FACULTAD DE CIENCIAS E INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA CON MENCIÓN EN TELECOMUNICACIONES

TESIS

Para optar el título profesional de Ingeniero Electrónico con Mención en Telecomunicaciones

Diseño de enlaces WAN para la mejora del QOS de la red de telecomunicaciones en medianas y grandes empresas mediante la interconexión de sedes por tecnología VPLS

PRESENTADO POR

Laura Asenjo, Cristhian Jesús

Macedo Salvatierra, Robert

ASESOR

Victor Jose Espinoza Araujo

Lima, Perú, 2025

INFORME DE ORIGINALIDAD ANTIPLAGIO TURNITIN

Mediante la presente, hago de conocimiento:

1. CRISTHIAN JESUS LAURA ASENJO, identificado con DNI 70462300
2. ROBERT MACEDO SALVATIERRA, identificado con DNI 41980224

Egresados de la Escuela de Ingeniería Electrónica con mención en telecomunicaciones del año 2018 - II y habiendo realizado[1] la Tesis para optar el Título Profesional[2] de Ingeniero Electrónico con mención en telecomunicaciones, se deja constancia que el trabajo de investigación fue sometido a la evaluación del Sistema Antiplagio Turnitin el 15 de enero del 2025, el cual, ha generado un porcentaje de originalidad[3] de 18 %

En señal de conformidad con lo declarado, firmo el presente documento el 15 de enero del 2025.

Egresado 1
Cristhian Jesus Laura Asenjo
DNI: 70462300

Egresado 2
Robert Macedo Salvatierra
DNI: 41980224

Asesor
Mgr Victor Jose Espinoza Araujo
DNI: 46211909

1 Especificar qué tipo de trabajo es: tesis (para optar el título), artículo (para optar el bachiller), etc.

2 Indicar el título o grado académico: Licenciado o Bachiller en (Enfermería, Psicología …), Abogado, Ingeniero Ambiental, Químico Farmacéutico, Ingeniero Industrial, Contador Público …

3 Se emite la presente declaración en virtud de lo dispuesto en el artículo 8°, numeral 8.2, tercer párrafo, del Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI, aprobado mediante Resolución de Consejo Directivo N° 033-2016- SUNEDU/CD, modificado por Resolución de Consejo Directivo N° 174-2019-SUNEDU/CD y Resolución de Consejo Directivo N° 084-2022- SUNEDU/CD.

1501

INFORME DE ORIGINALIDAD

18%	15%	3%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	abcxperts.com Fuente de Internet	2%
2	Submitted to Universidad de Ciencias y Humanidades Trabajo del estudiante	1%
3	1library.co Fuente de Internet	1%
4	hdl.handle.net Fuente de Internet	1%
5	www.juniper.net Fuente de Internet	1%
6	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	1%
7	Submitted to Universidad Politecnica Salesiana del Ecuado Trabajo del estudiante	<1%
8	distribucionelectrica4.minem.gob.pe Fuente de Internet	<1%

RESUMEN

Las redes de comunicaciones son un factor importante y crítico para las empresas o corporaciones que manejen flujos de información. Se requiere que la transmisión sea seguro, con un flujo de tráfico estable, dado que en la actualidad gran parte de las entidades comprenden estructuras distribuidas, contando con sedes en varios lugares o puntos geográficos. Las empresas en el Perú tienen la necesidad de interconectar sus sedes, debido a ello se necesita una red óptima con un tiempo de respuesta eficaz que permita la comunicación fluida de su información, además de tener sus datos protegidos y enlaces dedicados que no se compartan con otros clientes.

Actualmente las corporaciones requieren enlazar sus sedes sin tener la obligación de construir una infraestructura que ocasione altos costos, para atender esta necesidad existen proveedores de servicios que brindar el servicio de implementación y acceso que permiten interconectar redes LAN distantes, así mismo, el proveedor se encarga de la configuración necesaria para llevar la información de manera segura ante un posible robo de información, así no se tendrá problemas de intrusión en su red.

Por medio de este proyecto, se plantea la implementación de una red que permita interconectar sedes a nivel nacional por medio de una VPN de área extensa, con el fin de que las empresas puedan tener control y monitoreo del flujo de información de sus sedes, para subsanar costos logísticos, y mejorar sus servicios de comunicaciones.

Palabra clave: Red de interconexión, LAN, Red privada virtual, VPN, MPLS, VRRP.

ABSTRACT

Communications networks are an important and critical factor for companies or corporations that manage information flows. The transmission is required to be secure, with a sending and receiving of data in real time, given that at present a large part of the entities comprise distributed structures, having offices and headquarters in different geographical points.

Companies in Peru have the need to interconnect their headquarters, because of this you need an optimal network with an effective response time that allows the fluid communication of your information, in addition to having your data protected and dedicated links that are not shared with other customers.

Currently corporations require to link their headquarters without having the obligation to build an infrastructure that causes high costs, to meet this need there are service providers that have the transport and access infrastructure that allow interconnecting distant LAN networks, likewise, the provider is responsible for the necessary configuration to carry the information safely against a possible theft of information, this way you will not have intrusion problems in your network.

It is intended to carry out the implementation of a network that allows interconnecting headquarters nationwide through a virtual private network of wide area, so that companies can have control and monitoring of the flow of information from their headquarters, to correct logistics costs, and improve their communications services.

Keywords: Interconnect Network, LAN, Virtual Private Network, VPN, MPLS, VRRP

CONTENIDO

Lista de figuras

Lista de tablas

INTRODUCCIÓN

La necesidad de administrar, almacenar y comunicar la información en el sector empresarial, ha sido y es una prioridad. Con el surgimiento de los equipos informáticos y su desarrollo tecnológico, el compartir información en tiempo real entre los diferentes sistemas informáticos es vital, en consecuencia, surgieron las redes de comunicaciones (Canle Fernandez, 2025).

En un principio las redes de computadoras o comunicaciones tenían fines militares o políticos, sin embargo, con la surgimiento o extensión de las organizaciones corporativas y su expansión en distintos puntos geográficos, contener un sistema de comunicaciones estable, redundante y seguro se volvió un desafío para aquellas primeras redes de los años 60 (AQUAE FUNDACIÓN, 2021). Con la llegada de internet, se implementaron aplicaciones, protocolos, sistemas, etc. en redes locales (LAN, red área local) y globales (WAN, red de área global). Sin embargo, las deficiencias en la seguridad digital, confidencialidad e integridad en las transmisiones sobre internet, enlaces dedicados que comprendían costos muy altos, y la necesidad de velocidad en la transmisión de los datos, provocaron que nuevas aplicaciones y protocolos surgieran para generar redes altamente seguras y confiables, como las VPN (del español red privada virtual) y VPLS. (Barzola Abad, 2023)

Con el avance tecnológico, las empresas tienen la necesidad de seguir implementando y mejorando su conexión a internet, reemplazando tecnologías de antaño, como las estaciones intermedias, para dar paso a la tecnología moderna que ayude a mejorar su conexión para poder competir con la demanda del mercado actual.

Siendo así que a mediados de los 90, surgen las redes MPLS que han ayudado a mejorar la fluidez de las comunicaciones a nivel global. Asimismo, otro de sus grandes beneficios es que permite tener datos protegidos y enlaces dedicados que son exclusivos para cada cliente. (Penaloza Seijas, 2019).

En el Perú las empresas que cuentan con varias sedes requieren estar intercomunicadas, por lo cual necesitan de un ISP que pueda garantizar la instalación de la red tanto la configuración física como la lógica que facilitara llevar la información a todas sus sedes lejanas de manera segura y rápida. Sin

embargo, en general un ISP brinda un canal en el medio público de Internet, y para obtener, dependiendo de la zona geográfica, implementación de canales privados, tomaría sumas o costos exorbitantes que largo plazo afectaría el desarrollo económico de las empresas, además de requerir un canal dedicado por sede, puesto que se requiere hardware y medios para los servicios multimedia requeridos por las entidades, como lo menciona el Organismo Supervisor de Inversión Privada en Telecomunicaciones en las fichas técnicas de costo que publica (OSIPTEL, 2024).

A través de esta necesidad, el proyecto o trabajo de investigación se propone implementar enlaces de red de área extensa para la interconexión de sedes a nivel nacional mediante el servicio de LAN privada virtual o conocido por sus siglas VPLS, mediante la aplicación de protocolos y equipos de red configurados para dichos fines. El planteamiento, formulación del problema, se desarrolla en el capítulo I. Para el capítulo II se tiene el fundamento teórico, junto con los antecedentes, el marco teórico, metodológico, marco legal y la arquitectura del sistema. El desarrollo de la aplicación y lo que abarca las fases de diseño e implementación, se describe en el capítulo III. En base a la metodología elegida. La descripción del análisis de costo y beneficios correspondientes en el capítulo IV.

CAPÍTULO I: PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA DE INVESTIGACION

Las redes de comunicaciones o tecnología son vitales para las empresas, puesto que el flujo de información que viaja a través de sus canales debe mantenerse constante, ser enviada y recibida en tiempo real, además de ser rápida, y segura con anchos de banda moderados. Sin embargo, para lograr dicha característica, se requiere inversión en hardware y software para establecer canales privados o dedicados. Soluciones donde los costos son muy elevados tan solo para establecer un servicio único, dependiendo del punto geográfico. Smith (2021) menciona que solo tender 30 centímetros de fibra óptica, toma el precio de 1 a 6 dólares, dependiendo del tipo de fibra.

1.1.1. Planteamiento y descripción del problema

En los últimos cinco años, en el Perú, el número de empresas ha crecido exponencialmente. Según el Instituto Nacional de Estadística e Informática (2021) actualmente existen más de 3 millones empresas registradas activamente a nivel nacional. Solo en el 2021 ha habido un aumento del 11.9% en comparación con el periodo del año anterior. Debido a esta creciente demanda en los servicios que las empresas ofrecen, se ven en la necesidad de adquirir nuevas oficinas, mayor personal (recursos humanos), y extender su red de alcance geográfico, lo que implica jerarquizar la empresa en departamentos u oficinas para un mayor control y asignación de tareas y expandir sus únicas redes LAN. Dado que, para el tratamiento de sus datos, las empresas o entidades cuentan con servidores de correo electrónico, gestión y almacenamiento de archivos, y asimismo como acceso a la intranet (si se cuenta) de la empresa en su local principal o central (DACARTEC, 2024).

El crecimiento de una empresa demanda desafíos, requiere mayor administración del flujo de información y datos para los empleados, garantizando al acceso a las aplicaciones o servicios web de la empresa, independientemente de la ubicación, en cualquier parte del mundo. Para C3NTRO Telecom (2021) solventar estas

exigencias, es necesario que se implemente tecnologías similares a una WAN, permitiendo la intercomunicación entre sí de todas las oficinas o sedes que se encuentren distantes.

Para obtener altos grados de eficiencia, eficacia y productividad, las empresas deben proporcionar a sus empleados, servicios de red óptimos, con disponibilidad de trabajos a distancia, acceso seguro e integral. Las redes WAN (*Wide Area Network*) ocupan múltiples ventajas como la interconexión de los servicios o sistemas propios de la entidad, y solventan todas estas necesidades, sin embargo, también ofrecen desventajas de gran vulnerabilidad: altos costos de instalación, problemas de seguridad digital y mantenimiento de la red (PURPLE, 2023). Debido a la gran distancia que separan las sedes de algunas empresas a nivel nacional, es imposible llegar a través de un medio de transporte que permita conectar sus sedes remotas por cuenta propia, las redes de área amplia son complejas y complicadas, por lo que su configuración es realmente costosa, pues mientras más distante y grande sea la red WAN, mayor tendrá que ser la inversión. Obviamente los problemas de mantenimiento serán mayores, garantizar que el centro de datos o el servicio de comunicaciones esté disponible en todo momento, será una labor desafiante para los administradores. Contar con enlaces redundantes y cerrar brechas de seguridad será el mayor desafío para la empresa, con el fin de evitar tiempos de inactividad en los sistemas informáticos y comunicaciones.

Las redes de área amplia ofrecen ventajas muy significativas, pero utilizarlo en el escenario o lugar incorrecto, puede generar consecuencias económicas que pueden afectar gravemente a una empresa.

Como un camino alterno, la WAN publica más conocida: Internet, es una opción llamativa, su ventaja económica reduciría costos de instalación y configuración, pero sus inconvenientes frente a la seguridad, privacidad y balanceo de carga y descarga en el ancho de banda, requerirá implementación de tecnologías que cubran

estas brechas para emplearlo como medios de transmisión seguros, evitando utilizar canales dedicados o privados, para lograr así que las empresas conjuntamente con sus sedes y clientes tengan comunicación constante, pues como se mencionó, la inactividad es costosa, GLOBALSPEC (2015) estima que las empresas medianas y grandes pierden alrededor de 100 millones de dólares anuales por esos pequeños y largos tiempos de inactividad de TI (Tecnología e Información), afectando económicamente el crecimiento de la empresa.

1.1.2. Formulación del problema general

¿Cómo mejorar la calidad de servicio de la red de telecomunicaciones de empresas medianas y grandes sin la necesidad de implementar enlaces dedicados o privados?

1.1.3. Formulación de los problemas específicos

P.E.1: ¿Cuál es la situación actual de los servicios de redes y comunicaciones de sedes remotas que requieren interconectarse?

P.E.2: ¿Qué características técnicas se deben tener en cuenta para enlaces de redes dedicados?

P.E.3: ¿Cuáles serían los protocolos y medios de transporte adecuados para enlaces WAN redundantes y privados con el fin de mejorar el QoS de las redes de telecomunicaciones?

P.E.4: ¿Cómo implementar enlaces WAN que permitan mejorar el QoS de las redes de telecomunicaciones sin necesidad de emplear canales privados o dedicados?

P.E.5: ¿De qué manera se puede medir la eficiencia y rendimiento de los enlaces WAN?

1.2. DEFINICIÓN DE LOS OBJETIVOS DE LA INVESTIGACIÓN

1.2.1. Objetivo general

Implementar enlaces WAN mediante la interconexión de sedes por tecnología VPLS para mejorar el QoS de la red de telecomunicaciones sin la necesidad de implementar enlaces dedicados

1.2.2. Objetivos específicos

O.E.1: Describir la situación actual de los servicios de redes y comunicaciones de sedes remotas que requieren interconectarse.

O.E.2: Determinar las características técnicas que se deben tener en cuenta para enlaces de redes dedicados.

O.E.3: Diseñar enlaces WAN con protocolos y medios de transporte que permitan redundancia y privacidad para mejorar el QoS de las redes de telecomunicaciones.

O.E.4: Implementar enlaces WAN que permitan mejorar el QoS de las redes de telecomunicaciones sin necesidad de emplear canales privados o dedicados.

O.E.5: Realizar pruebas de estrés y conmutación a los enlaces de red de área extensa.

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.3.1. Justificación técnica

Actualmente existen diversas tecnologías para solucionar la problemática de la interconexión de sedes de las grandes empresas, como; OSPF, IS-IS, BGP, MPLS, VPLS, etc. Es factible implementar tecnologías que permitan la interconexión WAN, los beneficios que se tiene al usar estás tecnologías son: flexibilidad, escalabilidad y seguridad. Además, el sistema que se propone permitirá la conexión entre sedes, llevando el servicio de extremo a extremo con otros protocolos y tecnologías complementarias.

Algunas funciones que MPLS/VPLS permite usar son:

- Ingeniería de tráfico
- Calidad de servicio

- Alta disponibilidad de las redes
- Localización de fallas de extremo a extremo.
- Servicios múltiples desde una plataforma.

1.3.2. Justificación económica

La solución de emplear una WAN pública, es decir, contratar un ISP (proveedor de servicio), permite reducir el gasto en cuanto al despliegue de infraestructura e instalación de la red de transporte, debido a que el operador ya cuenta con una red implementada, además en caso de tener problemas de conectividad, es el ISP que se encargará de la solución a nivel de red de transporte.

1.4. ALCANCES Y LIMITACIONES DE LA INVESTIGACIÓN

1.4.1. Alcances

La implementación del enlace WAN abarca desde el CE (*Customer Edge*) en la sede central como el CE en las sedes remotas, pasando por la red del ISP.

La configuración necesaria para lograr la conectividad abarca protocolos *Layer 2* y *Layer 3* (capa 2 y 3) tomando como referencia el modelo OSI.

El diseño del enlace no considera la determinación del ancho de banda porque este parámetro es establecido por la empresa que requiere la interconexión en base al tipo de tráfico y número de comunicaciones entre sedes.

El protocolo de routing que se emplea es IS-IS (Sistema intermediario-Sistema intermediario) y para la ingeniería de tráfico se está implementado con MPLS. Tomando como referencia el modelo OSI, este estudio no abarca la capa física, transporte, sesión, presentación, ni aplicación.

1.4.2. Limitaciones

- El proyecto concluye con la simulación de una red WAN, mediante la implementación de equipos de red de gama media, que soporten protocolos de enrutamiento dinámico. Asimismo, también el servicio de LAN privada virtual, para la implementación de la interconexión entre sedes, empleando MPLS, creación de circuitos virtuales en capa 2, logrando comunicaciones, estable, segura y sin interrupciones a nivel WAN.
- El proyecto no abarca configuraciones de conmutadores, dado que la configuración principal se basa en VPLS, sin embargo, cabe mencionar que, al emplear conmutadores, se deben aplicar protocolos que eviten bucles, como spanning tree o sus versiones mejoradas.

CAPÍTULO II: FUNDAMENTO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Internacionales

López González (2017) en su tesis denominada “Diseño de una Red Privada Virtual usando una red MPLS”,definen el operador para interconectar sedes ubicados en distintos puntos geográficos, para la optimización de los servicios digitales que comprenden las empresas para su desarrollo económico y social. Buscando mejorar la disponibilidad, la seguridad y la escalabilidad de las redes de datos.

Según Lorío Cabezas & Mendoza Lopez (2015) en su tesis denominada “Estudio de la tecnología VPLS como solución de interconexión a las redes de datos que ofrecen los Proveedores de Servicios de Internet a los usuarios corporativos” de la Universidad Centroamericana, estudia está tecnología que brinda enlaces multipunto a multipunto, nos muestra las mejoras que se obtiene el ISP y la optimización del servicio para los clientes.

Barreto Priero (2013), en su artículo denominado “VPLS: alternativa de interconexión a través del *backbone* IP/MPLS de ETECSA” de la revista cubana de ciencias informáticas, describe una solución, la implementación *Virtual Private LAN Service* (VPLS), para la migración de servicios de *Virtual Private Network* que se conforman sobre la troncal *ATM/Frame Relay*, hacía la troncal *Internet Protocol Label Switching* (MPLS).

Según Hernández Hernández (2011), en su tesis denominada “VPLS una Opción de Transporte Ethernet” de la Universidad Central “Marta Abreu” de Las Villas, fundamenta las virtudes que se tiene al usar está tecnología, el objetivo es conectar sedes de una compañía, logrando facilidad, seguridad y velocidad, teniendo un mayor ancho de banda para brindar al cliente, en esta investigación se demostró los principios de funcionamiento de la tecnología VPLS.

Ospina & Zajar (2005) en su tesis denominada "MPLS/VPLS SERVICIO DE LAN PRIVADA VIRTUAL SOBRE MPLS" de la Universidad Tecnológica de Bolívar, explica la operación de VPLS y cómo implementar la conectividad en capa 2 a través del *backbone* metropolitano, finalmente en el documento se concluye algunas ventajas y limitaciones, los cuales servirá para el desarrollo de la investigación.

2.1.2. Nacionales

Según Espinoza Chipane (2018), en su tesis denominada "Propuesta de una red privada virtual para mejorar el servicio de comunicación en las tiendas *Mass* para la empresa Supermercados Peruanos SA" de la Universidad Autónoma del Perú, la investigación propone la solución de una Red Privada Virtual para mejorar los servicios de una empresa, reduciendo latencias, logrando una mejor comunicación con sus sedes, finalmente las conclusiones y recomendaciones nos ayudarán a mejorar nuestro proyecto.

Santamaría Silupu & Oviedo Calle (2016)en su tesis denominada "Estudio de los diferentes modelos de inter-as MPLS-VPNs para brindar una propuesta técnica que permita la comunicación entre múltiples proveedores de servicios" de la Universidad Nacional de Piura, estudia las características de MPLS-VPN sobre múltiples áreas, identifica también las ventajas y desventajas de la solución planteada.

Rojas Huamaní (2015), en su tesis denominada "Rápida reconvergencia en la ingeniería de tráfico aplicada a un escenario MPLS VPN" de la universidad Pontificia Universidad Católica del Perú, analiza la optimización de ingeniería de tráfico, y la finalidad la cual es la conmutación de rutas ante una falla.

Según Menéndez Avila (2012), en su tesis denominada “Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos” de la universidad Pontificia Universidad Católica del Perú, explica la solución que se tiene al implementar MPLS-VPN, se concluye con las ventajas y características que solucionan problemas a grandes empresas, este proyectó nos brinda un estudio del desempeño de estás soluciones.

