ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

"EVALUACIÓN DEL PROTOCOLO MPLS CON LA APLICACIÓN DE VPN PARA MEJORAR EL RENDIMIENTO DEL SISTEMA DE TRANSMISIÓN DE DATOS DE LA CORPORACIÓN NACIONAL DE ELECTRICIDAD REGIONAL BOLÍVAR."

AUTOR: ROBERTO BERNARDO USCA VELOZ

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGISTER EN INTERCONECTIVIDAD DE REDES

Riobamba – Ecuador

Febrero 2018

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyecto de Investigacion y Desarrollo, titulado "EVALUACIÓN DEL PROTOCOLO MPLS CON LA APLICACIÓN DE VPN PARA MEJORAR EL RENDIMIENTO DEL SISTEMA DE TRANSMISIÓN DE DATOS DE LA CORPORACIÓN NACIONAL DE ELECTRICIDAD REGIONAL BOLÍVAR", de responsabilidad del señor Roberto Bernardo Usca Veloz, ha sido prolijamente revisado y se autoriza su presentación.

Ing. Wilson Armando Zuñiga Vinueza M. Sc **PRESIDENTE**	FIRMA
Ing. Geovanni Danilo Brito Moncayo Mg. **DIRECTOR DE TESIS**	FIRMA
Ing. Tatiana Paola Zambrano Valverde Mg. **MIEMBRO DEL TRIBUNAL**	FIRMA
Ing. Santiago Mauricio Altamirano Meléndez Mg. **MIEMBRO DEL TRIBUNAL**	FIRMA

Riobamba, Febrero de 2018.

DERECHOS INTELECTUALES

Yo, Roberto Bernardo Usca Veloz, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

.

_____

Roberto Bernardo Usca Veloz

C.I.: 0603981796

DECLARACIÓN DE AUTENTICIDAD

Yo, Roberto Bernardo Usca Veloz, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documeto que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

_____

Roberto Bernardo Usca Veloz

C.I.: 0603981796

DEDICATORIA

Dedico este trabajo a Dios, a mi madre, esposa e hijo. A Dios porque ha estado conmigo a cada paso que doy, cuidándome y guiándome por el buen camino para continuar, a mis padres, quienes a lo largo de mi vida han velado por mi bienestar, salud y educación. Además a mi esposa e hijo que estuvieron en todo momento a mi lado, siendo un pilar fundamental en mi vida. Depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad.

Roberto Bernardo Usca Veloz

AGRADECIMIENTO

Agradezco a Dios por haberme escoltado y guiado a lo largo de esta carrera por ser mi fortaleza en los momentos de debilidad.

Deseo del mismo modo expresar mi agradecimiento y gratitud a mi Tutor Ing. Geovanni Danilo Brito Moncayo. Mg., Miembros del tribunal Ing. Tatiana Paola Zambrano Valverde. Mg. e Ing. Santiago Mauricio Altamirano Meléndez. Mg. Y al Ing. Jefferson Naranjo.Msc. Por la confianza, apoyo, dedicación y por haber compartido conmigo sus sabios conocimientos sobre todo su amistad.

Del mismo modo a la Corporacion Nacional de Electricidad Regional Bolívar por permitir la realización del proyecto de investigación, cojuntamente con el personal técnico y administrativo que presto la información pertinente para la ejecución de la misma.

Extiendo este agradecimiento a la Escuela Superior Politécnica de Chimborazo y a sus Autoridades y docentes quienes me permitieron alcanzar uno más de mis objetivos personales.

Roberto Bernardo Usca Veloz

ÍNDICE DE CONTENIDO

Pg.

INDICE DE TABLAS

Pág.

INDICE DE FIGURAS

Pág.

INDICE DE GRÁFICOS

Pág.

LISTA DE ABREVIATURAS

ATM	Asynchronous Transfer Mode
CNEL	Corporación Nacional Eléctrica
FEC	Forward Error Correction
GRE	Generic Routing Encapsulation
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IOS	Sistema Operativo Móvil Apple
IP	Internet Protocol
IPSec	Internet Protocol security
LAN	Local Area Network
LSP	Label-switched path
LSR	Label Switching Router
MPLS	Multiprotocol Label Switchin
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
POP	Point of Presence
PVC	Private Virtual Circuits
QoS	Calidad en el Servicio
VLAN	Red de Área Local Virtual
VPN	Red Privada Virtual
VRF	Enrutamiento Virtual y Reenvío
WAN	Wide Área Network
WLAN	Wireless Local Área Network

INDICE DE ANEXOS

RESUMEN

El objetivo fue evaluar el rendimiento del protocolo MPLS con la aplicación de VPN y verificar su influencia en el sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

La información recolectada se analizo en el software Radio Mobile, posteriormente se realizo la topología de la red en GNS3, el cual interactúa con los diferentes equipos, protocolos, topología y configuraciones que se utilizan en tiempo real, en Modeler es un escenario donde se diseña las Topologías de redes, conectadas por varios routers.

Se realizo la evaluación del rendimiento de la red, planteando seis escenarios de prueba, para el estudio de la red existente sin la aplicación del protocolo MPLS/VPN, y con la aplicación MPLS/VPN, con los cuales se realiza una comparación cuantitativa de la evolución de estas topologías de red, se analizo estadísticamente por Chi cuadrado para comprobar la validez de los datos de la investigación en la cual se demostro la necesidad de implementar el protocolo MPLS con VPN para mejorar del rendimiento de la red existente.

Se concluye que con la implementación del protocolo MPLS se logra un ahorro de capacidades de procesamiento, equipos físicos, baja del retardo, fluctuaciones y porcentaje de utilización. En los datos de MPLS se nota favorablemente el rendimiento de la red y su conmutación de paquetes permitiendo que la red sea más segura y confiable en la transmisión de datos. Se recomienda la utilización de sistemas flexibles como es MPLS con la aplicación de VPN para mejorar el sistema de transmisión de datos.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <TELECOMUNICACIONES>, <REDES VIRTUALES PRIVADAS (VPN)>, <MULTIPROTOCOLO POR CONMUTACIÓN DE ETIQUETAS (MPLS)>, <RADIO MOBILE (SOFTWARE)>, <MODELER (SOFTWARE)>, <GNS3 (SOFTWARE)>.

SUMMARY

The objective was to evaluate the performance of the MPLS protocol with the VPN application and verify its influence on the data transmission system of the Bolivar National Electricity Corporation. The gathered information was analysed in the Radio Mobile software, then the topology of the network was made in GNS3, which interacts with the different equipment, protocols, topology and configurations that are used in real time. The Modeller is a scenario where it is designed Network topologies, connected by several routers. The performance evaluation of the network was carried out, proposing six test scenarios for the study of the existing network, with and without the application of the MPLS/VPN protocol, by which it was carried out a quantitative comparison of the evolution of these network topologies. It was statistically analysed using the Chi-square test to verify the validity of the research data, in which it was demonstrated the need to implement the MPLS protocol with VPN to improve the performance of the existing network. It is concluded that with the implementation of the MPLS protocol a saving of processing capacities, physical equipment, low delay, fluctuations and percentage of use is achieved. In MPLS data, the performance of the network and its packet switching are favourably noted, allowing the network to be more secure and reliable in data transmission. It is recommended to use flexible systems such as MPLS with the VPN application to improve the data transmission system.

Keywords: Technology and Engineering Sciences, Telecommunications, Virtual Networks (VPN), Multiprotocol Label Switching (MPLS), Radio Mobile (Software), Modeller (Software), GNS3 (Software).

CAPÍTULO I

1. PROBLEMA

1.1 Tema

Evaluación del protocolo MPLS con la aplicación de VPN para mejorar el rendimiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

1.2 Antecedentes

Desde sus inicios que datan a partir de la década de los años setenta las redes de comunicaciones han ido creciendo notablemente, y a su vez presentando grandes cambios debido a la inclusión vertiginosa del internet en todos los ámbitos de la sociedad, que ha exigido cambios acelerados en la infraestructura de las mismas con el propósito de abarcar la mayor cantidad de distancias y de llegar a la mayor población mundial posible, es por ello que en la actualidad se busca implementar tecnologías, estándares y protocolos eficientes que garanticen la confiabilidad de la transmisión de datos en redes de comunicación (Salcedo, Pedraza, & Espinosa, 2012).

Según los autores Espinosa, Salcedo, y Gómez, (2013) desde la década de los noventa a nivel mundial las redes de datos se introdujeron al mercado empresarial de negocios con la finalidad de mejorar eficiencia en procesos transaccionales rápidos y estables, con ello proveer servicios de acceso electrónico a sus usuarios, en la actualidad las redes virtuales (VPN) son uno de los servicios más importantes dentro de las telecomunicaciones de banda ancha con la aplicación de distintos protocolos que se adaptan a distintas realidades y que permiten cumplir con las características necesarias para mejorar el rendimiento de los sistemas de transmisión de datos.

Para mejorar el sistema de transmisión de datos es muy importante e imprescindible contar con un sistema de radioenlace, en la que sea eficiente y sobretodo confiable incorporando los servicios que permitan una agilidad en el rendimiento de la corporación, como son voz, video y datos. Donde la transferencia de información llegue a su destino sin problema alguno y los servicios prestados por el mismo sean lo más óptimo posible. Es por ello que se han desarrollado herramientas eficaces que permiten realizar la evaluación del rendimiento de la calidad de servicios aplicando protocolos y técnicas como lo es VPN con MPLS.

En el Ecuador en los últimos años se han introducido comunicaciones corporativas como estrategia para ofrecer mejores servicios y captar la mayor cantidad de usuarios, para esto se han implementado servicios que incorporan voz, datos y video permitiendo conectar instalaciones separadas por grandes distancias mediante red de datos aumentando el beneficio y garantizando la confiabilidad de su información transmitida. Es así que Instituciones telefónicas (Claro, Movistar, CNT, entre otras) se han visto en la necesidad de incorporar tecnología sofisticada que garantice la confiabilidad de su información compartida, que mejore su productividad y competitividad. Lo que se ha plasmado en la implementación de redes privadas virtuales con la aplicación de protocolos (L2TP, MPLS, IPSEC, entre otros) que permiten mantener la interconexión de todas las sedes de una empresa manteniendo la integridad de las mismas.

Se realiza una revisión bibliográfica de investigaciones relacionadas con el tema y que tienen resultados positivos en la investigación.

- ✓ Revelo, (2014) estudia el impacto de túneles MPLS en la topología de internet, mismo que llega a valorar los métodos para vincular los LSR (Label Switching Router) dentro de un LSP (Label-switched path) y por otro lado presenta un disertación basado en la teoría de grafos para determinar de una mejor manera las características que presentan las redes MPLS y la interacción con las redes de IP (Internet Protocol) en Internet.

- ✓ Ullauri, (2015) menciona que el implementar MPLS en empresas medianas y grandes es unos de los requisitos fundamentales actualmente; es por ello que tener el adecuado diseño de las redes, es un requisito fundamental para el crecimiento y buen desempeño de cualquiera de las mismas.

- ✓ La VPN basada en protocolos MPLS se implementa en un ambiente donde toda la organización está conectada en una red de datos privada y requiere mayor velocidad en la transmisión de datos. En este escenario se implementa la topología de hub y spoke; la que establece la conectividad entre los sitios y también las decisiones de reenvío se hacen sobre la base de etiquetas MPLS en lugar de direcciones de protocolos de internet (Ahmed, Butt, & Siddiqui, 2016).

- ✓ Como mencionan Shahzad & Hussain, (2013) los modelos propuestos existentes con técnicas de despliegue de redes privadas virtuales con MPLS muestra mucha flexibilidad, escalabilidad, capacidad y beneficios de ingeniería en tráficos de datos en comparación con las redes VPN tradicionales basadas en IP.

1.3 Planteamiento del problema

Este trabajo investigativo se enfoca en el estudio del rendimiento de sistemas de transmisión de datos, mediante la evaluación de las nuevas tecnologías en las redes actuales, bajo mecanismos de transporte de datos como MPLS aplicando VPN y garantizando un buen rendimiento de sistemas de transmisión de datos.

Desde hace décadas ha concurrido muchas investigaciones científicas, y sus resultados apuntan que las entidades públicas y privadas es necesario poseer un mecanismo de encriptación de datos para los sistemas de redes, así como comenta (Camacho, 2015). La Ingeniería de Tráfico en redes MPLS ofrece importantes herramientas de optimización de red que logran ser utilizadas en situaciones de congestión, mediante el mecanismo de túneles que permiten enrutar el tráfico en caminos diferentes al definido por el IGP (Interior Gateway Protocol), obteniendo así excelentes niveles de rendimiento de red y optimización en la utilización de los recursos disponibles.

Es por ello que muchas empresas se han visto en la necesidad de incorporar nuevas tecnologías que permitan el correcto rendimiento de sus sistemas de transmisión de datos ya que toda su competitividad depende de la misma.

Corporación Eléctrica Regional Bolívar cuenta con doce agencias que constituyen los puntos de recaudación y atención al cliente, y preocupada en mantener el mejor servicio y atención al cliente busca en conocer las mejores alternativas que permitan mantener la integridad de su red de datos como también la eficiencia de la misma. Esto a consecuencia de que se ha detectado bajo rendimiento del sistema debido a inestabilidad, retardo en la transmisión de datos, disminución en la flexibilidad y velocidad de la red, lo que ahondado la necesidad de implementar nuevas técnicas que permitan contrarrestar los problemas presentados y a su vez permitan expandir las funcionalidades de la infraestructura de la red garantizando un alto rendimiento de la misma.

El presente trabajo contribuye con conocimientos en la evaluación de las nuevas tecnologías en las redes actuales, bajo mecanismos de transporte de datos como MPLS creado por la IETF (Internet Engineering Task Force) aplicando VPN y garantizando un buen rendimiento de sistemas de transmisión de datos.

1.4 Formulación del problema

¿La evaluación del protocolo MPLS con la aplicación de VPN permite mejorar el rendimiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar?

1.5 Delimitación del objeto de investigación

1.5.1 Delimitación del contenido

Área:	Interconectividad
Campo:	Redes
Aspecto:	Evaluación del protocolo MPLS

1.5.2 Delimitación espacial

La investigación se desarrolló en la Corporación Nacional de Electricidad Regional Bolívar.

1.5.3 Delimitación temporal

El trabajo investigativo se realizó durante el año 2017.

1.6 Justificación

En la era actual de las comunicaciones, es necesario e imprescindible realizar estudios de las distintas tecnologías existentes para la eficiente operacionalización de los sistemas de transmisión de datos. Por lo que en esta investigación se propone realizar el análisis teórico y práctico mediante simulación del Protocolo MPLS con la aplicación de VPN que permita obtener datos que coadyuven a un mejoramiento en el rendimiento de sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

Es por ello que para la eficiente operacionalización de la red de datos de una empresa se busca integrar tecnología que permita constituir todas las funcionalidades que presten la calidad de servicio lo más eficiente posible, integrando en su red voz, datos y video, permitiendo la compartición de la información y agilitando tareas que estén involucradas en la Corporación.

Además, mediante el análisis de dicho protocolo se cuenta con normas de seguridad vigentes, así como también con parámetros que permitan evaluar el rendimiento de MPLS/VPN, la eficiente operacionalización del sistema de transmisión, generando una disminución de costos en el mantenimiento y la posibilidad de incremento en su cobertura.

La corporación puede incorporar voz, video y datos en su red con la calidad de servicios que es muy imprescindible en la era actual de la información con los distintos requerimientos que hacen posible el mayor tráfico de la red teniendo en cuenta el ancho de banda, latencia, jitter, disponibilidad y seguridad permitiendo que estas redes sean escalables y con un bajo costo de interconectar subredes privadas de cualquier empresa en una sola red lógica como es el servicio de internet.

Se desarrolla pruebas a través de simuladores que permitan diseñar topologías de redes y estudiar en tiempo real los datos arrojados por el mismo permitiendo un mejor manejo de los requerimientos para futuras redes backbone basados en protocolo IP. Además, está orientada al Plan Integral de Seguridad Nacional, en donde las redes MPLS/VPN están dentro de esta necesidad que tiene cada organización empresarial.

Los beneficiarios principales son los usuarios de toda la provincia de Bolívar por el ágil y oportuno servicio de recaudación, así como también la Corporación Nacional de Electricidad Regional Bolívar que mejora el rendimiento del sistema de transmisión de datos con la aplicación de MPLS/VPN. Cabe recalcar, que en la era actual donde prima el uso de información es de vital importancia que la institución cuente con servicios que optimicen la transmisión de la información, de manera que esta sea competitiva y se convierta en un modelo a seguir por instituciones con sistemas similares.

Por lo tanto, es de vital importancia la realización del estudio ya que se elabora una Guía de implementación que contribuye con procesos de investigaciones similares que serán enmarcados para indagaciones futuras.

El aporte de la investigación se materializa en sistemas de conocimientos sobre la transmisión de datos con la aplicación de MPLS/VPN, sobre su comportamiento en los escenarios propuestos, así desarrollando una Guía de implementación de un Sistema de Transmisión de Datos basado en el protocolo MPLS con la aplicación de VPN para orientar en la consecución de proyectos similares. Con el cual se realiza el estudio necesario para mejorar el rendimiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

1.7 Objetivos

1.7.1 Objetivo general

Evaluar el protocolo MPLS con la aplicación de VPN para mejorar el rendimiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

1.7.2 Objetivos específicos

- ✓ Analizar el protocolo MPLS con la aplicación de VPN para respaldar teóricamente condiciones y requerimientos técnicos de un sistema de trasmisión de datos.

- ✓ Diseñar la Topología y radioenlace de la red de datos basado en el protocolo MPLS con la aplicación de VPN.

- ✓ Evaluar el rendimiento de la red y el tráfico de datos del sistema de transmisión de datos planteando escenarios de efectividad de la red.

- ✓ Desarrollar el procedimiento de configuración de un sistema de transmisión de datos basado en el protocolo MPLS con la aplicación de VPN para la Corporacion Nacional de Electricidad Regional Bolivar.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Redes Corporativas

La proliferación de nuevas tecnologías, que admiten la compartición de recursos por multitud de usuarios, un ejemplo, LAN, esta capacidad de transmisión se ejemplariza insuficiente, y se hace preciso el disponer de otras redes que permitan la interconexión e integración de distintos sistemas y equipos que componen la red corporativa, a mucha mayor velocidad. (Solsona, Moya, & Calero, 2016)

Es por ello que las redes corporativas permiten conectar todas las localizaciones de una empresa en particular de manera permanente, privada, segura y fiable a través de la tecnología MPLS aplicada en una red privada virtual que consienta el intercambio de la información, ya sean voz, datos y video, de manera que este sistema admita la rapidez, seguridad y sobretodo estar preparada para garantizar la calidad de servicios, lo cual se quiere obtener en el proyecto de investigación.

2.2 Transmisión de datos

Tiene como objetivo principal la transmisión de información de un lugar conocido como fuente hacia un receptor por medio de un canal. Que también depende del medio de transmisión de datos que se esté utilizando, ya sea medios transmitidos guiados o no guiados. Donde las particularidades básicas que se tiene en consideración son: ancho de banda, problemas de transmisión, interferencias, espectro electromagnético, entre otros. (Solsona, Moya, & Calero, 2016)

Los sistemas de transmisión de datos son todos los enlaces que excedan de 20m, donde las redes puedan conectar varias terminales de cómputo de edificios lejanos con la computadora principal de un centro especializado de datos. (Rodríguez & Vazquez, 2015)

2.3 Protocolos

Es un método estándar que nos permite la interconectividad entre procesos que se ejecutan en diferentes equipos. Por lo cual se utiliza un conjunto de reglas y diferentes procedimientos que

permiten ejecutar el proceso de envío y recepción de datos por medio de una red, y está dependiendo del protocolo que se esté usando para el intercambio de comunicación. (Rodríguez & Vazquez, 2015)

2.4 Protocolo MPLS

MPLS (Multi-Protocol Label Switching) es una tecnología de paquetes que comnutan en la capa tres que efectúa enrutamiento de tráfico de datos de manera efectiva, facilita el despliegue de técnicas de QoS y está estandarizada por la (IETF) (Valladares, 2014)

Según (Valladares, 2014), menciona que MPLS utiliza la técnica de conmutación de etiquetas que proporciona la posibilidad de administrar el tráfico de una red a través de etiquetas en las cabeceras de los paquetes y a routers específicos preparados de reconocerlas. Principalmente consiste en integrar los niveles de enlace y red eficazmente. Es decir, ajusta la inteligencia del routing con la velocidad del switching. (pág.18)

2.4.1 Funcionamiento de MPLS

Una red MPLS esencialmente funciona modificando las etiquetas de un paquete que previamente ya está etiquetado. Cuando un paquete se envía de un computador A, a un computador B, mediante la configutacion de una red MPLS, y la secuencia que sigue se evidencia en la Figura 1-2. (System, 2006).

Figura 1-2: Funcionamiento MPLS
Fuente: (Valladares, 2014)

A razón de la secuencia anteriormente mencionada se indica que el paquete enviado sale desde un computador para llegar al router que se encuentra en la subestructura interna, luego el paquete llega hasta un router con particularidades MPLS el cual es designado Router Extremo de Ingreso (Ingress Label Edge Router). En este punto se examina el destino del paquete, esto varía si el paquete proviene de una red ATM y una red IP. La peculiaridad de que MPLS difiera de la tecnología de comunicación global de redes implementadas es una de las superioridades que posee esta tecnología, ya que el mismo puede empezar a funcionar sobre redes que ya existen y no es necesario invertir en más hardware, esto se logra hacer sobre el hardware existente con cualquiera actualización de software.

En la Figura 2-2, se enuncia que el QoS (Calidad en el servicio) permite utilizar todos los recursos de la red puesto que, no necesariamente se van a utilizar las líneas más rápidas, o de tal forma se pueden utilizar todos los recursos de un modo más óptimo.

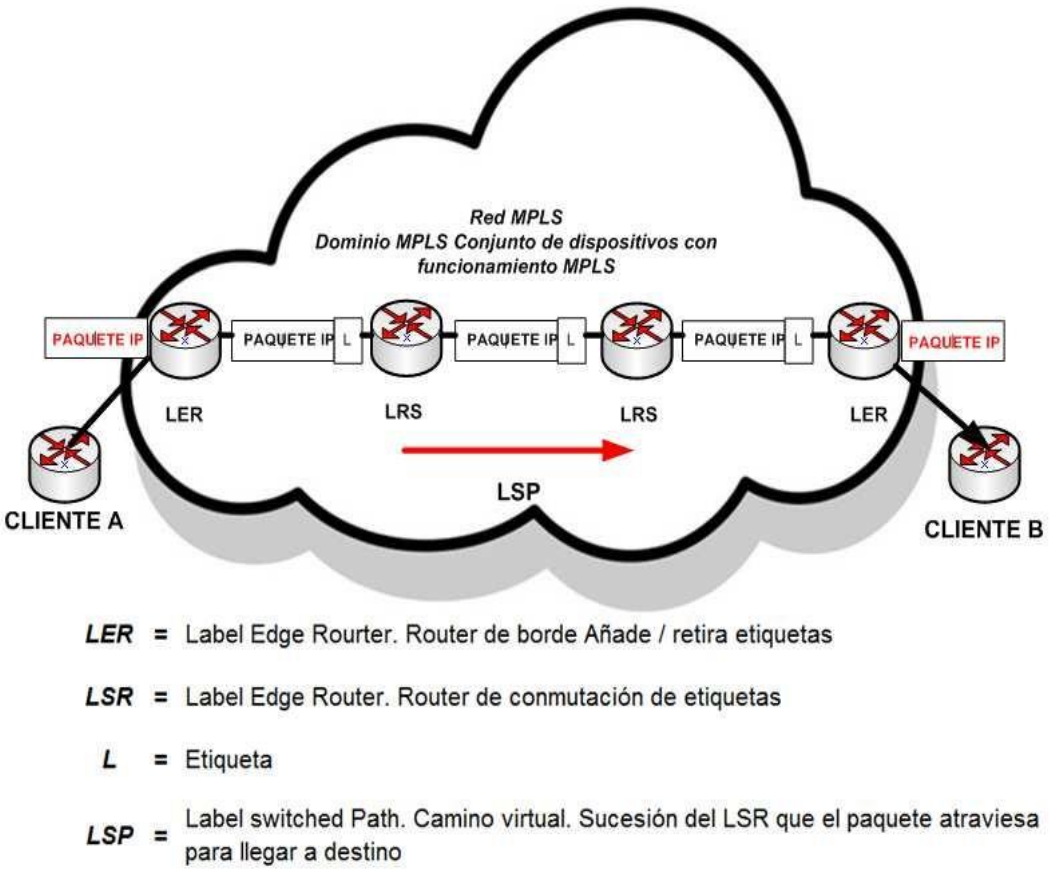


Figura 2-2: Funcionamiento de MPLS
Fuente: (Valladares, 2014)

Tabla 1-2: Funcionamiento de protocolos MPLS

Funcionamiento generalizado de protocolos MPLS	
1	Para determinar qué etiqueta asignarle al paquete se debe comparar con las etiquetas situadas en las tablas de enrutamiento que se van suministrando desde la dirección destino a la dirección fuente transferidos por medio de diminutos mensajes entre los routers. Normalmente ese camino es decidido antes de que se envie la información; el camino se forma en las tablas de enrutamiento cuando los dispositivos son conectados a la red.
2	Una vez que ya se tienen las tablas de enrutamiento al paquete se le asigna una etiqueta la cual va cambiando en cada conmutador o enrutador MPLS al que llega simplemente revisando esa etiqueta.
3	El paquete sigue su camino hasta que llega al enrutador extremo de egreso (Egress Label Edge Router) en el cual se le quitan todas las etiquetas que tenía y llega a la computadora destino o simplemente sale de la red MPLS.
4	Uno de los protocolos más usados en sistemas autónomos MPLS es OSPF (Open shortest path first) ya que por ser dinámico distribuye automáticamente la información de ruteo entre los equipos activos que compone una red WAN. Otras características importantes es que permite habilitar tanto enlaces redundantes como balanceo de carga.
5	Todas estas características son necesarias de tomar en cuenta ya que en la actualidad las redes de datos son de gran tamaño y transportan diversidad de información y aplicaciones.

Fuente: (Valladares, 2014)

El funcionamiento de los protocolos MPLS primeramente designa la etiqueta al paquete de datos indicándole su dirección de destino, posterior a ello revisar las etiquetas y distribuye automáticamente la información de ruteo entre los equipos activos, como se observa en la Tabla 1-2.

2.4.2 Aplicaciones de MPLS

Según Camacho, (2015) una red de comunicaciones IP y MPLS de extremo a extremo ayuda a las organizaciones públicas y privadas a encontrar un equilibrio entre las imposiciones de negocio

presentes y los objetivos del futuro. IP/MPLS se ha trasformado en la tecnología de elección para el backbone primordial de transmisión de datos a nivel nacional para todo tipo de empresa.

En la Figura 3-2, se identifica los medios aplicativos del protocolo MPLS, con este precedente y tomando en consideración que los administradores y usuarios de estas redes requieren cada vez un mayor grado de seguridad en la transmisión de los datos conciderando varios requerimientos.

