esta red desde el enfoque de seguridad son la siguientes:

- La Autenticación del usuario
- Gestión de direcciones
- Cifrado de datos
- Gestión de claves

Figura 7

Funcionamiento de una Red VPN



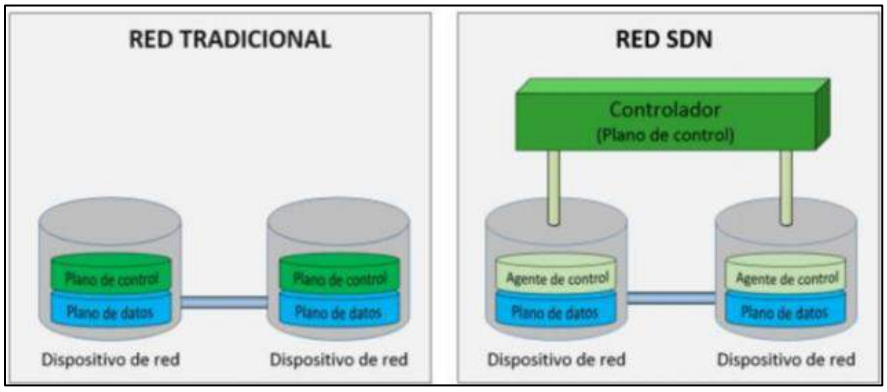
Nota. Tomado de (Quezada, 2016)

Introducción a redes SD-WAN

Para recopilar información de manera efectiva en las redes SD-WAN, el paso inicial implica obtener acceso a redes definidas por software (SDN) que están estructuradas para permitir el control y la programación centralizados de la red, a diferencia de las redes tradicionales. Esta centralización permite una gestión integral de la red, sea cual sea el acceso o punto de conectividad. Al separar los planos de datos y control, se puede automatizar y facilitar la administración de la red, como se muestra en la **Figura 8**.

Figura 8

Redes Tradicionales vs Redes SDN



Nota. Tomado de (Heydari & Ellawindy, 2019)

En las redes tradicionales, cada enrutador dispones de un plano de control independiente, si se ejecuta alguna función está solo afectará a ese dispositivo; mientras que en las redes definidas por software (SDN), al tener un plano de control que intervine a todos los dispositivos conectados, al ejecutar alguna función se aplicará en todos los dispositivos conectados en la red, logrando agilizar el proceso de configuración.

SD-WAN es una aplicación de soluciones de SDN que permite el uso eficiente y controlado de las conexiones WAN (Valero, 2019). Por una parte, las redes definidas por software se ubican en centros de datos internos en una sede, por el contrario, SD-WAN capta la base definida por un software similar y extrae el plano de control del plano de datos a la WAN. "*En el mundo empresarial, es característico encontrar una infraestructura compleja en las sucursales, como en el caso de conectividad con routers, controladores de rutas WAN, optimizadores de WAN, firewalls y otros, que resultan costosos en términos de compra y mantenimiento*" (Bustos, 2019).

En este sentido, la finalidad principal de una SD-WAN es viabilizar a los usuarios la posibilidad de acceso a servicios de conectividad de forma eficaz, al más bajo costo,

aprovechando la rápida expansión del internet por ser los más baratos en sobre todo en internet de fibra ancha, así como también en base al aumento del mercado de servicios en la Nube (Marín, 2021).

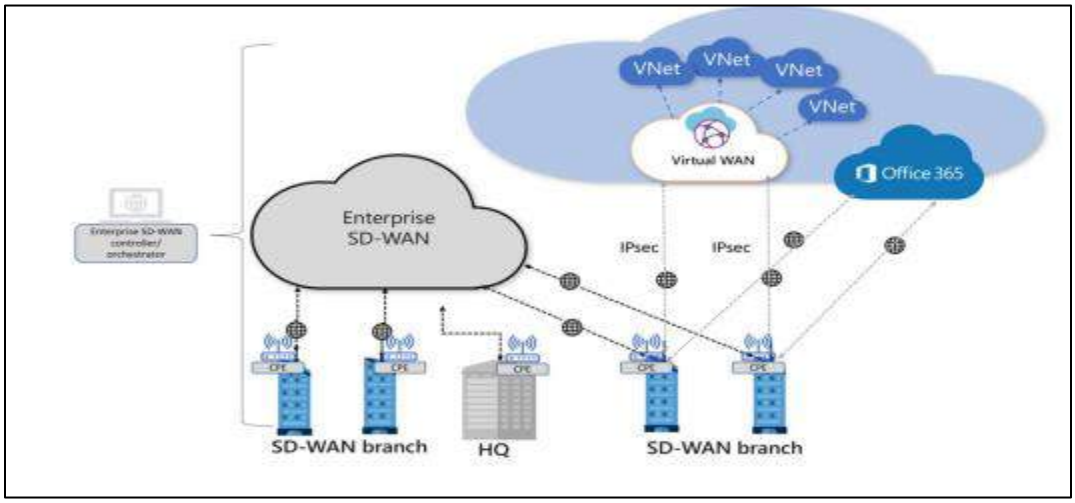
Por otra parte, desde varias décadas, las soluciones MPLS han sido los protagonistas en el mercado empresarial, pues han sido quienes han proveído redes privadas, sin importar el lugar, de estar en puntos remotos para conectar al internet se utilizaban grandes concentradores para concretar el tráfico unificando con grandes puntos de acceso. "C*on ello se hizo visible 2 problemas, el primero relacionado con el tráfico de internet por los enlaces de MPLS, siendo estos más caros que un internet normal, esto debido al crecimiento del tráfico de internet, donde las aplicaciones corporativas están quedando rezagados obligando a usar filtros y reglas para tener control*" (Barrios del Sol, 2020).

Al contrario, SD-WAN ofrece una solución integral segura adaptado a las soluciones MPLS con canales más baratos y variados, como en el caso de los de banda Ancha, una vez implementado, tiene la capacidad de enfocar el tráfico mucho más simplificada independientemente de los múltiples canales que se esté utilizando de forma segura y con calidad de servicio que se ve reflejado en los resultados y satisfacción (Mingrone, 2019).

Para López (2020), en comparación con las WAN tradicionales, SD-WAN ofrece una base de red que es fácil de administrar al reubicar la capa de control en la nube, centralizando y agilizando así la administración de la red, cuya arquitectura se expone en la **Figura 9**:

Figura 9

Arquitectura de la SD-WAN



Nota. Tomado de: (López, 2020)

El surgimiento de SD-WAN fue un resultado directo de los desafíos que plantean las WAN tradicionales, incluidos problemas como la latencia y fallas de conexión que conducen a la indisponibilidad del servicio. En el impredecible panorama de conectividad actual, es crucial que las empresas puedan compartir información y colaborar sin problemas. Por lo tanto, realizar un estudio exhaustivo sobre SD-WAN es de suma importancia.

Ventajas y Desventajas

Simplicidad: para las redes definidas por software la función principal, es el control de las rutas gestionado por aplicaciones en la nube, creados por interfaces que permite tener el control del almacenamiento de datos, así como también de las políticas, pudiéndose además realizar cambios en dispositivos de toda la red con tan solo dar un click (Beltran & Pisfil, 2021).

Seguridad: se centra en tres aspectos la encriptación, autenticación e integridad. Cabe tomar en cuenta que, tener una nueva conexión de punto de red es fácil, pero para realizar esto se debe considerar el proceso de autenticación que se lleva a cabo hacia con el sitio central que antecede al flujo de tráfico entre las sedes definidas, por lo que según la flexibilidad se

puede adaptar a conexiones cifrada, mismas que debe dar respuesta a requerimientos en equilibrio con el rendimiento y seguridad, incluso en conexiones complejas de administrar y operar como en el caso de la Full-mesh (Beltran & Pisfil, 2021).

Calidad de la experiencia: en la actualidad existen múltiples formas para mejorar la calidad y niveles de seguridad, tomando en cuenta que el Internet no es lo homogénea a una red privada. Por ello, la implementación de un SD-WAN debe permitir la disminución del tamaño de los circuitos MPLS, donde ciertas aplicaciones funcionan de forma óptima en la gran mayoría de tiempo con Internet, lo que se espera es medir en tiempo real la elección de una ruta MPLS para un dialogo especifico en un tiempo y momento determinado, puesto que la red tiene la capacidad suficiente para ello (Beltran & Pisfil, 2021).

En consenso, Mingrone (2019) manifiesta que está herramienta ofrece múltiples, pues posee un software de alto nivel eficaz y eficiencia en el plano de la administración, puesto que con ello se puede replicar configuraciones o esquemas de red estandarizados. Es por lo que las características más representativas y positivas de la SD-WAN son:

- Administración centralizada y sencilla sucesión: se administran los puntos de red de forma simultánea, por ejemplo, una política de seguridad se puede aplicar a todos y en un mismo tiempo a los equipos locales del cliente (CPEs).
- Los componentes del plano de control son 100% seguros y virtualizados
- Extensa captación de enlaces como canal de transporte, permite el uso de cualquier acceso a internet o MPLS.
- Abarata costos: Los CPEs para SD-WAN son sencillos y económicos, puesto que la mayor complejidad se ubica en el plano de control, igual para toda la red.
- Instalación eficaz y sencilla: un servicio se puede trasladar de un lugar a otro, usando de transporte la conectividad anterior en la nueva ubicación.