Adrianzen Rugel (2017), en su tesis denominada “Diseño de una red IPVPN con tecnología MPLS para interconectar sedes de la empresa Cosapidata” de la Universidad Nacional Tecnológica de Lima Sur, la solución planteada en esta investigación es el diseño de una red IPVPN con tecnología MPLS, para tener seguridad y eludir tráfico que llegue a congestionar la red de la empresa.

2.2. MARCO TEORICO

2.2.1. Modelo OSI – capa 2 y 3

La expansión exorbitante de internet de las últimas décadas conllevo al crecimiento de las redes a nivel mundial. Sin embargo, muchas de estas nuevas creaciones utilizaban software o hardware diferentes lo cual hacía incompatible poder utilizar o conectarse entre ellas originando un gran problema. Debido a eso, la ISO realizo muchas y variadas investigaciones, concluyendo que era importante tener o crear un esquema o modelo de red que fuera compatible y pudieran comunicarse trabajando en conjunto (Interoperabilidad). Es así que se elaboró el modelo OSI, que define una arquitectura de comunicación de red en siete capas. (Cisco Community, 2023)

El modelo de referencia OSI (*Open System Interconexion*) brinda una serie de estándares que permite una mejor interoperabilidad en los diversos tipos de tecnología de red.

Dicho modelo o sistema contempla siete capas, también conocida como “pilas de protocolos”. Cada una de ellas consta de una interfaz bien definida con las capas superior o inferior. Cada capa tiene funciones de los protocolos de datos y un nombre descriptivo de acuerdo a su funcionalidad:

7. $Aplicación$
6. $Presentación$
5. $Sesión$
4. $Transporte$
3. Red
2. $Enlace\ de\ datos$
1. $Físico$

Para el presente trabajo se describirán las capas 2 y 3 de los niveles, dado que se emplean sobre todo en los enlaces WAN.

A. Nivel de enlace de datos

   Se encarga de transportar información de manera directa a través de redes físicas de manera confiable. El principal propósito es brindar un esquema de dirección que es usado para identificar dispositivos físicos como dirección de MAC. La PDU o la unidad de datos de protocolo de la capa de enlace de datos es una trama que puede tener desde unos pocos cientos de bytes hasta unos pocos miles de bytes, y maneja los datos como tramas. Como lo menciona Mohammed (2014) esta capa proporciona distintos tipos de funciones para comunicaciones orientadas a conexión y sin conexión.

B. Nivel de red

   En esta capa, la PDU es un paquete. La capa de red se encarga de tareas muy importantes relacionadas con el *routing* o enrutamiento de datos de una red a otra, asimismo el control de la subred. El enrutamiento es una operación compleja en algunas o muchas ocasiones, dado que multitud de factores

contribuyen a la elección de la mejor ruta de origen a destino. (Mohammed, 2014)

Se enlista funciones de la capa:

Tabla 1: Funciones de la capa de red

CAPA	Función
Capa de Red	Enrutamiento y retransmisión
	Conexión de red y multiplexación
	Segmentación y bloqueo
	Detección y recuperación de errores
	Secuenciación y control de flujo
	Transferencia de datos acelerada
	Reset
	Selección de servicios
	Asignación de dirección de red a dirección de enlace de datos
	Gestión de la capa de red

Nota. Funciones descritas por Mohammed (2014)

2.2.2. Equipos de Red

A. Router

Los enrutadores en español, son equipos dedicados a la recepción y envío de información o tráfico de la red en general de una empresa o entidad. Estos equipos facilitan el acceso a internet y las conexiones entre sedes a nacional e internacional debido a sus funciones de enrutamiento dinámico. Los enrutadores guían todo tipo de tráfico hacia su destino; a través de IP de destino, el enrutador analiza esta capa, da prioridad a la data y selecciona la mejor ruta para cada transmisión. (CISCO, 2012) Hay varias categorías o niveles entre enrutadores, como router principal, perimetral, de borde, de distribución, inalámbrico, entre otros.

B. Switch

Los conmutadores tienen la función de conectar todos los dispositivos finales, tal como un servidor, impresora, computadora, puntos de acceso, etc. en la propia red dentro de campos, universidades, empresas, etc., es decir, una red local. De tal modo, los switches crean redes locales para usos o aplicaciones privadas y públicas. El conmutador logra una red de capa 2, permitiendo que todo dispositivo con una tarjeta de red se puede comunicar entre sí. Similar a los router, dependiendo de las versiones también pueden manejar conexiones fuera de la red para los servicios de internet y sedes interconectadas, como los conocidos switch o conmutadores de capa 3. Existen los administrables, y los no administrables (*plug and play*). (CISCO, 2012)

2.2.3. IP Públicas y Privadas

Para que un equipo con una tarjeta de red pueda comunicarse hacia los servicios de internet requiere de un número o dirección que se distinga de los demás, y los paquetes o información llegue a su destino correcto. Las direcciones IP, del protocolo de internet cumplen esta función. Sin embargo, tanto para una red local o de internet, se requieren dos tipos de direcciones IP: públicas y privadas.

Las direcciones IP públicas, son determinadas por el proveedor de servicio contratado, para permitir la salida e ingreso del tráfico hacia y desde una red local. Estas direcciones son asignadas por el SP para la conexión a internet. Por otro lado, las direcciones privadas son asignadas internamente en la red local por el router del usuario, lo que permite las comunicaciones entre los dispositivos conectados a esa red, como lo menciona Wendell (2020) en la guía para el CCNA 200-301. Sin las direcciones públicas, los equipos dentro de una red local, no podrían acceder a los servicios de internet.

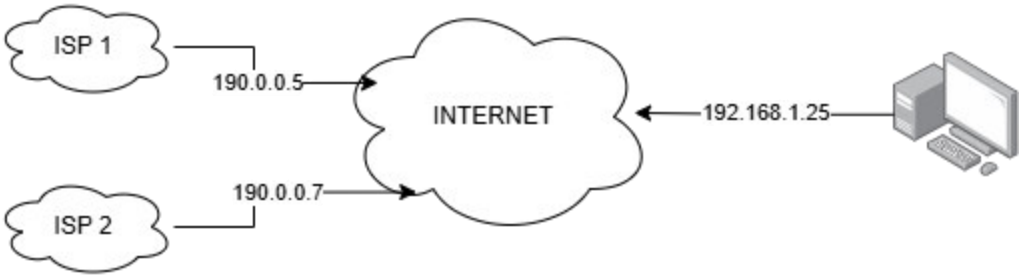

Figura 1: IP Públicas y Privadas

Fuente: Elaboración propia.

2.2.4. Enlaces WAN o red de área extensa

Las redes WAN conectan muchos equipos o redes locales en grandes áreas geográficas. Generalmente las entidades o empresas u organizaciones emplean enlaces WAN privados para interconectar sus sedes entre si a sus centros de datos o servicios públicos. Tecnologías como SD-WAN o MPLS se emplean comúnmente al implementar enlaces dedicados, o contratar proveedores de servicios. (López Cobos & Robalino Vásconez, 2018)

Existen dos tipos de WAN: privadas y públicas. Los enlaces WAN privados son redes propiedad de la organización y son administradas por la misma. Implementadas sea con líneas alquiladas o enlaces dedicados, con el objetivo de ofrecer y garantizar niveles altos de fiabilidad y seguridad. Por otra parte, una WAN pública es aquella empleada para conectar redes de diferentes organizaciones. Un ejemplo de ello es la red de Internet. (IONOS, 2020)

Una WAN está conformada por varias LAN. Una de sus características es que abarca una gran área geográfica y es muy útil cuando los usuarios desean acceder a otra red. Entre sus principales características se encuentran:

- Trabajan en áreas geográficas separadas
- Ayuda a los usuarios mantener comunicación con otros en tiempo real.
- Permite tener acceso a recursos remotos de otras LAN

Algunos ejemplos de WAN son:

- Red digital de servicio integrados (RDSI)
- Módems
- Línea de abonado digital
- Modo de transferencia Asincrónico (ATM)
- Portadoras T1, E1
- Red óptica Sincrónica (SONET)

2.2.5. Servicios de red y comunicaciones

Tanto en el ámbito privado o público, inclusive en las redes SOHO o red pequeña en casa, para definir el tipo de red o enlace a utilizar, este dependerá mucho de los servicios que van a viajar a través de la red.

Una empresa o entidad pública mediana o grande cuenta con distintas sedes en diferentes puntos geográficos. Principalmente el tipo de servicio más empleado son los sistemas de voz y video (telefonía fija e IP, Voz sobre IP, videollamada, reuniones virtuales, etc.) y centro de datos (Información de oficina, servidores, respaldo de datos, servicios públicos). Dependiendo del requerimiento o necesidad, se requieren la interconexión de las sedes o sucursales para que la información se encuentre en un flujo constante de movimiento, de ahí la importancia de una red WAN. (Rodríguez Toala et al., 2022)

Como consecuencia surgen las redes empresariales, creadas para atender las necesidades de las entidades, empresas u organizaciones, asimismo de las diferentes entidades públicas que cuentan con diferentes sedes. CLOUDFARE (2023) describe que estas redes empresariales son la interconexión de redes de área locales, conectándose a su vez con redes WAN, y plataformas *cloud* o servicio de nube.

Con lo expuesto anteriormente, se puede resaltar como principales servicios o información que viajaran a través de los enlaces de red como:

- ***Data* o información**, en el entorno empresarial o servicio público, los centros de datos, las nubes públicas y privadas son vital para el desarrollo de la empresa o entidad.
- **Servicios de comunicaciones**, la comunicación en tiempo real es pilar fundamental de toda entidad, estos servicios integran la telefonía por voz y video, reuniones virtuales, etc.
- **Plataformas en línea de acceso remoto**, para la distribución o adquisición de los servicios y datos.

En relación a la cantidad de dispositivos conectados, o información que viaja a través del medio, se le debe gestionar el ancho de banda.

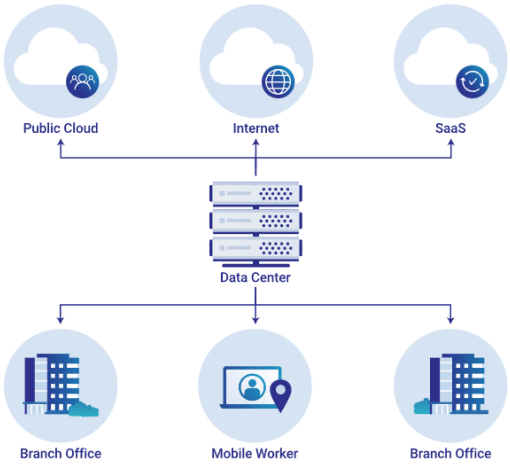

Figura 2: Red Empresarial

Fuente: CLOUDFARE (2023)

2.2.6. Ancho de banda y Rendimiento de la red

El ancho de banda y throughput o rendimiento en español, son dos aspectos técnicos similares, pero no iguales. Estos valores son el mayor interés en las redes LAN y WAN dentro del análisis global. Sin entrar en mucho detalle, el throughput es la cantidad de datos que puede enviarse en un determinado tiempo, por otro lado, el

ancho de banda es la capacidad que tiene un enlace para transportar la información. (Vesga Ferreira et al., 2015)

La elección del ancho de banda dependerá del servicio a transmitir, y la cantidad de enlaces a emplear para la transmisión de los datos. Para los servicios de voz y video, la importancia de disponer de un buen ancho de banda sin interrupciones es vital para que los sistemas de comunicaciones se mantengan estables.

2.2.7. Medios de transmisión

De manera similar como los autos viajan por las carreteras, del mismo modo la información que va través de la red, necesita un camino que pueda llevarlo a su destino. Los medios de transmisión son el canal por donde ira los datos o información. Empleando distintas tecnologías o tipos de medio físico por el cual viajara a través de la red. (Amazon Web Services, 2024)

Es necesario mencionar que los medios de transmisión para redes LAN y WAN, dependiendo de la aplicación, pueden ser diferentes. Los enlaces LAN son conexiones locales, a diferencia de las WAN, que interconectan sedes en áreas amplias. El proyecto se basa en redes WAN, por lo que generalmente se emplean enlaces de fibra óptica, conexiones satelitales, microondas, líneas telefónicas o antiguamente el ADSL.

A. Fibra óptica

   Tiene la capacidad de enviar gran cantidad de información por lo que es más utilizada actualmente por distintos SPs, a través de un hilo de fibra, se envía millones de bit por segundo, accediendo a servicios y plataforma sin retraso, en tiempo real y de manera simultánea, a altas velocidades, sin perder niveles de calidad óptimo. Dependiendo de la condición geográfica, el cable de fibra se puede adaptar por distintas infraestructuras internas y externas. Ofrece inmunidad al ruido y a las interferencias electromagnéticas.

Se tienen unos tipos de fibra óptica, que dependen del uso y el lugar de implementación: **Cable Auto Soportado o ADSS** empleado en estructuras áreas**, Cable Submarino** hundido bajo el agua**, Cable OPGW** empleado por las compañías eléctricas para la interconexión a largas distancias a través de las rutas de las líneas de alta tensión.

Como menciona WIN (2024), la fibra óptica tiene: Multimodo y Monomodo. Las Fibras ópticas multi-modo, transmiten varios rayos de luz por un solo hilo de fibra, empleado para cortas distancias. Las Fibras ópticas mono-modo transmiten un solo haz de luz a través de un hilo de la fibra, siendo su longitud de onda de igual tamaño del núcleo, debido, empleado para largas distancias.

B. Radio enlace

Los radioenlaces son una tecnología de comunicaciones inalámbricas que transmiten los datos u información por medio del aire, sin empleas cables o líneas fisicas. Emplean ondas electromagnéticas, sistemas microondas para transmitir las señales entre uno más puntos a largas distancias (SISTELEC, 2023)

Esto se logra gracias a sus características:

- **Alta velocidad de transmisión**
- **Baja latencia**
- **Conexiones confiables**

C. Enlace satelital

Los enlaces satelitales transmiten información como voz, video y otras aplicaciones a través de satélites que órbitan alrededor de la Tierra. Este tipo de medio logra la transferencia de datos en tiempo real, sin importan la distancia o ubicación entre las entre emisores y receptores. Gracias a esta característica, es una de las soluciones más empleadas por empresas

geográficamente distantes. Según SENCINET (2023), dependiendo de las partes involucradas, el servicio puede ser unidireccional o bidireccional, lo que permite el intercambio de tráfico entre dispositivos de direcciones opuestas.

Algunas de las ventajas son:

- Cobertura global
- Calidad
- Confiabilidad
- Flexibilidad

2.2.8. QoS – Calidad de Servicio

La calidad de servicio (QoS) es una variable vital en el campo de las redes. Hay varias definiciones concoretas sobre QoS pero sencillamente se le refiere a la calidad de servicio esperada en términos de tasa de pérdida de paquetes, retardo (*delay*), *jitter* y ancho de banda. Conocer la variación de estos valores permite gestionar, adecuar y priorizar el tipo de dato o tráfico entrante o saliente, optimizando la red a nivel general. Esto beneficia a las organizaciones en la administración de sus sistemas informáticos. (FORTINET, 2022)

QoS garantiza que las aplicaciones críticas muestren un rendimiento óptimo, en momentos que consumen altos anchos de banda en tiempo real. (Comunidad Huawei Enterprise, 2023)
Teniendo en cuenta el tráfico, los fabricantes de equipos de redes han implementado reglas, protocolos y técnicas para asegurar una gestión de priorización del tráfico de sus sistemas más críticos, se describe en la tabla 2:

Tabla 2: Técnicas para QoS

Técnica	Descripción
Priorización de Tráfico	Por ejemplo: VoIP, que es sensible al retrado cuando viaja por los routers y switchs
Reserva de recursos	Guarda recursos con el fin de utilizarlos y entregar niveles distintos de calidad de QoS
Cola de espera	Se crean políticas para proporcionar tratos preferenciales a ciertos flujos de datos
Marcado de tráfico	Cuando se requiere prioridad sobre el ancho de banda en una red, se marca dicho tráfico para identificarlo

Nota. La configuración y gestión del tráfico, dara como resultado excelente nivel de calidad de servicio, lo que se espera en una red WAN. (Comunidad Huawei Enterprise, 2023)

2.2.9. OSPF – Abrir el camino más corto primero

OSPF es un protocolo de enrutamiento dinámico, de pasarela interior. Es un protocolo de estado de enlace, que enruta paquetes dentro de un sistema autónomo único. Toma decisiones de *routing* empleando la información del estado de enlace, internamente realizando cálculos de ruta para determinar la ruta más corta primero (conocido como el algoritmo de Dijkstra). Su funcionamiento es simple, en el sistema autónomo, el equipo que ejecute OSPF inunda anuncios de estado de vinculo, estos contienen información sobre las interfaces conectadas y sus métricas de enrutamiento. Los *routers* emplean esta información anunciada de los estados para calcular la ruta de menor costo a cada red, creando una tabla de enrutamiento. (Juniper Networks, 2021)

Actualmente existen tres versiones: OSPF, OSPFv2 y OSPFv3.

2.2.10. VPLS – Servicio de LAN Privada Virtual

Según Nam-Kee (2005), los servicios de LAN privada virtual (VPLS) entran en escena porque permiten a los proveedores de servicios metropolitanos (SPs) con una infraestructura de conmutación de etiquetas multiprotocolo (MPLS) existente ofrecer servicios de Ethernet multipunto (EMS) geográficamente dispersos, también conocidos como servicios de LAN privada de Ethernet, definido por el *Metropolitan Ethernet Forum* (MEF). VPLS amplía literalmente el alcance físico de Ethernet para que funcione como una solución de red de área amplia (WAN).

VPLS es también una tecnología VPN L2 multipunto que permite al usuario final acceder directamente a varios sitios de destino asociados con la misma membresía VPN a través de una única conexión física o lógica. también requiere que la red tome una decisión de reenvío derivada de la dirección de destino del paquete. dentro del contexto de VPLS, la decisión de reenvío se basa en la dirección MAC de destino de la trama Ethernet.

Halabi (2003) describe que el servicio de LAN privada virtual, una L2VPN emula una LAN que proporciona capacidades completas de aprendizaje y conmutación. El aprendizaje y la conmutación se realizan al permitir que los enrutadores PE reenvíen tramas Ethernet basándose en el aprendizaje de las direcciones MAC de las estaciones finales que pertenecen al VPLS. VPLS permite que un cliente empresarial tenga el control total de sus políticas de enrutamiento WAN al ejecutar el servicio de enrutamiento de manera transparente sobre una red troncal IP / MPLS privada o pública. Los servicios VPLS son transparentes para los protocolos de capa superior y utilizan LAN emuladas L2 para transportar cualquier tipo de tráfico, como IPv4, IPv6, MPLS, IPX, etc.

Las siguientes secciones discuten los diferentes aspectos de un modelo VPLS:

- Requisitos de VPLS
- Singularización del servicio VPLS
- Encapsulación VPLS
- Crear una topología sin bucles
- Retiro de dirección MAC
- Aprendizaje no calificado versus calificado
- Escalado del servicio VPLS mediante VPL jerárquico (HVPLS)
- Descubrimiento automático
- Señalización usando BGP versus LDP
- Comparación de los enfoques *Frame Relay* y MPLS / BGP
- Modelo L2 VPN BGP
- Acceso Frame Relay con MPLS edge / core
- Servicio LAN transparente desacoplado (DTLS)

2.2.11. MPLS

De sus siglas *Multiprotocol Label Switching,* MPLS se le denomina como una tecnología empleada principalmente en las redes de telecomunicaciones a larga distancia, WAN. Sus funciones mejoran la eficiencia y velocidad para el envío de datos. Este multiprotocolo trabaja en base a etiquetas asignadas a los paquetes de datos, a diferencia de los protocolos convencionales que emplea exclusivamente las direcciones IP para guiar el tráfico. Con estas características los enrutadores logran tomas decisiones más rápidas en base a la etiqueta asignada, dado que no examina del todo el encabezado del paquete, acelerando la transmisión. (España Boquera, 2003)

La red MPLS o conmutación por etiquetas trabaja asignando etiquetas a los paquetes de datos para determinar la ruta por medio de la red. Los pasos que sigue son los siguientes:

Asignación de etiquetas: Cuando los paquetes ingresan a una red MPLS, se les asigna una etiqueta, indicando su destino y prioridad.

Enrutamiento por etiquetas. Los LSR (Label Switch Router) leen y verifican la etiqueta del paquete, para decidir el próximo salto y guiarlo a su destino.

Cambio de etiquetas. Cuando el paquete pasa por diferentes puntos o LSR, la etiqueta va siendo reemplazada, esto ayuda a los router mantener la ruta óptima, evitando procesamiento de cálculo periódicamente.

Entrega Final. Con el paquete llegado a su destino, la etiqueta se elimina y se le entrega según su dirección IP original. (André Pérez, 2020)

2.3. MARCO METODOLÓGICO

2.3.1. Tipo de investigación

La presente investigación es de tipo aplicada tecnológica, se basa en el desarrollo y aplicación de tecnología de conectividad para empresas privadas que desean compartir información fluida y en tiempo real entre las sedes de su dominio y, así evitar la filtración de datos importantes, mediante enlaces WAN privados en base protocolos de red y seguridad.