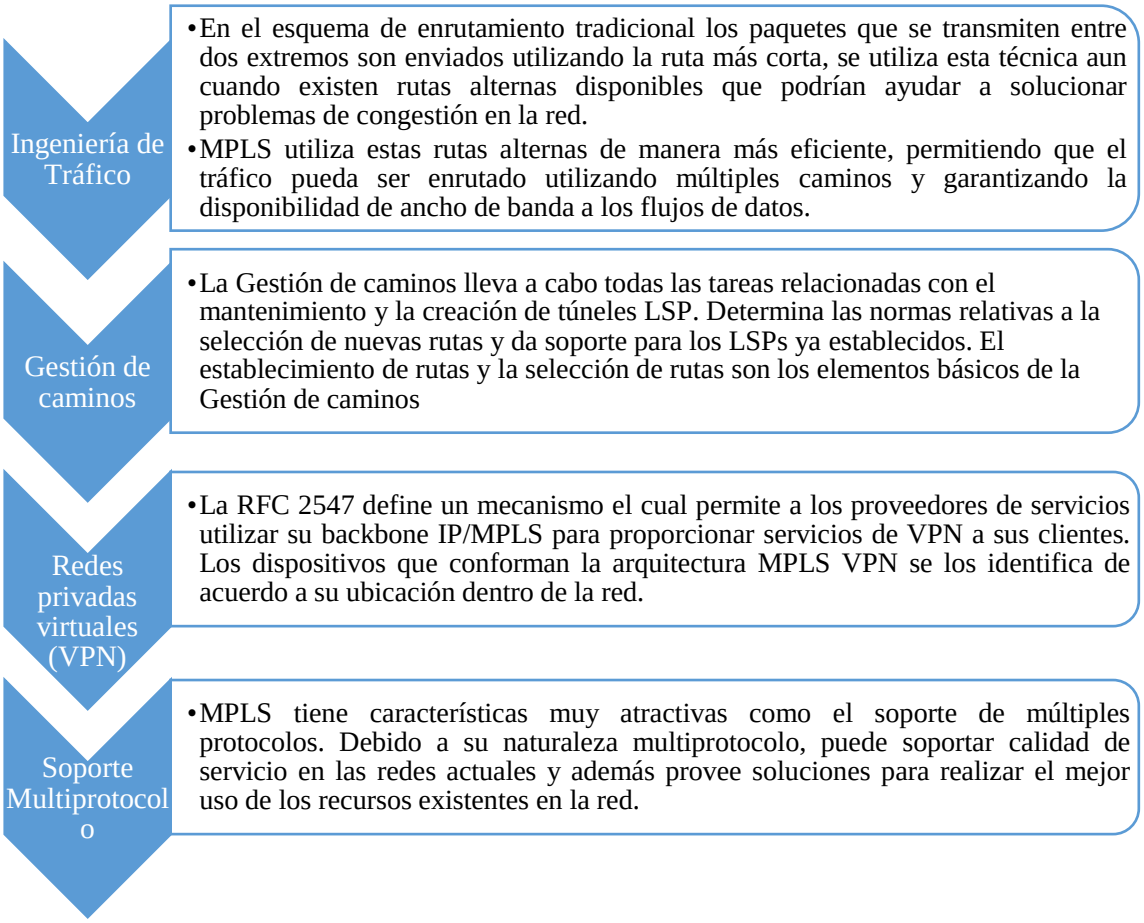


Figura 3-2: Aplicaciones MPLS
Fuente: (Camacho, 2015)

2.4.3 Beneficios principales de ingeniería de tráfico MPLS

Según (Morales, 2017)

- ✓ Permite al eje troncal (backbone) expandirse sobre las capacidades de la ingeniería de tráfico de las redes del tipo Modo de Transferencia Asíncrona (ATM) y Frame Relay de Capa 2.

- ✓ La ingeniería de tráfico es fundamental para los ejes troncales de proveedores de servicios. Estos ejes deben soportar una utilización elevada de su capacidad de transmisión.

- ✓ Utilizando MPLS las capacidades de ingeniera de tráfico son relacionadas e integradas a la Capa tres (OSI) lo que optimiza el ruteo de tráfico IP gracias a las guías establecidas por la topología y las capacidades de la troncal.

- ✓ La ingeniería de tráfico MPLS rutea el tráfico a lo largo de la red basándose en los recursos que el flujo requiere y en los recursos disponibles en la totalidad de la red.

- ✓ MPLS emplea la ruta más corta que cumpla con los requisitos del flujo de tráfico, que incluye: requisitos de ancho de banda, de medios y de prioridades sobre otros flujos.

2.4.4 Ventaja MPLS sobre otras tecnologías

El investigador Morales, (2017). Indica que las soluciones más comunes para implementar redes privadas son las siguientes:

- ✓ Frame Relay: Es un protocolo de transporte orientado a la conmutación de paquetes manejando velocidades desde 2.4 hasta 45 Mbps

- ✓ Circuitos ATM (Modo de transferencia asíncrona)

- ✓ Túneles tradicionales IP-IP y GRE, (Generic Routing Encapsulation y protocolos de internet).

- ✓ IPSec: Seguridad de protocolo de internet

- ✓ L2F: Reenvío de capa 2

- ✓ PPTP: Protocolo de tuneles punto a punto

- ✓ L2TP: Protocolos de tuneles de capa 2

- ✓ MPLS (a manera de comparación)

2.4.5 Ventajas específicas de MPLS

En el presente listado se presenta el dominio y las aptitudes que benefician el aspecto más relevante del protocolo MPLS y cuál es la mejora en el tráfico de datos, y los parámetros de mayor influencia, las mismas se analizan en la Tabla 2-2:

Tabla 2-2: Ventajas especificas del MPLS

N°	Ventajas
1	Un domino MPLS consiste de una serie de routers habilitados con MPLS continuos y contiguos. El tráfico puede entrar por un punto final físicamente conectado a la red, o por otro router que no sea MPLS y que esté conectado a una red de computadoras sin conexión directa a la nube MPLS.
2	Se puede definir un Comportamiento por Salto (PHB) diferente en cada router de la FEC. El PHB define la prioridad en la cola y las políticas de desechado de los paquetes.
3	Para determinar el FEC se pueden utilizar varios parámetros que define el administrador de la red. a. Dirección IP fuente o destino y/o las direcciones IP de la red. b. Utilizar el ID del protocolo IP. c. Etiqueta de flujo IPv6. d. Numero de puerto de la fuente o del destino. e. El punto de código (codepoint) de los servicios diferenciados (DSCP).
4	El reenvío de la información se lleva a cabo mediante una búsqueda simple (lookup) en una tabla predefinida que enlaza los valores de las etiquetas con las direcciones del siguiente salto (next hop).
5	Los paquetes enviados de mismos end points pueden tener diferente FEC, por lo que las etiquetas serán diferentes y tendrán un PHB distinto en cada LSR. Generar diferentes flujos en la misma red.

Fuente: (Morales, 2017).

2.5 Redes virtuales privadas (VPN)

De acuerdo a Valladares, (2014) una red privada virtual (VPN) se define en términos generales como una red privada que permite la conectividad de varios beneficiarios entre múltiples sitios, los cuales están dentro de una infraestructura de red compartida. En este sentido los autores Espinosa, Salcedo, y Gómez, (2013) comentan que una red de comunicaciones IP y MPLS de extremo a extremo beneficia a las organizaciones públicas y privadas a encontrar un equilibrio entre los requerimientos de negocio asistentes y los objetivos del futuro. IP/MPLS se ha trasformado en la tecnología de elección para el backbone primordial de transmisión de datos a nivel nacional para todo tipo de empresa.

Con este precedente y tomando en consideración que los administradores y usuarios de estas redes requieren cada vez un mayor grado seguridad para la transmisión de los datos es ineludible considerar varios requerimientos.

Una red privada virtual (VPN) se elabora basado en conexiones realizadas sobre una infraestructura compartida, con funcionalidades y de seguridad de red equivalentes a las que se consiguen con una red privada.

El objetivo principal de las redes VPN es la asistencia de aplicaciones intranet/extranet, integrando diligencias multimedia de video, voz y datos sobre las infraestructuras de comunicaciones rentables y eficaces. La seguridad en redes presume reclusión, y "privada" muestra que el usuario "cree" que tiene los enlaces.

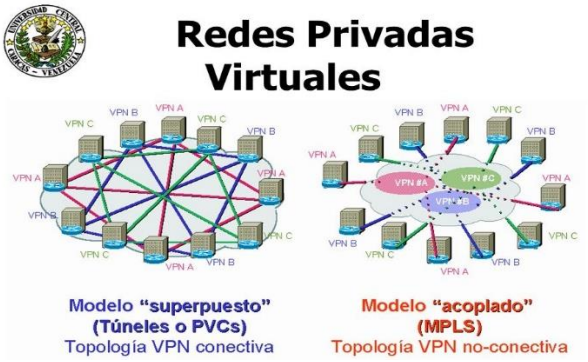


Figura 4-2: Redes Virtuales Privadas
Fuente: (Valladares, 2014)

En el Figura 4-2 se realiza una comparación entre el modelo de túneles (PVCs - Private Virtual Circuits) y un modelo de LSPs (label-switched path) de MPLS. La discrepancia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que las personas creen dentro de la red, basados en LSPs, y no de extremo a extremo a través de red.

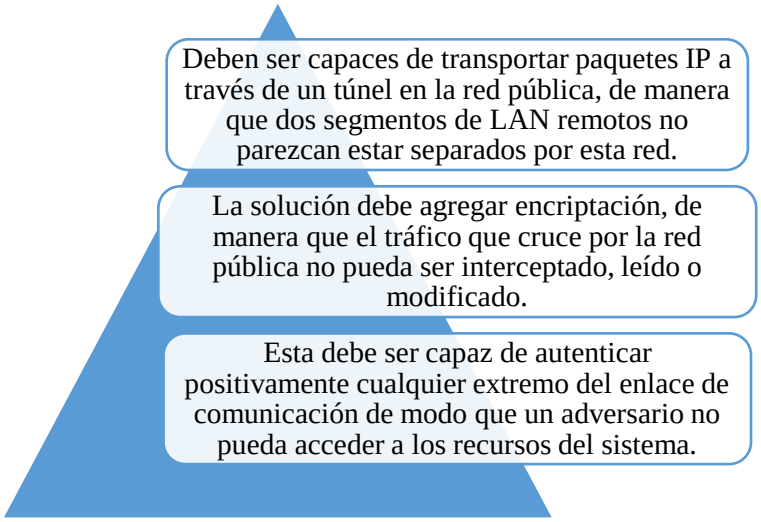


Figura 3-2: Tareas para lograr funcionalidad, redes seguras, privadas y virtuales.
Fuente: (Valladares, 2014)

Para ejecutar un enlace interno o privado, todos los datos enviados son encriptados en la red para tratar de tener confidencialidad en la informacion. Los paquetes que tratan de ser interceptados en toda red pública o compartida los cuales son indescifrables, así como se menciona en la Figura 5-2.

2.5.1 Tipos de topologías VPN

a) Topología HUB-AND-SPOKE

La topología que usualmente es la más utilizada es una topología hub-and- spoke, donde un número de centros remotos (spokes) se conectan a un espacio central (hub), como se modela en la Figura 6-2. Los centros remotos frecuentemente pueden intercambiar datos (no hay restricciones de seguridad explícitas entre centros de tráfico de datos), pero la cantidad de datos transferidos entre si es insignificante.

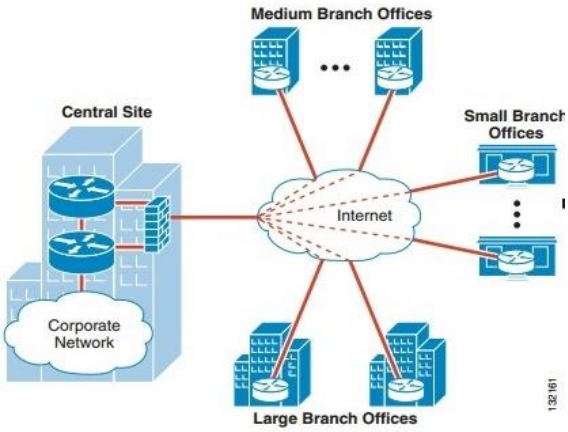


Figura 4-2: Topología Hub-Spoke
Fuente: (Valladares, 2014)

b) Topología malla parcial

El modelo de malla parcial es aquel en donde los sitios que disponen de una VPN están conectados por circuitos virtuales de acuerdo a la necesidad de un tráfico que los mismos requieran. Si uno o varios puntos remotos no disponen conectividad directa a todos los otros sitios que existen sometidos en la solución de comunicación la topología se llama una malla parcial; si cada uno de estos sitios tiene una conexión directa con cada otro sitio correspondiente, y por tal motivo la topología se le identifica con el nombre de malla completa. (Morales, 2017)

Una malla parcial no proporciona el nivel de redundancia de una topología de malla completa pero su ejecución es más económica. Las topologías de malla parcial generalmente se utilizan en

las redes periféricas que se conectan a un backbone de malla completa un ejemplo se puede ilustrar en la Figura 7-2.

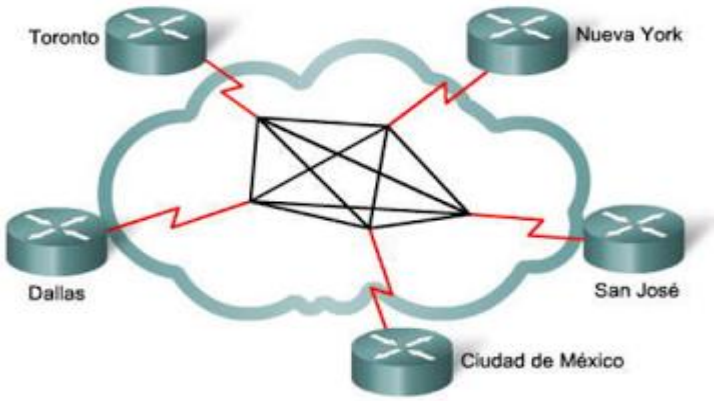


Figura 5-2: Topología malla parcial
Fuente: (Valladares, 2014)

c) Topología híbrida

La topología híbrida es una topología que utiliza VPN superpuestas y que combina los dos tipos de topología hub-and-spoke y la de malla parcial. Por ejemplo, una gran organización regional puede tener redes de acceso en cada provincia implementado con una topología de hub-and-spoke, mientras que la red central provincial se llevaría a cabo con una topología de malla parcial. El Figura 8-2 se muestra un ejemplo de tal organización.

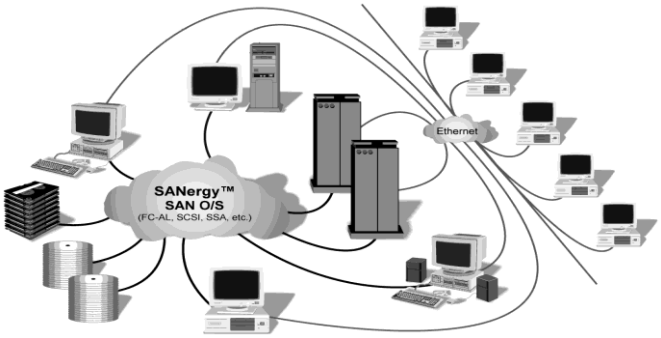


Figura 6-2: Topología Hibrida
Fuente: (Valladares, 2014)

2.5.2 Tipos de VPN (Nivel funcional)

Según Valladares, (2014) complementa que las mas comunes son 4 maneras claramente identificadas como se observa en la Figura 9-2.

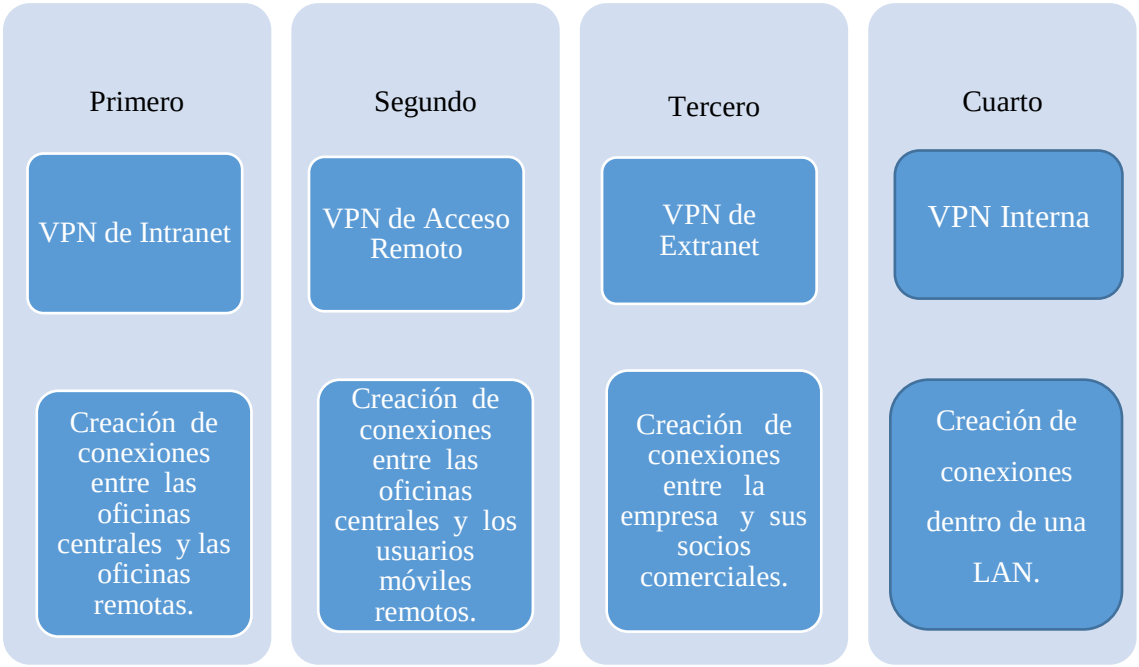
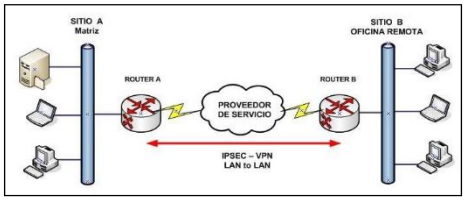
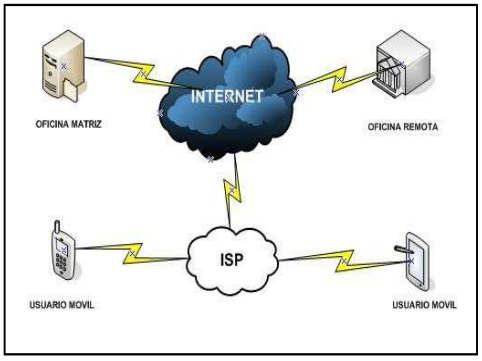
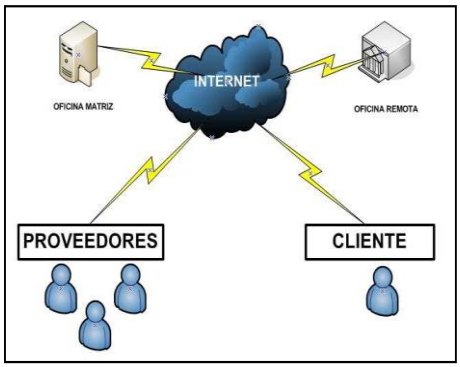
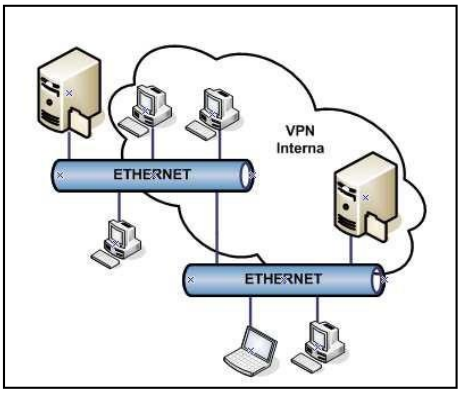


Figura 7-2: Implementaciones generalmente utilizadas en una VPN
Fuente: (Valladares, 2014)

Para implementar VPN es necesario conocer las características de conexión y beneficios establecidos en cada sistema, las cuales son VPN de Intranet, VPN de acceso remoto, VPN extranet y VPN de interna, se especifica en la Tabla 3-2.

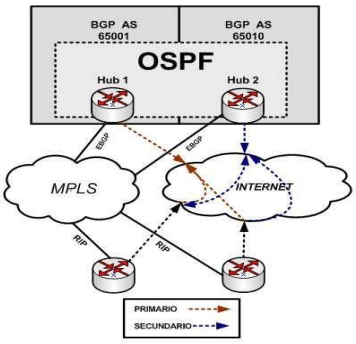
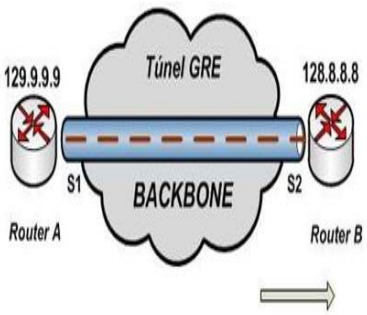
Tabla 3-2: Implementaciones generalmente utilizadas en una VPN

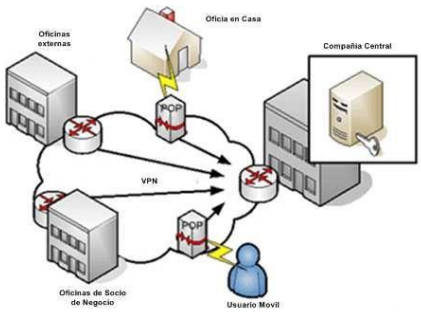
Tipo	Detalle	Descripción
VPN de Intranet	Esta implementación está dada por la creación de una conexión entre las oficinas centrales corporativas y las oficinas remotas que se encuentran en el exterior.	
VPN de Acceso Remoto	Una red privada virtual de acceso remoto se crea entre las oficinas centrales corporativas y los usuarios móviles remotos a través de un ISP. El usuario móvil levanta una conexión con un ISP y crea un túnel de conexión hacia las oficinas centrales corporativas.	

VPN de Extranet	Una red privada virtual de Extranet se crea entre la empresa y sus socios comerciales (clientes, proveedores), mediante el protocolo HTTP, que es el común de los navegadores de Web, o mediante otro servicio y protocolo ya establecido entre las dos partes involucradas.	
VPN Interna	Una red privada virtual interna, es una implementación que no tiene un uso frecuente en el entorno de las redes. Este tipo de implementación se crea en una LAN, siempre que se considere necesario transferir información con mucha privacidad entre departamentos de una empresa.	

Fuente: (Valladares, 2014)

Tabla.4-2: Tipos de VPN (Nivel técnico)

Tipo	Detalle	Descripción
VPN dinámicas (DMVPN)	Una de las principales preocupaciones y desafíos que existe al momento de la implementación de VPN sitio a sitio usando la topología Hub & Spoke con un gran número de sitios remotos es la escalabilidad que debería tener.	
Encapsulación de paquetes GRE	La implementación del protocolo GRE este protocolo es viable para ser aplicada en infraestructuras pequeñas, ya que por el tipo y cantidad de información utiliza menos recursos. VPN GRE, es una tecnología que proporciona un	

	mecanismo para hacer un túnel con paquetes de conmutación de protocolo (MPLS) sobre una red que no sea MPLS.	
Redes privadas virtuales - EASY VPN	La implementación de Easy – VPN, es una solución ideal para oficinas remotas con escaso soporte de TI o para las grandes instalaciones de equipos CPE (Customer Premises Equipment) de clientes en los que es poco práctico para configurar varios dispositivos remotos de forma individual.	

Fuente: (Valladares, 2014)

En la Tabla 4-2 se puede evidenciar los tipos de redes VPN caracterizado a nivel técnico, las cuales se consideran como: VPN dinámicas, encapsulación de paquetes GRE (Generic Routing Encapsulation) y Redes privadas virtuales EASY VPN.

2.6 Interconectividad de redes

Se considera como la comunicación que existe entre dos o más redes. Con la importancia de compartir los recursos y mantener un acceso a las bases de datos existentes y compartidas de manera instantánea, donde el administrador de la red tenga manipulación y efectivo control de una manera centralizada y monitorizada en todo instante, para consolidar esfuerzos y brindar solución a cualquier problema. (Aguilar, 2010)

(Real, 2012) Afirma. “La plataforma que conforma las redes de datos, y de la cual hoy en día dependen nuestras relaciones sociales y de negocios, se basa en un conjunto de tecnologías y servicios en donde se diseñan, desarrollan y mantienen redes modernas, en su mayoría completamente heterogéneas” (p.1)

2.6.1 Dispositivos de una red

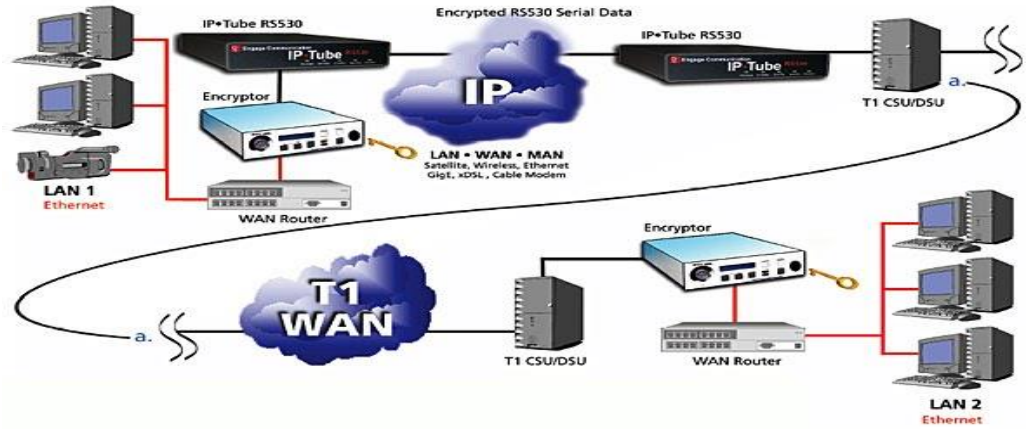


Figura 8-2: Interconexión de redes
Fuente: (Buettrich, 2007)

En la Figura 10-2, se evidencia los dispositivos principales que se considera dentro de una red, generalmente son:

- ✓ Enrutadores
- ✓ Conmutadores
- ✓ Firewalls
- ✓ Servidores

Como se puede observar en el Figura anterior, se encuentra una red que permite la compartición de los recursos con los distintos dispositivos de conexión que a su vez involucrando diversas tecnologías que permite la interconexión entre sí.

2.6.2 Importancia de la conectividad de redes

La importancia radica en que nuestra actual forma de vida globalizada nos exige a ser omnipresentes, para no transportar todo lo que necesitamos a todas partes se plantea el uso de una red que facilite y permita tener siempre a la mano cualquier cosa sin importar la ubicación geográfica en la que se encuentre las personas. (Real, 2012)

Según (Real, 2012) indica que la importancia y necesidad de estudiar la interconectividad de redes, radica en:

- ✓ Poder interconectar redes heterogéneas, sin importar el hardware, software y medios de comunicación.

- ✓ No tener limitaciones por distancias, tamaños de paquetes, ancho de banda ni potencia de transmisión.
- ✓ Contar con mayor seguridad, confiabilidad y desempeño.
- ✓ Facilidad de escalamiento, configuración, aislamiento, así como prevención y corrección de fallas. (p.1)

Además, se considera parte fundamental; la modalidad de compartir recursos dispersos coordinación de tareas, reducción de costos, incremento de la red geográficamente como físicamente, segmentación de la red y conversión de varios protocolos. Por lo cual se debe considerar aspectos principales a la hora de diseñar la red que se desea implementar.

2.6.3 Diseño de redes de datos

Para el diseño de la red de datos que se desea implementar es muy importante considerar la estructura física de la red, ya que un excelente diseño de la misma permite evitar problemas como; la pérdida de datos, caídas continuas de la red, problemas en la demora de procesamiento de la información transmitida, dificultad en la seguridad informática y sobretodo la estabilidad de la red en un futuro. (St-Pierre & Stéphanos, 2005). En la cual se diseña mediante software comúnmente utilizado como; radio-mobile o link-planner que permita los cálculos correspondientes en el diseño de la red de transmisión de datos.