Por otra parte, de acuerdo con Beltrán y Pisfin (2021), manifiestan que una SD-WAN no debe afectar en la mayor medida de lo posible el entorno de los servicios de red empresarial; para ello es importante contar con proveedores de SD-WAN confiables que garanticen la seguridad de información y datos. Entre las desventajas se puede encontrar:

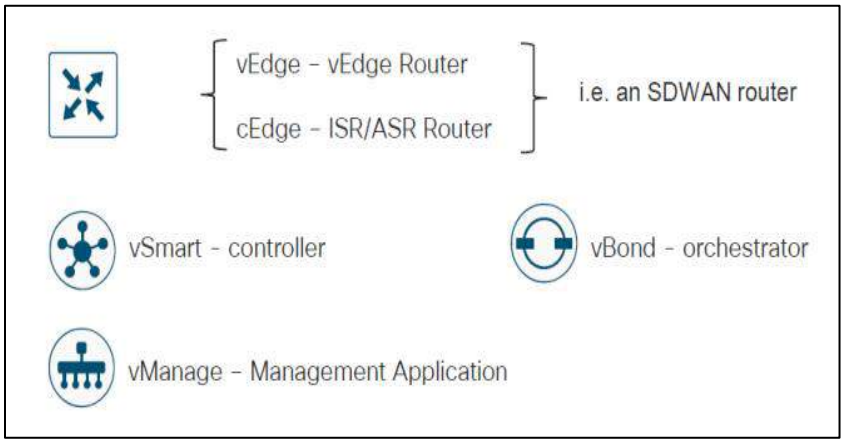
- El alto costo del ancho de banda
- No se puede utilizar el internet público
- Los proveedores cooperan con otros servicios para contribución en la cobertura global
- Inseguridad para encontrar proveedores confiables

Estructura de la SD-WAN

La SD-WAN se conforma de diversos planos, cada uno de los cuales se conforman por componentes que son parte de la solución en la siguiente **Figura 10** se presenta las nomenclaturas que se utilizan en la estructura:

Figura 10

Elementos de la arquitectura de SD-WAN



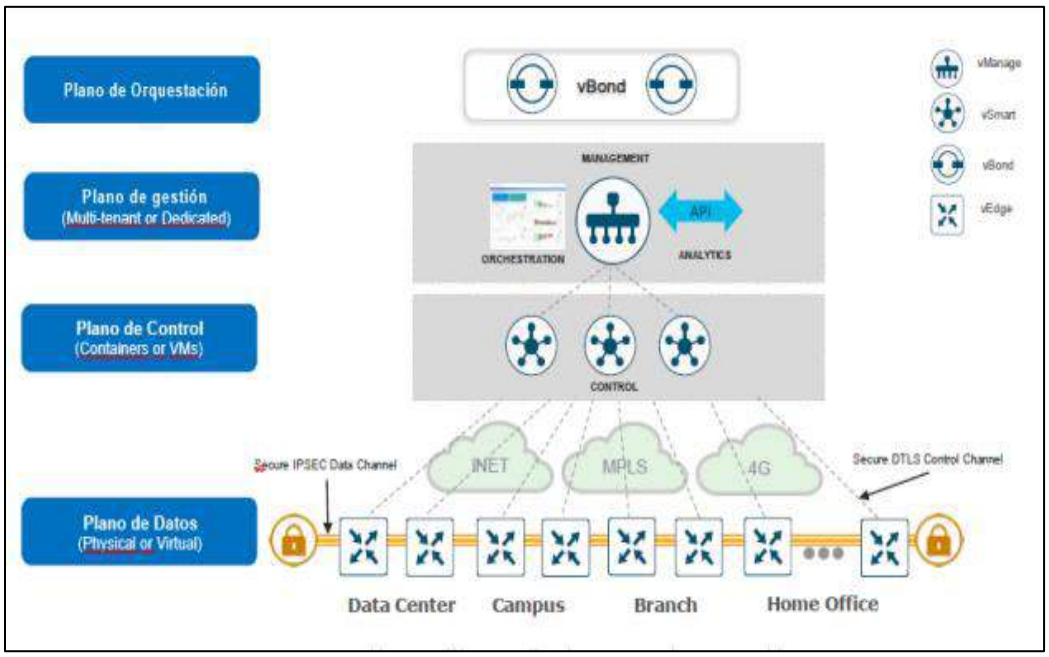
Nota. Tomado de (Carrillo & Roncansio, 2020)

Como se puede observar, en la **Figura 11**, la arquitectura de SD-WAN se subdivide en 4 planos: el Plano de control (Control plane), el plano de datos (Data plane), de orquestación (Orchestration plane) y de administración (Management plane). Cada uno tiene elementos como parte de una solución, mismos que se detallan (Carrillo & Roncansio, 2020).

En la **Figura 11** se presenta los principales componentes de una Red SD-WAN:

Figura 11

Arquitectura básica de una Red SD-WAN



Nota. Tomado de (Carrillo & Roncansio, 2020)

Plano de orquestación (Orchestration Plane): basado en software se centra en la autenticación de dispositivos vEdge, a la vez organiza la conectividad vSmart y vEdge. Otra de las funciones que realiza es la comunicación de dispositivos NATs., siendo importante la asignación de una IP pública fija (Carrillo & Roncansio, 2020).

Plano de gestión (Management Plane): es una red de administración centralizada provee una interfaz GUI que sirve como componente de configuración, monitoreo y poder

mantener de manera sencilla aplicaciones, dispositivos y enlaces SD-WAN en una red (Carrillo & Roncansio, 2020).

Plano de Control (Control Plane): es un componente basado en software realiza el control centralizado de la red SD-WAN. Forma una conexión segura a cada CPE (Equipo Local del Cliente), además distribuye rutas e información mediante protocolos de administración de superposición (OMP), este ejerce el rol de reflector de ruta. Establece una conectividad segura en un plano de datos a través de la distribución de datos con clave criptográfica (Carrillo & Roncansio, 2020).

Plano de Datos (Data Plane): refiere a dispositivos disponibles basados en hardware o software, se encuentran en un sitio físico o en la nube, para acceder a una conexión segura sobre un plano de datos entre las rutas, mediante una o más cargas WAN. Se realiza el reenvío de tráfico, cifrado, seguridad, la calidad de servicio (QoS), así como también de proveer de protocolos de enrutamiento: BGP y OSPF, y otros (Carrillo & Roncansio, 2020).

Comparación entre SD-WAN, MPLS y VPN

En la siguiente tabla, encontrará una descripción general completa de los pros y los contras clave asociados con las tecnologías SD-WAN, MPLS y VPN, lo que permite una fácil comparación.

Tabla 1

Comparación entre SD-WAN, MPLS y VPN

	VPN	MPLS	SD-WAN
Arquitectura	Utiliza diferentes protocolos de tunelización para crear conexiones seguras a través de una red	Maneja conmutación de etiquetas para dirigir el tráfico de manera eficiente.	Maneja software para gestionar la red de forma más dinámica y adaptable.

	VPN	MPLS	SD-WAN
	pública (generalmente Internet). Admite diversas implementaciones como Ipsec, SSL, PPTP, etc.	Requiere acuerdos con proveedores de servicios para establecer rutas MPLS.	Permite la configuración centralizada y dinámica de la red.
Costo	En general más económica, especialmente al utilizar conexiones a través de Internet.	Suele ser más costoso debido a la infraestructura dedicada, configuración y mantenimiento por parte del proveedor	Ofrece una solución más rentable al permitir la utilización eficiente de conexiones múltiples.
Conectividad y Topología	Puede utilizar Internet para establecer conexiones seguras. Topología más flexible, adapta la red a la infraestructura existente.	Proporciona conectividad segura y fiable entre ubicaciones Topología basada en circuitos y rutas predefinidas	Permite la utilización de múltiples conexiones, como MPLS, Internet y conexiones inalámbricas. Ofrece una topología dinámica y adaptable según las condiciones de la red.
Rendimiento y Latencia	Puede tener un rendimiento variable dependiendo de la conexión a Internet. Latencia puede ser mayor en comparación con MPLS	Ofrece un rendimiento confiable y predecible. Contribuye a la baja latencia.	Optimiza el rendimiento al utilizar múltiples conexiones de manera inteligente. Puede mejorar la latencia al seleccionar la mejor ruta para el tráfico.

	VPN	MPLS	SD-WAN
Seguridad	Encripta el tráfico para garantizar la confidencialidad de los datos.	Proporciona un nivel básico de seguridad, pero puede requerir medidas adicionales para niveles más altos de privacidad.	Incluye funciones de seguridad integradas como firewalls y encriptación.
Gestión y Configuración	Configuración más flexible y puede ser gestionada internamente.	Configuración más estática, requiere acuerdos con proveedores, para realizar cambios toma más tiempo.	Ofrece configuración centralizada y dinámica, facilitando la gestión de la red a través de software.
Adaptabilidad y Escalabilidad	Más adaptable y escalable, especialmente en entornos cambiantes.	Menos adaptable porque requiere más tiempo para cambios, escalabilidad limitada y puede requerir cambios significativos para expandirse.	Altamente adaptable y escalable, se ajusta a los cambios en los requisitos de la red.

En resumen, la tecnología MPLS ofrece rendimiento confiable, pero a un costo mayor, más adecuado para aplicaciones críticas, la tecnología VPN es más flexible y económica, ideal para empresas con presupuestos ajustados y por último SD-WAN combina la flexibilidad de VPN con la optimización de rendimiento, adaptándose bien a entornos cambiantes y optimizando costos.

Principales Proveedores de SD-WAN

De acuerdo con lo expuesto por Beltran y Pisfil (2021) existen varios fabricantes que han lanzado una versión de tecnología SD-WAN, la elección de un proveedor depende de los

diferentes factores, necesidades específicas de la red del cliente corporativo, los requisitos de seguridad y las características deseadas. Entre los proveedores se encuentran:

Cisco Meraki

- Interfaz de gestión intuitiva basada en la nube.
- Integración con otros productos de Cisco.
- Puede ser más adecuado para entornos donde ya se utiliza el ecosistema Meraki.
- Permite administrar el consumo de ancho de banda y uso de aplicaciones para impulsar políticas de bloqueo.
- Selección de una ruta inteligente de acuerdo con el flujo de datos y métricas de Qos que provee el mismo equipo.
- Alertas en tiempo real ante ataques que influyen en la seguridad de la red.