2.4. MARCO LEGAL

2.4.1. Ley n° 31809 – Ley para el fomento de un Perú Conectado

El 28 de junio del 2023, el Congreso de la República (2023) pone a disposición la presente Ley N° 31809, que tiene como objetivo implementar progresivamente la renovación tecnológica de redes de nueva generación en el servicio público de internet de banda ancha fija y móvil que faciliten una mejor conectividad en las zonas rurales y de prioritario interés social. La finalidad de la ley presente es reducir la brecha digital de los servicios públicos, permitiendo mejorar las condiciones económicas, productivas y sociales en las zonas rurales y urbanas.

2.4.2. Ley n° 29022 – Ley para la expansión de infraestructura en telecomunicaciones 2007

El Ministerio de Justicia (2007), mediante decreto supremo N°039-2007-MTC, la presente ley se centra es establecer regímenes especiales en el territorio nacional, principalmente en zonas rurales, para la implementación y desarrollo de los servicios públicos de telecomunicaciones, a través de medidas que promuevan la inversión privada en infraestructura necesaria, eliminando las barreras que intervengan en desarrollo de las actividades.

2.4.3. Estándares IEEE 802.

El comité 802 del IEEE (*Institute of electrical and electronic enineers*) desarrolla estándares para las redes LAN, posteriormente aprobados por la ANSI y la ISO.

Para propósitos del proyecto, se tienen en cuenta los siguientes estándares de dicho comité:

IEEE 802.3 CSMA/CD (MAC PARA ETHERNET)
IEEE 802.9 Integrated voice/data LAN (Voz y Datos en LAN)
IEEE 802.10 LAN Security
IEEE 802.12 100 VG any LAN cat.3

Los estándares mencionados permitirán seguir los reglamentos y protocolos para implementar enlaces de red a nivel WAN (Law, 2008)

2.5. DIAGRAMA DE BLOQUES Y ARQUITECTURA DEL SISTEMA

Se desarrolla el diagrama de bloques, según las fases del proyecto:

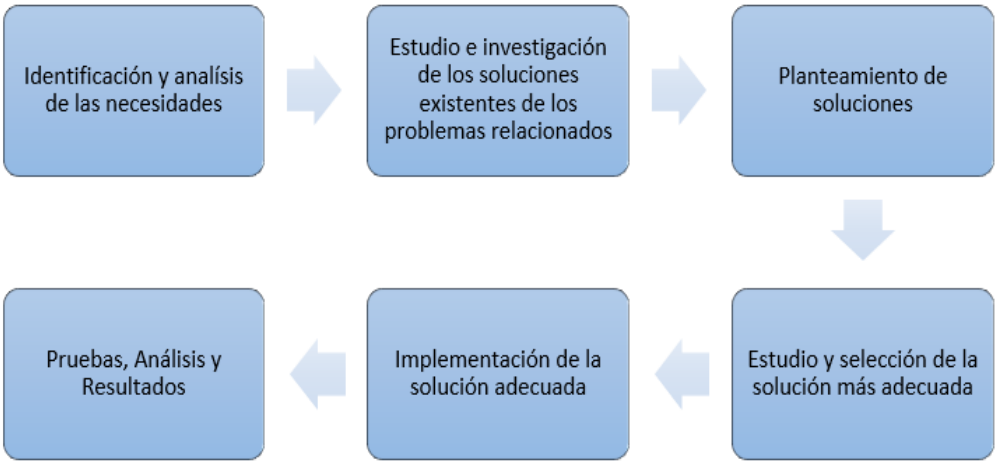

Figura 3: ***Diagrama de bloques general***

Fuente: Elaboración propia

El proyecto se basa en el sistema Usuario/Servidor. La red de área extensa consta de sedes centrales, que actúan como servidores, donde los usuarios podrán hacer uso de los distintos servicios informáticos y de telecomunicaciones, por medio de protocolos de red, y redes privadas virtuales.

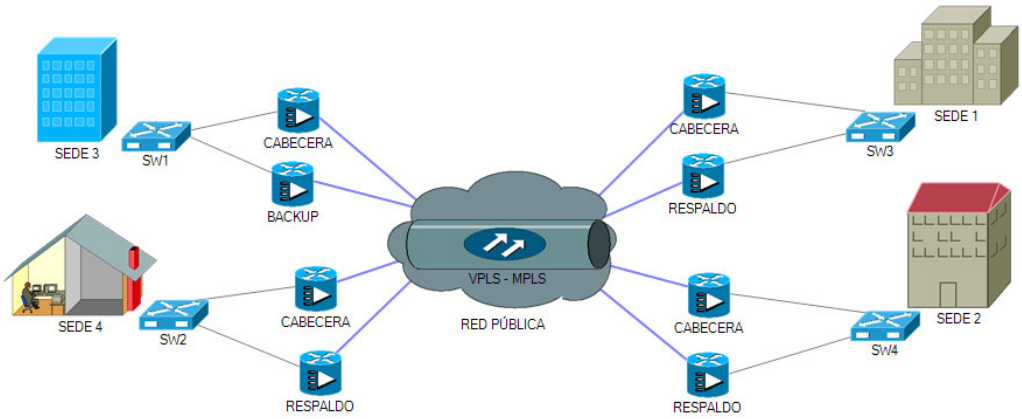

Figura 4: Arquitectura del sistema

Fuente: Elaboración propia

Habrá una interconexión entre sedes a nivel nacional, cada uno con enlaces redundantes, para una disponibilidad total. Como sede o servidor principal se tiene la cabecera, que se encargara en gestionar y controlar la red privada virtual

CAPÍTULO III: DESARROLLO DE LA APLICACIÓN

3.1. Analizar la situación actual de los servicios de redes y comunicaciones de sedes remotas que requieren interconectarse.

Al comparar los servicios de hace 25 años, con los nuevos avances tecnológicos en las redes de comunicaciones, existe un gran cambio radical de lo que se tiene actualmente. En los últimos 10 años, todo ha variado en el uso de los servicios de comunicaciones, como el tráfico de datos que se ha vuelto asimétrico, la arquitectura, su infraestructura, la creación de nuevos modelos de negocios o las mismas posiciones de las empresas. (Redondo Maíllo, 2022). Las redes de comunicaciones (o telecomunicaciones) son ahora un elemento clave de la infraestructura económica de una empresa, entidad o país, más aún con la aparición y desarrollo del internet. Con la llegada de la pandemia a nivel mundial, el estado de aislamiento empujo a los gobiernos la creación de nuevos servicios en línea, en áreas de la educación, salud, medio ambiente y economía, así también como el despliegue de las conexiones remotas y servicios de bases de datos entre las distintas sedes de una misma entidad o empresa, llegando a una transformación digital acelerada. Como lo comunico la Oficina de Prensa e Imagen Institucional de la Presidencia del Consejo de Ministros (2020).

Saltando a una evolución de las aplicaciones y uso de las redes, recordando solamente en los últimos veinticinco años, las necesidades y funcionalidades de las redes de datos y voz ampliamente han cambiado. A finales del siglo veinte, los servicios de telecomunicaciones se basaban fundamentalmente en el servicio telefónico (se trataba de un sector monopolístico que generaba grandes economías), y partir de los siguientes años, este mercado global de las telecomunicaciones se vio alterado por procesos de desregularización, surgimiento de nuevas tecnologías, la expansión de los servicios móviles, requerían la necesidad de mayores anchos de banda y enlaces de interconexión. (Rifa Pous et al., 2019)

A nivel nacional, empresas pequeñas y medianas que contemplan una o más sedes en diferentes zonas geográficas, no han establecido o implementado enlaces interconectados en sus redes de datos y voz. Al analizar su estado actual, muchas empresas (principalmente pequeñas y

medianas) y entidades del gobierno (urbano y rural) presentas problemas similares como:

A. Los servicios de comunicación entre sus sedes son deficientes, dado que sus únicos medios de comunicación es la telefonía móvil y correo electrónico, afectando el trabajo operativo y administrativo de la compañía. A pesar de que la digitalización o la era digital ha ido incrementando desde el 2013, según Choquehuanca De Villanueva (2023) en su estudio sobre la brecha digital de las MYPES.
B. No existe una administración correcta de las redes de datos y de voz, identificando gastos y consumos, para la toma de decisiones financieras y tecnológicas, por falta de habilidades o culturas antiguas, sobre la adaptación digital por parte de empresas con baja tolerancia al cambio. (MINERÍA Y ENERGÍA, 2025)
C. Muchos de los servicios web o centros de datos remotos no se pueden implementar en las sedes o sucursales debido a que las intranets se encuentran aisladas en la sede principal de la compañía, no están extendidas, dado que aproximadamente el 50% de las empresas en Perú no están capacitadas para los desafíos tecnológicos, como lo describe Mishima (2023)
D. No hay controles o políticas de seguridad. El filtro de los contenidos no es centralizado, en consecuencia, los usuarios finales no acceden al dominio principal y no hay protección de datos. (Rojas, 2024)
E. No cuenta con seguridad en la conectividad hacia las redes LAN y WAN. (EL COMERCIO, 2025)

Una de las razones, principalmente, es por la ignorancia de los costos por implementar enlaces dedicados, o desconocimiento de las mejoras tecnológicas de los equipos de redes y comunicaciones. Asimismo, empresas grandes, o entidades del estado o gobierno que tienen a su disposición distintas sedes en diferentes lugares, mantienen enlaces de red sobresaturados u obsoletos, debido al incremento del tráfico de datos que viajan a través de sus redes locales.

En consecuencia, al crecimiento de la solicitud de servicios relacionados con las comunicaciones dentro del ámbito operativo y administrativo tanto

a nivel de voz y datos y de las necesidades que cada compañía establece en sus planes de trabajo, es vital gestionar la mejoría de los servicios de las redes WAN en las distintas sedes que puedan contemplar.

3.2. Determinar las características técnicas que se deben tener en cuenta para enlaces de redes dedicados.

Para un enlace de red dedicado, es importante definir ciertos aspectos técnicos para el fin que se espera. De manera simplificada, el objetivo de un enlace dedicado es la conexión directa entre dos puntos o redes, que no puede o no debe utilizarse para otros medios o fines. A diferencia de un enlace convencional, la línea dedicada proporciona una conexión de alta capacidad directa para el intercambio de tráfico, garantizando el ancho de banda (real contratado) y ofreciendo niveles altos de rendimiento, baja latencia y alta fiabilidad (KEYFIBRE, 2024)

Sin embargo, para lograr los beneficios de un enlace dedicado, se deben tener en cuenta aspectos o características técnicas que permiten gestionar de manera adecuada la implementación de enlaces de red dedicado.

En ese aspecto, se consideran las siguientes características que se deben tener en cuenta para la implementación de enlaces de red dedicado:

A. Información o Servicios que viajan a través del medio

Es importante para determinar las características del enlace a implementar, si no se considera el servicio o información que viaja a través de la red, a futuro puede generar deficiencias en temas de rendimiento, escalabilidad y convergencia de las redes de comunicaciones.

Se puede resaltar como principales servicios o información que viajaran a través de los enlaces de red como:

- ***Data* o información**, en el entorno empresarial o servicio público, los centros de datos, las nubes públicas y privadas son vital para el desarrollo de la empresa o entidad. Muchos de los servicios web están alojados en servidores centrales, asimismo para los sistemas de archivos o ficheros a nivel WAN.

- **Servicios de comunicaciones**, la comunicación en tiempo real es pilar fundamental de toda entidad, estos servicios integran la telefonía por voz y video, reuniones virtuales, etc. Si hay demasiada interferencia o retardos, genera pérdidas económicas que afectar directa e indirectamente a la empresa o entidad. (DATADEC, 2023)

Dependiendo de la cantidad de dispositivos conectados, o información que viaja a través del medio, se le debe gestionar el ancho de banda.

B. Ancho de banda y Throughput de red

El ancho de banda adecuado para un sistema de comunicaciones o telefonía dependerá de la cantidad usuarios, llamadas en simultaneo, y el flujo de información, como acceso a servidores de alojamiento de datos, plataformas o aplicaciones.

El rendimiento actúa a la par con el ancho de banda, dado que el throughput o rendimiento dependerá de los factores internos y externos (el tipo de conexión, medios de transmisión, equipos empleados, retardos, tiempo de respuesta, etc.). Esto permitirá en términos simples, la velocidad de la red, la cantidad de datos que puede transmitir un enlace en un determinado tiempo o periodo.

Según SUGE3K (2020), para medianas o pequeñas, se considera generalmente 5 Mb/s por usuario, y en pequeñas o micro empresas, un ancho de banda de 7 a 10 Mb/s es suficiente para todos sus servicios. Sin embargo, los servicios y la cantidad de usuarios varia con el crecimiento de la empresa. Generalmente, una mediana empresa, con una navegación y servicios medios, puede tener de 5 a 30 usuarios. Estimando cada uno, una conexión simultánea a tope del 80%, navega empleando de 3 a 5 Mb/s (asumiendo que se tiene sistemas de control y seguridad como Firewalls). Con un promedio de 24 usuarios conectados, se tiene como 72 Mb/s de descarga, y añadiendo servicios extra de crecimiento de la compañía, redondeando se tiene un valor de ancho de banda de 100 Mb/s.

Esto no es definido, las redes varían y dependerá del departamento de tecnologías y comunicaciones como gestiona dichos valores.

C. Medios de transmisión

El medio de transmisión es importante a tener en cuenta, dado que es el canal por el cual viajara toda la información corporativa o los distintos servicios de comunicación empleados en las organizaciones. Dependiendo del costo y alcance de la organización, se puede optar por la utilización de líneas alquiladas, enlaces dedicados o el servicio público de internet, mediante protocolos de seguridad, como VPLS, IpSec, entre otros.

D. Calidad de Servicio

Para los fines del trabajo, se diferenciará el tráfico en clases de servicio, priorizando los sistemas de comunicaciones como telefonía IP o VoIP, transmisión de imágenes y video. La calidad de Servicio es un asunto a tener en cuenta para los enlaces WAN, dado que las empresas están en constante crecimiento. En ocasiones donde ampliar el ancho de banda no es lo correcto, sea por costo o infraestructura, la utilización del uso diferenciado del ancho de banda existente se vuelve un tema de importancia fundamental. La priorización del tipo de tráfico es vital para el rendimiento de la red. (Velarde Sagastegui, 2010)

E. Seguridad de enlace

Las redes WAN crecen de manera exorbitante, y con ello aumentan los desafíos en base al rendimiento y la seguridad. Este último debe ser abordado, no solo para proteger datos sensibles, sino también para resguardar a la empresa o entidad de posibles amenazas.

Dada la relevancia del tema, FLO NETWORKS (2024) menciona que la seguridad de un enlace es vital, tanto desde el punto origen al punto destino. Una red WAN conecta diferentes ubicaciones, permitiendo flujos de información sin interrupciones a través de las fronteras geográficas, el tener una brecha de seguridad puede ocasionar consecuencias catastróficas, como interrupciones de servicio, robo de información, pérdidas económicas, o daños en la reputación de una empresa o entidad pública. Por tanto, la seguridad es una característica técnica a tener en cuenta en la implementación de enlaces.

F. Costo de enlace

Dependiendo de la velocidad de conexión, el medio de transmisión, el ancho de banda y el rendimiento que pueda tener un enlace, su costo puede variar. Por ello, es importante tener en cuenta el coste de un enlace, dado que son directamente proporcionales al presupuesto y la necesidad del usuario. A mejor presupuesto, mejor servicio. (Instituto Federal de Telecomunicaciones, 2021)

3.3. Diseñar enlaces WAN con protocolos y medios de transporte que permitan redundancia y privacidad para mejorar el QoS de las redes de telecomunicaciones.

En este apartado se describe el diseño de la red para tener interconectadas las sedes remotas, esto puede aplicar para empresas medianas y grandes, por medio del servicio de LAN privada virtual.

Se tiene la siguiente la red de datos general de una empresa mediana con tres sedes aisladas entre si debido a que no mantienen enlaces dedicados o privados que permiten la interconexión global en sus distintos puntos geográficos. Esto no permite que los distintos servicios que mantienen las sedes centrales no estén disponibles o no accedan las demás sucursales, generando ralentización en el desarrollo socio-económico.

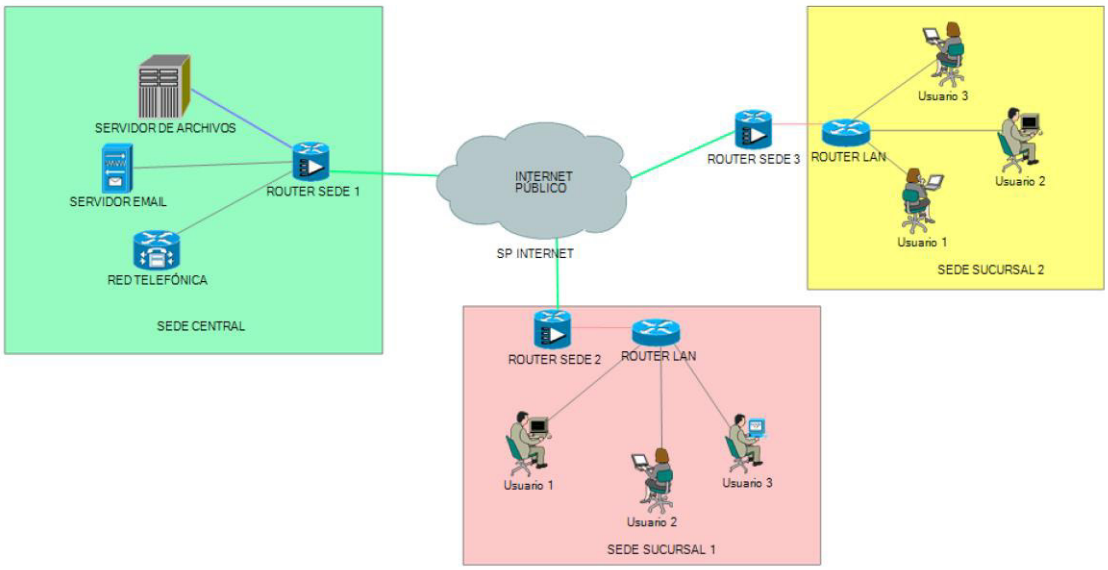

Figura 5: Red empresarial sin interconexión entre sedes

Fuente: Elaboración propia

Como se observa en la figura 5, las sedes remotas se encuentran aisladas de la red central que contiene los servicios públicos y empresariales. Se pueden nombrar ciertas deficiencias:

- **No existe interconexión o conectividad transparente**, por lo que los servicios de comunicaciones se encuentran aislados
- **Red Insegura**, dado que las conexiones se realizan a través del servicio de internet público y en su mayoría empresas medianas no implementan sistemas anti-intrusiones. (Castro, 2025)
- **Red central no jerarquizada**, lo que impide que los sistemas de redes sean flexibles y escalables.
- **Problemas en calidad de servicio**, al no existir un monitoreo de todo el tráfico en las sedes, aumenta la complejidad en dar prioridad al tipo de tráfico entrante y saliente.

Teniendo en cuenta estas deficiencias se llega a la meta del objetivo, que es diseñar una red WAN, que sea redundante y privada, sin establecer conexiones físicas o enlaces dedicados entre las partes involucradas.
Para ello se harán uso de diferentes protocolos y/o tecnologías para lograr dichos objetivos.
Para fines del proyecto, se ha analizado diferentes protocolos de red que puedan cumplir con estas exigencias presentadas. Independientemente de las marcas de los equipos de redes, al estudiar las características y beneficios de los protocolos, se concluye en que la mejor solución es VPLS, o el servicio de LAN privada virtual, puesto que integra protocolos avanzados que ofrece crear VPNs (red privada virtual) de área local (LAN) a través de una de red global, como el servicio de internet público.

La configuración de VPLS permite a las empresas u organizaciones interconectar múltiples ubicaciones por medio de un VPN, que requieren comunicarse entre sí, con una estructura confiable, privada y segura. En términos sencillos, toma las redes locales de cada sede o sucursal, y la convierte en una red WAN segura, creando redes virtuales que emulan una red local, logrando conectar ubicaciones remotas, como si de una red local física se tratase.

Con lo mencionado anteriormente, lo siguiente es detallar el diseño del enlace o la red WAN, como la topología, el hardware y software (protocolos de red) necesarios y que debe cumplir con lo siguiente:

- **Conectividad directa**, permitiendo a usuarios de diferentes sedes, en distintos puntos geográficos, acceder a los servicios y recursos compartidos.
- **Privada y Segura**, mediante técnicas seguridad digital, como encriptación y aislamiento, con el fin de garantizar la confidencialidad del tráfico entrante y saliente entre las sucursales de las organizaciones.
- **Escalable y Flexible**, no se requiere realizar cambios significativos en la infraestructura, permitiendo agregar nuevas sedes o equipos a la red existente.
- **Calidad de servicio (QoS)**, para priorizar en función de las necesidades de las aplicaciones, los distintos tipos de tráfico. Esto permitirá a la organización asegurar óptimas calidades de servicio en servicios como voz y video.
- **Redundancia,** en caso de que el router o equipo central falle por distintos motivos, contenga un sistema de respaldo que permita que la conexión sea constante y el tráfico siga fluyendo.
- **Reducción de costos**, lo más relevante en base al proyecto, eliminar la necesidad de implementar o establecer líneas o enlaces físicos dedicados entre sedes ubicados remotamente.