Según (St-Pierre & Stéphanos, 2005) , la metodología para el diseño de una red consta de:

- Preparación de un plan de diseño
- Análisis de la red en el sitio
- Definición de nuevas exigencias
- Estudios de viabilidad
- Determinación del tamaño de la red
- Cálculo del tráfico de la red
- Elaboración de un sistema de seguridad y control
- Configuración de la red
- Evaluación del costo
- Implantación

- Administración

2.6.4 Redes de comunicación

Como menciona (Pacheco, 2008). “Una red de comunicaciones es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los dispositivos.” (pág.1)

Es lo tanto se considera al conjunto de los medios técnicos que acceden realizar la comunicación a distancia entre distintos equipos autónomos, transmitiendo audio, video y datos, mediante ondas electromagnéticas por varios medios como: Cable de cobre, fibra óptica aire, vacío, entre otras. Además, la comunicación entre los distintos nodos se los puede efectuar de forma análoga, digital o mixta. Donde la velocidad de trasmisión depende del ancho de banda con el que se esté ejecutando y de otros factores que se toman en consideración a la hora del diseño de una red.

2.6.5 Redes de comunicación conmutadas

Como afirma (Tigridae, 2017). “Las redes de comunicación permiten establecer un camino entre dos o más puntos, compuesto por transmisores y receptores a través de nodos o diversos equipos de trasmisión. Por lo tanto, la conmutación permite la entrega de la señal transmitida desde su origen hasta el nodo de destino constituido por su receptor.” (pág.1)

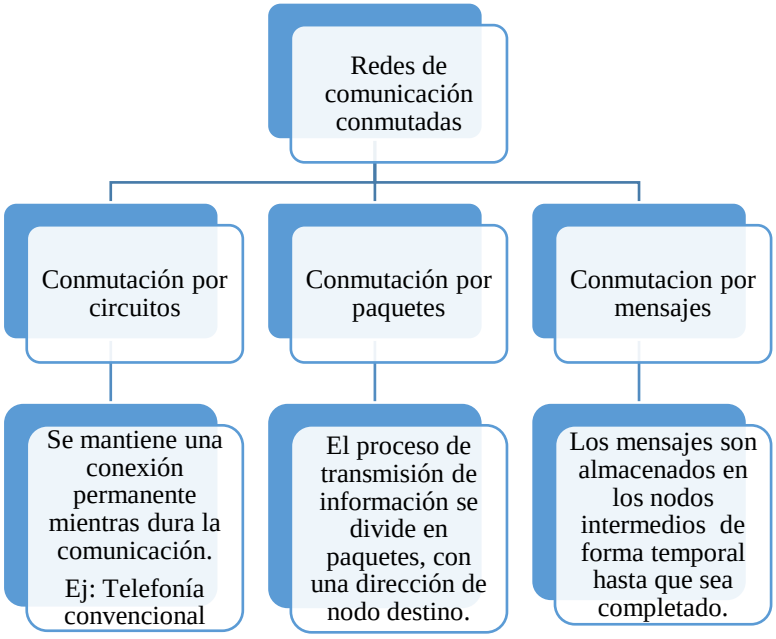


Figura 9-2: Clasificación de redes de comunicación conmutadas
Elaborado por: Roberto Usca, 2017

Como se puede observar en el Figura 11-2, se tiene tres tipos de conmutación. En la cual el proyecto de investigación está orientado en la conmutación de paquetes, aplicando MPLS/VPN considerando los requerimientos necesarios para el óptimo rendimiento del sistema de transmisión de datos.

a) Conmutación de circuitos

"En la conmutación de circuitos los dispositivos de conmutación deben establecer un camino físico entre varios medios de comunicación previo a la conexión entre los usuarios. Esta ruta permanece activa durante la comunicación entre los usuarios, liberándose al terminar la comunicación" (Tigridae, 2017). Ejemplo: red de telefonía conmutada. Su principal funcionamiento pasa por los siguientes períodos: solicitud, establecimiento, transferencia de datos y liberación de conexión.

b) Conmutación de paquetes

En la conmutación de por paquetes el emisor divide los mensajes a enviar en un número arbitrario de paquetes del mismo tamaño, en el cual también se adjunta una cabecera y la dirección origen y destino, así como datos de control que posteriormente serán transmitidos por diferentes medios de conexión entre nodos de corto tiempo para alcanzar a su destino. (Tigridae, 2017)

2.6.6 Eficiente operacionalización del backbone

En este estudio backbone se considera como el subsistema vertical o cableado troncal en la instalación de la red de área local que se aplica la normativa del cableado estructurado indicando así en la Figura 12-2. Es decir, la principal conexión que se basa mediante radioenlace, ya que será la que soporte mayor tráfico en la operacionalización de la red de datos de la Corporación.

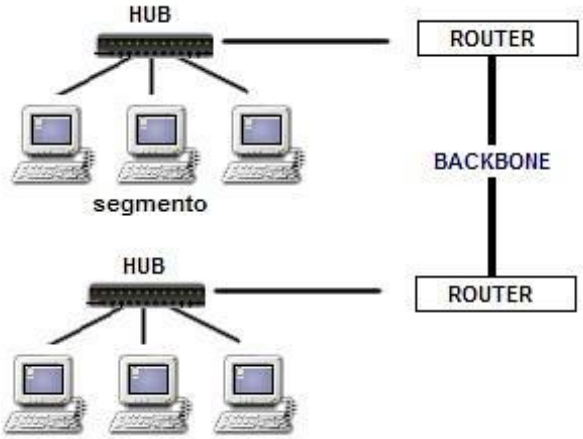


Figura 10-2: Esquema gráfico de segmento de red en una red de computadoras
Fuente: (Torres, Lewis, & Hernández, 2015)

Además, una red backbone requiere de una infraestructura especial que pueda ser posible el intercambio de información entre los distintos nodos y garantiza el alto rendimiento de la misma ya que a esta se considera como la red principal. Dando consigo la interconexión entre un gran conjunto de dispositivos dispersos territorialmente, así como clusters o subredes locales con mayor ancho de banda.

2.7 Protocolo MPLS con aplicación de VPN

Dentro de las redes de conmutación de paquetes, se considera las redes orientadas a conexión y redes no orientadas a conexión. Por lo que MPLS está enmarcada al establecimiento de conexión cuya característica adicional en el mantenimiento de circuitos virtuales.

Estos circuitos virtuales en las redes IP, permiten introducir una serie de mejoras en la red de transmisión de datos de la Corporación. Como redes virtuales privadas, establecimiento del tráfico, mecanismos de seguridad, soporte de multiprotocolo y sobretodo la consideración de QoS.

Es por esa razón que MPLS permite solucionar problemas como la velocidad de transmisión, escalabilidad, gestión en su rendimiento e ingeniería de tráfico. Además, MPLS es un estándar del IETF: RFC 3031 que está basado en la conmutación de marcas, donde evita las búsquedas en la tabla de enrutamiento durante la transferencia de información. A su vez facilita unificar el transporte de información de conmutación de paquetes y la conmutación de circuitos.

Además, VPN que permiten mayor funcionalidad de la red en cuanto a la seguridad y políticas de gestión de alguna red privada, realizando una conexión virtual punto a punto, a través del uso de conexiones dedicadas, cifrado o incluso la combinación de los dos métodos.

Es así que la aplicación de MPLS/VPN permite garantizar la transmisión de ciertas cantidades de información transmitidas en un tiempo determinado entre varios dispositivos, distribuyendo a su vez el ancho de banda disponible de acuerdo a las activaciones de los equipos disponibles.

2.7.1 Ventajas que MPLS ofrece para IP VPN

Según (Valladares, 2014) las ventajas que MPLS ofrece para IP VPN son:

- ✓ Proporcionar un modelo "acoplado" o "inteligente", ya que la red MPLS conoce de la existencia de VPN (lo que no ocurre con túneles ni PVCs).
- ✓ Evita la complejidad de los túneles y PVCs.

- ✓ Provee de un servicio sencillo: una nueva conexión afecta a un solo enrutador y tiene mayores opciones de crecimiento modular.

- ✓ Permite mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.

- ✓ Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda y retardo), lo que es necesario para un servicio completo VPN. (p.69)

2.7.2 Elementos generales de MPLS VPN

Los autores Ahmed, Butt, y Siddiqui, (2016) indican que los elementos que principalmente se utilizan en una red MPLS VPN se mencionan a continuación:

- ✓ Virtual Routing: Diferentes instancias o tablas de rating conocidas como VRF (VPN Routing and Forwaring) en los PE (Provider Edge).

- ✓ VRFs con el mismo identificador o nombre pueden intercambiar sus tablas de rutas.

- ✓ Propagación de información de VRF con MP-iBGP dentro de la Red MPLS.

- ✓ Asociación de un interface físico o lógico a un VRF.

- ✓ Vinculo de VRFs con VLAN 802.1Q

- ✓ A la Red MPLS no le afecta el direccionamiento de diversos proveedores externos. (p.85)

2.8 Características técnicas

2.8.1 Componentes del encabezado

MPLS permite a cada nodo, ya sea un switch o un router, la Tabla 5-2 permite determinar una etiqueta a cada uno de los componentes y comunicarla a sus nodos vecinos. Cuando MPLS está efectuado como una solución de nivel 3 o IP pura, la etiqueta es un fragmento de información añadido a la apertura del paquete. Los campos de la cabecera MPLS de 4 bytes, son los siguientes:

Etiqueta	Exp	S	TTL	32 bits
20 bits	3 bits	1 bit	8 bits	

Tabla 5-2: Pila de etiquetas de los componentes MPLS

N	Tamaño Bits	Pila de etiquetas
1	20	Etiqueta: La Etiqueta propiamente dicha, identifica un FEC, o sea un flujo de paquetes con el mismo tratamiento.
2	3	Exp: Bits para uso experimental, una propuesta es transmitir en ellos información de DiffServ o QoS.
3	1	S: Se pone en 1 para la primera entrada en la pila (la más antigua), 0 para el resto. Esta es la primera etiqueta introducida.
4	8	TTL: Contador del número de saltos. Este campo reemplaza al TTL de la cabecera IP durante el viaje del datagrama por la red MPLS.

Fuente: (Torres, Lewis, & Hernández, 2015)

2.8.2 Estrategias para la implementación del protocolo MPLS

A continuación, se menciona la planificación apropiada para que la implementación del protocolo MPLS tenga éxito y funcione de manera eficiente los cuales se mencionan en la Tabla 6-2.

Tabla 6-2: Estrategias para la implementación del protocolo MPLS

Preparación.	**Pruebas extensivas en el laboratorio (pruebas de regresión, funcionalidades)**
	Routers, y PE (Provider Edge routers), es necesario hacer upgrades para soportar las funcionalidades MPLS VPN.
	Revisar el hardware y software en todos los enrutadores de la red (Provider backbone)
	Enrutamiento. IGP Protocolo de estado de línea: OSPF o IS-IS BGP BGPv4 con soporte a Multiprotocolo BGP
Habilitar MPLS en el Core.	Habilitar LDP en todos los enrutadores de Backbone y equipos Provider Edge PE.
	MPLS TE puede ser habilitado en ciertas áreas si es necesario.
Conectividad MPLS VPN.	Habilitar MBGP entre los enrutadores PEs que brindaran el servicio de VPN.

Habilitar QoS en toda la red	Mecanismos de Scheduling
	Mecanismos de Encolamiento
	Mecanismos de Prevención y recuperación de Congestión

Fuente: (Torres, Lewis, & Hernández, 2015)

2.8.3 Consideraciones para desarrollar un radioenlace

Previo al desarrollo de un radioenlace s debe analizar ciertas consideraciones, de esta manera optimizar la funcionalidad de los radioenlaces, estas consideraciones se mencionan en la Figura 13-2.

1. Tener un buen presupuesto de enlace es un requerimiento básico para el buen funcionamiento del mismo.

2. Un presupuesto de enlace de una red inalámbrica es la cuenta de todas las ganancias y pérdidas desde el radio transmisor hacia el receptor.

3. Las pérdidas más grandes del enlace se producen en la propagación en espacio libre debido a la atenuación geométrica de la señal.

4. EIRP o PIRE es un valor que especifica la máxima potencia que está transmitiendo al espacio.

5. La sensibilidad del receptor es un parámetro que indica el valor mínimo de potencia que se necesita para alcanzar una cierta tasa de bit. (Buettrich, 2007)

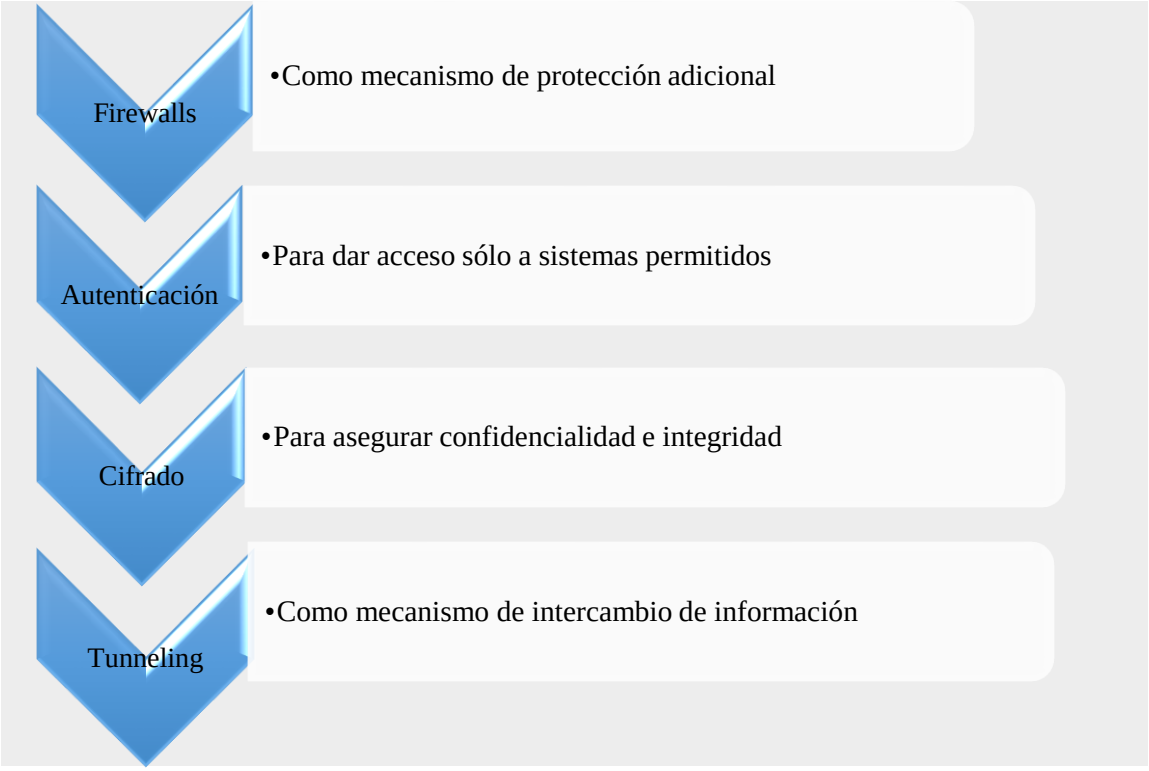


Figura 11-2: Elementos usados en VPN
Fuente: (Romero, 2004)

Para hablar de los protocolos más utilizados en VPN, se puede analizar el incremento de la tecnología del sistema de red, en los últimos tiempos el renombre de la tecnología de internet ha crecido, y de la misma manera los negocios han dado vuelta al mundo y han evolucionado, como medio para extender sus propias redes.

Anteriormente se encuadraron al mercado de las comunicaciones los intranets, estos son sitios diseñados para la utilización solamente por los empleados de una determinada compañía.

Hoy en día, muchas compañías crean sus propias redes privadas virtuales (VPN) para acomodar las necesidades inherentes de los empleados remotos y de las oficinas de sus sucursales más lejanas.

Según Delgado ed al. (2014), sostienen que, dentro de la multiplicidad de protocolos disponibles para su uso en las VPN, el acumulado estándar es IPSec, existiendo además otros protocolos como PPTP, L2F, SSL/TLS, SSH, MPLS, etc. (p.4)

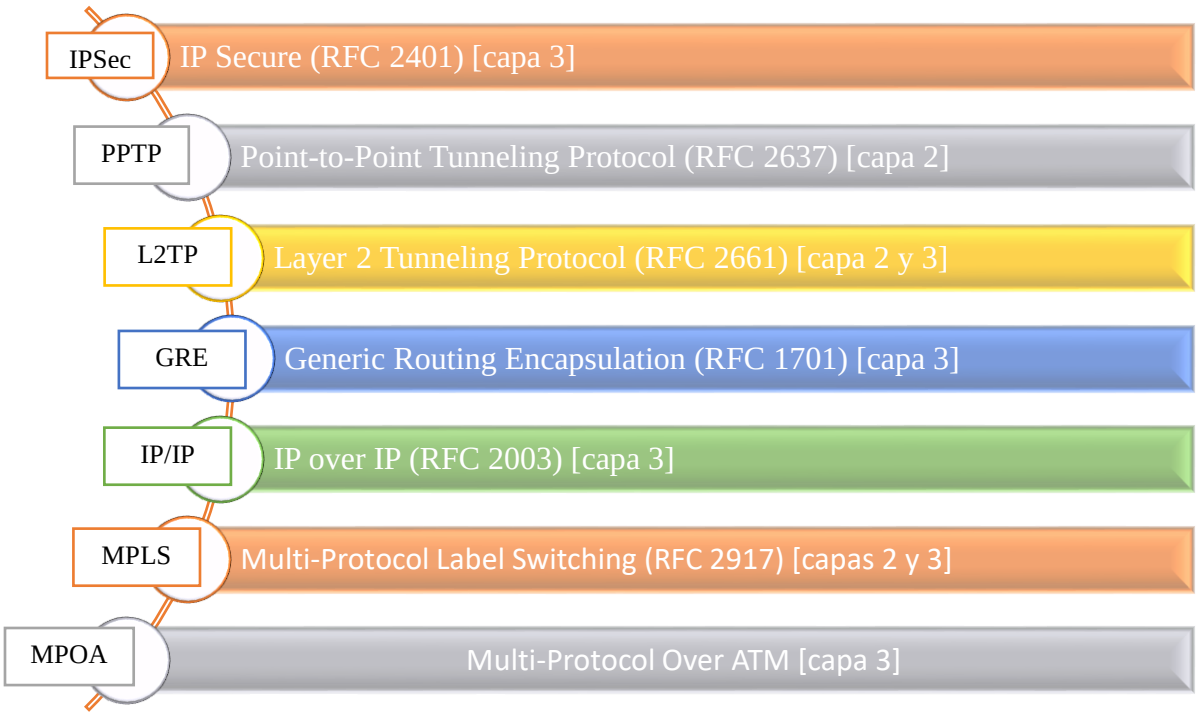


Figura 12-2: Protocolos comunmente utilizados en VPN
Fuente: (Romero, 2004)

En la Figura 12-2 se los protocolos que más se utilizan con redes VPN y a continuación, se describe la utilización y servicio de los protocolos, siendo los que tienen similares caracteristicas IPSec y MPLS.

- IPSec es un conjunto de estándares que se usa para añadir seguridad en IP, actúa a nivel de capa de red, autenticando y protegiendo los paquetes IP entre varios equipos participantes de la misma red. Estos también proporcionan confidencialidad, autenticación y integridad a través de una serie de algoritmos de cifrado, llaves públicas, hash y certificados digitales. IPSec tiene tres sobresalientes componentes los cuales se mencionan a continuación: dos protocolos de seguridad, los cuales son Autenticación de cabecera IP (AH) y carga de seguridad de encapsulado (ESP); y también se tiene uno de seguridad de llaves, Intercambio de llaves de Internet (IKE). Delgado ed. al. (2014)

- PPTP es un protocolo desarrollado por la Corporación Microsoft y normalizado por la IETF (RFC 2637) el mismo que accede el tráfico seguro de datos desde un punto o cliente externo o remoto a un servidor corporativo privado, el mismo que soporta múltiples protocolos de red (IP, IPX, NetBEUI), pero no es muy recomendado en seguridad. (Romero, 2004, pág. 103)

- L2TP es un estándar aprobado por la IETF, la cual es una organización internacional abierta de normalización, que tiene como principales objetivos contribuir a la ingeniería

de Internet, actuando en diversas áreas, entre las principales tenemos transporte, encaminamiento, seguridad. (Romero, 2004, pág. 103)

- Este protocolo no posee autentificación o cifrado por paquete, por lo que ha de combinarse con otro protocolo de apoyo, como IPSec o MPLS, ofrece la integridad de datos y confidencialidad exigidos para una interacción VPN, también aprueba el encapsulado de distintos protocolos entre los más utilizados están: IP, IPX, NetBEUI, etc. (Romero, 2004, pág. 104)

- GRE es un protocolo muy útil para el establecimiento de túneles a través de la red Internet. El mismo que está definido en la RFC 1701 y en la RFC 1702, pudiendo transportar un máximo de 20 protocolos del nivel de red (nivel 3 del modelo OSI) de distintas características. Este protocolo soporta también la secuencialidad de paquetes y la creación de varios túneles sobre redes de alta velocidad. (Romero, 2004, pág. 105)

- IP/IP son protocolos de internet que normalmente se usan para enviar las señales de voz sobre la red de protocolo IP se identifican como protocolos de voz sobre IP. Adicional también el tráfico de voz sobre IP puede transitar por cualquier red de la misma configuración, incluyendo redes las LAN.

- MPLS permite solucionar problemas como la velocidad de transmisión, escalabilidad, gestión en su rendimiento e ingeniería de tráfico. Igualmente, MPLS es un estándar del IETF: RFC 3031 que está asentado en la conmutación de marcas, la cual evita las búsquedas en la tabla de enrutamiento en la transferencia de información. El mismo que a su vez facilita unificar el transporte de información de conmutación de paquetes y la conmutación de circuitos. (Ahmed, Butt, & Siddiqui, 2016)

Son muchos los protocolos que se pueden utilizar en el tráfico de datos VPN, pero en la aplicación de seguridad en el encapsulamiento de la información existe una similitud entre IPSec y MPLS, pero además la diferencia entre IPSec y MPLS es que MPLS interconecta de forma segura todas las sucursales de una entidad permitiéndole disponer de una conectividad privada de extremo a extremo, sin necesidad de encriptar el tráfico. En contrario con VPN IPsec que usan un direccionamiento IP público fijo, la misma que encripta el tráfico e interconecta las redes de forma segura todas las localizaciones de la entidad. (Frenkel, 2017)

La utilización de un determinado protocolo en redes VPN se realiza de acuerdo a la necesidad, seguridad y dimensionamiento de cada empresa, en entidades que se requiere un respaldo o un margen de seguridad en el encapsulamiento de la transmisión de información se puede utilizar el

protocolo MPLS, la decadencia de personal calificado en las empresas puede implicar una dificultad al momento de configurar la red con este tipo de protocolo.

2.9 Operación del Protocolo MPLS

Córdoba, (2017), manifiesta que una red MPLS reside de un conjunto de enrutadores de conmutación de etiquetas (LSR) que poseen la capacidad de rutear y conmutar paquetes de datos en base a la etiqueta que se ha añadido a su respectivo paquete. Cada una de las etiquetas define un flujo de paquetes entre dos puntos extremos. (p.21)

En este sentido cada flujo es distinto llamado comúnmente clase de equivalencia de reenvío (FEC), de la misma manera también cada flujo tiene un camino específico a través de los LSR de la red, por esta razón se dice que la tecnología MPLS es "orientada a conexión". Cada Clase de Equivalencia de Reenvío, asi mismo ruta de los paquetes contiene una serie de caracteres la cual define los requerimientos de QoS del flujo de información. Así también los routers de la red MPLS no requieren examinar ni procesar el encabezado IP, solo es necesario reenviar cada paquete dependiendo el valor de su etiqueta. (Cordoba, 2017, pág. 22)

2.9.1 Ubicación del protocolo MPLS en cuanto al modelo OSI

Cure & Gonzales, (2014), mencionan que el protocolo opera entre la capa de enlace de datos (capa 2) y la capa de red (capa 3) del modelo OSI como se observa en la Figura 15-2, en reconocimiento a esto puede juntar las características de las dos capas de enlace haciendo uso de la velocidad del forwarding y del control del routing. (pág.7)

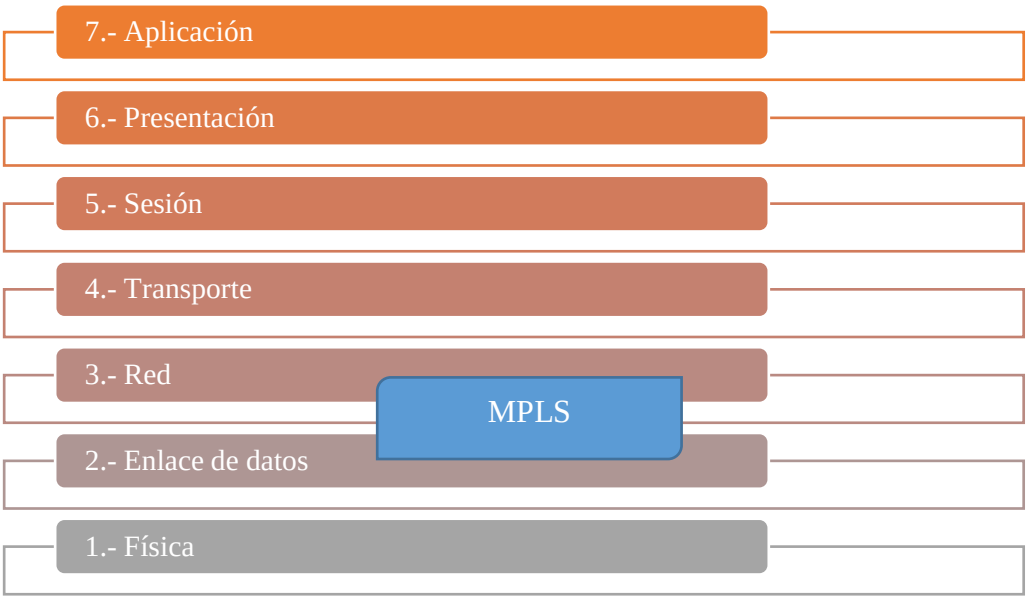


Figura 13-2: Capas de red modelo OSI
Fuente: (Camacho, 2015)

Se menciona el diagrama básico que se utiliza para la comunicación MPLS en la Figura 16-2:

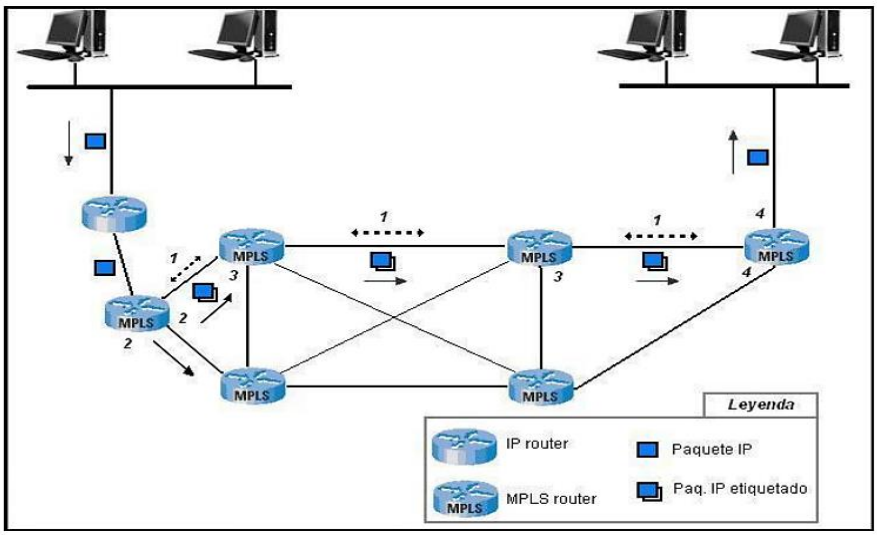


Figura 14-2: Diagrama general de operación MPLS
Fuente: (Cordoba, 2017, pág. 23)

Los pasos que sigue el flujo de paquetes MPLS en un esquema organizado y esquematizado en un diagrama general de operación como se observa en la Tabla 7-2.

