



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Académico Profesional de Ingeniería Electrónica

**Implementación de una red privada virtual para una
empresa comercializadora utilizando la estructura de
un ISP**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniera Electrónica

AUTOR

Miluska Doris CRISTOBAL REMUZGO

ASESOR

Carlos Alberto SOTELO LOPEZ

Lima, Perú

2021



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Cristobal, M. (2021). Implementación de una red privada virtual para una empresa comercializadora utilizando la estructura de un ISP. [Trabajo de suficiencia profesional, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Académico Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Miluska Doris Cristobal Remuzgo
Tipo de documento de identidad	DNI
Número de documento de identidad	70113662
URL de ORCID	
Datos de asesor	
Nombres y apellidos	Carlos Alberto Sotelo Lopez
Tipo de documento de identidad	DNI
Número de documento de identidad	07017259
URL de ORCID	https://orcid.org/0000-0001-8960-6567
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Teofilo Matias Huablocho Perez
Tipo de documento	DNI
Número de documento de identidad	25420840
Miembro del jurado 1	
Nombres y apellidos	Salomon Aristides Luque Gamero
Tipo de documento	DNI
Número de documento de identidad	07960620
Miembro del jurado 2	
Nombres y apellidos	Rejis Renato Paredes Penafiel
Tipo de documento	DNI
Número de documento de identidad	06758404

Datos de investigación	
Línea de investigación	Desarrollo de modelo y aplicación de las tecnologías de información y comunicaciones
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Santiago de Surco Urbanización: Monterrico Calle: Manuel Olguin Latitud: -12.087227 Longitud: -76.972951
Año o rango de años en que se realizó la investigación	Enero 2020 - Junio 2020
URL de disciplinas OCDE	Ingeniería eléctrica, Ingeniería electrónica https://purl.org/pe-repo/ocde/ford#2.02.00



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezcua 375 – Lima 1 – Perú



ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL Nº 021/FIEE-EPIE/2021

Los suscritos Miembros del Jurado, nombrados por la Comisión Ejecutiva del Programa de Perfeccionamiento Profesional de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha, Bajo La Presidencia Del **Ing. Huablocho Perez, Teofilo Matias** integrado por **Mg. Sotelo Lopez, Carlos Alberto** y el **Ing. Luque Gamero, Salomon Aristides**.

Después de escuchar la Sustentación de Trabajo de Suficiencia Profesional de la **Bach. CRISTOBAL REMUZGO, MILUSKA DORIS** con código Nº **11190121** que para optar el Título Profesional de Ingeniero Electrónico sustentó su Trabajo de Suficiencia Profesional titulada **"IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL PARA UNA EMPRESA COMERCIALIZADORA UTILIZANDO LA ESTRUCTURA DE UN ISP"**

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió **aprobar** otorgándole el calificativo de (17)

Ciudad Universitaria, 14 de diciembre del 2021

Ing. Huablocho Perez, Teofilo Matias
Presidente de Jurado

Mg. Sotelo Lopez, Carlos Alberto
Miembro de Jurado

Ing. Luque Gamero, Salomon Aristides
Miembro de Jurado

RESUMEN

El presente trabajo de suficiencia profesional tiene como objetivo determinar la importancia de la implementación de una RPVL (Red privada virtual local), garantizando la comunicación segura, íntegra y privada entre sedes de una empresa comercializadora de productos Falabella S.A.C. Dicha implementación se inicia enfocándose en el análisis de los parámetros más resaltantes de la tecnología MPLS, la cual cumple con las exigencias de las nuevas aplicaciones, críticas y sensibles a la seguridad de la información. Así mismo se define el problema raíz que llevó a cabo la implementación RPVL, siendo este el resultado planteado por un ISP(Proveedor de servicios de internet), posteriormente se presenta el marco teórico el cual permite entender la tecnología MPLS-VPN y los conocimientos previos para su comprensión, así mismo se determina el desarrollo de posibles alternativas de solución a implementar, comparando y eligiendo la mejor alternativa, con la finalidad de alinearnos al requerimiento de la empresa, se definen las apreciaciones técnicas, recursos, así como el desarrollo del escenario de contingencia para la sede principal. Posteriormente, se da a conocer los resultados adquiridos de la implementación y análisis correspondiente. Finalmente se determinan las conclusiones y recomendaciones frente a la implementación del servicio para la empresa Falabella S.A.C.

Palabras claves: implementación, RPVL, proveedor de servicio de internet, MPLS-VPN, contingencia.

ABSTRACT

The objective of this work of professional sufficiency is to determine the importance of the RPVL (Local Virtual Private Network) implementation, guaranteeing a secure, integrated and private communication between the branch offices of product marketing company Falabella S.A.C. That implementation begins by focusing on the analysis of the most outstanding parameters of MPLS technology, which meets the demands of new applications, critical and sensitive to information security. Likewise, the root problem carried out by the RPVL implementation is defined, being that the result raised by an ISP (Internet Service Provider), later the theoretical framework is presented which allows understanding the MPLS-VPN technology and previous knowledge for its understanding, likewise, the development of possible solution alternatives to be implemented is determined, comparing and choosing the best alternative. In order to align to the requirements of the company, technical assessments, resources and development of a contingency scenario for the main branch are defined. Subsequently, it disclosed the results obtained from the corresponding implementation and analysis. Finally, the conclusions and recommendations are determined after the implementation of the service for the company Falabella S.A.C.

Keywords: implementation, RPVL, Internet Service Porvider, MPLS-VPN, contingency

TABLA DE CONTENIDOS

RESUMEN	i
ABSTRACT	ii
TABLA DE CONTENIDOS	iii
LISTA DE TABLAS	vi
LISTA DE FIGURAS	vii
I. INTRODUCCIÓN	1
II. INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	2
III. DESCRIPCIÓN DE LA ACTIVIDAD	3
3.1. Descripción de la realidad del problema	3
3.2. Definición del problema	4
<i>3.2.1 Problema General</i>	<i>4</i>
<i>3.2.2 Problemas Específicos</i>	<i>5</i>
3.3. Justificación e importancia de la investigación	5
3.4. Objetivos de la Actividad	6
<i>3.4.1 Objetivo General</i>	<i>6</i>
<i>3.4.2 Objetivo Específicos</i>	<i>6</i>
3.5. Antecedentes de la Investigación	6
a. Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos.	6
b. Diseño de una red privada virtual para interconectar las sucursales de la empresa Terracargo S. A. C.	7
c. “Propuesta de una red privada virtual para mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.”	8
3.6. Bases Teóricas	8
<i>3.6.1 MPLS (Multiprotocol Label Switching)</i>	<i>8</i>

3.6.2. VPN (Virtual Private Network)	9
3.6.3. VPNs de capa 3	9
3.6.4. Enrutamiento BGP	10
3.6.4.1 Route-maps.	11
3.6.5. Protocolo HSRP	11
3.6.5.1. Operación de HSRP.....	11
3.6.5.2 Soporte de HSRP con MPLS VPN.....	12
3.6.6. Medios de Transmisión	12
3.6.6.1 Fibra Óptica.....	12
3.6.6.2 Radio Enlace.....	14
3.6.7. Dispositivos de Red	15
3.6.7.1 Router.	15
3.6.7.2 Switch.....	16
3.7. Diseño de la Investigación	17
3.7.1 Diseño de la red	17
3.7.1.1 Consideraciones de la red privada virtual local.....	18
3.7.1.2 Condiciones y restricciones de la red privada virtual local.....	18
3.7.2 Comparación entre alternativas de solución	18
3.7.2.1 Servicio Local Private Line.	19
3.7.2.2 Servicio de red exclusivo IP.....	19
3.7.2.3 Red Privada Virtual Local.	20
3.7.3 Elección de la solución	21
3.7.4 Diagrama de red	22
3.7.5 Conexión Física.....	24
3.7.5.1 Equipos principales para el enlace de Fibra Óptica	25
3.7.5.2 Equipos principales para el Radio Enlace	30
3.7.5.3 Sede Oficinas Administrativas	35
3.7.5.4 Sede Data Center	36
3.7.5.5 Sede Sucursal	38
3.7.5.6 Sede Mall Aventura Plaza, Enlace Principal y Contingencia	39
3.7.5.7 Visualización del Media Converter	43
3.7.6 Asignación de Recursos Lógicos en la red IP/MPLS.....	44
3.7.6.1 Sede de oficinas administrativas	45

3.7.6.2	Sede Data Center	46
3.7.6.3	Sede Sucursal	47
3.7.6.4.	Sede Mall Aventura Plaza, Enlace Principal y Contingencia.	48
3.7.7	Configuración de MPLS VPN.....	50
3.7.7.1	Proceso de enrutamiento entre P-PE y PE-PE..	51
3.7.7.2	Proceso de enrutamiento PE-CPE.	53
3.7.7.3	Proceso de enrutamiento en el CPE	56
3.7.8	Distribución de BW para las sedes	57
3.7.9	Enlace principal y contingencia para la sede Tienda Mall Aventura Plaza	58
3.7.9.1	Influencia del tráfico de entrada.	58
3.7.9.2	Influencia del tráfico de salida.	60
3.8.	Presentación de resultados	63
3.8.1	Conectividad entre equipo PE y CPE	63
3.8.2	Establecimiento del protocolo BGP entre CPE y PE.....	63
3.8.3	Conexión entre sedes	64
3.8.4	Actividad de alta disponibilidad para la sede Mall Aventura Plaza	65
IV.	CONCLUSIONES.....	69
V.	RECOMENDACIONES	71
VI.	BIBLIOGRAFIA.....	72

LISTA DE TABLAS

Tabla 1. <i>Ventajas y Desventajas de Fibra Óptica</i>	13
Tabla 2. <i>Ventajas y Desventajas de Radio Enlace</i>	15
Tabla 3. <i>Esquema comparativo de IPLS y RPVL</i>	22
Tabla 4. <i>Características iTN2100</i>	26

LISTA DE FIGURAS

Figura 1. Estructura de un Red Privada Virtual.....	9
Figura 2. Diagrama HSRP con MPLS/VPN	13
Figura 3. Fibra Óptica	13
Figura 4. Radio Enlace	15
Figura 5. Representación simbólica de un router.....	16
Figura 6. Representación simbólica de un switch	17
Figura 7. Topología de Servicio Local Private Line.....	20
Figura 8. Servicio Red Exclusivo	21
Figura 9. Topología de Servicio Red Privada Virtual Local.....	22
Figura 10. Esquema de Red Propuesto.....	25
Figura 11. Concentrador iTN2100.....	27
Figura 12. Slots y Tarjetas de Concentrador iTN.....	28
Figura 13. Media Converter RC552	28
Figura 14. Interconexión física de equipos del enlace Fibra Óptica	30
Figura 15. Comunicación de IP-10 Ceragon en una red Ethernet Metropolitana	31
Figura 16. Panel Frontal IDU	32
Figura 17. FibeAir RFU-C	33
Figura 18. Interconexion Fisica de los equipos de Radio Enlace.....	35
Figura 19. Enlace físico entre la sede administrativa y el equipo de acceso a la red.....	36
Figura 20. Ubicación de la Tarjeta MC en el POP 4	37
Figura 21. Enlace físico entre la sede Data Center y el equipo de acceso a la red.....	37
Figura 22. Ubicación de la Tarjeta MC en el POP 3	38
Figura 23. Enlace físico entre la sede sucursal y el equipo de acceso a la red	39
Figura 24. Ubicación de la Tarjeta MC en el POP 2	40

Figura 25. Enlace físico entre la sede Principal y el equipo de acceso a la red	40
Figura 26. Ubicación de la Tarjeta MC en el POP 1	42
Figura 27. Ubicación de Interfaz en IDU de Radio Lado Nodo	43
Figura 28. Ubicación de Interfaz en IDU de Radio Lado Cliente.....	44
Figura 29. Topología de Interconexión entre iTN2100 y Media Converter...	44
Figura 30. Estado de Media Converter RC552-FE-B.....	45
Figura 31. Topología de red para la sede Of. Administrativas	47
Figura 32. Topología de red para la sede Data Center.....	48
Figura 33. Topología de red para la sede Sucursal	49
Figura 34. Topología de red para la sede Mall Aventura Plaza-Enlace Principal	50
Figura 35. Topología de red para la sede Mall Aventura Plaza-Enlace Contingencia.....	51
Figura 36. Topología de equipos de red para enrutamiento	52
Figura 37. Indicadores de VRF para importación y exportación de rutas	53
Figura 38. Redistribución de rutas conectadas y estáticas	53
Figura 39. Verificación de la propagación de prefijos entre PE	54
Figura 40. Establecimiento de la sesión BGP entre PE y CPE	56
Figura 41. Anuncio de prefijos hacia la red MPLS del ISP.....	56
Figura 42. Establecimiento de la sesión BGP entre Router del cliente y CPE	58
Figura 43. Anuncio de redes LAN del router del cliente hacia el CPE	58
Figura 44. Configuración de route-map en el CPE principal y secundario...	60
Figura 45. Configuración de listas route-map en los PE	60
Figura 46. Rutas obtenidas en la red con valor de Local Preference.....	61
Figura 47. Diagrama de enlace redundante con HSRP	62
Figura 48. Diagrama de configuración HSRP sobre R1.....	62
Figura 49. Diagrama de configuración HSRP sobre R5.....	63
Figura 50. Verificación de estatus de R1 como router activo HSRP	63
Figura 51. Verificación de conectividad entre PE y CPE	64
Figura 52. Sesión BGP establecida entre CPE y PE	65
Figura 53. Redes LAN recibidas por sede remota	65
Figura 54. Redes LAN recibidas por sede remota	66

Figura 55. Traceroute desde los equipos de red hacia la LAN del cliente ...	67
Figura 56. Verificación de prioridad HSRP en CPE	68
Figura 57. Traceroute desde CPE hacia otra sede remota	68
Figura 58. Gráfica cacti del enlace Principal	69
Figura 59. Gráfica cacti del enlace Contingencia	69

I. INTRODUCCIÓN

Actualmente los servicios de telecomunicaciones se han vuelto indispensables para las empresas de comercialización, las cuales requieren desplegar múltiples sedes tales como oficinas administrativas, data centers, sucursales entre otros, manteniendo una comunicación segura e integra. Esto se ha convertido en una solución ideal a su requerimiento, la implementación de las llamadas redes privadas virtuales (VPNs), las cuales tienen la particularidad de permitir el uso de infraestructura compartida ofrecida por un ISP para ser implementadas.

Lo que se analizara en el estudio actual es la implementación del servicio VPN de capa 3 sobre la tecnología MPLS ofrecido con la finalidad de proveer conectividad entre las diferentes sedes de la empresa de manera escalable, objetiva y económica, donde el proveedor de servicio tiene el rol más importante en cuanto a las operaciones de enrutamiento.

Al final se propone al lector a revisar el estudio planteado en las posteriores páginas que en compilación busca presentar una solución para la empresa comercializadora, la cual se encuentra expuesta a constantes cambios socioeconómicos y tecnológicos.

II. INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

Las actividades vistas en el presente trabajo de suficiencia profesional se realizaron en la empresa AMERICATEL. El periodo de duración fue de seis meses, específicamente desde enero del 2020 hasta junio del 2020.

La finalidad y objetivos es que se desarrolló una solución de conectividad de datos para una empresa comercializadora de productos sobre la infraestructura de un ISP, la cual cuenta con 4 sedes, una sede principal ubicada en el centro comercial Mall Aventura Plaza de mucha afluencia de público, sede data center, sede sucursal y sede of. administrativas, por lo que es ideal para mostrar las ventajas y mejores bondades de diseñar una red Privada Virtual Local para dicha empresa. La razón social es AMERICATEL PERU S.A, la dirección se encuentra Av. República de Colombia Nro. 791 Int. 18, San Isidro; y por último, el correo electrónico del profesional a cargo es jose.burga@entel.pe.

III. DESCRIPCIÓN DE LA ACTIVIDAD

3.1. Descripción de la realidad del problema

Con el pasar de las décadas en el Perú y el mundo entero las empresas comerciales han cambiado mucho en cuanto a su visión de llevar a cabo el mercado global, local y logístico. Muchas de ellas tienen la necesidad de distribuir sus recursos a través de todo el país y también fuera de este. Es por ello que el uso de las VPN se ha convertido en un factor muy importante para dichas organizaciones, ya que transmiten información de manera segura, confiable y rentable a través del entorno geográfico.

La empresa Falabella S.A.C es un grupo empresarial de comercio a nivel de todo Lima, el cual cuenta con una sede central ubicada en el centro comercial Mall Aventura Plaza de Santa Anita, primer establecimiento comercial de la empresa en Lima, el cual requiere de un sistema de contingencia para sus demás dependencias, las cuales son: una sede de of. administrativas, donde están ubicadas las agencias encargadas de las operaciones administrativas de la empresa, una sede Data Center donde se encuentran los equipos de red y servidores pertenecientes a la empresa y gestionados por la misma, y una sede sucursal utilizada para realizar operaciones complementarias que competen a la empresa, dichas sedes se encuentran ubicados en los distritos de Santa Anita, San Borja, San Juan de Lurigancho y Miraflores respectivamente. La sede central cuenta con un sistema global de automatización de procesos operacionales para la organización, sin embargo, sus dependencias no cuentan con dicho sistema global, aquellas dependencias operan la información de manera aislada y particular de la sede central, y para el procesamiento de sus datos no consideran las aplicaciones utilizadas actualmente en la sede central, sino que

en realidad disponen de una aplicación tradicional desarrollada anteriormente por la empresa.

