UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“DISEÑO E IMPLEMENTACIÓN DE UN SERVICIO DE SEGURIDAD ADMINISTRADA E INTERCONEXIÓN DE DATOS UTILIZANDO TECNOLOGÍA MPLS PARA EL INSTITUTO DEL MAR DEL PERU.”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

VELASQUEZ RUIZ, GUSTAVO ADOLFO

Villa El Salvador

2017

DEDICATORIA

El presente trabajo está dedicado a mi madre que ha sabido formarme con buenos sentimientos, hábitos y valores, lo cual me ha ayudado a salir adelante a pesar de los obstáculos que nos pone la vida.

A mis hermanos que siempre han estado apoyándome.

A mi padre el cual me inculco el valor del trabajo y de una profesión.

A mi pequeña hija que es mi motor y motivo para seguir adelante en la vida.

Y a mi familia en general, porque me han brindado su apoyo incondicional y por compartir conmigo buenos y malos momentos.

AGRADECIMIENTO

A mis padres y hermanos por haber confiado en mí siempre y por haberme apoyado económicamente en mis estudios.

A los grandes amigos que conocí en la carrera, porque con ellos se quedan los mejores momentos que pasé en la universidad, y porque de broma y broma siempre hubo palabras que motivaron el esfuerzo.

A Yuriko Vizcardo, que me motivo y me apoyo a que sea un profesional.

Por último, a los grandes profesores que aún siguen impartiendo su sabiduría en las aulas y a los grandes profesores que ya no están con nosotros, pero serán recordados por sus clases impartidas.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCIÓN

El presente proyecto de ingeniería realizado lleva por título: “DISEÑO E IMPLEMENTACION DE UN SERVICIO DE SEGURIDAD ADMINISTRADA E INTERCONEXION DE DATOS UTILIZANDO TECNOLOGIA MPLS PARA EL INSTITUTO DEL MAR DEL PERU”, para optar por el título de Ingeniero Electrónico y Telecomunicaciones, presentado por el alumno Gustavo Adolfo Velásquez Ruiz.

En un marco global comienza a ser habitual que empresas privadas y del estado establezcan varias sedes distribuidas geográficamente con la finalidad de la descentralización o investigación.

Esta distribución o descentralización requiere de una importante red de telecomunicaciones que soporte las siguientes características:

- Intercambio fluido de información entre sedes.
- Facilidad de administración y mantenimiento
- Ahorro de costos en comunicación

En la actualidad el avance en telecomunicaciones ha favorecido a dicho diseño y su elaboración para que cumplan con los requisitos de cada empresa. Por un lado, tenemos el avance en tecnología de comunicación como lo es MPLS el cual puede resolver muchos aspectos tales como: soportar servicios como tecnología VOIP, Redes Privadas Virtuales, Videoconferencia, etc.

Por otro lado, el avance de Seguridad Administrada cuya finalidad es brindar seguridad y optimizar la red para que la comunicación entre sedes no se vea

afectada. Avance de equipos como balanceadores de carga, monitoreo de redes, administración de correos, controladores de tráfico, filtros web, etc.

De lo anterior este proyecto de ingeniería tiene por finalidad diseñar e implementar una red con tecnología MPLS que soporte la comunicación entre su sede central y sus sedes remotas, además la administración de todos sus equipos de gestión tanto como router, switches, balanceadores, controladores de tráfico, etc.

Con el diseño e implementación se ha tratado de optimizar temas de seguridad informática, interconexión entre sedes remotas, filtros web, red redundante, etc.

Como resultado se ha diseñado una red en la que todas las sedes estén interconectadas mediante una Red Privada Virtual diseñada para administrar múltiples servicios como voz, video y datos, de la misma manera se aplica MPLS el cual permite manejar etiquetas y múltiples tablas de enrutamiento, de esta manera se optimiza la red para que el cliente tenga la mejor impresión del servicio.

La estructura que hemos seguido en este proyecto se compone de 4 capítulos. El primer capítulo comprende el planteamiento del problema, el segundo capítulo el desarrollo del marco teórico el tercer capítulo corresponde al desarrollo del proyecto y por último el capítulo cuatro comprende las conclusiones y recomendaciones.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Realidad Problemática

El Instituto del Mar del Perú – IMARPE es un Organismo Técnico Especializado del Ministerio de la Producción, orientado a la investigación científica, así como al estudio y conocimiento del mar peruano y sus recursos, para asesorar al estado en la toma de decisiones respecto al uso racional de los recursos pesqueros y la conservación del ambiente marino, contribuyendo activamente con el desarrollo del país.

IMARPE cuenta con laboratorios costeros ubicados estratégicamente en el litoral dónde se efectúan trabajos de seguimiento de las pesquerías y de los principales recursos de importancia económica y social, como son las pesquerías pelágicas (anchoveta, sardina, jurel, caballa, atún y otras), pesquerías (merluza y otras) e invertebrados marinos (pota, concha de abanico, chanque, almeja, macha y otros).

En la actualidad el Instituto del Mar del Perú (IMARPE) presenta dificultades al intentar comunicarse con sus sedes ya que presenta una red básica de internet brindada por un operador, entre la sede principal a las sedes remotas, interconectados mediante módems con protocolo punto a punto (PPP); al intentar comunicarse todos al mismo tiempo se genera tráfico de red lo que ocasiona que la red no sea optima; también presentan dificultades como:

- Reciben correos no deseados que al momento de abrir son propagandas que no tienen importancia para la Institución.
- Trabajadores de la institución acceden a páginas sin importancia para la institución como por ejemplo las redes sociales, internet radio y tv
- A cierta hora el tráfico de red es alto por lo que es necesario reiniciar las sesiones.
- La red no está monitoreada, cuando un equipo pierde gestión toma demasiado tiempo poder recuperar su gestión.

De todo su servicio de internet es de 10 Mbps en la sede principal y 5Mbps en las sedes remotas, por tal motivo la falta de implementación de una red privada con tecnología MPLS para la comunicación entre la sede principal y las sedes remotas y de seguridad administrada para la optimización de su red provoca una deficiencia en él envió de información, en la comunicación entre sus sedes, en la gestión o administración de red y en el monitoreo de toda su red.

1.2. Justificación del Problema

Debido a que El Instituto del Mar del Perú (IMARPE) es un organismo técnico especializado del Ministerio de la Producción, orientado a la investigación científica para asesorar al estado en toma de decisiones respecto al uso formal de los recursos pesqueros; es necesario que cuente con un diseño e implementación de un servicio de interconexión de la sede principal a las sedes remotas que pueda soportar tráfico sin ningún problema, contando con lo último en tecnología MPLS, así mismo contar con un servicio de seguridad administrada que nos permita apaciguar ataques externos, controlar el tráfico de red, monitorear los equipos desde una sede principal, gestionar el ingreso de correos deseados y no deseados, realizar reportes mensuales, etc. también tener una red de contingencia que este ubicada en otra sede para tener controlado en caso se presente un problema en la sede principal. Es por esta razón que se requiere una implementación seria que resuelva la problemática ya mencionada.

1.3. Delimitación de la Investigación

1.3.1. Espacial

La implementación se realizará en las sedes de lima ubicadas en la avenida Mariscal Gamarra S/N, avenida Argentina Zona Industrial y las sedes remotas en ILO, Tumbes, Puno, Matarani, Pisco, Huacho, Chimbote, Trujillo, Chiclayo y Piura.

1.3.2. Temporal

Los servicios se presentarán en un plazo de 90 días calendario.

1.3.3. Conceptual

El diseño y la Implementación considera las siguientes variables fundamentales: Red privada Virtual, Tecnología MPLS, Seguridad de datos y Calidad del Servicio.

1.4. Formulación del problema

1.4.1. Problema general

¿Cómo diseñar e implementar un servicio de Seguridad Administrada e interconexión de datos utilizando tecnología MPLS que sea confiable y eficaz, logrando mayor velocidad y seguridad desde sus diferentes sedes remotas de IMARPE?

1.4.2. Problemas específicos

- ¿Cómo controlar y monitorear el tráfico desde la sede principal hacia las sedes remotas?
- ¿Cómo diseñar e implementar una red VPN-MPLS para la interconexión de datos entre la sede principal y las sedes remotas?
- ¿Cuánto se requiere el servicio de Seguridad Administrada para prevenir ataques cibernéticos en la red de IMARPE?
- ¿Cómo diseñar e implementar una red básica de contingencia ante alguna problemática en la red principal?

1.5. Objetivos

1.5.1. Objetivo general.

Diseñar e implementar un Servicio de Seguridad Administrada e Interconexión de Datos Utilizando Tecnología MPLS para el Instituto del Mar del Perú, cuyo principal propósito sea la comunicación eficaz entre sedes y la seguridad administrada desde la sede principal.

1.5.2. Objetivos específicos.

- Controlar y monitorear el tráfico de red desde la sede principal hacia las sedes remotas.
- Diseñar e implementar una red VPN – MPLS para la interconexión de datos entre la sede principal y las sedes remotas.
- Utilizar servicios de seguridad administrada para prevenir ataques cibernéticos en la red de IMARPE.
- Diseñar e implementar una red básica de contingencia ante alguna problemática en la red principal.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

Existen proyectos de investigación nacional e internacional que me ayudaron a aportar diseño y soluciones al presente proyecto, los cuales cito a continuación:

2.1.1. Antecedentes Internacionales

a. En su tesis, diseño de una red privada virtual con tecnología MPLS para la carrera de ingeniería de networking de la universidad de Guayaquil, concluyó:

   - ✓ En el presente trabajo de tesis se detalla las características generales de MPLS así como también la arquitectura para realizar ingeniería de tráfico, la misma que se puede definir como viable en un tiempo de mediano a largo plazo según la estructura organizacional, para poder definir el diseño se necesitó un emulador de configuración de enrutadores como GNS3 que nos facilitó realizar la configuración

específica para un posterior análisis de resultados ayudados con la herramienta del wireshark.

- ✓ La tecnología MPLS permite a los ISP incrementar la fiabilidad y confianza en sus redes por lo que beneficia al reducir tiempos en su transmisión de información y brinda seguridad requerida por el cliente. Cabe indicar que pueden ser usados varios protocolos de enrutamiento dinámico como RIP, EIGRP, OSPF o inclusive enrutamiento estático, pero por las bondades que tiene cada uno de ellos se prefiere trabajar con OSPF por sus ventajas con respecto a los otros protocolos.
- ✓ MPLS VPN con su implementación en la Universidad de Guayaquil con la carrera de Ingeniería de Networking ayudará a la comunicación entre las mismas así también a la especialización de la tecnología para los estudiantes de la carrera de manera tal que podrían tener mejor aprendizaje y posiblemente las mejoras de velocidades se verán incrementadas en los próximos años y estarán en un nivel de poder hacer las respectivas actualizaciones si ameritan.
- ✓ MPLS VPN va a permitir que las demás facultades o carreras que no se encuentran radicadas físicamente en la universidad matriz utilicen la tecnología en un futuro para así poder tener las comunicaciones online de manera segura con calidad de servicio.
- ✓ La implementación de una red basada MPLS VPN en Guayaquil revolucionará el mercado tecnológico, ya que con la capacidad diseñada se podrá transportar muchos servicios de diferentes formatos, permitiendo ser a la Universidad una entidad que brinda calidad de

servicio, así como una red segura para la transmisión de data a nivel MAN (Orozco,2014, pag.79).

b. En su tesis, diseño y simulación de una red MPLS para interconectar estaciones remotas utilizando el emulador GNS3, concluyó:

- ✓ Después de implementar el diseño entre sucursales en el simulador GNS3 he llegado a la conclusión que MPLS es un protocolo que presenta varios beneficios para empresas medianas y grandes existentes en el mercado ecuatoriano, puesto que su servicio de calidad y su ingeniería de tráfico disminuye notablemente el tráfico de una red.
- ✓ Adicionalmente las razones por la cual la IETF creó el protocolo MPLS fueron los correctos porque soporta nuevos servicios que las redes IP convencionales no hacen, además de funcionar con cualquier otro tipo de tecnología de transporte.
- ✓ MPLS puede integrar distintos dominios de red independientemente de su protocolo de capa 2 a través de distintas técnicas de encapsulamiento, esto se debe a la gestión multi-etiquetas que permite la combinación del enrutamiento de la capa de red con la conmutación de la capa de enlace para el envío de paquetes utilizando etiquetas cortas de longitud fija, separando el plano de control del plano de datos.
- ✓ Para finalizar MPLS permite a los proveedores de servicios ser más competitivos y estar más actualizados en cuanto a avance tecnológico se refiere, también permite tener una infraestructura mejor preparada

para soportar nuevos clientes y ofrecer mejor servicios a sus usuarios finales, adicionalmente GNS3 permite a los profesionales que carecen de experiencia básica obtenerla ya que el software posee una interface grafica amigable y fácil de entender (Castro,2015, pag.90).

c. En su tesis, análisis del tráfico de la red para la optimización y mejora del sistema VSAT del CNT EP, concluyó:

- ✓ Después de implementar el diseño entre sucursales en el simulador GNS3 he llegado a la conclusión que MPLS es un protocolo que presenta varios beneficios para empresas medianas y grandes existentes en el mercado ecuatoriano, puesto que su servicio de calidad y su ingeniería de tráfico disminuye notablemente el tráfico de una red.
- ✓ Adicionalmente las razones por la cual la IETF creó el protocolo MPLS fueron los correctos porque soporta nuevos servicios que las redes IP convencionales no hacen, además de funcionar con cualquier otro tipo de tecnología de transporte.
- ✓ MPLS puede integrar distintos dominios de red independientemente de su protocolo de capa 2 a través de distintas técnicas de encapsulamiento, esto se debe a la gestión multi-etiquetas que permite la combinación del enrutamiento de la capa de red con la conmutación de la capa de enlace para el envío de paquetes utilizando etiquetas cortas de longitud fija, separando el plano de control del plano de datos. Para finalizar MPLS permite a los proveedores de servicios ser más competitivos estar más actualizados en cuanto a avance

tecnológico se refiere, también permite tener una infraestructura mejor preparada para soportar nuevos clientes y ofrecer mejor servicios a sus usuarios finales, adicionalmente GNS3 permite a los profesionales que carecen de experiencia básica obtenerla ya que el software posee una interface grafica amigable y fácil de entender (Páez, 2014, pag.100).

2.1.2. Antecedentes Nacionales

a. En su tesis, diseño e implementación del centro de operación y gestión de la Red Académica Peruana en Software Libre, concluyó:

- ✓ Se analizaron las características de la RAAP, y en función a ellas, se diseñó e implementó un sistema para su monitoreo y gestión.
- ✓ El sistema permite obtener y almacenar estadísticas del rendimiento de la red, observando sus características actuales y su evolución histórica.
- ✓ El sistema hace posible monitorear el estado de los equipos y los servicios que corren en ellos, generando una alarma en caso ocurra un error.
- ✓ El sistema permite realizar cambios en los equipos, para efectuar alguna modificación en la configuración o corregir un estado erróneo.
- ✓ El sistema ha sido implementado utilizando software libre, esto proporciona ahorros en licencias y además la posibilidad de modificar el código para adaptar los programas a necesidades específicas.
- ✓ El sistema es modular, lo cual hace posible que sea adaptado conforme las necesidades de la RAAP evolucionen. Además, puede ser adecuado al monitoreo de diversos escenarios e incluso a aplicaciones del tipo educativo (Rosemberg, 2007, pag70).

b. En su tesis, diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña, concluyó:

- ✓ El servidor de correo, que compartía recursos con el antispam, presentaba un alto consumo de recursos debido a que cada correo entrante debe ser analizado por los motores de análisis del antispam para luego ser enviado al motor del servicio de correo y finalmente depositado el correo en la casilla del usuario. En cada una de estas etapas, una copia temporal del correo es escrita en el disco duro. Esta es una razón adicional para justificar la implementación de una solución antispam fuera del servidor de correo electrónico. Una evaluación posterior realizada posteriormente a la implementación de la solución propuesta corroboró esta teoría.
- ✓ Las fórmulas utilizadas del Firewall Perimetral para calcular el número de sesiones concurrentes no son un cálculo exacto y puede variar de acuerdo con los hábitos de uso de internet de los usuarios de la empresa. Sin embargo, pueden proveer un dato bástate útil y que puede ser utilizado para dimensionar un equipo para este propósito. En caso se identifique que existen otras aplicaciones que puedan significar un aumento en el número de sesiones, como, por ejemplo: telefonía por internet, telefonía IP a través de un proveedor externo; debe replantearse la formula o utilizar algún otro método para calcular el total de sesiones concurrentes que debe soportar el equipo. En caso de no poder obtener una formula convincente, es necesario medirlo de manera práctica. Una buena práctica para este fin es colocar alguno de los equipos propuestos en modo transparente de manera que nos permita obtener la información necesaria.

- ✓ La selección de los fabricantes o marcas de los productos no necesariamente debe basarse en la información provista por Gartner. Existen además otras empresas dedicadas a evaluar los distintos productos existentes en el mercado. Sin embargo, un dato bastante apreciado en el mercado local son las empresas que actualmente utilizan ese producto. La selección del producto muchas veces se puede realizar basándose únicamente en referencias.
- ✓ Tal y como mencionó, cada red cuenta con requerimientos específicos que deben ser considerados como prioridad al diseñar su arquitectura o topología de red, sin embargo, la presente tesis puede servir como referencia o base para dicho diseño (Valenzuela, 2012, pag.75).

Estas fueron las tesis con mayor influencia al proyecto de ingeniería, que a su vez se ha querido enfocar a dos temas importantes para servicio; la Seguridad Administrada y la interconexión de datos.

2.2. Bases Teóricas

2.2.1. Seguridad Administrada

Según el artículo “Retos y oportunidades de los proveedores de servicio de seguridad Administrada”. La seguridad administrada es un término que adopta una solución de equipos que hacen que la red se encuentre optimizada, a su vez se refiere al proceso de administrar la seguridad por parte de una unidad de negocio o empresa especializada. La seguridad administrada incluye en términos generales la prestación de servicios de monitoreo, administración y reacción ante incidentes.

La seguridad administrada monitorea y gestiona las políticas de seguridad en tu conexión a Internet, permite reaccionar ante incidentes de seguridad y evitando la pérdida de tu información [4].

Administra y monitorea los siguientes equipos:

a) FIREWALL
b) IDS (Sistema de detectores de Intrusos)
c) GESTION DE ANCHO DE BANDA

a) FIREWALL

A continuación, se resume la definición, tipos de Firewall y ventajas y desventajas según el argumento publicado por cisco. Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet [3].

Un firewall puede ser hardware, software o ambos.

❖ **Tipos**

✓ **Firewall proxy**

Un firewall proxy, uno de los primeros tipos de dispositivos de firewall, funciona como Gateway de una red a otra para una aplicación específica. Los servidores proxy pueden brindar funcionalidad adicional, como seguridad y almacenamiento de contenido en caché, evitando las conexiones directas desde el exterior de la red. Sin embargo, esto también puede tener un impacto en la capacidad de procesamiento y las aplicaciones que pueden admitir [3].

✓ **Firewall de administración unificada de amenazas (UTM)**

Un dispositivo UTM suele combinar en forma flexible las funciones de un firewall de inspección activa con prevención de intrusiones y antivirus. Además, puede incluir servicios adicionales y, a menudo, administración de la nube. Los UTM se centran en la simplicidad y la facilidad de uso [3].

- **Ventajas y desventajas**

Ventajas

- Administran los accesos provenientes de Internet hacia la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Por ello la seguridad en la red privada depende de la "dureza" con que el firewall cuente.
- Administran los accesos provenientes de la red privada hacia el Internet.

- Permite al administrador de la red mantener fuera de la red privada a los usuarios no-autorizados (tal, como, hackers, crackers y espías), prohibiendo potencialmente la entrada o salida de datos.
- El firewall crea una bitácora en donde se registra el tráfico más significativo que pasa a través él.
- Concentra la seguridad. [3]

Desventajas.

- Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación. Por ejemplo, si existe una conexión PPP (POINT-TO-POINT) al Internet.
- El firewall no puede prohibir que se copien datos corporativos en disquetes o memorias portátiles y que estas se substraigan del edificio.
- El firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él, pues el firewall no es un antivirus.
- El firewall no puede ofrecer protección alguna una vez que el agresor lo traspasa. [3]

b) SISTEMA DE DETECTORES DE INTRUSIONES (IDS)

Los Sistemas Detectores de intrusos (IDS) son utilizados para monitorear una red o un grupo específico de computadoras. Los IDS pueden ser configurados para buscar ataques, analizar logs de auditoría, alertar al administrador cuando los ataques suceden, proteger sistemas de archivos, exponer técnicas de hackeo, mostrar que vulnerabilidades etc. [6]

- ✓ **Funcionalidad**

Entre sus principales funciones, se encuentran no sólo la de identificar la actividad maliciosa, sino la de detener esta actividad. En la figura 1 se puede observar donde se pueden ubicar los sistemas IPS. [6]

Se tiene que puede alertar al administrador ante la detección de intrusiones o actividad maliciosa, establecer políticas de seguridad para proteger al equipo o a la red de un ataque. [6]

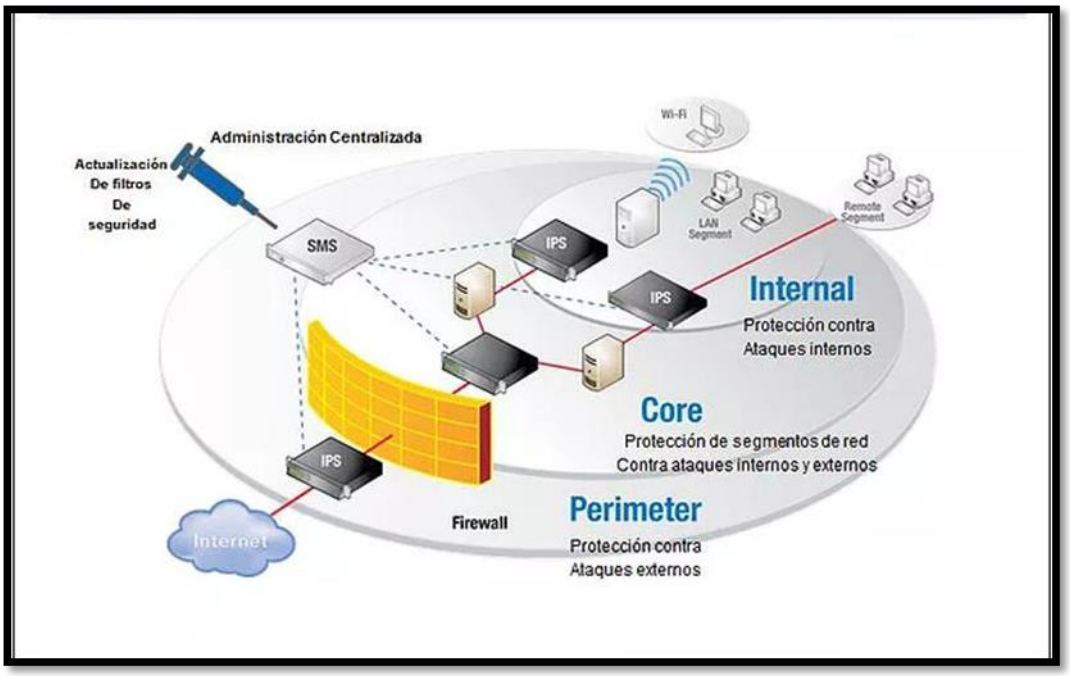


Figura 1: *Lugar de prevención y detección de intrusos en la Red.*
Fuente: *Página web de seguridad INFORMATICA.*

c) GESTION DE ANCHO DE BANDA

La gestión de ancho de banda es una actividad crítica para minimizar los riesgos en las organizaciones de negocios y maximizar la productividad de los trabajadores. Permite a las organizaciones extender efectivamente el filtrado de páginas Web más allá del bloqueo de sitios con las siguientes capacidades:

trabajo, bloqueo o restricción de descargas por extensión, bloqueo de mensajeros instantáneos, bloquea completamente los programas de descargas como Emule. Acceso a Internet programado por usuario por día y hora. [5]

El software de WEBSENSE permite que los administradores de red de todos los sectores de la industria, desde los negocios y la educación hasta el gobierno, entre otros, controlen o supervisen el tráfico de red a Internet. [5]

- Minimice el tiempo de inactividad de los empleados que acceden a información en Internet que puede ser considerada cuestionable, inapropiada o no relacionada con el trabajo. Evite el uso inadecuado de los recursos de la red y la amenaza de acciones legales debido a accesos inapropiados.
- Incorpore un sólido nivel de seguridad en la red, que brinda protección frente a posibles ataques de spyware, malware, hacking y otras intrusiones. [5]

2.2.2. MPLS

MPLS (Multiprotocol Label Switching) es una arquitectura de red que garantiza QoS mediante la conmutación por etiquetas simplificando, considerablemente, la conmutación de paquetes. Este modelo de red surgió del trabajo conjunto de la IETF y fabricantes, como Cisco System, Toshiba, Ipsilon e IBM, para mejorar la compatibilidad entre la capa de Red (IP) y la capa de Enlace (ATM, Frame Relay, PPP) del modelo OSI. [8]

Según la figura 2 del modelo OSI, MPLS se ubicaría entre la capa 2 y capa 3 es decir opera entre la capa de enlace de datos y la capa de red del modelo OSI,

fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes, puede ser utilizado para transportar diferentes tipos de tráfico incluyendo tráfico de voz y de paquetes IP. [8]

Figura 2: *Descripción de la ubicación de MPLS en el modelo OSI*
Fuente: *Pagina web capas del Modelo OSI*

A la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM, conocido como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de “tunneling”), o bien, como una técnica para acelerar el encaminamiento de paquetes. [8]

El estándar MPLS viene por la necesidad de dotar las redes IP de nuevas capacidades, permitiendo mejoras y nuevas funcionalidades, destacando:

- Ingeniería de tráfico.
- Mecanismos de protección y recuperación frente a fallos.
- Redes privadas virtuales.
- Soporte de QoS y CoS para servicios que requieren flujos de datos de tiempo real.

- Integración de las redes IP con distintas tecnologías de nivel 2.

Además, tiene una serie de características fundamentales:

- Multiprotocolo: Es aplicable a cualquier protocolo de capa de red, e independiente de la capa de enlace utilizada.
- Conmutación por etiquetas. El reenvío (fordwarding) de los paquetes se realiza basándose en etiquetas con las que estos son marcados. Las etiquetas contienen información de encaminamiento y atributos de servicio.
- Se desacopla la función de reenvío con la de encaminamiento (routing).
- Tiene dos niveles funcionales en la red: frontera (edge) y núcleo (core). [8]

I. Estructura de una Red MPLS

Según la estructura MPLS acelera el transporte de paquetes IP, reemplazando el enrutamiento basado en las direcciones de capa 3 por una conmutación basada en etiquetas. Para ello, se inserta entre las cabeceras de los protocolos de capa 2 y capa 3 como se observa en la figura 3. La cabecera MPLS posee 32 bits de longitud, distribuidos en cuatro campos, cada uno con una función específica. [6]

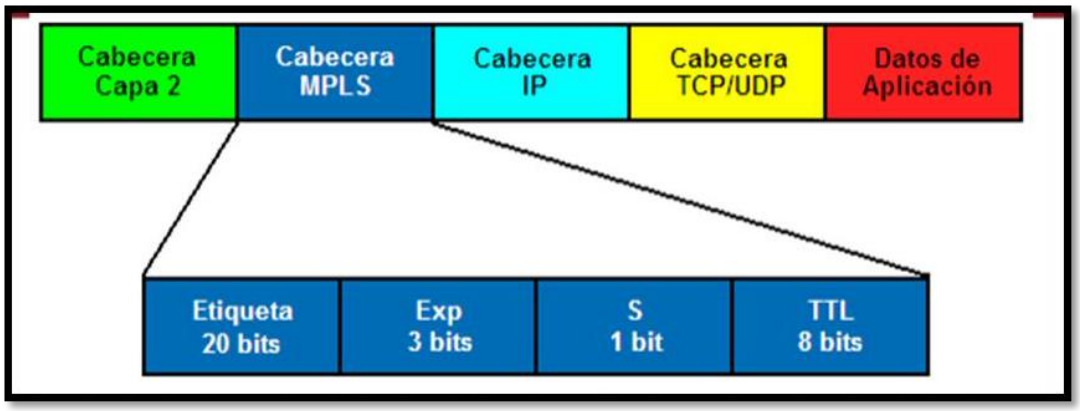


Figura 3: *Descripción de la cabecera de la Red MPLS*
Fuente: *Investigación de medición y análisis de tráfico en MPLS*

Para poder entender la tecnología MPLS debemos tener en conocimiento los siguientes términos:

- **LSR (Label Switching Router):** es un enrutador de alta velocidad en el corazón de la red MPLS, el cual debe soportar los protocolos de intercambio de etiquetas utilizando el protocolo de señalización de etiquetas adecuado. Permite conmutación de tráfico de datos a alta velocidad basado en las trayectorias establecidas, típicamente es un conmutador. Además, los enrutadores LSR en MPLS se clasifican en base a la dirección del flujo de datos, como enrutadores ascendentes (upstream, origen) o enrutamiento IP y participa en el establecimiento de las trayectorias de descendentes (downstream, destino). [6]
- **LER (Label Edge Router)**: Constituye el elemento de entrada y salida de la red MPLS como se muestra en la figura 4 y se encuentra en la frontera de esta. Se suele distinguir entre el equipo de entrada (ingress) y el de salida (egress). [6]

  A la entrada de la red se realiza la función de procesar los paquetes, seleccionarlos y aplicar la etiqueta que les corresponda.

  En la salida de la red se encarga de suprimir las etiquetas y reenviar los paquetes hacia el destino utilizando el reenvío de la capa 3. [6]

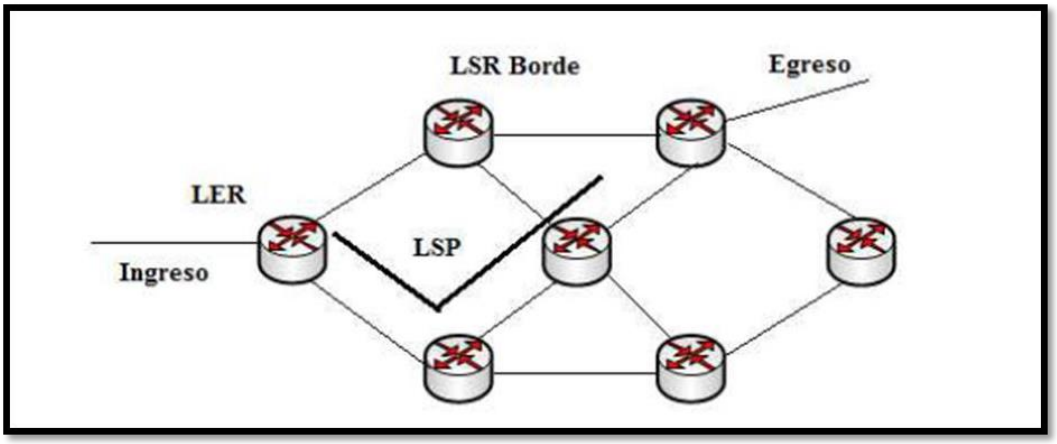


Figura 4: *Componentes de una Red MPLS.*
Fuente: *Tesis diseño de una Red para la universidad de Guayaquil*

- **FEC (Forwarding Equivalent Class):** Conjunto de paquetes que son tratados de la misma forma en el proceso de reenvío, siguiendo la misma ruta con independencia de los destinos finales. [6]

- **NHLFE (Next Hop Label Forwarding Entry):** Es una entrada a una tabla de envío en la que se indica la etiqueta del siguiente hop. Por lo tanto, cuando un paquete entra a una red MPLS, se le asigna un determinado FEC. [6]

- **Etiquetas MPLS**

  La etiqueta MPLS es un identificador dentro de la cabecera de los paquetes que permite clasificar un paquete con respecto a la FEC a la que pertenece. Esta asociación FEC-etiqueta puede no ser unívoca, y puede utilizarse la misma etiqueta para diferentes FECs (por ejemplo, para darle el mismo tratamiento a diferentes FEC dentro de un segmento de la red), o

pueden asociarse varias para la misma FEC (para realizar reparto de carga, por ejemplo). [6]

MPLS añade una sobrecarga adicional para la comunicación entre routers adyacentes, sumada a la propagación de los prefijos de enrutamiento se agregan las funcionalidades de mantenimiento de las LIB y LFIB junto con las tablas de adyacencia, generado un consumo de recursos extra. CEF, LDP y otros procesos contribuyen también al aumento de consumo de dichos recursos. [6]

La distribución de etiquetas se lleva a cabo a través de un protocolo de distribución de etiquetas, como LDP particularmente MPLS LDP.

Hay que tener en cuenta que la arquitectura de MPLS permite dos formas de propagar la información necesaria:

- ✓ Extender la funcionalidad de los protocolos existentes.
- ✓ Crear nuevos protocolos dedicados a la tarea de intercambios de etiquetas.

Extender la funcionalidad de un protocolo existente requiere bastante tiempo y esfuerzo, especialmente en BGP y OSPF. [6]

En una arquitectura MPLS la decisión de asignar una etiqueta en particular a un FEC es propiedad del LSR en cada host a lo largo del camino. El LSR anterior informa al siguiente LSR sobre etiquetas decididas para esa FEC, esto implica esencialmente que las etiquetas se asignan en sentido ascendente hacia el destino. [6]

El flujo del tráfico es un factor importante teniendo en cuenta que ocurre en un sentido bidireccional, es decir, que las etiquetas serán propagadas en ambas direcciones. Split Horizon hace que las etiquetas sean

distribuidas en sentido descendente evitando que se propaguen hacia el vecino que propago la etiqueta. La FIB está sujeta a las normas de horizonte dividido por defecto desde el punto de vista del enrutamiento, por lo tanto, la LIB y la LFIB también lo están. [6]

- **LSP (Label Switched Path):** Camino que se establece dentro de la red MPLS para todo tráfico de una misma FEC. Todos los paquetes identificados por esa FEC tendrán el mismo encaminamiento a través de la red. [6]
- **LIB:** Forma parte del Plano de control cuya base de datos es usada por el LDP para distribución de etiquetas. Cuando esto ocurre los prefijos IP son asociados con sus entradas de etiquetas locales y el próximo salto con la información aprendida anteriormente. [6]

Se observa según la definición de cada término, que la parte importante está en los equipos de entrada y salida denominados LSRs y LERs ocupan un lugar muy importante a la hora de definir la arquitectura MPLS.

II. MODO DE TRABAJO

Según la definición anterior lo primero es establecer un LSP entre los routers que van a transmitir el tráfico FEC. Los LSPs hacen las veces de túneles de transporte e incluyen los parámetros QoS específicos del flujo, que sirven para determinar la cantidad de recursos a reservar para el LSP y las políticas de desechado y la cola de procesos en cada LSR. [9]

Para intercambiar información los router MPLS usan los protocolos LDP o TDP. Cada flujo de tráfico FEC es asignado a una etiqueta particular. La asignación de nombres y rutas se puede realizar manualmente o bien a través del protocolo empleado. [9]

Cuando un paquete ingresa al dominio MPLS, el Edge LSR determina los servicios de red que requiere. Luego, asigna el paquete a una FEC y a un LSP particular, lo etiqueta y lo envía. Si no existe ningún LSP, el router de borde trabaja en conjunto con los demás LSRs para definirlo. Una vez dentro del dominio MPLS, en cada LSR que recibe el paquete se llevan a cabo los siguientes procesos:

- Se retira la etiqueta de entrada y se le añade la nueva etiqueta de salida al paquete.
- Se envía el paquete al siguiente LSR dentro del LSP.

Finalmente, El LSR de salida “abre” la etiqueta y lee el encabezado IP para enviarlo a su destino final. Como se indica en la figura 5:

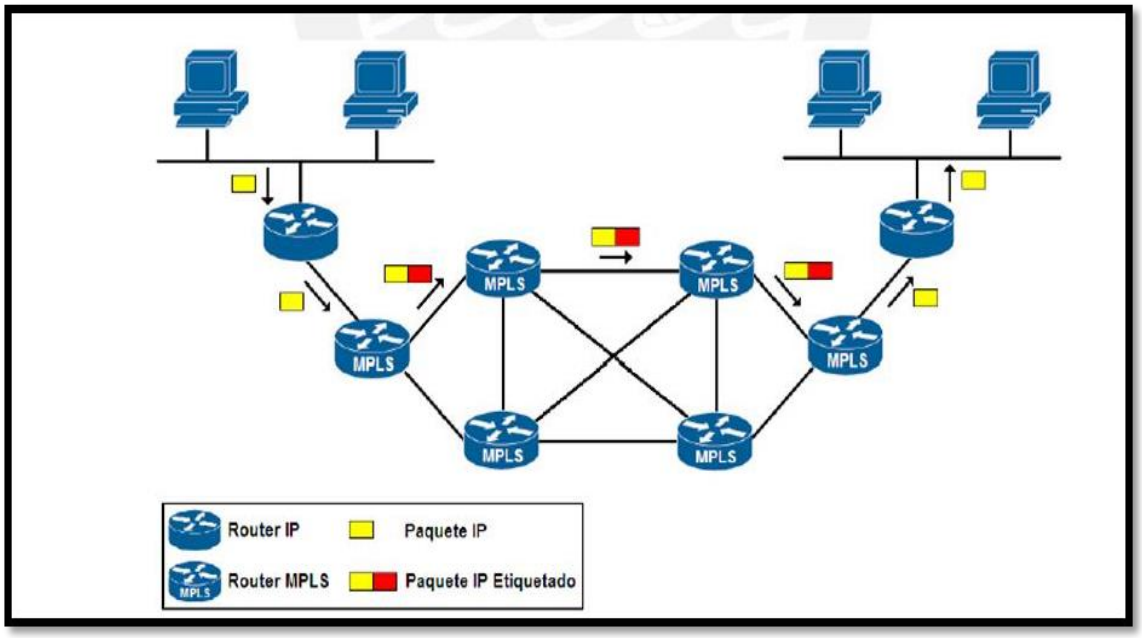


Figura 5: *Operación MPLS.*
Fuente: *Investigación de Redes VPN con tecnología MPLS.*

III. ARQUITECTURA MPLS

Los principales elementos que conforman una red MPLS son:

- **COMPONENTES LOGICOS:** La arquitectura MPLS comprende 2 componentes lógicos principales.
  - ✓ **Plano de control**: Hace el intercambio de etiquetas y rutas en capa 3.
  - ✓ **Plano de datos**: Reenvía los paquetes basados en las etiquetas. [9]

IV. Aplicaciones de la Red MPLS

La potencialidad de MPLS consiste en que ha dado origen a una serie de aplicaciones desde la Ingeniería de Tráfico hasta Redes Privadas Virtuales (VPN), que hacen del concepto de convergencia una realidad. [12]

A continuación, vamos a definir la aplicación que utilizaremos para este proyecto de ingeniería.

I. VPN- MPLS

Utiliza el método de conmutación de etiquetas multiprotocolo (MPLS) para crear redes privadas virtuales (VPN). MPLS-VPN es un método flexible para transportar y enrutar varios tipos de tráfico de red utilizando una backbone MPLS [12]

Hay tres tipos de VPN- MPLS desplegadas en redes hoy en día, mencionamos las dos más importantes para este proyecto:

- ✓ **VPN de Capa 2 (VPLS)**

  Servicio de LAN privada virtual, ofrece una tecnología de tipo “conmutador de nube”. La VPLS proporciona la capacidad de extender VLAN entre sitios. Se usa típicamente para enrutar tráfico de voz, de video y AMI entre la sede principal y las sedes remotas. [12]

- ✓ **VPN de capa 3 (VPRN)**

Red Enrutada privada Virtual, utiliza la capa 3 VRF (VPN/ Virtual Rounting and Forwarding y Reenvió virtual) para segmentar tablas de enrutamiento para cada cliente que utiliza el servicio. El cliente compara con el router (enrutador) del proveedor de servicios y las dos rutas de intercambio, que se colocan en una tabla de enrutamiento específica para el cliente. El multiprotocolo BGP es necesario en la nube para utilizar el servicio, lo que aumenta la complejidad de diseño e implementación. Normalmente no se despliegan en redes de servicios públicos debido a su complejidad; sin embargo, se podría usar una VPN de capa 3 para enrutar el tráfico entre las sedes remotas. [12]

CAPÍTULO III

DISEÑO E IMPLEMENTACIÓN DE LA RED

3.1. Descripción del Proyecto

Este proyecto de ingeniería está enfocado a la interconexión a nivel de WAN que van a tener las sedes remotas y la principal del Instituto del Mar del Perú (IMARPE) además de la propuesta de la seguridad administrada para IMARPE.

Para la solución a la problemática actual que presenta IMARPE se implementa una red segura bajo la plataforma VPN-MPLS con la cual integraremos sus servicios e interconectaremos sus sedes remotas, aprovechando sus bondades de MPLS; en la tabla 1 se puede ver la interconexión que va existir entre las sedes remotas y la principal, además una red de respaldo en ruta y nodo diferente (distinto punto geográfico) esta comunicación se implementara mediante o a través de la red MPLS del proveedor de servicios. Para la comunicación de todas las sedes se va a configurar una VRF (Virtual Routing Forwarding) que se crea en la Nube MPLS.

Específicamente en los router de tipo PE, la cual garantiza una conexión segura y libre de tráfico que no corresponda a la data del cliente.

Los enrutadores utilizados para el servicio de Internet y Red de Datos, considera las siguientes características técnicas:

- Los enrutadores y switches (que más adelante se detallara), soportan en todos sus puertos de comunicación velocidades de transmisión del orden de 10/100/1000BaseT, según lo solicitado por las Bases de la entidad en los Términos de Referencia.

A continuación, la tabla 1, resumen de los anchos de banda solicitados por el cliente de acuerdo con el Concurso Público N° 0004-2015 IMP/CE-Primera Convocatoria para las sedes central y remota.

Tabla 1: *Ancho de Banda Requerido*

ITEM	SEDES	SERVICIO	ROUTER	BW
1	Tumbes	RED MPLS (RPV)	JN SRX220	6Mbps
2	Piura – Paita	RED MPLS (RPV)	JN SRX220	6Mbps
3	Lambayeque - Chiclayo	RED MPLS (RPV)	JN SRX220	6Mbps
4	La Libertad – Trujillo	RED MPLS (RPV)	JN SRX220	6Mbps
5	Ancash – Chimbote	RED MPLS (RPV)	JN SRX220	6Mbps
6	Lima – Huacho	RED MPLS (RPV)	JN SRX220	6Mbps
7	Ica – Pisco	RED MPLS (RPV)	JN SRX220	6Mbps
8	Moquegua - ILO	RED MPLS (RPV)	JN SRX220	6Mbps
9	Puno – Puno	RED MPLS (RPV)	JN SRX220	6Mbps
10	Camaná - Arequipa	RED MPLS (RPV)	JN SRX220	6Mbps
11	Lima – Callao, Sede Central	RED MPLS (RPV)	JN SRX550	12Mbps
12	Lima – Callao, Sede Av. Argentina	RED MPLS (RPV)	JN SRX550	12Mbps
13	Lima – Callao, Sede Central (Principal y Contingencia)	SERVICIO DE INTERNET	JN SRX220	40Mbps
14	Lima – Callao, Sede Av. Argentina	SERVICIO DE INTERNET	JN SRX220	40Mbps

Fuente: *Términos de Referencia.*

En resumen, se propone una Topología basada en dos sedes; una sede principal (Av. A. Gamarra) y otra sede de contingencia (Av. Argentina) el internet dedicado en la sede principal será de 40 Mbps e interconectará con la sede de contingencia (Av. Argentina) por medio de un enlace de datos de 10Mbps y con las sedes remotas por enlaces de 6 Mbps. Teniendo en cuenta lo anterior, si aconteciera un accidente de cualquier tipo en alguna de las dos sedes (Av. A. Gamarra y Av. Argentina), el servicio seguiría ofreciéndose a través de la sede de contingencia. A este servicio de contingencia se le conoce como internet dedicado simétrico.