3.3.1. Diseño de la Red General y/o Estándar

Para que la nueva red WAN mediante VPLS cumple con lo mencionado, se realiza un nuevo diseño de las redes locales, reorganizando y ordenando las ultimas millas. Se tiene lo siguiente:

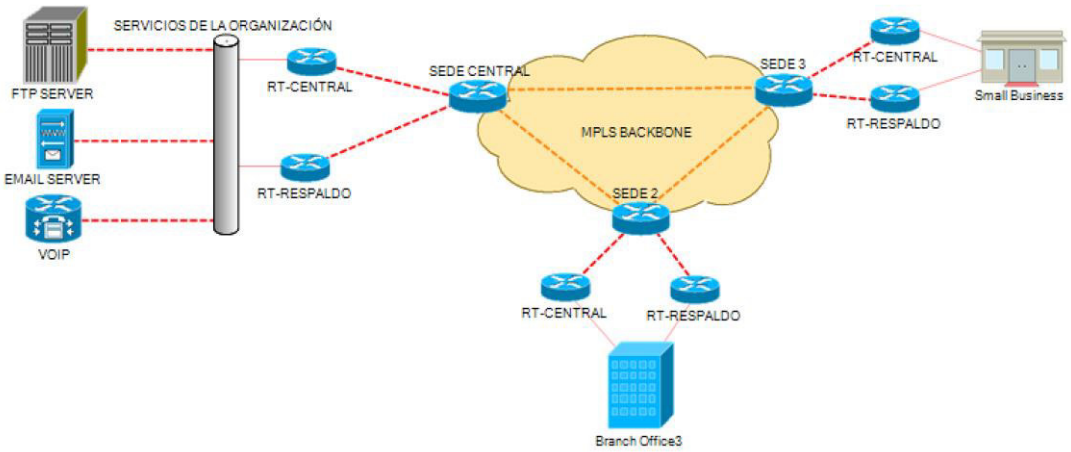

Figura 6: Red general con VPLS

Fuente: Elaboración propia

Se tiene la topología en la figura 6, que une las redes locales de tres sedes remotas, donde las sucursales dos y tres pueden acceder a los servicios de la sede central, proporciones conexiones directas, privadas de manera eficiente y segura. Al emplear MPLS como base subyacente, aplicar VPLS otorgara enlaces directos, flexibles y escalables, con el fin de expandir la infraestructura de la red empresarial.

Asimismo, se rige en router principales y de respaldo para generar redundancia en la red. Si en caso fallase un enlace, dependiendo de la necesidad del usuario o las aplicaciones, se configurará para responder antes los incidentes. Dando seguridad y calidad de servicio mediante la implementación de los protocolos, que continuación se detalla.

3.3.2. Elección de los equipos de red

Para el proyecto, se optó por emplear software y hardware de red de equipos de la marca Huawei, debido a que emplean protocolos estandarizados y compatibles con diferentes equipos de distintas marcas.

La configuración de los protocolos a emplear es similar para los diferentes equipos de distintas marcas. Al emplear protocolos

estandarizados, siguen la misma nomenclatura, por lo que no existe mucha diferencia entre usar Huawei, Cisco, Juniper, entre otras marcas.

En este diseño se tiene como propuesta dos enlaces para cada sede (cabecera y sedes remotas), en la última milla se enlazaría a diferentes nodos del proveedor del servicio, para una máxima disponibilidad del servicio de datos a nivel WAN.

Para los fines del proyecto se emplearon los modelos ATN-910, equipos de gama alta que soporta diferentes protocolos a nivel WAN.

Figura 7: Router HUAWEI ATN-910

Fuente: Elaboración propia

3.3.3. Configuración de etiquetas MPLS

Como se mencionó anteriormente, MPLS es un protocolo que emplea etiquetas para direccionar los paquetes a velocidades altas, por medio de la red IP troncal. Este protocolo es eficiente frente al enrutamiento tradicional, dado que es dinámico, asignado etiquetas a las direcciones IP, e intercambiando las mismas a través de la ruta, en reemplazo de las búsquedas por tablas IP. Esto permite a MPLS establecer túneles lógicos en la red, dado que es compatible con muchos protocolos de la capa de red y enlace, proporcionando

túneles en la red pública para diferentes servicios como L2VPN, L3VPN y EVPN.

En un primer escenario, se tiene la siguiente topología. Para simular esta red, se emplea el software de simulación eNSP de Huawei, que permite realizar configuraciones simuladas, aunque un poco limitadas.

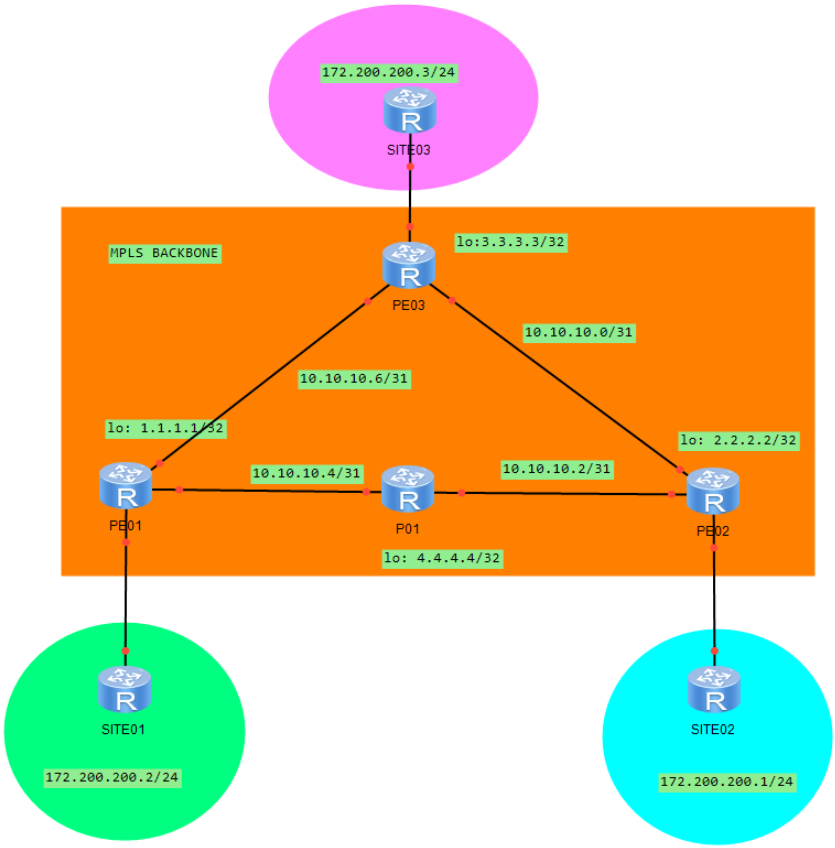

Figura 8: Red VPLS

Fuente: Elaboración propia

Para implementar MPLS en los equipos, se inicia nombrando los ID de los LSR (rutas de conmutación de etiquetas), las interfaces con sus direcciones IP, asimismo las *loopback*. Estas últimas son empleadas más que nada para gestión de los equipos y otras características técnicas.

Se tiene tres sitios a conectar, y el *backbone* MPLS integra a PE01, PE02, PE03 y P01.

Para PE01 se tiene

```
PE01
sysname PE01
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
mpls ldp
#
interface Loopback 0
ip address 3.3.3.3 32
#
interface GigabitEthernet0/0/0
ip address 10.10.10.7 31
mpls
mpls ldp
#
interface GigabitEthernet0/0/1
ip address 10.10.10.1 31
mpls
mpls ldp
#
commit
```

Figura 9: Configuración de MPLS para PE01

Fuente: Elaboración propia

Como primer comando se crea la etiqueta MPLS, y que el protocolo trabajara en Capa 2 (Modelo OSI) además de la ruta de la etiqueta (mpls ldp). Se crea la interfaz *loopback* y se le configura las direcciones IP en las interfaces y se les asocia el protocolo MPLS.

En el equipo PE01:

```
 sysname PE01
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
mpls lsr-id 1.1.1.1
mpls
#
mpls l2vpn
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 15
#
interface GigabitEthernet0/0/0
 ip address 10.10.10.7 255.255.255.254
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 10.10.10.1 255.255.255.254
 mpls
 mpls ldp
#
```

Figura 10: Configuración en equipo PE01 en software eNSP

Fuente: Elaboración propia

De igual modo, se configura para PE02, PE03 y P01:

```
PE02
sysname PE02
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
mpls ldp
#
interface Loopback 0
ip address 2.2.2.2 32
#
interface GigabitEthernet0/0/0
ip address 10.10.10.0 31
mpls
mpls ldp
#
interface GigabitEthernet0/0/1
ip address 10.10.10.2 31
mpls
mpls ldp
#
commit
```

Figura 11: Configuración de PE02

Fuente: Elaboración propia

```
PE03
sysname PE03
#
mpls lsr-id 3.3.3.3
mpls
#
mpls l2vpn
#
mpls ldp
#
interface Loopback 0
ip address 3.3.3.3 32
#
interface GigabitEthernet0/0/0
ip address 10.10.10.7 31
mpls
mpls ldp
#
interface GigabitEthernet0/0/1
ip address 10.10.10.2 31
mpls
mpls ldp
#
commit
```

Figura 12: Configuración para PE03

Fuente: Elaboración propia

```
P01
sysname P01
#
mpls lsr-id 4.4.4.4
mpls
#
mpls l2vpn
#
mpls ldp
#
interface Loopback 0
ip address 4.4.4.4 32
#
interface GigabitEthernet0/0/0
ip address 10.10.10.5 31
mpls
mpls ldp
#
interface GigabitEthernet0/0/1
ip address 10.10.10.3 31
mpls
mpls ldp
#
commit
```

Figura 13: Configuración para P01

Fuente: Elaboración propia

Como paso siguiente se requiere configurar las sesiones remotas peer LDP entre los Pes. Esta configuración permite generar la redundancia entre equipos de respaldo.

Tabla 3: Configuración de sesiones LDP para equipos remotos

Equipo	Configuración
PE01	*mpls ldp remote-peer 2.2.2.2* *remote-ip 2.2.2.2* *mpls ldp remote-peer 3.3.3.3* *remote-ip 3.3.3.3*
PE02	*mpls ldp remote-peer 1.1.1.1* *remote-ip 1.1.1.1* *mpls ldp remote-peer 3.3.3.3* *remote-ip 3.3.3.3*
PE03	*mpls ldp remote-peer 1.1.1.1*

	remote-ip 1.1.1.1 *mpls ldp remote-peer 2.2.2.2* *remote-ip 2.2.2.2*

3.3.4. Configuración de las VSI (Inicio de implementación de VPLS)

Siguiendo la misma topología, lo siguiente es crear las VSIs en los PEs, y vincularlas a las interfaces AC conectando los sitios clientes. Una VSI es una instancia de switch virtual (*Virtual Switch Instance*) Los comandos que se emplean son los siguientes:

Tabla 4: Configuración de VSI, circuitos virtuales

Equipo	Configuración
PE01	vsi 333 pwsignal ldp vsi id 333 peer 3.3.3.3 peer 2.2.2.2 interface GigabitEthernet0/0/2.333 vlan type dot1q 333 l2 binding vsi 333
PE02	vsi 333 pwsignal ldp vsi id 333 peer 3.3.3.3 peer 1.1.1.1 interface GigabitEthernet0/0/2.333 vlan type dot1q 333 l2 binding vsi 333
PE03	vsi id 333 peer 1.1.1.1 peer 2.2.2.2 interface GigabitEthernet0/0/2.333 vlan type dot1q 333 l2 binding vsi 333

En las interfaces, se crean subinterfaces (generalmente con el mismo número que la VSI) con el fin de conectar muchos más sitios remotos. Si se usara la interfaz directamente, no podría emplearse más dicha interfaz y agregarle otros sitios. Los peer (3.3.3.3 y 2.2.2.2) son las etiquetas de los sitios remotos.
El comando ***vlan type dot1q*** permite asociar una subinterfaz ethernet con VLANs, configurando el tipo de encapsulación de VLAN para esa subinterfaz ethernet como dot1q. Este protocolo estándar inserta una etiqueta de 4 bytes en la trama ethernet, que conlleva admitir redes de área local virtuales (VLAN).

Entonces ¿En qué condiciones puede una VSI estar activo en una red VPLS (*Virtual Private LAN Service*)?

En el caso de que las configuraciones sean correctas, VPLS puede estar activo cuando se cumple una de las siguientes condiciones:

- mVSI: requiere un Up PW o un Up AC en el VSI.
- Servicio VSI: requiere dos o más interfaces Up AC, o una interfaz Up AC y un Up PW.

Adicionalmente:
Una interfaz de AC es una interfaz vinculada a un VSI. En una red VPLS de Martini, si el par es una UPE, el PW (Pseudo Wire) que conecta la UPE se maneja como una AC en el procesamiento interno. La información detallada de VSI muestra que el tipo PW de la UPE es MEHVPLS.

3.3.5. Configuración de protocolo ISIS

El protocolo IS-IS (*Intermediate System to Intermediate System)* denominado IGP, o protocolo de borde interior, dado que guía el tráfico en un solo sistema autónomo, es un protocolo de estado

enlace, es decir, emplea la información de estado del vínculo o enlace para decidir las rutas que debe tomar el paquete.
ISIS trabaja de manera similar a OSPF, para decidir la ruta más corta. La principal diferencia es que ISIS funciona en capa 2 del modelo OSI, en contrate a OSPF que trabaja en capa 3

Los comandos para configurar IS-IS son los siguientes:

Tabla 5: Configuración de IS-IS nivel 1

Tipo	Configuración
IS-IS 1	isis 1
	cost-style wide
	timer lsp-generation 11 100 level-1
	flash-flood 15 level-1
	circuit-cost 100 level-1
	network-entity 47.1000.0a0a.0200.00
	is-name CENTRAL-2

ISIS trabaja en base a niveles, áreas organizadas jerárquicamente, esto es posible mediante la configuración de IS-IS de *nivel 1* y *nivel 2*. En este caso, se emplea IS-IS en nivel 1.
Los routers configurados para trabajar en nivel 1, envían información de routing interna o intra-área, y los routers de nivel 2 comparten información entre áreas sobre las direcciones IP disponibles en cada área. Los router con ISIS pueden trabajar en nivel, como nivel 2, compartiendo, enviado información de rutas internas para los de nivel 1, y rutas externas para routers de nivel 2. Cada entidad, o área en el único sistema autónomo, tiene un *título de entidad de red* (*NET*). Estas NET son direcciones hexadecimales y van entre 8 y 20 octetos de longitud. Normalmente, el formato consta de un identificador de autoridad y formato (AFI), un ID de dominio, un ID de área, un identificador de sistema y un selector. Por ejemplo, la dirección NET **47.0002.1922.6800.1001.00** consta de las siguientes partes:

47 – AFI

0002 – ID de área

1922.6800.1001 – Identificador de sistema

00 - Selector

Cabe mencionar que el identificador del sistema debe ser único dentro de la red.

Para el caso de la red del proyecto, se aplica IS-IS en nivel 1 y con un identificador de red de: 47.1000.0a0a.0a02.0200.00

Esta configuración es similar para los equipos restantes.

3.3.6. Configuración de QoS

Para la configuración de calidad de servicio se tiene según la prioridad de tráfico. Se rige una nomenclatura de códigos para la gestión de las colas prioritarias en equipos Huawei:

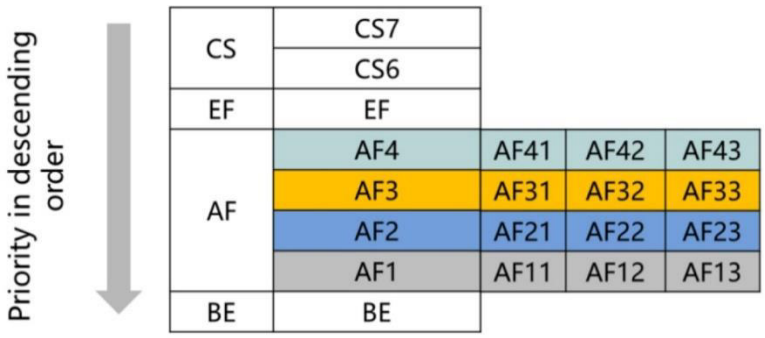

Figura 14: Prioridad de colas para equipos Huawei

Fuente: Elaboración propia

Donde el BE significa *Best Effort,* que implica prioridad por defecto, y así de manera ascendente.

Para configurarlo en un equipo Huawei, se realiza de la siguiente manera:

Tabla 6: Configuración de QoS

Interface	Configuración
interface GigabitEthernet0/2/3	interface GigabitEthernet0/2/3 carrier up-hold-time 500 carrier down-hold-time 750 description QOS FOR BE

```
undo shutdown
trust upstream default
undo dcn
port-queue be wfq weight 20 port-wred best_effort outbound
port-queue af1 wfq weight 40 port-wred low-priority outbound
port-queue af2 wfq weight 15 port-wred high_priority outbound
port-queue af3 wfq weight 5 outbound
port-queue af4 wfq weight 60 port-wred high_priority outbound
port-queue ef pq port-wred voice outbound
```

Los comandos que inician con ***port-queue*** indican la prioridad de las colas, y dependiendo del tráfico se emplean las etiquetas presentadas en la figura 14.

Por ejemplo, para la primera línea: ***port-queue be wfq weight 20 port-wred best_effort outbound*** se tiene la prioridad estándar (be, de *best effort*), y el peso de la cola programa es 20.

Cabe mencionar que esta configuración se debe realizar en cada interfaz que se le va a dar prioridad de tráfico. Esta configuración ayuda cuando la red está sobrecargada o congestionada, la QoS va a garantizar que el tráfico importante no se retrase ni se descarte, asegurando el funcionamiento eficiente de la red.

3.3.7. Configuración de redundancia en red

En este diseño se tiene como propuesta dos enlaces para cada sede (cabecera y sedes remotas), en la última milla se enlazaría a diferentes nodos del proveedor del servicio, asegurando una alta disponibilidad para el servicio de datos a nivel WAN.

En parte por los *routers*, la configuración para generar redundancia está dentro de la configuración de mpls, con los comandos *ldp remote peer* en cada equipo. Esto permite que, si algún enlace cae, el equipo de respaldo actúe y permite que el tráfico no se pierda.

```
#
mpls ldp remote-peer CENTRAL-2
 remote-ip 10.10.10.2
#
mpls ldp remote-peer REMOTO-1
 remote-ip 10.10.10.3
#
mpls ldp remote-peer REMOTO-2
 remote-ip 10.10.10.4
```

Figura 15: Configuración de ldp remote peer para redundancia

Fuente: Elaboración propia

3.4. Implementar enlaces WAN que permitan mejorar el QoS de las redes de telecomunicaciones sin necesidad de emplear canales privados o dedicados.

En el proyecto se ha considerado como parte del diseño, usar la tecnología de fibra óptica GPON. Como se mencionó, la implementación de equipos *routers* en la cabecera y las sedes remotas se basará en los equipos marca Huawei, que cubre las necesidades de ancho de banda, configuración requerida en cada sitio y crecimiento a futuro.

3.4.1. Implementación de los equipos de red

Para la inplementación del enrutador cabecera, se consideró un escenario donde exista un consumo del tráfico de datos equivalente a la suma de los anchos de banda de las sedes remotas. Para lo cual se instalará un router Huawei de la serie ATN 950B. como equipo principal para configuraciones como ISIS-MPLS-VPLS, el cual tiene incorporado 2x10G+10x1G+16E1 puertos *GigabitEthernet*, para direccionamiento WAN y LAN. Se instalará para las sedes remotas un router Huawei de la serie ATN 910C, para configuraciones como ISIS-MPLS-VPLS, el cual tiene incorporado puertos para direccionamiento WAN y LAN.