Por lo tanto, es necesario establecer una conexión segura entre la sede central y sus dependencias, de tal forma que las aplicaciones puedan ser utilizadas de manera global por las dependencias, evitando generar sobrecostos y una doble operación al conservar la información de datos en la organización de manera independiente.

Para dar solución al problema presentando por la empresa comercializadora Falabella S.A.C vamos a desarrollar una VPN utilizando la tecnología MPLS haciendo uso de la infraestructura de un ISP, quien tiene el rol más importante en cuanto a las operaciones de enrutamiento, logrando de esta manera la transmisión de datos de manera eficiente entre las sucursales de la empresa. Así mismo se desarrolló un sistema de contingencia para la sede central, lugar que tiene una gran demanda de usuarios debido a estar ubicado en un centro comercial, dicho sistema reemplazara efectivamente las funciones realizadas por el enlace principal, manteniendo la misma distribución de ancho de banda y utilizando la adecuada tecnología de respaldo, por lo cual se optó elegir un medio de transmisión diferente al enlace principal, debido a su accesible implementación de contingencia.

3.2. Definición del problema

3.2.1 Problema General

- ¿Cómo implementar una red privada virtual para la empresa comercializadora utilizando la infraestructura de un ISP?

3.2.2 Problemas Específicos

- ¿Cómo implementar la topología de la red privada virtual para la empresa comercializadora?
- ¿Cuál sería la arquitectura de la red privada virtual de la empresa comercializadora?
- ¿Cuál sería el tipo de servicio de red privada virtual se implementaría para la empresa comercializadora?
- ¿Cuál sería el dimensionamiento de capacidad para la red privada virtual de la empresa comercializadora?

3.3. Justificación e importancia de la investigación

A medida que los años pasan las empresas crecen y requieren efectuar cambios funcionales y estructurales en su red de manera eficiente, segura y económica. La empresa Falabella S.A.C busca minimizar los gastos de inversión hardware y servicios de telecomunicaciones relacionados a la distancia comprendida en la conexión de sus sedes y ello es posible con el empleo de las VPNs a través de la infraestructura de un ISP. Los ISP buscan continuamente extender los alcances de sus redes MPLS. La tecnología MPLS provee una gran velocidad y escalabilidad en la transmisión de datos, en donde las VPNs son su servicio más utilizado. Así mismo esta tecnología tiene la característica de ser independiente en cuanto a la selección del ISP, por lo cual la empresa puede realizar cambios de proveedor cuando este lo prefiera sin la obligación de realizar cambios en el equipamiento.

La finalidad es presentar las ventajas que ofrece la implementación de la VPN en la empresa Falabella S.A.C, siendo una de ellas la escalabilidad que presenta esta tecnología, permitiendo la expansión de la empresa a nivel de sedes y usuarios, la administración remota según régimen de la empresa, y los bajos costos de inversión a nivel de actualizaciones informáticas.

3.4. Objetivos de la Actividad

3.4.1 Objetivo General

- Implementar una red privada virtual a través de la infraestructura de un ISP para la empresa comercializadora Falabella S.A.C aplicando los beneficios que otorga la tecnología MPLS.

3.4.2 Objetivo Específicos

- Diseñar la topología de la red privada virtual para la empresa.
- Diseñar la arquitectura de la red privada virtual para la empresa.
- Diagnosticar el tipo de servicio de red privada virtual que se implementara para la empresa.
- Determinar el dimensionamiento de capacidad de la red privada virtual para la empresa.

3.5. Antecedentes de la Investigación

Para el desarrollo de implementación de una red privada virtual a través de la infraestructura de un ISP, se tuvo como antecedentes algunos trabajos de investigación relacionado a implementación de redes privadas virtuales, como se mencionan a continuación.

a. Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos.

Menéndez (2012) brindó una propuesta técnica para la implementación de una red MPLS sobre Múltiples Sistemas Autónomos, realizando un estudio del desempeño de cuatro diferentes modelos de implementación para

proporcionar dicha solución. Presenta un marco teórico que permite entender y conocer las redes VPN, y las arquitecturas implicadas en su funcionamiento, específicamente la tecnología MPLS. Posteriormente se exponen los diferentes modelos de red para la implementación de las VPN Multi-AS y se desarrolla un estudio del desempeño de cada uno ellos.

En esta tesis citada, estudia el desempeño de las redes privadas virtuales a través de la tecnología MPLS, utilizando sistemas autónomos con enrutamiento eBGP (Eternal Border Gateway Protocol), así mismo muestra diferentes formas de implementar una VPN, como método de instrucción.

b. Diseño de una red privada virtual para interconectar las sucursales de la empresa Terracargo S. A. C.

Días y Vieyra (2015) realizaron el perfeccionamiento de interconexión entre las sedes de la empresa Terracargo SAC, la cual tiene sucursales en diferentes ciudades del Perú. Este perfeccionamiento se realizó a través de la implementación de una VPN, permitiendo la intercomunicación en tiempo real entre sus sucursales, de manera eficiente y segura. La investigación fue realizada en 3 etapas. En la primera etapa se realizó un diagnóstico de la actualidad de la empresa, la arquitectura de cada una de sus sucursales, la disponibilidad de hardware, usuarios y el trabajo de interconexión, toda esta información permite seleccionar y diseñar el modelo de VPN adecuado. En la segunda etapa se diseñó un modelo de red VPN acorde a los requerimientos de la empresa ofreciendo la mejor solución sin generar gastos económicos excesivos.

En esta tesis citada, se expone el trabajo de conexión de las sucursales remotas mediante el uso de una red privada virtual, así mismo debido a la ubicación geográfica de las diferentes sedes en toda la región, se optó por utilizar una tecnología adecuada, de fácil administración y mantenimiento, así mismo presenta una evaluación de presupuesto.

c. “Propuesta de una red privada virtual para mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.”

Espinoza (2018) propone una solución de VPN para mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A. Esta investigación se realizó en base a la metodología PPDIOO de Cisco Systems, lo cual brindara los procesos, habilidades y técnicas necesarias para lograr la propuesta de implementación. El mejoramiento del servicio de comunicación en las tiendas Mass se comprueba por medio del enlace virtual enlazando dos o más sucursales geográficamente separadas. Se utilizó el modelo OSI como referencia en la interpretación de capas de red.

En esta tesis referenciada, se presenta la implementación de una red privada virtual utilizando como infraestructura un proveedor ISP, el Internet, permitiendo mejorar la comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A. Lo cual conlleva mejorar el tiempo de latencia del servicio de comunicación, disminuir las incidencias por temas de lentitud o intermitencia en la red, proporcionar escalabilidad en la red y evitar los sobrecostos por el servicio de comunicación.

3.6. Bases Teóricas

3.6.1 MPLS (*Multiprotocol Label Switching*)

Cisco (s.f.-c) menciona que la tecnología MPLS permite a las empresas y proveedores de servicios construir redes inteligentes de próxima generación que puedan distribuir una amplia variedad de servicios avanzados y de valor agregado sobre una misma infraestructura de red. Esta económica solución puede ser integrada similarmente sobre cualquier infraestructura ya existente como lo es IP, Frame Relay, ATM o Ethernet. Empresas con diferentes

enlaces de acceso pueden ser agregados a un borde de la red MPLS sin la necesidad de cambiar su entorno actual, por lo que MPLS es independiente de las tecnologías de acceso.

La integración de los componentes de la aplicación MPLS, incluyendo VPNs de capa 3, VPNs de capa 2, Ingeniería de tráfico, QoS, GMPLS, e IPV6 permiten el desarrollo de redes altamente eficientes, escalables y seguras que garantizan los acuerdos de nivel de servicio (SLA).

3.6.2. VPN (Virtual Private Network)

Menéndez (2012) menciona que una VPN es una estructura de red que emula una red privada sobre infraestructura pública existente, que provee la comunicación a nivel de las capas 2 o 3 del modelo OSI. La VPN pertenece generalmente a una compañía y le permite tener diferentes locales interconectados a través de la infraestructura de un proveedor de servicios (Figura 1).

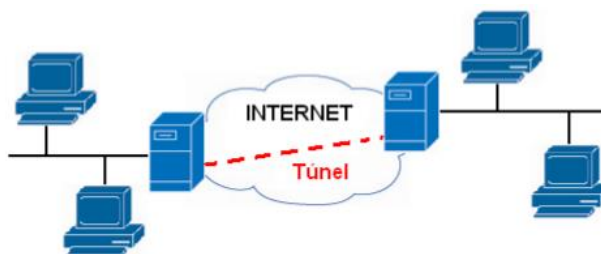


Figura 1. Estructura de un Red Privada Virtual (Fuente: Menéndez, 2012)

3.6.3. VPNs de capa 3

Cisco (s.f.-a) menciona que las VPNs de capa 3 en MPLS usan el modelo peer-to-peer¹, el cual utiliza el protocolo de enrutamiento BGP (Border Gateway Protocol) para distribuir información relacionada con la VPN. Este

¹ Modelo Peer-to-peer: tipo de arquitectura para la comunicación entre aplicaciones.

modelo altamente escalable, permite a los usuarios empresariales externalizar el envío de información de enrutamiento a los proveedores, de tal manera que resulte en un significativo ahorro de costos y reducción en la complejidad operacional para las empresas.

Las VPN's basadas en IP usan la tecnología VRF-Lite (Virtual Routing/Forwarding instance), llamada Easy Virtual Network (EVN). Este mecanismo simplifica la virtualización de redes de capa 3 y permite a los usuarios proporcionar fácilmente la separación de tráfico y el aislamiento de caminos en infraestructura de red compartida, quitando la necesidad de desarrollar MPLS en la red de la empresa.

3.6.4. Enrutamiento BGP

Ariganello y Barrientos (2010) mencionan que BGP (Border Gateway Protocol) es un protocolo de enrutamiento moderno diseñado para ser escalable y poder utilizarse en grandes redes creando rutas estables entre las organizaciones. BGP soporta VLSM (Variable Length Subnet Mask), CIDR (Classless Interdomain Routing) y sumarización.

BGP es el único protocolo que actualmente soporta enrutamiento entre dominios. Los dispositivos, equipos y redes controlados por una organización son llamados sistemas autónomos, AS. Por lo tanto, BGP comunica los AS con independencia de los sistemas que utilice cada organización.

Otro punto clave es que BGP pretende que las redes permanezcan despejadas de tráfico innecesario el mayor tiempo posible. Las configuraciones de BGP requieren determinaciones de políticas muy complicadas. El sistema que BGP utiliza para controlar la selección de rutas es bastante sofisticado, habrá momentos en que el administrador tendrá que influir en ese comportamiento modificando los atributos del protocolo. Existen muchos métodos para influenciar la selección de caminos en BGP, pero los route-maps son los más utilizados.

3.6.4.1 Route-maps. Ariganello y Barrientos (2010) mencionan que los route-maps son herramientas que establecen coincidencias con un determinado patrón y que pueden utilizarse para cambiar la cabecera del paquete, el mapa de ruta, etc. Los route-maps son similares a las listas de acceso, pero más complejos debido a que permiten hacer muchas más cosas.

3.6.5. Protocolo HSRP

Cisco (2011) menciona que una forma de lograr que el tiempo de actividad de la red esté cerca del 100 % es utilizar HSRP², es el método estándar de Cisco de proporcionar alta disponibilidad de la red, ofrece redundancia para las redes IP, asegurando que el tráfico de usuarios se recupere de forma inmediata y transparente de las fallas del enrutador de primer salto.

HSRP permite que varios routers que pertenecen a una sola red LAN compartan una dirección MAC e IP, la cual está configurada como puerta de enlace predeterminada en los hosts.

3.6.5.1. Operación de HSRP. Del grupo de routers configurados en un grupo HSRP, el que tiene la prioridad más alta funciona como el enrutador activo y el que tiene la segunda prioridad más alta funciona como el router standby. El router activo tiene la función de reenviar paquetes enviados a la dirección IP virtual. Si el enrutador activo falla, el standby toma el control como el nuevo router activo. El enrutador activo responde a todas las consultas del Protocolo de mensajes de control de Internet (ICMP) y del Protocolo de resolución de direcciones (ARP) enviadas a la dirección IP virtual.

² HSRP: Hot Standby Router Protocol

3.6.5.2 Soporte de HSRP con MPLS VPN. En la figura 2, se muestra dos PE con HSRP ejecutándose entre sus interfaces VPN. Se configura el CE con una dirección IP virtual HSRP como su ruta predeterminada. Y se configura el HSRP para rastrear las interfaces que conectan los PE al resto de la red proveedora.

Si la interfaz E1 de PE1 falla, la prioridad de HSRP se verá reducida de modo tal que PE2 tomará el control del reenvío de paquetes a la dirección IP/MAC virtual.

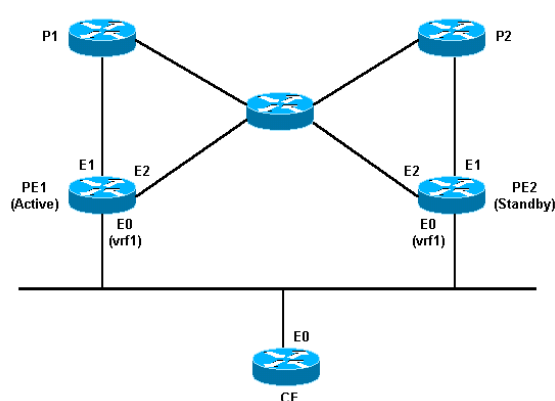


Figura 2. Diagrama HSRP con MPLS/VPN (Fuente: Cisco, 2011).

3.6.6. Medios de Transmisión

3.6.6.1 Fibra Óptica. Tanto EcuRed (s.f) y Wikipedia (2020b) mencionan que la fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir (Figura 3).

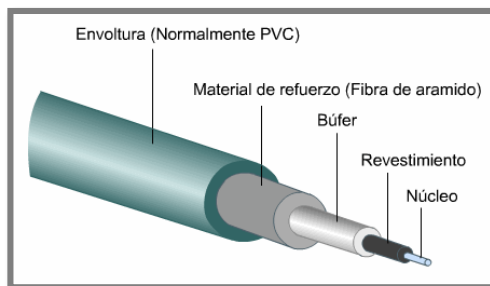


Figura 3. Fibra Óptica (Fuente: Chen, 2015)

Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio y superiores a las de cable convencional.

Para las comunicaciones se emplean fibras multimodo y monomodo, usando el multimodo para distancias cortas (hasta 500 m) y las monomodo para acoplamientos de larga distancia. En la tabla 1, se muestran las ventajas y desventajas de la Fibra Óptica.

Tabla 1.

Ventajas y Desventajas de Fibra Óptica

Ventajas	Desventajas
Inmunidad a interferencia electromagnética	Una inversión inicial mayor
Sin lazos de tierra por ser dieléctrica	Las conexiones, empalmes y prueba son más complicadas
Pérdidas muy bajas	Requiere personal adecuadamente entrenado
Gran ancho de banda	Miedo al material desconocido
Más pequeña que el UTP	Requiere que algunos equipos y herramientas sean cambiados
Más segura	
Cero riesgos de choques eléctricos	

Un rango amplio de temperatura

Baja cantidad de repetidores

Mejor relación costo/beneficio

No obsolescente

Mejor relación costo/beneficio

Fuente: Elaboración propia

3.6.6.2 Radio Enlace. Ruesca (2016) denomina radio enlace a cualquier interconexión entre los terminales de telecomunicaciones efectuados por ondas electromagnéticas (Figura 4). El radioenlace, establecen un concepto de comunicación del tipo dúplex, de donde se deben transmitir dos portadoras moduladas: una para la Transmisión (Tx) y otra para la Recepción (Rx). Al par de frecuencias asignadas para la transmisión y recepción de las señales, se lo denomina radio canal.



Figura 4. Radio Enlace (Fuente: Ruesca, 2016).

El radioenlace de microondas se realiza sólo si existe una línea de vista (LOS), proveen conectividad de una manera practica entre dos o más sitios. En la tabla 2, se muestra las ventajas y desventajas frente al sistema de línea metálica.

Tabla 2.
Ventajas y Desventajas de Radio Enlace

Ventajas	Desventajas
Instalación más rápida y sencilla.	Explotación restringida a tramos con visibilidad directa para los enlaces.
Volumen de inversión generalmente más reducido.	Necesidad de acceso adecuado a las estaciones repetidoras en las que hay que disponer de energía y acondicionamiento para los equipos y servicios de conservación.
Conservación generalmente más económica y de actuación rápida.	Las condiciones atmosféricas pueden ocasionar desvanecimientos intensos y desviaciones del haz, lo que implica utilizar sistemas de diversidad y equipo auxiliar requerida, supone un importante problema en diseño.