Tabla 7-2: Flujo de paquetes MPLS

FLUJO	Descripción
1	Antes de mandar la información por el flujo es necesario establecer un Camino de Conmutación de Etiquetas (LSP) entre los routers que van a transmitir la FEC. Dichos LSP sirven como túneles de transporte a lo largo de la red MPLS e incluyen los parámetros QoS específicos del flujo. Estos parámetros sirven para determinar dos cosas: a. La cantidad de recursos a reservar al LSP. b. Las políticas de desechado y la cola de procesos en cada LSR.
2	En esta sección el paquete entra al dominio MPLS mediante un LSR frontera que determina que servicios de red requiere, definiendo así su QoS. Al terminar dicha asignación el LSR asigna el paquete a una FEC y a un LSP particular, lo etiqueta y lo envía. Si no existe ningún LSP, el router frontera trabaja en conjunto con los demás LSRs para definirlo.
3	En este momento el paquete ya está dentro del dominio MPLS, cuando los routers contiguos del LSR reciben el paquete se llevan a cabo los siguientes procesos. a. Se deshecha la etiqueta de entrada y se le añade la nueva etiqueta de salida al paquete. b. Se envía el paquete al siguiente LSR dentro del LSP.
4	El LSR de salida "abre" la etiqueta y lee el encabezado IP para enviarlo al destino final.

Fuente: (Frenkel, 2017)

2.10 Análisis de redes privadas virtuales basadas Multiprotocol Label Switching

Las VPN de conmutación por etiquetas multi-protocolo o MPLS (por sus siglas en inglés) son utilizadas con mayor eficacia para las conexiones del tipo sitio a sitio (punto a punto), sin necesidad de realizar encriptación el tráfico. Las redes VPN MPLS resumen la configuración y facilitan la gestión global de la red, así como su mantenimiento. Esto corresponde principalmente por el hecho de que las MPLS es la opción más flexible que se adapta de mejor manera con la finalidad de transmitir paquetes de dados. Se trata de un recurso de base estándar que se utilizan para acelerar la distribución de varios paquetes de red en múltiples protocolos. Las VPN MPLS son sistemas que están ajustados al proveedor ISP. (Frenkel, 2017)

Indica Frenkel, (2017), que una VPN ajustada a ISP es cuando dos o más bandas están conectadas para formar una VPN utilizando el mismo ISP. Sin embargo, la mayor desventaja de usar una VPN MPLS es el hecho de que la red no es tan fácil de realizar configuraciones en comparación con otras VPN. Este tipo de protocolo no es sencillo hacer modificaciones. Por eso, este tipo de VPN generalmente es mucho más costoso.

Con las VPN se soporta aplicaciones de intra/extranet, integrando voz, datos y video sobre infraestructuras de comunicaciones eficientes y beneficiosas. El presente trabajo tiene como objetivo especificar las VPN sobre MPLS de Capa 3 y 2, ya que los SP requieren transportar tanto tráfico de Capa 2 como de Capa 3. Una red privada virtual (VPN, Virtual Private Network) se construye a base de conexiones realizadas sobre una infraestructura simultánea con funcionalidades de red y de seguridad semejantes a las que se obtienen con una red privada real. (Valdivia & Peña, 2015)

Para realizar el análisis de protocolos VPN, Valdivia & Peña, (2015) mencionan un ejemplo hipotético de conexión de túneles de red de un protocolo MPLS/VPN, en el cual se describe dos puntos de presencia POP (Point of Presence), uno que se denomina PE1 y el siguiente que se denomina PE2, estando los POP enlazados a través de dos enrutadores de núcleo denominados P1 y P2.

En el ejemplo planteado, el sistema tiene dos sucursales su esquematización se muestra en la Figura 2.17 y su denominación a continuación:

- Sucursal A que conformara la VPN-A, con el sitio-1 y el Sitio-2 conectado a PE1 y el sitio-3 conectado a PE2.

- Sucursal B que conformara la VPN-B con el sitio-1 conectado a PE2 y el sitio-2 conectado a PE1. La red descrita anteriormente es mostrada en la siguiente Figura.

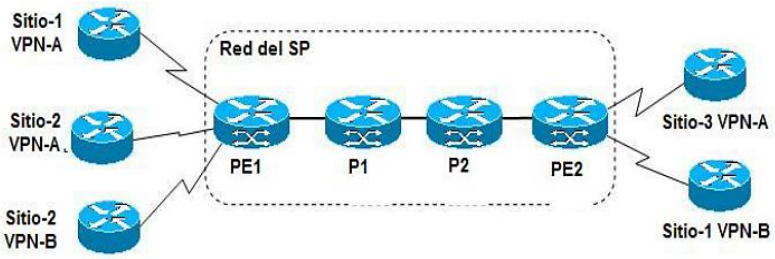


Figura 15-2: Ejemplo de red y sucursales del sistema de transmisión.
Fuente: (Valdivia & Peña, 2015)

Acorde a las terminologías de los enrutadores en el Figura 17-2 y se poseen las siguientes funciones:

- Los enrutadores PE1 y PE2 que enlazan a la red con sus clientes son enrutadores de la frontera del proveedor de servicio el mismo que puede ser: PE, Provider Edge.

- Los enrutadores P1 y P2 que no tiene conexiones directas con los clientes son enrutadores del núcleo de la red del proveedor principal (P, Provider).

- Los enrutadores de los clientes conectados al PE1 en el sitio-1 y sitio-2 de la Sucursal A y en el sitio-2 de la Sucursal B al igual que los conectados al PE2 en los sitio-1 y sitio-3 de la Sucursal B y la Sucursal A respectivamente son enrutadores de la frontera del cliente (CE, Customer Edge).

Así también el proveedor de servicio procura ofertar un servicio basado en el modelo par a par (no un número de túneles IP sobre IP), pero hay que tener en cuenta un número de detalles porque el espacio de direcciones IP de los dos sitios conectados al mismo enrutador de configuración PE1 se solapan. (Valdivia & Peña, 2015)

Se da a conocer efectivamente un número de enrutadores virtuales son creados en un único enrutador físico, como se muestra en la Figura 18-2:

Figura 16-2. Enrutadores Virtuales creados en un enrutador PE1
Fuente: (Valdivia & Peña, 2015)

El concepto de enrutadores virtuales les accede a los clientes usar cualquier espacio de direcciones externas o privadas en cada una de las VPN. Para cada cliente o sitio concerniente a una VPN existe un solo requerimiento, que el espacio de direcciones sea único dentro de la VPN. La exclusividad de direcciones de red no es preciada entre VPN, excepto cuando dos VPN de alguna manera comparten el mismo espacio de direcciones privadas quieran comunicarse.

Con la intención de ilustrar el intercambio de los protocolos de enrutamiento por VPN con el MPLS utilizado en el núcleo intrínseco de la red del SP, se considera el caso de la Sucursal A en la red, se consigue que el sitio-1 en el PE1 utiliza OSPF para interactuar con el backbone, el sitio-2 no utiliza protocolos de enrutamiento, es configurado con rutas estáticas y que el sitio-3 utiliza RIP (Routing Information Protocol). (Valdivia & Peña, 2015)

Figura 17-2:. Iintercambio de los protocolos de enrutamiento por VPN con el MPLS
Fuente: (Valdivia & Peña, 2015)

En la Figura 19-2, se resume el análisis de redes VPN de conmutación por etiquetas multi-protocolo o MPLS, y de acuerdo al ejemplo expuesto se deduce que la estandarización de esta tecnología ha jugado un papel significativo en el tratamiento de aplicaciones sobre esta arquitectura, entre las que inciden las Redes Privadas Virtuales (VPN) de Capa 2 y 3. Valdivia & Peña, (2015). Las MPLS/VPN de Capa 3 están desarrolladas e implementadas basadas en estándares como la RFC 2745, no obstante, las MPLS/VPN de Capa 2 a pesar de la existencia de gran cantidad de especificaciones acerca su implementación en varios borradores del IETF (“drafts Martini”, “draft Kompella”, “draft Lasserre-Kompella” y otros), aún no están estandarizadas en RFC por el IETF, algo a tener muy en cuenta por los SP en el momento de invertir en equipamiento.

2.11 Análisis del rendimiento de sistemas de transmisión de datos basados en MPLS/VPN

El rendimiento de una red de datos depende del servicio y la calidad de la misma, que presente a la hora de transmitir datos, en la cual se determina la eficiencia de esta con los parámetros conseguidos en su análisis previsto, además se debe mantener la eficiente operacionalización, estabilidad, escalabilidad, seguridad, velocidad de transmisión de datos y robusto ante interferencias.

Para comprender debidamente la tecnología que ofrecen las VPN sobre MPLS es necesario comprender anticipadamente los posibles problemas que pueden surgir. Las VPN en MPLS son una solución WAN de capa 3 que soluciona el problema de las WAN de capa 2, proporcionando conectividad de muchos a muchos entre sitios de una manera económica y efectiva. En el pasado cada vez que era necesario extender la topología suponía un desembolso importante de dinero lo que siempre hacía difícil dicha extensión. Una topología de malla extendida puede ser muy robusta pero extremadamente costosa, mientras que otras menos caras no ofrecen la solución adecuada.

MPLS significó la respuesta y la solución a este problema. Con esta tecnología es posible tener una topología de malla completa, pero con la capacidad de hacerlo a nivel de capa 3. La posibilidad de arquitectura que proporciona esta solución es la creación de redes WAN entre los circuitos existentes a nivel de capa 2.

La idea de las VPN siempre se asocia con los conceptos de privacidad y seguridad.
Las VPN permiten el uso de infraestructura compartida ofrecida por un ISP para implementar redes privadas. En la Figura 20-2 se sustenta el uso de seguridad está sujeto a negociación, los ISP ofrecen servicios adicionales tales como firewall para filtrar tráfico indeseado.

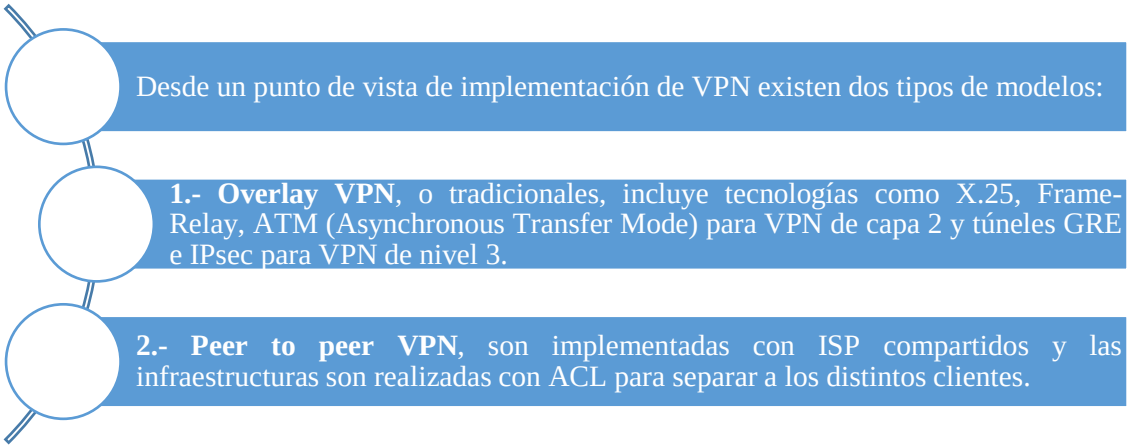


Figura 18-2: Modelos de tipos de redes VPN
Fuente: (Valdivia & Peña, 2015).

VPN peer to peer

Las VPN peer to peer hacen que el ISP tenga un papel más activo en las operaciones de enrutamiento de cada cliente. El ISP mantiene información de instancias de enrutamiento separadas dentro de su red. El router CE (Customer Edge) comparte información sólo con el router PE (Provider Edge) a través del circuito del ISP. Esta conexión e intercambio de información con el ISP facilita el concepto de VPN peer to peer.

Esta evolución hace que la VPN no sólo transporte tráfico de capa 3 sino que además sepa de qué tipo de tráfico se trata y sepa para qué utilizarlo. La siguiente Figura 21-2 ilustra este concepto:

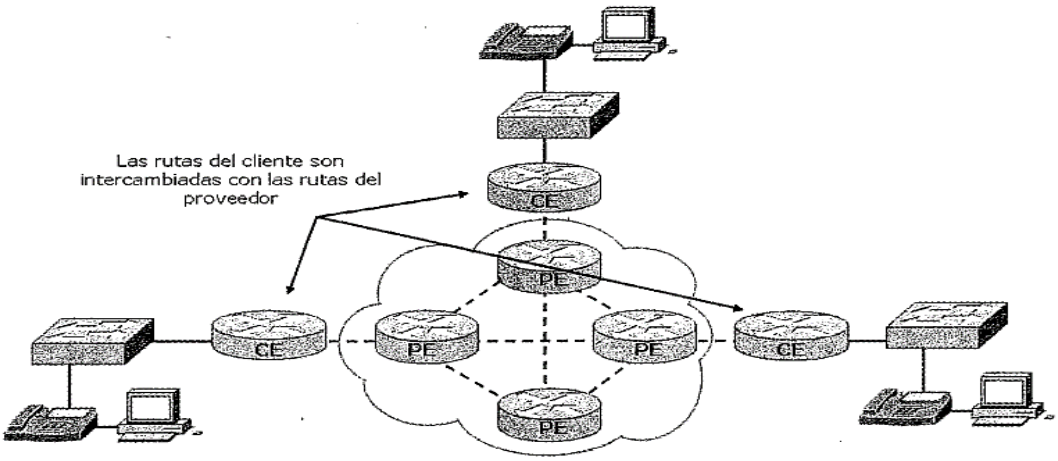


Figura 19-2: Esquema VPN peer to peer
Fuente: (Valladares, 2014)

2.11.1 Ancho de banda

Según Filippis, (2012) el ancho de banda es la cantidad de información que puede transmitir de una sola vez, en un paquete desde el punto de origen hacia el destino y se mide en Kbps, Mbps y Gbps. Considerada como la medida de datos y recursos de comunicación que van hacer disponibles o consumidas en una red establecida, expresados en Bits o múltiplos de ella. En que la velocidad de transmisión máxima que esta transmite la información depende de la misma.

Es por ello que se debe considerar esta variable ya que de esta depende que se pueda llevar la suficiente información como para sostener la transmisión de voz, datos y video de una manera eficiente y estable, para ello se debe considerar generalmente la sucesión de conexiones que están presentes en la red como también dando el suficiente ancho de banda para cada una de ellas ya que si una de estas conexiones es más lenta que las otras y se encontrara en el punto de mayor operación , actuara como un cuello de botella causando lentitud en la comunicación.

2.11.2 Latencia

En (Filippis, 2012) , se menciona que latencia “Es el tiempo que demora un paquete de datos en llegar desde el origen al destino. Esto está limitado por leyes físicas de los medios de transmisión (cables de fibra, cables de cobre, enlaces satelitales, etc.) y adicionalmente por los dispositivos intermedios de transmisión de datos (routers, switchs, gateways y firewalls)”. (pág.1)

Por lo que se debe hacer referencia al ancho de banda y también a la latencia presente en la comunicación de la red y todo esto se logra gracias a la optimización de una correcta

infraestructura con el uso de tecnología adecuada, de modo que estas redes de datos sean lo más veloces y eficientes posibles.

Valores recomendados

La latencia o retardo entre el punto de inicio y fin de la comunicación se recomienda que debiera ser inferior a 150 ms. El oído humano es capaz de detectar latencias de unos 250 ms, 200 ms en el caso de personas bastante sensibles. Si se supera ese umbral la comunicación se vuelve molesta. (Brognara, 2016).

Criterios de mejoramiento de Latencia

Las soluciones de mejoramiento de la red son complejas. Muchas veces depende de los equipos tecnológicos por los que pasan los paquetes, es decir, de la red misma. Se puede pretender reservar un ancho de banda de punto de origen a destino o señalizar los paquetes con valores de TOS (Campo de tipo de servicio) para pretender que los equipos sepan que se trata de tráfico en tiempo real y lo traten con mayor prioridad, pero actualmente no suelen ser medidas muy eficaces ya que no disponemos del control de la red. (VoipForo, 2017)

Si el problema de la latencia está en nuestra propia red interna podemos aumentar el ancho de banda o velocidad del enlace o priorizar esos paquetes dentro de nuestra red.

2.11.3 Jitter

(APOGEE, 2014) , comenta que "Es la desviación no deseada de una señal periódica de el momento ideal" (p.1), que es asumida como periódica por lo que esta se convierte en un factor importante y no deseado en el interior del diseño y desempeño de las redes de comunicación. Por lo tanto, es la variación en un determinado tiempo de arribo al receptor de la información, el mismo parámetro se tiene en cuenta en el proyecto de investigación.

Valores recomendados

(Brognara, 2016), menciona que el jitter entre el punto inicial y final de la comunicación debiera ser inferior a 100 ms. Si el valor es menor a 100 ms el jitter puede ser compensado de manera apropiada. En caso contrario debiera ser minimizado.

Criterios de mejoramiento del Jitter

La solución considerablemente aceptada es la utilización del jitter buffer. El jitter buffer consiste fundamentalmente en asignar una pequeña cola o almacén para que de esta forma iniciar

recibiendo los paquetes y sirviéndolos con un pequeño retraso. Si algun paquete no está en el buffer (se perdió o puede ser que no ha llegado todavía) cuando sea necesario este se descarta. Normalmente en los teléfonos IP (hardware y software) se pueden variar los buffers. Un incremento del buffer involucra menos pérdida de paquetes, pero más retraso. Una reducción implica menos retardo en la transmisión, pero más pérdida de paquetes. (VoipForo, 2017)

2.11.4 Throughput

En fines corporativos es muy importante tener en cuenta la medición de esta variable mediante la generación de tráfico. En donde se conocerá la tasa promedio de éxito en la respectiva entrega de datos sobre un canal de comunicación, es decir que nos indicara la capacidad efectiva que tiene la red en el momento de la transferencia de información sobre el enlace. (Ríos, 2009, pág. 2)

2.11.5 Velocidad de transmisión

Según el Departamento de Investigación de la universidad de Cornell, (2003), menciona que, las velocidades mostradas son máximos teóricos, que rara vez se encuentran en las instalaciones de cada entidad, si llegaran a encontrarse. Observe que la red más rápida es casi 175.000 veces más rápida que la más lenta. Una vez que uno sabe la velocidad de transmisión de una red es posible calcular el tiempo aproximado que le tomará atravesarla a un archivo de cualquier tamaño en particular. p.6

En resumen, del análisis de rendimiento se denota que MPLS ha sido desarrollado para ofrecer un estándar a los proveedores que permitirá evolucionar de los Conmutadores ATM a Routers de Backbone de altas prestaciones, los nuevos avances en tecnologías de Silicio ASIC (circuitos integrado para aplicaciones especificas) permite a los Routers realizar con una rapidez análoga para la consulta de tablas a las de los conmutadores ATM. De esta manera se identifica que MPLS mejora significativamente el rendimiento del mecanismo de envío de paquetes. La evaluación del rendimiento de la red es de mucha importancia, puesto que con ello se determina el progreso de la configuración de un determinado protocolo, y de esta forma comparar los protocolos, y sus beneficios en cuanto a la transmisión de datos, así como puede ser ancho de banda, velocidad de transmisión, latencia, etc. (Pino, 2009)

CAPÍTULO III

3 METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Enfoque de la investigación

El enfoque en que se orienta la presente investigación es cualitativo, porque es de carácter social, permite establecer la relación entre el sujeto de estudio y el entorno, y cuantitativo porque se basa en métodos para la recolección de datos; a través del análisis e interpretación deductiva se identifica si como resultado de esta interrelación concurre una consecuencia en la población objeto de estudio, orienta al descubrimiento de la hipótesis, y verificando así el nivel de validez y confiabilidad de los eventos y respuestas obtenidas en el presente estudio.

3.2 Tipo de investigación

- ✓ Investigación de Campo. - La investigación se realiza en el lugar donde se producen los acontecimientos, se obtiene información a través de técnicas de recolección de datos para su posterior experimentación.

- ✓ Investigación Bibliográfica. - Se concurre a fuentes escritas con la finalidad de detectar, ampliar y profundizar distintos enfoques, teorías, conceptualizaciones y criterios de varios autores sobre el problema detectado, basándose en documentos, libros, revistas y otras publicaciones. Su desarrollo se basa en consultas bibliográficas, y de campo.

3.3 Alcance de la investigación

El alcance es correlacional ya que la investigación busca establecer la relación entre el sistema MPLS/VPN y la eficacia de operacionalidad del mismo, fundamentada en datos recolectados y pruebas de simulación basadas en los parámetros para mejorar el rendimiento de la red de datos y su respectivo comportamiento.

3.4 Población y muestra

3.4.1 Población

Chávez, (2007), afirma que “la población de un estudio es el universo de la investigación sobre el cual se pretende generalizar los resultados, está constituida por características o estratos que

permiten distinguir lo sujetos unos de otros y cuyas características se deben delimitar con la finalidad de establecer los parámetros muestrales". En este sentido, las agencias involucradas en el estudio de esta investigación son de carácter finita y de fácil acceso y se muestran en la Tabla 1-3.

Tabla 1-3: Agencias de la Corporación Nacional de Electricidad Regional Bolívar.

N	NOMBRE
1	Matriz CNEL Bolivar
2	Ag. Caluma
3	Ag. Echeandia
4	Ag. Chimbo
5	Ag. San Miguel
6	Ag. Chillanes
7	Ag. El Tambo
8	Ag. San Luis de Pambil
9	Ag. Las Naves
10	Ag. Facundo Vela
11	Ag. Simiatug
12	Ag. Balsapamba

Elaborado por: Roberto Usca, 2017

3.4.2 Muestra

Según los autores Tamayo & Tamayo (2004), afirma que la muestra "es el grupo de individuos que se toma de la población, para estudiar un fenómeno estadístico" (pp.38)

Debido a que la población de éste estudio es reducida; no amerita la obtención de una muestra; por lo tanto, en la presente investigación se aplican a las 11 agencias y la matriz de la Corporación Nacional de Electricidad Regional Bolívar.

3.5 Métodos, Técnicas e instrumentos de recolección de datos

3.5.1 Métodos

- ✓ Método Deductivo: Puesto que se analiza el problema desde su globalidad para establecer soluciones específicas que ayudan a determinar la eficacia del sistema MPLS/VPN.

- ✓ Método Inductivo. – Con el presente método se va a permitir analizar factores primordiales de la investigación, así como la velocidad de transmisión, jitter, ancho de

banda, Latencia y porcentaje de pérdida, permitiendo lograr los objetivos propuestos y colaborando con la verificación de las variables.

- ✓ Método Analítico. – Con el cual se va a analizar a profundidad la información que proporcione los escenarios pudiendo explicar así su similitud y comprender su comportamiento de acuerdo a los parámetros de rendimiento analizados.

3.5.2 Técnicas

Fuentes Primarias. - Dentro de esta categoría se destacan dos aspectos muy importantes para la recolección de información y datos como son: observación, encuestas y fichaje.

- ✓ Observación directa. - A través de la observación directa se basa generalmente en el desempeño global del sistema de rendimiento de datos de la Corporación Nacional de Electricidad Regional Bolívar, verificando de manera directa el fenómeno a investigar, con la finalidad de incrementar el rendimiento de datos en la corporación.

- ✓ Fichaje. – Con la presente técnica se pretende registrar los datos que se van obteniendo en los instrumentos llamados fichas, las cuales, debidamente ordenadas y elaboradas con esta se adquiere la mayor parte de la información que se recopila en la investigación.

- ✓ Encuestas. - Con la realización de las encuestas se procura plantear preguntas relacionadas con las falencias que atraviesa el rendimiento de red de la Corporación Nacional de Electricidad Regional Bolívar, permite también saber las expectativas y necesidades de la misma para establecer estrategias y fortalecer un mejor desempeño de la red.

Fuentes Secundarias. - Este tipo de técnica ayuda recopilando información de revistas, libros, internet, en la cual se enfoca la información más importante, sea confiable y lo más actualizada posible para la estructuración correcta del tema de investigación.

3.5.3 Instrumento

- ✓ Fichas de observación. – Es un instrumento de la investigación de campo que permite tomar y registrar notas o datos de investigación.

- ✓ El Cuestionario de chequeo. – Unos de los instrumentos más importantes debido a que por medio de este se obtiene la información deseada a escala masiva y estará constituido por preguntas previamente estructuradas, permitiendo obtener opiniones y c7riterios alrededor de las variables en estudio.

- ✓ Libros digitales y físicos referentes al tema de investigación.
- ✓ Acceso a Internet, para la búsqueda de información referencial.

3.6 Identificación de variables

3.6.1 Variable independiente

Protocolo MPLS con la aplicación de VPN

3.6.2 Variable dependiente

Rendimiento del Sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

3.7 Operacionalización de variables

Tabla 2-3: Matriz de consistencia

Formulación del problema	Variables	Conceptualización	Indicadores	Índices	Técnicas	Instrumentos
¿La evaluación del protocolo MPLS con la aplicación de VPN permite mejorar el rendimiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar?	**Variable Independiente** Protocolo MPLS con la aplicación de VPN	• MPLS Es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de servicios.	• Servicios • Escalabilidad • Flexibilidad • Seguridad	• Características de servicios • Dimensionamiento de escalabilidad • Topología de la red • Características de seguridad	• Observación • Investigación • Encuesta	• Ficha de observación • Cuadros comparativos
	Variable Dependiente Rendimiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar	• Rendimiento del sistema Analiza el rendimiento y la eficiencia de red de los recursos virtuales de una máquina, con el fin de proporcionar orientación para la solución de errores.	• Rendimiento • Eficiencia • Ancho de banda • Latencia • Jitter	• Calidad en el servicio • Transmisión de datos • Cantidad de información • Tiempo de transmisión • Interrupción en la transmisión de datos	• Observación • Investigación • Encuesta	• Ficha de observación • Cuestionario de encuesta

Elaborado por: Roberto Usca, 2017

3.8 Procesamiento y análisis para la información

3.8.1 Plan de recolección de información

La presente investigación se ha aplicado la técnica de la encuesta, con su respectivo instrumento el cuestionario de chequeo (Check list), aplicado a las agencias respectivas de la Corporación Nacional de Electricidad Regional Bolívar, en la Tabla 3-3 se analiza las preguntas sobre hechos y aspectos que interesan investigar de las variables dependiente e independiente respectivamente.

Tabla 3-3: Plan de recolección de información

Nº.	PREGUNTA BÁSICA	EXPLICACIÓN
1	¿Para qué?	Para conseguir los objetivos de la investigación
2	¿De qué personas u objetos?	Agencias de CNEL Regional Bolívar
3	¿Sobre qué aspectos?	Indicadores de la operacionalización de variables
4	¿Quién?	Investigador
5	¿Cuándo?	Septiembre-octubre del 2017
6	¿Dónde?	CNEL Regional Bolívar
7	¿Cuántas veces?	Una vez en cada agencia
8	¿Qué técnicas de recolección?	Encuesta
9	¿Con qué?	Cuestionario de chequeo
10	¿En qué situación?	De sinceridad y respeto

Elaborado por: Roberto Usca, 2017

3.8.2 Plan de procesamiento de información

Para analizar la información recopilada durante la investigación se persigue los siguientes pasos:

- La información obtenida es revisada y codificada, en lo posible para evitar posibles errores y permita organizar de manera clara y precisa, para la interpretación de las observaciones experimentales desarrolladas en los escenarios de la evaluación del protocolo MPLS/VPN en el Sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

- El siguiente paso se realiza la categorización y tabulación de la información, la cual se elabora de forma manual en fichas de observación, para determinar el cuestionario de chequeo, las mismas que serán ilustrados en cuadros con sus respectivos porcentajes.