Se tiene lo siguiente, colocando los equipos en un gabinete:

Figura 16: Equipos ATN910 en gabinete

Fuente: Elaboración propia

La red que toma en este escenario es el siguiente:

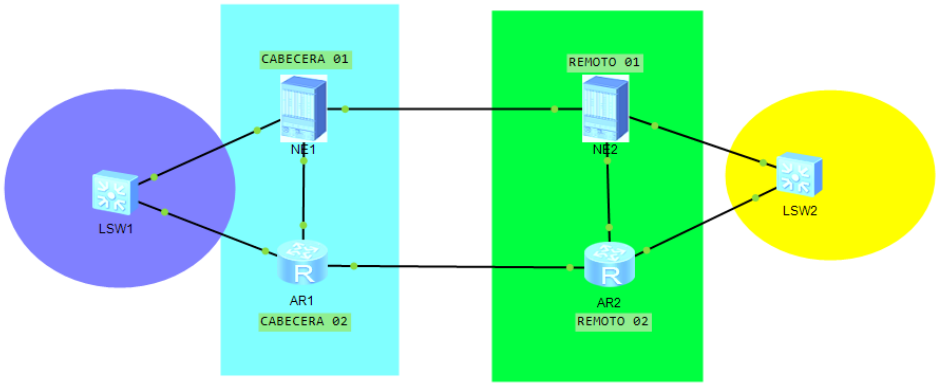

Figura 17: Red lógica a implementar

Fuente: Elaboración propia

Integrando el cableado de la fibra y cobre en el gabinete:

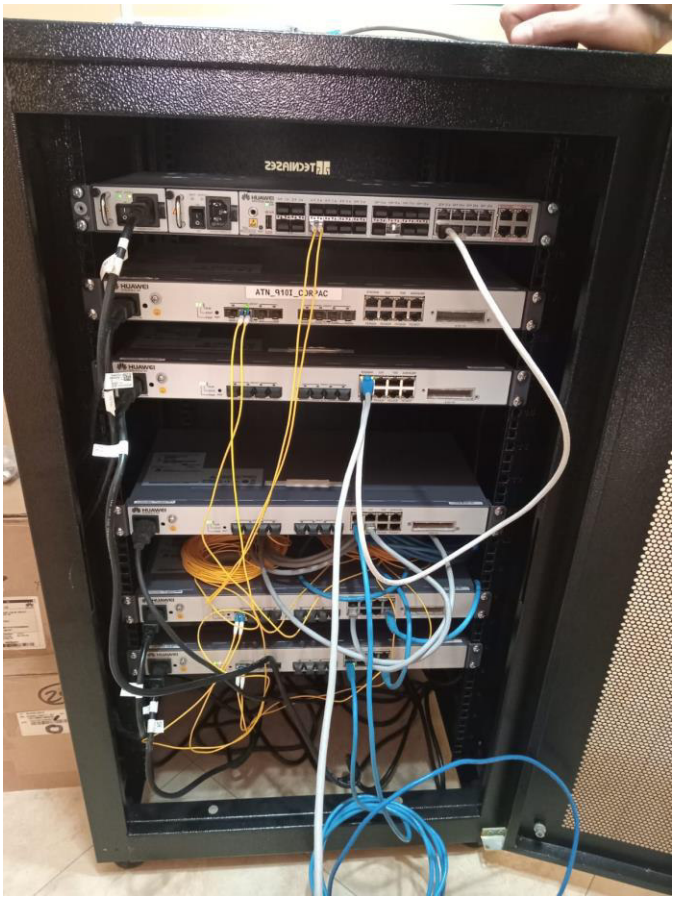

Figura 18: Cableado en el gabinete

Fuete: Elaboración propia

Se agregan el cableado para realizar la conexión de equipos finales como computadoras, que simularán el usuario final y verificar las conexiones.

Se tiene el siguiente diagrama lógico dibujado en pizarra:

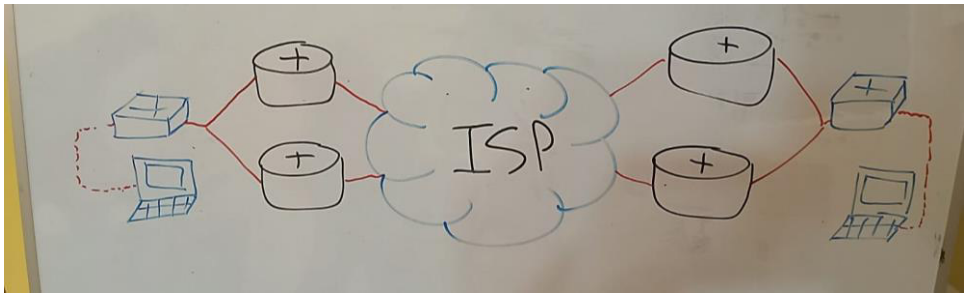

Figura 19: Diagrama implementado

Fuente: Elaboración propia

Se tienen cuatro enrutadores ATN910, que simularan dos sedes a distancia, cada uno con un equipo principal y de respaldo, con el objetivo de generar redundancia. En la figura 18, se muestra el diagrama en que trabajaran las sedes. Ambos *routers* de cada sede se conectan a un proveedor de servicios, y asimismo también se conectan a dispositivos finales (como computadoras o *switchs*), que actúa como sede origen y destino que se interconectaran por medio del túnel MPLS/VPLS para crear una LAN privada por medio de la red pública sin necesidad de implementar enlaces dedicados.

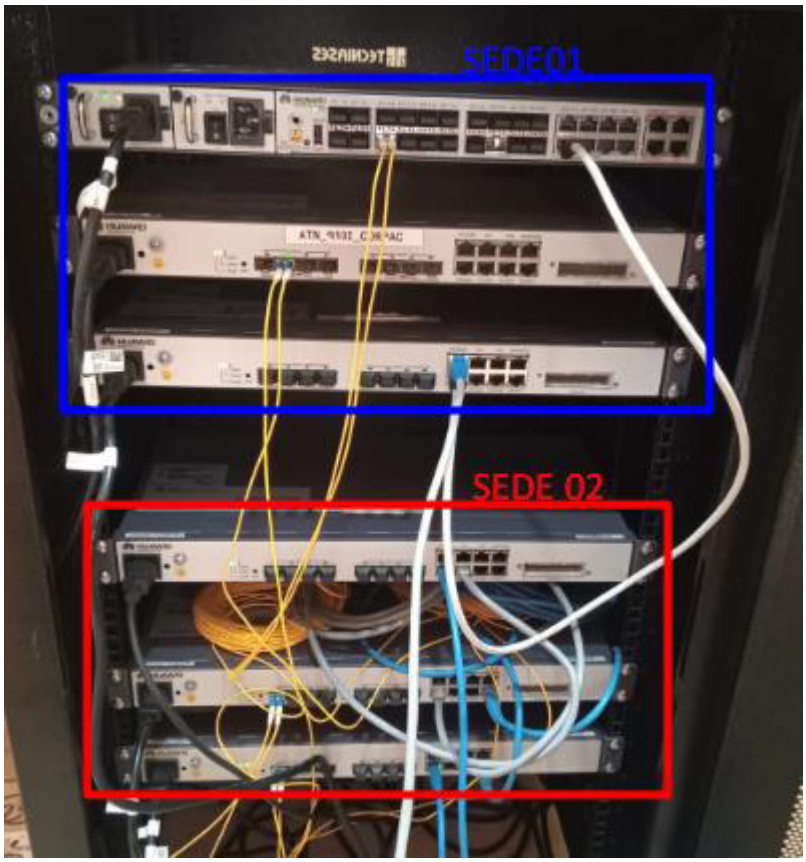

Figura 20: Conexión física de la red

Fuente: Elaboración propia

Ambas sedes se interconectarán generando una LAN privada.

3.4.2. Configuración MPLS en equipos Huawei

Como primer paso, se le agrega direcciones IP para crear la conexión local y verificar que cada sede tenga una conexión directa en su propia red.

Se tiene la siguiente distribución:

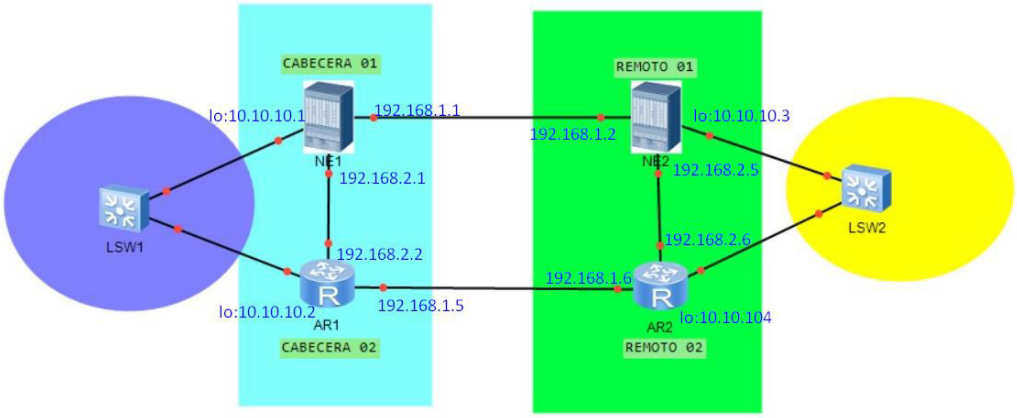

Figura 21: Red con direccionamiento IP

Fuente: Elaboración propia

Se comprueba que no haiga conexión entre sedes:

```
C:\WINDOWS\system32\cmd.exe - ping  -t 192.168.50.1
(c) Microsoft Corporation. All rights reserved.

C:\Users\junio>ping -t 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.2: Destination host unreachable.
Reply from 192.168.50.2: Destination host unreachable.
Reply from 192.168.50.2: Destination host unreachable.
Reply from 192.168.50.2: Destination host unreachable.
Reply from 192.168.50.2: Destination host unreachable.
Reply from 192.168.50.2: Destination host unreachable.
Reply from 192.168.50.2: Destination host unreachable.
Reply from 192.168.50.2: Destination host unreachable.
Reply from 192.168.50.2: Destination host unreachable.
```

Figura 22: Ping origen a destino

Fuente: Elaboración propia

Se tienen 4 enrutadores, de los cuales representan dos sedes: Central y Remoto. Cada uno tiene su router cabecera y respaldo. Por tanto, se requiere configurar el MPLS en los cuatro equipos para que puedan interconectarse entre origen y destino.

Se tiene para el central cabecera o central 1 su configuración del etiquetado MPLS detallado en lo siguiente.

La primera línea: mpls lsr-id 10.10.10.1 corresponde a la etiqueta MPLS, y el comando l2vpn que va a trabajar en capa 2. Configurando en el equipo:

```
mpls lsr-id 10.10.10.1
#
mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
#
mpls l2vpn
#
```

Figura 23: MPLS central cabecera

Fuente: Elaboración propia

Del mismo modo, para los siguientes equipos. Para central de 2 (respaldo):

```
mpls lsr-id 10.10.10.2
mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
#
```

Figura 24: MPLS en central respaldo por teraterm

Fuente: Elaboración propia

Para la sede remota, el equipo cabecera:

```
mpls lsr-id 10.10.10.3
mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
#
```

Figura 25: MPLS en remoto cabecera

Fuente: elaboración propia

Para el equipo remoto de respaldo:

```
mpls lsr-id 10.10.10.4
mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
#
```

Figura 26: MPLS en remoto respaldo

Fuente: elaboración propia

Configurado las sesiones, se verifica que estén activas o pasivas dependiendo de la conexión.

```
[REMOTO-2]display mpls ldp session

LDP Session(s) in Public Network
Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
A '*' before a session means the session is being deleted.
------------------------------------------------------------------------------
PeerID            Status      LAM  SsnRole  SsnAge       KASent/Rcv
------------------------------------------------------------------------------
10.10.10.1:0      Operational DU   Active   0000:03:24   817/818
10.10.10.2:0      Operational DU   Active   0000:05:46   1388/1388
10.10.10.3:0      Operational DU   Active   0000:01:00   242/242
------------------------------------------------------------------------------
TOTAL: 3 session(s) Found.
```

Figura 27: Sesiones MPLS para remoto respaldo

Fuente: elaboración propia

Cabe mencionar, para la gestión de los equipos, se crearon unas interfaces *loopback* para realizar las configuraciones ingresando a los equipos mediante telnet o *Secure Shell*.

Para un orden en los comandos, las direcciones *loopback* llevan la misma etiqueta MPLS de cada equipo. Para el central uno o cabecera se tiene:

```
interface LoopBack0
description Loopback de Gestion
ip address 10.10.10.1 255.255.255.255
isis enable 1
isis circuit-level level-1
#
```

Figura 28: Loopback de gestión para central principal

Fuente: elaboración propia

Asimismo, se configuraron subinterfaces con una vlan 1000, para generar una conexión directa entre cabecera y respaldo. Para

ambos equipos se crea en la interface número 27 de los enrutadores:

```
#
interface GigabitEthernet0/2/27.1000
 vlan-type dot1q 1000
 description to REMOTO-2
 set flow-stat interval 10
 ip address 192.168.2.5 255.255.255.252
```

Figura 29: Subinterface vlan 1000

Fuente: Elaboración propia

La creación de subinterfaces permitirá realizar conexiones para agregar sedes remotas que requieran interconectarse.

3.4.3. Configuración VSI en equipos Huawei

Se tiene la configuración de las VSI.

Para central cabecera:

```
vsi PRUEBA static
 pwsignal ldp
  vsi-id 5000
  peer 10.10.10.2
  peer 10.10.10.3
  peer 10.10.10.4
#
```

Figura 30: VSI cabecera

Fuente: Elaboración propia

En este caso la VSI tiene un de 5000 y está apuntando a los tres router mediante los peer correspondientes.

Para central respaldo:

```
#
vsi PRUEBA static
 pwsignal ldp
  vsi-id 5000
  peer 10.10.10.3
  peer 10.10.10.4
  peer 10.10.10.1
#
```

Figura 31: VSI respaldo

Fuente: Elaboración propia

Para sede remota cabecera:

```
#
vsi PRUEBA static
 pwsignal ldp
  vsi-id 5000
  peer 10.10.10.1
  peer 10.10.10.2
#
```

Figura 32: VSI sede remota principal

Fuente: Elaboración propia

Para sede remota respaldo:

```
#
vsi PRUEBA static
 pwsignal ldp
  vsi-id 5000
  peer 10.10.10.1
  peer 10.10.10.2
#
```

Figura 33: VSI sede remota respaldo

Fuente: Elaboración propia

A diferencia de la cabecera, la sede remota apunta solo dos peer, dado que la central debe apuntar a todos los equipos y mantener la conexión entre todos los equipos de su área.

La dirección va de este modo:

- Cabecera 1: peer hacia remotos 1 y 2, peer hacia cabecera 2
- Cabecera 2: peer hacia remoto 1 y 2, peer hacia cabecera 1
- Remoto 1: peer hacia Cabecera 1 y 2
- Remoto 2: peer hacia cabecera 1 y 2

Los remotos (principal y respaldo) solo apuntan a la sede cabecera, dado que si apuntaran entren ellos mismos, generarían bucles de red.

3.4.4. Configuración IS-IS en equipos Huawei

Se tiene la configuración de IS-IS

Para central cabecera:

```
isis 1
 is-level level-1
 cost-style wide
 timer lsp-generation 1 1 100 level-1
 flash-flood 15 level-1
 circuit-cost 100 level-1
 network-entity 47.1000.0a0a.0a01.0200.00
 is-name CENTRAL-1
 timer spf 1 1 100
 traffic-eng level-1
```

Figura 34: IS-IS en central cabecera

Fuente: Elaboración propia

De la figura 34, se observa que se está empleando IS-IS de nivel 1. El nivel 1 se aplica cuando es área interna, es decir una red local. En el proyecto se escenifico una red local para la simulación de una WAN, pero físicamente es local, por tanto, se aplica Nivel 1. La entidad de red es 47, que emplea para redes WAN, si fuese una red privada o local, se usa 49 como entidad de red.

Los comandos restantes se configuran de acuerdo al requerimiento de tiempo de respuesta o costo de trabajo para que no sobrecargue el equipo de red.

Las configuraciones son similares para los demás equipos en la red.

Para central respaldo:

```
isis 1
 is-level level-1
 cost-style wide
 timer lsp-generation 11 100 level-1
 flash-flood 15 level-1
 circuit-cost 100 level-1
 network-entity 47.1000.0a0a.0a02.0200.00
 is-name CENTRAL-2
 timer spf 11 100
 traffic-eng level-1
#
```

Figura 35: IS-IS en central respaldo

Fuente: Elaboración propia

Para remoto cabecera:

```
<REMOTO-1>display current-configuration | begin isis 1
isis 1
 is-level level-1
 cost-style wide
 timer lsp-generation 11 100 level-1
 flash-flood 15 level-1
 circuit-cost 100 level-1
 network-entity 47.1000.0a0a.0a03.0200.00
 is-name REMOTE-1
 timer spf 11 100
 traffic-eng level-1
```

Figura 36: IS-IS en remoto cabecera

Fuente: Elaboración propia

Para remoto respaldo:

```
<REMOTO-2>display current-configuration | begin isis
isis 1
 is-level level-1
 cost-style wide
 timer lsp-generation 1 1 100 level-1
 flash-flood 15 level-1
 circuit-cost 100 level-1
 network-entity 47.1000.0a0a.0a04.0200.00
 is-name REMOTO-2
 timer spf 1 1 100
 traffic-eng level-1
```

Figura 37: IS-IS en remoto respaldo

Fuente: Elaboración propia

3.4.5. Configuración de los puertos para QoS

Se tiene los comandos para la calidad de servicio.

Para central cabecera:

```
 port-queue af1 wfq weight 20 outbound
 port-queue af2 wfq weight 40 outbound
 port-queue af3 wfq weight 60 outbound
 port-queue af4 wfq weight 80 outbound
 port-queue ef wfq weight 1 outbound
#
```

Figura 38: Configuración de QoS en interfaces

Fuente: Elaboración propia

El comando ***port-queue*** establece parámetros de programación para las colas de puertos en la dirección de salida de una interfaz que no es de baja velocidad.

De forma predeterminada, las colas BE, AF1, AF2, AF3 y AF4 se programan utilizando el modo de programación WFQ (Cola ponderada justa), con ponderaciones de programación de 10, 10, 10, 15 y 15, respectivamente, y las colas EF, CS6 y CS7 se programan utilizando el modo de programación PQ (Prioridad justa). El porcentaje de modelado se establece en 100 para todas las colas y se utiliza el modo de eliminación de cola.

Como se mencionó anteriormente, la programación de cola ponderada justa (WFQ) es un mecanismo de QoS que distribuye el ancho de banda de manera equitativa entre diferentes tipos de tráfico.

En este caso se tiene la primera línea: **port-queue af1 wfq weight 20 outbound.**

Cuando una red está congestionada, se puede ejecutar el comando **port-queue** para configurar la programación de colas de modo que los paquetes de servicio en las colas de alta prioridad, como paquetes de VoIP y paquetes de video, se programen según las prioridades.

Una vez que los paquetes ingresan a las colas de una interfaz, la interfaz programa los paquetes según políticas.

Los valores af1-af4 especifica el valor de la calidad de servicio de la cola, conforme a las políticas establecidas. Para la línea mostrada, se emplea wfq, es decir programación de cola ponderada justa. El siguiente termino es el peso o **weight** que define el valor de peso de una cola de puertos. Para ser más específico, el porcentaje del ancho de banda restante después de que el ancho de banda se asigna a las colas PQ. Este valor es un número entero que va de 1 a 100. Finalmente, **outbound** que implica salida en el puerto.

Se tiene las siguientes configuraciones:
Para central respaldo:

```
#
interface GigabitEthernet0/2/27
 description to CENTRAL-1
 undo shutdown
 dcn
 port-queue be wfq weight 1 outbound
 port-queue af1 wfq weight 20 outbound
 port-queue af2 wfq weight 40 outbound
 port-queue af3 wfq weight 60 outbound
 port-queue af4 wfq weight 80 outbound
#
```

Figura 39: QoS en central respaldo

Fuente: Elaboración propia

Para remoto cabecera:

```
port-queue af1 wfq weight 20 outbound
port-queue af2 wfq weight 40 outbound
port-queue af3 wfq weight 60 outbound
port-queue af4 wfq weight 80 outbound
port-queue ef wfq weight 1 outbound
```

Figura 40: QoS en remoto cabecera

Fuente: Elaboración propia

Para remoto respaldo:

```
port-queue be wfq weight 1 outbound
port-queue af1 wfq weight 20 outbound
port-queue af2 wfq weight 40 outbound
port-queue af3 wfq weight 60 outbound
port-queue af4 wfq weight 80 outbound
#
```

Figura 41: QoS en remoto respaldo

Fuente: Elaboración propia

3.4.6. Configuración de redundancia en la red

Se tiene los siguientes comandos:

Para central cabecera:

```
#
mpls ldp
 #
 ipv4-family
#
mpls ldp remote-peer CENTRAL-2
 remote-ip 10.10.10.2
#
mpls ldp remote-peer REMOTO-1
 remote-ip 10.10.10.3
#
mpls ldp remote-peer REMOTO-2
 remote-ip 10.10.10.4
```

Figura 42: Redundancia en central cabecera

Fuente: Elaboración propia

El comando ***mpls ldp remote-peer*** crea un par remoto y muestra la vista del par remoto. Para esta configuración, en generar la redundancia de la red, se crean tres sesiones LDP, que apuntan al respaldo de la cabecera y los equipos remotos.

Se puede establecer una sesión LDP remota entre dos LSR conectados indirectamente o dos LSR conectados directamente y del mismo modo, es posible configurar sesiones LDP remotas y locales y respaldarlas entre sí, lo que garantiza la conectividad de la sesión LDP, permitiendo redundancia en la red. Si un equipo o

enlace cae, de manera automática se levantan las otras sesiones para mantener la conectividad de la red.