Fuente: Elaboración propia

3.6.7. Dispositivos de Red

3.6.7.1 Router. Graziani y Johnson (2008), Diseño Gráfico (2010), Ramírez y Contador (2014), y Wikipedia (2020a) mencionan que un router es un tipo especial de computador, el cual cuenta con los mismos componentes básicos que una computadora estándar de escritorio, tiene una CPU, memoria, bus de sistema y distintas interfaces de entrada/salida (Figura 5).



Figura 5. Representación simbólica de un router (Fuente: Redes Avanzadas Sección 7001, 2020)

La principal función de un router es dirigir los paquetes destinados a redes locales y remotas al determinar la mejor ruta y enviar los paquetes hacia su destino, dicho proceso se denomina “enrutamiento”.

El router usa su tabla de enrutamiento para determinar la mejor ruta y reenviar el paquete. Es así como la tabla de enrutamiento de un router específicamente identifica lo siguiente:

- Red de destino
- Métrica asociada a la red de destino
- Gateway para llegar a la red de destino

Los routers usan protocolos de enrutamiento estático y dinámico para aprender sobre redes remotas y construir sus tablas de enrutamiento.

3.6.7.2 Switch. Wikipedia (2020c) menciona que un switch es un dispositivo de red que conecta de manera eléctrica y lógica otros dispositivos entre sí (Figura 6). Múltiples cables de datos son conectados a un switch para permitir la comunicación entre los diferentes dispositivos de red. Cada dispositivo de red conectado a un switch puede ser identificado mediante una dirección de red (MAC), permitiendo que el switch pueda regular el flujo de tráfico. Esto maximiza la seguridad y la eficiencia de la red.



Figura 6. Representación simbólica de un switch (Fuente: Redes Avanzadas Sección 7001, 2020)

El Switch Ethernet opera en la capa de enlace de datos (capa 2) del modelo OSI³ para crear un dominio de colisión independiente para cada puerto del switch.

3.7. Diseño de la Investigación

3.7.1 Diseño de la red

El diseño de la red privada virtual se basa en un análisis de alternativas de solución, consideraciones, condiciones y limitaciones, para luego de un proceso de implementación obtener la solución propuesta y poder validarla.

Con relación a la red se va a diseñar una red privada virtual local (RPVL) permitiendo interconectar todas las sedes de la empresa Falabella S.A.C sobre la plataforma MPLS de un proveedor de servicios (ISP), cada sede consta de un ancho de banda apropiado a su funcionamiento las cuales están distribuidas de la siguiente manera: sede Data Center 4Mbps, sede Sucursal 4Mbps, sede Administrativa 6Mbps, la sede principal tienda Mall Aventura Plaza 4Mbps y la sede contingencia tienda Mall Aventura plaza 4Mbps, cuya topología será el resultado del análisis de alternativas de solución entre los tres tipos de servicios VPN tales como Servicio Local Private Line, Servicio Red Exclusivo IP y Red Privada Virtual Local, seguidamente a la topología se debe asociar la arquitectura de la red, definiendo el equipamiento de fibra

³ OSI, modelo de interconexión de sistemas abiertos.

óptica y de radio enlace a emplearse y también el equipamiento de networking, así como los equipos de última milla que se van a brindar.

3.7.1.1 Consideraciones de la red privada virtual local. Para la red privada virtual local, se van a tomar las siguientes consideraciones:

- Accesibilidad a la red MPLS del proveedor de internet (ISP)
- La disponibilidad de los enlaces físicos de radioenlace y fibra óptica establecen la disponibilidad del servicio.
- Capacidad suficiente en Mbps para cada sede remota para atender los servicios de transmisión de datos y servicios futuros.

3.7.1.2 Condiciones y restricciones de la red privada virtual local.

- La red privada virtual debe ser escalable
- El servicio de transmisión de datos debe ser utilizado simultáneamente por diversos usuarios de las diferentes sedes de la empresa de manera eficiente, óptima y constante.

3.7.2 Comparación entre alternativas de solución

Como solución al requerimiento de la empresa Falabella S.A.C de interconectar sus sedes a través de la infraestructura del ISP, existen tres servicios que se les puede brindar al cliente, dentro de estas tenemos el servicio Local Private Line, el Servicio Red Exclusivo IP y la Red Privada Virtual Local.

A continuación, se explica y detalla las características, ventajas y desventajas de las posibles soluciones.

3.7.2.1 Servicio Local Private Line. El Servicio Local Private Line (LPL), atendido a través de una plataforma de red SDH/SONET, escalable y de gran capacidad, servicio de clase L1VPN la cual soporta conexiones de enlaces punto a punto en forma transparente y privado entre sus sucursales o sedes de clientes empresariales. El servicio LPL asegura mayor rendimiento debido al uso privado dedicado de líneas. La empresa puede hacer transmisiones de datos, voz y video a través de un enlace de capa 1 dedicado.

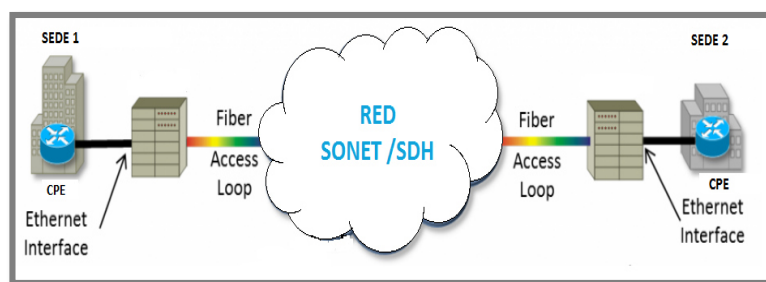


Figura 7. Topología de Servicio Local Private Line (Fuente: Elaboración propia).

3.7.2.2 Servicio de red exclusivo IP. El servicio Red Exclusivo IP (IPLS) se trata de una VPN de tipo VPLS (Virtual Private LAN Services), el cual es una clase L2VPN que permite la conexión de varios sitios dentro de un único dominio sobre una red IP/MPLS gestionada. VPLS presenta una interfaz Ethernet a los usuarios, lo cual simplifica la frontera LAN/WAN para las empresas y proveedores de servicios, permitiendo un aprovisionamiento rápido y flexible de servicios, debido a que el ancho de banda del servicio no está vinculado a la interfaz física.

Como solución del problema planteado se ofrecerá a la empresa Falabella S.AC el servicio RPVL de tal manera que pueda interconectar sus sedes haciendo uso de la infraestructura del ISP.

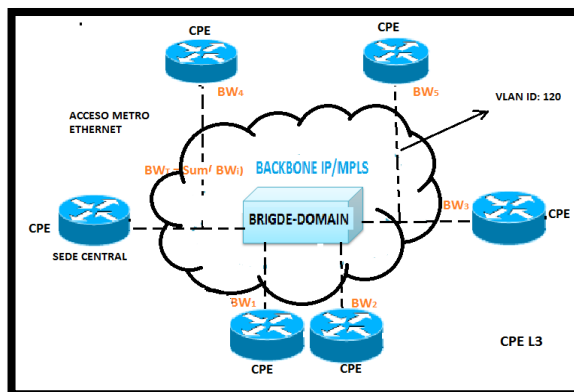


Figura 8. Servicio Red Exclusivo (Fuente: Elaboración propia).

3.7.2.3 Red Privada Virtual Local. El servicio de Red Privada Virtual Local (RPVL) se basa en la tecnología VPN/MPLS la cual crea servicios de clase L3 VPN, gracias a que VPN/MPLS reside en la capa 3 del modelo OSI, se puede proveer servicios de valor agregado a distintos grupos de usuarios dentro de una VPN, proporcionando el transporte para cualquier tipo de información, añadiendo a la interconexión de sedes remotas el establecimiento de niveles de clases de servicio (CoS) diferenciadas, asignando la prioridad adecuada para las aplicaciones de voz, video, datos críticos y datos no críticos. Lo cual asegura que las aplicaciones críticas tengan mayor preferencia en el transporte interno de la red, así como la política de encolamiento diferencial de paquetes para el caso de que ocurra una congestión. Manteniendo el nivel de desempeño que el cliente necesita.

La adición de valor al concepto tradicional de conexiones punto-multipunto que se brindara sobre la tecnología IP/MPLS, se basa en el uso del modelo de topología de red Full-Mesh “todos contra todos”, en donde cada sitio conoce a todo otro sitio de la misma VPN. En la figura 14, se representa la topología del servicio.

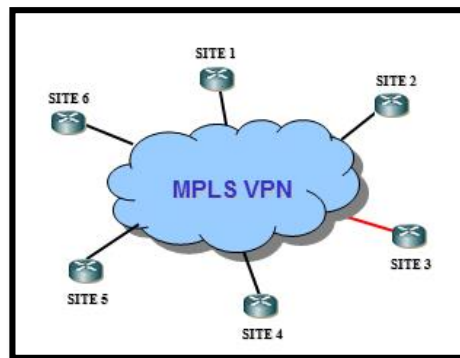


Figura 9. Topología de Servicio Red Privada Virtual Local (Fuente: Elaboración propia).

3.7.3 Elección de la solución

En primera instancia se evaluó, el servicio LPL el cual ofrece un enlace punto a punto, debido a que la empresa requiere interconectar sus cuatro sedes, se tendría que implementar 12 conexiones para lograr la conectividad de sus locales, lo cual es poco escalable y rentable para la empresa en caso quiera aperturar más sucursales en un futuro. Es debido a ello que la elección de la solución se dará entre el servicio IPLS basado en VPLS y el servicio RPVL basado en IP/MPLS VPN.

Por lo cual se realizó un esquema de comparación entre ambos servicios, y eligió la mejor solución a implementar (Tabla 3).

Tabla 3.
Esquema comparativo de IPLS y RPVL

Servicio Red Exclusivo IP	Servicio Red Privada Virtual Local (L3 VPN)
Basado en la tecnología VPLS (L2 VPN).	Basado en la tecnología IP/MPLS (L3 VPN).
Escalable ancho de banda Ethernet, bajo costo de servicios multipunto L2 VPN por parte del ISP	Escalable y fácil adición de nuevas sucursales del cliente
El cliente es responsable total de su red, tanto del direccionamiento como el ámbito de enrutamiento.	La capacidad de soportar estrictos acuerdos de nivel de servicio. Representa una base sólida para el desarrollo posterior de servicios IP/MPLS.

Fuente: Elaboración propia.

Considerando la necesidad de la empresa de hacer posible la comunicación entre todas sus sucursales, y con la particularidad de excluir la comunicación entre sedes del mismo tipo mediante la implementación de enrutamiento WAN el cual es posible con el protocolo BGP, y además priorizar el tipo de tráfico de acuerdo con la importancia u funcionalidad de sus servicios, se procedió a realizar la implementación del servicio RPVL.

3.7.4 Diagrama de red

De acuerdo con la elección de solución al problema planteado, el servicio RPVL permitirá a la empresa Falabella S.A. interconectar todas sus sedes sobre la plataforma MPLS del ISP.

Se tomó las siguientes consideraciones para las sedes de la empresa:

- Se utilizará como PE⁴ los routers Cisco ASR9006 (Cisco, 2017b).
- Se utilizará como equipos de acceso a la red del ISP el switch BlackDiamond 8810 (Extreme, 2014).
- Todos los CPEs del servicio RPV tendrán sesiones eBGP con los Routers situados en las sedes de la empresa (Zamora, 2013).
- Se considerará escenario Activo-Standby bajo un mismo CPE para la sede Tienda Principal de la empresa perteneciente al enlace principal y al de contingencia. No se considera este tipo de escenario para las demás sedes tales como la sede oficina administrativa, sede Data Center y sede sucursal.
- Esquema de contingencia automática (protocolo HSRP y BGP). Se considera router Cisco 2911 (SL-29-DATA-K9) para el enlace principal, así como para el enlace de contingencia (Cisco, 2006; Cisco, s.f.-b).
- La ruta de Enlace principal (Fibra Óptica) es considerada de un PE distinto al del Enlace Contingencia (Radio enlace). Por el enlace de contingencia se pasarán los mismos servicios que en el enlace principal en caso este tenga una caída.
- Se utilizará como routers CPE⁵ ubicados en la sede de la empresa tales como sede administrativa, sede sucursal y sede data center de igual manera el modelo de Router Cisco CISCO2911/K9 (Cisco, 2017a).
- Se creará una “route-map”, para aplicar los prefijos de gestión donde no se incluya los segmentos de los usuarios.
- Se asignará prefijo de gestión para los CPE: 190.24.248.0/24
- La empresa empleara el segmento de Red: 172.24.0.0/16 para su direccionamiento LAN en Lima.

Con este previo estudio, se define el tipo de equipamiento con las características técnicas apropiadas al esquema diseñado. Después de determinar diversas opciones, se decidió optar como conexiones físicas punto

⁴ PE: Provider Edge: Equipo de red de borde del ISP (Proveedor de Servicios).

⁵ CPE: Costumer Premises Equipment, equipo de borde ubicado en la sede del cliente.

a punto la fibra óptica y el radioenlace, los cuales interconectarán cada una de las sedes de la empresa con el equipo de acceso del ISP. En la figura 10, se puede observar cómo queda el diagrama de red final propuesto para la empresa Falabella S.A.

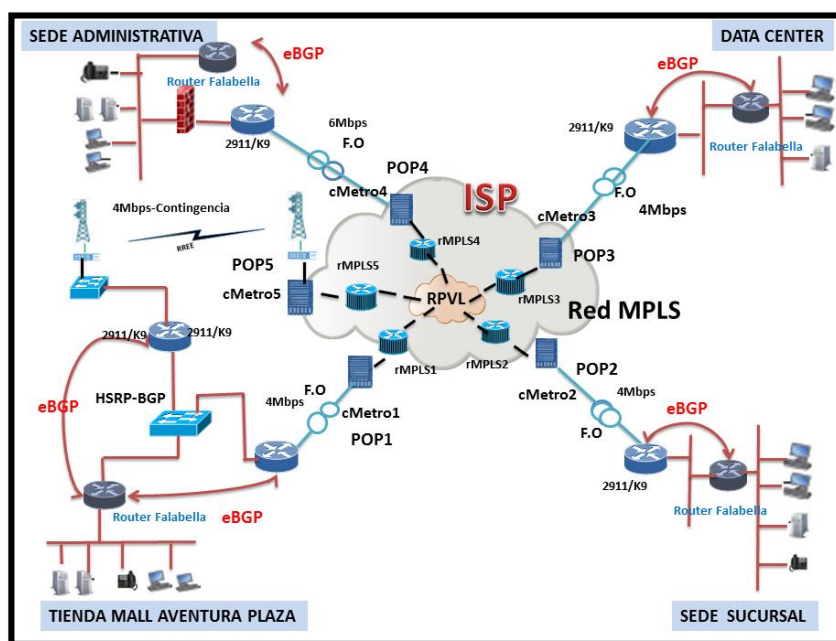


Figura 10. Esquema de Red Propuesto (Fuente: Elaboración propia).

3.7.5 Conexión Física

Para la conexión entre el equipo de acceso del ISP más cercano al local de la empresa y los CPEs, los cuales están ubicados en las sedes, se utilizarán enlaces de fibra óptica para el enlace principal de la sede principal (Tienda Mall Aventura Plaza), la sede administrativa, la sede data center y sede sucursal, y el radioenlace para el enlace de contingencia de la sede principal.

Raisecom (s.f.-b) mencionó que para la instalación del enlace de fibra óptica por sede, se requiere la asignación de un chasis (concentrador iTN 2100) el cual cuenta con diferentes tarjetas de tributarios (Slots), los cuales están compuestos a su vez por puertos, es desde el slot donde se realiza el

tendido de fibra óptica con conector SFP hacia el equipo Media Converter, ubicado en la sede de la empresa, este dispositivo transceptor flexible está destinado a implementar y optimizar los enlaces de fibra por lo cual funciona como un conversor de la señal de luz a eléctrica la cual es transportada a través de cable UTP y de tal manera recepcionada por el CP⁶.

En cuanto a la instalación del radioenlace para el enlace de contingencia de la sede principal. Se requiere la asignación de un puerto Ethernet del Switch de acceso de la red del ISP (BlackDiamond 8810), puerto desde donde se realiza la conexión de cable UTP hacia la radio lado Nodo, dispositivo que tiene la capacidad de comunicación dúplex, teniendo en cuenta la importancia de establecer un enlace con una altura libre de obstáculos, adecuada para la propagación de la señal en toda la época del año. Por consiguiente, se realiza la selección de un puerto Ethernet ubicado en la radio lado cliente, la conexión se da por medio del cable UTP con terminación RJ-45 hacia el CP.

3.7.5.1 Equipos principales para el enlace de Fibra Óptica

3.7.5.1.1 Concentrador ITN 2100. Raisecom (s.f.-a) mencionó que El ITN2100, es una plataforma modular PTN7 (Packet Transport Network) de alta capacidad con 15 Slots, la cual se caracteriza por presentar una arquitectura de núcleo y red dual por entregar el tráfico a través de Ethernet y TDM.