Se propone para cada sede (Principal y contingencia) una solución Activo-Pasivo con distinta ruta o nodo con el motivo de que no se pierda la conexión de datos e internet.

Los dos switches son usados como punto de interconexión por lo cual deben contar con gran capacidad de puertos y de acuerdo con el número y el tipo de estos, la capacidad de conmutación deberá ser calculada; es recomendada la alta disponibilidad a nivel de hardware.

Los tipos de puertos pueden variar de acuerdo con las capacidades de los puertos de las plataformas que se conectan a ellos.

En cuanto a los dos routers de acceso a la red MPLS al no ser estos los puntos de interconexión deberán contar con pocas interfaces, pero de gran capacidad; interfaces 10 Gigabitethernet se recomienda para ser conectados a los switches ya que a través de estas interfaces pasará todo el tráfico hacia el exterior recolectado por los dos switches. Debido a que estos routers tendrán que mantener la tabla de ruteo de toda la red se recomienda contar con una buena

capacidad de procesamiento y memoria RAM además de contar con alta disponibilidad a nivel de hardware.

Se implementará un hardware en la interconexión de datos de tal forma que pueda soportar servicios de video - conferencia, transmisión de archivos, de tal forma que, durante el tiempo de servicio, el rendimiento de la red de datos y salida a internet no sea perjudicado.

Así mismo implementaremos un servicio de seguridad administrada o seguridad perimetral donde se implementará servicios como monitoreo de equipos mediante la sede principal hacia las sedes remotas, administración de ancho de banda y análisis de tráfico en caso la red se sature, balanceo de internet dedicado, etc.

En la figura 6 se observa el diagrama total de la implementación en IMARPE.

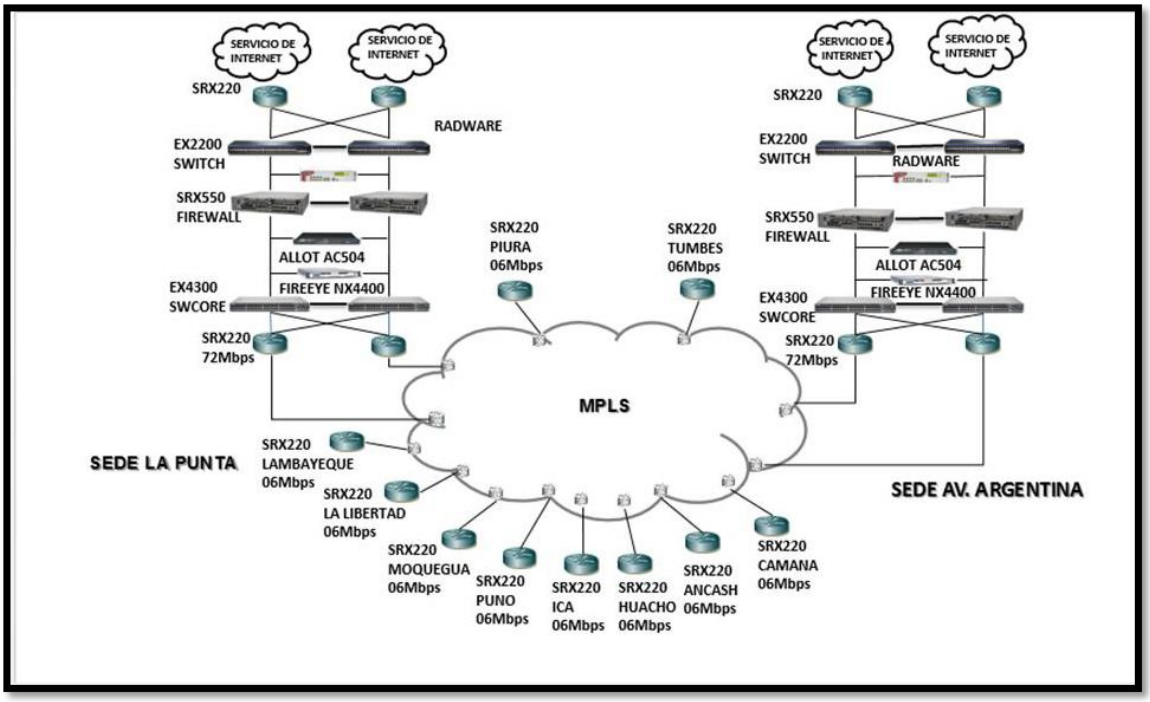


Figura 6: *Diagrama total de IMARPE*
Fuente: *Topología propuesta (Oferta Técnica)*

3.2. Diseño de la topología de red para IMARPE

Cuando se trata de diseñar una red, se deben considerar aspectos importantes ya que al momento de implementar es necesario asegurarse que el diseño escogido fue la topología más adecuada con los equipos de buen desempeño que puedan ofrecer, confiabilidad y robustez al INSTITUTO DEL MAR DEL PERU que deseen utilizar la red de un proveedor para el transporte de su información. Las consideraciones de diseño para la red se hacen pensando en una red mallada completa (Full mesh), construida con equipos de la plataforma Cisco Catalyst 4500, de tal forma que un proveedor con un diseño Full Mesh en su núcleo de red pueda ofrecer garantías de envío de información y que además cuente con caminos adicionales y redundantes según se dé el caso de que falle algún nodo en el núcleo de la nube como se muestra en la figura 7.

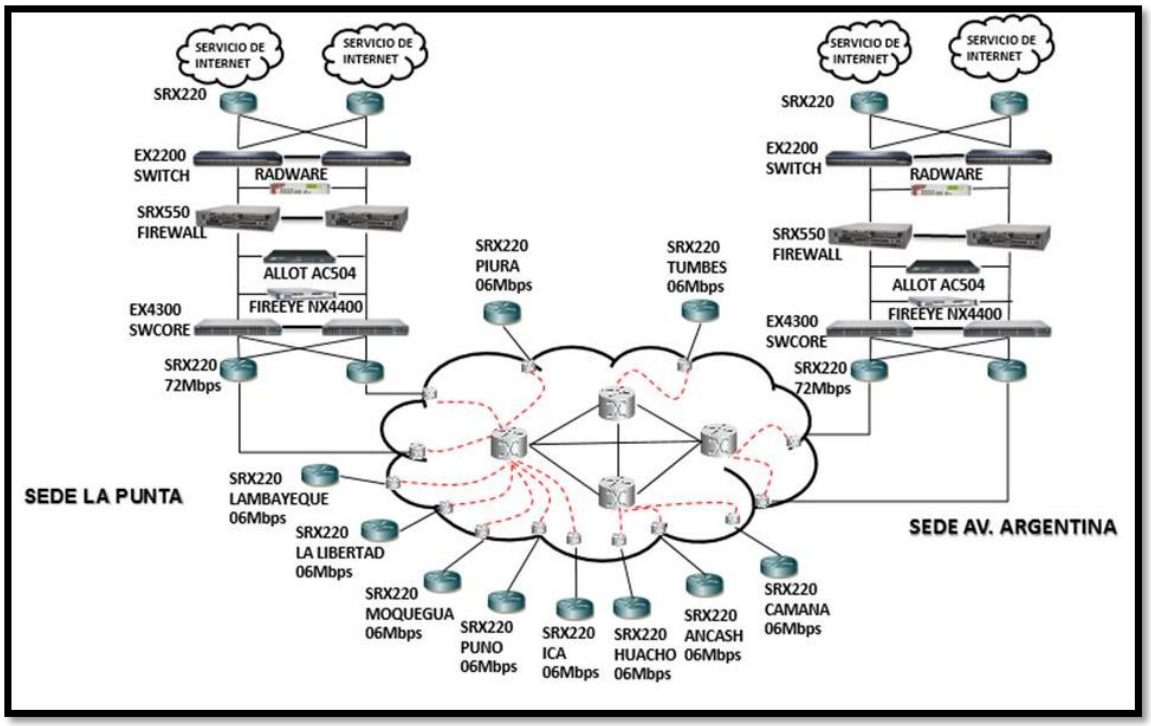


Figura 7: *TOPOLOGIA FULL MESH.*
Fuente: *Estructura Propia del operador*

3.2.1. Topología Full Mesh

Como se puede observar (Ver Figura 7), el arreglo de los equipos de red de un proveedor es una topología de malla completa en el Core. Este tipo de arreglo (full mesh) se caracteriza por tener todos sus nodos conectados entre sí para el intercambio de información. Dada su gran cantidad de redundancias en lo que se refiere a enlaces, este tipo de topologías es usual en los Backbones de los proveedores. Al existir redundancia de enlaces se garantiza una estructura de Backbone confiable, capaz de manejar grandes cantidades de información.

Para el diseño de una red MPLS, es necesario siempre estudiar la posibilidad de crear un núcleo mallado completo, dado que pueden existir situaciones en las que se presenten problemas en algún enlace y es necesario contar con respaldos que reemplacen a la ruta principal. Además, se tiene que considerar este tipo de topología para atender los requerimientos del IMARPE que demanda gran uso de ancho de banda mediante el uso de aplicativos que así lo requiera (Voz, Video, Datos) y que mediante la existencia de enlaces redundantes la información pueda ser direccionada por diferentes caminos según permite la Calidad de Servicio en la red del proveedor.

3.2.2. Alta Disponibilidad

Para la “Alta Disponibilidad” se ha planteado la utilización de protocolos que permitan a este proyecto encontrar una solución a la falla temporal que exista en la red. A continuación, se detalla los protocolos que utilizaremos.

a) IP FRR (Internet Protocol Fast Re-Route).

En redes IP tradicionales cuando ocurre una falla en la capa inferior del enlace, la interfaz física del router pasa a estado “down”, eso indica a las

capas superiores iniciar el proceso de recalcular rutas y hacer una actualización a sus tablas de ruteo, todo este proceso para seleccionar una ruta disponible puede llevar varios segundos, para la red de IMARPE que no toleran alto delay y altas tazas de pérdidas de paquetes, el tiempo de convergencia de los protocolos de ruteo es intolerante ya que eso podría ocasionar interrupciones en el servicio. IP FRR asegura que el sistema de reenvío conmute inmediatamente a la ruta que queda disponible (enlace de contingencia), lo cual hace que la interrupción del servicio en caso de falla sea imperceptible.

b) VRRP.

Este protocolo para utilizar es tolerante a fallas, y en general lo que hace es agrupar dos o más routers en un solo “router virtual”, en el caso de que el router que está como primario falle, algún router restante del grupo puede tomar el procesamiento del tráfico inmediatamente lo cual asegura la continuidad y confiabilidad de una comunicación.

c) GR.

Esta tecnología se emplea para asegurar el reenvío normal de tráfico y NSF durante el reinicio de protocolos de ruteo, dichos protocolos llegan a reiniciarse cuando las controladoras de los equipos conmutan.

En modo GR, el plano de reenvío continua con el envío de datos una vez que ha ocurrido un reinicio, y las acciones del plano de control, como el restablecimiento de las vecindades y el cálculo de rutas, no afectar al plano de reenvío. De esta manera la interrupción del servicio causada por la inestabilidad del ruteo es prevenida con lo que la confiabilidad de la red mejora.

d) Sistema Backbone.

Este sistema es el encargado principalmente de interconectar a la sede principal (La Punta) con la sede remota (Av. Argentina) y de recibir la ruta de default hacia Internet generada por el proveedor de servicios y advertida por los equipos del sistema de ISP y/o sistemas que requieran salir a Internet.

En este sistema es necesario aplicar políticas de ruteo para marcado de comunidades en BGP para marcar la ruta de default recibida del sistema de ISP, esto con el fin de balancear el tráfico hacia Internet en caso de falla.

Estos dos equipos por ciudad son de los elementos más importantes y podríamos llamarles el backbone de la red ya que si estos dos equipos fallan, el servicio entre ciudades es afectado completamente. Entre este sistema y el de acceso se corre un IGP; para el escenario propuesto de IMARPE el IGP usado es OSPF, el cual sirve de fuente de información para el protocolo MPLS TE.

OSPF es el encargado de anunciar las Loopback de servicio de todos los routers, con el que se establecen vecindades iBGP hacia los BGP RR para intercambiar rutas VPN además de servir de fuente de información para MPLS TE. Es sobre estos dos últimos protocolos (BGP & MPLS TE) donde se implementan los mecanismos de alta disponibilidad.

Los protocolos de alta disponibilidad implementados en este sistema son:

- BGP Route Policy para marcado de comunidades en BGP.
- MPLS TE FRR Link Protection.

I. BGP ROUTE POLICY

Empleado para marcado de comunidad en ruta de default para alta disponibilidad en la salida a Internet. Cuando el firewall del sistema de ISP advierte la ruta de default hacia el interior de la red, se tiene al igual que en el sistema de acceso, un esquema Dual-homed CE por lo cual con el fin de proveer redundancia a nivel de salida a Internet es necesario asignar un RD distinto para cada plano. Sin embargo, estas rutas al ser importadas a la VRF de Internet deben marcarse con comunidades para tener un criterio y punto de diferenciación al momento de escoger la salida primaria y la de backup a nivel de sedes. [14]

De esta forma los routers del sistema de acceso reciben rutas de default agrupadas en dos grupos de comunidades, de esta forma al aplicar una política en BGP podemos definir cuál salida será la primaria y cual secundaria por medio del atributo LOCAL PREFERENCE de BGP asignando un valor mayor a las rutas de default locales basado en el valor de la comunidad con la cual han sido marcadas.

II. MPLS TE FRR Link Protection

En el backbone es necesario tener un sistema de alta disponibilidad muy eficiente, ya que es donde cruza la mayor cantidad de tráfico y una falla en esta parte resulta en una afectación de servicio grave. Además de tener un mecanismo de alta disponibilidad, es necesario manejar el ancho de banda de los enlaces inteligentemente para evitar enlaces ociosos dentro del backbone. Tomando estas premisas como base, se toma MPLS TE como la mejor opción ya que cumple con ambas condiciones: Alta disponibilidad y uso inteligente del ancho de banda.

Así dentro del backbone MPLS se tiene una solución MPLS TE FRR con la cual se tiene protección a nivel de enlace, es decir, el tráfico es conmutado a un

camino secundario de forma rápida en caso de que falle algún enlace protegido, reduciendo así la cantidad de tráfico afectado cuando un enlace falla.

e) SISTEMA DE ISP

Este sistema es el encargado de dar salida al servicio de Internet de toda la red de IMARPE, sin este la red entera estaría aislada del resto del mundo.

Para tal propósito se tienen dos salidas redundantes cada una conectándose al proveedor de servicio. Del proveedor se recibe la tabla completa de Internet con propósito de optimizar el ruteo además de una ruta de default la cual es inyectada a la red por medio de OSPF.

Los dos firewalls son los encargados de realizar el filtrado de tráfico saliente y entrante (IPSEC o servicios que necesitan comunicarse desde el exterior) además de realizar NAT a las IP's públicas asignadas a la compañía. Entre ellos se corre un protocolo propietario que se encarga de mantener la tabla de sesiones igual en ambos firewalls, con el fin de que al haber una falla en uno de ellos la sesión no sea reiniciada.

3.3. Análisis de flujo para la Red de IMARPE

Después de la descripción y el diseño de la topología a continuación se realizará una explicación breve del funcionamiento en condiciones normales y en caso de que se presenten fallas en la solución.

3.3.1. Funcionamiento en condiciones normales

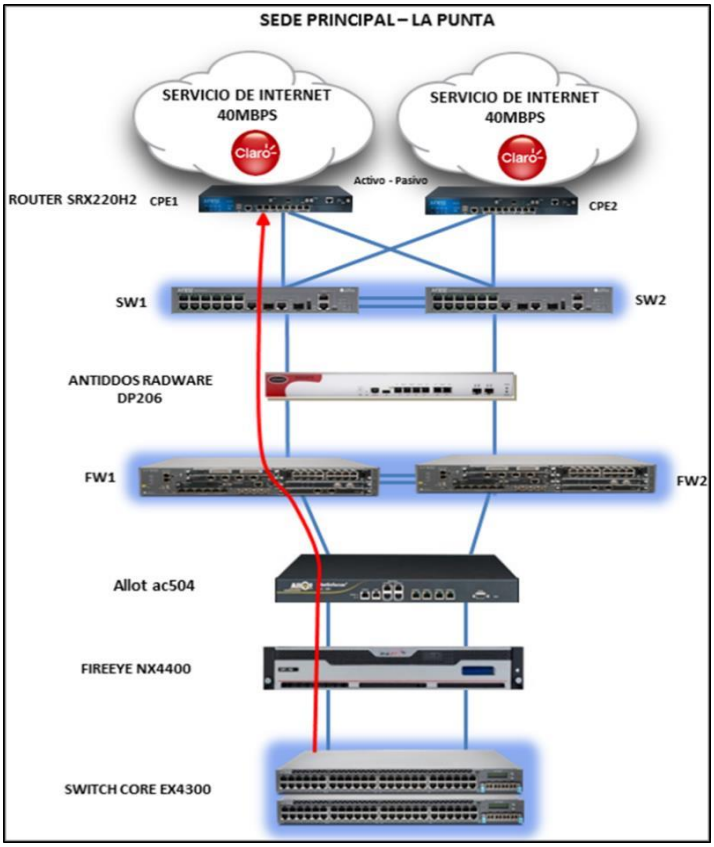


Figura 8: *Ruta de tráfico de Internet*
Fuente*: Topología de red (Oferta Técnica)*

En la figura 8 representa el flujo normal más importante dentro del proceso IP para tener funcionando en condiciones normales el servicio de internet lo cual se explica de la siguiente manera:

El Host envía un paquete.

Para los dos routers de acceso se configura una ruta de default a la IP del Virtual Gateway (VRRP entre ambos).

Al enviar un paquete hacia su Gateway, el router de acceso con el rol de máster recibe el paquete destinado a una IP ubicada en la nube de internet.

El router de acceso busca en su tabla de ruteo y encuentra cuatro rutas publicadas por cada router de backbone; estando las rutas locales de salida a

Internet marcadas con comunidad 1111 y las de la sede de contingencia con comunidad 2222.Para las rutas marcadas de la comunidad 2222 el router de acceso reduce el atributo de BGP “LOCAL PREFERENCE” a ochenta, quedando las rutas de la sede de contingencia con “LOCAL PREFERENCE” de cien, el cual es su default por lo que el router de acceso elije la ruta con menor valor.

Al ser el paquete enviado por una VRF, este lleva consigo una etiqueta de VPN por lo que para poder llegar al router es necesario que exista un LSP entre el router de acceso y el router de backbone.

Este LSP es el CR-LSP creado entre ambos routers, acceso y backbone, y debe existir uno en cada dirección, por lo que, para enviar el paquete, el router de acceso debe añadir la etiqueta de VPN y la etiqueta de MPLS TE. El paquete por medio de la etiqueta de MPLS TE es enrutado hasta el router de backbone donde la etiqueta de MPLS es quitada quedando sólo la etiqueta de VPN la cual indica al router la VRF que corresponde y hacia qué interfaz debe enviar el paquete.

El router de backbone después de haber quitado las dos etiquetas revisa la dirección destino del paquete y lo envía hacia el firewall, debido a que de este recibe la ruta de default.

El firewall recibe el paquete y revisa la inter-zona correspondiente para confirmar si el paquete está o no permitido pasar, si está permitido, el firewall cambia la dirección IP de origen por medio de NAT y registra la sesión en su tabla de sesiones la cual se encuentra sincronizada con el FW2 por medio del protocolo SSO.

El paquete es enviado hacia los routers de ISP los cuales reciben la tabla completa de BGP de los routers del proveedor de servicio y que corren a su vez IBGP entre ellos.

Entre los dos routers de ISP se decide cual es la mejor salida basada en los atributos advertidos por el proveedor de servicios. El paquete sale a Internet.

Después de haber llegado el paquete hasta su destino, es necesario regresar una respuesta para que la comunicación se establezca.

Pues bien, la respuesta sale hacia Internet, de acuerdo con los atributos de BGP como AS-PATH, elige la ruta.

Ya estando en la red, se tienen dos rutas para llegar al segmento, una por medio de la sede principal (LA PUNTA) y la otra por medio de contingencia (AV. Argentina), esto debido a la redundancia geográfica.

Elige la primera opción ya que esta cuenta con un AS-PATH menor y envía el paquete hacia el router de ISP de la sede principal.

Ya en el router de la sede principal, revisa su tabla de ruteo y ve que recibe la ruta hacia el segmento del Pool para NAT.

El firewall uno al advertir el segmento con menor costo recibe el paquete, esta vez no se revisa la inter-zona ya que el paquete es la respuesta a una sesión anteriormente permitida e iniciada registrada en su tabla de sesiones.

El firewall uno revisa su tabla de translaciones NAT y modifica en este caso la IP de destino a la IP original, revisa su tabla de ruteo y lo envía al router de backbone.

Ya en el router de backbone, al recibir el paquete en la interfaz ligada a la VRF de servicio de Internet, revisa la tabla de ruteo de esta VRF y encuentra dos rutas, una por cada router de acceso, ambas con igual métrica (atributos), sin embargo, por ser el router de acceso uno, el que tiene el menor costo en el IGP, toma esta ruta por medio de BGP siendo el next-hop la interfaz loopback del router uno.

Al ser un paquete de VRF, es necesario que exista un LSP que transporte el paquete hasta su destino, este LSP es el CR-LSP de MPLS TE que existe entre ambos equipos.

El router de backbone añade al paquete la etiqueta de VPN y la etiqueta de MPLS y lo envía por la interfaz que indica el LSP.

El paquete llega al router de acceso por medio de la etiqueta de MPLS y ahí se revisa la etiqueta de VPN para definir la VRF, el router de acceso revisa su tabla de ruteo y ve que la tiene directamente conectada así que lo envía por su subinterfaz conectada al Switch de acceso con el tag de la VLAN correspondiente.