Para central respaldo:

```
mpls ldp
#
#
mpls ldp remote-peer central-1
 remote-ip 10.10.10.1
#
mpls ldp remote-peer remoto-1
 remote-ip 10.10.10.3
#
mpls ldp remote-peer remoto-2
 remote-ip 10.10.10.4
#
```

Figura 43: Redundancia en central respaldo

Fuente: Elaboración propia

Para remoto cabecera:

```
#
mpls ldp
#
#
mpls ldp remote-peer central-1
 remote-ip 10.10.10.1
#
mpls ldp remote-peer central-2
 remote-ip 10.10.10.2
```

Figura 44: Redundancia en remoto cabecera

Fuente: Elaboración propia

Para remoto respaldo:

```
#
mpls ldp
#
#
mpls ldp remote-peer central-1
 remote-ip 10.10.10.1
#
mpls ldp remote-peer central-2
 remote-ip 10.10.10.2
```

Figura 45: Redundancia en remoto respaldo

Fuente: Elaboración propia

3.5. Realizar pruebas de estrés y conmutación a los enlaces de red de área extensa

Para comprobar y verificar la redundancia de los enlaces, asimismo como la calidad de servicio de la red, se simularon enlaces caídos o equipos desconectados y revisar la permanencia de la red, sin cortes o mínima perdida de paquetes.

Con las configuraciones realizadas, se revisa y comprueba la conexión entre dos dispositivos finales, entre router central y router remoto:

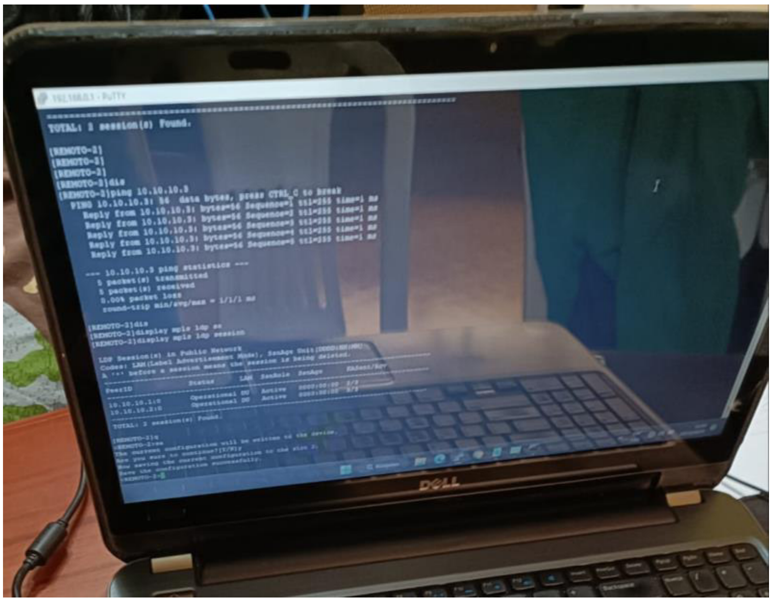

Figura 46: Conexión entre sedes, ping entre routers

Fuente: Elaboración propia

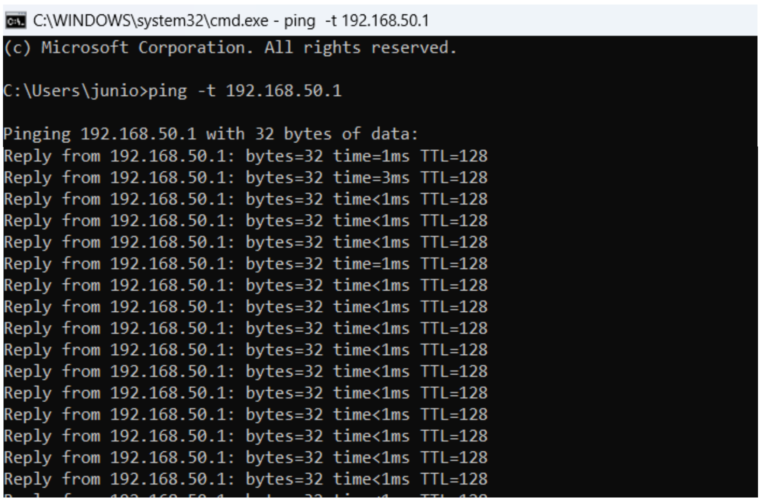

Figura 47: Ping entre sedes, hacia laptop remoto

Fuente: Elaboración propia

Se tiene una conexión estable entre sedes, sin corte o retraso de paquetes. Para simular un corte, o una caída de enlace, físicamente se desconectó la fibra que conecta el router de la sede principal hacia el router remoto:

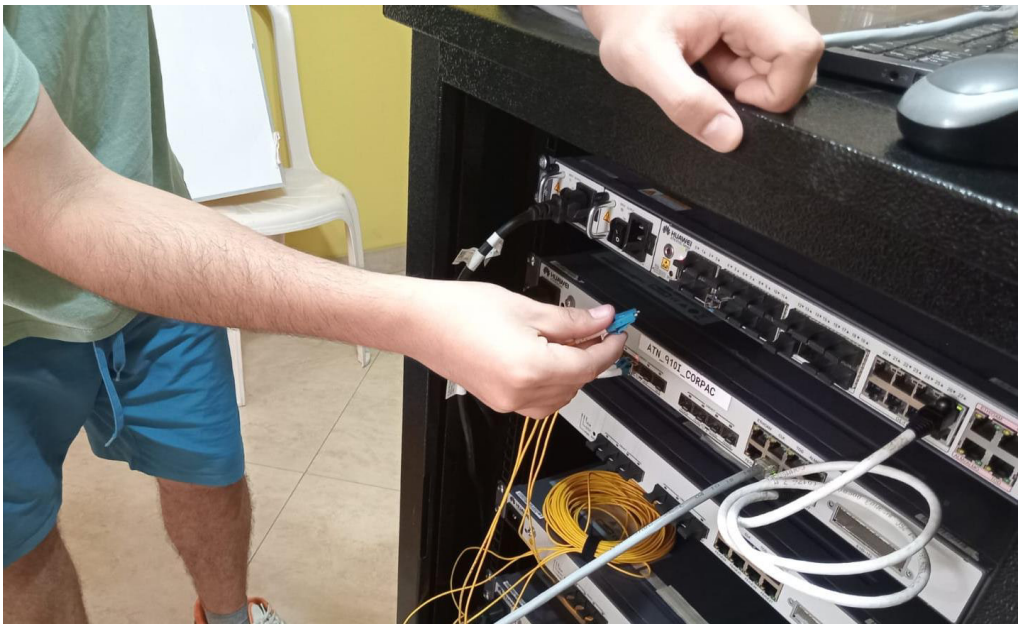

Figura 48: Fibra desconectada del router principal

Fuente: Elaboración propia

Entre ambas maquinas, se mandó un ping constante, revisando el equipo conectado al router central:

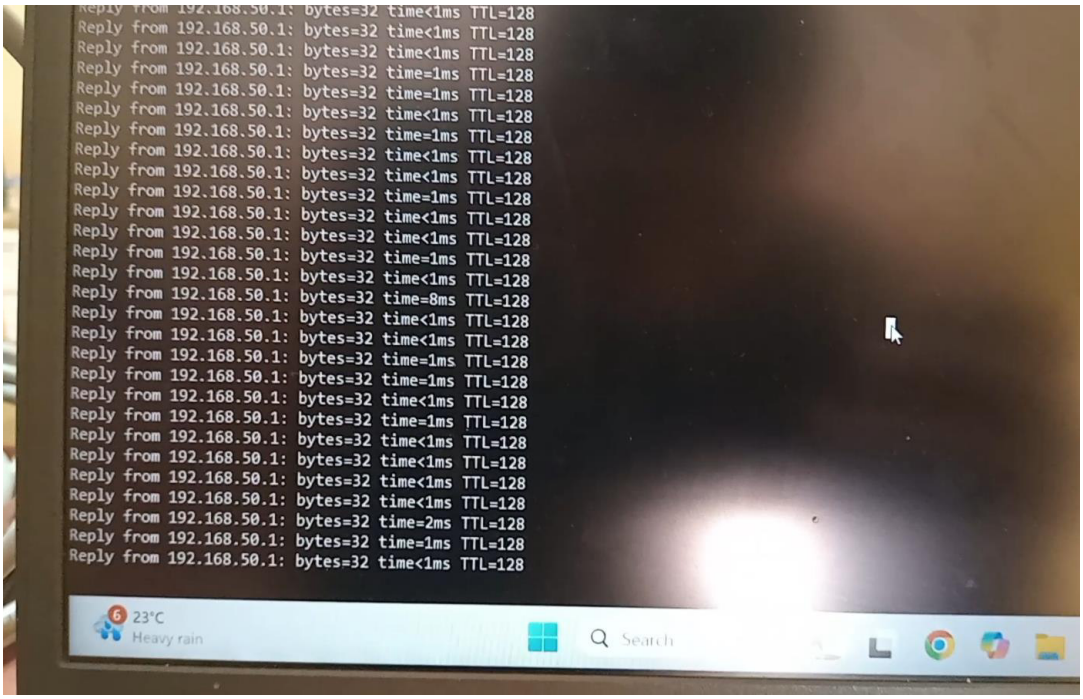

Figura 49: Ping constante entre sedes

Fuente: Elaboración propia

Desde la sede remota, no se registra una pérdida de paquetes, dado que la reconexión es entre milisegundos, en pequeñas cantidades de tiempo, que, en algunas ocasiones, los dispositivos finales ni perciben la perdida de conexión.

Para este primer escenario, al perder un enlace con el router central, el equipo de respaldo (en sede principal) entra en acción y toma su lugar, manteniendo una disponibilidad continua de la conexión.

Del mismo modo, al conectar otro equipo al router de respaldo en la sede remota, la conexión se reestablece luego de un corte:

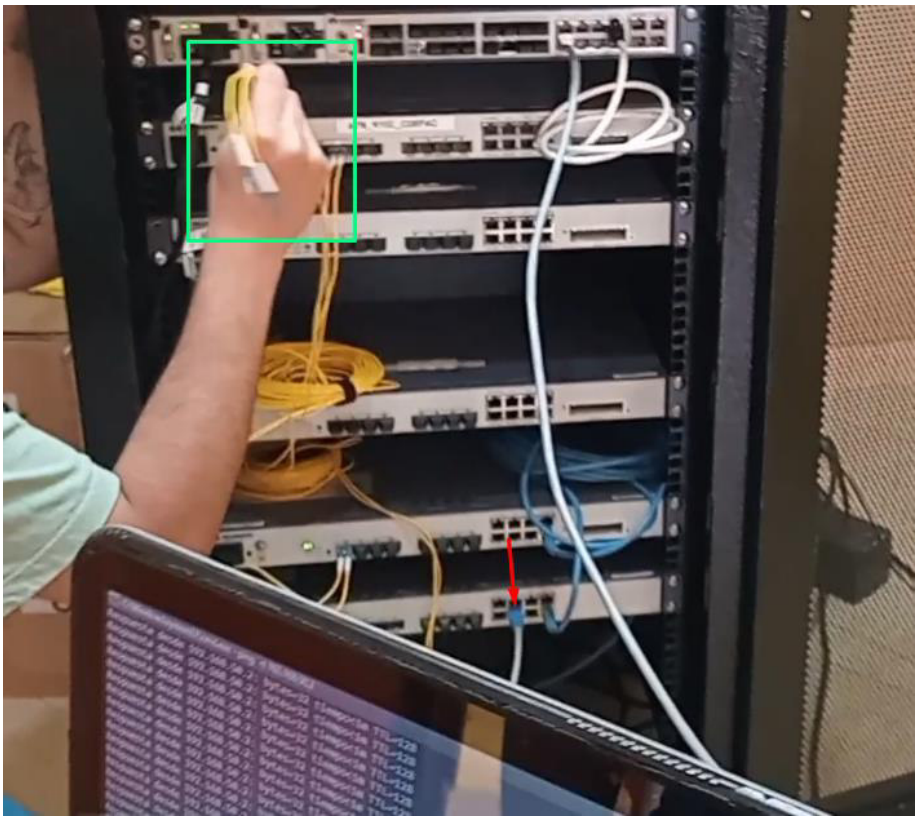

Figura 50: PC conectada a router respaldo remoto

Fuente: Elaboración propia

Con el enlace principal desconectado, se cae la sesión LDP entre el router principal y los restantes en la sede remota, y en segundos la sesión establecida con el router de respaldo de la sede principal, levanta o continua con la conexión, permitiendo el ingreso y salida de tráfico.

Se conecta otra vez el enlace principal, y las demás sesiones se reestablecen al estado original.

Figura 51: Reestableciendo el enlace principal

Fuente: Elaboración propia

Con el enlace principal restablecido, si se llegare a desconectar el enlace de respaldo, aun estando conectado el dispositivo final en el router remoto de respaldo, la conectividad no se pierde, dado que la sesión LDP se mantiene, y el tráfico sabe que ruta tomar gracias a MPLS y el protocolo de enrutamiento IS-IS:

Figura 52: Desconexión de enlace de respaldo

Fuente: Elaboración propia

Verificando la conexión continua:

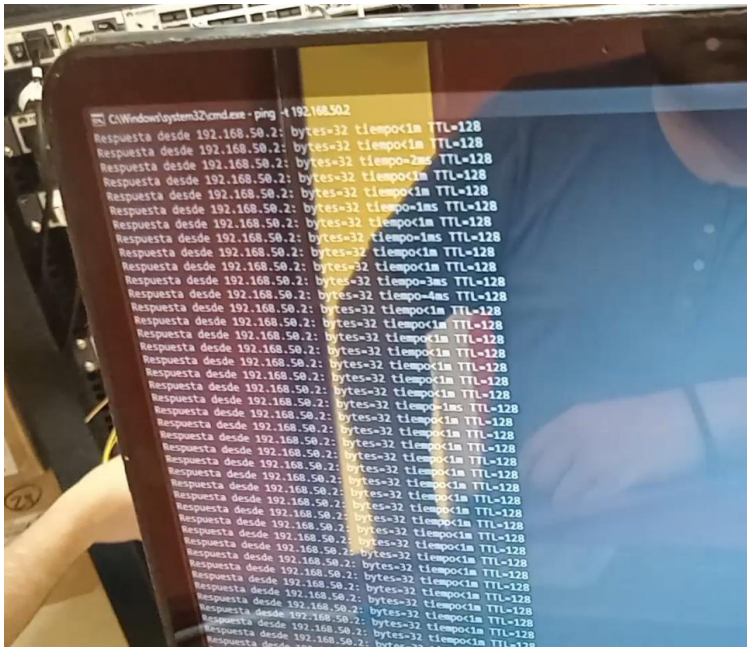

Figura 53: Ping desde equipo respaldo remoto

Fuente: Elaboración propia

Se verifica que, por parte de sede principal, los equipos cabecera y respaldo trabajan como se espera, manteniendo una conexión estable y una buena calidad de servicio, dado que no se pierden paquetes.

Para un segundo escenario, se invierten los papeles. Se verificará la funcionalidad en el enlace de respaldo. Se cambia el equipo de cómputo hacia el router de respaldo en la sede central:

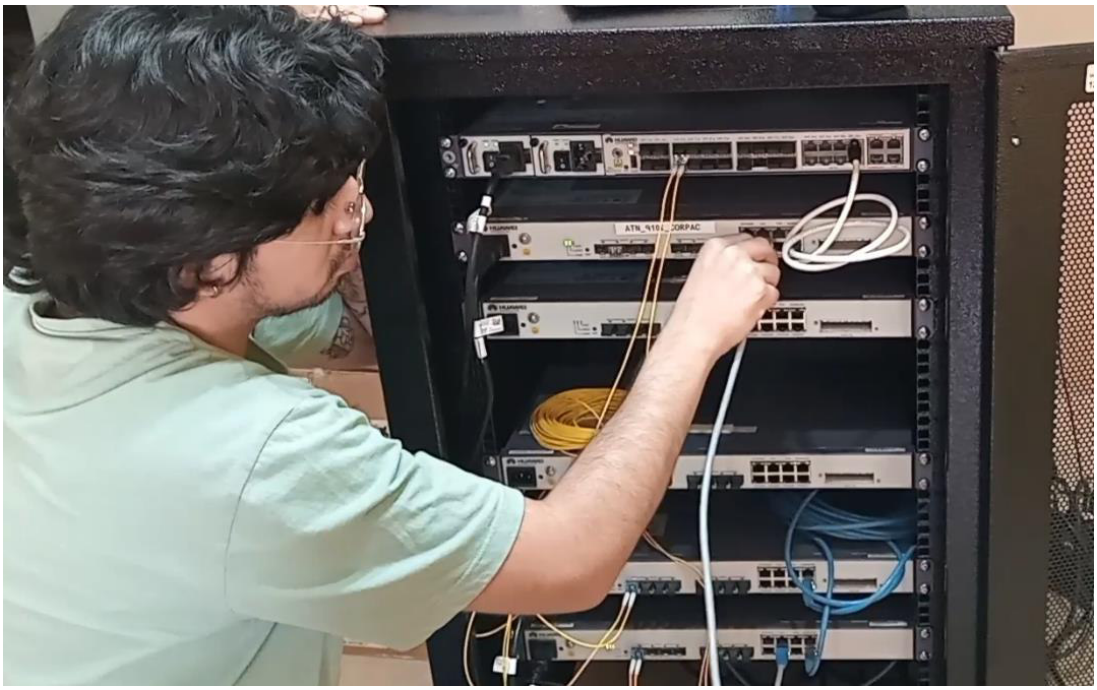

Figura 54: Cambiando a router de respaldo en sede central

Fuente: Elaboración propia

Como las conexiones y las sesiones LDP están establecidas en todos los equipos, solo hay mínima perdida de paquetes, y es porque se desconectó el dispositivo final del router principal, al router de respaldo.

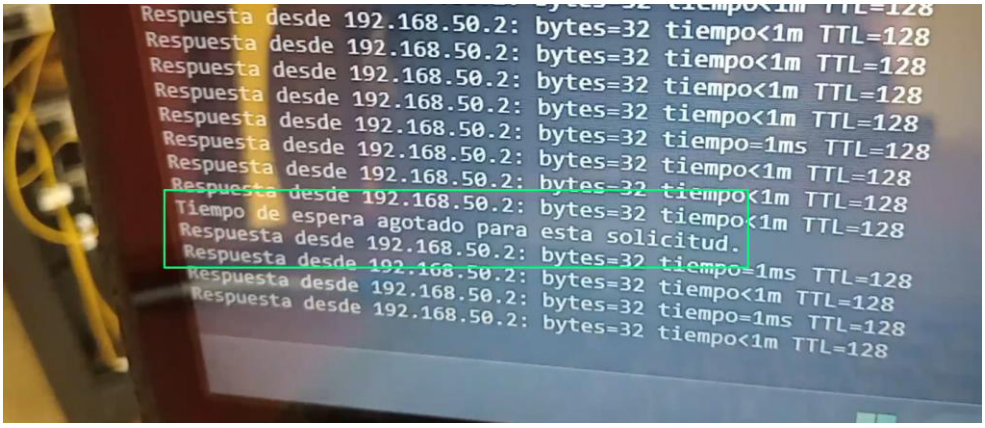

Figura 55: Ping constante entre dispositivos finales

Fuente: Elaboración propia

Para comprobar la funcionalidad del enlace de respaldo, se desconecta la fibra y se revisa el tiempo o la desconexión de paquetes:

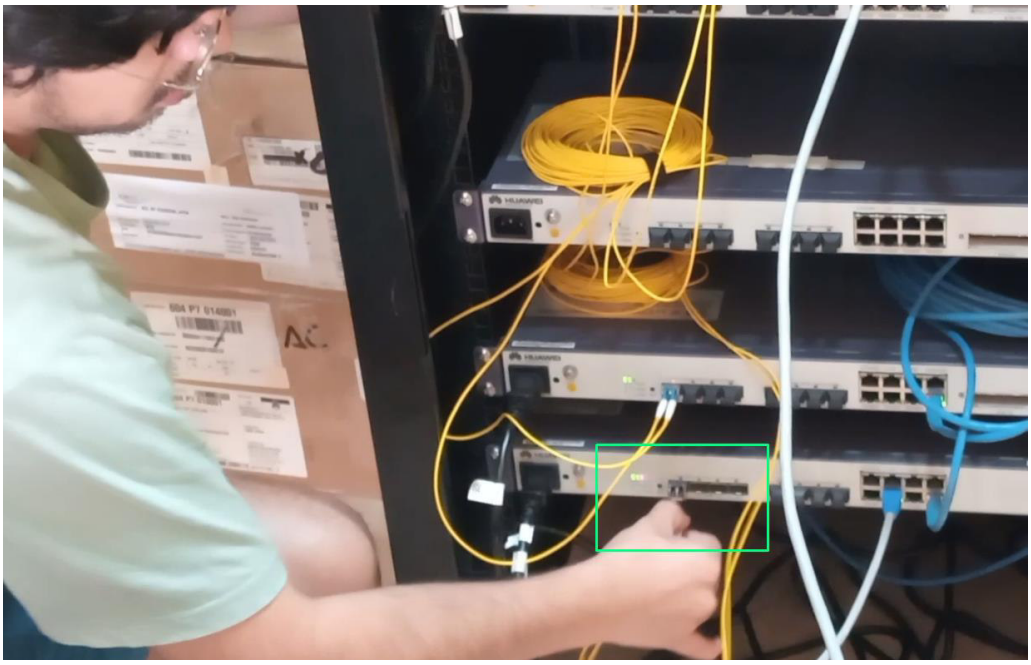

Figura 56: Desconexión del enlace de respaldo

Fuente: Elaboración propia

En teoría el enlace debería reestablecerse y mantener una conexión constante, con poca o nada perdida de paquetes, dado que las sesiones peer establecen un túnel directo gracias a MPLS/VPLS.