Esta tecnología soporta redundancia completa de hardware y proporciona una amplia capacidad de gestión, soporta los protocolos de operación, administración y mantenimiento (OAM), a través de su interfaz gráfica en el Sistema de Gestión de Red (NMS), brindándose de esta manera un monitoreo del servicio de extremo a extremo, así como el troubleshooting del servicio. Por lo tanto, la calidad de la red y servicio (QoS) son medibles y estimables. Tanto las características se encuentran en la tabla 4.

⁶ CP: Customer Premise (equipo en sede de cliente)

⁷ PTN: Packet Transport Network (red de transporte de paquetes)



Figura 11. Concentrador iTN2100 (Fuente: Raisecom, s.f.-a)

Tabla 4.
Características iTN2100

Estructura	Características
Distribución Slot	✓ Totalidad de 15 slots ✓ 1 para módulo NMS ✓ 2 para módulo de Poder ✓ 2 para módulo uplink 10 G/GE ✓ 8 o 10 para los módulos tributarios
Características IP	✓ Soporta QoS. ✓ Lista de control de Acceso (ACLs).
Característica de Administración	✓ Telnet/CLI/SNMP (v1, v2, v3). ✓ Soporta Protocolo RIP. ✓ Gestión de Extremo a Extremo.

Fuente: Modificado de Raisecom, s.f.-a

En cuanto a la estructura del concentrador ITN2100 está compuesto de un chasis, fans, fuentes de poder, tarjetas, y cables. A continuación, se muestra la relación entre slots y tarjetas en la figura 12

RC552-FE (B). Son conversores de medios a nivel operador, diseñado para escenarios de acceso empresarial, tiene una gran capacidad de reenvío de paquetes de gran alcance, esta serie es compatible con los escenarios punto a punto y punto a multipunto. Instalado en el Chasis ITN2100, este dispositivo es compatible con la gestión Web, facilitando la localización de averías y mantenimiento remoto. Todas las características de la RC552-FE se encuentran en la tabla 5.

Tabla 5.
Características RC552-FE

Características	Descripción
Puerto Lado Cliente	10/100Mbps auto negociación, RJ-45 Conector
Puerto Lado Nodo	SFP slots para 100M fibra óptica SFP conector, LC, 1:1 protección uplink
Opciones de Fibra Óptica	Modo Monomodo/Multimodo, fibra de doble hebra, Modo Monomodo, Fibra de una sola hebra
Distancia de Transmisión	Fibra de doble hebra: 0-120km, Fibra de una sola hebra: 0-100km

Fuente: Modificado de Raisecom, s.f.-c

A continuación, en tabla 6 se detalla el nivel de potencia para las tarjetas media converter.

Tabla 6.

Tabla de Potencias para tarjeta Media Converter

Lado POP	Longitud de Onda	Modo	Distancia	Pt x min	Pt x Max	Pr x min	Tipo	Servicio	Lado Cliente
ITN2 101	1310	monomodo	0-25 km	- 15	- 8	- 33	dúplex	datos	RC5 52-FE-B
ITN2 102	1310	monomodo	10-60 km	- 5	- 0	- 33	dúplex	datos	RC5 52-FE-B
ITN2 103	1550/1310	monomodo	0-25 km	- 12	- 3	- 30	simplex	datos	RC5 52-FE-B
ITN2 104	1550/1310	monomodo	10-50 km	- 5	- 0	- 32	simplex	datos	RC5 52-FE-B

Fuente: Elaboración propia

A continuacion se muestra en la figura 14, la interconexion fisica entre los equipos del enlace de fibra optica.

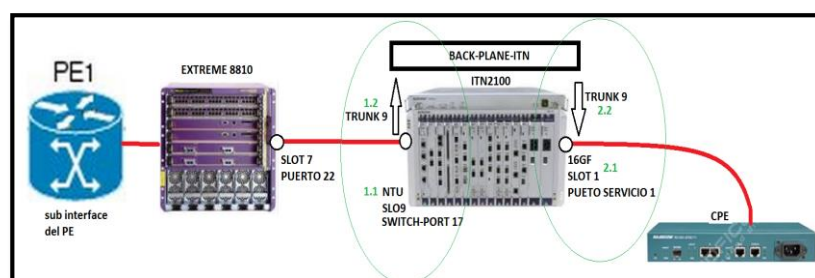


Figura 14. Interconexión física de equipos del enlace Fibra Óptica (Fuente: Elaboración propia)

3.7.5.2 Equipos principales para el Radio Enlace

3.7.5.2.1 FibeAir IP-10 Ceragon. Radio IP-10 constituye una solución de red IP completa de alta capacidad de Ceragon, fue diseñado como una plataforma de radio de microondas Ethernet Nativo. IP-10 permite un ancho de banda flexible que comparten entre tráfico TDM y Ethernet asegurando la tasa de transferencia óptima para todas las necesidades de transmisión de sus medios de comunicación (Figura 15).

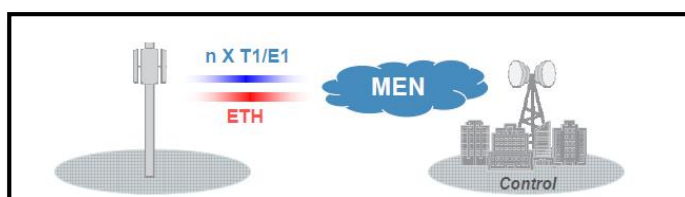


Figura 15. Comunicación de IP-10 Ceragon en una red Ethernet Metropolitana (Fuente: Ceragon Networks, 2008)

Algunos de los puntos que colocan al IP-10 por encima de las redes IP inalámbricas son:

- La más alta eficiencia Espectral
- Soporta todas las bandas licenciadas, desde 6 a 38 GHz.
- La capacidad del equipo soporta anchos de banda de canales desde 7 MHz a 56 MHz.
- Brinda la más alta escalabilidad, soporta tasas de transferencia desde 10 a 500 Mb/s.
- Emplea el Código y Modulación Adaptativo (ACM).

3.7.5.2.2 IDU. El panel Frontal IDU (Figura 16, Tabla 7) está conformado por las siguientes interfaces auxiliares: Consola terminal, Canal de servicio, Canal de usuario y alarmas externas.

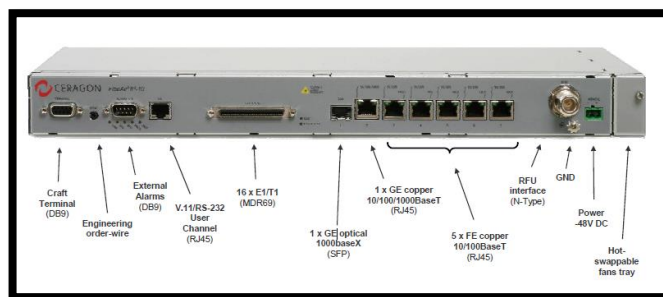


Figura 16. Panel Frontal IDU (Fuente: Ceragon Networks, 2008)

Tabla 7.
Resumen de detalles del Sistema IDU

Sistema IDU	Detalle
Arquitectura	Split-mount (IDU y RFU/ODU)
Compatibilidad	Todos los Ceragon RFUs/ODU existentes
Voltaje nominal de entrada CD	-48V
Interfaces de tráfico por cada IDU IP-10	1 x 10/100/1000Base-T SFP 1000Base-X 16 x T1/E1 (opcional) RFU/ODU, conector tipo N

Fuente: Ceragon Networks, 2008

Ceragon provee gestión con tecnología de punta basada en SNMP y HTTP, permite al operador que realice la configuración del elemento, monitoreo del funcionamiento RF, Ethernet y PDH, diagnósticos remotos e información de alarmas. Cuenta con un sistema de administración de redes de Ceragon PolyView.

3.7.5.2.3 FiberAir RFU-C. FiberAir IP-10 es instalado junto con el RFU y ODU FiberAir, para este caso se utilizó el FiberAir RFU-C (Figura 17). RFU FiberAir soporta múltiples capacidades y configuraciones para varios requerimientos de red. El RFU opera en los rangos de frecuencia de 6-38 GHz, y soportan capacidades de 10 Mb/s a 500 Mb/s, tanto

para interfaces TDM y IP. En la tabla 8, se brindará un resumen del sistema IDU.



Figura 17. FibeAir RFU-C (Fuente: Ceragon Networks, 2011)

Tabla 8.
Resumen de las especificaciones del Sistema IDU

Especificación	23 GHz	24-26 GHz	28 GHz	32 GHz	38 GHz
Estándar	ETSI, FCC	ETSI, FCC	ETSI, FCC	ETSI, FCC	ETS I, FC C
Rango de Frecuencia de Operación (GHz)	21.2- 23.65	24.2- 26.5	27.35- 31.3	31.8- 33.4	37- 40
Selección de Canal de RF	Vía EMS/NMS				
Rango de TX (Manual/ ATPC)	Rango dinámico 20dB				

Fuente: Ceragon Networks, 2008

En la tabla 9, se brindará las especificaciones de la Capacidad de Radio.

Tabla 9.
Especificaciones de la Capacidad de Radio

Nivel de Operación	Modulación	Capacidad mínima de la licencia requerida	Numero de E1s soportados	Tasa de Transferencia Ethernet	
				Min	Max
1	8 QPSK	25	6	14	20
2	16 QAM	25	8	20	28
3	32 QAM	25	10	23	34
4	64 QAM	25	12	28	40
5	128 QAM	50	13	33	47
6	256 QAM	50	16	38	55

Fuente: Ceragon Networks, 2008

En la tabla 10, se brindará las potencias de la transmisión con RFU-C

Tabla 10.
Potencia de Transmisión con RFU-C (dBm)

Modulación	6 GHz	7-8 GHz	11-15 GHz	18 GHz	23-28 GHz	32-38 GHz
16 QAM	26	25	23	21	21	18
32 QAM	25	24	22	20	20	17
64 QAM	25	24	22	20	20	17
128 QAM	25	24	22	20	20	17
256 QAM	23	22	20	18	18	15

Fuente: Ceragon Networks, 2008

En la tabla 11, se brindaras las características de Interfaces Ethernet IP-10.

Tabla 11.
Interfaces Ethernet IP-10

Interfaces Ethernet IP-10	
Interfaces Ethernet Soportadas	5 x 10/100base-T (RJ45) 1 x 10/100/1000Base-T (RJ45) 1 x 1000base-X (SFP)
Tipo de SFP soportadas	1000Base-LX (1310 nm) o SX (850 nm) o 1000base-T

Fuente: Ceragon Networks, 2008

A continuacion se muestra en la figura 18 la interconexion fisica entre los equipos del Radio Enlace.

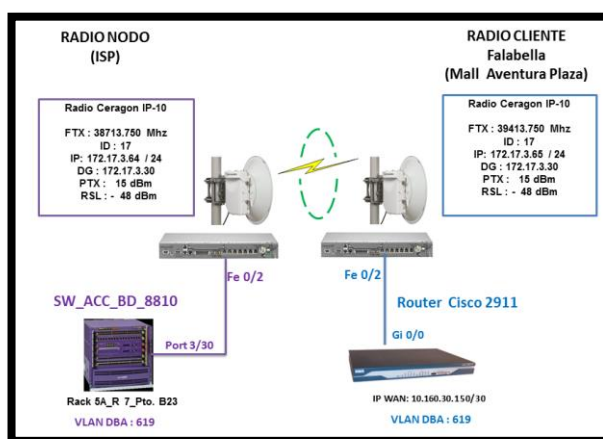


Figura 18. Interconexion Fisica de los equipos de Radio Enlace (Fuente: Elaboración propia)

Ventajas

- Integración de tráfico Usuario-Administración, reducción de capex y opex. Mejora considerablemente la disponibilidad de la red y la fiabilidad.

- Funcionalidad de integración complementaria integrada L2 Ethernet, conmutación basada VLAN.
- Soporta topología de Redes Múltiples, tales como Malla, Anillo, Cadena, Punto a Punto.

A continuación, se detallará estas conexiones físicas para cada sede.

3.7.5.3 Sede Oficinas Administrativas

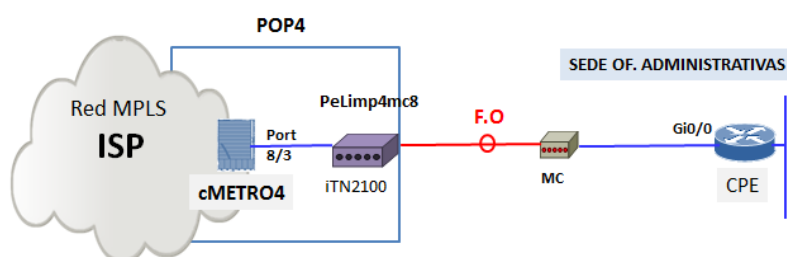


Figura 19. Enlace físico entre la sede administrativa y el equipo de acceso a la red (Fuente: Elaboración propia)

Observaciones generales

Se considera la habilitación del enlace de última milla para el servicio en la sede, RPVL Acceso 6 Mbps, desde el equipo de acceso del ISP hasta el punto de conexión previo al equipo de Acceso a la red LAN de la sede (Figura 19):

Se realiza el tendido de jumper de fibra SM simplex con terminación en conector SC hacia un rack. Para la conexión entre el MC y el Equipo de Acceso se utiliza cableado Ethernet categoría cat6 marca Panduit.

Características del enlace de Fibra Óptica

- Tipo: Monofibra
- Modo: Monomodo
- Distancia: 1512 mts

- Atenuación: F38 = 0.52 dB
- Modelo de equipo MC en Cliente: RC552-FE-B
- Modelo de equipo en POP: INT2100
- Ubicación y estado de la tarjeta MC en el POP 4 (Figura 20).
- Nombre del chasis y ubicación de la tarjeta: PeLimp4mc8 Slot 01 Puerto 14
- **PeLimp4mc8**, Pe=Perú, Lim=Lim, p=POP, 4=POP 4, mc=Media Converter, 8 =chasis 8

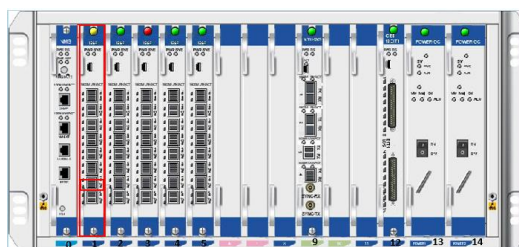


Figura 20. Ubicación de la Tarjeta MC en el POP 4 (Fuente: Elaboración propia)

3.7.5.4 Sede Data Center

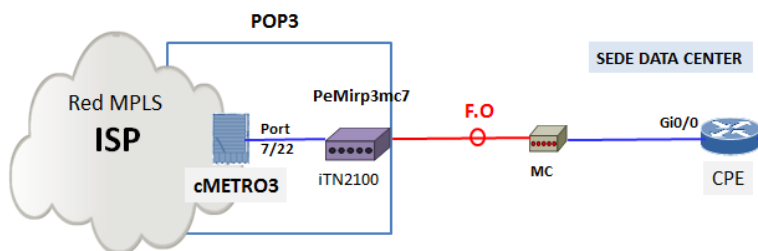


Figura 21. Enlace físico entre la sede Data Center y el equipo de acceso a la red (Fuente: Elaboración propia)

Observaciones Generales

Se considera la habilitación del enlace de última milla para el servicio en la sede, RPVL Acceso 4 Mbps, desde el equipo de acceso del ISP

hasta el punto de conexión previo a equipos de Acceso a la red LAN de la sede (Figura 21).

Para la conexión entre el MC y el Equipo de Acceso se utiliza cableado Ethernet categoría cat6. Así como se realiza el tendido de jumper de fibra SM simplex con terminación en conector SC hacia un rack.

Características del enlace de Fibra Óptica

- Tipo: Monofibra
- Modo: Monomodo
- Distancia: 8365 mts
- Atenuación: F32=2.85 dB
- Modelo de equipo MC en Cliente: RC552-FE-B
- Modelo de equipo en POP: iTN2100
- Ubicación y estado de la tarjeta MC en el POP 3 (Figura 22).
- Nombre del chasis y ubicación de la tarjeta: Pemirp3mc7 Slot 3 Puerto 4
- PeMirp3mc7, Pe=Perú, Mir=Miraflores, p=POP, 3=POP 3, mc=Media Converter, 7 =chasis 7



Figura 22. Ubicación de la Tarjeta MC en el POP 3 Fuente: Elaboración propia)

3.7.5.5 Sede Sucursal

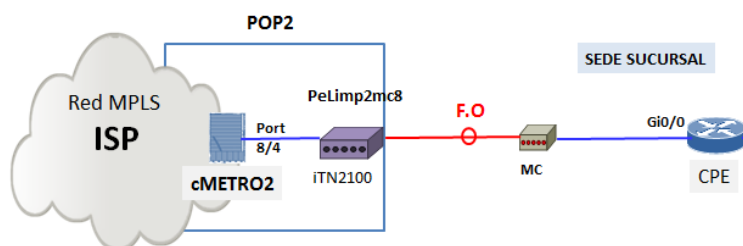


Figura 23. Enlace físico entre la sede sucursal y el equipo de acceso a la red
Fuente: Elaboración propia)

Observaciones generales

Se considera la habilitación del enlace de última milla para el servicio en la sede, RPVL Acceso 4 Mbps, desde el equipo de acceso del ISP hasta el punto de conexión previo al equipo de Acceso a la red LAN de la sede (Figura 23).