El switch de acceso recibe el paquete con tag, revisa la VLAN a la que pertenece y lo transmite por el puerto correspondiente.

El host recibe la respuesta.

3.3.2. Funcionamiento en caso de pérdida en el ROUTER de acceso.

El router de acceso uno pierde poder y se apaga.

Al apagarse, el equipo deja de emitir la señalización de VRRP que corre entre los dos routers de acceso.

El router de acceso número dos al detectar que el router uno no responde a los mensajes, asume que el equipo está fuera de servicio y toma el rol de master, es decir, toma la IP virtual como propia y comienza a recibir el tráfico enviado por el equipo final hacia su GW.

El router de acceso número dos recibe el tráfico, revisa la dirección destino y al buscar en su tabla de ruteo encuentra que la opción más adecuada es la ruta

de default, ruta para la cual tiene cuatro opciones, las dos advertidas localmente y las dos advertidas por los routers de backbone de la sede AV. Argentina.

Sin embargo, las rutas anunciadas (sede principal) cuentan con una LOCAL PREFERENCE mejor, debido a las políticas aplicadas sobre las rutas anunciadas por la sede Av. Argentina.

De las dos rutas con menor LOCAL PREFERENCE, elige aquella con menor MED, que es heredada de la métrica con la cual se importó del proceso de OSPF. De esta forma el router de acceso elige la ruta anunciada por el router de backbone principal y busca el túnel que lo lleve a este, en este caso tiene un túnel directo al router de backbone principal. El router de acceso número dos tomas el paquete y lo etiqueta con las dos etiquetas correspondientes: etiqueta de VPN y etiqueta de MPLS y lo envía.

El router de backbone uno recibe el paquete y lo envía hacia el firewall de Internet, ya que de este recibe la ruta de default.

El proceso desde este punto hacia la ubicación en Internet a la cual se desea llegar sigue el mismo esquema ya explicado en condiciones normales.

Luego para el proceso de respuesta El análisis comenzará desde que el paquete llega al router de backbone uno, ya que el proceso hasta este punto sigue el mismo esquema explicado en el caso del funcionamiento normal.

Llegando el paquete al router de backbone uno, el router revisa su tabla de ruteo y encuentra que ya no existen dos rutas hacia este destino, puesto que uno de los routers de acceso está fuera de servicio, lo cual implica que su relación de BGP está en estado de desconexión.

El router de backbone toma entonces la única opción que tiene por BGP hacia el NEXTHOP que es router de acceso dos, revisa los LSP que tiene hacia ese NEXT-HOP y encuentra que tiene un túnel configurado hacia este destino.

El router de backbone uno toma el paquete IP y lo encapsula con dos etiquetas: etiqueta de VPN y etiqueta de MPLS y lo envía.

El paquete llega al router de acceso dos y al revisar la IP de destino se da cuenta que tiene el segmento directamente conectado a él, por lo cual el paquete es enviado hacia el switch con la dirección MAC de destino del host.

El paquete llega a su destino. Se muestra en la figura 9:

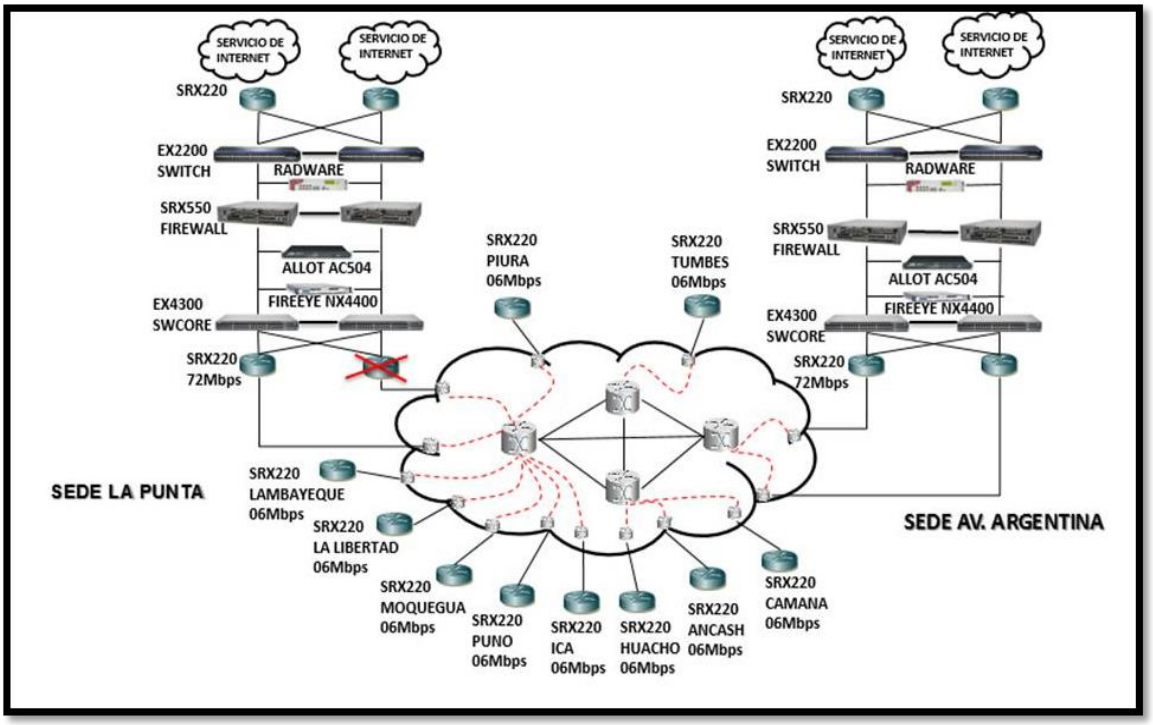


Figura 9: *Diseño en caso de fallas.*
Fuente*: Topología de red propuesta*

3.3.3. Funcionamiento en caso de pérdida de gestión en el SWITCH.

Para el caso de pérdida de poder o falla en el switch de acceso, se tiene un escenario donde se requiere que el equipo terminal conectado al switch tenga un sistema de redundancia a nivel de hardware que sea capaz de detectar la pérdida de conexión física hacia el switch dañado y conmutar el tráfico hacia la tarjeta que conecta con el switch activo.

A nivel de capa dos, la pérdida de poder de un switch significa la fragmentación del dominio de broadcast y aislamiento entre ambos routers los cuales se comunican por medio del troncal que existe entre ambos switches.

Por tanto, al tener una falla en cualquiera de los dos switches, se tiene un corte en la señalización del protocolo de redundancia VRRP lo cual se refleja en la convergencia del protocolo tomando el router SLAVE el papel de MASTER dando salida al tráfico generado por el equipo conectado al switch.

Para la carga del Switch el tráfico en el equipo conectado es conmutado al puerto secundario y entregado al switch activo el cual lo entrega al nuevo router MASTER que a partir de ese punto entrega el tráfico a la red MPLS.

Para el proceso de descarga la falla se refleja de inmediato, esto debido a que el router uno deja de advertir el segmento de red que se encontraba configurado en las interfaces conectadas al switch afectado, así, el tráfico de descarga llega al equipo final por medio del router dos. Se muestra en la figura 10

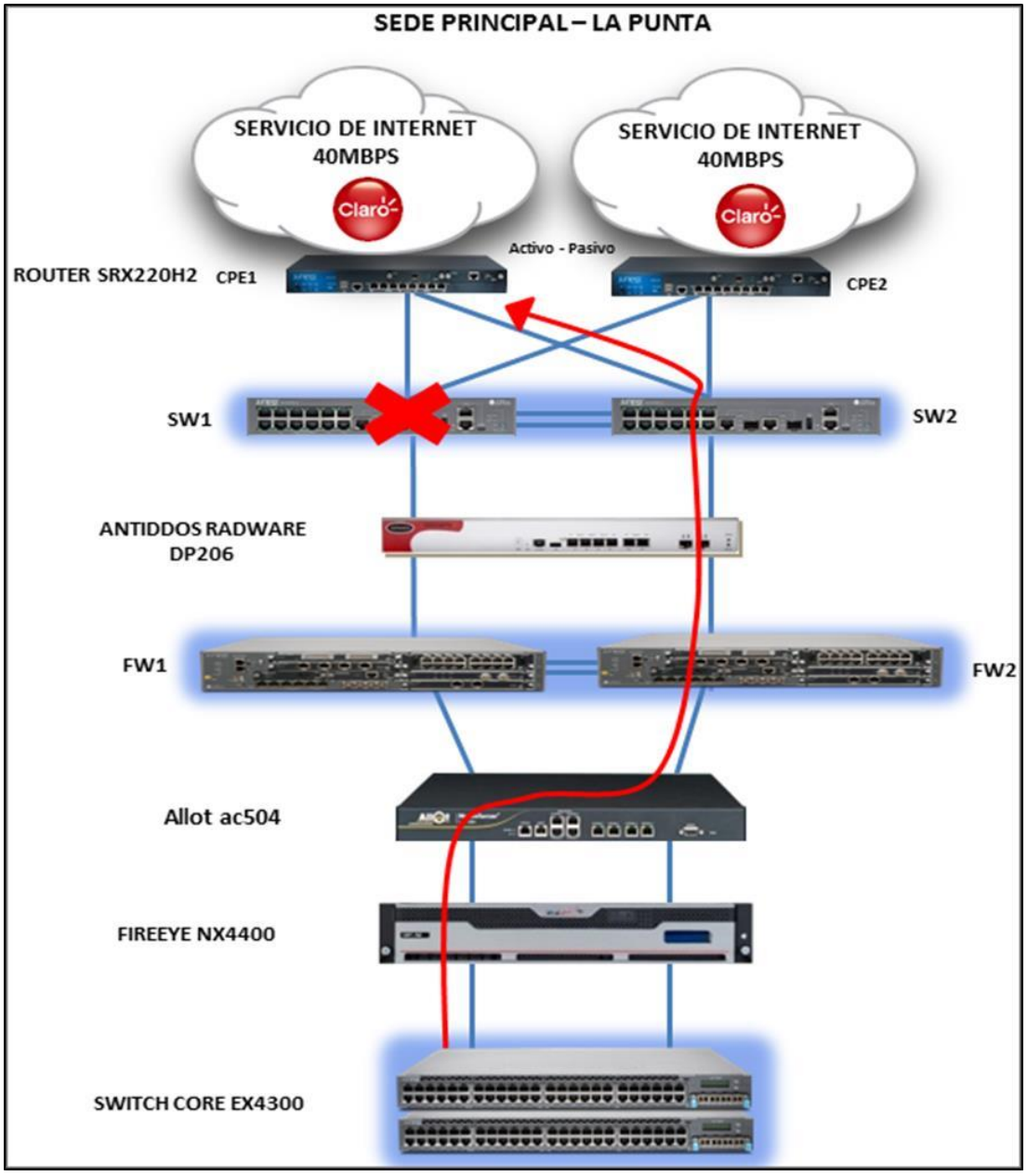


Figura 10: *Topología de red en caso de falla del switch*
Fuente: *Topología propuesta (Oferta Técnica)*

3.3.4. Funcionamiento en caso falle el equipo RADWARE.

En caso falle el equipo RADWARE, se activa su característica de bypass haciendo que no pierda conectividad hacia internet y por ende no caiga el servicio, como se muestra en la figura 11.

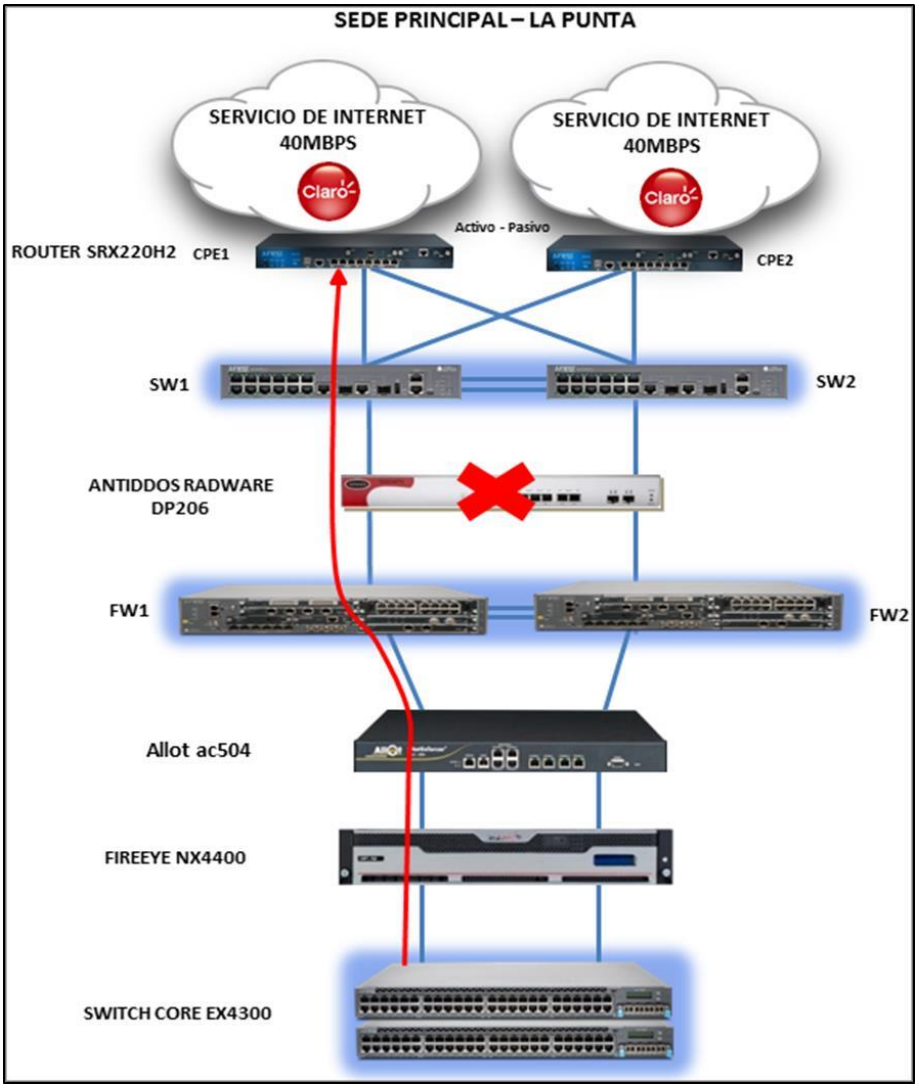


Figura 11: *Topología de red en caso de falla del equipo RADWARE.*
Fuente: *Topología propuesta (Oferta Técnica)*

3.3.5. Funcionamiento en caso falle el FIREWALL

En caso de mal funcionamiento del FIREWALL se observa de la siguiente manera:

El tráfico llega a los routers de acceso desde el equipo conectado a los switches de acceso buscando lograr llegar a Internet.

El router de acceso revisa su tabla de ruteo y nota que el router principal, no anuncia más la ruta de default debido a que el equipo que se la anunciaba, el firewall de ISP, está fuera de servicio.

Por lo anterior el router de acceso envía el tráfico hacia la segunda opción que tiene para salir a Internet que es por medio del router dos el cual recibe todavía la ruta de default por medio del firewall de ISP el cual no ha sufrido afectación.

El tráfico llega al router dos y es procesado y enviado al firewall dos el cual a su vez lo envía al router principal y de ahí el tráfico sale a Internet.

Una vez que se completó la primera etapa la siguiente ruta seria:

El tráfico proveniente desde Internet llega a los routers de ISP los cuales solo tienen una ruta posible por medio del firewall de ISP dos ya que el firewall de ISP uno se encuentra fuera de servicio.

El tráfico es enviado al firewall de ISP 2 (FW 2) y este lo envía al router dos, este revisa su tabla de ruteo y observa que tiene dos posibles NEXT-HOP (router de acceso 1 y router de acceso 2), sin embargo, por métricas de IGP elige el NEXT-HOP router de acceso 2.

El tráfico llega al router de acceso 2 y este al tener el segmento de destino directamente conectado lo envía a nivel capa 2 por la VLAN correspondiente hacia el equipo origen.

El flujo es completado correctamente, como se muestra en la figura 12.

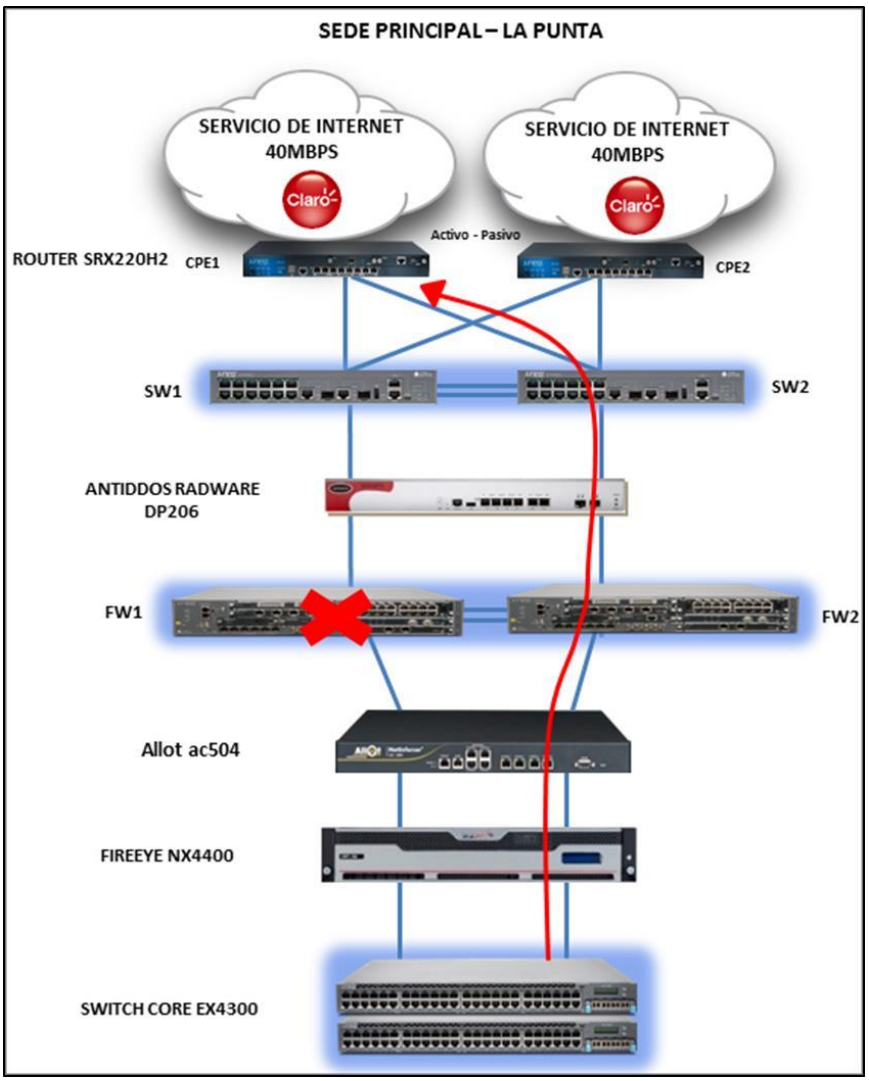


Figura 12: *Topología de red en caso de falla del FIREWALL*
Fuente*: Topología propuesta (Oferta Técnica)*

3.3.6. Funcionamiento en caso falle el equipo ALLOT.

En caso falle el ALLOT o el FIREEYES, el flujo de tráfico no se verá interrumpido por la funcionalidad Bypass que tienen dichos equipos como se muestra en la figura 13.

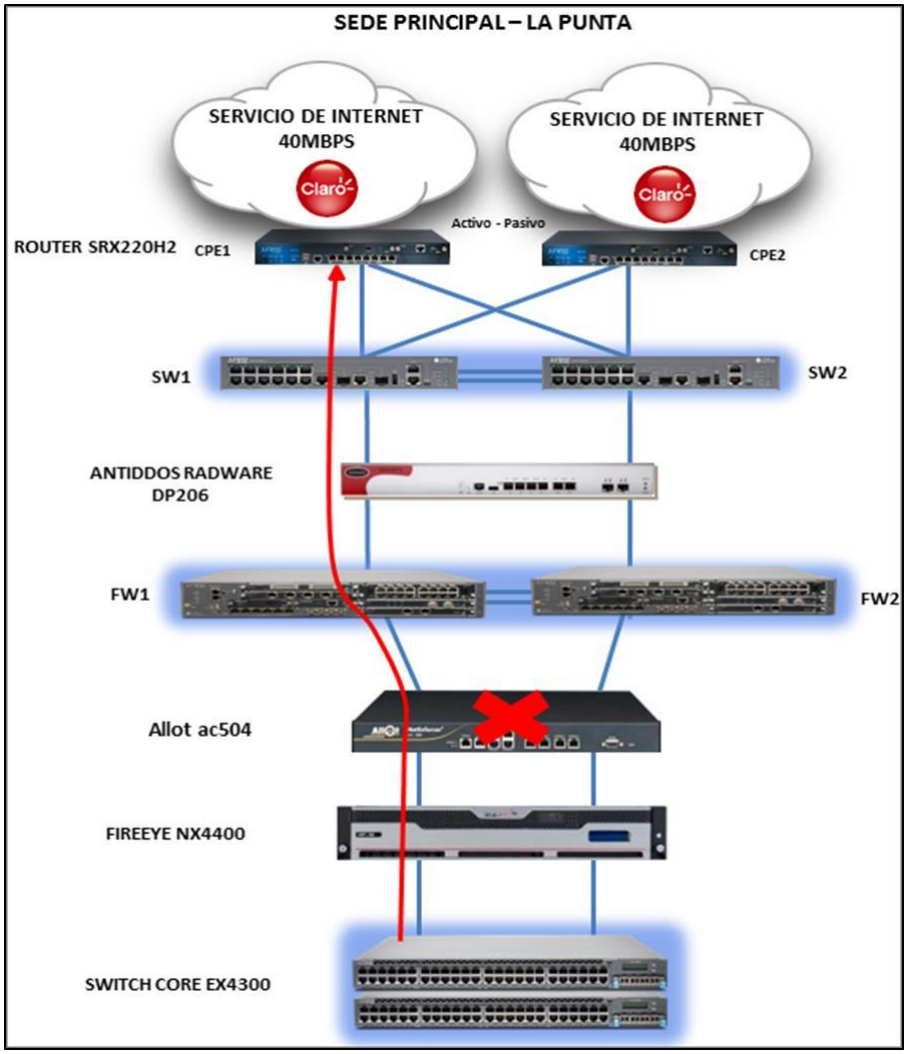


Figura 13: *Topología de red en caso de falla del equipo ALLOT*
Fuente: *Topología propuesta (Oferta Técnica)*

3.3.7. Funcionamiento en caso de falla, pérdida de poder en ambos Router de Internet

En este análisis funcional describiremos el proceso en el cual se tiene fuera de servicio ambos routers por que dejaron de recibir del ISP las rutas por default y por consiguiente se dejan de advertir las rutas de default a los firewall de Internet.