Fortinet

- Baja Automatización, los cambios se realizan sobre los equipos, sin plantillas, se obtiene una mayor overhead de gestión.
- Integración con soluciones de seguridad de Fortinet.
- Algunas características avanzadas pueden requerir hardware específico.

Silver Peak

- Enfoque en aceleración de WAN y SD-WAN, escalabilidad, optimización de rendimiento.
- Conocido por su énfasis en el rendimiento de la red.

Citrix SD-WAN

- Enfoque en la experiencia del usuario, optimización de aplicaciones, gestión centralizada.

- Adecuado para entornos donde la optimización de aplicaciones es crucial.

VMware SD-WAN by VeloCloud

- Adquirido por VMware, ofrece integración con soluciones de virtualización y centros de datos.
- Escalabilidad y flexibilidad en la implementación.
- Puede ser especialmente adecuado para empresas que ya utilizan productos VMware.

Nuage Networks (Nokia)

- Enfoque en SD-WAN y SDN, escalabilidad, automatización.
- Puede ser más adecuado para entornos específicos

Aruba, a Hewlett Packard Enterprise Company

- Enfoque en seguridad y movilidad.
- Puede ser preferido en entornos donde ya se utilizan productos de Aruba.

Versa Networks

- Enfoque en SD-WAN y servicios de seguridad integrados, escalabilidad.
- Relativamente nuevo en comparación con algunos competidores.

Métricas de QoS (Calidad de Servicio)

De acuerdo con Estavillo (2017) la calidad de servicio (QoS), “describe la habilidad de una red desde el punto de vista técnico para proveer servicios” (p.2), dentro de estas se detallan los parámetros de calidad en servicios de voz, mensajes, y servicios de datos bajo criterios de nivel de transmisión, latencia, jitter (varianza en latencia) y pérdida de paquetes. Por lo que para alcanzar un nivel adecuado de calidad se debe tomar en cuenta lo siguiente:

- El servicio/contenido (video, redes sociales)
- El dispositivo de recepción del servicio

- Ubicación del usuario
- Las condiciones de la red

Dentro de las principales métricas de calidad de servicio QoS se muestra en la **Tabla 2**;

Tabla 2

Métricas QoS

Disponibilidad de Servicio	Capacidad de servicio (TI) Se calcula en porcentajes Determinadas por la seguridad, rendimiento, mantenibilidad y TI
Retardo o Jitter	Variación de tiempo de llegada de paquetes Es un efecto de las redes de datos
Pérdida de Paquetes	El protocolo UDP no se orienta a una conexión al producir una pérdida de paquetes no los reenvían. La pérdida de paquetes máxima admitida es inferior al 1%.
Caudal o Velocidad de datos	Es el volumen de información neto Se mide en Mbit/s y es inferior al ancho de banda.

Fluctuación de retardo	Tiempo que tarda el paquete desde la fuente al destino Es un problema de las redes de telecomunicación.

Nota. Tomado de (Coggle, 2016)

Capítulo III: Diseño e Implementación

Situación inicial del cliente corporativo

En el presente trabajo se pretende realizar el diseño de la red SD-WAN para un cliente corporativo de una empresa proveedora de servicios de Internet corporativos. Como antecedentes, el cliente corporativo en una empresa ecuatoriana que nació en1959, dedicada a la comercialización de vehículos y su mantenimiento tanto preventivo como correctivo. Cuenta con 9 agencias a nivel Nacional en las ciudades de Cuenca, Quito, Sangolquí, Ambato, Riobamba, Santo Domingo y Latacunga, calculando un aproximado de 1400 clientes dentro de la red del cliente corporativo, distribuidos en las agencias anteriormente mencionadas.

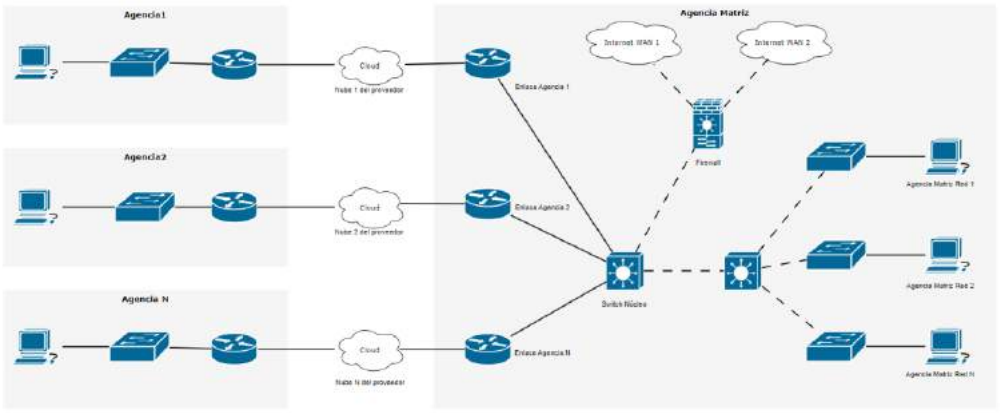
Actualmente, la infraestructura de su red es híbrida ya que tiene conexiones basadas en tecnología MPLS y VPN. En las 9 sucursales posee accesos MPLS de 5 Mbps mediante cable de cobre, contratados a otro diferente proveedor de servicio de internet. En la sucursal de Cuenca donde se encuentra la oficina matriz, dispone de un núcleo de servicio de red junto con el firewall y el data center. Esta red híbrida, al estar sobre tecnología MPLS, trabaja en topología estrella la misma que se encuentra obsoleta.

Adicional, se tiene configurado en cada sucursal como enlace de backup una IPsec VPN sobre internet, el túnel de comunicación va desde el switch de core hacia el router de la nube de nuestra empresa proveedora de servicios de internet corporativo. El esquema de la red anteriormente descrito se puede visualizar en la

Figura 12.

Figura 12

Topología de la red actual del cliente corporativo.



El cliente corporativo con su red actual manifiesta tener problemas que dificultan la operación adecuada de la empresa. Entre estos problemas se detalla los siguientes: la difícil administración y control del tráfico en cada agencia, inconvenientes para detectar ataques a la seguridad de la red, congestionamiento del tráfico, la demora en presentar alarmas a los administradores de la red ante alguna caída de esta. Adicional el cliente menciona que al trabajar con conexiones por cobre la transmisión del tráfico es lenta, como también si en la red se desea realizar algún cambio de configuración o alguna expansión es necesario para estos soportes que un técnico se dirija a cada agencia para realizar este proceso, tomando más tiempo de gestión, mano de obra y costos. Todo esto limita al cliente corporativo a la toma de decisiones ágiles como a su vez el análisis de la red para mejoras.

Por lo tanto, las necesidades son las siguientes:

- Tener una administración centralizada.
- Aumentar anchos de banda.

- Monitoreo de los servicios a nivel de red, sin gestión presencial.
- Controlar el tráfico, contenido y apps.
- Mejorar la latencia, pérdida de paquetes, gestión de la red WAN.
- Seguridad en el tráfico de las aplicaciones.
- Reducción de costos.

Selección del proveedor de equipos SD-WAN

Inicialmente se debe elegir el proveedor adecuado que ofrezca la solución acorde a las necesidades del cliente corporativo, en el mercado internacional existen varias empresas que desarrollan equipos para la tecnología SD-WAN, de acuerdo con el cuadrante de Gartner en su último informe de septiembre 2023, se tiene a Fortinet y VMware como líder de SD-WAN, seguidos por Cisco, Aruba y Versa Networks.

Figura 13

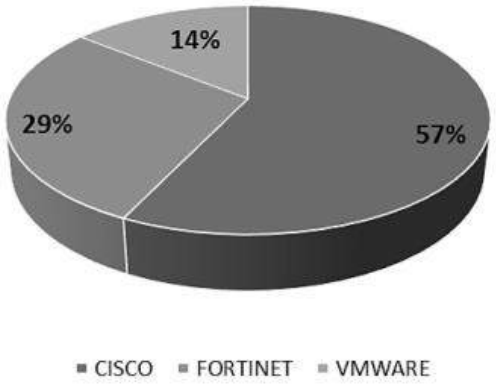
Cuadrante mágico de Gartner para SD-WAN

Nota. Tomado de (Gartner, 2023)

Según estudio realizado por (Cusco Perez, Cabrera Mejía, & Lugo García, 2022), en Ecuador el 57% de las empresas tienen implementado SD-WAN con soluciones Cisco, el 29% con soluciones Fortinet y apenas un 14% con VMware.

Figura 14

Proveedores para implementar la tecnología SD-WAN en el Ecuador.



Nota. Tomado de (Cusco Perez, Cabrera Mejía, & Lugo García, 2022)

Acorde con la información descrita anteriormente, para este estudio, se considerará que el proveedor utilizará para el diseño e implementación propuesta será con soluciones Cisco mediante la plataforma de Meraki.