Se realiza el tendido de jumper de fibra SM simplex con terminación en conector SC hacia un rack. Para la conexión entre el MC y el Equipo de Acceso se utiliza cableado Ethernet categoría cat6 marca Panduit.

Características del enlace de Fibra Óptica

- Tipo: Monofibra
- Modo: Monomodo
- Distancia: 1512 mts
- Atenuación: F38 = 0.52 dB
- Modelo de equipo MC en Cliente: RC552-FE-B
- Modelo de equipo en el POP: iTN2100
- Ubicación y estado de la tarjeta MC en el POP 2 (Figura 24).
- Nombre del chasis y ubicación de la tarjeta: PeLimp2mc8 Slot 01 Puerto 14

- PeLimp2mc8, Pe=Perú, Lim=Lim, p=POP, 2=POP 2, mc=Media Converter, 8 =chasis 8



Figura 24. Ubicación de la Tarjeta MC en el POP 2 Fuente: Elaboración propia)

3.7.5.6 Sede Mall Aventura Plaza, Enlace Principal y Contingencia

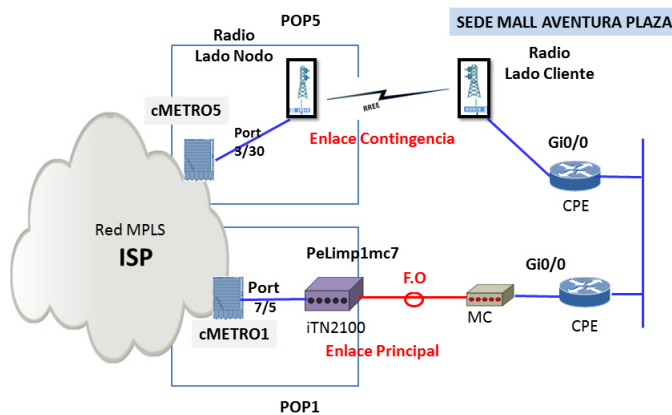


Figura 25. Enlace físico entre la sede Principal y el equipo de acceso a la red Fuente: Elaboración propia)

Observaciones generales

En el Proyecto se considera la habilitación de los enlaces de última milla desde los equipos de acceso del ISP en el POP1 para el enlace principal y en el POP 5 para el enlace de contingencia, para el servicio en la sede. Ambos enlaces se realizan hasta el punto de conexión previo al Equipo de Acceso a la red LAN de la sede, debido a la implementación de dos diferentes medios de transporte, por el cual se atenderá la sede Principal, se considerará CPEs distintos para ambos enlaces (Figura 25).

La conexión de los routers CPE se realiza hacia un Switch Catalyst del cliente, el cual está ubicado en su rack de comunicaciones. De igual manera se considera el cableado UTP categoría cat6.

Para el enlace principal el cual se da por medio del Enlace Óptico, se realiza el tendido de jumper de fibra SM simplex con terminación conector SC hacia un rack. Para la conexión entre el MC y el Equipo de Acceso a la red LAN del cliente se utiliza cableado Ethernet categoría cat6 marca Panduit.

Para el enlace de contingencia el cual se da por medio de Radio Enlace, se realiza el tendido de conexión UTP con terminación RJ-45 desde el equipo de Acceso del ISP hacia la radio lado nodo y de manera análoga se realiza la conexión UTP con terminación RJ-45 desde la radio lado cliente hacia el CP de la sede.

RPVL Acceso de 4 Mbps, desde el equipo de acceso del ISP hasta el punto de conexión previo al equipo de Acceso a la red LAN de la sede.

Características del enlace de Fibra Óptica Principal

- Tipo: Simplex
- Modo: Monomodo
- Distancia: 5096 m
- Atenuación: F37 = 1.73 dB
- Modelo de equipo MC en Cliente: RC552-FE-B
- Modelo de equipo en el POP: iTN2100
- Ubicación y estado de la tarjeta MC en el POP 1 (Figura 26).
- Nombre del chasis y ubicación de la tarjeta: PeLimp1mc06 Slot 05 Puerto 4
- **Pe**L**imp**1**mc**6, **Pe**=Perú, **Lim**=Lim, **p**=POP, **1**=POP 1, **mc**=Media Converter, **6**=chasis 6



Figura 26. Ubicación de la Tarjeta MC en el POP 1 Fuente: Elaboración propia)

Características del Radio Enlace de Contingencia

- Tipo: Dúplex
- Longitud de enlace: 4.5 Km
- Parámetros Radio Lado Nodo
- FTx: 38713.750 Mhz
- PTx: 15 dBm
- RSL: - 48 dBm
- Parámetros Radio Lado Cliente
- FTx: 39413.750 Mhz

- PTx: 15 dBm
- RSL: - 48 dBm
- Modelo de Equipos en POP: IDU Ceragon IP-10, RFU 38 GHz, Antena Ceragon.
 - Modelo de Equipos en Cliente: IDU Ceragon IP-10, RFU 39 GHz, Antena Ceragon, UPS APC Pro1200, Fuente de Alimentación 240-48 Mean Wells, 80 m de cable coaxial y tierra.

En la figura 27 y 28, se brindará la ubicación de interfaces del Radio Lado Nodo y lado cliente respectivamente.

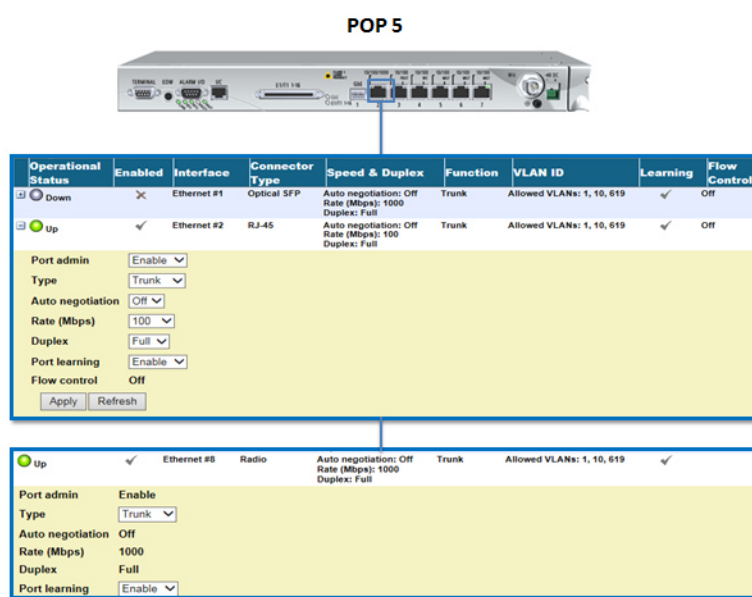


Figura 27. Ubicación de Interfaz en IDU de Radio Lado Nodo Fuente:
(Elaboración propia)

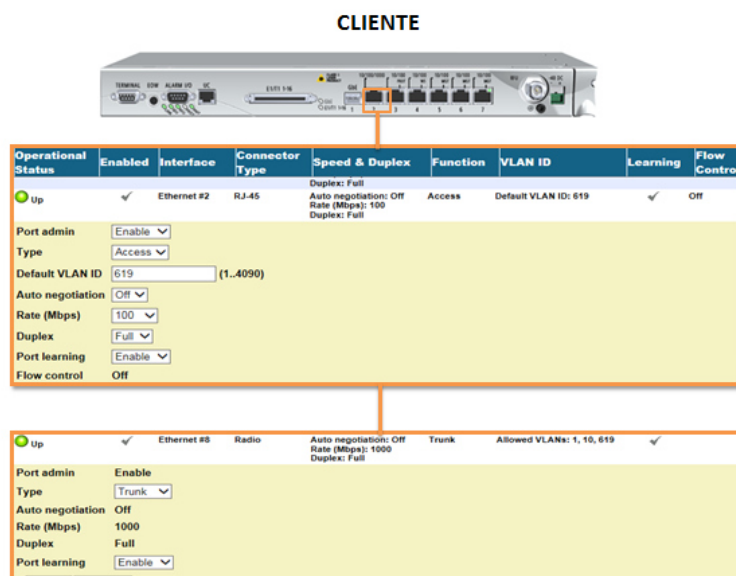


Figura 28. Ubicación de Interfaz en IDU de Radio Lado Cliente Fuente: Elaboración propia)

3.7.5.7 Visualización del Media Converter

En el Concentrador iTN2100

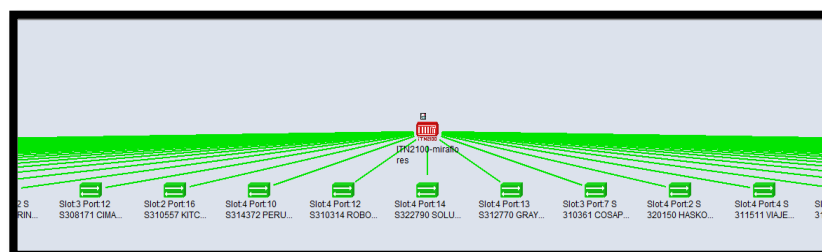


Figura 29. Topología de Interconexión entre iTN2100 y Media Converter Fuente: Elaboración propia)

Para el correcto funcionamiento del servicio los puertos tanto ópticos como Ethernet deben estar en estado UP y establecido en full dúplex y con las correctas velocidades, consideramos la velocidad en ambos extremos a 100 Mbps (Figura 29 y 30).

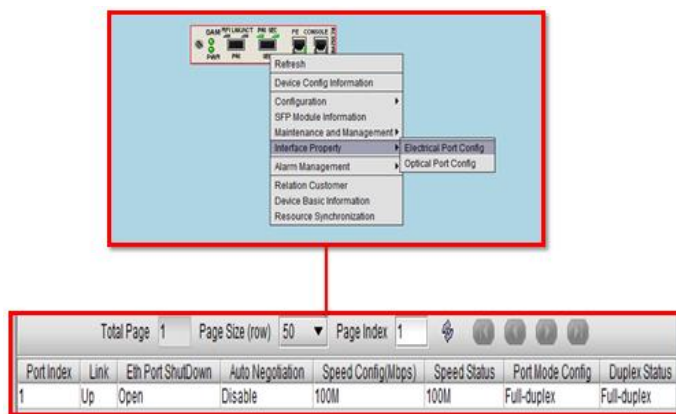


Figura 30. Estado de Media Converter RC552-FE-B Fuente: Elaboración propia)

3.7.6 Asignación de Recursos Lógicos en la red IP/MPLS

Dado que se procedió a desarrollar un servicio de RPVL basada en la tecnología VPN L3/MPLS, se realizó la asignación de recursos lógicos para cada sede de la empresa. Los recursos para asignar por sede son los siguientes:

- VLAN: Se asignó una VLAN (Virtual Local Access Network) por sede, de tal manera que se forme una red lógica independiente por cada sede de la empresa dentro de la misma red física.
- Subinterfaz del PE: Utilizaremos una subinterfaz para cada sede de la empresa, la cual estará encapsulada dentro de la VLAN.
- VRF (Virtual Routing and Forwarding): La VRF incluye las tablas de envío y encaminamiento de las sedes pertenecientes a una misma VPN. La VRF es única para todas las sedes de la misma empresa, dicha empresas está compartiendo una misma infraestructura de ISP.

- IP WAN: Se asignó un segmento de IPs privadas de clase A con mascarará /30, el cual se forma entre la subinterfaz del PE y CPE.
- IP de Gestión: Se asignó una IP de gestión para cada sede, con la finalidad de poder habilitar la administración remota.
- Password BGP: Dado que BGP es el protocolo para el enrutamiento, se asignará una contraseña para establecer la vecindad entre el equipo de capa 3 del ISP y CPE.

3.7.6.1 Sede de oficinas administrativas

- Acceso: cMETRO4 Port 7/20
- VLAN: 541
- PE: rMPLS4 TenGigE0/3/0/18.541
- VRF: INF-FALABELLA
- IP WAN: 10.160.80.146/30
- IP DG: 10.160.80.145/30
- IP ADM: 190.24.248.32/32
- Password BGP f414B3114\$ (único para todas las sedes del cliente)

En la figura 31, se mostrará la topología de red para la sede de oficinas administrativas.

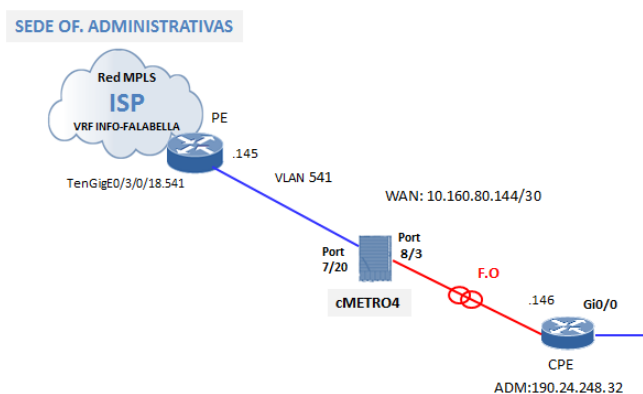


Figura 31. Topología de red para la sede Of. Administrativas Fuente:
Elaboración propia)

3.7.6.2 Sede Data Center

- Acceso: cMETRO3 Port 8/5
- VLAN: 715
- PE: rMPLS3 TenGigE0/3/0/18.715
- VRF: INF-FALABELLA
- IP WAN: 10.140.1.222/30
- IP DG: 10.140.1.221/30
- IP ADM: 190.24.248.81/32
- Password BGP f414B3114\$ (único para todas las sedes del cliente)

En la figura 32, se mostrará la topología de red para la sede Data Center.

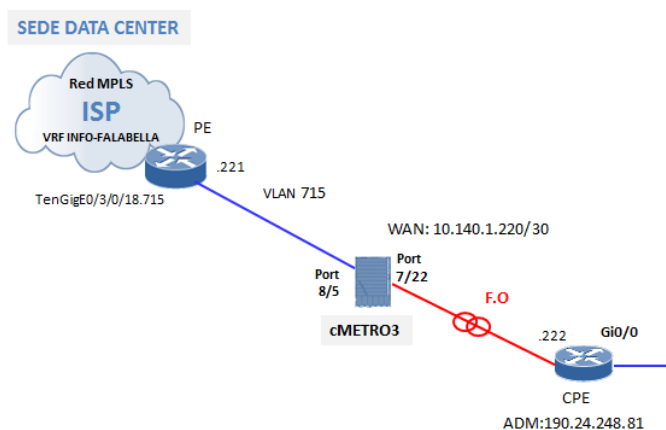


Figura 32. Topología de red para la sede Data Center Fuente: Elaboración propia)

3.7.6.3 Sede Sucursal

- Acceso: cMETRO2 Port 7/21
- VLAN: 618
- PE: rMPLS2 Bundle-Ether1.618
- VRF: INF-FALABELLA
- IP WAN: 10.150.30.146/30
- IP DG: 10.150.30.145/30
- IP ADM: 190.24.248.22/32
- Password BGP f414B3114\$ (único para todas las sedes del cliente)

En la figura 33, se mostrará la topología de red para la sede Sucursal.

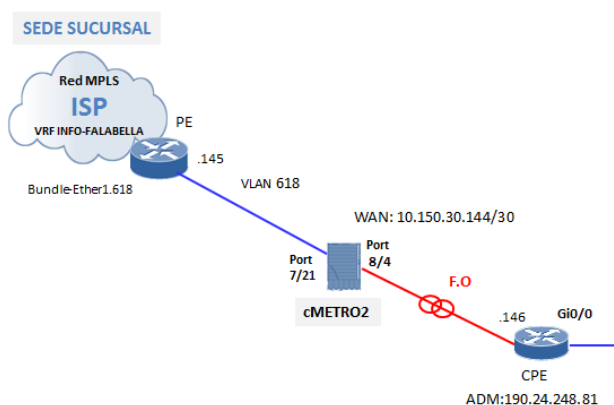


Figura 33. Topología de red para la sede Sucursal Fuente: Elaboración propia)

3.7.6.4. Sede Mall Aventura Plaza, Enlace Principal y Contingencia.

Enlace principal

- Acceso: cMETRO1 Port 7/20
- VLAN: 428
- PE: rMPLS1 Bundle-Ether1.428
- VRF: INF-FALABELLA
- IP WAN: 10.130.30.74/30
- IP DG: 10.130.30.73/30
- IP ADM: 190.24.248.15/32
- Password BGP f414B3114\$ (único para todas las sedes del cliente)

En la figura 34, se mostrará la topología de red para la sede Mall Aventura Plaza.