El tráfico llega a los routers de acceso los cuales han dejado de recibir la ruta de default por parte de ambos router de la backbone debido a que ambos equipos que se las anunciaban (firewall -sede principal) dejaron de recibirlas por parte de los routers de Internet.

Sin embargo, en la red MPLS los routers de acceso, sede de contingencia, aún reciben dos rutas de default advertidas por los dos routers de backbone de la sede de contingencia pero con una "**LOCAL PREFERENCE**" menor.

De ambas rutas el router de acceso revisa cual NEXT-HOP representa una menor métrica y envía el tráfico al router de backbone relacionada a la sede de contingencia.

El tráfico en el router de backbone de la sede de contingencia es enviado usando la ruta de default advertida por el firewall de ISP de su misma sede.

El tráfico en el firewall de ISP de la sede de contingencia es "NATeado" con el segmento propio y enviado a Internet.

Lo anterior protege el flujo de datos y evita la pérdida de servicio sin embargo también representa un aumento en el uso del ancho de banda y procesamiento en los equipos de la sede de contingencia.

El tráfico al haber sido enviado a Internet con las IP's públicas de la sede de contingencia, retorna por medio también de los routers de ISP de la sede de contingencia.

El router de ISP de la sede de contingencia no se percata que el tráfico pertenece a la sede principal ya que para él lo que pasa detrás del NAT es transparente así que envía el tráfico hacia el firewall de ISP de la sede principal.

Este revisa la IP de destino la cual coincide con los segmentos advertidos por el router de backbone principal que pertenecen a la sede de contingencia.

El tráfico recibido en el router de backbone de la sede de contingencia es enviado al router de acceso de la sede principal por medio del túnel TE que existe entre ellos esto después de haber revisado su tabla de ruteo y notar que el prefijo existía en su tabla con NEXT-HOP el router de acceso de la sede de contingencia.

El tráfico llega al router de acceso de la sede principal el cual de forma normal envía el tráfico al equipo origen cuyo segmento él tiene directamente conectado.

El tráfico se completa satisfactoriamente como se muestra en la figura 14.

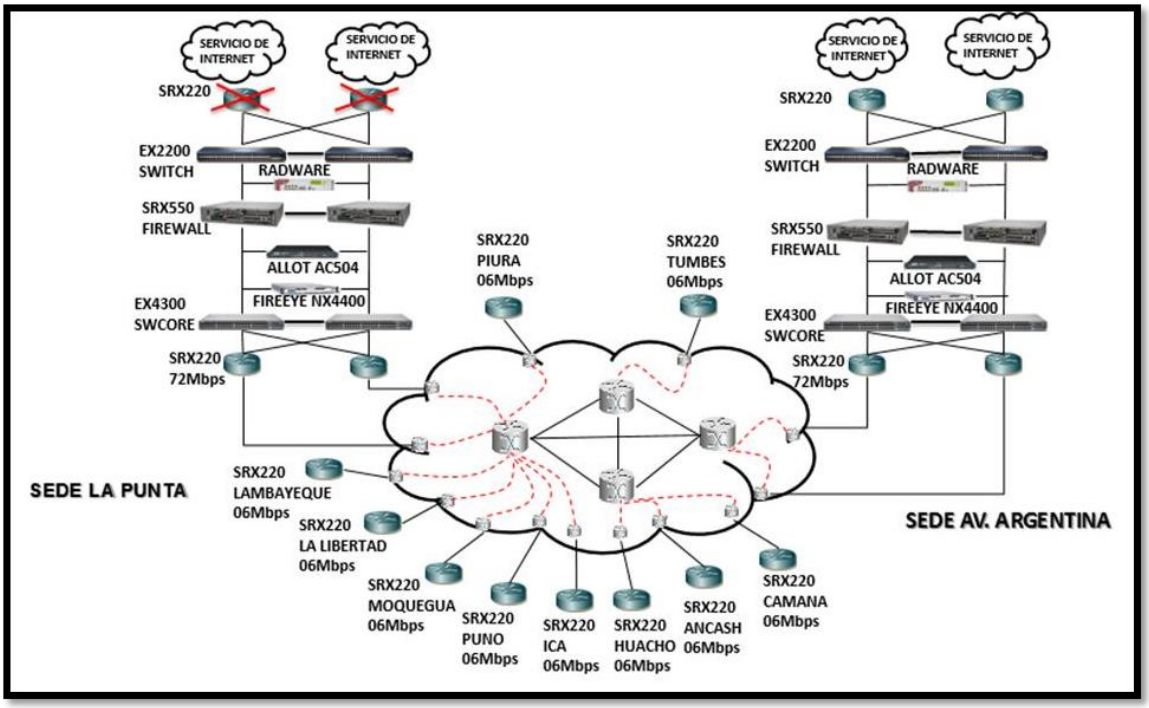


Figura 14: *Topología de red, tráfico hacia las sedes remotas.*
Fuente: *Topología propuesta (Oferta Técnica)*

3.4. Implementación del servicio de Seguridad Administrada e Interconexión de Datos.

Como resultado tenemos las fases de implementación del servicio, implementación, protocolo de pruebas y fotografía de los equipos instalados.

3.4.1. Cronograma de implementación

De acuerdo con las fechas establecidas en las bases integradas se tiene el siguiente cronograma que nos servirá para tener organizado todo el proceso desde la aceptación del servicio hasta la validación por parte del cliente.

***Tabla 2*:** Cronograma de implementación

ITEM	ACTIVIDAD	AREA RESPONSABLE	Abr-15				May-15				Jun-15				Jul-15			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Consolidado del estudio Técnico	Planificación																
2	Aprobación, solicitud de la inversión	Empresas																
3	Emisión de Orden de Compra																	
4	Importación de Equipos	Producto																
5	Diseño Planta Externa	Planificación																
6	Licencias Planta Externa	STC																
8	Instalación Equipos, Configuración y Pruebas	STC																

Fuente: Oferta Técnica

3.4.2. CHECKLIST

Checklist de validación de servicio para la sede remota de CAMANA.

Se le hace las pruebas respectivas como saturación y conectividad para validar el servicio con el cliente.

Se verifica la configuración a través del comando show no-more como se muestra en la figura 15.

CHECKLIST DE VALIDACIÓN DE SERVICIO RPVL 6Mps
INSTITUTO DEL MAR DEL PERU (IMARPE) – SEDE CAMANA
PROY: 3695876 SOT: 21338161 CID: 4329745

VERIFICACION DE LA CONFIGURACION

SHOW CONFIGURATION:

Muestra la configuración del equipo router:

```
show | no-more
## Last changed: 2016-05-11 04:40:05 UTC
version 12.1X46-D40.2;
system {
    host-name R_Imarpe_LabCamana;
    authentication-order [ tacplus password ];
    root-authentication {
        encrypted-password "$1$Rd5AnfHr$k9MAB1SuS9yRuP7OmANFN/"; ## SECRET-DATA
    }
    tacplus-server {
        10.192.17.27 {
            secret "$9$hIjceM8LNYgJYgGiq.F3BIEcSebwg4JDKMDk.mF3p0BIEydVY"; ##
SECRET-DATA
            source-address 10.233.26.65;
        }
    }
    tacplus-options {
        service-name telmex-junos;
    }
    accounting {
        events [ login change-log interactive-commands ];
        destination {
```

Figura 15: *Checklist de validación*
Fuente: *informe de validación.*

Se verifica la conectividad por medio del Ping como se muestra en la figura 16 y 17.

VERIFICACIÓN DE CONECTIVIDAD

SHOW ROUTE:

```
[edit]
NOC@R_Imarpe_LabCamana# run show route

inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 00:05:40
                    > to 10.116.40.93 via ge-0/0/0.0
10.116.40.92/30    *[Direct/0] 00:05:40
                    > via ge-0/0/0.0
10.116.40.94/32    *[Local/0] 00:07:36
                      Local via ge-0/0/0.0
10.233.26.65/32    *[Direct/0] 00:08:16
                    > via lo0.0
172.16.10.0/24     *[Direct/0] 00:02:34
                    > via vlan.2
172.16.10.2/32     *[Local/0] 00:07:45
                      Local via vlan.2
```

PING WAN:

Muestra la conectividad entre el router y el equipo de acceso (Red de CLARO).

```
[edit]
NOC@R_Imarpe_LabCamana# run ping 10.116.40.93 rapid count 1000
PING 10.116.40.93 (10.116.40.93): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 10.116.40.93 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 4.550/5.452/33.134/1.635 ms
```

Figura 16: *Verificación de conectividad.*
Fuente: *Informe de validación*

PING LAN:

Muestra la conectividad entre el router y un equipo del cliente (Servidor de correos, servidos de datos, etc)

```
[edit]
NOC@R_Imarpe_LabCamana# run ping 172.16.10.100 rapid count 1000
PING 172.16.10.100 (172.16.10.100): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.10.100 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.598/2.342/6.727/0.497 ms
```

PING LAN TO LAN:

Muestra la conectividad entre la sede que se está instalando y una sede remota o la principal.

```
[edit]
NOC@R_Imarpe_LabCamana# run ping 192.168.50.1 source 172.16.10.2 rapid count 1000
PING 192.168.50.1 (192.168.50.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
--- 192.168.50.1 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 17.287/18.061/42.875/1.258 ms
```

Figura 17: *Muestra de conectividad*
Fuente: *Informe de Validación.*

Se observa el consumo de ancho de banda de acuerdo a la interface a verificar como se indica en la figura 18.

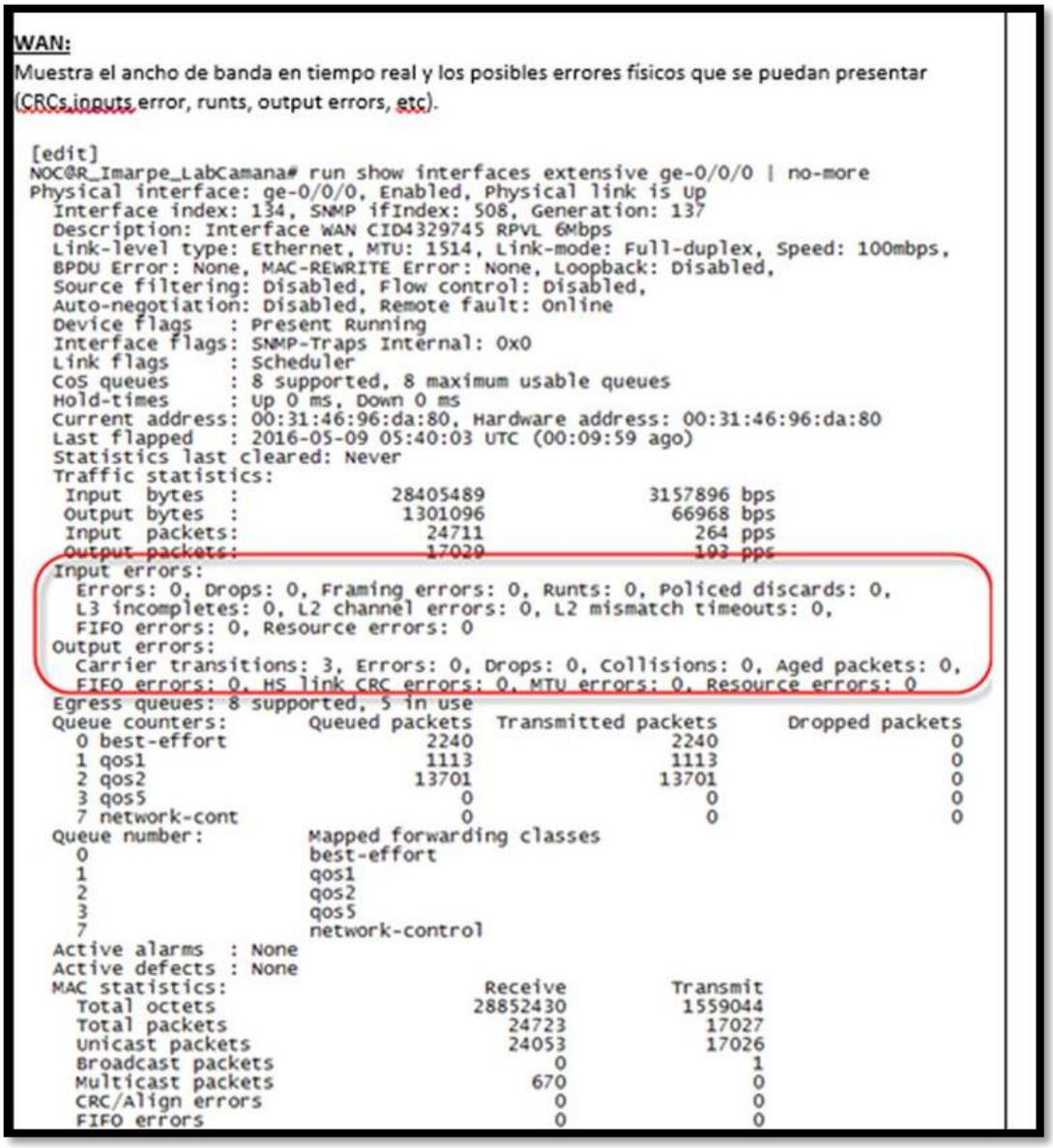
SHOW INTERFACES QUEUE FE-0/0/0:

Muestra el consumo de ancho de banda por calidad de servicio en tiempo real en la parte WAN.

```
[edit]
NOC@R_Imarpe_LabCamana# run show interfaces queue ge-0/0/0| no-more
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 134, SNMP ifIndex: 508
  Description: Interface WAN CID4329745 RPVL 6Mbps
Forwarding classes: 8 supported, 5 in use
Egress queues: 8 supported, 5 in use
Queue: 0, Forwarding classes: best-effort
  Queued:
    Packets              :                2240                    0 pps
    Bytes                :              221880                    0 bps
  Transmitted:
    Packets              :                2240                     0 pps
    Bytes                :              221880                    0 bps
    Tail-dropped packets :                   0                    0 pps
    RED-dropped packets  :                   0                    0 pps
     Low                 :                   0                    0 pps
     Medium-low          :                   0                    0 pps
     Medium-high         :                   0                    0 pps
     High                :                   0                    0 pps
    RED-dropped bytes    :                   0                    0 bps
     Low                 :                   0                    0 bps
     Medium-low          :                   0                    0 bps
     Medium-high         :                   0                    0 bps
     High                :                   0                    0 bps
Queue: 1, Forwarding classes: qos1
  Queued:
    Packets              :                1113                  156 pps
    Bytes                :            17689312              1627500 bps
  Transmitted:
    Packets              :                1113                  156 pps
    Bytes                :            17587261              1627500 bps
    Tail-dropped packets :                   0                    0 pps
    RED-dropped packets  :                   0                    0 pps
     Low                 :                   0                    0 pps
     Medium-low          :                   0                    0 pps
     Medium-high         :                   0                    0 pps
     High                :                   0                    0 pps
    RED-dropped bytes    :                   0                    0 bps
     Low                 :                   0                    0 bps
     Medium-low          :                   0                    0 bps
     Medium-high         :                   0                    0 bps
     High                :                   0                    0 bps
Queue: 2, Forwarding classes: qos2
  Queued:
    Packets              :              565612                  563 pps
    Bytes                :           176695216              4196541 bps
  Transmitted:
    Packets              :              565316                  163 pps
    Bytes                :           176596245              4196541 bps
    Tail-dropped packets :                   0                    0 pps
    RED-dropped packets  :                   0                    0 pps
```

Figura 18: *Consumo de ancho de banda en tiempo real.*
Fuente: *Informe de Validación.*

Se muestra los posibles errores de acuerdo a las interfaces analizadas como se indica en la figura 19.



WAN:

Muestra el ancho de banda en tiempo real y los posibles errores físicos que se puedan presentar (CRCs,inputs error, runts, output errors, etc).

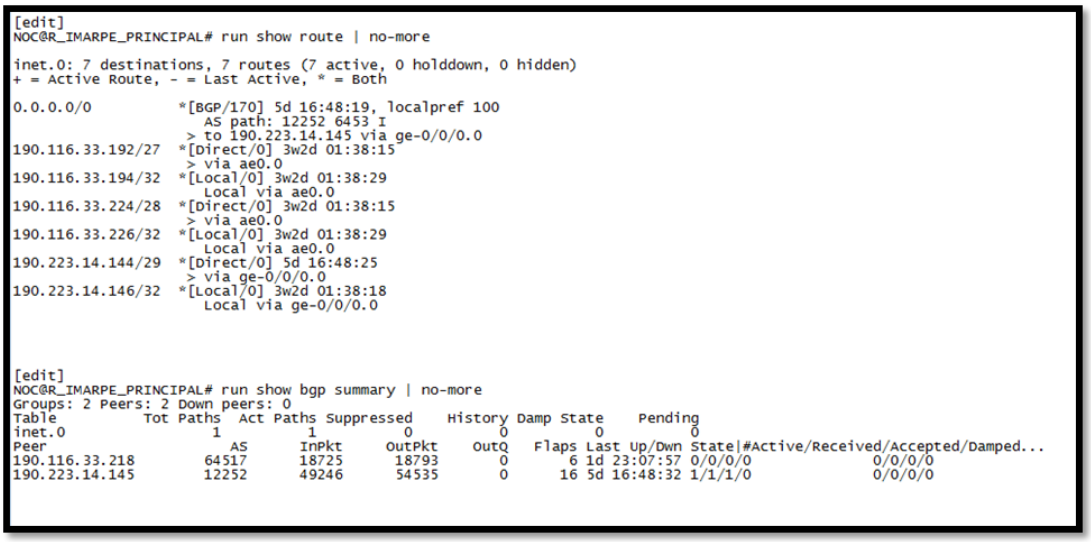
```
[edit]
NOC@R_Imarpe_LabCamana# run show interfaces extensive ge-0/0/0 | no-more
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 134, SNMP ifIndex: 508, Generation: 137
  Description: Interface WAN CID4329745 RPVL 6Mbps
  Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 100mbps,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled,
  Auto-negotiation: Disabled, Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x0
  Link flags     : Scheduler
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:31:46:96:da:80, Hardware address: 00:31:46:96:da:80
  Last flapped   : 2016-05-09 05:40:03 UTC (00:09:59 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :              28405489                3157896 bps
   Output bytes  :               1301096                  66968 bps
   Input  packets:                 24711                    264 pps
   Output packets:                 17029                    193 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
    L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
    FIFO errors: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 3, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
    FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
  Egress queues: 8 supported, 5 in use
  Queue counters:       Queued packets  Transmitted packets      Dropped packets
    0 best-effort                2240                 2240                   0
    1 qos1                       1113                 1113                   0
    2 qos2                      13701                13701                   0
    3 qos5                          0                    0                   0
    7 network-cont                  0                    0                   0
  Queue number:         Mapped forwarding classes
    0                   best-effort
    1                   qos1
    2                   qos2
    3                   qos5
    7                   network-control
  Active alarms  : None
  Active defects : None
  MAC statistics:                      Receive         Transmit
    Total octets                      28852430          1559044
    Total packets                        24723            17027
    Unicast packets                      24053            17026
    Broadcast packets                        0                1
    Multicast packets                      670                0
    CRC/Align errors                         0                0
    FIFO errors                              0                0
```

Figura 19: *Consumo en tiempo real y con verificación de errores.*
Fuente: *Informe de Validación.*

Estas pruebas se realizaron en forma similar a todas las sedes remotas; con estas pruebas podemos observar que el servicio presenta conectividad y es tolerante a la saturación del tráfico.

Se realizó el protocolo de pruebas para la sede principal de los ROUTER de acceso a Internet de 40 Mbps obteniendo los siguientes resultados:

- ✓ El comando **run show route | no-more**, con este comando se comprueba que todas las rutas se encuentren en la tabla de enrutamiento como se muestra en la figura 20.



```
[edit]
NOC@R_IMARPE_PRINCIPAL# run show route | no-more

inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[BGP/170] 5d 16:48:19, localpref 100
                      AS path: 12252 6453 I
                    > to 190.223.14.145 via ge-0/0/0.0
190.116.33.192/27  *[Direct/0] 3w2d 01:38:15
                    > via ae0.0
190.116.33.194/32  *[Local/0] 3w2d 01:38:29
                      Local via ae0.0
190.116.33.224/28  *[Direct/0] 3w2d 01:38:15
                    > via ae0.0
190.116.33.226/32  *[Local/0] 3w2d 01:38:29
                      Local via ae0.0
190.223.14.144/29  *[Direct/0] 5d 16:48:25
                    > via ge-0/0/0.0
190.223.14.146/32  *[Local/0] 3w2d 01:38:18
                      Local via ge-0/0/0.0



[edit]
NOC@R_IMARPE_PRINCIPAL# run show bgp summary | no-more
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0                 1          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|#Active/Received/Accepted/Damped...
190.116.33.218        64517      18725      18793       0       6 1d 23:07:57 0/0/0/0                0/0/0/0
190.223.14.145        12252      49246      54535       0      16 5d 16:48:32 1/1/1/0                0/0/0/0
```

***Figura 20**: Validación de las rutas en la tabla.*
***Fuente:** Informe de Validación.*

- ✓ Se realizó prueba de conectividad desde el Router de acceso realizando ping a una IP pública de internet como se muestra en la figura 21.