- Una vez que se elaboré la tabulación de los datos, se procede al análisis de la información obtenida para identificar los verdaderos motivos y causas que permitan la implementación del protocolo MPLS con la aplicación de VPN, de forma clara y concreta facilitando la comprensión de los resultados.

- Finalmente, se verifican la hipótesis planteada verificando la fiabilidad de la información mediante el análisis de varianza de los datos y mediante la prueba de chi cuadrado comprobar la relación de ellas y asertividad de los datos, para el establecimiento de conclusiones y recomendaciones se procedió a explicar el procedimiento de la investigación.

3.9 Hipótesis

3.9.1 Hipótesis general

La aplicación del protocolo MPLS con VPN permite mejorar el rendimiento del sistema de trasmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

3.9.2 Hipótesis específicas

- El análisis del protocolo MPLS con la aplicación de VPN permite determinar condiciones y requerimientos técnicos necesarios en un sistema de trasmisión de datos.

- El Diseño de la topología de red de datos basado en el protocolo MPLS con la aplicación de VPN permite mejorar el rendimiento del sistema de transmisión de datos.

- Mediante el planteamiento de ecsenarios de prueba se puede realizar la evaluacion del rendimiento de red y el tráfico de datos del sistema de transmisión

- El desarrollo de una Guía de Implementación de un sistema de transmisión de datos basado en el protocolo MPLS con la aplicación de VPN, permite mejorar su rendimiento.

CAPÍTULO IV

4 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de información

Para analizar la información que se recopiló durante la investigación se sigue los siguientes pasos:

- La información obtenida es revisada, para evitar posibles errores y de esta manera organizar de forma clara y correcta para un buen entendimiento y comprensión de los lectores, en el cuestionario de chequeo, que se aplicó en la Corporación Eléctrica Regional Bolívar.

- El segundo punto está la categorización y tabulación de la información, la misma que se elabora de forma manual, para establecer cuántas veces se repite cada una de las alternativas de respuesta oportunas a cada pregunta, estas se ilustran en cuadros con su forma porcentual.

- En consiguiente se procede al análisis de la información obtenida para identificar los principales motivos y causas que originaron el problema, esto se ilustra en estadígrafos de barras y pastel, de forma clara y concreta facilitando la comprensión de los resultados.

- Finalmente, se verifica la hipótesis de investigación planteada mediante la prueba de Chi Cuadrado, en la cual se comparan las frecuencias obtenidas en la técnica aplicada, y estas también expresadas con las frecuencias teóricas esperadas analizando en el software estadístico SPSS.

4.1.1 Plan de Análisis e Interpretación de Resultados

- Análisis de los resultados estadísticos. - Se efectúa destacando tendencias o crónicas esenciales de acuerdo con los objetivos de la investigación e hipótesis planteadas en el presente estudio.

- Interpretación de los resultados. - se lo realiza con el apoyo del marco conceptual o teórico, en el aspecto pertinen|te en el interior de la investigación con las variables.

- Comprobación de hipótesis. - Se realiza mediante la prueba estadística de Chi Cuadrado, la misma que tiene la siguiente estructura, como se observa en la Figura 1-4:

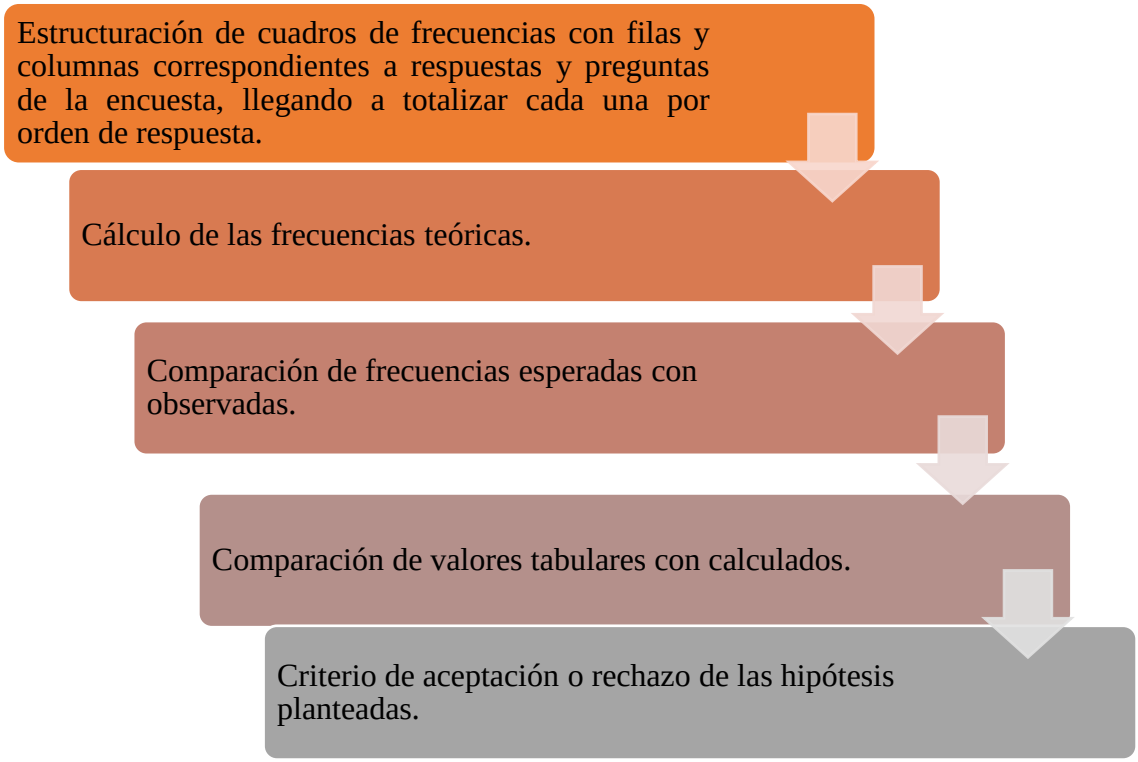


Figura 1-4: Estructura de comprobación de hipótesis.

Fuente: (ÁLVAREZ, 2012)

- Análisis de la fiabilidad de los datos con los que se comprobó la hipótesis de estudio los cuales se realiza mediante la ayuda del software estadístico SPSS, para demostrar si el checklist realizado cumple satisfactoriamente la necesidad de las variables de estudio.

- Establecimiento de conclusiones y recomendaciones. - Se procedió a la explicación del procedimiento generalizado de obtención de las respectivas conclusiones y recomendaciones. Las conclusiones nacen de la ejecución y cumplimiento de los objetivos específicos de la investigación planteada. Las recomendaciones se derivan de las conclusiones establecidas del presente trabajo.

4.2 Análisis descriptivo

Se presenta un análisis estadístico descriptivo en el cual obtiene, organiza, presenta y describe el conjunto de datos del Checklist, mediante el apoyo de tablas, medidas numéricas y gráficas. Se procede a realizar un cuestionario de chequeo el cual se aplica a la matriz y once agencias que componen la Corporación de Electricidad Regional de Bolívar.

4.2.1 Análisis por ítem

A continuación, se realiza un análisis descriptivo de cada una de las preguntas realizadas en el cuestionario estructurado que se realizó en la Corporación Nacional de Electricidad de Bolívar., iniciando asi en la Tabla 1-4, con la tabulación de la pregunta 1.

Pregunta 1: ¿Existe fiabilidad en el servicio en la transmisión de datos?

Tabla 1-4: Tabulación pregunta 1.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Siempre	2	16,67
Casi siempre	10	83,33
Nunca	0	0,00
TOTAL	**12**	**100%**

Elaborado por: Roberto Usca, 2017

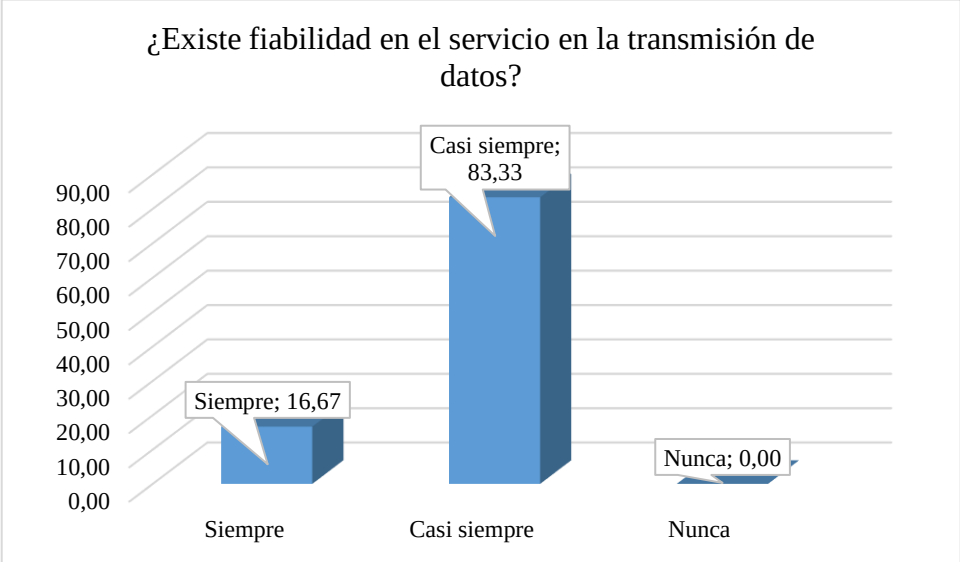


Gráfico 1-4: Resultados estadísticos pregunta 1.
Elaborado por: Roberto Usca, 2017

Análisis e interpretación

El Gráfico 1-4. De los datos obtenidos, tenemos que el 83,33% de las agencias encuestadas mencionaron “casi siempre” existe fiabilidad en el servicio en la transmisión de datos, mientras el 16,67% de las agencias encuestadas restantes afirmaron que siempre existe fiabilidad en el servicio en la transmisión de datos, en la red de la Corporación Eléctrica Regional de Bolívar.

Pregunta 2: ¿La capacidad de trabajo es suficiente en el sistema de transmisión de datos?

Tabla 2-4: Tabulación pregunta 2.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Siempre	8	66,67
Casi siempre	4	33,33
Nunca	0	0,00
TOTAL	**12**	**100%**

Elaborado por: Roberto Usca, 2017

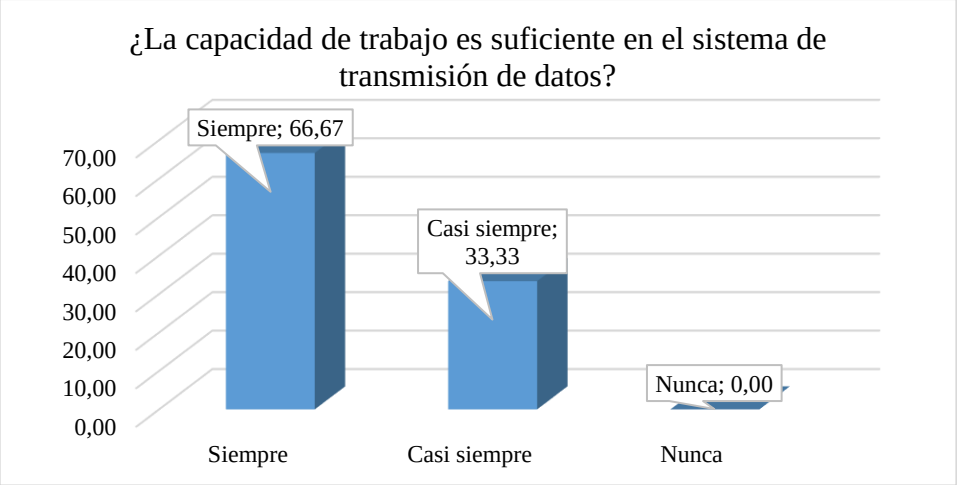


Gráfico 2-4: Resultados estadísticos pregunta 2.
Elaborado por: Roberto Usca, 2017

Análisis e interpretación

El Gráfico 2-4. Se tiene que el 66,67% de las agencias encuestadas mencionaron "siempre", que la capacidad de trabajo es suficiente en el sistema de transmisión de datos, es decir que es relativamente bueno, mientras el 33,33% de las agencias encuestadas restantes afirmaron que "casi siempre" la capacidad de trabajo es suficiente en el sistema de transmisión de datos, en la red de la Corporación Eléctrica Regional de Bolívar, Ninguna de las preguntas respondieron negativamente "Nunca".

Pregunta 3: ¿Existe capacidad de adaptación en la infraestructura de red para la transmisión de datos?

Tabla 3-4: Tabulación pregunta 3.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Siempre	8	66,67
Casi siempre	4	33,33
Nunca	0	0,00
TOTAL	**12**	**100%**

Elaborado por: Roberto Usca, 2017

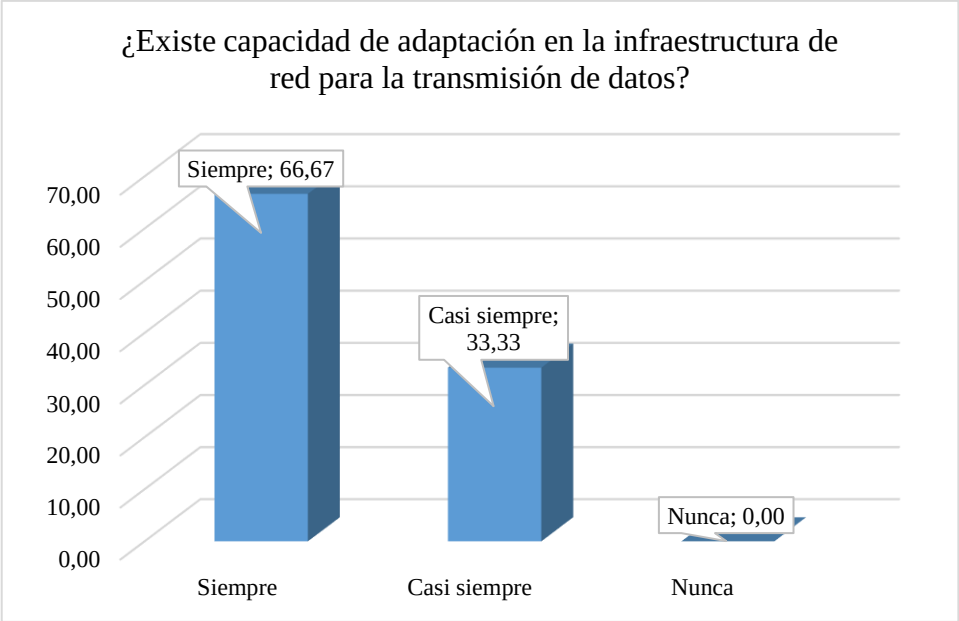


Gráfico 3-4: Resultados estadísticos pregunta 3.
Elaborado por: Roberto Usca, 2017

Análisis e interpretación

El Gráfico 3-4. de los datos obtenidos, tenemos que el 66,67% de las agencias encuestadas mencionaron "siempre", existe capacidad de adaptación en la infraestructura de red para la transmisión de datos, es decir que es relativamente bueno, mientras el 33,33% de las agencias encuestadas restantes afirmaron que "casi siempre" existe capacidad de adaptación en la infraestructura de red para la transmisión de datos en la red de la Corporación Eléctrica Regional de Bolívar, Ninguna de las preguntas respondieron negativamente "Nunca".

Pregunta 4: ¿Existe seguridad en la base de registro de datos de la red CNEL Bolívar?

Tabla 4-4: Tabulación pregunta 4.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Siempre	11	91,67
Casi siempre	1	8,33
Nunca	0	0,00
TOTAL	**12**	**100%**

Elaborado por: Roberto Usca, 2017

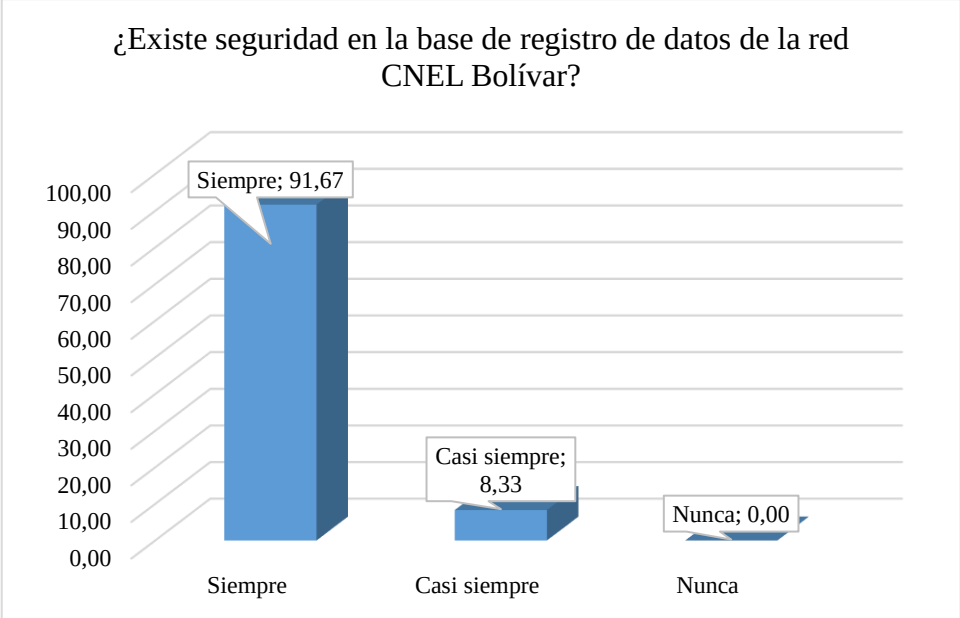


Gráfico 4-4: Resultados estadísticos pregunta 4.

Elaborado por: Roberto Usca, 2017

Análisis e interpretación

De acuerdo a los datos obtenidos, tenemos que el 91,67% de las agencias encuestadas mencionaron "siempre", existe seguridad en la base de registro de datos de la red CNEL Bolívar, es decir que es excelente, mientras el 8,33% de las agencias encuestadas restantes afirmaron que "casi siempre" existe seguridad en la base de registro de datos en la red de la Corporación Eléctrica Regional de Bolívar, Ninguna de las preguntas respondieron negativamente "Nunca", muestra el Gráfico 4.4.

Pregunta 5: ¿El rendimiento de red es adecuado para responder a la calidad en el servicio?

Tabla 5-4: Tabulación pregunta 5.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Siempre	6	50,00
Casi siempre	6	50,00
Nunca	0	0,00
TOTAL	**12**	**100%**

Elaborado por: Roberto Usca, 2017

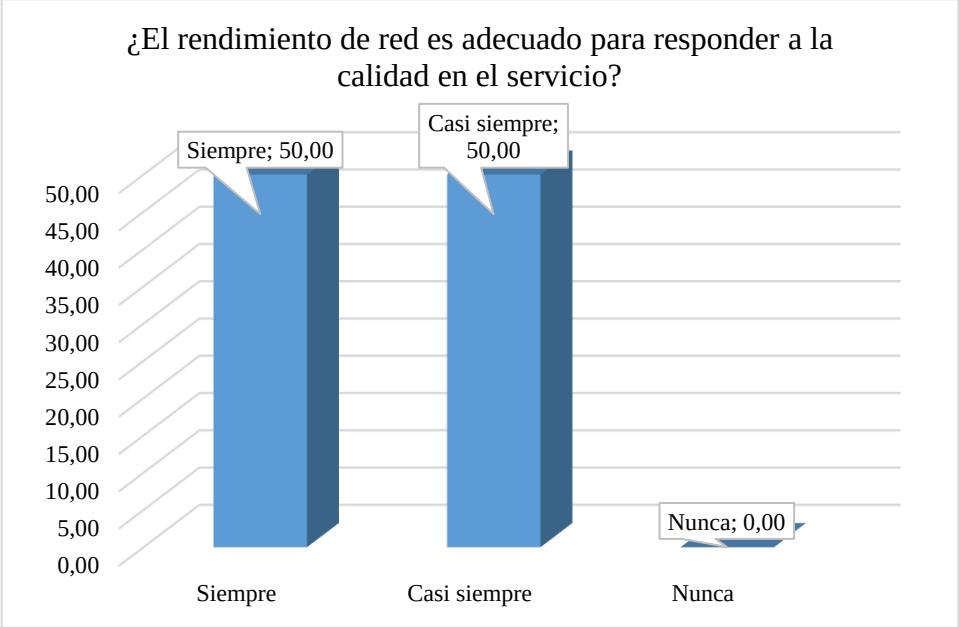


Gráfico 5-4: Resultados estadísticos pregunta 5.

Elaborado por: Roberto Usca, 2017

Análisis e interpretación

De acuerdo a los datos obtenidos en el Gráfico 5-4., tenemos que el 50% de las agencias encuestadas mencionaron "Siempre" el rendimiento de red es adecuado para responder a la calidad en el servicio, 50% de las agencias encuestadas mencionaron "casi siempre" el rendimiento de red es adecuado para responder a la calidad en el servicio en la red de la Corporación Eléctrica Regional de Bolívar.

Pregunta 6: ¿Es eficiente la transmisión de datos al presentar servicio al público?

Tabla 6-4: Tabulación pregunta 6.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Siempre	7	58,33
Casi siempre	5	41,67
Nunca	0	0,00
TOTAL	**12**	**100%**

Elaborado por: Roberto Usca, 2017

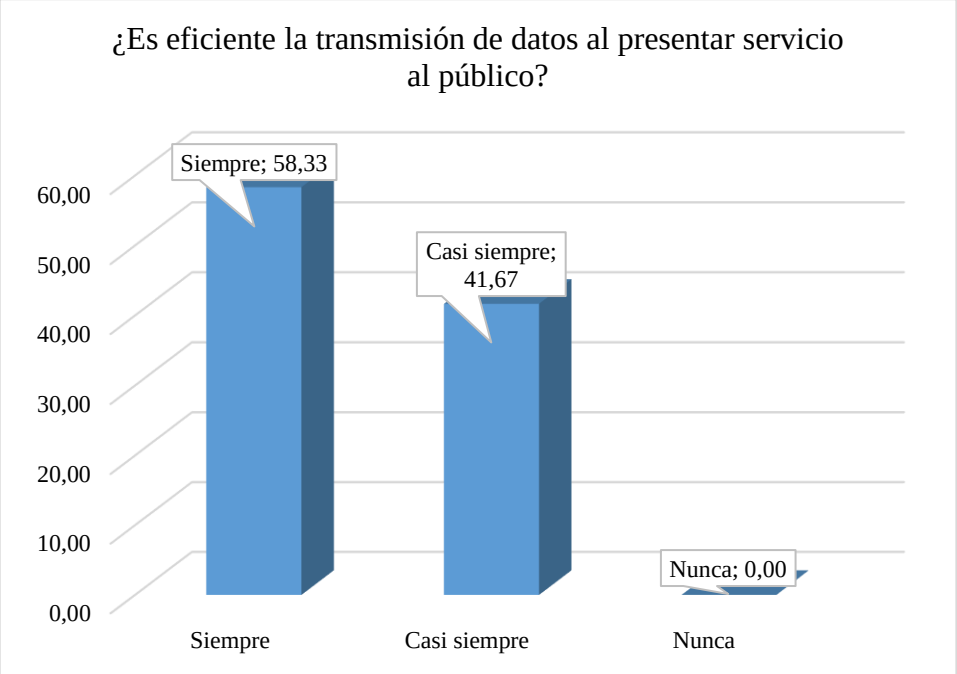


Gráfico 6-4: Resultados estadísticos pregunta 6.
Elaborado por: Roberto Usca, 2017

Análisis e interpretación

De acuerdo a los datos obtenidos en el Gráfico 6-4., tenemos que el 58,33% de las agencias encuestadas mencionaron "siempre", es eficiente la transmisión de datos al presentar servicio al público, mientras el 41,673% de las agencias encuestadas restantes afirmaron que "casi siempre" es eficiente la transmisión de datos al presentar servicio al público en la red de la Corporación Eléctrica Regional de Bolívar, Ninguna de las preguntas respondieron negativamente "Nunca".

Pregunta 7: ¿Cuándo se ingresa gran cantidad de información la velocidad de transmisión de datos es eficiente?

Tabla 7-4: Tabulación pregunta 7.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Siempre	3	25,00
Casi siempre	9	75,00
Nunca	0	0,00
TOTAL	**12**	**100%**

Elaborado por: Roberto Usca, 2017

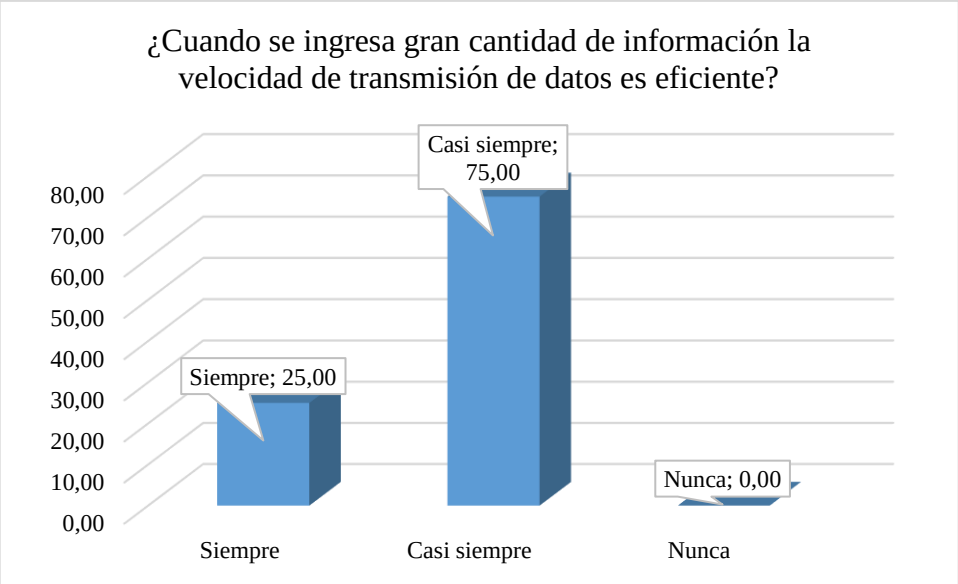


Gráfico 7-4: Resultados estadísticos pregunta 7.

Elaborado por: Roberto Usca, 2017

Análisis e interpretación

De acuerdo a los datos obtenidos en el Gráfico 7-4, tenemos que el 75% de las agencias encuestadas mencionaron "Casi siempre", la velocidad de transmisión de datos es eficiente al momento de ingresa gran cantidad de información, mientras el 25% de las agencias encuestadas restantes afirmaron que "casi siempre" la velocidad de transmisión de datos es eficiente al momento de ingresa gran cantidad de información en la red de la Corporación Eléctrica Regional de Bolívar, Ninguna de las preguntas respondieron negativamente "Nunca".

Pregunta 8: ¿Es considerablemente bueno el tiempo de transmisión de voz, datos y video?