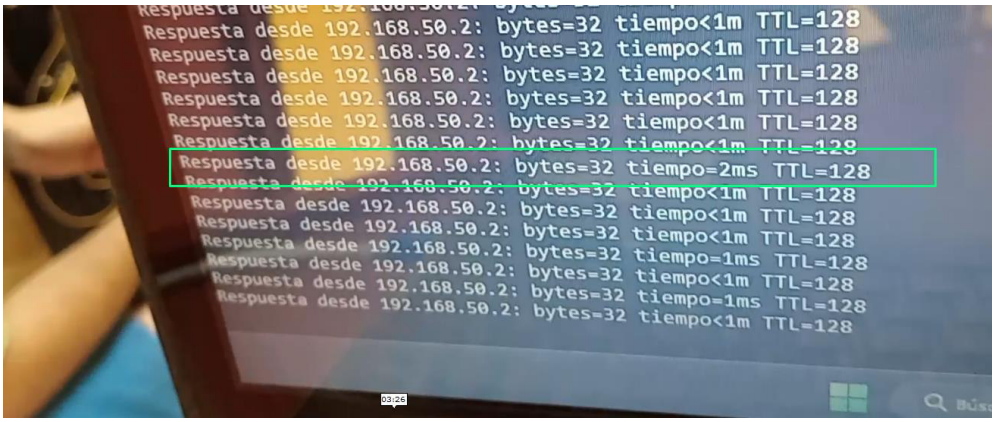

Figura 57: Demora en entrega de paquetes

Fuente: Elaboración propia

Hubo una demora de un milisegundo más, pero la conexión no se perdió o los paquetes no se perdieron. Como el cambio o restablecimiento entre todos los enlaces se hacen a velocidades entre milisegundos, el protocolo TCP puede hacer llegar los paquetes, verificando que lleguen a su destino. Para el caso de UDP, que es el protocolo empleado para los servicios de

videollamadas o VoIP, la perdida es mínima o nada en la mayoría de los casos, dado que siguen un camino con varias rutas de llegada, por lo que los paquetes al ser enviados, llegan a su destino.

CAPÍTULO IV: ANÁLISIS DE COSTO Y BENEFICIO

4.1. ANÁLISIS DE COSTOS

4.1.1. Recursos Humanos

En base a los recursos humanos utilizados para el proyecto, se abarco principalmente profesores y especialistas en redes y tecnología. Se realizaron consultas y se analizó el desarrollo del proyecto y en conjunto con los asesoramientos, se dieron mejores soluciones para realizar los objetivos propuestos. Todo ello se resume en la tabla 1:

Tabla 7: Costo de recursos humanos empleados en el proyecto

Descripción de la actividad	Personal	Costo
Profesor de redes	2	S/. 500.00
Profesor de networking	1	S/. 400.00
Especialista en equipos WAN	1	S/. 800.00
Asesores en diseño e implementación	1	S/. 700.00
TOTAL	5	S/. 2400.00

4.1.2. Recursos de hardware

En parte por los recursos materiales requeridos, incluye solamente los gastos necesitados para la implementación del enlace WAN en conjunto con su respaldo. No abarca gastos en la adquisición de teléfonos IP o Gateway de voz, *Routers* o *switchs* a gran escala. Como se mencionó, la red de comunicación es escalable, el tamaño o cantidad de usuarios o equipos que se conecten, los enlaces entre sedes o centrales, dependerán exclusivamente de la empresa que planea implementar una interconexión entre las diferentes sedes que contenga la empresa. El fin es que la misma empresa defina sus límites y lo que simplemente desea. Los materiales se muestran en la tabla 2:

Tabla 8: Recursos humanos

Und.	Material	Precio Uni.	Monto Soles
4	Router ATN	9500	38000
4	Patchcord fibra óptica	120	480
2	Ultima milla fibra	2000	4000
4	Transceivers	250	1000
	Total		43480

En la tabla se muestra los costos por hardware. No se menciona los costos por software pues los sistemas empleados son de uso libre, es decir gratis, como *Putty* o *Teraterm*, empleados para la configuración de equipos.

4.2. ANÁLISIS DE BENEFICIO

4.2.1. Beneficios Tangibles

Uno de los objetivos del proyecto es la disminución de costos por la implementación de enlaces dedicados para la interconexión de sedes. Habiendo expuesto el desarrollo y las increíbles ventajas que trae la implementación VPLS mediante el uso de la red pública, se puede afirmar que los beneficios tangibles que entrega el uso de VPLS son en gran manera muy útiles para pequeñas o medianas empresas. En primer lugar, a diferencia de los costos de enlaces privados o dedicados, no requieren pagos exorbitantes por emplear una conexión directa, segura y privada sea por fibra óptica, satelital o microondas. Es decir, los gastos son solo en implementación de la red propia y el servicio de un proveedor de internet (como cualquier servicio), y para futuras mejoras, soporte técnico si es requerido. Este es un gran beneficio económico ya que ahorra en gran manera gastos por enlaces dedicados a largas distancias, dado que mientras más largo el trayecto, más grande el costo.

4.2.2. Beneficios Intangibles

Implementar enlaces WAN con VPLS, con una calidad de servicio alta y redundancia para una alta disponibilidad, genera en el

entorno de la empresa, agilidad y trabajo ordenado por parte de los sistemas de comunicaciones. La implementación de enlaces WAN que ofrece calidad de voz y video, seguridad y redundancia genera un ambiente profesional en parte de los empleados, hacia los clientes y viceversa, puesto que mantiene un sistema de comunicaciones rápido y confiables. Cuando existe sistemas que agilizan y mejoran el rendimiento de trabajadores, el desarrollo económico llega como un increíble resultado, dando literalmente buenos frutos como empresa.

4.3. ANÁLISIS DE SENSIBLIDAD

4.3.1. Desarrollo del flujo de caja

El flujo de caja o cash Flow trata la diferencia entre los cobros y pagos realizados en periodo de tiempo concreto. Es decir, refleja las salidas y entradas financieras de la empresa. Por lo tanto, para realizar una visión del proyecto como producto en el mercado, se realiza el siguiente flujo de caja durante 4 años, se tiene la tabla 3:

Tabla 9: Flujo de caja anual

AÑO	N° Clientes	Ingreso S/. (A)	Egreso S/. (B)	Flujo de efectivo neto S/. (A-B)
1	1	55000	48000	7000
2	2	110000	96000	14000
3	4	220000	192000	28000
4	6	330000	288000	42000
	TOTAL	715000	624000	91000

De la tabla, el ingreso viene a ser el costo del enlace WAN. El egreso vendría a ser gasto requerido para su implementación. Teniendo a la diferencia de ambos como el flujo de efectivo neto.

4.3.2. Análisis del VAN

Para el cálculo del valor actual neto (VAN) en este proyecto. Se tiene la siguiente formula:

$$VAN = -I + \sum_{n=1}^{N} \frac{Q_n}{(1+r)^n}$$

Figura 58: Formula VAN

Fuente: Elaboración propia

Donde:

I = Inversión

Qn = Flujo de caja del tiempo n (normalmente años)

r = tasa de interés

N = Número de años de inversión

Para este caso se tiene:

I = S/. 50000

r = 12% = 0.12

N = 4 años

Para más facilidad, se calcula mediante una tabla de Excel, la figura 59 muestra la formula:

Qn	INVERSION=	50000	TASA=12%
7000			
14000			
28000			
42000			
	VAN=	44032.32	

$$VAN = -I + \sum_{n=1}^{N} \frac{Q_n}{(1+r)^n}$$

Figura 59: Análisis del VAN

Fuente: Elaboración propia

Para analizar este resultado, es sencillo:

$$VAN < 0 = Sin\ ganancias = Rechazado$$

$$VAN = 0 = No\ se\ pierde\ o\ gana = Impasible$$

$$VAN > 0 = Con\ ganancias = Aceptado$$

En este caso, como el VAN es mayor que cero, se concluye en un proyecto rentable.

4.3.3. Análisis del TIR

La tasa interna de retorno parte del flujo efectivo neto, pero también fuerza al VAN a cero. Lo que se pretende con TIR, es identificar la tasa de interés que vuelve al VAN a cero.

TIR = kTIR: VAN(kTIR) = 0

Donde kTIR es la tasa de descuento que representa la TIR.

También se le encuentra de la siguiente manera:

$$TIR = \sum_{T=0}^{n} \frac{Fn}{(1+i)^n} = 0$$

Figura 60: Ecuación de TIR

Fuente: Elaboración propia

Para el cálculo, en la figura 60 se muestra en una tabla de Excel:

Inversión Inicial	S/ 50,000.00

Flujo de Egresos	
Año	Egresos
1	S/ 48,000.00
2	S/ 96,000.00
3	S/ 192,000.00
4	S/ 288,000.00

Flujo de Ingresos	
Año	Ingresos
1	S/ 55,000.00
2	S/ 110,000.00
3	S/ 220,000.00
4	S/ 330,000.00

Flujo - Efectivo Neto	
Año	Efec. Neto
1	S/ 7,000.00
2	S/ 14,000.00
3	S/ 28,000.00
4	S/ 42,000.00

NEGOCIO	
Año	F. Caja
0	-S/ 20,000.00
1	S/ 7,000.00
2	S/ 14,000.00
3	S/ 28,000.00
4	S/ 42,000.00

Tasa. Descuento (K)	12%

TIR	>	K
69%	>	12%

TIR	69%	Rentable

VAN	S/ 44,032.32	Ganancias

Figura 61: Análisis del TIR

Fuente: Elaboración propia

Para analizar, se realiza de la siguiente manera:

$$TIR < k = No\ rentable = Rechazado$$

$$TIR = k = No\ se\ pierde\ o\ gana = Impasible$$

$$TIR > k = Rentable = Aceptado$$

En la figura 60 se muestra una tasa de descuento del 12%, como resultado en la formula, se obtiene un 69%, lo que corresponde como rentable al proyecto.

CONCLUSIONES

La llegada de la era digital influyo directa e indirectamente a las empresas o entidades del gobierno. Actualmente muchos de los servicios brindados son digitales o virtuales. Sin embargo, a la par de ello, muchas empresas pequeñas o medianas carecen de los sistemas o tecnología para mejorar sus sistemas comunicaciones o acceso a la información. Como se describió en el desarrollo del objetivo uno, el origen o la causa de estos muros yace en la carencia de habilidades o capacitaciones en nuevas tecnologías y sistemas de redes. Hasta el 2023, el 50% de las empresas en el Perú no se encuentran capacitadas para los desafíos futuros hacia adelante. Asimismo, mientras más información se digitaliza, los ataques o intrusiones de seguridad aumentan. Se ha descrito que muchas empresas no ofrecen protección de datos o sistemas de seguridad anti-ataques informáticos. Los avances tecnológicos mejoran cada vez más rápido, ello conlleva sistemas de redes e informáticos estables, disponibles y seguros. A la par, las empresas crecen económicamente junto con sus infraestructuras. Para mantener una comunicación centralizada y los servicios brindados por la empresa o entidades entre sedes en distintos puntos geográficos, además de sus sistemas de comunicación, requieren enlaces directos y privados para la agilización de sus bases de datos o todo tipo de información digital que se requiera. Sin embargo, muchas empresas pequeñas o medianas no pueden implementar enlaces dedicados o privados, a causa de los altos costos que implica un enlace directo. Para ello, el proyecto plantea la implementación de todos los beneficios de enlaces dedicados sin ninguna adquisición física de infraestructura o tendido de cables de fibra, microondas o satelital, por medio del protocolo MPLS junto con VPLS, que a través de la red pública, virtualmente se crean túneles directo y cifrados para ofrecer rapidez y seguridad en los enlaces WAN que interconectaran las distintas sedes que contenga una empresa o entidad, reduciendo costos en la implementación de enlaces WAN, mejoran la calidad de servicio.

Para implementar un enlace de red dedicado, se determinó seis características a tomar en cuenta: 1. Información o servicio que se envía a través del medio, no considerar este aspecto, puede causar falencias en el rendimiento o

escalabilidad de una red. 2. El ancho de banda y rendimiento de la red, vital cuando se tiene definido la cantidad de usuarios o servicios que se emplean en simultaneo, en tiempo real y no tener retrasos o cuellos de botella en red. 3. El medio de transmisión, que será el canal por donde viaja el tráfico de datos, que, dependiendo del presupuesto de la entidad u organización, se define. 4. Calidad de servicio, cuando el ancho de banda no es opción para mejorar el flujo de datos, se realizan colas o priorización de datos, evitando retraso en el envió de la información. 5. La seguridad del enlace, para evitar pérdidas catastróficas por el robo de información o secuestro de datos, dado que la información regularmente viaja por medios públicos. 6. Costo de enlace, es importante tener en cuenta el coste de un enlace, dado que son directamente proporcionales al presupuesto y la necesidad del usuario.

Al diseñar enlaces WAN con protocolos y medios de transporte que tengan redundancia y privacidad, se determinaron cuatro deficiencias comúnmente halladadas en red rústica: sin interconexión o conectividad transparente, red insegura, red central no jerarquizada y problemas en calidad de servicio. Para ello, el servicio de LAN privada virtual es un tipo de VPN (red privada virtual) que vincula varios sitios en un solo dominio a través de una red IP o de conmutación de etiquetas multiprotocolo (MPLS). Las empresas, entidades u organizaciones con VPLS tienen sus sitios vinculados a la misma red segura y de alta velocidad. Esto proporciona una conectividad transparente para las aplicaciones y servicios de red. Es decir, las ubicaciones remotas pueden acceder a recursos compartidos, como servidores, bases de datos y sistemas de almacenamiento, como si estuvieran conectados directamente a la misma LAN física. VPLS resuelve este desafío al crear una red virtual que emula una LAN, permitiendo a las ubicaciones remotas conectarse como si estuvieran en la misma red local física.

Para la implementación del proyecto, se empleó tecnología GPON, conectados a equipos HUAWEI de gama media, con tecnología que soporta las necesidades del ancho de banda, protocolos y servicios como VPLS, MPLS, IS-IS y configuración de QoS. Se simularon dos sedes, cada uno equipo central y respaldo, con el objetivo de generar redundancia. En caso de caer el enlace

principal, el respaldo se activa y mantiene conectados los flujos de datos entre ambas sedes. Al mantener enlaces directos virtuales como túneles, VPLS tiene la capacidad de mantener la privacidad y seguridad de la comunicación entre las ubicaciones remotas. Al utilizar una VPN, los datos transmitidos a través de la red VPLS están cifrados y protegidos contra accesos no autorizados. Esto garantiza la confidencialidad y la integridad de la información transmitida.

Al realizar pruebas de conexión, simulando caídas de enlace o la desconexión de equipos, se observa que la reconexión toma milisegundos, en pequeñas cantidades de tiempo, solo entre los enlaces principales toma 1 a 2 milisegundos. Con el enlace principal desconectado, se cae la sesión LDP entre el router principal y los restantes en la sede remota, y en segundos la sesión establecida con el router de respaldo de la sede principal, levanta o continua con la conexión, permitiendo el ingreso y salida de tráfico. Cuando se reestablece el enlace principal, si se llegare a desconectar el enlace de respaldo, aun estando conectado el dispositivo final en el router remoto de respaldo, la conectividad no se pierde, dado que la sesión LDP se mantiene, y el tráfico sabe que ruta tomar gracias a MPLS y el protocolo de enrutamiento IS-IS. Se comprueba la fiabilidad y el uso de VPLS para mejorar la calidad de servicio y seguridad sin emplear canales dedicados o privados.

RECOMENDACIONES

La implementación de VPLS implica el uso de etiquetas y túneles para encapsular el tráfico de datos y enviarlo a través de la red. Al configurarlo en distintos equipos, para generar redundancia y otros servicios, es necesario tener en cuenta la numeración de las etiquetas, en redes de largo alcance, duplicar o configurar de manera inadecuada puede generar perdida de paquetes o bucles en la red que pueden generar congestión que haga caer la red.

Con VPLS, la red también es escalable y flexible. Las organizaciones pueden agregar fácilmente nuevas ubicaciones a la red VPLS sin necesidad de realizar cambios significativos en la infraestructura existente. Además, VPLS admite la conexión de diferentes tipos de redes, como Ethernet, Frame Relay o ATM, lo que permite la integración de tecnologías existentes en la red VPLS. Por ello, al agregar nuevas sedes o generar redundancia entre ellas, se debe tener en cuenta la implementación de protocolos que evitar bucles de red. Sino se tiene en cuenta, la red se llena de tráfico y congestiona la red, haciendo caer los enlaces. La aplicación de protocolos como spanning tree, VRRP o HSRP son de interés para la implementación de enlaces redundantes a gran escala.

Asimismo, es importante tener en cuenta que la implementación de VPLS puede requerir un ancho de banda considerable, especialmente si hay muchas ubicaciones remotas o si se transmiten grandes volúmenes de datos. Además, la latencia y la calidad de la conexión pueden verse afectadas si la red VPLS está sujeta a congestión o si hay limitaciones en la infraestructura de la WAN. Por ello, se agregó la configuración de calidad de servicio en los puertos que manejan tráfico. El manejo de QoS es importante, para gestionar y mantener balance entre el tráfico entrante y saliente, evitando bloqueo o congestión de los datos.

REFERENCIAS

Adrianzen Rugel, C. M. (2017). *Diseño De Una Red IPVPN Con Tecnología MPLS Para Interconectar Sedes De La Empresa Cosapidata* [Tesis de ingeniería, Universidad Nacional Tecnológica de Lima Sur]. Repositorio Institucional Alicia https://alicia.concytec.gob.pe/vufind/Record/UNTL_dd441bfe1d5582203f9ae1c2121b72b4

Amazon Web Services. (15 de mayo de 2024). *¿Qué son las redes de computadoras? - Explicación de las redes de computadoras*. https://aws.amazon.com/es/what-is/computer-networking/

Anónimo. (1 de mayo de 2023). *¿Qué es la calidad de servicio QoS en redes de datos?* Comunidad Huawei Enterprise https://forum.huawei.com/enterprise/intl/es/thread/%C2%BFqu%C3%A9-es-la-calidad-de-servicio-em-qos-em-en-redes-de-datos/667235462626033664?blogId=667235462626033664

Pérez, A. (2020). *La seguridad de las redes*. Iste Internacional. https://iste-international.es/product/la-seguridad-de-las-redes/

Aquae Fundación. (24 de febrero de 2021). *Día Mundial de Internet, el invento de la nueva era*. https://www.fundacionaquae.org/wiki/dia-mundial-internet/

Barreto Priero, O. (2013). VPLS: alternativa de interconexión a través del backbone IP/MPLS de ETECSA VPLS: alternative of interconnection through ETECSA´s IP/MPLS backbone. *Revista Cubana de Ciencias Informáticas*, *7*(1), 32–43. http://rcci.uci.cu

Barzola Abad, D. G. (1 de agosto de 2023). *Virtual Private LAN Service (VPLS): Un enfoque avanzado para la conectividad de redes*. ABCXPERTS. https://abcxperts.com/virtual-private-lan-service-vpls-un-enfoque-avanzado-para-la-conectividad-de-redes/

C3NTRO Telecom. (26 de agosto de 2021). *Ventajas de usar SD-WAN en su empresa*. https://www.c3ntro.com/es-mx/blog/que-ventajas-brinda-utilizar-sd-wan-en-una-empresa

Canle Fernandez, E. (26 de febrero de 2025). *Historia de las redes informáticas: ¡lo que debes saber!* Tokio.School. https://www.tokioschool.com/noticias/historia-evolucion-redes-informaticas/

Castro, J. (25 de febrero de 2025). *Empresas peruanas bajo asedio: Más de 9 millones de ciberataques en un año*. America malls y Retail. https://america-retail.com/paises/peru/empresas-peruanas-bajo-asedio-mas-de-9-millones-de-ciberataques-en-un-ano/

Choquehuanca De Villanueva, A. M. (2023). *Madurez digital en las empresas peruanas*. Ministerio de la Producción. https://cdn.www.gob.pe/uploads/document/file/5573137/4954834-estudio-de-madurez-digital-en-las-empresas-peruanas.pdf

Cisco. (2012). Lo que usted necesita saber sobre routers y switches. *Cisco para pequeñas y medianas empresas*. https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

Cloudfare. (26 de febrero de 2023). *¿Qué son las redes empresariales?* https://www.cloudflare.com/es-es/learning/network-layer/enterprise-networking/

Dacartec. (15 de septiembre de 2024). *Consultoría y Servicios Informáticos*. https://dacartec.com.co/intranet-corporativa-cual-es-la-importancia-de-tenerla-su-empresa/

Datadec. (1 de marzo de 2023). *¿Cúal es el coste de la pérdida de datos en las empresas?* https://www.datadec.es/blog/cual-es-el-coste-de-perdida-datos-en-empresas

El comercio. (28 de enero de 2025). *Perú registra más de 1 millón de ciberataques en 2024: alertan sobre el aumento del phishing y ransomware*. Redacción EC. https://elcomercio.pe/respuestas/tecnologia/peru-registra-mas-de-1-millon-de-ciberataques-en-2024-alertan-sobre-el-aumento-del-phishing-y-ransomware-ciberdelincuentes-inteligencia-artificial-ia-ultimas-noticia/

España Boquera, M. C. (2003). *Servicios avanzados de telecomunicación* (1a ed., Vol. 1). Editorial Diaz de Santos

Espinoza Chipane, C. R. (2018). *Propuesta de una red privada virtual para mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.* [Tesis de ingeniería, Universidad Autónoma del Perú]. Repositorio Institucional UAP. http://repositorio.autonoma.edu.pe/handle/20.500.13067/487

Flo networks. (2024). *Seguridad de Red en la Implementación de WAN: Mejores Prácticas*. https://flo.net/es/seguridad-de-red-en-la-implementacion-de-wan-mejores-practicas/

Fortinet. (23 de septiembre de 2022). *¿Qué es la calidad de servicio (QoS) en las redes?* https://www.fortinet.com/lat/resources/cyberglossary/qos-quality-of-service

Globalspec. (21 de febrero de 2015). *ICT Downtime Costs Businesses $100 Million a Year, IHS Infonetics Says*. https://insights.globalspec.com/article/567/ict-downtime-costs-businesses-100-million-a-year-ihs-infonetics-says

Halabi, S. (2003). *Metro Ethernet: the definitive guide to enterprise and carrier Metro Ethernet applications*. Cisco Press.