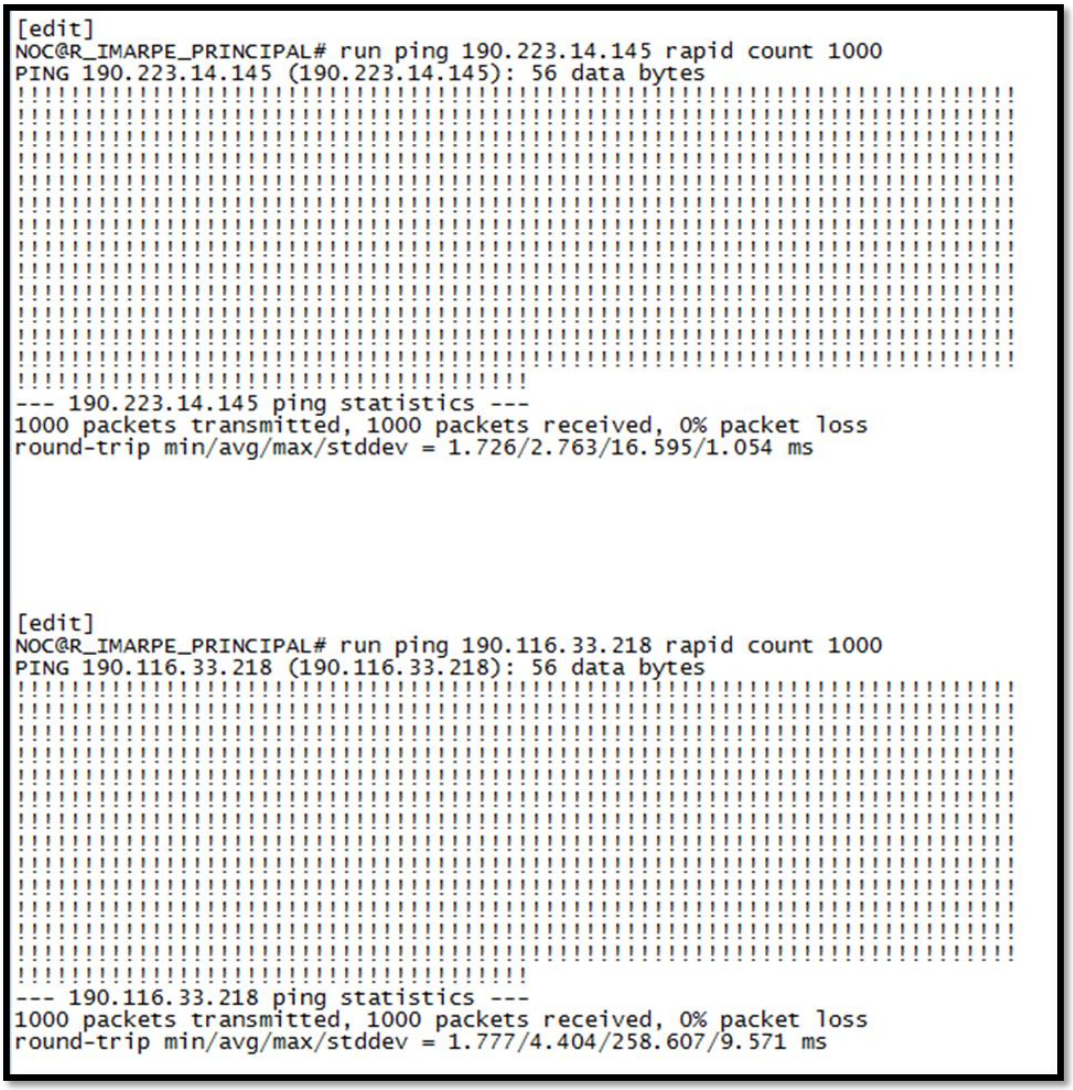


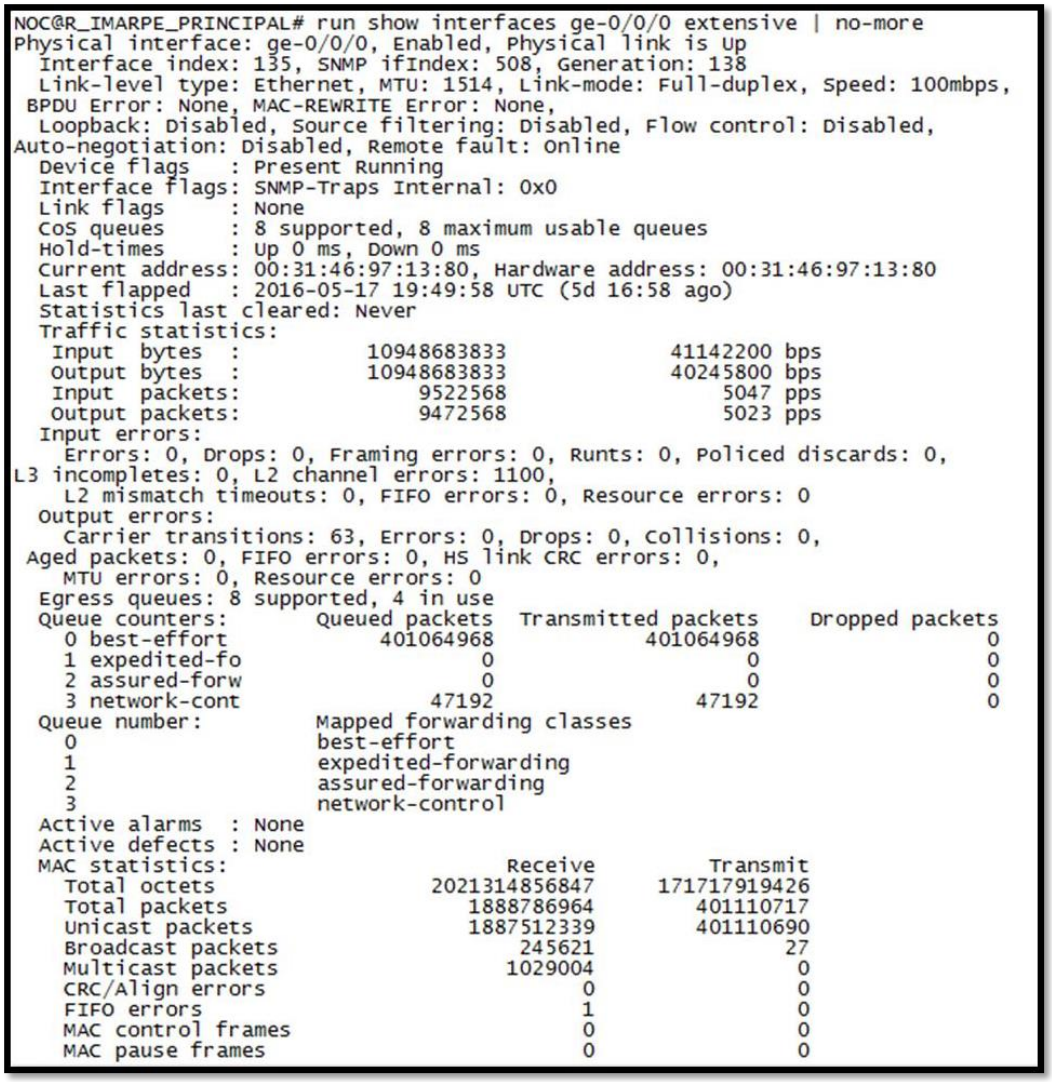
Figura 21: *Ping a una IP pública.*
Fuente: *Informe de Validación*

- ✓ Con el comando **run show interface queue ge-0/0/0 | no-more**, nos muestra el consumo de ancho de banda por calidad de servicios en tiempo de real en la parte WAN como se indica en la figura 22.

```
[edit]
NOC@R_IMARPE_PRINCIPAL# run show interfaces queue ge-0/0/0 | no-more
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 135, SNMP ifIndex: 508
Forwarding classes: 8 supported, 4 in use
Egress queues: 8 supported, 4 in use
Queue: 0, Forwarding classes: best-effort
  Queued:
    Packets              :              9420211                 5547 pps
    Bytes                :          12021202210             42401840 bps
  Transmitted:
    Packets              :              9420210                 5047 pps
    Bytes                :          10021202127             40201050 bps
    Tail-dropped packets :                    0                    0 pps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets              :                    0                    0 pps
    Bytes                :                    0                    0 bps
  Transmitted:
    Packets              :                    0                    0 pps
    Bytes                :                    0                    0 bps
    Tail-dropped packets :                    0                    0 pps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
Queue: 2, Forwarding classes: assured-forwarding
  Queued:
    Packets              :                    0                    0 pps
    Bytes                :                    0                    0 bps
  Transmitted:
    Packets              :                    0                    0 pps
    Bytes                :                    0                    0 bps
    Tail-dropped packets :                    0                    0 pps
```

Figura 22: *Consumo de Ancho de Banda en la WAN.*
Fuente*: Informe de Validación.*

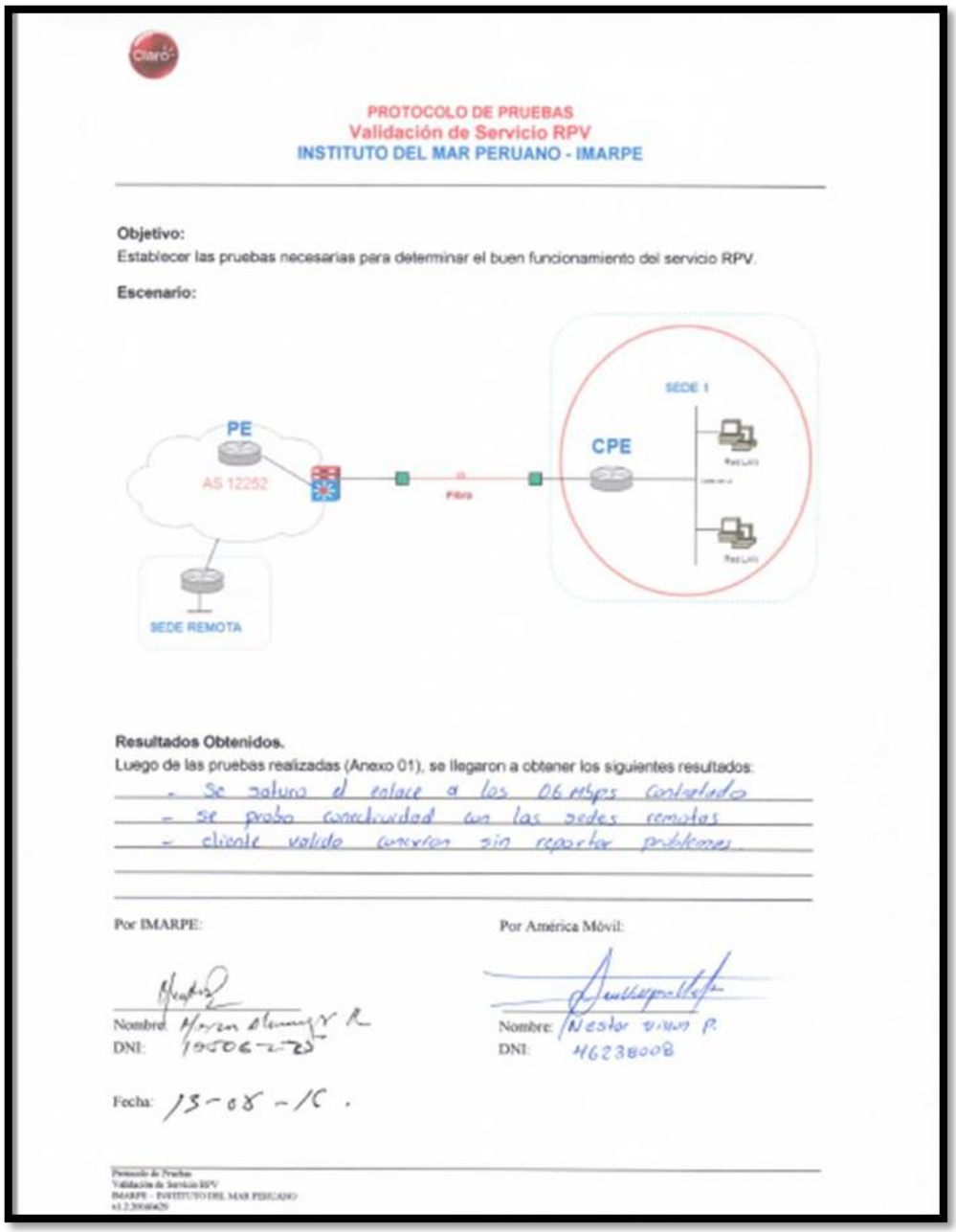
- ✓ Con el comando **run show interface ge-0/0/0 extensive | no-more**, muestra el ancho de banda en tiempo real y los problemas físicos que se pudieran presentar como se indica en la figura 23.



```
NOC@R_IMARPE_PRINCIPAL# run show interfaces ge-0/0/0 extensive | no-more
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 135, SNMP ifIndex: 508, Generation: 138
  Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 100mbps,
 BPDU Error: None, MAC-REWRITE Error: None,
  Loopback: Disabled, Source filtering: Disabled, Flow control: Disabled,
Auto-negotiation: Disabled, Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x0
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:31:46:97:13:80, Hardware address: 00:31:46:97:13:80
  Last flapped   : 2016-05-17 19:49:58 UTC (5d 16:58 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :          10948683833             41142200 bps
   Output bytes  :          10948683833             40245800 bps
   Input  packets:              9522568                 5047 pps
   Output packets:              9472568                 5023 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 1100,
    L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 63, Errors: 0, Drops: 0, Collisions: 0,
 Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0,
    MTU errors: 0, Resource errors: 0
  Egress queues: 8 supported, 4 in use
  Queue counters:       Queued packets  Transmitted packets    Dropped packets
    0 best-effort          401064968           401064968                  0
    1 expedited-fo                 0                   0                  0
    2 assured-forw                 0                   0                  0
    3 network-cont             47192               47192                  0
  Queue number:         Mapped forwarding classes
    0                   best-effort
    1                   expedited-forwarding
    2                   assured-forwarding
    3                   network-control
  Active alarms  : None
  Active defects : None
  MAC statistics:                  Receive         Transmit
    Total octets              2021314856847     171717919426
    Total packets                1888786964        401110717
    Unicast packets              1887512339        401110690
    Broadcast packets               245621               27
    Multicast packets              1029004                0
    CRC/Align errors                     0                0
    FIFO errors                          1                0
    MAC control frames                   0                0
    MAC pause frames                     0                0
```

***Figura 23**: Consumo de Ancho de Banda y problemas físicos.*
***Fuente:** Informe de Validación.*

- ✓ Para cada servicio implementado en cada una de las sedes se validó con el cliente mediante un documento formal o ficha técnica donde valida que todo es conforme como se muestra en la figura 24.



PROTOCOLO DE PRUEBAS
Validación de Servicio RPV
INSTITUTO DEL MAR PERUANO - IMARPE

Objetivo:
Establecer las pruebas necesarias para determinar el buen funcionamiento del servicio RPV.

Escenario:

Resultados Obtenidos.
Luego de las pruebas realizadas (Anexo 01), se llegaron a obtener los siguientes resultados:

- Se aprueba el enlace a los 06 Mbps contratados
- Se probo conectividad con las sedes remotas
- cliente valido correos sin reportar problemas.

Por IMARPE:

Nombre: Marco Aleman Y. R.
DNI: 19506-23

Por América Móvil:

Nombre: Nestor Vivas P.
DNI: 46238008

Fecha: 15-08-16.

Protocolo de Pruebas
Validación de Servicio RPV
IMARPE - INSTITUTO DEL MAR PERUANO
v1.2 20160629

Figura 24: *Documento de aceptación del servicio.*
Fuente: *Protocolo de Pruebas.*

CONCLUSIONES

- Participar en el diseño e implementación de este proyecto me ayudo profesionalmente y pude aplicar mis conocimientos teóricos en Networking.
- Se presenta una solución para el INSTITUTO DEL MAR DEL PERU para que pueda migrar hacia una red MPLS de un proveedor de servicios para poder entablar enlaces de datos, voz, video, etc. entre sus sucursales.
- La conexión de la sede Principal con las sedes Secundarias también cuenta con una conexión de contingencia en caso de que la sede principal deje de funcionar.
- El diseño de la red y la topología ha sido realizado para que el INSTITUTO DEL MAR DEL PERU pueda migrar y disfrutar de una red de altas prestaciones.
- MPLS con su implementación el INSTITUTO DEL MAR DEL PERU ayudara a la comunicación entre las mismas así también a la especialización de la tecnología y la comunicación fluida.
- Adicionalmente las razones por la cual la IETF creó el protocolo MPLS fueron los correctos porque soporta nuevos servicios que las redes IP convencionales no hacen, además de funcionar con cualquier otro tipo de tecnología de transporte.
- Luego de un análisis de las Redes Privadas Virtuales se ha podido determinar que la implementación de estas es una de las mejores opciones de comunicación, ya que resultan muy beneficiosas tanto en aspectos económicos como en la fiabilidad de la transmisión de la información.

- MPLS puede integrar distintos dominios de red independientemente de su protocolo de capa 2 a través de distintas técnicas de encapsulamiento, esto se debe a la gestión multi-etiquetas que permite la combinación del enrutamiento de la capa de red con la conmutación de la capa de enlace para el envío de paquetes utilizando etiquetas cortas de longitud fija, separando el plano de control del plano de datos.

- La interconexión de redes constituye una tendencia fuerte en el manejo de transporte de información, debido a que los requerimientos de los usuarios son más complejos día a día y varían rápidamente. Las soluciones de interconexión deben ser cada vez más cómodas y fáciles de implementar. Las VPN ofrecen una alternativa en este aspecto debido a su flexibilidad y a la filosofía con la que han sido creadas.

- Para finalizar MPLS permite a los proveedores de servicios ser más competitivos y estar más actualizados en cuanto a avance tecnológico se refiere, también permite tener una infraestructura mejor preparada para soportar nuevos clientes y ofrecer mejor servicios a sus usuarios finales.

RECOMENDACIONES

- Se tiene que tomar en consideración con el cliente el servicio a implementar y saber las características técnicas que cada dispositivo que se desee usar para la implementación.
- Es importante destacar que las redes privadas virtuales es una aplicación fundamental para los proveedores de servicios, ya que hoy en día, las grandes empresas quieren establecer una comunicación total, fluida y privada entre sus distintas sedes; mejorando la rentabilidad de estas mismas.
- Es posible aumentar la seguridad de la información de cada interconexión si se combina con protocolos de encriptación de datos como IPSec, el cual es también utilizado para implementar túneles VPN. Dicha encriptación se aplicará en los equipos de borde, que son la interfaz de comunicaciones con otras redes.

BIBLIOGRAFÍA

[1] Rossemberg, (2007). *Diseño e implementación del centro de operación y gestión de la Red académica peruana en Software Libre (tesis de pregrado). Pontificia Universidad católica del Perú,* Lima, Perú.

[2] Barbera, (2007). Funcionamiento MPLS. Obtenido de http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

[3] CISCO,(2015).Obtenido de http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html)

[4] Medina,(2016).Obtenido de https://www.ciberseguridadcolombia.com/Inicio/ArticleID/16/Retos-y-Oportunidades-de-los-Proveedores-de-Servicios-de-Seguridad-Administrada-MSSP

[5] WEBSENSE. (2015). Obtenido de *Soluciones de productividad* obtenido de http://www.technet.com.do/productos-y-servicios/soluciones-de-productividad. Soluciones de productividad.

[6] Luna, (2009). *Medición y análisis de tráfico en redes MPLS (tesis de pregrado). Pontificia Universidad católica del Perú, Lima, Perú.*

[7] Peralta, (2012). *MPLS*. Obtenido de http://prezi.com/acr_j2s2ofmt/mpls-multiprotocol- label-switching/

[8] Tejedor, (2012). MPLS. Obtenido de http://www.todotecnologia.net/wpcontent/uploads/2010/06/Caracteristicas_definicion_MPLS_GMPLS_ASON.pdf

[9] Ricardo, (2012). *Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos*

[10] Gavilanes,(2007). *Diseño e implementación mediante el simulador Dynamips.* Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/1064/1/1892.pdf

[11] Valenzuela, (2012). *Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña (tesis de pregrado). Pontificia Universidad católica del Peru,*Lima,Peru.

[12] Salviat,(2005). *Redes MPLS.* Obtenido de http://cybertesis.uach.cl/tesis/uach/2005/bmfcic828r/sources/bmfcic828r.pdf

[13] Orozco, (2014). *Diseño de una red privada virtual con tecnología MPLS para la carrera de Networking de la Universidad de Guayaquil (tesis de pregrado).Universidad de Guayaquil, Ecuador*.

ANEXOS

❖ ANEXO I: Glosario de términos

- ✓ **ATM** (Asynchronous Transfer Mode)**:** Modo de Transferencia Asincrónico.
- ✓ **AS-PATH** (Autonomous System Path; en español: Camino de Sistemas Autónomos). Atributo de BGP para evitar bucles de ruteo.
- ✓ **BACKBONE:** Se refiere a las principales conexiones troncales de Internet. Está compuesta por enrutadores comerciales, gubernamentales de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.
- ✓ **BGP** (Border Gateway Protocol)**:** Protocolo de gateway fronterizo.
- ✓ **BER** (Bits Error Rate): Tasa de Bits Erróneo. La tasa de errores de desempeño.
- ✓ **CE** (Customer Edge): Router de cliente.
- ✓ **CoS** (Quality of Service): Calidad de Servicio.
- ✓ **CR-LSP** (Constraint-based Routing Label Distribution Protocol; en español: Protocolo de enrutamiento de distribución de etiquetas basado en restricciones). Es un mecanismo que amplía las capacidades de LDP para cumplir con los requisitos de ingeniería de tráfico.
- ✓ **Dual-homed** (en español: doblemente alojada). Término usado en redes de datos para referirse a escenarios donde se tienen dos enlaces de Internet para fines de recuperación ante fallas.
- ✓ **EIGRP** (Enhanced Interior Gateway Routing Protocol)**:** Protocolo de enrutamiento de gateway interior mejorado.
- ✓ **ETHERNET**: Estándar de redes de área local para computadores con acceso al medio por detección de la portadora con detección de colisiones.