Tabla 8-4: Tabulación pregunta 8.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Siempre	6	50,00
Casi siempre	6	50,00
Nunca	0	0,00
TOTAL	**12**	**100%**

Elaborado por: Roberto Usca, 2017

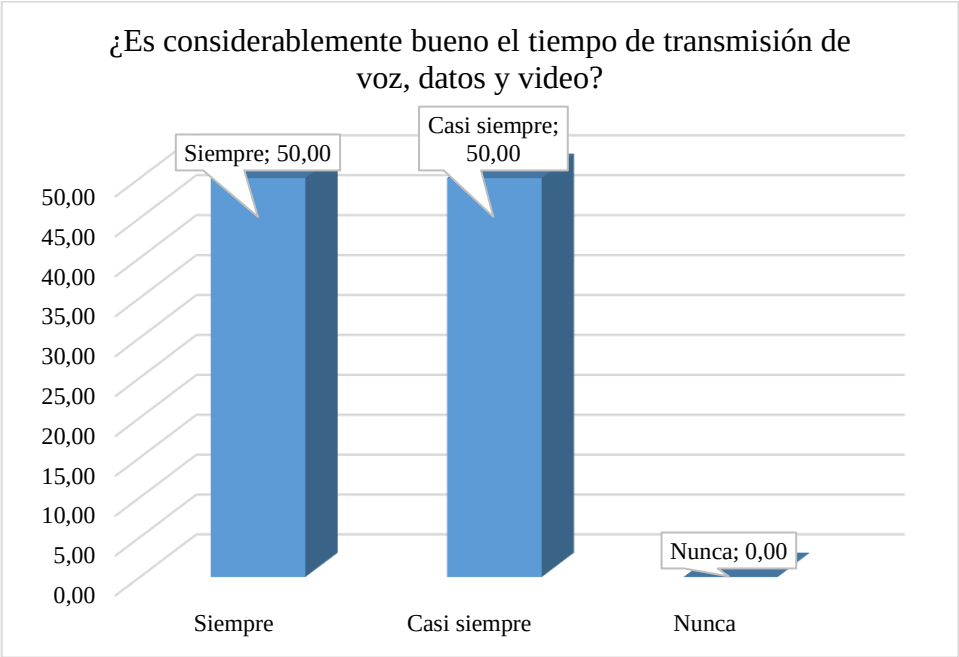


Gráfico 8-4: Resultados estadísticos pregunta 8.

Elaborado por: Roberto Usca, 2017

Análisis e interpretación

De acuerdo a los datos obtenidos en el Gráfico 8-4, tenemos que el 50% de las agencias encuestadas mencionaron "Siempre", es bueno el tiempo de transmisión de voz, datos y video, y 50% de las agencias encuestadas mencionaron "casi siempre" es bueno el tiempo de transmisión de voz, datos y video en la red de la Corporación Eléctrica Regional de Bolívar.

Pregunta 9: ¿Existen interrupciones en la transmisión de datos de manera periódica?

Tabla 9-4: Tabulación pregunta 9.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Siempre	0	0,00
Casi siempre	11	91,67
Nunca	1	8,33
TOTAL	**12**	**100%**

Elaborado por: Roberto Usca, 2017

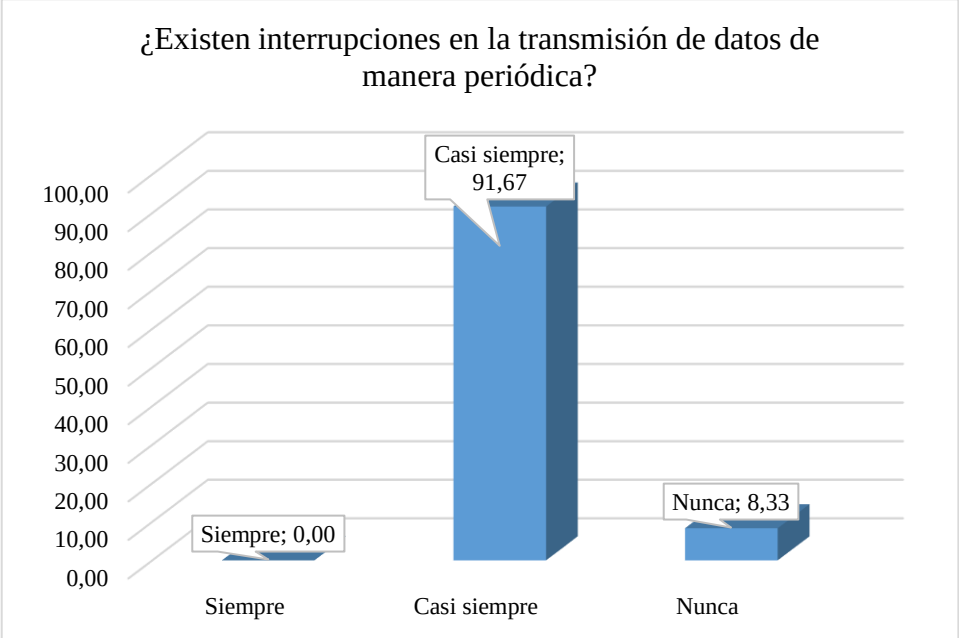


Gráfico 9-4: Resultados estadísticos pregunta 9.
Elaborado por: Roberto Usca, 2017

Análisis e interpretación

De acuerdo a los datos obtenidos en el Gráfico 9-4, tenemos que el 91,67% de las agencias encuestadas mencionaron "casi siempre" existen interrupciones en la transmisión de datos de manera periódica, mientras el 8,33% de las agencias encuestadas restantes afirmaron "Nunca" existen interrupciones en la transmisión de datos de manera periódica, en la red de la Corporación Eléctrica Regional de Bolívar.

Los resultados del cuestionario de chequeo que se aplicó a las once agencias y la matriz de la Corporación Nacional de Electricidad de Bolívar, se muestran en la siguiente tabla:

Tabla 10-4: Cuestionario de chequeo aplicado a CNEL Bolívar

N°	Interrogantes	Siempre	Casi siempre	Nunca	Total
Variable Independiente					
1	Existe fiabilidad en el servicio en la transmisión de datos	2	10	0	12
2	La capacidad de trabajo es suficiente en el sistema de transmisión de datos.	8	4	0	12
3	Existe capacidad de adaptación en la infraestructura de red para la transmisión de datos.	8	4	0	12
4	Existe seguridad en la base de registro de datos de la red CNEL Bolívar.	11	1	0	12
Variable dependiente					
5	El rendimiento de red es adecuado para responder a la calidad en el servicio.	6	6	0	12
6	Es eficiente la transmisión de datos al presentar servicio al público.	7	5	0	12
7	Cuando se ingresa gran cantidad de información la velocidad de transmisión de datos es eficiente.	3	9	0	12
8	Es considerablemente bueno el tiempo de transmisión de voz, datos y video	6	6	0	12
9	Existen interrupciones en la transmisión de datos de manera periódica	0	11	1	12
	Total	51	56	1	108

Elaborado por: Roberto Usca, 2017

Tabla 11-4: Resultados acumulados del Checklist aplicado a CNEL Bolívar

ALTERNATIVAS	FRECUENCIAS	PORCENTAJES
Siempre	51	47,706422
Casi siempre	56	51,3761468
Nunca	1	0,91743119
TOTAL		**100%**

Elaborado por: Roberto Usca, 2017

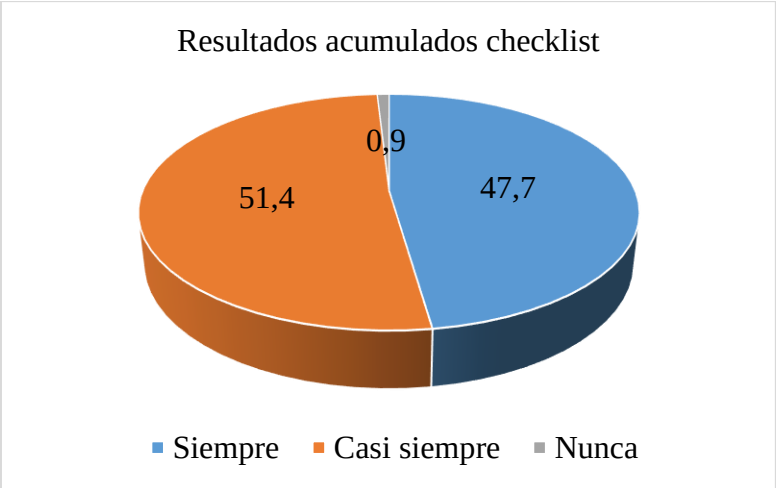


Figura 2-4: Resultados acumulados del Checklist aplicado a CNEL Bolívar

Elaborado por: Roberto Usca, 2017

ANÁLISIS E INTERPRETACIÓN:

La Figura 2-4 de la encuesta realizada a las 12 agencias (incluida la central) de la Corporación Eléctrica Regional de Bolívar, muestra un análisis descriptivo en el cual se puede evidenciar que la mayoría de respuestas corresponden a la opción "Casi siempre" con un 51,4 por ciento del total encuestado y un 47,7 que responden afirmativamente según el criterio de evaluación "Siempre", y el porcentaje de incumplimiento es insignificante o numéricamente despreciable por tener un 0,9 por ciento del total de las cuestiones realizadas.

4.3 Análisis inferencial

4.3.1 Verificación de hipótesis

Para la evaluación inductiva de la verificación de la Hipótesis en la presente investigación se utiliza la prueba de Chi Cuadrado (Ji cuadrado: x^2) con un 95.00% de confianza, y un 5% de error de muestreo en las 12 agencias de estudio de la Corporación Eléctrica de Bolívar.

En este caso investigativo para la verificación de hipótesis es necesario el planteamiento de hipótesis nula que desaprueba el análisis de proceso de control y de hipótesis alternativa la que, valida la fiabilidad de la investigación, continuamente se plantea cada una de ellas.

4.3.2 Planteamiento de la hipótesis.

Hipótesis Nula Ho: La aplicación de un sistema (MPLS/ VPN) no permite mejorar el rendimiento del sistema de trasmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

Hipótesis Alterna Ha: La aplicación de un sistema (MPLS/ VPN) permite mejorar el rendimiento del sistema de trasmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

4.3.3 Prueba de Chi-cuadrado

La fórmula de la prueba de Chi-cuadrado es:

$$x^2 = \sum \frac{(o_i - e_i)^2}{e_i}$$

Donde;

x^2 Chi-cuadrado

o_i Frecuencias observadas

e_i Frecuencias esperadas

4.3.4 Preguntas utilizadas en la comprobación de la hipótesis

Para la comprobación de la hipótesis, hacemos uso de las preguntas más relevantes y significativas de la investigación, para seleccionar las mencionadas preguntas aplicamos la condición, que cada una deba contener la variable dependiente y variable independiente, en la Tabla 12-4 se procede a analizar las preguntas las cuales son:

1. ¿Existe fiabilidad en el servicio en la transmisión de datos?

7 ¿Cuándo se ingresa gran cantidad de información la velocidad de transmisión de datos es eficiente?

4.3.5 Tabla de frecuencias observadas y frecuencias esperadas

Tabla 12-4: Frecuencias observadas

FRECUENCIAS OBSERVADAS (o_i)				
PREGUNTAS	7 ¿Cuándo se ingresa gran cantidad de información la velocidad de transmisión de datos es eficiente?			
		Siempre	Casi siempre	**TF**
1. ¿Existe fiabilidad en el servicio en la transmisión de datos?	Siempre	2	0	2
	Casi siempre	1	9	10
TOTAL	**TC**	**3**	**9**	**12**

Elaborado por: Roberto Usca, 2017

Posterior a ello se calcula las frecuencias esperadas como se muestra en la Tabla 13-4, la fórmula para obtener las observaciones esperadas (OE)

$$\boldsymbol{E = \frac{TF * TC}{n}}$$

En donde:

- TF = Total Fila
- TC = Total Columna
- n = Población

$$E = \frac{3 * 2}{12} = 0{,}5$$

$$E = \frac{9 * 2}{12} = 1{,}5$$

$$E = \frac{3 * 10}{12} = 2{,}5$$

$$E = \frac{9 * 10}{12} = 7{,}5$$

Tabla 13-4: Frecuencias esperadas

FRECUENCIAS ESPERADAS (e_i)				
PREGUNTAS	7 ¿ Cuándo se ingresa gran cantidad de información la velocidad de transmisión de datos es eficiente?			
		Siempre	Casi siempre	**TOTAL**
1. ¿ Existe fiabilidad en el servicio en la transmisión de datos?	Siempre	0,5	1,5	2
	Casi siempre	2,5	7,5	10
TOTAL		**3**	**9**	**12**

Elaborado por: Roberto Usca, 2017

4.3.6 Cálculo del Chi-cuadrado

A continuación, en la Tabla 14-4 se tiene el cálculo del Chi-cuadrado:

Tabla 14-4: Cálculo del Chi-cuadrado

FRECUENCIAS OBSERVADAS (o_i)	FRECUENCIAS ESPERADAS (e_i)	$o_i - e_i$	$(o_i - e_i)^2$	$\frac{(o_i - e_i)^2}{e_i}$
2,00	**0,5**	1,5	2,25	4,5
0,00	**1,5**	-1,5	2,25	0,56
1,00	**2,5**	-1,5	2,25	0,9
9,00	**7,5**	1,5	2,25	1,7
Chi-cuadrado calculado = $\sum \frac{(o_i - e_i)^2}{e_i}$				**7,66**

Fuente: CNEL Bolívar
Elaborado por: Roberto Usca, 2017

Chi-cuadrado calculado X^2c **=7,66**

4.3.7 Nivel de significación y regla de decisión

A continuación, se tiene los parámetros y datos que se han utilizado para demostrar la hipótesis:

- Probabilidad: **P**=0.05%

De la misma manera se calcula los grados de libertad para aplicar la prueba Chi-cuadrado, utilizando la siguiente formula:

- **GL**= (número de filas-1)*(número de columnas -1)

Donde:

- **GL**: Grados de libertad

- **Numero de filas:** Corresponden al número de preguntas a tomar en cuenta para la prueba Chi-cuadrado.

- **Numero de columnas:** Corresponden al número de alternativas de cada pregunta.

Cálculo grados de libertad

Se realiza las operaciones necesarias:

- GL= (2-1)*(2-1)

- GL= 1

De acuerdo a **p**=0.05% y **GL**=1, se procede a intersecar los dos valores en la tabla nominal de Chi-cuadrado y se obtiene de la Tabla 15-4.

Tabla 15-4: Tabla de Chi – Cuadrado

DF	P = 0,05	P = 0,01	P = 0,001
1	3,84	6,64	10,83
2	5,99	9,21	13,82
3	7,82	11,35	16,27
4	9,49	13,28	18,47

Elaborado por: Roberto Usca, 2017

Chi cuadrado de la tabla **X^2t = 3,84**

X^2c = 7,66 > X^2t = 3,84

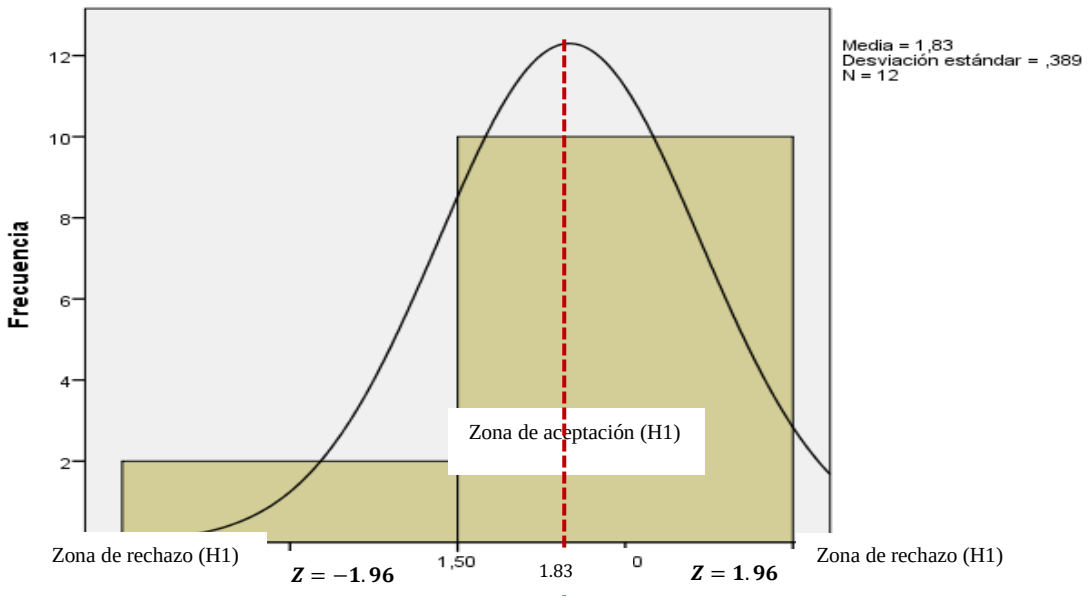


Gráfico 10-4: Representación de Chi cuadrado en la campana de Gauss
Fuente: Software estadístico SPSS
Elaborado por: Roberto Usca, 2017

4.3.8 Verificación de hipótesis

- *Si Chi*-cuadrado calculado $\boldsymbol{X^2c = 7.66}$ < Chi cuadrado de la tabla $\boldsymbol{X^2t = 3.84}$, aceptamos la Hipótesis nula (H0) y rechazamos la Hipótesis alternativa (H1)

- *Si* Chi-cuadrado calculado $\boldsymbol{X^2c = 7.66}$ > Chi cuadrado de la tabla $\boldsymbol{X^2t = 3.84}$, rechazamos la Hipótesis nula (H0) y aceptamos la Hipótesis alternativa (H1)

En virtud de los resultados observados y analizados se puede evidenciar que el valor de Chi-cuadrado calculado es mayor que el Chi-cuadrado de la tabla, por lo cual cae en la zona de rechazo de la Hipótesis nula (H0), por lo que se acepta Hipótesis alternativa (H1), la cual indica que: *"La aplicación de un sistema (MPLS/ VPN) permite mejorar el rendimiento del sistema de trasmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar".*

4.3.9 Comprobación mediante el software SPSS

En la Tabla 16-4 se puede notar que el software SPSS es de gran ayuda para evidenciar las medidas de tendencia central para el numero de muestras N=12, la media es de 1,83 conociendo que 1: Siempre; 2: Casi siempre; 3: nunca, la moda equivale el valor que más se repite en la adquisición de muestras del Checklist, es decir las respuestas más repetitivas respondieron "casi siempre", La desviación estándar implica cuánto pueden alejarse los valores respecto a la media lo cual está entre el 39% y un 51%. La asimetría del -2,055 muestra que existe un sesgo en la gráfica en el lado izquierdo por ende los datos se encuentran agrupados en el lado derecho, estando estos más próximos a la media.

Tabla 16-4: Medidas estadísticas de tendencia central

		Existe fiabilidad en el servicio en la transmisión de datos	Es eficiente la transmisión de datos al presentar servicio al público.
N	Válido	12	12
	Perdidos	0	0
Media		1,8333	1,4167
Moda		2,00	1,00
Desviación estándar		,38925	,51493
Asimetría		-2,055	,388
Error estándar de asimetría		,637	,637
Curtosis		2,640	-2,263
Error estándar de curtosis		1,232	1,232

Fuente: Software estadístico SPSS
Elaborado por: Roberto Usca, 2017

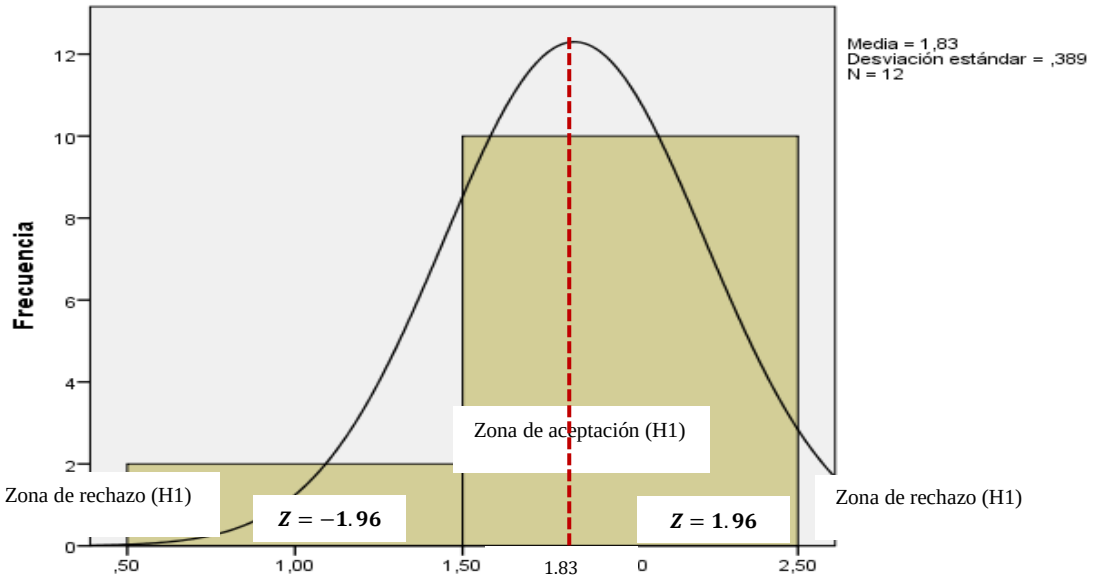


Gráfico 11-4: Representación de Chi cuadrado en la campana de Gauss
Fuente: Software estadístico SPSS
Elaborado por: Roberto Usca, 2017

De la Figura 11-4 se analiza también la curtosis analiza "el grado de concentración que presentan los valores alrededor de la zona central de la distribución", en el caso estudiado se evidencia una curtosis (2,6) con una curva leptocúrtica que presenta un elevado grado de concentración de datos alrededor de los valores centrales de la variable, es un valor relativamente bueno que garantiza confianza en los datos analizados en la investigación, los datos analizados.

Para la comprobación del Chi-Cuadrado, se hizo uso del software estadístico SPSS que es un software estadístico que permite realizar este tipo de cálculos o análisis del mismo. A continuación, se tiene las Tablas 17-4 y Tabla 18-4 que se generan en el software.

T**abla 17-4**. Correlación observada entre las variables de estudio

PREGUNTAS		7. ¿ Cuándo se ingresa gran cantidad de información la velocidad de transmisión de datos es eficiente?		**Total**
		Siempre	Casi siempre	
1. ¿ Existe fiabilidad en el servicio en la transmisión de datos?	Siempre	2	0	2
	Casi siempre	1	9	10
Total		**3**	**9**	**12**

Elaborado por: Roberto Usca, 2017

Tabla 18-4: Correlación esperada entre las variables de estudio chi-cuadrado

	Valor	gl	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)	Probabilidad en el punto
Chi-cuadrado	7,200	1	,007	,045	,045	

Corrección de continuidad	3,200	1	,074			
Razón de verosimilitud	6,994	1	,008	,045	,045	
Prueba exacta de Fisher				,045	,045	
Asociación lineal por lineal	6,600	1	,010	,045	,045	,045
N de casos válidos	12					

a. 3 casillas (75,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,50.

b. Sólo se ha calculado para una tabla 2x2

Elaborado por: Roberto Usca, 2017

Se analiza con pruebas asintóticas cuando el tamaño de la muestra es relativamente alto (Superior a 30) y se utiliza pruebas exactas cuando el tamaño de la muestra es menor a 30. Se puede evidenciar el nivel de significación es del 0.045, es decir mayor al 95 % de confiabilidad. Y un valor de chi-cuadrado calculado de 7.2

Una vez realizado el cruce de las variables utilizando las *preguntas "7. ¿Cuándo se ingresa gran cantidad de información la velocidad de transmisión de datos es eficiente?"* y 1. *"¿Existe fiabilidad en el servicio en la transmisión de datos?"*, se puede observar que los datos obtenidos muestran un nivel de significancia inferior al 5%(0,045), por lo cual se concluye que el proyecto de investigación es viable aceptando la hipótesis alternativa.

4.4 Análisis de fiabilidad con Alfa de Cronbach

Para determinar la fiabilidad de los datos se analiza mediante la consistencia interna es el método Alfa de Cronbach, para ello es necesario la aplicación del software estadístico SPSS. Para lo cual se utiliza la encuesta planteada con 9 preguntas o ítems, la cual determina el nivel de aceptación de las agencias de la Corporación Nacional Eléctrica Regional de Bolívar.

Para evaluar los coeficientes de alfa de Cronbach se recomienda considerar los siguientes criterios generales:

- Coeficiente alfa >.9 es excelente
- Coeficiente alfa >.8 es bueno
- Coeficiente alfa >.7 es aceptable
- Coeficiente alfa >.6 es cuestionable

- Coeficiente alfa >.5 es pobre

- Coeficiente alfa <.5 es inaceptable

El objetivo del siguiente análisis de fiabilidad es establecer cuáles son las preguntas de la encuesta que contribuyen datos consistentes, para lo cual utilizaremos el método de Alfa de Cronbach, a continuación, se detallan y analizan cada una de las tablas.

En la siguiente tabla tenemos el número de casos, es decir el número de personas que han respondido a la encuesta, en este caso 12 Agencias a ser analizadas.

Tabla 19-4: Resumen de procesamiento de casos.

Resumen de procesamiento de casos			
		N	%
Casos	Válido	12	100,0
	Excluido		
	Total	12	100,0

Elaborado por: Roberto Usca, 2017

La siguiente tabla corresponde al Alfa de Cronbach general, tomando en cuenta las 9 preguntas, siendo el valor de Alfa de Cronbach igual a 0,79, siendo un valor aceptable según la escala.

Tabla 20-4: Estadísticas de fiabilidad con Alfa de Cronbach

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
0,779	10

Elaborado por: Roberto Usca, 2017

A continuación, se estudia cada una de las preguntas en cuanto al aporte que estas ofrecen, en la tabla siguiente se tiene valores de todas las preguntas, para poder medir la correlación de elementos, se toma en cuenta la tercera columna "Correlación total de elementos corregida".

En la Tabla 21-4, se puede observar que la pregunta ocho (8) tiene un valor de 0,15 en correlación y la pregunta nueve (9) un valor de 0,18, de acuerdo al criterio de: (0 – 0,25 escasa o nula; 0,26-0,50 débil; 0,51- 0,75 entre moderada y fuerte; 0,76- 1,00 entre fuerte y perfecta), son valores relativamente bajos y por ende no están aportando en nada a la obtención de datos significativos y confiables, por ello se puede eliminar dichos ítems o preguntas, con el propósito de incrementar el valor del Alfa de Cronbach y por ende el nivel fiabilidad.

Tabla 21-4: Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
1. Existe fiabilidad en el servicio en la transmisión de datos	12,0000	2,727	0,85	0,67
2. La capacidad de trabajo es suficiente en el sistema de transmisión de datos.	12,5000	3,727	0,29	0,99
3. Existe capacidad de adaptación en la infraestructura de red para la transmisión de datos	12,5000	2,636	0,68	0,69
4. Existe seguridad en la base de registro de datos de la red CNEL Bolívar.	12,7500	3,841	0,42	0,94
5. El rendimiento de red es adecuado para responder a la calidad en el servicio.	12,3333	2,424	0,84	0,62
6. Es eficiente la transmisión de datos al presentar servicio al público.	12,4167	2,265	0,97	0,54
7. Cuando se ingresa gran cantidad de información la velocidad de transmisión de datos es eficiente.	12,0833	2,629	0,79	0,79
8. Es considerablemente bueno el tiempo de transmisión de voz, datos y video.	12,3333	3,152	0,15	0,87
9. Existen interrupciones en la transmisión de datos de manera periódica.	11,7500	3,659	0,18	0,90

Elaborado por: Roberto Usca, 2017

Luego de haber eliminado las preguntas ocho (8) y nueve (9), en la Tabla 22-4 se observa como el valor de Alfa de Cronbach aumenta y los valores de la tabla de "Estadísticas de total de elemento" también.

Tabla 22-4: Estadísticas de fiabilidad

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
0,80	7

Elaborado por: Roberto Usca, 2017

Por ende, el promedio de análisis de confiabilidad se incrementa, las preguntas involucradas en el análisis se encuentran inmersas en el estudio y su coeficiente confiabilidad se encuentra en un nivel óptimo.