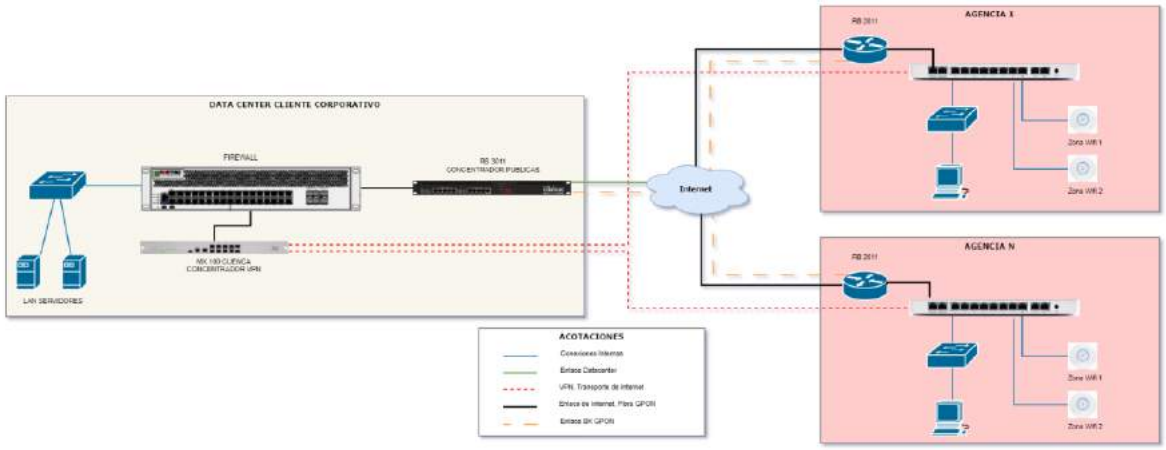
Diseño de la red Hub and Spoke SD-WAN

Tomando como una de las consideraciones la ampliación de la empresa, se estima un alcance de crecimiento para 3 años del 10% por año, por lo tanto, si actualmente se tiene 1400 clientes en 3 años, serán aproximadamente 1820 clientes, que en efecto causa el aumento del tráfico. Como solución por parte de nuestro proveedor de servicios de internet corporativo, se ofrece servicios de conexión dedicados bajo fibra óptica, que ofrecen un mayor ancho de banda y una menor latencia. Los nuevos anchos de banda se visualizan en la **Tabla 3**.

El nuevo diseño de la red para el cliente corporativo parte de una topología hub and spoke en SD-WAN, esta topología se elige, debido a que los equipos cisco Meraki en su configuración solo permiten trabajan en este tipo de topología. En la **Figura 15**se puede observar el nuevo diseño de la red sobre SD-WAN, donde en la sucursal de Cuenca se implementa un equipo cisco Meraki MX100, esté funcionará como HUB y las sucursales restantes trabajaran con un equipo cisco Meraki MX65.

Figura 15

Diseño de red SD-WAN para el cliente corporativo.

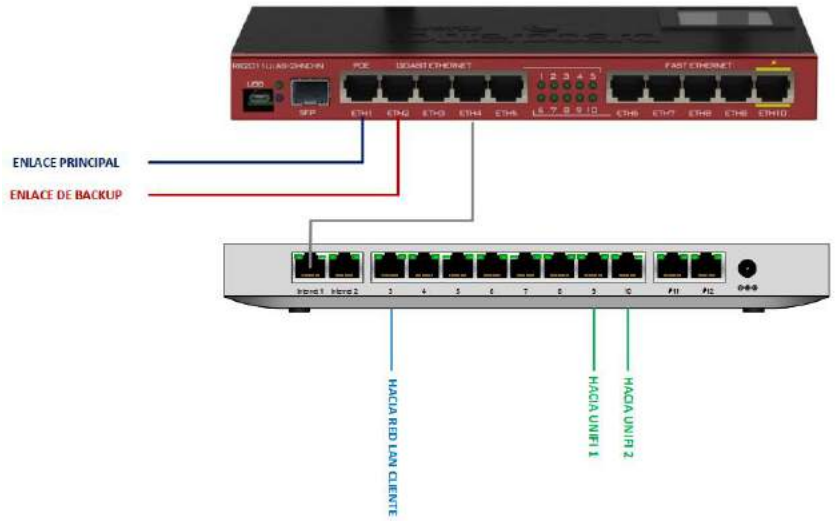


La topología de Hub and Spoke está implementada sobre la infraestructura del proveedor de servicios de Internet corporativo. Toda la red de servidores, así como el equipo Meraki MX100 se encuentran protegidos detrás del firewall Fortinet del cliente. Como enlace de backup están las conexiones de fibra óptica brindadas por nuestro proveedor de servicios de internet corporativo.

En cada sucursal se tienen 2 equipos, 1 RB2011 y el SD-WAN Meraki MX65. Quedando de la siguiente manera **Figura 16**.

Figura 16

Diseño de conexiones hacia equipo meraki MX65.



El cliente corporativo tiene actualmente instalados 9 puntos de internet con tecnología GPON, los cuales se detallan en la siguiente tabla.

Tabla 3

Direccionamiento y detalle de enlaces del cliente corporativo

Enlace	IP Pública	Equipo Terminal	Clientes	Ancho de banda	Tecnología
Ambato	190.57.X.X	Meraki MX65	60	15 Mbps	Fibra Óptica
Quito G	190.12.X.X	Meraki MX65	100	35 Mbps	Fibra Óptica
Cuenca DC	190.110.X.X	Meraki MX100	600	50 Mbps	Fibra Óptica
Latacunga	181.188.X.X	Meraki MX65	50	35 Mbps	Fibra Óptica
Riobamba	190.57.X.X	Meraki MX65	400	35 Mbps	Fibra Óptica

Enlace	IP Pública	Equipo Terminal	Clientes	Ancho de banda	Tecnología
Santo Domingo	190.12.X.X	Meraki MX65	80	35 Mbps	Fibra Óptica
Quito L	190.12.X.X	Meraki MX65	80	35 Mbps	Fibra Óptica
Quito M	190.12.X.X	Meraki MX65	300	50 Mbps	Fibra Óptica
San Rafael	179.49.X.X	Meraki MX65	60	35 Mbps	Fibra Óptica

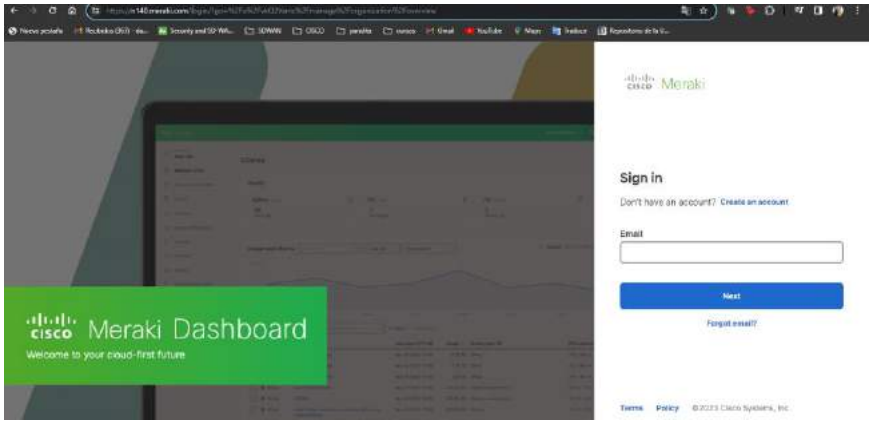
Implementación

Para la implementación de la red hub and spoke sobre tecnología SD-WAN, se han utilizado 9 equipos Cisco Meraki, los mismos que se encuentran distribuidos de la siguiente forma: el equipo cisco Meraki MX100 se instalará en la sucursal principal de Cuenca y los 8 equipos cisco Meraki MX65 en las sucursales restantes.

Accedemos a la plataforma de Meraki más conocida como dashboard en el siguiente enlace http://dashboard.meraki.com, donde se puede crear una cuenta, al ser los equipos del proveedor del servicio de internet, este se encarga de crear las cuentas de acceso con las cuentas de correo de los empleados solicitadas por el cliente corporativo y a su vez de los administradores del proveedor del servicio**.**

Figura 17

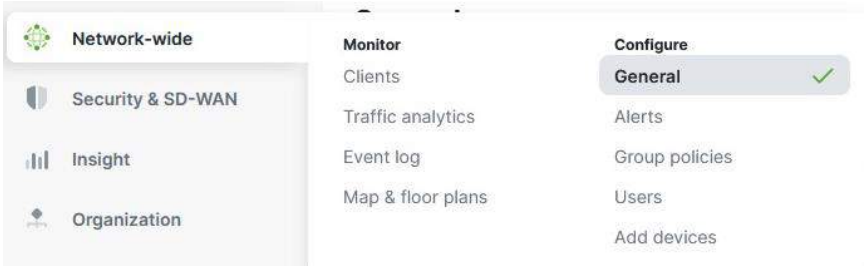
Página de Logueo Dashboard Cisco Neraki del cliente corporativo.



Se procede con la creación de los enlaces en el dashboard, en la sección de “Network-wide”, seleccionar “General”.

Figura 18

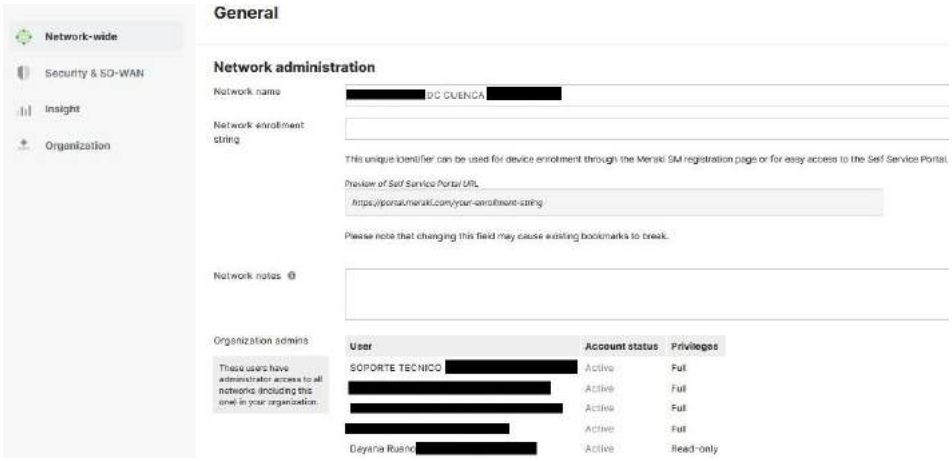
Creación de los enlaces en la plataforma de Meraki.



En la opción de “General” se abre una nueva pantalla, donde definimos el nombre de cada network o enlace.