- ✓ **FEC** (Forward Error Correction): Corrección de errores.
- ✓ **FIB** (Forwarding information base): Base de información de envío.
- ✓ **FO** (Fiber optic): Fibra Óptica.
- ✓ **GR** (Graceful Restart; en español: reinicio agraciado). Protocolo encargado de evitar pérdida de datos durante una falla en protocolos de ruteo que lo implementan además de ser un mecanismo que propicia la rápida convergencia del protocolo de ruteo ante una falla.
- ✓ **Full-Mesh** (en español: malla completa). Tipo de topología que pueden seguir las redes de datos.
- ✓ **IP-FRR** (Internet Protocol Fast Re-Route; en español: desvío rápido del protocolo IP). Técnica de alta disponibilidad que funciona sobre IP para protección de flujos de tráfico.
- ✓ **IEEE** (Institute of Electrical and Electronics Engineers): Instituto de ingenieros eléctricos y electrónicos.
- ✓ **IETF** (Internet Engineering Task Force): Grupo de trabajo de Ingeniería de Internet.
- ✓ **IGP** (Interior Gateway Protocol): Protocolo de pasarela interno IOS.
- ✓ **IP** (Internet Protocol): Protocolo de Internet.
- ✓ **IPSEC** (Internet Protocol security): es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando cada paquete en un flujo de datos.
- ✓ **ISP** (Internet service Provider): Proveedor de servicios de Internet.
- ✓ **ITU** (Internacional Telecommunications Unión): Unión Internacional de Telecomunicaciones.

- ✓ **LOCAL PREFERENCE** (en español: preferencia local). Atributo del protocolo BGP que influye en la decisión para la salida del tráfico del sistema autónomo.
- ✓ **LDP** (Label Distribution Protocol): Protocolo de Distribución de Etiquetas.
- ✓ **LER** (Label Edge Router): Enrutadores de Etiquetas de Borde.
- ✓ **LFIB** (Label Forwarding Instance Base): Base de información de envío de etiquetas.
- ✓ **LIB** (Label Information Base): Base de información de etiquetas.
- ✓ **LSP** (Label Switched Path): Nombre genérico que se le da al túnel MPLS establecido entre dos dispositivos, el LSP es unidireccional.
- ✓ **LSR** (Label Switching Router): Enrutadores Conmutadores de Etiquetas.
- ✓ **LOG**: es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema. Se utiliza en muchos casos distintos, para guardar información sobre la actividad de sistemas variados.
- ✓ **MPLS** (Multiprotocol Label Switching): Conmutación Multi-Protocolo mediante Etiquetas.
- ✓ **MPLS TE FRR** (Multi Protocol Label Switching Traffic Engineering Fast Re-Route; en español: conmutación de etiquetas multiprotocolo, ingeniería de tráfico, re-enrutamiento rápido). Protocolo de alta disponibilidad usado en arquitecturas MPLS que provee protección ante fallas físicas en enlaces o equipos.
- ✓ **NEXT-HOP** (en español: siguiente salto). Término usado en BGP relativo al siguiente punto donde debe ser enviado el tráfico.
- ✓ **OSI** (Open Systems Interconnection): Interconexión de Sistemas Abiertos.

- ✓ **OSPF** (Open Shortest Path First): El camino más corto primero.
- ✓ **PE** (provider edge; en español: borde del proveedor). Elemento que se encuentra en la frontera de la red del proveedor de servicios, generalmente se conecta a un equipo en la red del cliente llamado CE.
- ✓ **PPP** (Point-to-point Protocol): Protocolo punto a punto.
- ✓ **PPTP** (Point-To-Point Tunneling Protocol): Protocolo punto a punto de túnel
- ✓ **RIP Routing Information Protocol**: Protocolo de Información de enrutamiento.
- ✓ **QoS** o Calidad de Servicio (**Quality of Service**) es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red.
- ✓ **ROUTER**: Es un dispositivo que proporciona conectividad a nivel de red en el modelo OSI, su función principal consiste en encaminar paquetes de datos de una red a otra.
- ✓ **RD** (Route Distiguisher, en español: Caracterizador de ruta). Atributo en BGP para definir una instancia de ruteo.
- ✓ **SWITCH**: Es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red.
- ✓ **SSO** (Stateful Switchover; en español: Conmutación de estado). Protocolo para la sincronización de tablas de sesiones entre dos firewalls que se encuentran en alta disponibilidad.
- ✓ **TCP** (Transmission Control Protocol): Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet.

- ✓ **UPSTREAM** Se refiere a la velocidad con que los datos pueden ser transferidos de un cliente a un servidor, lo que podría traducirse como velocidad de carga:
- ✓ **VLAN Virtual Local Area Network**: Red de Area Local Virtual.
- ✓ **VPN Virtual Private Network**: Red Privada Virtual supone una tecnología de red que, por razones de costo y comodidad, brinda la posibilidad de conectarse a una red pública generando una extensión a nivel de área local.
- ✓ **VRF Virtual Routing and Forwarding**: permite múltiples tablas de rutas separadas las cuales pueden coexistir en el mismo router y al mismo tiempo.
- ✓ Virtual Chassis (VC) es una tecnología de virtualización de red que se ofrece en varios modelos de switches Juniper Ethernet, como el EX4200. Con VC, entre 2 y 10 conmutadores Ethernet físicos pueden ser "apilados" para formar un único factor de forma lógico con un plano de control unificado y un archivo de configuración, así como una única instancia del SO que funciona en toda la pila
- ✓ **VRRP** (Virtual Router Redundancy Protocol; en español: Protocolo de redundancia de router virtual). Protocolo de redundancia que permite incrementar la disponibilidad de la puerta de enlace predeterminada en una misma subred.
- ✓ **WAN** (Wide Area Network): Red de Area Amplia.

❖ ANEXO II

✓ Sede principal

- **Router**

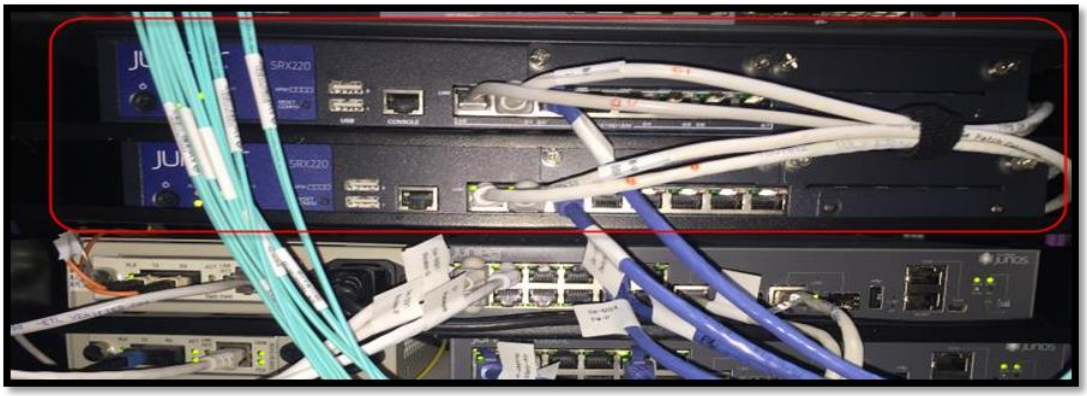


Figura 25: *Router SRX220 en clouster instalado en la sede principal*
Fuente: *Reporte de instalación.*

- **Firewall**

Figura 26: *FIREWALL SRX550 en clouster instalado en la sede principal*
Fuente: *Reporte de instalación.*

- **SW – CORE**

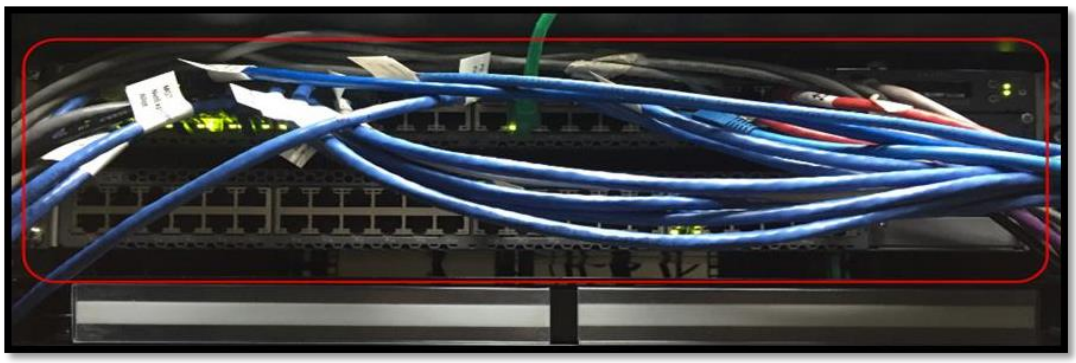


Figura 27: *Switch core en cluster instalado en la sede principal.*
Fuente: *Reporte de Instalación.*

- **Radware**

Figura 28: *Equipo RADWARE instalado en la sede principal.*
Fuente: *Reporte de Instalación.*

- **ALLOT**

Figura 29: *Equipo ALLOT instalado en la sede principal.*
Fuente: *Reporte de Instalación.*

- **WebSense**

Figura 30: *Equipo WEBSENSE instalado en la sede principal.*
Fuente: *Reporte de Instalación.*

- **FireEye**

Figura 31: *Equipo FIREEYE instalado en la sede principal.*
Fuente: *Reporte de Instalación.*

- **Servidor del cliente para la Solución**

Figura 32: *Servidores instalados en la sede principal para la seguridad administrada.*
Fuente: *Reporte de Instalación.*

- **JUNOS SPACE (Instalado en el rack de servidores)**

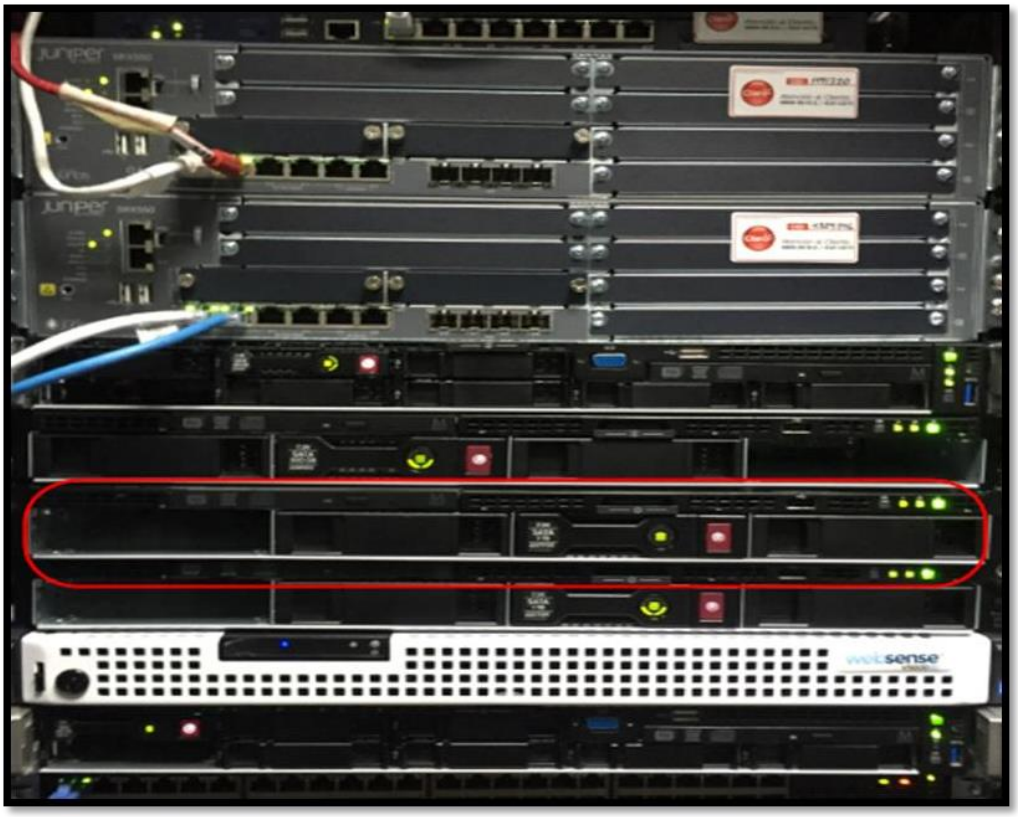


Figura 33: *JUNOS SPACE instalado en uno de los servidores en la sede principal.*
Fuente: *Reporte de Instalación.*

- **Imagen del Rack de los equipos instalados en la sede**

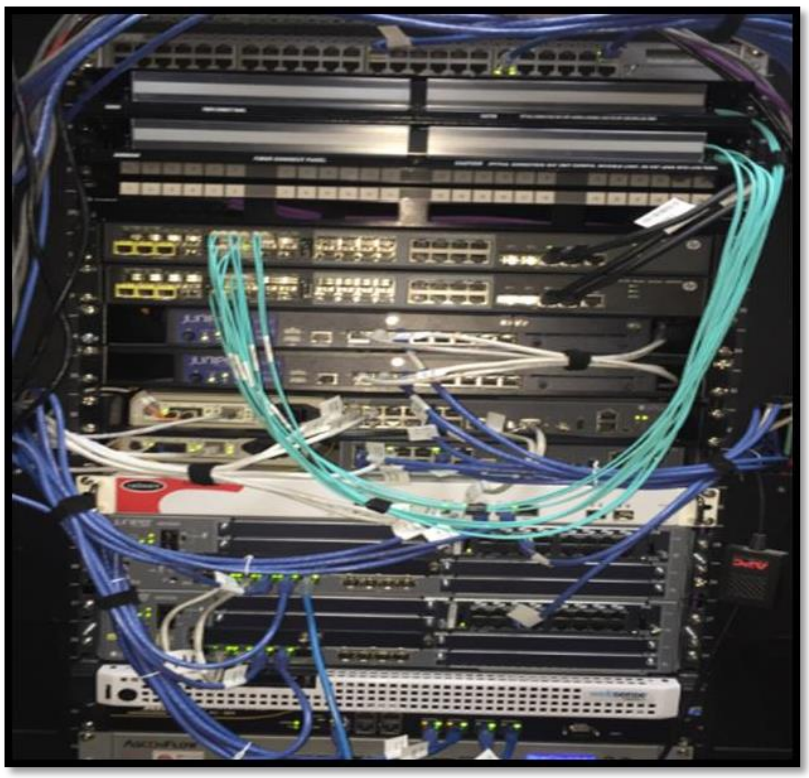


Figura 34: *Rack instalado en la sede principal*
Fuente: *Reporte de Instalación.*

✓ **Sede Av. Argentina**

- **CONJUNTO DE EQUIPOS INSTALADOS EN LA SEDE**

Figura 35: *Equipos RADWARE, ALLOT, FIREWALL, SWITCH, WEBSENSE.*
Fuente: *Reporte de Instalación.*

❖ **ANEXO III: Detalles Técnicos.**

a. ROUTER

Tanto el activo como el pasivo fueron creados los links *agregation ae*1 y *ae2*, con el fin de aumentar el rendimiento más de lo que una sola conexión podría sostener, además de proporcionar redundancia si es que un enlace llegara a fallar, estos equipos están en bajo el protocolo VRRP, ya que al ser activo/pasivo poseen una interface virtual diseñado para aumentar la disponibilidad de la puerta de enlace.

- **Características**

El SRX220 Services Gateway es muy importante ya que consolida seguridad, enrutamiento, switching y conectividad WAN en un dispositivo compatible hasta 950 Mbps firewall, tiene un moderno sistema de prevención de intrusos (IPS) de 100 Mbps y de 100 Mbps IPsec VPN.

La familia de productos de Juniper Networks SRX Series servicios Gateways puede ofrecer protección de firewall de próxima generación con controles de aplicación conocimiento y usuario basada en funciones, además de opciones de administración (UTM) como lo describimos en las bases teóricas, mejor en su clase unificada de amenazas para proteger y controlar los activos de su empresa. El SRX220 Services Gateway (figura 36) es ideal para la seguridad de empresas pequeñas y medianas y empresas distribuidas.

***Figura 36**: Router SRX 220.*
***Fuente:** Pagina de proveedor de JUNIPER.*

***Tabla 3**: Características del Router SRX220*

CARACTERISTICAS	METRICA
Versión Junos OS Software probado	Junos OS 12.1
Rendimiento Firewall (max)	950 Mbps
Rendimiento IPS	80 Mbps
AES256 + SHA-1 / 3DES + SHA-1 El rendimiento de VPN	100 Mbps
Máximo de sesiones simultáneas	96000
Nuevas sesiones / segundo (sostenido, TCP, de 3 vías)	2800
Políticas de máxima seguridad	2048

***Fuente**: Soporte JUNIPER página Web.*

b. SWITCHES

Los swiches fueron configurados de tal manera que formen un virtual chassis, la cual hace que ambos equipos se comporten como si fuera uno solo, la configuración es la misma para ambos swiches, dando la ventaja de que si el enlace activo falla automáticamente pasa a tomar el papel de master el otro switch, no viéndose interrumpido la conexión hacia internet.

- **Características**

  La línea EX2200 de switches cuenta con una configuración fija con tecnología de Virtual chasis que satisface la rama y requerimientos de conectividad de cableado de baja densidad de hoy, para negocios de alto rendimiento. Cuatro configuraciones de la plataforma están disponibles con 24 y 48 puertos de 10/100/1000BASE-T con o sin Power over Ethernet (PoE). Los modelos EX2200 incluyen un presupuesto máximo de 405 W para proporcionar hasta 15,4vatios basados en estándares 802.3af, para apoyar

los dispositivos en red tales como teléfonos, cámaras de vídeo, wireless LAN (WLAN) acceder a puntos y teléfonos de video en redes convergentes.

En la presente propuesta se consideran los modelos:

- EX2200–48P(figura 37), el cual brinda 48 interfaces 10/100/1000 BaseT. Conmutador recomendado como switches de acceso.

Figura 37: *Switch JUNIPER*
Fuente: *Pagina proveedor JUNIPER*.

Tabla 4: *Características de SW JUNIPER*

CARACTERISTICAS	METRICA
Dimensiones (An X Al X Pr)	17.4 x 1.7 x 10 in (44.1 x 4.4 x 25.4 cm) 1 rack unit
Compatibilidad con estándares	Auto MDI/MDIX, Alimentación a Través de Ethernet, con tramas Jumbo
Puerto USB	si
Puerto de consola	si
Número de puertos en el conmutador	48 x Ethernet 10/100/1000 Mbit/s
Número de VLANs	1024
El tamaño de la tabla de direcciones MAC	16,000

Fuente*: Soporte JUNIPER página Web.*

c. RADWARE

El equipo DefensePro se encuentra en una configuración en línea a nivel de topología, por lo cual pasa todo el tráfico a través de él. En el caso de existir algún inconveniente con el equipo, éste entraría a funcionar simplemente como un cable permitiendo el paso de todo el tráfico y evitandode este modo algún corte en el servicio. Sin embargo, existen dos enlaces a considerar: uno en la interface G1 el cual será el principal, y otro en la interface G3 que actuará como secundario o backup.

- ✓ **Características**

Este equipo se encarga de la prevención de intrusos y protección en tiempo real contra ataques de red conocidos y emergentes.

Ataques basados en vulnerabilidades que explotan las debilidades de la aplicación de servidor como Web, correo, DNS, FTP, SIP, vulnerabilidades de servidores SQL.

Los ataques se basan en vulnerabilidades de recursos del servidor como:

DoS de aplicación – HTTP, SIP y otros ataques de inundación, robo de información, y aplicación de análisis.

Servicio en tiempo real contra troyanos y Anti-Phishing, para luchar contra los fraudes financieros, robo de información y malware propagados**.**

a. Prevención de ataques precisos

Firmas en tiempo real se generan para cada patrón de ataque, de hasta 20 parámetros de diferentes ataques sin bloquear el tráfico de los usuarios legítimos.

b. Alto rendimiento

Selección de plataforma de hasta 40Gbps además de protección y control del tráfico de red dedicado al hardware de aceleración contra ataques DDoS:

Bloqueo de ataques que abuso de los recursos de la CPU de su equipo de seguridad y redes.

No hay necesidad de comprometer la seguridad cuando la red está bajo ataque. DefensePro figura 38.

***Figura 38**: Equipo RADWARE.*
***Fuente:** Pagina Proveedor de JUNIPER.*

***Tabla 5:** Características Técnicas RADWARE*

CARACTERISTICAS	METRICA
Licencias de rendimiento escalable de OnDemand	200Mbps
Máximas Sesiones concurrentes	2,000.000
Tasa de prevención de ataques de inundación máxima de DDoS	1,000.000 pps
Latencia	< 60 micro segundos
Firmas en tiempo real	Detectar y proteger de ataques en menos de 18 segundos
Ethernet de 10/100/1000 cobre	4
1 GE	2(SFP)

Fuente: Soporte página Web RADWARE

d) FIREWALL

Se hizo la conexión formando un clúster entre ambos equipos, esta configuración hace que los equipos estén sincronizados es decir al hacer un cambio y ejecutar el comando commit se reflejara en ambos nodos. Las conexiones del clúster dependen del modelo de cada equipo en este caso para el SRX550 se utilizaron las interfaces ge-0/0/1 y ge-0/0/6 para *managment* y control respectivamente.

✓ **Características**

Los equipos Juniper SRX550 Gateway (figura 39) es un todo en uno. Se presenta en forma de un dispositivo con dos unidades de rack con seguridad integrada, enrutamiento, conmutación y conectividad WAN. Es compatible con un firewall para un rendimiento máximo de 5,5 Gbit/s, un rendimiento de VPN IPSec de hasta 1 Gb/s e IPS con un rendimiento de hasta 800 Mbit /s.