Tabla 23-4: Estadísticas de total de elemento

Estadísticas de total de elemento				
	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
1. Existe fiabilidad en el servicio en la transmisión de datos	12,0000	2,727	0,849	0,8436
2. La capacidad de trabajo es suficiente en el sistema de transmisión de datos.	12,5000	3,727	0,2865	0,99
3. Existe capacidad de adaptación en la infraestructura de red para la transmisión de datos	12,5000	2,636	0,6825	0,69
4. Existe seguridad en la base de registro de datos de la red CNEL Bolívar.	12,7500	3,841	0,4215	0,9405
5. El rendimiento de red es adecuado para responder a la calidad en el servicio.	12,3333	2,424	0,8385	0,621
6. Es eficiente la transmisión de datos al presentar servicio al público.	12,4167	2,265	0,9716	0,68

7. Cuando se ingresa gran cantidad de información la velocidad de transmisión de datos es eficiente.	12,0833	2,629	0,7905	0,8379

Elaborado por: Roberto Usca, 2017

Los resultados debidamente detallados en la Tabla 23-4, se concluye que el cuestionario de chequeo aplicado a las 12 agencias de la Corporación Nacional Eléctrica de Bolívar, determina la influencia del rendimiento de la red de transmisión de datos y la velocidad de transmisión y la fiabilidad de transmisión de datos es imprescindible, por ello es necesario la implementación de un protocolo MPLS para mejorar el rendimiento de la red por ende la velocidad de transmisión y Redes Privadas Virtuales para que la red presente fiabilidad y seguridad.

4.5 Selección de protocolo

La selección del mejor protocolo se analiza en la siguiente tabla, en las cuales se realiza pondera un valor cuantitativo de las características de prestaciones de cada protocolo y depende también del nivel de seguridad, esto se analiza a continuación:

Tabla 24-4. Comparación entre las tecnologías utilizadas para la optimización del ancho de banda en las VPN.

Protocolo	Cuando se utiliza	Nivel de seguridad	Prestaciones	Total prestaciones
IPSec	Conexión a un servidor VPN de terceros	Alto	• Permite conectar a un servidor VPN que no sea de Microsoft.	1
MPLS	Conexión a un servidor VPN de terceros	Alto	• Permite compartir un único acceso a Internet entre todas las redes. No es necesario que las redes estén conectadas a Internet para acceder a la VPN. • Otorga mayor control a los administradores sobre sus redes. • Mejora la interacción del usuario con el sistema y reduce costos al asignar recursos con mayor eficiencia al ancho de banda.	3
L2TP	Internet Security and Acceleration (ISA) Server 2004	Alto	• Usa enrutamiento y acceso remoto. • Menos complicada que la solución de túnel IPSec, pero requiere que el servidor VPN remoto sea un equipo	2

	Servidor VPN de Windows		servidor ISA o un servidor VPN de Windows.	
PPTP	ISA Server 2004 ISA Server 2000 Servidor VPN de Windows	Moderado	• Usa enrutamiento y acceso remoto. • Las mismas restricciones que L2PT, aunque algo más fácil de configurar. • Se considera que L2TP es más seguro, ya que utiliza cifrado IPSec.	3

Fuente: (Gutiérrez, 2015)

El protocolo que presenta mayores prestaciones de servicio es el protocolo MPLS y su nivel de seguridad es alto, por lo que se considera la mejor opción y el protocolo que se encuentra con mayor eficacia en la conexión de VPN con terceros servidores.

CAPÍTULO V

5 PROPUESTA

5.1 Análisis de la red de datos actual en la Corporación Nacional de Electricidad Regional Bolívar.

Actualmente la Corporación Nacional de Electricidad Regional Bolívar disponen de una red conectada por radioenlaces en la banda de 5.8 GHz usando antenas Ubiquiti y Mikrotik, los antecedentes técnicos evidencian que se ha producido muchas falencias en la red por lo cual los administradores de red de CNEL han visto prudente usar a un ISP como es CNT para comunicar las diferentes agencias y su matriz. CNT provee el servicio de interconectividad por medio de fibra lo cual brinda confiabilidad a CNEL, en caso de que pierda este enlace principal entra a funcionar o falle la infraestructura de radioenlaces propia de CNEL de esta manera se ha implementado mayor confiabilidad a la red.

CNEL está formado la Matriz CNEL ubicado en la ciudad de Guaranda que es Provincia de Bolívar, 11 agencias distribuidas estratégicamente en toda la provincia de Bolívar además de 6 subestaciones.

En la Matriz CNEL, disponen de servidores de datos, audio y video. Además de un Firewall HUAWEI USG6600 lo que permite políticas de seguridad en la red, además disponen de servidores de Elastix appliance ELX3000 para el servicio de voz, Huawei VCN3000 para el servicio de video y para datos un servidor en Linux. En cada agencia disponen de entre 2 a 3 computadoras para el proceso de cobros de sus planillas de consumo.

El direccionamiento IP manejado en los radioenlaces punto a punto es 172.17.191.1/25 lo que permite la interconectividad, puesto que todo se encuentra en la misma red no hay la necesidad de usar un protocolo de enrutamiento.

Con respecto al año 2013 que se usaba equipos inalambricos ROR 1000 y COR1100 en la banda de 2,4 GHz se ha procedido a cambiar de equipos y actualmente usan equipos en las marcas Ubiquiti y mikrotik en la banda de 5,8 GHz.

Para el monitoreo de Red se usa “THE DUDE” que es una herramienta integrada en equipos Mikrotik y también “CACTI”. Son las herramientas de red que permiten monitorizar y visualizar gráficas y estadísticas de dispositivos conectados a una red y que tengan habilitado el protocolo SNMP.

Políticas de seguridad

- ✓ Los administradores de CNEL proceden a realizar backups de datos una vez por semana.
- ✓ Los mantenimientos de red se realizan cada seis meses.
- ✓ Monitoreo de Red con “THE DUDE” y “CACTI”
- ✓ Existen tres áreas en CNEL, comercial, recaudación y contratos cada una de estas áreas tienen sus permisos dentro de la red, como es acceso a ciertos servicios restricción de redes sociales, bloqueo de aplicaciones entre otras políticas de seguridad.
- ✓ Si el enlace principal de CNT falla, entra a funcionar la red de backup inmediatamente.
- ✓ Los cambios de contraseñas se lo realiza cada 70 días, no poseen un gestor de contraseñas.

En **la topología de la red CENEL Bolívar** mostrada a continuación presenta una deficiencia y que podría provocar que casi el 60 % de las agencias queden sin servicio e imposibilitadas. Exactamente en el radioenlace REP PISCOQUERO – REP SUSANGA si este fallase varias agencias terminarían sin servicio, además se puede ver claramente que no existe redundancia en la red. También se puede describir que los enlaces son de 10 Mbps, para mejorar el desempeño de la red se propone modificar la red, con el objetivo que la red sea más robusta con respecto a fallos de caídas de enlaces y seguridad en el manejo de la información.

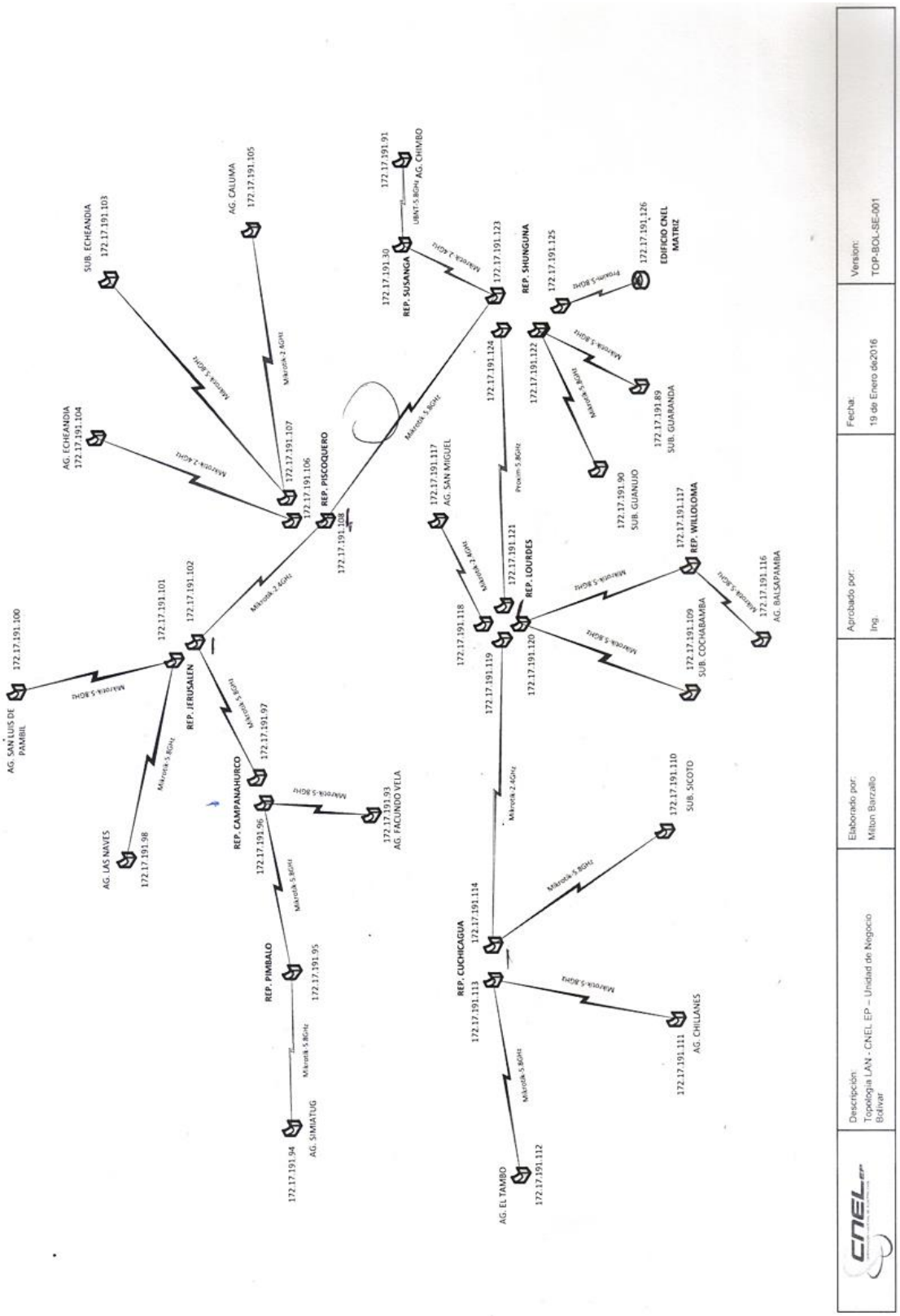


Figura 1-5: Topología de Red Actual de CNEL

Fuente: CNEL Bolivar, 2017

5.2 Equipamiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar

A continuación, los principales equipos de la Corporación Nacional de Electricidad Regional Bolívar que actualmente se encuentran utilizando.

Tabla 1-5: Lista de Equipos de radio para las Sub-Estaciones y Agencias

Cantidad	Equipo	Marca	Modelo
1	Antena parabólica 2,4 GHz	HYPERLINK	HG4958DP-25D
1	Antena parabólica 5,8 GHz	HYPERLINK	HG4958DP-30D
1	Tarjeta 411	MIKROTIK	411AH Licence4
1	Radio y pigtails	MIKROTIK	R52Hn
1	Fuentes POE	UBIQUITI	GP420-240-100

Realizado por: Roberto Usca, 2017

Tabla 2-5: Lista de Equipos para Repetidora Shunguna

Cantidad	Equipo	Marca	Modelo
2	Tarjeta y radio integrado	PROXIM	Q8100
1	Tarjeta 433	MIKROTIK	433AH
4	Tarjeta MiniPci	MIKROTIK	R52Hn
2	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-30D
2	Antena parabólica 2,4 Ghz	HYPERLINK	HG4958DP-25D
1	Antena grilla 2,4 Ghz	HYPERLINK	25 dBi
2	Fuentes POE	PROXIM	48G
2	Fuentes POE	UBIQUITI	GP420-240-100
1	Switch	HP	V1405-8
1	APS	TRIPP-LITE	APS-1250
1	Pararrayos	Parres	EP-D
1	Conexión a tierra		
4	Patch cord 3F	LEVITON	
1	Torre 21 m		
1	Caja para exterior		
2	Baterías	BLESS POWER	6FM100E-X

Fuente: (Usca, 2017)

Tabla 3-5: Repetidora Lourdes

Cantidad	Equipo	Marca	Modelo
2	Tarjeta y radio integrado	PROXIM	Q8100
1	Tarjeta 433	MIKROTIK	433AH
2	Tarjeta 411	MIKROTIK	411AH
3	Tarjeta MiniPci	MIKROTIK	R52Hn
1	Tarjeta MiniPci	UBIQUITI	XR2
1	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-30D
2	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-25D
2	Antena parabólica 2,4 Ghz	HYPERLINK	HG2429
4	Protectores de cable	MOTOROLA	600SS
1	Fuentes POE	PROXIM	48G
3	Fuentes POE	UBIQUITI	GP420-240-100
1	Switch	HP	V1405-8
1	APS	TRIPP-LITE	APS-1250
1	Conexión a tierra		
4	Patch cord 3F	LEVITON	
2	Baterías	BLESS POWER	6FM100E-X

Fuente: (Usca, 2017)

Tabla 4-5: Repetidora Cuchicagua

Cantidad	Equipo	Marca	Modelo
2	Tarjeta 433	MIKROTIK	433AH LICENCE 4
3	Tarjeta MiniPci	MIKROTIK	R52Hn
1	Tarjeta MiniPci	UBIQUITI	XR2
3	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-30D
1	Antena parabólica 2,4 Ghz	HYPERLINK	HG2429
2	Protectores de cable	MOTOROLA	600SS
2	Fuentes POE	UBIQUITI	GP420-240-100
1	Switch	HP	V1405-8
1	APS	TRIPP-LITE	APS-1250
1	Pararrayos	PARRES	EP-D
2	Patch cord 3F	LEVITON	
1	Torre 24m		
1	Caja para exterior		
2	Baterías	BLESS POWER	6FM100E-X

Fuente: (Usca, 2017)

Tabla 5-5: Repetidora Piscoquero

Cantidad	Equipo	Marca	Modelo
2	Tarjeta 433	MIKROTIK	433AH LICENCE 4
1	Tarjeta 411	MIKROTIK	433AH LICENCE 4
2	Tarjeta MiniPci	MIKROTIK	R52Hn
3	Tarjeta MiniPci	UBIQUITI	XR2
2	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-30D
3	Antena parabólica 2,4 Ghz	HYPERLINK	HG2429
3	Protectores de cable	MOTOROLA	600SS
3	Fuentes POE	UBIQUITI	GP420-240-100
1	Switch	HP	V1405-8
1	APS	TRIPP-LITE	APS-1250
1	Pararrayos	PARRES	EP-D
1	Conexión a tierra		
3	Patch cord 3F	LEVITON	
1	Torre 24m		
1	Caja para exterior		
2	Baterías	BLESS POWER	6FM100E-X

Fuente: (Usca, 2017)

Tabla 6-5: Repetidora Jerusalen

Cantidad	Equipo	Marca	Modelo
1	Tarjeta y radio integrado	PROXIM	Q8100
1	Tarjeta 433	MIKROTIK	433AH
2	Tarjeta 411	MIKROTIK	411AH
3	Tarjeta MiniPci	MIKROTIK	R52Hn
1	Tarjeta MiniPci	UBIQUITI	XR2
1	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-30D
2	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-25D
1	Antena parabólica 2,4 Ghz	HYPERLINK	HG2429
4	Protectores de cable	MOTOROLA	600SS
1	Fuentes POE	PROXIM	48G
3	Fuentes POE	UBIQUITI	GP420-240-100
1	Switch	HP	V1405-8
1	APS	TRIPP-LITE	APS-1250

1	Conexión a tierra		
4	Patch cord 3F	LEVITON	
2	Baterías	BLESS POWER	6FM100E-X
1	Torre 24m		

Fuente: (Usca, 2017)

Tabla 7-5: Repetidora Campanahurco

Cantidad	Equipo	Marca	Modelo
3	Tarjeta 411	MIKROTIK	411AH
2	Tarjeta MiniPci	MIKROTIK	R52Hn
3	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-30D
4	Protectores de cable	MOTOROLA	600SS
1	Fuentes POE	PROXIM	48G
3	Fuentes POE	UBIQUITI	GP420-240-100
1	Switch	HP	V1405-8
1	APS	TRIPP-LITE	APS-1250
1	Conexión a tierra		
4	Patch cord 3F	LEVITON	
2	Baterías	BLESS POWER	6FM100E-X
1	Torre 24m		

Fuente: (Usca, 2017)

Tabla 8-5: Repetidora Pimbalo y Willoloma

Cantidad	Equipo	Marca	Modelo
2	Tarjeta 411	MIKROTIK	411AH
2	Tarjeta MiniPci	MIKROTIK	R52Hn
2	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-30D
4	Protectores de cable	MOTOROLA	600SS
1	Fuentes POE	PROXIM	48G
3	Fuentes POE	UBIQUITI	GP420-240-100
1	Switch	HP	V1405-8
1	APS	TRIPP-LITE	APS-1250
1	Conexión a tierra		
4	Patch cord 3F	LEVITON	
2	Baterías	BLESS POWER	6FM100E-X
1	Torre 24m		

Fuente: (Usca, 2017)

5.3 Rediseño de radioenlace de la red de datos de la Corporación Nacional de Electricidad Regional Bolívar en Radio Mobile.

A continuación, se determina el rediseño de Enlaces de Radio de la Corporación Nacional de Electricidad Regional de Bolívar como se observa en la Figura 2-5, se utiliza enlaces a 5,8Ghz que posteriormente se especifica su funcionalidad y configuración con más detalles, además se puede evidenciar que la red cubre toda la provincia de Bolívar. También se puede describir que hay enlaces fundamentales que en el caso de que fallen, un porcentaje de Agencias se quedaran inhabilitadas, para evitar este tipo de problemática se usara MPLS con VPN posteriormente.

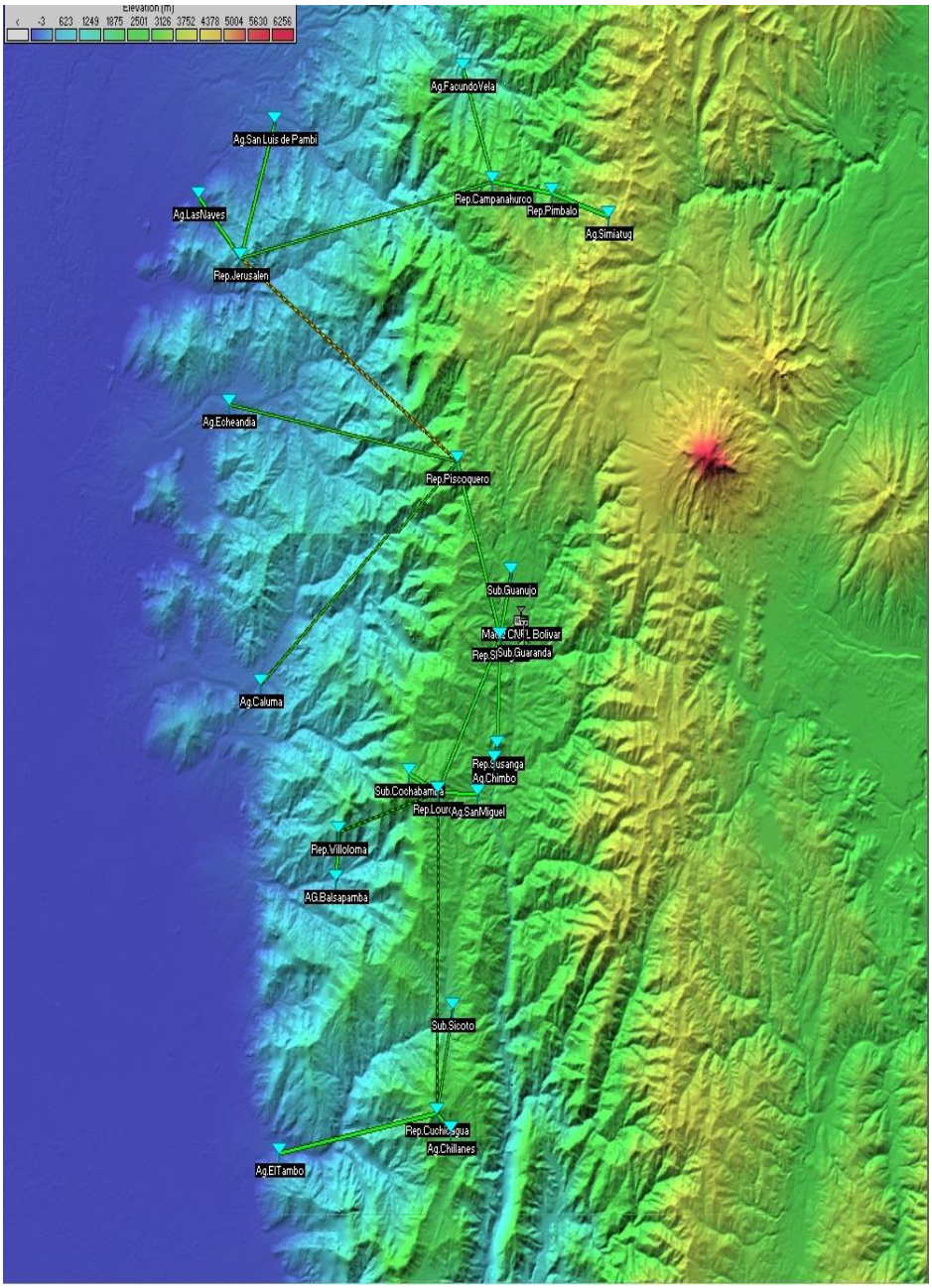


Figura 2-5: Diseño de Enlaces de Radio Actual
Elaborado por: Roberto Usca, 2017

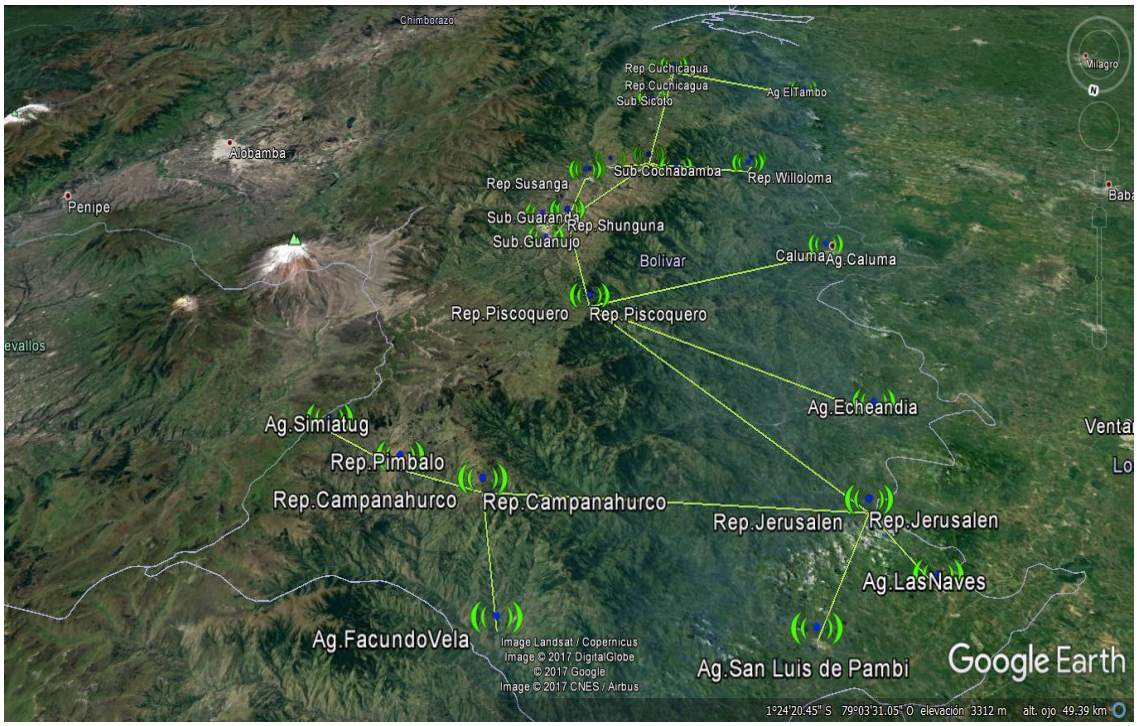


Figura 3-5. Radio Enlaces en Google Earth
Elaborado por: Roberto Usca, 2017

Se identifica la conexión de radioenlace de las agencias y sus repetidoras en toda la Corporación Eléctrica Regional de Bolívar, para esto se realiza con el software de Radio Mobile para identificar la ubicación aproximada de sus puntos en longitud y latitud de todos los puntos de red como se muestra en la Tabla 9-5:

Ubicación geográfica de enlaces de radio de CNEL Bolívar

Es indispensable identificar los puntos en los cuales están situados en la red, para determinar el radio enlace y realizar su configuración en Radio Mobile.

Tabla 9-5: Identificación de puntos de red

NOMBRE	LATITUD	LONGITUD
Matriz CNEL Bolivar	1°35'2.96"S	78°59'54.13"O
Rep. Shunguna	1°35'52.80"S	79° 1'8.00"O
Rep. Susanga	1°40'26.90"S	79° 1'18.18"O
Rep. Piscoquero	1°28'14.30"S	79° 3'43.10"O
Rep. Lourdes	1°42'19.74"S	79° 4'46.40"O
Rep. Cuchicagua	1°55'44.00"S	79° 4'51.00"O
Rep. Campanahurco	1°16'32.49"S	79° 1'38.79"O
Rep. Jerusalen	1°19'42.14"S	79°16'22.09"O

Rep. Pimbalo	1°17'0.57"S	78°58'10.64"O
Rep. Willoloma	1°43'58.62"S	79°10'33.78"O
Sub. Cochabamba	1°41'35.30"S	79° 6'28.20"O
Sub. Guaranda	1°35'45.54"S	78°59'45.96"O
Sub. Guanujo	1°35'45.54"S	78°59'45.96"O
Sub. Sicoto	1°51'19.80"S	79° 3'52.92"O
Ag. Caluma	1°37'48.72"S	79°15'7.10"O
Ag. Echeandia	1°25'51.42"S	79°16'58.32"O
Ag. Chimbo	1°41'1.92"S	79° 1'27.06"O
Ag. San Miguel	1°42'27.24"S	79° 2'27.72"O
Ag. Chillanes	1°56'30.12"S	79° 4'0.54"O
Ag. El Tambo	1°57'25.00"S	79°14'1.00"O
Ag. San Luis de Pambil	1°14'3.16"S	79°14'20.56"O
Ag. Las Naves	1°17'12.22"S	79°18'47.99"O
Ag. Facundo Vela	1°11'49.76"S	79° 3'21.84"O
Ag. Simiatug	1°18'0.69"S	78°54'52.34"O
AG. Balsapamba	1°46'1.01"S	79°10'44.06"O

Fuente: Roberto Usca, 2017

En la Tabla 10-5 se efectúo un analisis de radioenlace que se realizó en Radio Mobile y a su vez se muestran en el Anexo A, y todos los enlaces de la nueva red están trabajando a 5.8Ghz y las alturas de las antenas son un promedio de 24m, además de usar equipos MikroTik por varios aspectos como es su potencia de Tx para cada punto de transmisión de datos y su ganancia específicamente lo que permite cubrir largas distancias.