Hernández Hernández, V. (2011). *VPLS una Opción de Transporte Ethernet* [Tesis de ingeniería, Universidad Central Marta Abreu de las Villas]. Repositorio Institucional UCLV. https://dspace.uclv.edu.cu/bitstreams/e7bf6d1a-6a75-43c9-b6a3-e4bdba6117be/download

Instituto Federal de Telecomunicaciones. (2021). *Modelo de Costos de Enlaces Dedicados de Interconexión*. https://www.ift.org.mx/politica-regulatoria/modelo-de-costos-de-enlaces-dedicados-de-interconexion

Instituto Nacional de Estadistica e Informatica. (11 de junio de 2021). *En el Perú existen más de 2 millones 838 mil empresas*. https://m.inei.gob.pe/prensa/noticias/en-el-peru-existen-mas-de-2-millones-838-mil-empresas-12937/

Ionos. (3 de febrero de 2020). *¿Qué es una WAN?* https://www.ionos.com/es-us/digitalguide/servidores/know-how/wan/

Juniper Networks. (23 de junio de 2021). *Introducción a OSPF*. https://www.juniper.net/documentation/mx/es/software/junos/ospf/topics/topic-map/ospf-overview.html

Keyfibre. (septiembre de 2024). *¿Qué es una acometida para un Enlace Dedicado?* https://www.keyfibre.com/que-es-una-acometida-para-un-enlace-dedicado/

Law, D. (2008). IEEE 802 Standards Overview. *Joint ITU-T/IEEE Workshop on Next Generation Optical Access Systems*. ITU https://www.itu.int/dms_pub/itu-t/oth/06/13/T06130000010005PDFE.pdf

Ley 31809. (2023). *Ley para el fomento de un Perú conectado*. Congreso de la Republica del Perú.

Ley 29022. (2007). *Ley para la expansión de infraestructura en telecomunicaciones*. Ministerio de Justica del Perú

López Cobos, C. A. y Robalino Vásconez, M. A. (2018). *Diseño de una red wan para interconectar las empresas de la Fundación Familia Salesiana Salinas utilizando Mikrotik* [Tesis de ingeniería, Universidad Politécnica Salesiana]. Respositorio Institucional UPS. http://dspace.ups.edu.ec/handle/123456789/15228

López González, U. (2017). *Diseño de una Red Privada Virtual usando una red MPLS* [Tesis de ingeniería, Universidad Politécnica de Madrid]. Repositorio institucional UPM. https://oa.upm.es/49980/1/PFC_UNAI_LOPEZ_GONZALEZ.pdf

Lorío Cabezas, D. M. y Mendoza Lopez, M. A. (2015). *Estudio de la tecnología VPLS (Virtual Private LAN Service) como solución de interconexión a las redes de datos que ofrecen los Proveedores de Servicios de Internet a los usuarios corporativos* [Tesis de ingeniería, Universidad Centroamericana]. Repositorio Institucional UCA. https://core.ac.uk/download/pdf/79471972.pdf

Menéndez Avila, R. A. (2012). *Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos* [Tesis de ingeniería, Pontificia Universidad Católica del Perú]. Repositorio Institucional. http://hdl.handle.net/20.500.12404/1500

Minería y energía. (10 de febrero de 2025). *El 76% de las empresas peruanas ha iniciado su Transformación Digital*. https://mineriaenergia.com/el-76-de-las-empresas-peruanas-ha-iniciado-su-transformacion-digital/

Mishima, M. (28 de septiembre de 2023). *Más del 50% de empresas peruanas no están preparadas para los desafíos del futuro*. https://www.ey.com/es_pe/newsroom/2023/09/empresas-peruanas-no-preparadas-desafios-futuro

Mohammed, A. (2014). OSI Model, *SpringerBriefs in Computer Science*. 5–17. https://doi.org/10.1007/978-3-319-05152-9_2

Nam-Kee, T. (2005). *MPLS for metropolitan area networks* (1a ed.). Auerbach. https://www.routledge.com/MPLS-for-Metropolitan-Area-Networks/Tan/p/book/9780849322129

Oficina de Prensa e Imagen Institucional de la Presidencia del Consejo de Ministros. (14 de mayo de 2020). *Ejecutivo acelera transformación digital del Estado para hacer frente a emergencia producida por el COVID-19*. https://www.gob.pe/institucion/pcm/noticias/154677-ejecutivo-acelera-transformacion-digital-del-estado-para-hacer-frente-a-emergencia-producida-por-el-covid-19

Osiptel. (2024). *Ficha informativa de la tarifa no teint2020000039*. Servicios Web Osiptel. https://serviciosweb.osiptel.gob.pe/ConsultaSIRT/Buscar/FrmVerTarifa.aspx?pTarifa=161952

Ospina, V. H., & Zajar, J. A. (2005). *Mpls/Vpls: servicio de Lan privada virtual sobre Mpls* [Tesis de ingeniería, Universidad Tecnológica de Bolivar]. Repositorio institucional UTB https://hdl.handle.net/20.500.12585/1206

Penaloza Seijas, S. D. (21 de marzo de 2019). *Introducción a MPLS*. Cisco Community. https://community.cisco.com/t5/documentos-routing-y-switching/introducci%C3%B3n-a-mpls/ta-p/3407436

Purple. (9 de noviembre de 2023). *Las ventajas y desventajas de las WAN*. https://purple.ai/es/blogs/las-ventajas-y-desventajas-de-las-wan/

Redondo Maíllo, J. L. (24 de noviembre de 2022). *El drástico cambio de Internet en los últimos 10 años*. Telefónica. https://www.telefonica.com/es/sala-comunicacion/blog/el-drastico-cambio-de-internet-en-los-ultimos-10-anos/

Rifa Pous, H., Gallego Terris, R., y Huertas García, V. (2019). *Contexto actual y evolución hacia las redes de nueva generación* (2a ed.). Editorial Fuoc.

Rodríguez Toala, B. A., Pincay Segovia, E. J., & Maldonado Zúñiga, K. (2022). Las redes wan y su importancia para los ordenadores. *UNESUM-Ciencias: Revista Científica Multidisciplinaria*, *6*(1), 1–14. https://revistas.unesum.edu.ec/index.php/unesumciencias/article/download/510/497/1849

Rojas Huamaní, D. (2015). *Rápida reconvergencia en la ingeniería de tráfico aplicada a un escenario MPLS VPN* [Tesis de ingeniería, Pontificia Universidad Católica del Perú]. Repositorio institucional PUCP. http://hdl.handle.net/20.500.12404/6223

Rojas, P. (19 de enero de 2024). *Los tipos de empresas que más incumplen la política de protección de datos personales: los casos más graves*. GESTIÓN. https://gestion.pe/economia/las-tipos-de-empresas-que-mas-incumplen-la-politica-de-proteccion-de-datos-personales-los-casos-mas-graves-anpdp-empresas-peruanas-noticia/

Santamaría Silupu, J. L., y Oviedo Calle, I. E. (2016). *Estudio de los diferentes modelos de inter-as MPLS-VPNs para brindar una propuesta técnica que permita la comunicación entre múltiples proveedores de servicios* [Tesis de ingeniería, Universidad Nacional de Piura]. Repositorio institucional UNP. https://repositorio.unp.edu.pe/items/b466f91e-2d76-422f-b297-c55dc666f429

Sencinet. (19 de abril de 2023). *Comunicación vía satélite: ¿Qué es, cuáles son sus ventajas y cómo funciona?* https://www.sencinet.com/es/blog/post/comunicacao-via-satelite-o-que-e-vantagens-e-como-funciona

Sistelec. (13 de noviembre de 2023). *Radioenlaces: Guía Completa*. https://sistelec.es/blog/radioenlaces/

Smith, A. (8 de diciembre de 2021). *Fiber Optic Cable Price Per Foot: How Much Does it Cost to Lay Fiber Optic Cable?* Costowl. https://www.costowl.com/b2b/cabling-wiring/cabling-fiber-optic-cabling-cost/

Suge3k. (2 de febrero de 2020). *El Internet y ancho de banda ideal para su empresa*. https://www.sugeek.co/el-internet-y-ancho-de-banda-ideal-para-su-empresa/

Tim, T. (4 de julio de 2023). *Protocolos de red básicos en la comprensión del modelo OSI*. Cisco Community https://community.cisco.com/t5/blogs-general/protocolos-de-red-b%C3%A1sicos-en-la-comprensi%C3%B3n-del-modelo-osi/ba-p/4810310

Velarde Sagastegui, J. (abril de 2010). *Calidad de Servicio en Internet*. Comisión Interamericana de Telecomunicaciones. https://www.oas.org/es/citel/infocitel/2010/abril/calidad_e.asp

Vesga Ferreira, J. C., Granados Acuña, G., y Vesga Barrera, J. A. (2015). Evaluación del rendimiento de una red lan sobre power line communications para la transmisión de voip. *ITECKNE*, *1*, 13.

Wendell, O. (2020). *CCNA 200-301: Official Cert Guide* (T. Mark, Ed.; 1a ed., Vol. 1). Cisco Press. https://elhacker.info/manuales/Redes/CCNA-200-301%201.pdf

WIN. (2024). *Fibra Óptica: Qué es, para qué sirve y ventajas*. WIN. https://win.pe/blog/conectate-al-futuro-todo-sobre-la-fibra-optica/

GLOSARIO

WAN: Red de área extensa

LAN: Red de área local

MPLS: Conmutación de etiquetas multiprotocolo

BGP: Protocolo de puerta de enlace

VPLS: Servicio de LAN privada virtual

VPN: Red privada virtual

SPT: Spanning Tree

QOS: Calidad de servicio

OSI: Interconexión de sistemas abiertos

ISO: Organización Internacional de Normalización

PDU: Unidades de datos de protocolo

AC: Punto de acceso

IP: Protocolo de internet

VOIP: Voz sobre IP

SD-WAN: Red global definida por software

RDSI: Red digital de servicios integrados

ATM: Modo de transferencia asíncrona

SONET: Red Óptica Síncrona

SOHO: Oficina pequeña Oficina en casa

ADSL: Línea de abonado digital asimétrica

OPGW: Cable óptico de tierra

RSVP: Protocolo de reserva de recursos

COS: Clase de servicio

DSCP: Punto de código de servicios diferenciados

OSPF: Abrir primero el camino más corto

ISIS: Sistema intermedio a sistema intermedio

SP: Proveedor de servicios

EMS: Ethernet multipunto

L2: Capa 2

MAC: Acceso de control al medio

DTLS: Servicio LAN transparente desacoplado

FEC: Clase equivalente de reenvío

LSP: Rutas de conmutación de etiquetas

LFIB: Base de información de envío de etiquetas

LDP: Protocolo de distribución de etiqueta

LIB: Información base de etiqueta

RIB: Información base de enrutamiento

PE: Proveedor de borde

MINJUS: Ministerio de Justicia

ANSI: Instituto Nacional Estadounidense de Estándares

IEEE: Instituto de ingenieros eléctricos y electrónicos

PCM: Presidencia de consejo de ministros

VLAN: LAN virtual

PQ: Prioridad justa

WFQ: Cola ponderada justa

ANEXOS

Guideline Router ATN 910 B Huawei

1) Descripción del hardware

El *router* HUAWEI necesita – 48 v DC como voltaje de entrada, el cual tiene los siguientes puertos para la conexión a la red metro Ethernet:

- 2 puertos *10 Gbps*
- 16 puertos SFP de 1 *Gbps*
- 8 puertos electricos of 1 *Gbps*

La figura 1.1 muestra una descripción grafica de puertos del *router*.

Figura 1.1 *Descripción de puertos en router HUAWEI*

El router posee dos módulos para conexión DC en modo 1:1 para energizar al equipo, la conexión se realiza como se muestra en la figura 1.2.

Figura 1.2 *Conexión eléctrica del router Huawei*

ANEXO F: MATRIZ DE INVESTIGACIÓN

Tabla 10: IMPLEMENTACIÓN DE ENLACES WAN PARA LA MEJORA DEL QOS DE LA RED DE TELECOMUNICACIONES EN MEDIANAS Y GRANDES EMPRESAS MEDIANTE LA INTERCONEXIÓN DE SEDES POR TECNOLOGÍA VPLS

PROBLEMÁTICA	PREGUNTA DE INVESTIGACIÓN	OBJETIVO GENERAL	PREGUNTA DE INVESTIGACIÓN	OBJETIVOS ESPECÍFICOS	ACCIONES	MARCO TEÓRICO	DESARROLLO	EVALUACIÓN	CONCLUSIONES	RECOMENDACIONES
Las redes de comunicaciones o tecnología son vitales para las empresas, puesto que el flujo de información que viaja a través de sus canales debe mantenerse constante, ser enviada y recibida en tiempo real, además de ser rápida, y segura con anchos de banda moderados. Sin embargo, para lograr dicha característica, se requiere inversión en hardware y software para establecer canales privados o dedicados. Soluciones donde los costos son muy elevados tan solo para establecer un servicio único, dependiendo del punto geográfico	¿Cómo mejorar la calidad de servicio de la red de telecomunicaciones de empresas medianas y grandes sin la necesidad de implementar enlaces dedicados o privados?	Implementar enlaces WAN mediante la interconexión de sedes por tecnología VPLS para mejorar el QoS de la red de telecomunicaciones sin la necesidad de implementar enlaces dedicados	¿Cuál es la situación actual de los servicios de redes y comunicaciones de sedes remotas que requieren interconectarse? *¿Qué características técnicas se deben tener en cuenta para enlaces de redes dedicados? *¿Cuáles serían los protocolos y medios de transporte adecuados para enlaces WAN redundantes y privados con el fin de mejorar el QoS de las redes de telecomunicaciones? * Cómo implementar enlaces WAN que permitan mejorar el QoS de las redes de telecomunicaciones sin necesidad de emplear canales privados o dedicados?	* Describir la situación actual de los servicios de redes y comunicaciones de sedes remotas que requieren interconectarse. * Determinar las características técnicas que se deben tener en cuenta para enlaces de redes dedicados. * Diseñar enlaces WAN con protocolos y medios de transporte que permitan redundancia y privacidad para mejorar el QoS de las redes de telecomunicaciones. * Implementar enlaces WAN que permitan mejorar el QoS de las redes de telecomunicaciones sin necesidad de emplear canales privados o dedicados.	*Identificar como están los servicios de comunicaciones entre sedes remotas. *Estudiar las características técnicas para implementar enlaces dedicados. *Analizar y estudiar los enlaces WAN y los protocolos que conlleva. *Instalación de equipos para la configuración de VPLS y protocolos *Comprobar la conexión o perdida de paquetes en distintos escenarios	*Modelo OSI – Capa 2 y 3 *Equipos de red *IP públicas y privadas *Enlaces WAN *Servicios de red *Ancho de banda y rendimiento de red *Medios de transmisión *QoS – calidad de servicio *OSPF *VPLS *MPLS	Se definió los conocimientos técnicos y teóricos para comprender el funcionamiento de los protocolos y servicios, con el objetivo de emplear y definir las configuraciones mas óptimas para el proyecto	Se realizó el cálculo del VAN y el TIR para evaluar el proyecto, obteniendo resultados de aprobación.	*La llegada de la era digital influyo directa e indirectamente a las empresas o entidades del gobierno. Actualmente muchos de los servicios brindados son digitales o virtuales. Sin embargo, a la par de ello, muchas empresas pequeñas o medianas carecen de los sistemas o tecnología para mejorar sus sistemas comunicaciones o acceso a la información. Como se describió en el desarrollo del objetivo uno, el origen o la causa de estos muros yace en la carencia de habilidades o capacitaciones en nuevas tecnologías y sistemas de redes. Hasta el 2023, el 50% de las empresas en el Perú no se encuentran capacitadas para los desafíos futuros hacia adelante. Asimismo, mientras más	*La implementación de VPLS implica el uso de etiquetas y túneles para encapsular el tráfico de datos y enviarlo a través de la red. Al configurarlo en distintos equipos, para generar redundancia y otros servicios, es necesario tener en cuenta la numeración de las etiquetas, en redes de largo alcance, duplicar o configurar de manera inadecuada puede generar perdida de paquetes o bucles en la red que pueden generar congestión que haga caer la red. *Con VPLS, la red también es escalable y flexible. Las organizaciones pueden agregar fácilmente nuevas ubicaciones a la red VPLS sin necesidad de realizar cambios significativos en la infraestructura existente. *Asimismo, es importante tener en cuenta que la implementación de VPLS puede requerir un ancho de banda considerable,

			*¿De qué manera se puede medir la eficiencia y rendimiento de los enlaces WAN?	* Realizar pruebas de estrés y conmutación a los enlaces de red de área extensa					información se digitaliza, los ataques o intrusiones de seguridad aumentan * Para implementar un enlace de red dedicado, se determinó seis características a tomar en cuenta: 1. Información o servicio que se envía a través del medio, 2. El ancho de banda y rendimiento de la red, 3. El medio de transmisión, 4. Calidad de servicio, 5. La seguridad del enlace y 6. Costo de enlace. * Al diseñar enlaces WAN con protocolos y medios de transporte que tengan redundancia y privacidad, se determinaron cuatro deficiencias comúnmente halladadas en red rústica: sin interconexión o conectividad transparente, red insegura, red central no jerarquizada y problemas en calidad de servicio. Para ello, el servicio de LAN privada virtual es un tipo de VPN (red privada virtual) que vincula varios sitios en un solo dominio a través	especialmente si hay muchas ubicaciones remotas o si se transmiten grandes volúmenes de datos. Además, la latencia y la calidad de la conexión pueden verse afectadas si la red VPLS está sujeta a congestión o si hay limitaciones en la infraestructura de la WAN. Por ello, se agregó la configuración de calidad de servicio en los puertos que manejan tráfico. El manejo de QoS es importante, para gestionar y mantener balance entre el tráfico entrante y saliente, evitando bloqueo o congestión de los datos.

									de una red IP o de conmutación de etiquetas multiprotocolo (MPLS). *Para la implementación del proyecto, se empleó tecnología GPON, conectados a equipos HUAWEI de gama media, con tecnología que soporta las necesidades del ancho de banda, protocolos y servicios como VPLS, MPLS, IS-IS y configuración de QoS. *Al realizar pruebas de conexión, simulando caídas de enlace o la desconexión de equipos, se observa que la reconexión toma milisegundos, en pequeñas cantidades de tiempo, solo entre los enlaces principales toma 1 a 2 milisegundos. Con el enlace principal desconectado, se cae la sesión LDP entre el router principal y los restantes en la sede remota, y en segundos la sesión establecida con el router de respaldo de la sede principal, levanta o continua con la conexión, permitiendo	

									el ingreso y salida de tráfico	