Figura 39: *Equipo Firewall SRX550 JUNIPER*
Fuente: *Soporte página Web JUNIPER*

También incluye la función Unified Threat Management (UTM) que consiste en: antivirus, seguridad de aplicaciones, IPS, filtrado Web anti-spam y avanzado. Los Servicios SRX550 Gateway es ideal para asegurar las medianas y grandes filiales.

Tabla 6: *Características Técnicas FIREWALL SRX550 JUNIPER.*

CARACTERISTICAS	METRICA
Versión Junos OS Software probado	Junos OS 12.1
Rendimiento Firewall (max)	5.5 Gbps
Rendimiento IPS (NSS 4.2.1)	800 Mbps
AES256 + SHA-1 / 3DES + SHA-1 El rendimiento de VPN	1.0 Gbps
Máximo de sesiones simultáneas	375000
Nuevas sesiones / segundo (sostenido, TCP, de 3 vías)	27000
Políticas de máxima seguridad	7256

Fuente: Pagina de Soporte JUNIPER

e) ALLOT

Este Administrador de Ancho de Banda cuenta con un módulo Bypass interno, están conectadas a la red en las interfaces Internal0, External0 e Internal1, External1; las interfaces están configuradas en el modo bypass por lo que si se produce algún error en el equipo la conexión a internet no se pierde; además la administración de este equipo se hace a través del NetXplorer, que está instalado en un servidor, donde creamos las políticas para limitar los diferentes servicios.

- ✓ **Características**

AllotNetEnforcer® AC-504 (figura 40) gestiona el tráfico de Internet en varios enlaces Ethernet a velocidades de hasta 1 Gbps. Este dispositivo flexible proporciona análisis en tiempo real, la aplicación de políticas y de direccionamiento del tráfico para ayudar a la utilización de ancho de banda de control de los operadores y los costes a la vez que garantiza la calidad de experiencia (QoE) para todos los usuarios de la red.

Figura 40: *Equipo de análisis y gestión en tiempo real.*
Fuente: *Pagina Web de ALLOT*

f) FIREEYES

FireEye wMPS instalada en la red de IMARPE tiene la finalidad de brindar un sistema de protección de Malware Web de FireEye Inc. Provee seguridad Web de siguiente generación para combatir el Malware Moderno de Día Cero y ataques específicos tipo ATP.

Los dispositivos de seguridad Web de FireEye utilizan varias técnicas para detectar código desconocido y sospechoso, eliminando los molestos falsos positivos que invaden a las tecnologías de seguridad tradicionales

- **Características**

El FireEye Network Security (figura 41) identifica y bloquea los exploits y devoluciones de petición de múltiples protocolos para ayudar a las organizaciones para sus defensas de amenaza avanzadas a través de una gama de implementaciones, desde la sede de multi-gigabit a control remoto, sucursales y casa oficinas. Seguridad de red de FireEye con FireEye Intrusion Prevention (IPS), Optimiza el sistema, reduce falsos positivos y permite el cumplimiento durante la conducción de seguridad a través de amenazas conocidas y desconocidas. Los delincuentes cibernéticos utilizan la Web como un vector principal para amenazas.

Seguridad de la red está diseñada para evitar conducir por medio de las descargas los ataques combinados de Web y correo electrónico. Además,

ofrece la seguridad de la red en defensa contra las infecciones que tienen lugar fuera de la red.

Figura 41: *Equipo de Seguridad FIREEYE.*
Fuente: *Pagina Web FIREEYE.*

Tabla 7: *Características Técnicas Equipo FIREEYE NX400*

CARACTERISTICAS	METRICA
Dimensiones (An X Al X Pr)	17.2" x 27.8" x 1.70" (437 x 706 x 43.2 mm)
Performance	100 Mbps or 250 Mbps
IPS Performance	100 Mbps or 250 Mbps
Número de puertos en el conmutador	2x 10/100/1000 BASE- T Ports
UserCount	1,000 or 2,500
ConcurrentConnections	80K

Fuente: Pagina de Soporte FIREEYE.

g) SWITCH EX4300

Línea de switches EX4300 Ethernet cuenta con la tecnología del Virtual Chassis, combina la fiabilidad de clase portadora de sistemas modulares con la economía y flexibilidad de plataformas, entregando un alto rendimiento, una solución escalable para data centers, ambientes de la oficina del campus y las sucursales.

Ofreciendo un conjunto completo de capa 2 y capa 3 de capacidades de conmutación, el EX4300 permite una variedad de implementaciones, incluyendo acceso de centro campus, rama y datos. Un único 24-puerto o

switch de 48 puertos EX4300 puede implementarse inicialmente. Requisitos de crecimiento, tecnología de Virtual Chassis de redes permite hasta 10 switches EX4300 que perfectamente interconectado y administrado como un dispositivo único, entrega escalable, solución para la expansión de los entornos de red. Un par de switches de fibra de EX4300 de 32 puertos también se puede implementar como una agregación consolidada.

En la presente implementación se consideró los modelos:

- ✓ **EX4300-48P** (figura 42), el cual brinda 48 interfaces 10/100/1000 BaseT. Conmutador recomendado como switches de acceso.

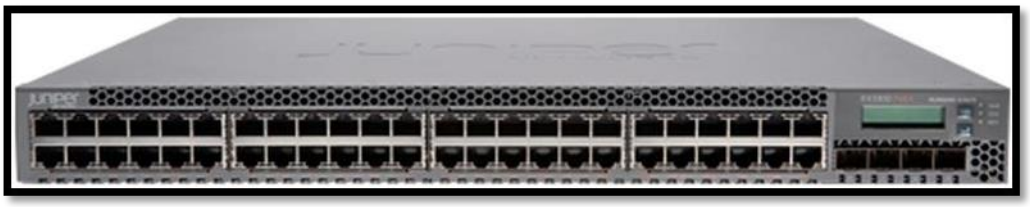


Figura 42: *SWITCH EX4300-48P.*
Fuente*: Sitio Web del proveedor JUNIPER.*

Tabla 8: Características del SWITCH EX43000.

CARACTERISTICAS	METRICA
Dimensiones (An X Al X Pr)	17.41 x 1.72 x 16.43 in (44.21 x 4.32 x 41.73 cm)
Puerto USB	Si
Puerto de consola	Si
Número de puertos en el conmutador	48-port 10/100/1000BASE-T
Número de VLANs	4,093
El tamaño de la tabla de direcciones MAC	64,000

Fuente: *Soporte WEB equipos JUNIPER.*

h) WEBSENSE

El WEBSENSE instalado en IMARPE tiene como función primordial permitir o bloquear el acceso a páginas web en la red en la que se encuentra instalada. Esto debido a que posee categorías de filtrado predeterminadas, listas negras y listas blancas, las cuales pueden ser usadas para crear políticas de filtrado para determinados sectores de red en toda la solución de networking en el cliente IMARPE. Esto permitirá el control de acceso a los usuarios que no tengan permitido a webs de entretenimiento.

- ✓ **Características**

Por lo general disponibles en la actualidad, el nuevo aparato de WEBSENSE V5000 (figura 43) es el aparato ideal para sucursales empresariales y despliegues comerciales. Con soporte para hasta 2000 usuarios, el V5000 está preconfigurado para simplificar la implementación de las soluciones WEBSENSE Web Security Gateway (incluyendo Web Security Gateway en cualquier lugar). El V5000 proporciona otra opción para los clientes tomar ventaja de la arquitectura WEBSENSE TRITON para reducir la complejidad de TI y proporcionar pequeñas y medianas empresas el mismo despliegue flexible, modelos de seguridad flexibles de implementación del estado de la técnica inherentes dentro de las soluciones de WEBSENSE.

Aparatos V-Series ofrecen una combinación única de extensibilidad, hacen que el rendimiento y la instalación sea sencilla. La virtualización se consolida a bordo de múltiples funciones de seguridad a una sola plataforma de hardware, mientras que el apoyo a futuras mejoras. Aparatos

de la serie V reducen significativamente el tiempo de implementación y los costos operativos de los clientes de WEBSENSE Web Security Gateway.

Figura 43: *Equipo WEBSENSE.*
Fuente: *Pagina WEB soporte WEBSENSE.*

Tabla 9*: Características del FORCEPOINT WEBSENSE.*

CARACTERISTICAS	METRICA
Max users/Appliance	2000
Processor	1 x Intel Xeon E3-1231
Memory	16GB
hdd	2 x 500 GB SATA
Nic	4 x 10/100/1000 Base-T
Power supply	Single 250W (100V~240V)

Fuente: *Soporte WEBSENSE*

i) SOLARWINDS SL2000

Este Software analiza y supervisa estadísticas de rendimiento de red en tiempo real para todos los componentes con SNMP habilitado.

Nos permite representar de forma gráfica los equipos que están amarrados en IMARPE y rastrear visualmente las estadísticas de rendimiento en tiempo real, además identifica a los usuarios, aplicaciones y protocolos que están consumiendo la mayor cantidad de banda ancha de la red y destacará las direcciones IP de los principales talkers de la red.

Acelera la detección y resolución de problemas, resuelve los problemas de desempeño de red y reduce el tiempo de inactividad. Monitorea y muestra el tiempo de respuesta, la disponibilidad y el rendimiento de los dispositivos de red.

- ✓ **Network Performance Monitor (NPM):**

Este software de monitoreo de redes le permite detectar, diagnosticar y resolver rápidamente los problemas de desempeño de la red y los cortes del servicio, antes de que empiece a recibir llamadas preguntado si la red se cayó. El software SOLARWINDS Network Performance Monitor es un monitor de red fácil de usar. Esto significa que usted puede dedicar su tiempo a monitorear su red en lugar de tener que ayudar a su software de monitoreo de la red con ello podemos verificar Latencia, disponibilidad, rendimiento y error de la red.

- Acelera la detección y resolución de problemas, resuelve los problemas de desempeño de red y reduce el tiempo de inactividad
- Monitorea y muestra el tiempo de respuesta, la disponibilidad y el rendimiento de los dispositivos de red.
- Mejora la eficiencia operativa con paneles, alertas e informes predeterminados.
- Descubre y mapea automáticamente los dispositivos de red y normalmente se implementa en menos de una hora.

- ✓ **NetFlow Traffic Analyzer (NTA):**

Este software permite capturar datos de flujos continuos de tráfico de red y convertir esos números en gráficos y tablas fáciles de interpretar que

cuantifican exactamente cómo se utiliza la red corporativa, quién la utiliza y con qué fin.

- Monitorea el ancho de banda de la red y los patrones de tráfico a nivel de la interfaz.

- Identifica qué usuarios, aplicaciones y protocolos consumen la mayor parte del ancho de banda.

- Señala las direcciones IP de los usuarios más activos, almacena y muestra datos de flujo con una granularidad de visibilidad de hasta un minuto.

j) JUNOS SPACE Security Director

La gestión de la política de seguridad empresarial se ha convertido en una tarea extremadamente compleja. El crecimiento en el tráfico de red, incluyendo el tráfico móvil y el procedente de los dispositivos personales, así como el desarrollo de los servicios de tecnología de cloud, se han combinado para dar lugar a una nueva gama de posibilidades para los hackers.

La gestión de la seguridad es una tarea que puede resultar propensa a errores y requerir mucho tiempo si las soluciones de gestión son lentas o difíciles de utilizar, o bien la granularidad de control es restringida. Los errores de configuración resultantes pueden dar lugar a una vulnerabilidad de la empresa de cara a amenazas, así como a un incumplimiento de normativas y políticas.

JUNOS SPACE Security Director, una de las aplicaciones de gestión de JUNOS SPACE, ayuda a las empresas a mejorar el alcance, la facilidad y la precisión de la administración de políticas de seguridad gracias a una

herramienta de gestión escalable basada en la interfaz de usuario. Automatiza el aprovisionamiento de seguridad a través de una interfaz centralizada basada en web, que ayuda a los administradores a gestionar todas las fases del ciclo de vida de las políticas de seguridad con mayor rapidez y de forma más intuitiva, desde la creación de las políticas hasta su corrección.

k) SWITCH EX2200-C

El SWITCH EX2200-C con tecnología de Virtual chasis ofrece una compacta, silenciosa y eficiente plataforma de poder para implementaciones de baja densidad, entornos de grupo de trabajo, acceso o empresa comerciales.

Con puertos de acceso de 12 10/100/1000BASE-T con y sin Power over Ethernet Plus (PoE +) en un diseño sin ventilador, los SWITCH EX2200-C proporcionan una solución potente para servicios de apoyo tales como comunicaciones unificadas, telefonía IP, circuito cerrado de televisión (CCTV) y otras aplicaciones de oficina, aula, hospitalidad y entornos de cableado limitado.

En la presente implementación se consideran los modelos:

1. EX2200-C-12T-2G (figura 44), el cual brinda 12 interfaces 10/100/1000 BaseT. Conmutador recomendado como switches de acceso.

Figura 44: *SWTICH JUNIPER.*
Fuente*: Sitio WEB JUNIPER.*

Tabla 10: *Características SWITCH JUNIPER EX2200-C.*

CARACTERISTICAS	METRICA
Dimensiones (An X Al X Pr)	10.6 x 1.7 x 9 in (26.9 x 4.4 x 22.8 cm) 1 rack unit
Puerto USB	si
Puerto de consola	si
Número de puertos en el conmutador	12-port 10/100/1000BASE-T
Número de VLANs	1024
El tamaño de la tabla de direcciones MAC	16,000

Fuente: *Pagina de soporte JUNIPER*

ANEXO III: Requerimientos del cliente.

b) El POSTOR, deberá contar con una Red Principal o Backbone Propio (No rentado a Terceros), el cual tenga como medio de transporte Fibra Óptica en todo su recorrido (Red de Acceso y Backbone).
c) La tecnología a utilizar el POSTOR, para la prestación del servicio estará basada enteramente en MPLS en el Backbone del proveedor por donde se cursará el tráfico de Internet y Datos.
d) El POSTOR, deberá demostrar técnicamente en su propuesta que el tramo local es un enlace simétrico y dedicado 100%, sin utilizar esquemas de acceso compartido o acceso del tipo asimétrico. (Dedicado, No compartido).
e) El POSTOR deberá **garantizar mediante una declaración jurada** que cuenta con redundancia para conectarse al backbone internacional de Internet es decir la salida a internet debe ser como mínimo dos operadores internacionales TIER-1 (en la declaración jurada se deberán indicar los nombres de dichos operadores, su ubicación y de forma opcional la velocidad contratada), cada uno de los nodos internacionales deberá estar ubicado en diferentes puntos geográficos, para ello también se presentara un diagrama de la salida internacional.
f) El POSTOR deberá contar con un SOC (Security Operation Center) **local y/o rentado a terceros**. Deberá poseer Servidores DNS redundantes y distribuidos en locales distintos.
g) El POSTOR, debe ser miembro de alguna organización internacional que agrupe a los grupos de respuesta de incidentes de seguridad (como el FIRST – Forum for incident Response and Security Teams).
h) El POSTOR deberá considerar el equipamiento necesario hasta el ingreso al puerto RJ45 del Switch de la Sede Central de IMARPE, Local de la Av. Argentina y Sedes Remotas (Laboratorios Costeros y Continental), transmitiendo a una velocidad mínima en la interface de comunicación de 10/100/1000 Base-T. IMARPE será responsable de garantizar espacio para el rack o gabinete, energía estabilizada, tomacorrientes.
i) El POSTOR debe ser miembro activo formal e integrante de la Asociación NAP Perú además de poseer conexión directa al NAP Perú con infraestructura propia (No rentado a Terceros).

Figura 45: *Requerimientos del cliente.*
Fuente: *Términos de Referencia.*

j) El servicio de acceso a Internet debe estar configurado a una velocidad no menor de 40 Mbps, con un grado de concentración del servicio de 1:1 en el tramo local e Internacional, debidamente garantizado desde el local de la Sede Central de IMARPE hasta el POP Internacional normalmente dentro de los Estados Unidos.
k) El POSTOR, deberá considerar realizar administración compartida de toda la solución con la finalidad de minimizar los tiempos de respuesta en relación al soporte técnico.
l) El POSTOR, deberá considerar incluir el hardware necesario (Sin costo para el IMARPE), para la implementación de la interconexión de la red de datos, de tal forma que pueda soportar servicios de Video-Conferencia, Transmisión de Cámaras de Seguridad, descarga de imágenes satelitales y transmisión de archivos, de tal forma que durante el tiempo de servicio, el rendimiento de la red de datos y salida a internet no sea perjudicado.

Figura 46: *Requerimientos del cliente.*
Fuente: *Términos de Referencia.*

CARACTERISTICAS DEL SERVICIO

c) El POSTOR, deberá instalar un enlace de contingencia del servicio de Internet en la Sede de la Av. Argentina, con el mismo ancho de banda de 40 Mbps y Sistema de Seguridad con el que se configurara el de la Sede Central del IMARPE. Este enlace de Internet deberá activarse en caso haya una caída de los enlaces de la Sede Central y deberá soportar el tráfico de salida de las Sedes Remotas de forma automática.

d) El POSTOR, deberá proporcionar al enlace de Contingencia de la Sede Av. Argentina la misma cantidad de direcciones IP públicas de Internet IPv4, que se asignaran a la Sede Central del IMARPE, con el fin de activar los principales servicios de la institución en caso de desastre en la Sede Central.

e) El POSTOR, deberá instalar un enlace a Internet independiente de 10 Mbps, en la Sede Central del IMARPE, este enlace deberá contar con un pull de 08 IP públicas, esta conexión ira conectado a los equipos de seguridad.

f) Los niveles de compresión (Overbooking) para todo el enlace solicitado, deben ser de 1:1 y simétrico.

g) El servicio de acceso a Internet deberá contar con última milla por fibra óptica canalizada y subterránea desde el local de la entidad hasta nodo IP de Internet más próximo del proveedor del servicio.

h) El ancho de banda para la interconexión de Datos e Internet entre la Sede Central de IMARPE y la Sede de la Av. Argentina será de 12 Mbps con un nivel de compresión para este enlace de 1:1 y simétrico. El servicio para este enlace deberá contar con última milla por fibra óptica canalizada y subterránea desde este local hasta el nodo IP de Internet más próximo del proveedor del servicio.

***Figura 47**: Requerimientos del cliente.*
***Fuente:** Términos de Referencia.*

i) El ancho de banda para la interconexión de Datos e Internet entre la Sede Central de IMARPE y los Laboratorios Costeros y Continental será de 06 Mbps para cada uno de los enlaces y con un nivel de compresión para cada uno de los enlaces de 1:1 y simétrico. El servicio para estos enlaces deberá contar con última milla por fibra óptica canalizada, subterránea o aérea desde este local hasta el nodo IP de Internet más próximo del proveedor del servicio. La ubicación de los Laboratorios que deberán tener este enlace de datos se detalla en el punto a) del numeral 04 del presente documento.

j) La topología física y lógica de la red WAN propuesta deberá permitir la conectividad de "todos contra todos" (Full Mesh) mediante el uso de esquemas de conmutación virtual.

k) Todos los equipos de comunicaciones instalados por el POSTOR deberán soportar configuraciones de QoS (Calidad de Servicio), aseguramiento de ancho de banda para aplicaciones TCP/IP y priorización de aplicaciones tanto en entrada como salida, a nivel de TCP/IP para aplicaciones de voz, video y datos. La calidad de servicio se refiere sólo al tráfico de salida en todos los dispositivos.

l) El POSTOR deberá proporcionar la información necesaria en idioma ingles y/o español que sustente las especificaciones técnicas de los equipos requeridos, para ello deberá adjuntar brochures o folletos donde se detalle las características mínimas solicitadas. Los equipos a incluir serán nuevos, sin uso y de tecnología vigente para ello deberá adjuntar brochures o folletos que correspondan a los equipos ofrecidos.

***Figura 48:** Requerimientos del cliente.*
***Fuente:** Términos de Referencia.*

CRONOGRAMA PARA EL CONCURSO PÚBLICO

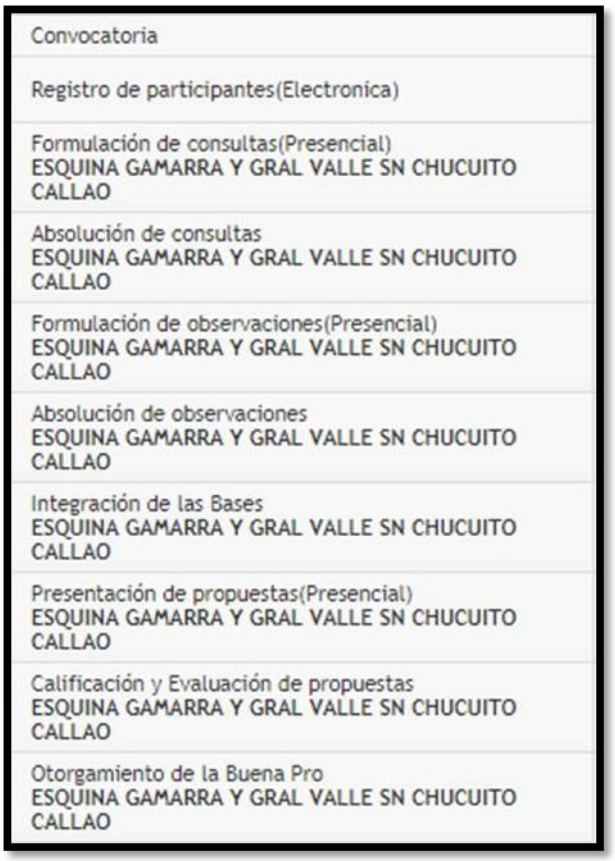


Figura 49: *Cronograma del Concurso Público.*
Fuente: *Pagina del SEACE.*

El valor con la que se obtuvo la Buena Pro del concurso Público fue de

S/. 7, 688,880.00 (Siete millones seiscientos ochenta y ocho mil ochocientos ochenta con 00/100 Nuevos soles)