Figura 19

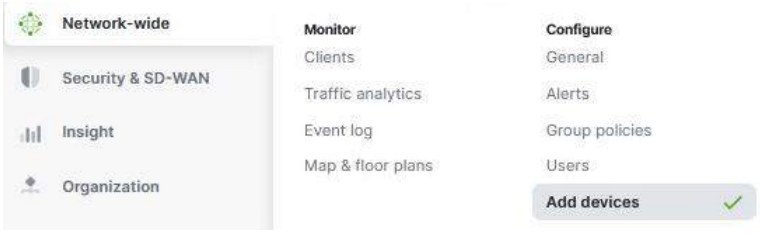
Definición de nombre a la network o enlace del cliente corporativo.



A cada network se procede agregar el equipo por la serie o mac address de cada uno según corresponda, esto se realiza desde la sección de “Network-wide”, seleccionar “Add devices”.

Figura 20

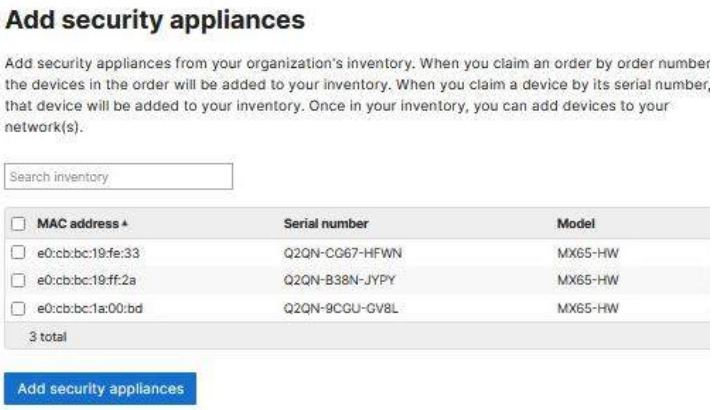
Asignación de equipos a cada enlace o network.



En la pantalla se visualizarán las Mac Address y serial numbers de los dispositivos que están disponibles en el sistema para asignarlos a la red de la sucursal que correspondan.

Figura 21

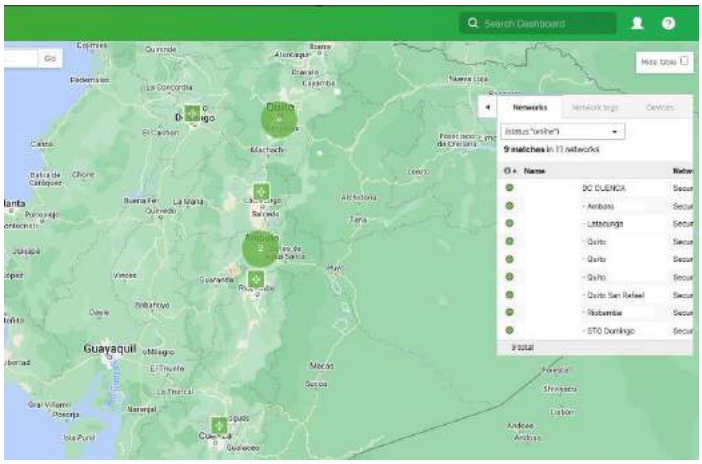
Visualización de equipos por Mac Address y serial number para la asignación a los enlaces.



Una vez agregados los dispositivos, se visualizará en el dashboard de la plataforma de Meraki la ubicación de cada agencia en el mapa, para tener un mejor control y administración, como se indica en la **Figura 22**.

Figura 22

Ubicación de las redes o agencias en SD-WAN.



Configuración del direccionamiento IP

Configuramos el direccionamiento de los equipos de forma estática en la plataforma gráfica de Meraki o dashboard. En la **Figura 23** se indica la configuración ip del enlace de Cuenca en el equipo MX100 y del enlace de Quito M en el equipo MX65, esto se realiza en cada enlace en base a la **Tabla 3** .

Figura 23

Configuración de direccionamiento ip en MX100 y MX65.

Configuración de la capa de acceso y direccionamiento LAN

Para la configuración de la red LAN, seleccionamos la sección “Security & SD-WAN”, en las opciones seleccionamos “Addressing & VLANs”, en esta opción **Figura 24**, escogemos “Routed” para que el equipo funcione en capa 3 y pueda traducir las direcciones a IP.

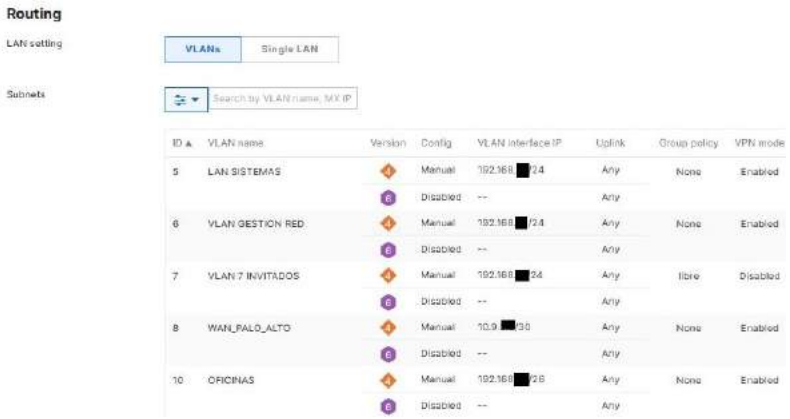
Figura 24

Elección del modo de trabajo del equipo Meraki

En la misma ventana, se realiza la configuración de la LAN y VLANs que requiere el cliente corporativo, como se puede observar en la **Figura 25**.

Figura 25

Configuración de LAN y VLANs.



Al finalizar la configuración del direccionamiento, los puertos del equipo se activan y el tráfico se puede visualizar de manera gráfica sin necesidad de una aplicación adicional, esta es una ventaja de la plataforma de Cisco Meraki SD-WAN.

Figura 26

Visualización de Puertos y Tráfico.

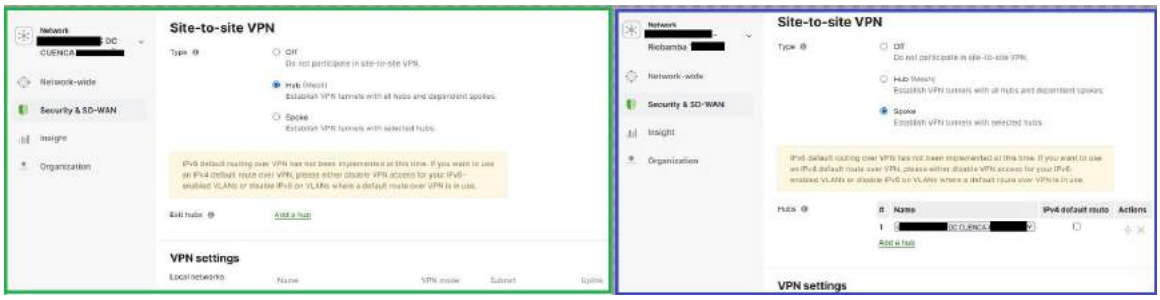
Configuración de la VPN

Para que el cliente corporativo pueda acceder a los servicios de la infraestructura del proveedor de servicio de internet, en cada punto se tiene que implementar la VPN site to site con Ipsec, lo que permite asegurar las comunicaciones sobre el protocolo de internet hacia el concentrador de datos. Esto se realiza desde el dashboard en la sección “Security & SD-WAN”, opción “Site-to-site VPN”, donde se presentan dos tipos de VPN: Hub y Spoke.

En el enlace o red de Cuenca DC, se ha seleccionado tipo Hub, ya que en este se encuentra el concentrador de datos y a su vez corresponde al equipo MX100, las demás agencias sucursales, se selecciona tipo Spoke.

Figura 27

Configuración de tipo de VPN site to site Hub y Spoke.

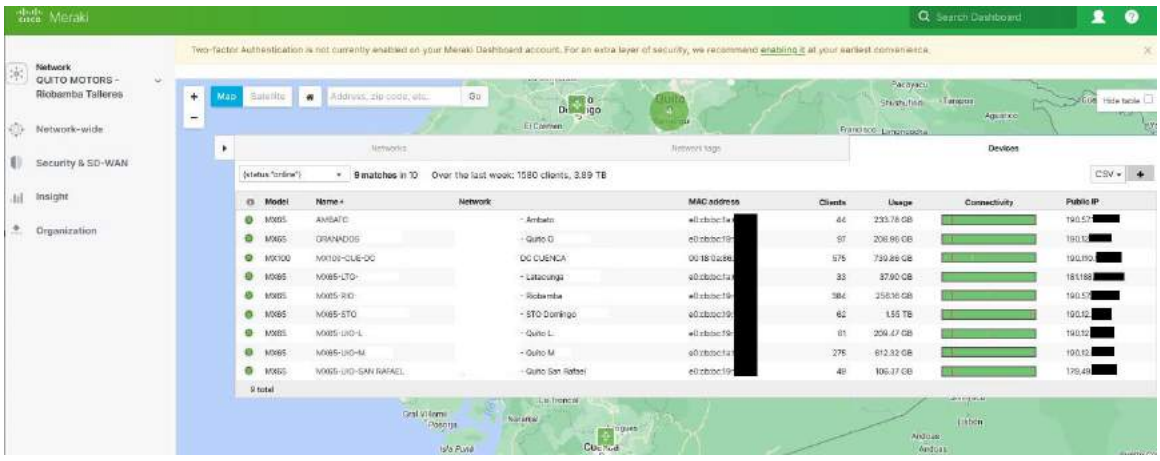


Fuente: Elaboración Propia

El proceso de configuración se realiza en los 9 enlaces y al finalizar el mismo podemos visualizar el dashboard completo para su administración y control, tal como se detalla en la **Figura 28**.

Figura 28

Configuración de tipo de VPN site to site Hub y Spoke.



Configuración de Seguridad

La plataforma de cisco Meraki, tiene integrada su función interna de firewalls, la que permite crear las reglas de acceso y seguridad de la red, como también bloquear el acceso a ciertas apps o puertos, para mejorar la gestión de la seguridad en la red, esto se configura desde la sección de “Security & SD-WAN” en la opción “Firewall”, como se observa en la **Figura 29**.