Enlace Principal

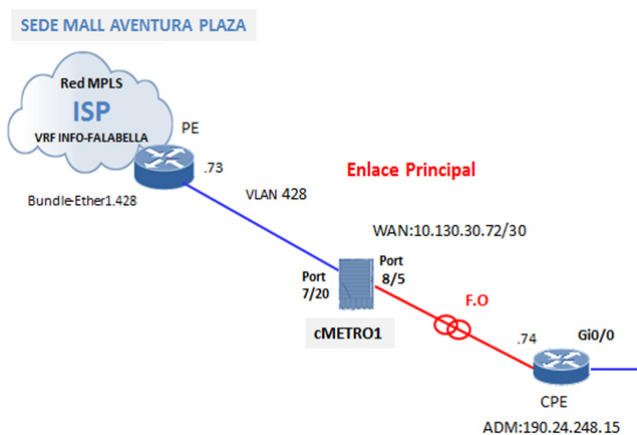


Figura 34. Topología de red para la sede Mall Aventura Plaza-Enlace Principal Fuente: Elaboración propia)

Enlace Contingencia

- Acceso: cMETRO5 Port 7/20
- VLAN: 649
- PE: rMPLS5 TenGigE0/3/0/18.649
- VRF: INF-FALABELLA
- IP WAN: 10.170.80.118/30
- IP DG: 10.170.80.117/30
- IP ADM: 190.24.248.10/32
- Password BGP f414B3114\$ (único para todas las sedes del cliente)

En la figura 35, se mostrará la topología de red para la sede Mall Aventura Plaza-Enlace Contingencia.

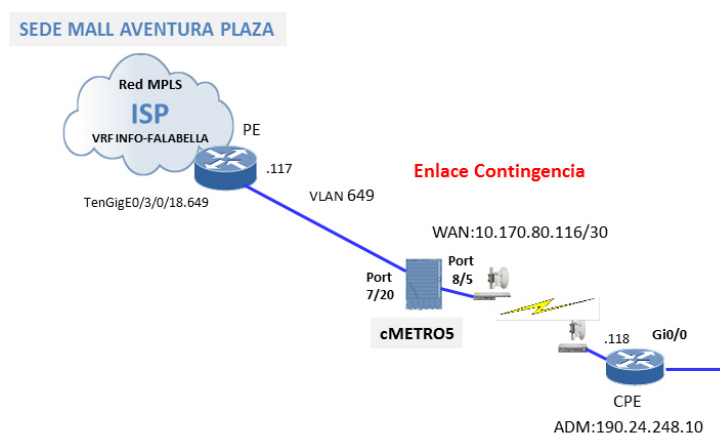


Figura 35. Topología de red para la sede Mall Aventura Plaza-Enlace Contingencia Fuente: Elaboración propia)

3.7.7 Configuración de MPLS VPN

Protocolos de enrutamiento

Para entender el funcionamiento de una red MPLS VPN, es importante conocer los siguientes términos:

- P: Router interno del proveedor
- PE: Router frontera del proveedor
- CE: Router frontera de la empresa que solicita el servicio
- Sitio: Intranets de los clientes, los cuales están separados físicamente pero lógicamente unidos vía una VPN.

En la figura 36, se muestra la topología de equipos que intervienen en el enrutamiento, los cuales hacen posible la comunicación entre las sedes de la empresa.

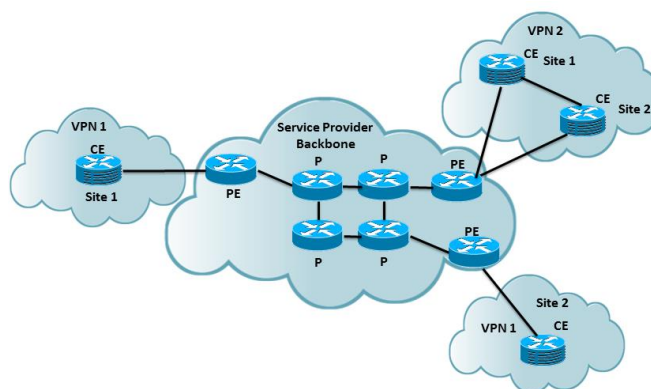


Figura 36. Topología de equipos de red para enrutamiento Fuente:
Elaboración propia)

El servicio ofrecido para los usuarios finales es posible gracias a los protocolos de enrutamiento, es debido a ello que se procede a clasificar el proceso de enrutamiento de la siguiente manera:

3.7.7.1 Proceso de enrutamiento entre P-PE y PE-PE. Cisco (2007) menciona que para la implementación de la red MPLS/VPN, los PEs y Ps comparten el IGP y para armar sesiones entre los PEs se utiliza el protocolo MP BGP Interno, el cual informa sobre los sitios y VPNs conectadas a dichos PEs.

De esta manera la conectividad entre las empresas se logra con la exportación e importación de los valores correctos para Router Targets⁸(RT), los cuales son distribuidos por las actualizaciones BGP. De manera consecuente los prefijos son exportados de una VRF⁹ local a la sesión MP-BGP e importados dentro de las VRFs remotas.

Se utiliza el concepto de VRF, para evitar que los prefijos de una empresa sean recibidos por otros clientes, de tal manera se crea una tabla de ruteo en cada PE propio de la empresa (Figura 37)

⁸ Router Targets: Ruta Objetivo, cada PE define un valor numérico llamado RT, el cual está asociado con la importación y exportación de rutas.

⁹ VRF: VPN Routing and Forwarding.

Estos prefijos son exportados hacia los demás PE con el route target (RT) “19180:577” de exportación, e importadas en los demás PE con el RT “19180:577” de importación, ya que deben contar con el mismo route target.

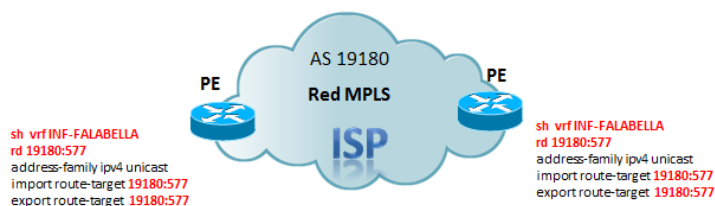


Figura 37. Indicadores de VRF para importación y exportación de rutas
Fuente: Elaboración propia)

En cuanto a la configuración BGP, procedemos a crear el address-family para la VRF de la empresa (INF-FALABELLA), donde se indica la redistribución de los segmentos conectados directamente y las rutas estáticas que se configuren (Figura 38).

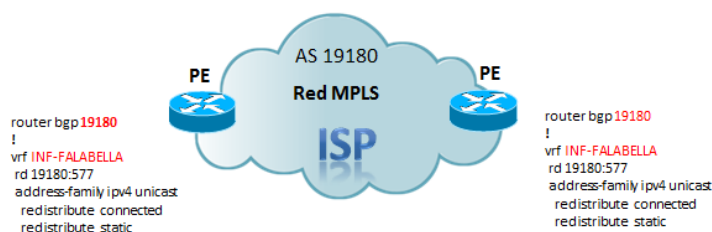


Figura 38. Redistribución de rutas conectadas y estáticas Fuente:
Elaboración propia)

Finalmente procedemos a verificar como los prefijos enviados desde el CPE hacia su PE correspondiente, son exportados hacia los demás PE y de manera consecuente ser advertidos a las demás sedes (Figura 39).

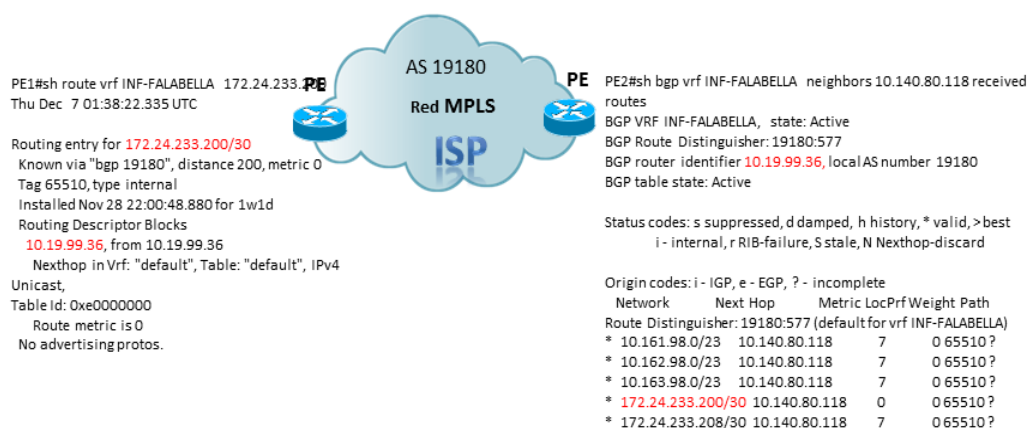


Figura 39. Verificación de la propagación de prefijos entre PE Fuente:
Elaboración propia)

3.7.7.2 Proceso de enrutamiento PE-CPE. Este proceso de enrutamiento nos permite la comunicación entre la red del ISP y las redes de la empresa, para cumplir con ello haremos uso de los protocolos de enrutamiento estático y dinámico (BGPv4), a continuación, se detalla el funcionamiento de cada uno de ellos:

a) Enrutamiento Estático

- Todos los sitios de la empresa tienen un solo acceso a la red del ISP, dicho enrutamiento soporta una menor capacidad de prefijos.
- Para este caso, se debe configurar únicamente una ruta por default (0.0.0.0/0) desde el PE hacia la sede principal del cliente, así mismo debe configurarse una ruta por default (0.0.0.0/0) desde el CPE hacia el equipo PE.

- Los PE tienen la tarea de incorporar los prefijos a la tabla BGPv4, por medio de la distribución de redes estáticas y conectadas.

b) Enrutamiento Dinámico BGPv4

- Utilizado para los sitios de la empresa con dos o más enlaces de acceso a la red del ISP, dicho enrutamiento soporta una mayor capacidad de prefijos.
- Utilizaremos el comando Network de BGP para anunciar las redes de las empresas desde el equipo CPE, equipo local del cliente.
- Soporta más de 15 prefijos en cada sesión BGP determinados para cada sede de la empresa. Para el caso futuro de un incremento de rutas, estas serán evaluadas previamente a su implementación.
- Utilizaremos el atributo de BGP llamado Local Preference¹⁰, el cual determina la ruta principal y de backup en comunidades BGP.
- De acuerdo con el tipo de solución que se le brinda a la empresa, donde su sede principal está respaldada por un enlace principal y de contingencia, y contar con un apropiado soporte al crecimiento futuro de la red de la empresa, el cual pronostica 12 sedes en los próximos dos años, son motivos suficientes para considerar el enrutamiento dinámico BGPv4 como el apropiado.
- Entre el equipo PE y CPE, se establecen la sesión eBGP, por lo cual el CPE anuncia los prefijos de la sede a través del comando Network, a continuación, se indica el procedimiento:
- En primer lugar, se da establecimiento de la sesión eBGP entre el CPE y PE utilizando los comandos expuestos en la parte inferior de cada router. Se usa el Sistema Autónomo (AS) 65510 para el

¹⁰ Local Preference: Atributo BGP enviado entre peers IBGP dentro del mismo sistema autónomo local, determina cual es la salida preferida en el sistema autónomo.

CPE, y el AS 19180 para el ISP. A continuación, se muestra en la figura 40.

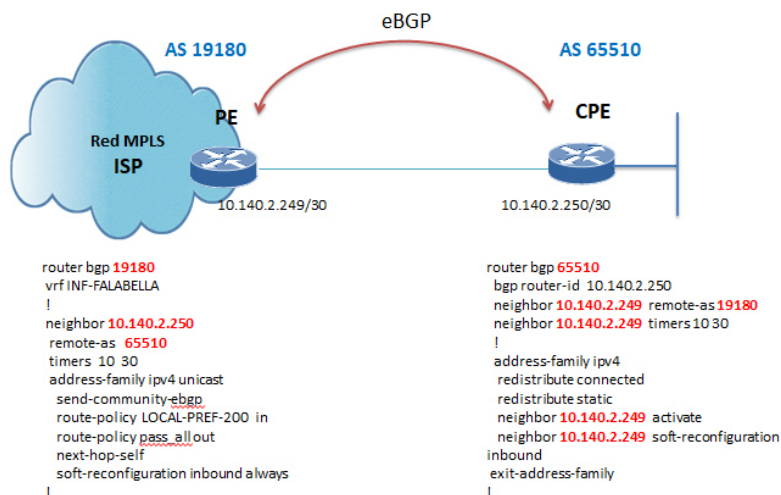


Figura 40. Establecimiento de la sesión BGP entre PE y CPE Fuente: Elaboración propia)

Posteriormente el PE realiza la función de aprehender los prefijos deseados, los cuales son anunciados por el CPE y que posteriormente serán redistribuidos a través de la red MPLS (Figura 41).

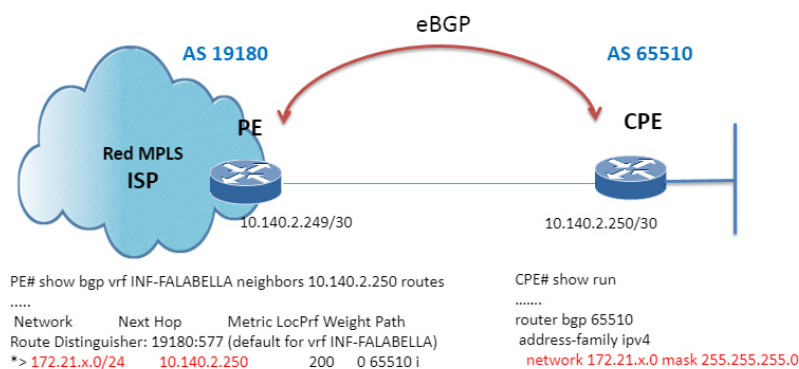


Figura 41. Anuncio de prefijos hacia la red MPLS del ISP Fuente: Elaboración propia)

3.7.7.3 Proceso de enrutamiento en el CPE – Red interna del Cliente. Se utilizó un protocolo de enrutamiento para la red interna de la empresa, el cual no debe redistribuirse al proceso BGPv4 utilizado para la comunicación con los equipos PE.

Los protocolos de enrutamiento interno permitidos en este proceso son: Enrutamiento estático, EIGRP, RIPv1, RIPv2 y OSPF.

Con fines prácticos se estableció la sesión eBGP entre el router de la empresa y el CPE, eBGP posibilita que el CPE pueda aprehender los prefijos asignados por sede, los cuales posteriormente serán anunciados a la red del ISP. En la topología de red (Figura 41), se aprecia la asignación del AS 65510 para el CPE, a continuación, se consideró los siguientes AS de acuerdo con el tipo de sede.

- El peer AS en las sucursales es 64516
- El peer AS en el Data Center es 65110
- El peer AS en la Oficina Administrativa es 65501
- El peer AS en la tienda del cliente es 65500 (Enlace Principal) y 65100 (Enlace secundario).

Se toma como ejemplo la sede Oficina Administrativa, la cual cuenta con el segmento LAN 172.21.152.0/22, en el siguiente grafico se observa la configuración de comandos en el CPE, los cuales muestran la configuración de la sesión BGP (Figura 42).

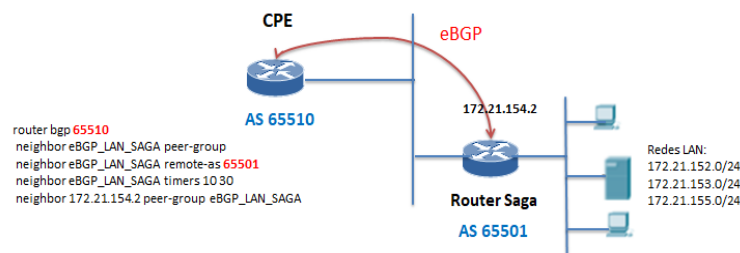


Figura 42. Establecimiento de la sesión BGP entre Router del cliente y CPE
Fuente: Elaboración propia)

A continuación, en la Figura 43, se observa como las redes de la empresa son aprehandidas por el CPE debido a la sesión BGP.

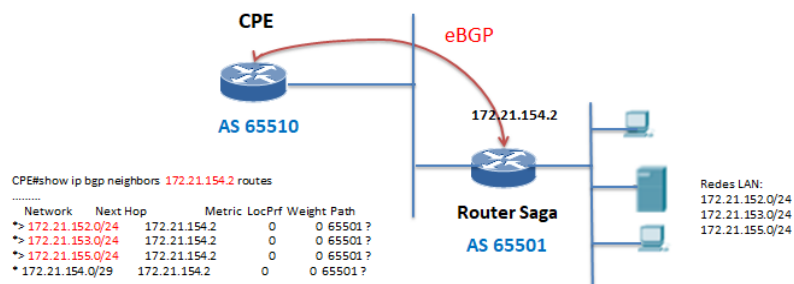


Figura 43. Anuncio de redes LAN del router del cliente hacia el CPE Fuente: Elaboración propia)

3.7.8 Distribución de BW para las sedes

De acuerdo con el requerimiento solicitado por la empresa, se procedió a implementar BW de 6Mbps,4Mbps,4Mbps,4Mbps y 4Mbps para sede Oficinas Administrativas, Data Center, sede surcusal, sede principal y contingencia Tienda Mall Aventura plaza respectivamente,

3.7.9 Enlace principal y contingencia para la sede Tienda Mall Aventura Plaza

Para poder brindar un servicio de alta disponibilidad para la empresa, se optó por implementar una solución de respaldo para la sede Tienda Mall Aventura Plaza, la cual consta de un enlace principal y de respaldo. Se trabajó con los protocolos HSRP y BGP, cumpliendo dos objetivos principales.

El primer objetivo para lograr una ruta de salida totalmente redundante se realiza con HSRP, por lo cual todo el tráfico saliente proveniente de la red LAN de la empresa y destinado a la nube MPLS debe enrutarse a través de CPE 1 hacia el PE rMPLS1. Sin embargo, si CPE 1 falla, todo el tráfico saliente debe redirigirse a través del CPE 5 hacia el PE rMPLS5.

El segundo objetivo es lograr una ruta de entrada totalmente redundante lo cual se realiza con BGP, todo el tráfico entrante destinado a el sistema autónomo, AS 65500, desde la nube MPLS debe enrutarse a través de PE rMPLS1 hacia el CPE1. En el caso de que falle el enlace, el tráfico entrante debe redirigirse automáticamente a través de PE rMPLS5 hacia el CPE 5.

Consecuentemente se describe los pasos y el análisis correspondiente para ofrecer dicha solución.

3.7.9.1 Influencia del tráfico de entrada. Se procedió a asignar el local preference 200 para las rutas que el CPE aprehende del PE rMPLS1 a través del neighbor instaurado en la WAN del enlace principal e influenciar el tráfico de entrada por dicho enlace, por otro lado se estableció un local preference 100 para la rutas recibidas del PE rMPLS5 a través del neighbor instaurado en la WAN del enlace de contingencia, dado que el local preference para las rutas aprendidas por el enlace principal es mayor ($200 > 100$), dicho enlace será seleccionado como ruta para el tráfico de entrada de manera prioritaria.

En primer lugar, se establece el route-map “PRI_ISP_FALABELLA” utilizado para las rutas declaradas por el CPE a través del enlace principal, y el route-map “SEC_ISP_FALABELLA” para las rutas declaradas por el enlace de contingencia (Figura 44).

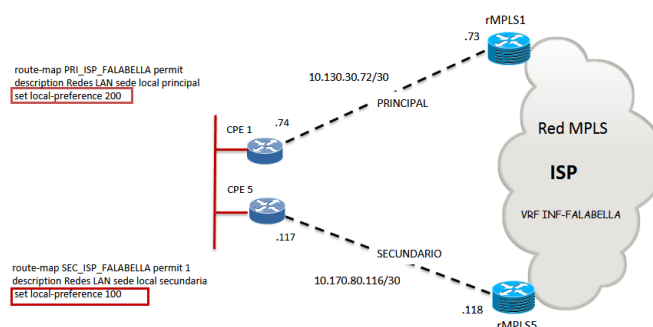


Figura 44. Configuración de route-map en el CPE principal y secundario
Fuente: Elaboración propia)

Estos route-map se asocian con las listas creadas en los PE rMPLS1 y rMPLS5 (Figura 45).

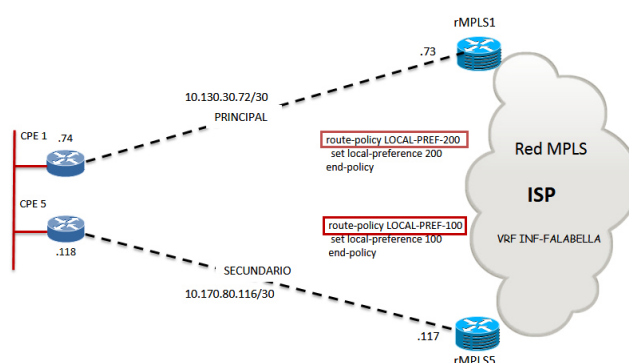


Figura 45. Configuración de listas route-map en los PE Fuente: Elaboración propia)

Posteriormente se observa que las rutas aprehandidas para PE rMPLS1 tienen local preference 200, y para PE rMPLS5 tienen local preference de 100 (Figura 46).

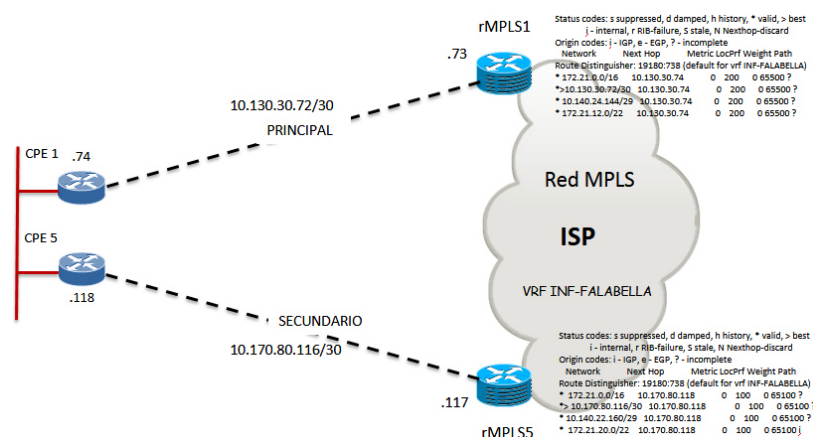


Figura 46. Rutas obtenidas en la red con valor de Local Preference Fuente:
(Elaboración propia)

3.7.9.2 Influencia del tráfico de salida. Una ruta de salida totalmente redundante se logró con el protocolo HSRP, por lo tanto, todo el tráfico saliente de la red 172.24.0.0/24 y destinado a la nube MPLS se enruta a través de CPE 1 al PE rMPLS1. En el caso falle CPE 1, todo el tráfico saliente se redirigirá a través de CPE 5 al PE rMPLS5.

Los equipos R1 y R5 son configurados con HSRP sobre la misma LAN. Los hosts de la LAN tienen una ruta por defecto, la cual apunta hacia la dirección IP HSRP standby 172.24.0.4.

En la figura 47, R1 y R5 tienen una conexión eBGP e iBGP con rMPLS 1 y rMPLS 5 respectivamente, asegurando de esta manera un óptimo enrutamiento, y llevar a cabo la alta disponibilidad al servicio de red.

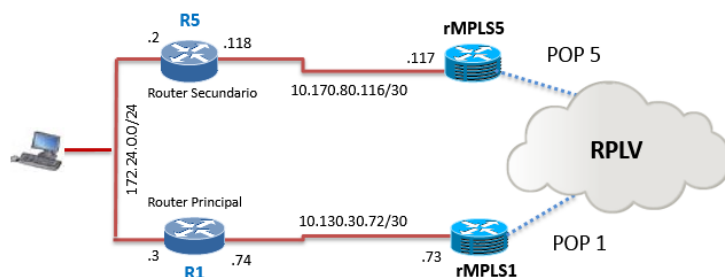


Figura 47. Diagrama de enlace redundante con HSRP Fuente: Elaboración propia)

Para el caso de R1, el cual se configura como router activo con una prioridad 150 y donde la línea de comando track cumple la función sensor la ip default configurada en el nodo de donde se atiende R1, en caso de una caída el evento track pasa de estado Up a Down o viceversa, reduciéndose la prioridad, lo cual conduce a que el router R5, tenga la prioridad más alta (prioridad 100). Así R5 se convierte en router activo y atrae el tráfico destinado a la dirección activa HSRP 172.24.0.4 (Figura 48),

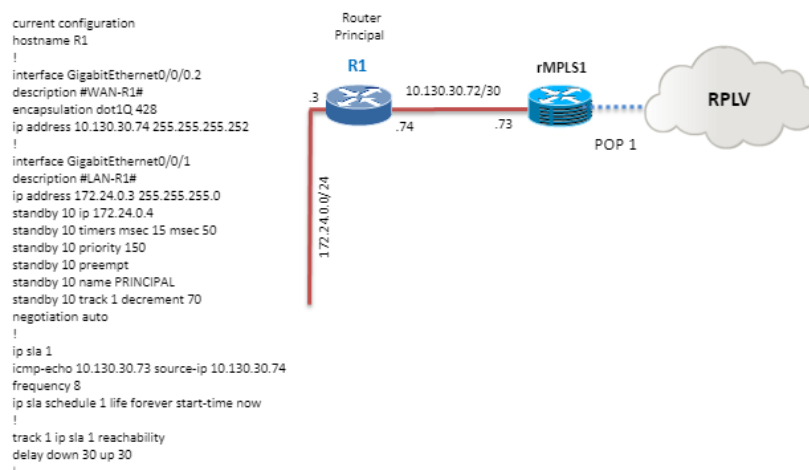


Figura 48. Diagrama de configuración HSRP sobre R1 Fuente: Elaboración propia)

El router secundario R5 está configurado con una prioridad de espera por defecto la cual es 100 (Figura 49).

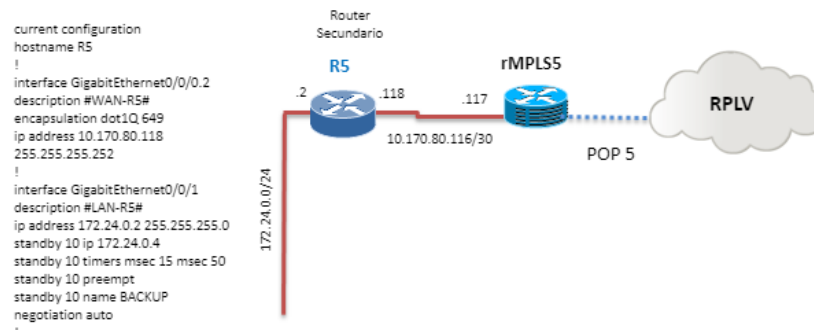


Figura 49. Diagrama de configuración HSRP sobre R5 Fuente: Elaboración propia)

Posteriormente, utilizando el comando “show standby” se observa el estatus de R1 como router activo con la prioridad 150. Por lo cual R1 posee la dirección IP standby 172.24.0.4 y todo el tráfico IP del host configurado hacia dicha IP se enruta a través de R1 (Figura 50).

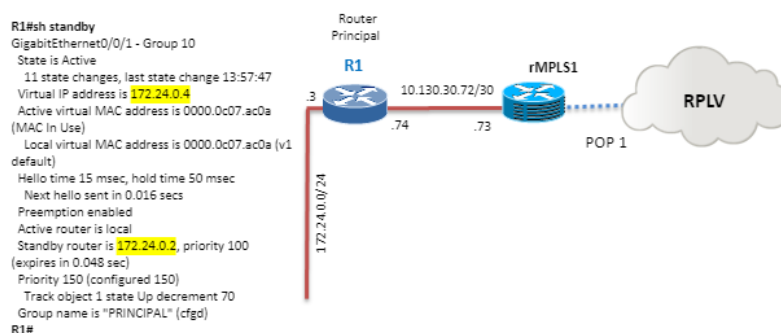


Figura 50. Verificación de estatus de R1 como router activo HSRP Fuente: Elaboración propia)

3.8. Presentación de resultados

3.8.1 Conectividad entre equipo PE y CPE

Procedemos a verificar la conectividad entre el PE y CPE localizado en las sedes de la empresa. Todo ello validado a través de la herramienta software Secure CRT, comprobando conexión a nivel de capa 1, 2 y 3 entre los equipos (Figura 51).

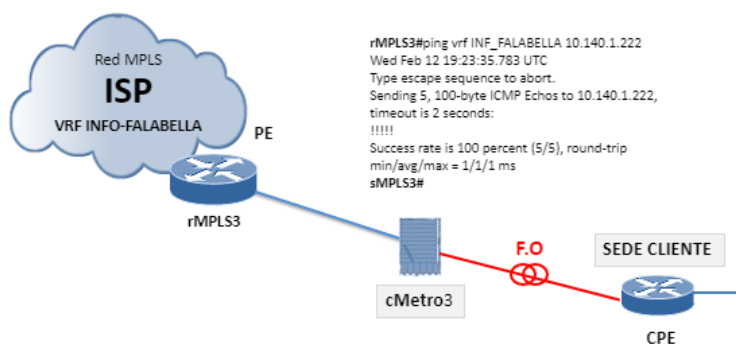


Figura 51. Verificación de conectividad entre PE y CPE Fuente: Elaboración propia)

3.8.2 Establecimiento del protocolo BGP entre CPE y PE

De manera posterior a comprobar la conectividad entre los equipos CPE Y PE, procedemos a verificar el establecimiento BGP entre dichos equipos y que las rutas LAN sean recibidas y enviadas a través de la red del ISP. A continuación, en las figuras 52 y 53, se muestran como ejemplo el enlace de la sede Administrativa.

```

rMPLS4#show bgp vrf INF-FALABELLA summary | begin neighbors
Mon Feb 17 11:47:17.867 UTC
Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.160.80.146 0 65501 8287753 4925603 611524676 0 0 7w6d 7

```

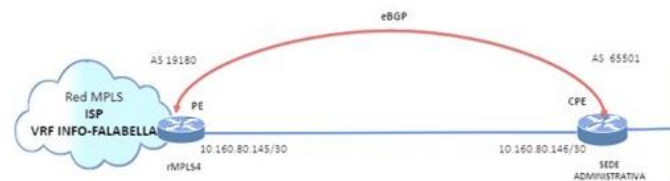


Figura 52. Sesión BGP establecida entre CPE y PE Fuente: Elaboración propia)

```

rMPLS4#sh bgp vrf INF-FALABELLA neighbors 10.160.80.146 routes
Mon Feb 17 16:17:16.472 UTC
BGP VRF INF-FALABELLA, state: Active
BGP table state: Active

```

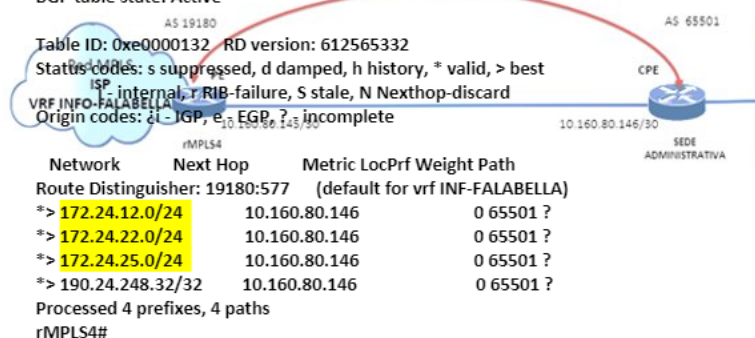


Figura 53. Redes LAN recibidas por la red del ISP Fuente: Elaboración propia)

3.8.3 Conexión entre sedes

Las redes LAN de una sede son anunciadas hacia la red del ISP, estas son redistribuidas a través de la nube MPLS hacia los demás PEs para posteriormente ser anunciados hacia las demás sedes de la empresa estableciendo conexión entre ellas. A continuación, se observa como la ruta apprehendida por la red en la figura 54 es propagada a los demás PEs y por último a los CPEs.

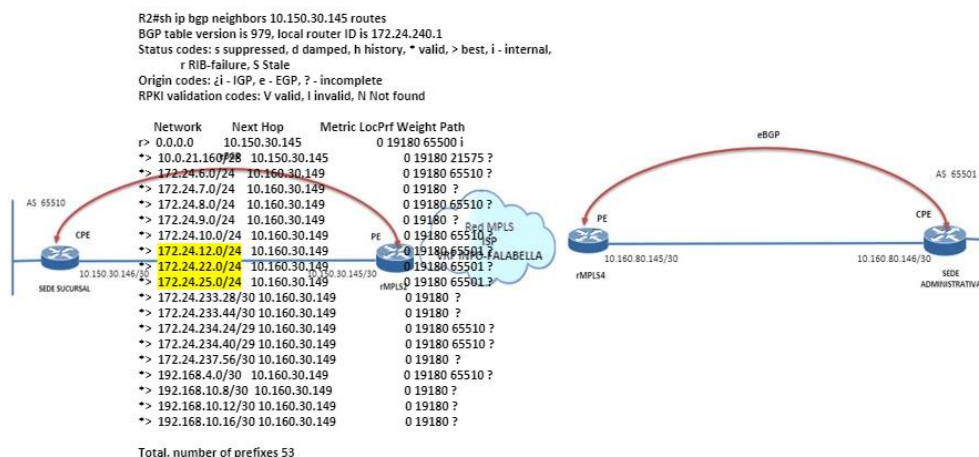


Figura 54. Redes LAN recibidas por sede remota Fuente: Elaboración propia)

Se valida que la conexión exitosa entre las diferentes sedes, debido a que se dio el intercambio de rutas entre las diferentes sedes, comprobando que, desde el CPE de la sede Administrativa, se tiene conexión las redes LAN de las diferentes sedes.