Figura 29

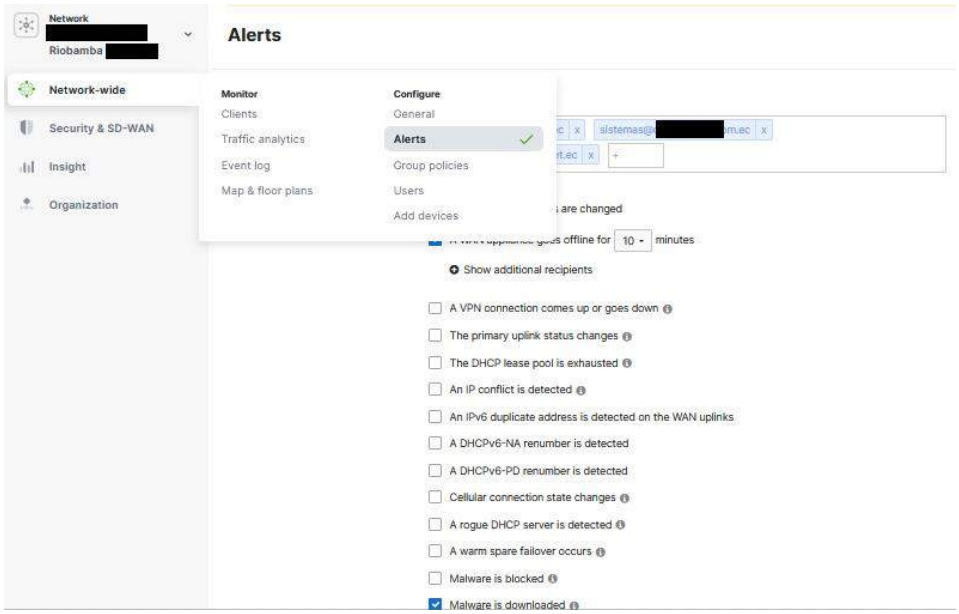
Configuración de Firewalls.

Configuración de Alertas

Dentro de los requerimientos del cliente, se solicitó un reporte de alarmas que facilite la gestión a los administradores de red del cliente corporativo, para ello el dashboard de Meraki posee una herramienta denominada “Alerts” , esta herramienta permite seleccionar las cuentas de correo de los usuarios de administración de la red, y a su vez seleccionar los motivos de alerta, los mismo que llegarán como notificación al correo del administrador, esto se configura desde la sección “Network-wide” opción “Alerts”, como se visualiza en la **Figura 30**.

Figura 30

Configuración de Alertas.


Network
[redacted]
Riobamba [redacted]
Network-wide
Security & SD-WAN
Insight
Organization
Alerts
Monitor
Clients
Traffic analytics
Event log
Map & floor plans
Configure
General
Alerts
Group policies
Users
Add devices
sistemas@[redacted]m.ec
[redacted].ec
are changed
offline for 10 minutes
Show additional recipients
A VPN connection comes up or goes down
The primary uplink status changes
The DHCP lease pool is exhausted
An IP conflict is detected
An IPv6 duplicate address is detected on the WAN uplinks
A DHCPv6-NA renumber is detected
A DHCPv6-PD renumber is detected
Cellular connection state changes
A rogue DHCP server is detected
A warm spare failover occurs
Malware is blocked
Malware is downloaded

Capítulo IV: Resultados

Finalizada la implementación de la red hub and spoke sobre tecnología SD-WAN, se procede a realizar las siguientes pruebas de funcionamiento con las herramientas que ofrece la misma plataforma de Cisco Meraki.

Se realiza pruebas para determinar la latencia desde el punto Hub, es decir del equipo MX100 en la agencia de Cuenca hacia los puntos spoke del cliente corporativo, agencias restantes a nivel nacional con equipo MX65 como se observa en la **Figura 31**. Adicionalmente en la **Tabla 4** se observan los valores de latencia de todas las sucursales.

Figura 31

Prueba de latencia (ping) con la herramienta del dashboard desde MX100 hacia los equipos MX65 de las sucursales del cliente corporativo.

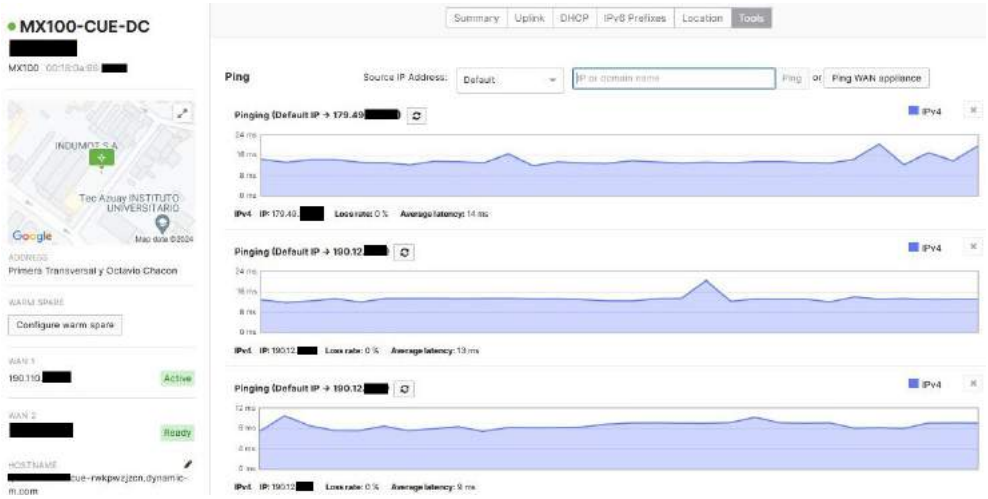


Tabla 4

Resultados de latencia y tasa de pérdida entre los enlaces de Cuenca (Hub) y las demás sucursales del cliente corporativo (spoke).

Agencias	**Latencia**	**Tasa de pérdida**
Ambato	14 ms	0
Latacunga	12 ms	0
Riobamba	14 ms	0
Santo Domingo	15 ms	0
Quito L	12 ms	0
Quito G	9 ms	0
Quito M	13 ms	0
San Rafael	14 ms	0

El valor de latencia promedio es de 13 ms de los enlaces desde la sucursal de Cuenca que es el punto Hub hacia las demás sucursales como spokes, que representa un valor menor con lo establecido para conexiones VPN donde oscila entre 20 ms y 100 ms (Interpretar Datos de Monitoreo SD-WAN, s.f.), este valor depende de la ubicación y la congestión de la red. La tasa de pérdida es 0, indicando que hay ausencia de pérdida de paquetes en la red.

En otro escenario se realiza una prueba similar a la anterior, pero en este caso se hace desde cada sucursal hacia el internet, haciendo ping a la dirección 8.8.8.8, como se observa en la **Figura 32**, y los datos de los resultaos se presentan en la tabla 5.

Figura 32

Prueba de latencia (ping) desde las sucursales del cliente corporativo hacia internet.

Tabla 5

Resultados de latencia y tasa de pérdida entre cada agencia del cliente corporativo e internet.

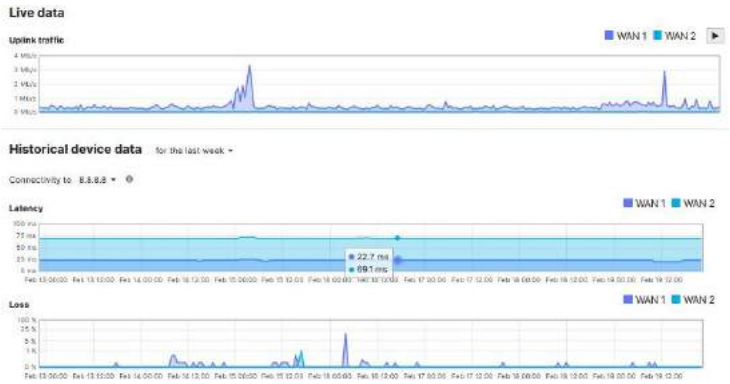
Agencias	Latencia	Tasa de pérdida
Cuenca DC	23 ms	0
Ambato	16 ms	0
Latacunga	15 ms	0
Riobamba	17 ms	0
Santo Domingo	15 ms	0
Quito L	13 ms	0
Quito G	13 ms	0
Quito M	13 ms	0
San Rafael	16 ms	0

El valor de latencia promedio es de 16 ms de los enlaces desde cada una de las sucursales del cliente corporativo hacia el Internet, como se observó en la prueba anterior es un valor menor a 20 ms. La tasa de pérdida es similar a la prueba anterior.

La plataforma de cisco Meraki también nos permite obtener un reporte de latencia y pérdida de paquetes en un período de tiempo, para poder determinar el estado de la red en tiempo real y agilizar la toma de decisiones.

Figura 33

Estado de la red sucursal Cuenca



A su vez nos permite obtener el valor del cálculo de la tasa real de transferencia (throughput), como se observa en la **Figura 34**. Este proceso se realizó en todas las sucursales y se presenta los datos en la Tabla 6.

Figura 34

Throughput de la red sucursal Cuenca

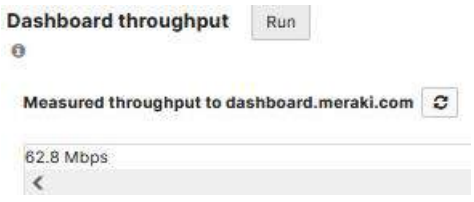


Tabla 6

Throughput de cada agencia del cliente corporativo.

Agencias	**Throughput**
Cuenca DC	62.8 Mbps
Ambato	16.7 Mbps
Latacunga	9.1 Mbps
Riobamba	16.9 Mbps
Santo Domingo	8.4 Mbps
Quito L	12.6 Mbps
Quito G	8.2 Mbps
Quito M	60.3 Mbps
San Rafael	12.4 Mbps

En seguridad, el firewall del dashboard de Meraki permite la detección de amenazas frecuentes con el número de ataques hacia la red, los clientes que presentaron vulnerabilidades e ips, ayudando en la red del cliente corporativo a mejorar la seguridad tomando en cuenta que ya cuenta con un equipo firewall de su red anterior.