3.8.4 Actividad de alta disponibilidad para la sede Mall Aventura Plaza

Previamente se indicó que para llevar a cabo la influencia del tráfico de entrada las rutas que el CPE aprehende de la red del ISP serian asignadas al atributo local preference de 200 en caso de ser declaradas a través del enlace principal y en caso ser publicadas a través del enlace de contingencia al atributo local preference de 100.

Se valida a modo de prueba la preferencia que tiene el enlace principal frente al de contingencia para las demás redes que son aprehendidas por la red del ISP utilizando la herramienta traceroute, por lo cual analizamos que desde el PE rMPLS1 correspondiente al enlace principal, los saltos se ejecutan de manera directa hacia el CPE, sin embargo, al realizarla desde el PE rMPLS5 correspondiente al enlace de contingencia, analizamos que el primer salto se da hacia la IP 10.130.30.73 perteneciente al PE rMPLS1, y que

posteriormente se ejecutan los mismos saltos observamos en la prueba realizada para el enlace principal (Figura 55).

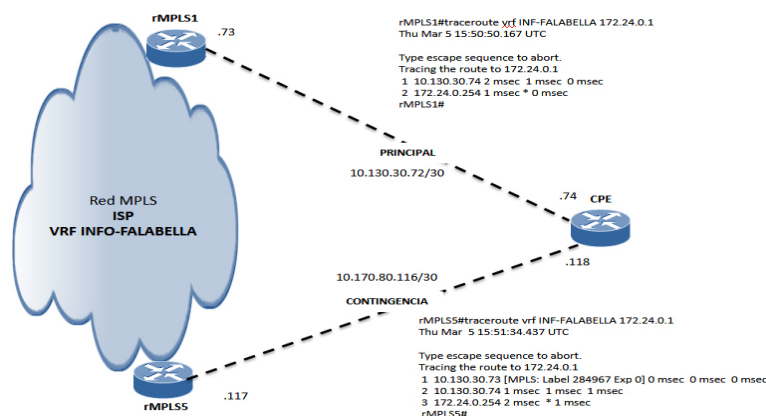


Figura 55. Traceroute desde los equipos de red hacia la LAN del cliente Fuente:
Elaboración propia)

En cuanto al tráfico de salida, se determinó el uso del protocolo HSRP para lograr una ruta de salida totalmente redundante, por lo cual las rutas anunciadas por el CPE a través de la sesión BGP-HSRP del enlace principal son determinadas por la prioridad 150 mientras que a las anunciadas a través del enlace de contingencia por la prioridad 100, estableciendo que la mejor ruta sea a través del enlace principal (Figura 56):

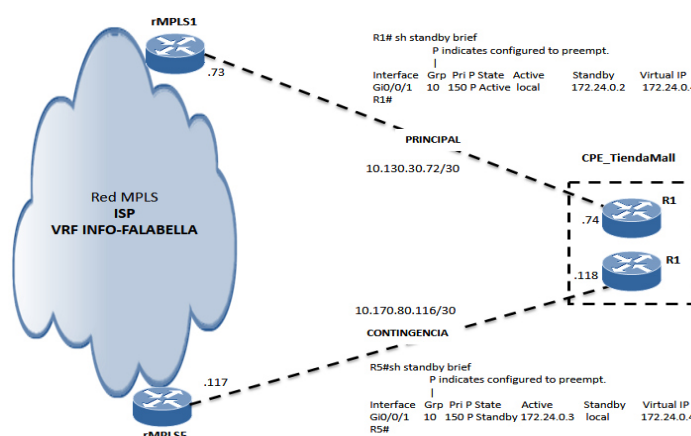


Figura 56. Verificación de prioridad HSRP en CPE Fuente: Elaboración
propia)

Se valida a modo de prueba la preferencia que tiene el enlace principal, al efectuar una prueba de traceroute desde el CPE hacia una de las redes que fueron aprehendidas tanto desde el PE del enlace principal, como el de contingencia, la cual ejecuta el primer salto hacia la IP 10.130.30.73 (IP en rMPLS1) (Figura 57).

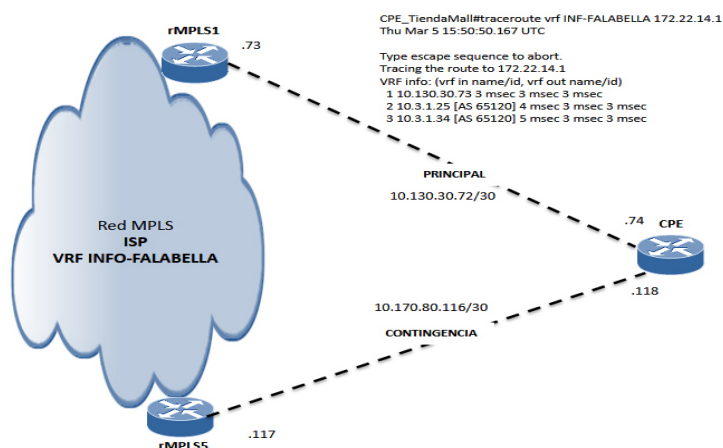


Figura 57. Traceroute desde CPE hacia otra sede remota Fuente: Elaboración propia)

A continuación, en la figura 58, se presenta el tráfico entrante y saliente registrado a través de la interfaz WAN del CPE correspondiente al enlace principal al realizar pruebas de traceroute y conectividad hacia otras sedes, utilizando la herramienta cacti.

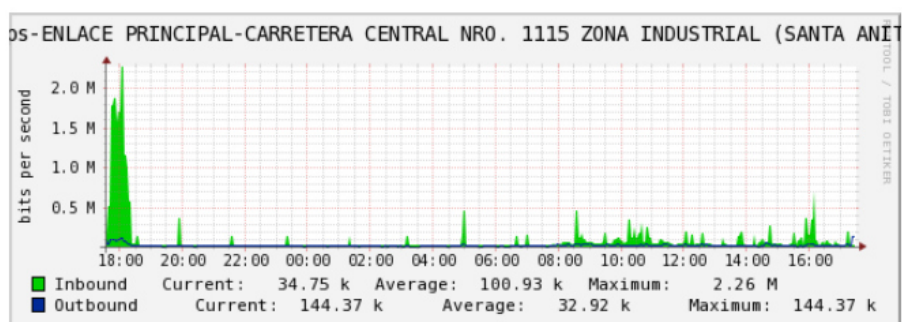


Figura 58. Gráfica cacti del enlace Principal Fuente: Elaboración propia)

De igual manera en la figura 59 se observa la gráfica registrada a través del CPE correspondiente al enlace de contingencia, el cual es mínimo ya que la preferencia de datos se tiene a través del enlace principal.

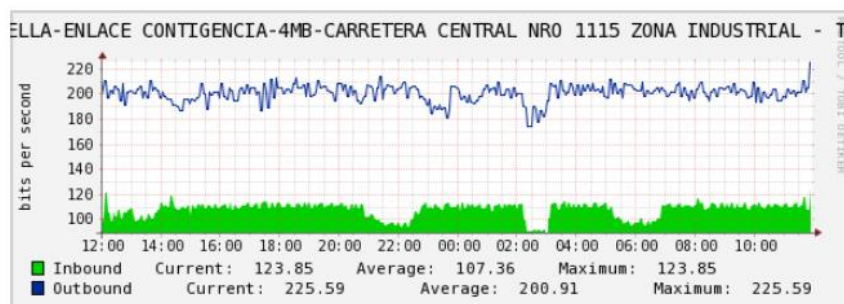


Figura 59. Gráfica cacti del enlace Contingencia Fuente: Elaboración propia)

IV. CONCLUSIONES

El presente trabajo de suficiencia profesional logro el objetivo principal y los objetivos específicos en la medida que se diseñó la topología de la red privada virtual propuesta para la empresa cumpliendo con las consideraciones y condiciones constituidas inicialmente, asegurando de esta manera la calidad y disponibilidad del servicio, en cuanto al diseño de la arquitectura de red se realizó un exhaustivo análisis para seleccionar del equipamiento de transporte y acceso adecuado, de este modo sobre la base de un diagnóstico de las necesidades de la empresa y el modo de funcionamiento del mismo se determinó el tipo de red privada virtual a implementar y el dimensionamiento de la capacidad de la red de la empresa.

Así mismo se concluye que con la implementación del servicio de red Privada Virtual Local sobre la infraestructura de un ISP los siguientes beneficios:

- El servicio RPVL brinda una excelente capacidad, es decir se entrega un ancho de banda constante e integro para cada servicio.
- El servicio RPVL ofrece cobertura de conectividad, por lo cual, al ser red sólida y robusta, posibilitara la conexión remota local entre todas las sucursales de manera local, las cuales están localizadas dentro de la cobertura del ISP.
- El servicio RPVL proporciona una gran conectividad, permitiendo una sencilla implementación de conexiones de red entre sucursales diferentes y sistemas de redundancia, los cuales respaldan la continuidad del servicio de red.

- El servicio RPVL otorga confiabilidad, garantizando que toda la información trasladada a través de la red sea de total confidencialidad y con altos niveles de seguridad.
- El servicio RPVL genera ahorro de costos, al poseer diferentes servicios a través de una única red y con una sola puerta.
- El servicio RPVL provee un incremento de competitividad, permitiendo el intercambio de información a través de herramientas que facilitan la comunicación, incrementando de esta manera la productividad del personal.

V. RECOMENDACIONES

De acuerdo con la conclusión de implementación del servicio de red privada virtual local para la empresa, se sugiere lo siguiente:

- Desarrollar mantenimientos preventivos de manera mensual y/o anual del equipamiento instalado en la sucursal del cliente con la finalidad de reducir las probables averías del servicio en el futuro.
- Brindar un continuo soporte de monitoreo para el servicio, y poder gestionar las fallas, configuración e informes en general del servicio, garantizando de esta manera el cumplimiento del SLA (acuerdo de nivel de servicio).
- Brindar la posibilidad de realizar cambios configurativos sobre el servicio del cliente, tales como la adición de nuevos prefijos de red del cliente, variaciones de BW, creación de puertos, etc.
- Brindar al cliente la implementación de servicios adicionales, como la instauración de nuevas sucursales dentro de la topología de red brindada originalmente, resultando como beneficio en el crecimiento de red del cliente.
- Realizar pruebas de contingencia de manera trimestral y/o semestral para constatar el correcto funcionamiento del enlace de emergencia frente a una caída del enlace principal.

VI. BIBLIOGRAFIA

- Ariganello, E. & Barrientos, E. (2010). *Redes CISCO. CCNP a fondo. Guía de estudio para profesionales*. España: Grupo Editorial RA-MA.
- Ceragon Networks (2008). *FibeAir® IP-10*. Ceragon. Recuperado de https://www.academia.edu/30616991/IP_10_CERAGON
- Ceragon Networks (2011). *FibeAir® RFU-C*. Ceragon. Recuperado de https://www.winncom.com/pdf/Ceragon_FibeAir_RFU_C/Ceragon_RFU-C_Product_Description.pdf
- Chen, J. (2015). *¿Qué es la "fibra óptica"? y ¿Porqué utilizarlas?*. Apac Opto Electronics Inc. Recuperado de: <http://apacoe.weebly.com/conocimiento/que-es-la-fibra-optica>
- Cisco (2006). *Hot Standby Router Protocol Features and Functionality*. Cisco. Recuperado de <https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>
- Cisco (2011). *Cisco ME 3400E Ethernet Access Switch Software Configuration Guide*. Cisco. Recuperado de https://www.cisco.com/c/en/us/td/docs/switches/metro/me3400e/software/release/12-2_58_se/configuration/guide/ME3400e_scg.pdf
- Cisco (2017a). *Cisco 2900 Series Integrated Services Routers Data Sheet*. Cisco. Recuperado de https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html
- Cisco (2017b). *Cisco ASR 9910 and ASR 9906 Route Switch Processor Data Sheet*. Cisco. Recuperado de <https://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-series-aggregation-services-routers/datasheet-c78-737234.html>
- Cisco (s.f-a). *Layer 3 VPNs (L3VPN)*. Cisco. Recuperado de <https://www.cisco.com/c/en/us/products/ios-nx-os-software/layer-3-vpns-l3vpn/index.html>

- Cisco (s.f-b). *Sample Configuration for iBGP and eBGP With or Without a Loopback Address*. Cisco. Recuperado de <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13751-23.pdf>
- Cisco (s.f-c). *What is MPLS - Multiprotocol Label Switching*. Cisco. Recuperado de: <http://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html>
- Díaz Llatance, M. A., & Vieyra Dioses, G. L. A. (2015). *Diseño de una red privada virtual para interconectar las sucursales de la empresa Terracargo SAC*. (Tesis de grado, Universidad Nacional Pedro Ruiz Gallo). Recuperado de <http://repositorio.unprg.edu.pe/handle/UNPRG/462>.
- Diseño Gráfico 7° (2010). *Enrutador*. Casiopea. Recuperado en: <https://wiki.ead.pucv.cl/Enrutador>.
- EcuRed (s.f). *Fibra óptica*. EcuRed. Recuperado de http://www.ecured.cu/index.php/Fibra_%C3%B3ptica.
- 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 SA* (Tesis de grado, Universidad Autónoma del Perú). Recuperado de <http://repositorio.autonoma.edu.pe/handle/AUTONOMA/487>
- Extreme (2014). *Switch BlackDiamond 8800 Series Switches Hardware Installation Guide*. Extreme. Recuperado de <http://www.extremenetworks.com/wp-content/uploads/2014/02/BlackDiamond8800SeriesSwitchesHardwareInstallationGuide-100284Rev07.pdf>
- Graziani, R., & Johnson, A. (2008). *Conceptos y protocolos de enrutamiento: guía de estudio de CCNA Exploration*. Pearson Educación.
- Menéndez Ávila, R. A. (2012). *Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos* (Tesis de grado, Pontificia Universidad Católica del Perú). Recuperado de <http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/1500>
- Prieto Cristancho, Y. Y. (2011). *Implementación de la red privada virtual (VPN) a las sucursales y usuarios externos de la empresa Hardsoft SA*. (Tesis

- de grado, Universidad Libre). Recuperado de <https://repository.unilibre.edu.co/handle/10901/8838>.
- PT Prima Telekom Intermedia (2016). *RC552-FE, RC552-GE Ethernet over Fiber*. PT Prima Telekom Intermedia. Recuperado de <https://primatel.co.id/home/site/product-detail/rc552-fe,-rc552-ge>
- Puse Huangal, R. O., & Ruíz La Torre, M. E. (2015). *Diseño e implementación de un sistema de monitoreo y gestión, mediante el uso de VPNs, para optimizar el servicio de soporte en los sistemas de video vigilancia implementados por la empresa Netkrom. Technologies* (Tesis de grado, Universidad Nacional Pedro Ruiz Gallo). Recuperado de <http://repositorio.unprg.edu.pe/handle/UNPRG/455>
- Raisecom (2015). *iTN2100 (P100R002) Hardware Description (Rel_05)*. Raisecom. Recuperado de [http://raisecom.su/Datasheet/iTN2100%20\(P100R002\)%20Hardware%20Description%20\(Rel_05\).pdf](http://raisecom.su/Datasheet/iTN2100%20(P100R002)%20Hardware%20Description%20(Rel_05).pdf)
- Raisecom (s.f-a). *iTN2100 Multi Services PTN Platform*. Raisecom Technology Co. Recuperado de http://www.davantel.com/files/iTN2100_platform.pdf
- Raisecom (s.f-b). *RC512-FE Remote Manageable Media Converter*. Raisecom Technology Co. Recuperado de <http://www.davantel.com/files/RC512-FE-new.pdf>
- Raisecom (s.f-c). *RC552-FE (Rev.B) 10/100M OAM Media Converter with 1:1 Uplink Protection*. Raisecom Technology Co. Recuperado de <https://www.davantel.com/files/rc552-ferev-b.pdf>
- Ramirez, A., & Contador, N. (2014). *Principios básicos de enrutamiento y switching CCNA1 V5*. Cisco Networking Academy
- Redes Avanzadas Sección 7001 (2020). *Cisco Packet Tracer*. Redes Avanzadas Sección 7001. Recuperado de <http://ftorresnetworking.blogspot.com/>
- Ruesca, P. (2016). *Radio Enlace - ¿Qué es un radioenlace?* Radio Comunicaciones. Recuperado de: <http://www.radiocomunicaciones.net/radio/radio-enlace-que-es-un-radioenlace/>

Wikipedia (2020a). *ARPANET*. Wikipedia. Recuperado de
<https://es.wikipedia.org/wiki/ARPANET>

Wikipedia (2020b). *Fibra Óptica*. *Wikipedia*. Recuperado de:
https://es.wikipedia.org/wiki/Fibra_%C3%B3ptica

Wikipedia (2020c). *Network switch*. Wikipedia. Recuperado de
https://en.wikipedia.org/wiki/Network_switch

Zamora, J. (2013). *Yo sé networking – BGP*. Networks. Recuperado de
<http://networksjuan.blogspot.com/2013/01/yo-se-networking-bgp.html>