Figura 35

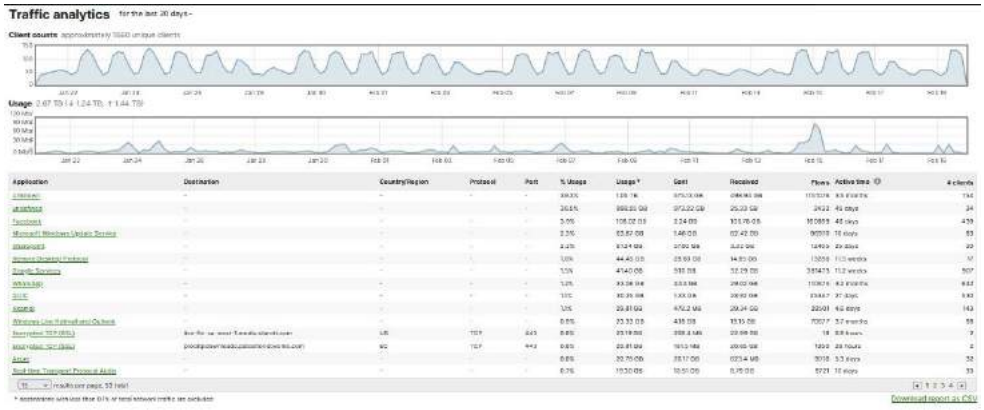
Centro de Seguridad de toda la red SD-WAN del cliente corporativo.

El tablero del centro de seguridad permite tomar acciones efectivas para mejorar la seguridad de la red, como también la creación de nuevas reglas en la configuración de firewalls que permitan mejorar la seguridad y control de la red, adicional identificar los clientes o redes más vulnerables. Adicional está herramienta permite limitar el acceso ya sea por vlans o sucursales a diferentes aplicaciones, como redes sociales, juegos, y ciertas plataformas de streaming.

Entre otras herramientas que presenta el dashboard de Meraki se encuentra el análisis de tráfico, el mismo que nos permite visualizar el consumo de ancho de banda que hay en la red, como también las aplicaciones que se utilizan dentro de la red y la cantidad de clientes que hacen el uso de ellas, como se muestra en la **Figura 36**.

Figura 36

Análisis del tráfico SD-WAN del cliente corporativo.

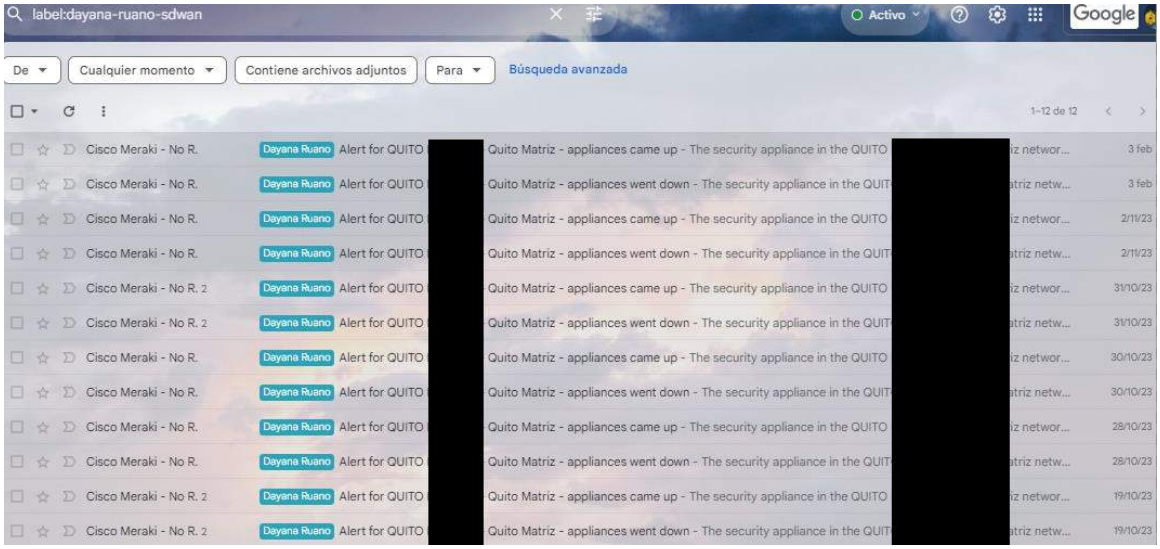


Esto permite al administrador de la red del cliente corporativo, analizar el balanceo del tráfico como a su vez generar reglas para limitar el tráfico según la importancia de algunas aplicaciones como VoIP.

Para ver el funcionamiento del sistema de alarmas que se explicó en la sección de la implementación, se dio autorización al usuario dayana.ruano para que lleguen las notificaciones por correo en el caso de haber algún problema de seguridad en la red de la sucursal Quito M, como se observa en la **Figura 37**. Las alarmas en el correo indican el problema existente como también cuando este se soluciona.

Figura 37

Alertas de seguridad en el buzón de correo.



Gracias al diseño implementado la red del cliente corporativo paso de 40 Mbps con tecnología de cobre a 350 Mbps en fibra óptica, servicio Wi-fi en diferentes zonas para clientes y áreas corporativas. Es decir, separados por VLANS, hemos podido administrar varias aplicaciones priorizando VoIP, acceso a la nube, control de la red WAN y LAN, control del tráfico y anchos de banda, gestión de la seguridad, entre otros. Cumpliendo de esta forma con la gestión centralizada y automatización de la red solicitada por el cliente corporativo.

A continuación, se presenta en la

Tabla 7 un resumen de resultados del despliegue de la solución del diseño e implementación de la red hub and spoke sobre SD-WAN.

Tabla 7

Check list de resultados del proveedor de servicios de internet hacia el cliente corporativo.

Checks:	
Verificación de SDWAN puede ser configurado en Cisco Meraki MX.	Pass: ☒ Fail: ☐
Facilidad de implementación	Pass: ☒ Fail: ☐
Gestión Centralizada	Pass: ☒ Fail: ☐
Monitoreo de interfaces y tráfico en Tiempo Real	Pass: ☒ Fail: ☐
Herramientas de troubleshooting	Pass: ☒ Fail: ☐
Creación de Redes LAN	Pass: ☒ Fail: ☐
Configuración de Alertas	Pass: ☒ Fail: ☐
Configuración de Usuarios	Pass: ☒ Fail: ☐
Visualización de trafico de usuarios	Pass: ☒ Fail: ☐
Aplicación de políticas de priorización de tráfico	Pass: ☒ Fail: ☐
Aplicación de Políticas de Seguridad	Pass: ☒ Fail: ☐
Resultados Esperados:	Cisco Meraki SDWAN en MX trabaja según los resultados esperados.

Capítulo V: Conclusiones Y Recomendaciones

Conclusiones

- En el estudio de la tecnología SD-WAN para aplicación en diseños de redes corporativas, se logró concluir que es más conveniente a diferencia de tecnologías como MPLS y VPN, como se evidencio en la Tabla 1, donde se pudo comparar las tres tecnologías, siendo SD-WAN una tecnología más completa que permite a las redes corporativas adaptabilidad y escalabilidad junto al desarrollo de las telecomunicaciones a la era digital.
- Se consideró los diferentes proveedores de tecnología SD-WAN existentes, concluyendo como mejor opción los equipos Cisco Meraki ya que en Ecuador son los más utilizados por otras empresas, adicional es la opción prioritaria del proveedor de servicios de internet corporativo.
- Se desarrollo el diseño de la red, tomando los antecedentes y requisitos de la red antigua del cliente corporativo, permitiendo con el nuevo diseño bajo la tecnología SD-WAN, reducir el número de dispositivos que eran usados por la tecnología MPLS que antes tenía el cliente, como a su vez reducción de costos al no usar enlaces dedicados sino VPN sitio a sitio bajo IPsec como enlaces de fibra que son menos costosos y su ancho de banda es mayor desde 15 Mbps hasta 1Gbps.
- Se implemento una topología Hub and Spoke dado que los equipos cisco Meraki tienen esta limitación en el desarrollo de su software, seleccionando como Hub a la sucursal donde se encuentra la central de datos y las demás sucursales se configuraron como spoke, permitiendo una gestión centralizada.
- Se realizó pruebas de latencia entre los enlaces de las sucursales hacia la salida de internet como también entre la sucursal designada como Hub y las sucursales spoke,

donde el valor promedio en los dos casos fue menor a 20 ms como se muestran en las tablas 4 y 5 de resultados, esto nos indica que la latencia obtenida es menor al promedio que se obtiene en enlaces de VPN y fibra óptica que varía entre 20ms a 100ms.

- Se reviso la herramienta de seguridad que tiene el dashboard de Meraki, donde se puede observar las amenazas registradas en cada red de las sucursales como general, lo que permite disminuir las vulnerabilidades que puede presentar la red corporativa. Crear nuevas reglas para aplicar en el firewall que viene integrado dentro del dashboard.
- Se verifico el funcionamiento de la herramienta de análisis de tráfico que permite tomar decisiones precisas para el balanceo de carga en el tráfico de la red, como también establecer políticas que limiten el ancho de banda para ciertas aplicaciones y a su vez generar prioridad para otras, limitar el acceso a ciertas aplicaciones como redes sociales, juegos, etc en cada vlan de la red.
- En la implementación se concluyó que es más sencillo la configuración de la red, ya que solo es necesario conectar el equipo Meraki con una licencia activa a una fuente de internet, ingresar al dashboard de Meraki con la cuenta asignada al usuario, configurar y realizar soporte remotamente.
- Se conoció varias herramientas y funciones que presenta el dashboard de Meraki, las mismas que facilitan la administración y automatización de la red, como por ejemplo las notificaciones de alarmas que llegan a los correos de los administradores de la red cuando hay algún inconveniente o caída de los enlaces.
- El diseño e implementación de la red del cliente corporativo bajo la tecnología SD-WAN evidenció los varios beneficios que se obtiene al migrar a esta tecnología permitiendo

que otros clientes del proveedor de servicios de internet se interesen por este tipo de tecnología que adicional va de la mano con el crecimiento de las telecomunicaciones en la era digital, IoT y cloud.

Recomendaciones

- Conocer los objetivos comerciales y tecnológicos que requiere el cliente corporativo, como los antecedentes de la red actual, incluyendo la topología, tecnología y calidad del servicio, para realizar un preciso diseño de red.
- Identificar y priorizar las aplicaciones críticas para la red del cliente corporativo. Configurar la SD-WAN para optimizar el tráfico de estas aplicaciones y garantizar su rendimiento.
- Después de la implementación del nuevo diseño de red, dar un monitoreo continuo para evaluar el rendimiento de la red. Ajustar la configuración según sea necesario del cliente corporativo.
- Realiza auditorías de seguridad periódicas para garantizar que la SD-WAN cumpla con las políticas de seguridad de la organización y para identificar y abordar posibles vulnerabilidades.
- Seleccionar proveedores de SD-WAN confiables que se ajusten a las necesidades de la red, considerando que este sea compatible con los equipos que se posee para generar un costo menor, como también que sean escalables y con una fácil gestión de soporte.
- Para la implementación es muy importante verificar que las licencias de los equipos Meraki estén activas, ya que sin una licencia no hay como configurar las características que son necesarias para que este acceda a la red de SD-WAN en la nube.

Trabajos Futuros

Como trabajos futuros se propone realizar un estudio de cada una de las funciones que dispone el dashboard de Cisco Meraki, para poder sacar más beneficios de las herramientas.

Comparar la tecnología Cisco Meraki con otro proveedor de servicio de SD-WAN como Fortinet o VMware, al ser los proveedores más utilizados en Ecuador.

Realizar un estudio sobre el avance de la tecnología SD-WAN en el Ecuador para permitir que más empresas opten por esta tecnología y mejorar la brecha digital en el país.

Referencias Bibliografía

Barrios del Sol, M. (Junio de 2020). Diseño y despliegue de escenarios de red sobre un entorno de pruebas virtualizado SD-WAN basado en tecnología Viptela. Madrid, España: Universidad Politécnica de Madrid.

Beltran, E., & Pisfil, D. (Marzo de 2021). Red virtual privada basada en SDWAN y VPN IPSec como alternativa para teletrabajo seguro. . Guayaquil, Guayas, Ecuador: Universidad de Guayaquil.

Bustos, C. (10 de Diciembre de 2019). Análisis de factibilidad técnico y económico entre una red MPLS Traffic Engineering (TE) con IPSEC y una red Sd-Wan moderna. Sangolquí, Ecuador: Universidad de las Fuerzas Armadas.

Cabarcas , A., & Marrugo, A. (2008). *Diseño y arquitectura de redes WAN.* Cartagena de Indias: Universidad Tecnológica de Bolívar.

Carrillo, Á., & Roncansio, I. (22 de Junio de 2020). DISEÑO DE RED PARA LA INTEGRACIÓN DE SEDES TIPO MARKET DE UNA EMPRESA DE PRODUCCIÓN Y COMERCIALIZACIÓN DE ALIMENTOS BASADO EN CONECTIVIDAD SDWAN. Bogotá, Colombia: Universidad el Bosque.

CCNA. (10 de Agosto de 2019). *ccna desde cero*. Obtenido de ccnadesdecero.es/topologias-red-lan-y-wan/

Coggle. (Junio de 2016). *coggle.it*. Obtenido de https://coggle.it/diagram/WanktBOxzQABmNT8/t/m%C3%A9tricas-qos

ComputerWorld. (21 de Marzo de 2018). *computerworld.es*. Obtenido de https://www.computerworld.es/telecomunicaciones/como-funciona-mpls?xtor=erec-1

Cusco Perez, W. X., Cabrera Mejía, J. B., & Lugo García, J. (26 de Mayo de 2022). Análisis de las tecnologías SD-WAN usadas en Ecuador. *Revista Científica Dominio de las Ciencias*, págs. 870-886.

Datacom. (10 de Septiembre de 2018). Obtenido de https://datacom.global/cisco-meraki-sd-wan-2-2/

De la Fuente, E. (12 de Abril de 2011). Introducción a las redes WAN. Chile: Universidad Andrés Bello.

Estavillo, E. (29 de Junio de 2017). *ift.org.* Obtenido de http://www.ift.org.mx/sites/default/files/conocenos/pleno/presentaciones/maria-elena-estavillo-flores/comenorcalidad170628.pdf

Gartner. (Septiembre de 2023). *Fortinet*. Obtenido de https://www.fortinet.com/lat/solutions/gartner-wan-edge

Graaff, B. (Enero de 2021). *ngena.et*. Obtenido de https://www.ngena.net/es/what-is-sd-wan/

Guanoluisa, E. (2019). Diseño de la arquitectura de una red SDN mediante el protocolo Openflow con simulación en el software mininet para la infraestructura de una PYMES. Quito: Universidad de las Américas. Obtenido de https://repositorioslatinoamericanos.uchile.cl/handle/2250/2795725

Heydari, S. S., & Ellawindy, I. (2019). *"QoE-Aware Real-Time Multimedia Streaming in SD-WANs.* Paris: IEEE Conference on Network Softwarization (NetSoft). doi:10.1109/NETSOFT.2019.8806622

Hinojosa, M. (Julio de 2009). 1ESCUELA POLITÉCNICA NACIONAL FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA DISEÑO DE UNA RED MPLS UTILIZANDO EL PROTOCOLO IPV6 PARA PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES. . Quito, Pichincha: Escuela Politécnica Nacional.

Imagar. (16 de Febrero de 2021). *imagar.com*. Obtenido de https://www.imagar.com/blog-desarrollo-web/que-es-la-arquitectura-mpls/

Interpretar Datos de Monitoreo SD-WAN. (s.f.). Obtenido de Watch Guard Help Center: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/sd-wan/sd_wan_data.html

Jiménez, N. (Noviembre de 2020). IMPLEMENTACIÓN DE UN PROTOTIPO DE UNA RED SDWAN (SOFTWARE - DEFINED WIDE AREA NETWORK) UTILIZANDO TECNOLOGÍA DE JUNIPER NETWORKS. Quito, Pichincha, Ecuador: Escuela Politécnica Nacional .

López, J. (27 de Octubre de 2020). Emulación de una red SD-WAN (Software-Defined Wide Area Network) utilizando tecnología Fortinet y el software GNS3. Quito, Pichincha, Ecuador: Escuela Politécnica Nacional.

Marín, L. (2021 de Agosto de 2021). Diseño y simulación de una red WAN definida por software, mediante la tecnología SD-WAN, para optimizar la disponibilidad de red y aplicar control por aplicativos. Guayaquil, Ecuador: Universidad Católica de Santiago de Guayaquil.

Mingrone, N. (2019). Red privada de centro médico aplicando tecnología SD - Wan. Argentina: Universidad Argentina de la Empresa.

Netec. (28 de Marzo de 2019). *Netec expertos enseñando a expertos*. Obtenido de https://www.netec.com/post/viptela-simplifica-la-gestion-de-su-red-wan

Olmo, J. (8 de Enero de 2019). Presente y futuro de las redes WAN: SD-WAN y NFV. España: Universitat Oberta de Catalunya (UOC).

OptimaFacility. (30 de Septiembre de 2020). Obtenido de https://www.optimagrupo.com/redes-de-oficinas-satelite-el-nuevo-futuro-de-las-empresas-tecnologicas/

ORACLE. (2018). *docs.oracle.com*. Obtenido de https://docs.oracle.com/es/solutions/hub-spoke-network/index.html#GUID-005D02B1-AC7B-437E-A28B-1FC02822D363

Quezada, H. (22 de Marzo de 2016). Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja. Loja, Ecuador: Universidad Nacional de Loja.

Quintana, S., & Tabares, M. (Noviembre de 2011). MULTIPROTOCOL LABEL SWITCHING (MPLS): USOS, APLICACIONES Y ÁREAS PROMISORIAS DE LA TECNOLOGÍA. Cartagena de Indias, Colombia: Universidad Técnologica de Bolivar.

Romero, E., & Cuenca, J. (6 de Noviembre de 2020). Implementación de SD-WAN Corporativo para el uso eficiente de las telecomunicaciones para el Holding Quito Motors. *Polo del Conocimiento*, 163-179.

Romero, I. (2017). Estudio del protocolo Openflow usando el modelo de red definida por Software (Software Define Networks). Caso de estudio la Universidad Técnica de Manabí. Quito: Pontificia Univeridad Católica del Ecuador. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/14424/TESIS%20WILSON%20-%20PUCE-10-11-17.pdf?sequence=1&isAllowed=y

Stackscale. (27 de Julio de 2021). *stackscale.com*. Obtenido de https://www.stackscale.com/es/blog/que-es-una-vpn/

Suárez, D. (Junio de 2020). Redes wan definidas por software SD-WAN. Esapña: Universitat Oberta de Catalunya (UOC).

Universidad Politécnica de Valencia . (28 de Junio de 2013). Obtenido de https://ingenieriaaeroportuaria.blogs.upv.es/2013/06/28/hub-and-spoke/

Valero, E. (16 de Julio de 2019). ROYECTO DE EVOLUCIÓN DE UNA RED WAN TRADICIONAL DE UNA EMPRESA A UNA RED SD-WAN. España, Valencia: Universidad Politécnica de Valencia.

Zheng , L. (12 de Mayo de 2017). DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN PARA LA EMPRESA PALINDA. Quito, Pichincha, Ecuador: Universidad San Fracisco de Quito.