Tabla 10-5: Parametros de radioenlace de la red CNEL Bolívar realizadas en RadioMobile

Transmisión	Rep. Shunguna	Recepción	Matriz CNEL Bolívar
Tx Power	100 W-50 dBm	Requiered E Field	6,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=89,13 kW ERP=54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	21	Antena height(m)	7
Transmisión	Rep. Shunguna	Recepción	Sub Guaranda
Tx Power	1,1585 W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=5,62 W ERP=3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	21	Antena height(m)	3

Transmisión	Rep. Shunguna	Recepción	Sub Guanujo
Tx Power	1,1585 W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=5,62 W ERP=3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	21	Antena height(m)	3
Transmisión	Rep. Shunguna	Recepción	Rep Susanga
Tx Power	0,5012 W-27 dBm	Requiered E Field	20,24 dBµV/m
Line loss (dB)	0,0 dB	Antenna gain	10 dBi-7,8 dBd
Antena gain	10 bBi-7,8 dBd	Line loss	0,0 dB
Radiated power	EIRP=5,01 W ERP=3,06 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	21	Antena height(m)	21
Transmisión	Rep. Shunguna	Recepción	Rep Piscoquero
Tx Power	0,1585 W-22 dBm	Requiered E Field	21,2 dBµV/m
Line loss (dB)	0,5-0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=6,31 W ERP=3,85 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	16,5	Antena height(m)	24
Transmisión	Rep. Shunguna	Recepción	Rep Lourdes
Tx Power	100 W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP=54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	21	Antena height(m)	21
Transmisión	Rep. Susanga	Recepción	Ag. Chimbo
Tx Power	0,3981W-26 dBm	Requiered E Field	3,08 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	34 dBi-31,8 dBd
Antena gain	34 bBi-31,8 dBd	Line loss	0,5-o,5 dB
Radiated power	EIRP=891,25 W ERP=543,45 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	21	Antena height(m)	3
Transmisión	Rep. Lourdes	Recepción	Ag. San Miguel
Tx Power	0,5012W-27 dBm	Requiered E Field	20,24 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	10 dBi-7,8 dBd
Antena gain	10 bBi-7,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=4,47 W ERP=2,72 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	21	Antena height(m)	4
Transmisión	Rep. Lourdes	Recepción	Sub. Cochabamba
Tx Power	0,1585W-27 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5*9 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB

Radiated power	EIRP=0,71 W ERP=0,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	4
Transmisión	Rep. Lourdes	Recepción	Sub. Wiloloma
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=5,62 W ERP=3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	23,5
Transmisión	Rep. Lourdes	Recepción	Rep. Cuchicagua
Tx Power	0,5012W-27 dBm	Requiered E Field	20,24 dBµV/m
Line loss (dB)	8 dB	Antenna gain	10 dBi-7,8 dBd
Antena gain	10 bBi-7,8 dBd	Line loss	0 dB
Radiated power	EIRP=5,01 W ERP=3,06 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24
Transmisión	Rep. Wiloloma	Recepción	Ag. Balsapamba
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5-0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=6,31 W ERP=3,85 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	23,5	Antena height(m)	15
Transmisión	Rep. Cuchicagua	Recepción	Sub. Sicoto
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=5,62 W ERP=3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	6
Transmisión	Rep. Cuchicagua	Recepción	Ag. Chillanes
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=5,62 W ERP=3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	3
Transmisión	Rep. Cuchicagua	Recepción	Ag. El Tambo
Tx Power	0,3981W-26 dBm	Requiered E Field	3,08 dBµV/m
Line loss (dB)	0,5-0,5 dB	Antenna gain	34 dBi-31,8 dBd
Antena gain	34 bBi-31,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=1 kW ERP= 0,61 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	3
Transmisión	Rep. Piscoquero	Recepción	Ag. Caluma

Tx Power	0,5012W-27 dBm	Requiered E Field	20,24 dBµV/m
Line loss (dB)	0,5-0,5 dB	Antenna gain	10 dBi-7,8 dBd
Antena gain	10 bBi-7,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=4,47 W ERP= 2,72 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	3
Transmisión	Rep. Piscoquero	Recepción	Ag. Echeandia
Tx Power	0,5012W-27 dBm	Requiered E Field	20,24 dBµV/m
Line loss (dB)	0,5-0,5 dB	Antenna gain	10 dBi-7,8 dBd
Antena gain	10 bBi-7,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=4,47 W ERP= 2,72 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	12,5
Transmisión	Rep. Piscoquero	Recepción	Rep. Jerusalen
Tx Power	0,5012W-27 dBm	Requiered E Field	20,24 dBµV/m
Line loss (dB)	0,5-0,5 dB	Antenna gain	10 dBi-7,8 dBd
Antena gain	10 bBi-7,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=5,01 W ERP= 3,06 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	23,5	Antena height(m)	23,5
Transmisión	Rep. Jerusalen	Recepción	Ag. San Luis de Pambi
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=5,62 W ERP= 3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	3
Transmisión	Rep. Jerusalen	Recepción	Ag. Las Naves
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=5,62 W ERP= 3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	3
Transmisión	Rep. Jerusalen	Recepción	Rep. Campanahurco
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5-0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=6,31 W ERP= 3,85 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	21
Transmisión	Rep. Campanahurco	Recepción	Ag Facundo Vela
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5-0,5 dB
Radiated power	EIRP=5,62 W	Rx sensitivity	0,3981µV_-115dBm

	ERP= 3,43 W		
Antena height(m)	24	Antena height(m)	13
Transmisión	Rep. Campanahurco	Recepción	Rep. Pimbalo
Tx Power	0,1585W-22 dBm	Requiered E Field	21,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=5,62 W ERP= 3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24
Transmisión	Rep. Pimbalo	Recepción	Ag. Simiatug
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=5,62 W ERP= 3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	3
Transmisión	Rep. Pimbalo	Recepción	Ag. Simiatug
Tx Power	0,1585W-22 dBm	Requiered E Field	20,7 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-13,8 dBd
Antena gain	16 bBi-13,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=5,62 W ERP= 3,43 W	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	3

Elaborado por: Roberto Usca, 2017

5.4 Procedimiento de configuración del sistema de transmisión de datos MPLS/VPN.

En esta sección se describe cómo configurar el sistema de transmission de datos con un protocol MPLS, con la aplicación de VPN. En el cual se realiza el rediseño de radioenlace de la red de datos de CNEL Regional Bolívar en Radio Mobile con la aplicación de MPLS-VPN, posterior a ello se enlista los equipos necesarios para el rediseño de la red, tambien se realiza el rediseño topografico de la red, se comprueba su estado de configuración y se evalua el trafico de red.

5.4.1 Rediseño de radioenlace de la red de datos de CNEL Regional Bolívar en Radio Mobile con la aplicación de MPLS-VPN.

Para el rediseño de la red CNEL Bolívar se tomó como referencia la experiencia de la red anterior y su respectivo estudio, el programa para realizar el diseño de radioenlace es Radio Mobile. Aunque existen otros softwares, así como SPLAT que brindan prestaciones agregados en el análisis de interferencias, se ha seleccionado usar Radio Mobile por que reúne las aracteristcas de análisis de propagacion, entorno grafico y aceptable fiabilidad que muestra en los resultados. Radio Mobile usa Longley-Rice, o conocido igualmente como Modelo de Terreno Irregular

(ITM), como también modelo de radiopropagación en el rango estimado de frecuencias de 20 MHz a 20GHz.

Para el diseño de los radioenlaces mediante simulación se establece los valores nominales mínimos de la ganancia de cada una de las antenas, potencia en transmisión, sensibilidades de los radios, y de la pérdida de los cables a utilizar y respectivos conectores necesario para su implementación de ser el caso. En base a dichos valores se establecen los requisitos mínimos y máximos para la elección de los equipos y sistemas necesarios que ofrece el mercado.

El diseño de los radioenlaces por medio del software Radio Mobile permite identificar los rangos de la ganancia de cada una las antenas, la pérdida tolerable de la red de las conexiones, y también la potencia mínima de transmisión de datos de los radios en cada enlace de red.

Para iniciar con la simulación se requiere la ubicación de los puntos involucrados en la red, los mismos que se describen en las coordenadas geográficas de la ubicación de las torres para el nuevo diseño para la red CNEL Bolívar en la Tabla 11-5.

Tabla 11-5. Coordenadas geográficas para el nuevo diseño

NOMBRE	LATITUD	LONGITUD
Repetidor2	1°21'12.70"S	78°58'30.50"O
Repetidor3	1°43'27.80"S	78°54'34.50"O
Repetidor MPLS	1°38'4.08"S	78°56'58.97"O
Repetidor MPLS2	1°23'26.60"S	79° 3'49.40"O

Elaborado por: Roberto Usca, 2017

Con esta implementación en la red CNEL BOLÍVAR permite tener mayor redundancia en los enlaces, mayor confiabilidad además de ser propicio para la aplicación de MPLS.

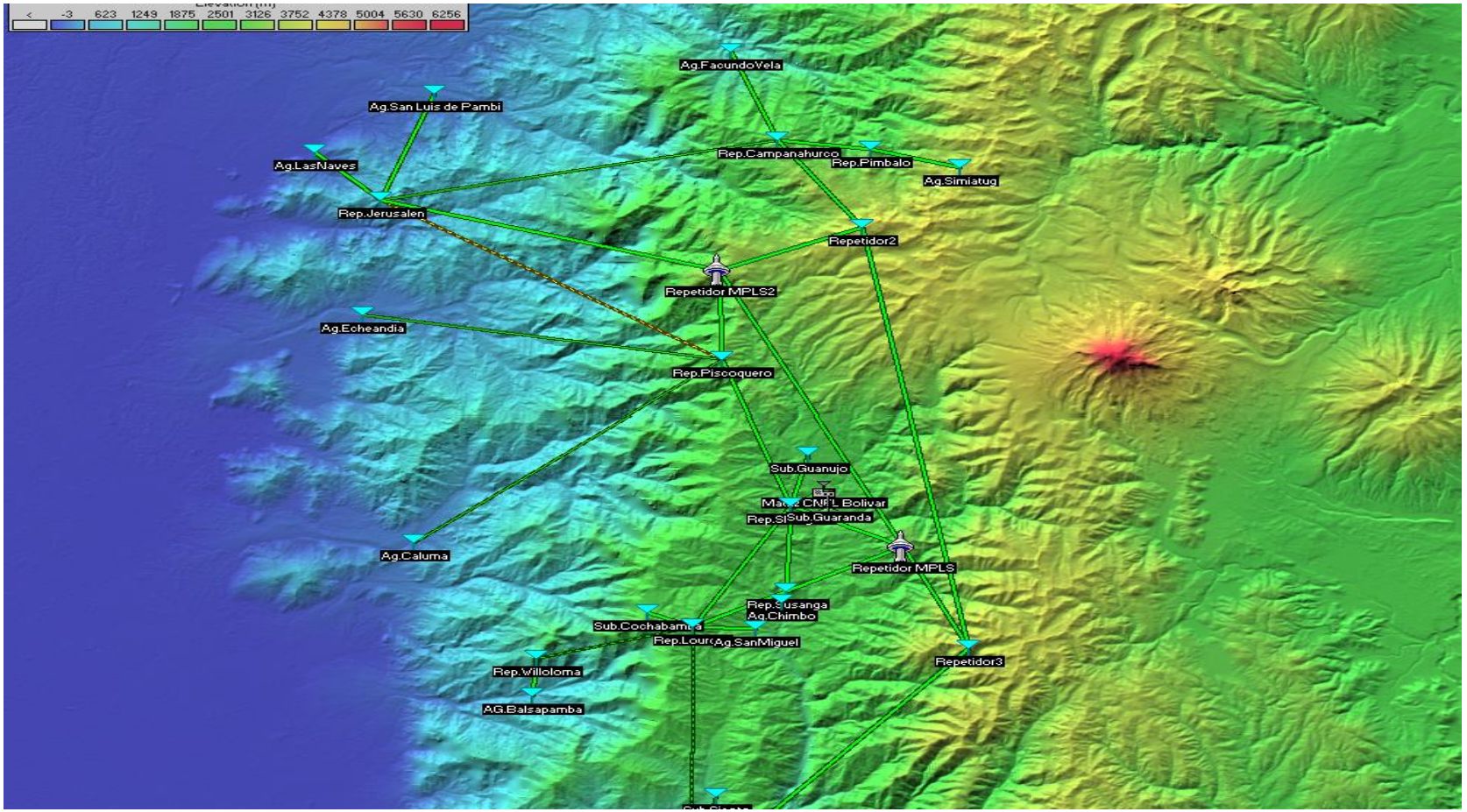


Figura 4-5: Diseño de Enlaces de Radio MPLS/VPN

Elaborado por: Roberto Usca, 2017

Como se muestra en la Figura 4-5 del rediseño de radio enlace de red, se puede especificar que se debe crear nuevos enlaces de red, y sus características se muestran en el Anexo B, el resumen se muestra en la Tabla 12-5.

Tambien se encuentran todos los enlaces de la nueva red trabajando a 5.8Ghz y las alturas de las antenas son de 24m aproximadamente, además de usar equipos electrónicos ProMix por varios aspectos como es su potencia de Tx y su ganancia específicamente lo que permite cubrir largas distancias.

Tabla 12-5: Rediseño de radioenlace de la red CNEL Bolívar

Transmisión	Rep. Campanahurco	Recepción	Repetidor 2
Tx Power	100-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	16 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24
Transmisión	Repetidor 2	Recepción	Repetidor 3
Tx Power	100W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24
Transmisión	Repetidor 3	Recepción	Rep. Cuchicagua
Tx Power	100W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24
Transmisión	Repetidor MPLS	Recepción	Repetidor 3
Tx Power	100W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm

Antena height(m)	24	Antena height(m)	24
Transmisión	Repetidor MPLS	Recepción	Rep. Lourdes
Tx Power	100W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24
Transmisión	Repetidor MPLS	Recepción	Rep. Shunguna
Tx Power	100W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	21
Transmisión	Repetidor MPLS	Recepción	Repetidor MPLS2
Tx Power	100W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24
Transmisión	Repetidor MPLS2	Recepción	Repetidor 2
Tx Power	100W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24
Transmisión	Repetidor MPLS2	Recepción	Rep. Jerusalen
Tx Power	100W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24

Transmisión	Repetidor MPLS2	Recepción	Rep. Piscoquero
Tx Power	100W-50 dBm	Requiered E Field	7,2 dBµV/m
Line loss (dB)	0,5 dB	Antenna gain	30 dBi-27,8 dBd
Antena gain	30 bBi-27,8 dBd	Line loss	0,5 dB
Radiated power	EIRP=89,13 kW ERP= 54,34 kW	Rx sensitivity	0,3981µV_-115dBm
Antena height(m)	24	Antena height(m)	24

Elaborado por: Roberto Usca, 2017

5.4.2 Equipos de radioenlace para aplicar MPLS-VPN

Los equipos necesarios para realizar el radio enlace de los repetidores implementados denominados repetidores dos y tres, para MPLS y MPLS2, la cantidad de los equipos se realiza en base al rediseño del radioenlace, la cantidad de equipos según la necesidad de antenas para una nueva comunicación de radioenlace e implementación del protocolo MPLS los cuales se detallan en la Tabla 13-5:

Tabla 13-5. Requerimientos de equipos para MPLS

Cantidad	Equipo	Marca	Modelo
20	Antena parabólica 5,8 Ghz	HYPERLINK	HG4958DP-30D
16	Protectores de cable	MOTOROLA	600SS
20	Fuentes POE	PROXIM	48G
4	Conexión a tierra		
16	Patch cord 3pies	LEVITON	
8	Baterías	BLESS POWER	6FM100E-X
4	Torre 24m		
26	Routers	CISCO	C2901-srst/k9

Elaborado por: Roberto Usca, 2017

5.4.3 Rediseño de la red de datos de CNEL Regional Bolívar en GNS3.

Las siguientes figuras muestran el esquema de la red CNEL Regional Bolívar y luego respectivamente su configuración y equipos utilizados. En la red CNEL Regional Bolívar se establece el sentido de los enlaces de la transmisión y recepción de datos proporcionalmente. A continuación, se presenta la propuesta de diseño de red.

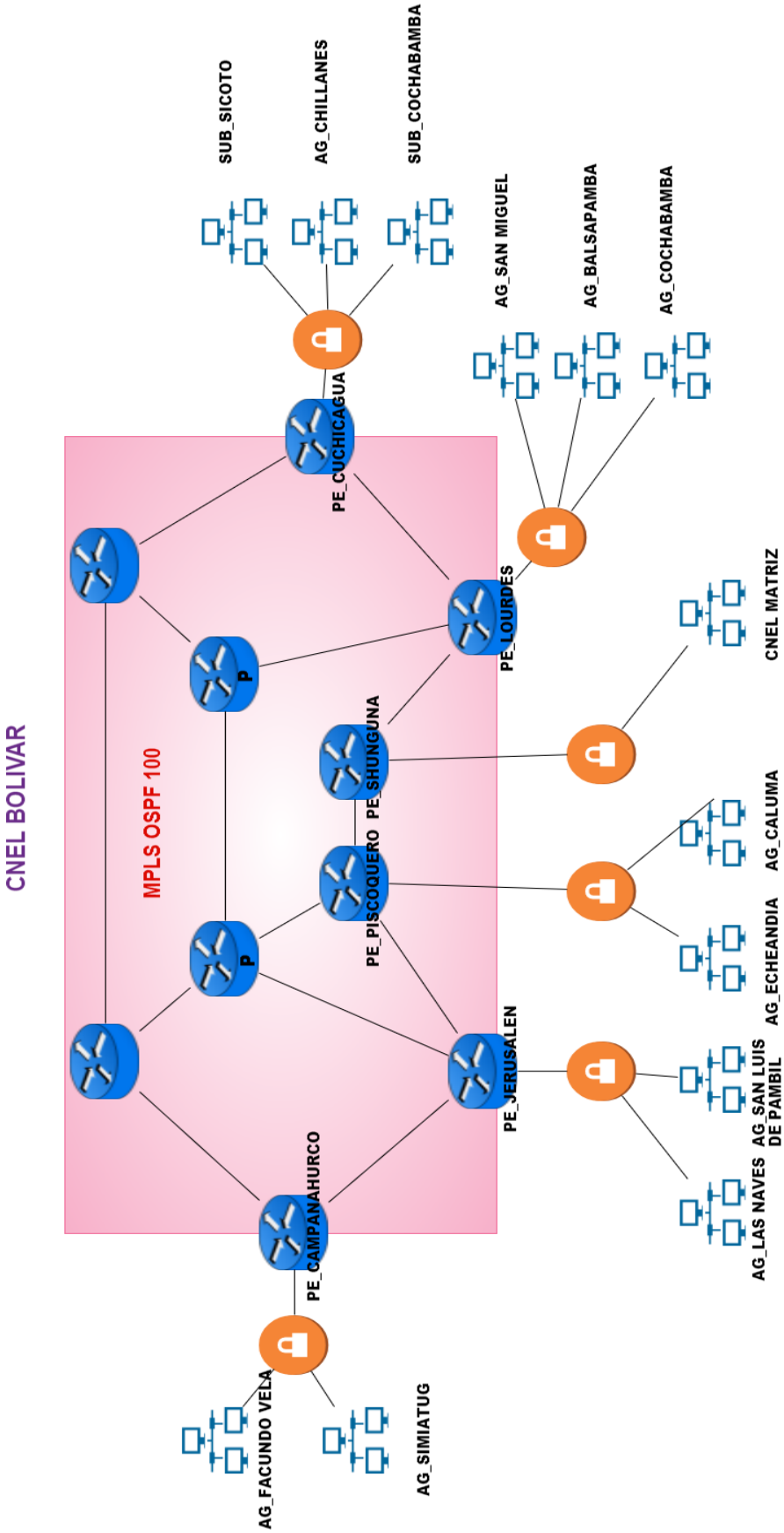


Figura 5-5: Diseño de red con protocolo MPLS
Elaborado por: Roberto Usca, 2017

En el diseño de red de la Figura 5-5, se nota que está compuesto por redundancia de enlaces lo que permite que la red sea robusta en contra de fallos o caídas de enlaces, si un enlace falla o toma otro sentido para evitar que se paralicen los servicios de CNEL, además está configurado MPLS con la aplicación de VPN para darle mayor velocidad en la conmutación de paquetes y seguridad al acceder a la información.

Puesto que en una red no se maneja equipos de un solo fabricante, sino que la mayoría usan una mezcla de varios equipos, el protocolo de enrutamiento que se maneja por este motivo es OSPF un protocolo genérico que está presente en la mayoría de equipos de diferentes fabricantes.

Para realizar el rediseño y configurar la red se ha utilizado GNS3 que es un simulador de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Para permitir completar simulaciones, GNS3 está estrechamente vinculada con: Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios IOS de Cisco System. El esquema se muestra en la Figura 6-5.

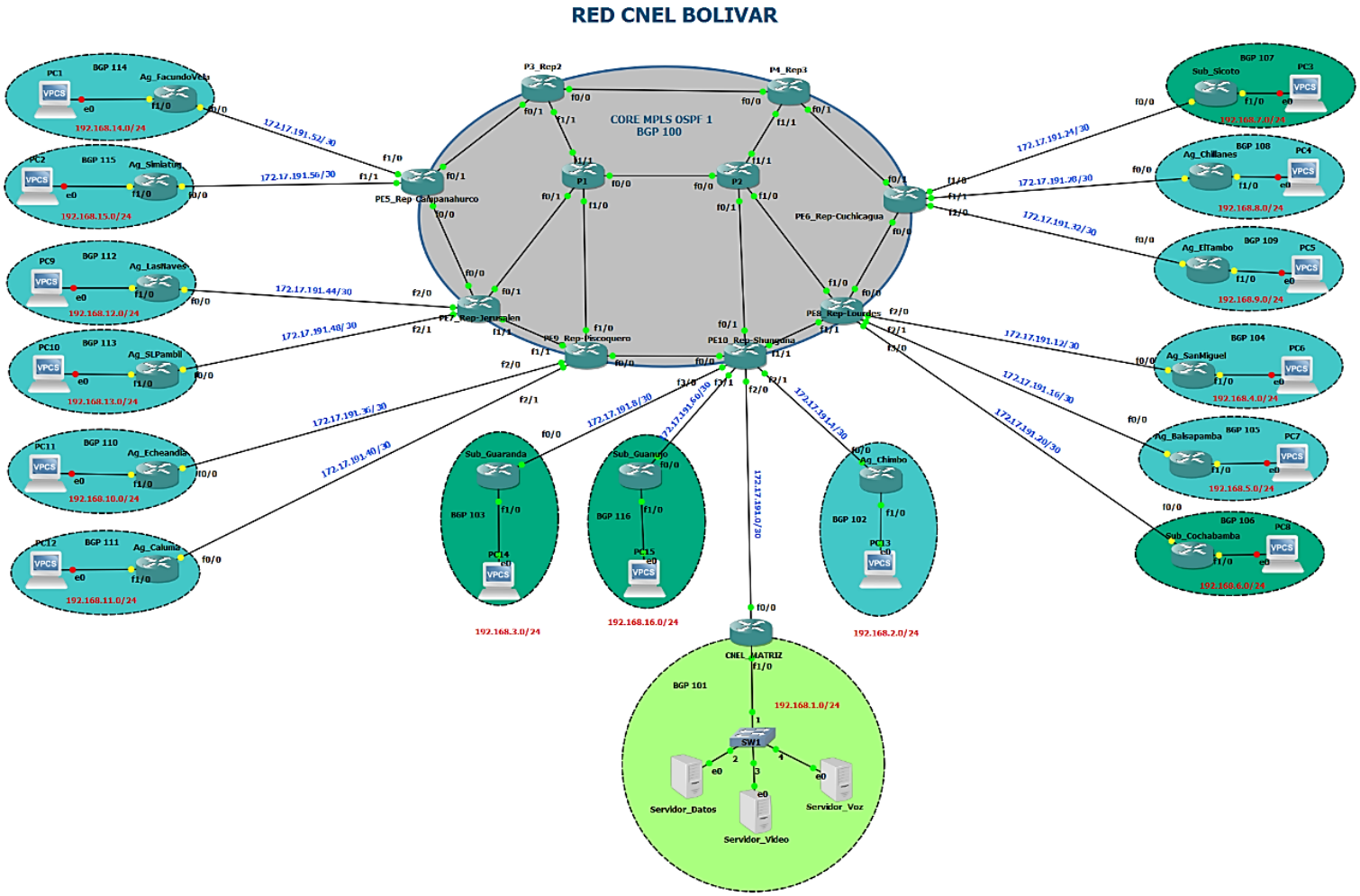


Figura 6-5: Topologia de red MPLS/VPN

Elaborado por: Roberto Usca, 2017

Este es el diseño de red con MPLS y VPN que permiten la interconectividad en CNEL de Bolívar, que brindara seguridad y confiabilidad a los servicios de la Empresa Eléctrica.

El Direccionamiento de la red se identifica en el Anexo D, así como el esquema de configuración de la implementación del protocolo MPLS, se presenta en el Anexo E.

5.4.4 Comprobación del estado de configuración de VPN de algunas agencias de CNEL

De acuerdo a la teoria de MPLS, en las Figuras 7-5 y 8-5 se determina los label o etiquetas que se asignan por lo provider y se distribuyen mediante LDP, esto permite saber que PATH o camino toma el paquete desde el origen hacie el destino.

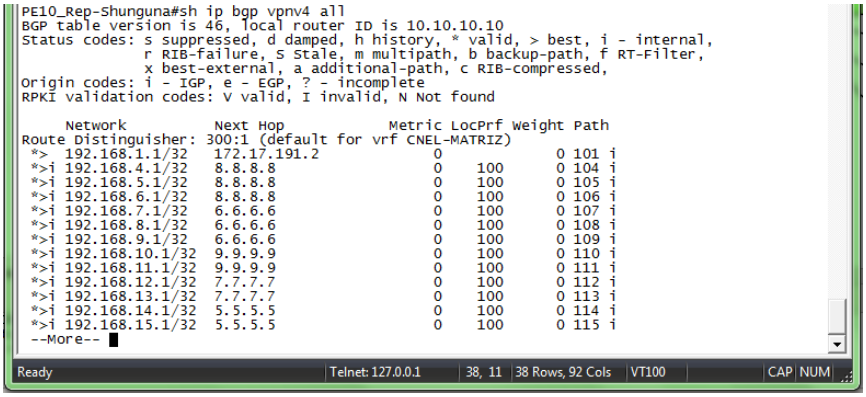


Figura 7-5: Estado de configuracion de red
Elaborado por: Roberto Usca, 2017

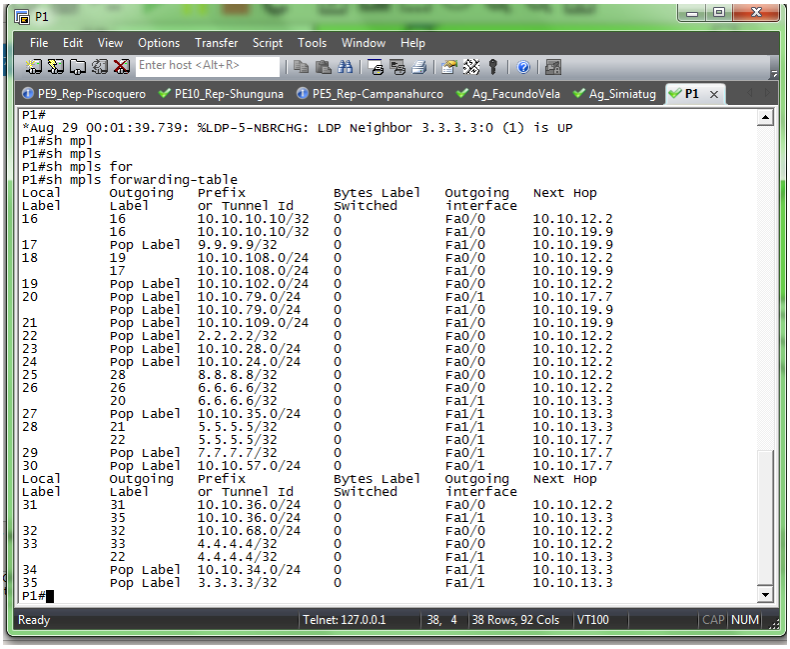


Figura 8-5: Verificacion de la configuracion de MPLS sobre el core
Elaborado por: Roberto Usca, 2017

Para medir el desempeño de la red se ha planteado un escenario con MPLS-VPN y uno que solo ejecute un protocolo de enrutamiento para ver sus diferencias y demostrar el beneficio y las prestaciones del protocolo MPLS. Como se muestra en la Figura 9-5.

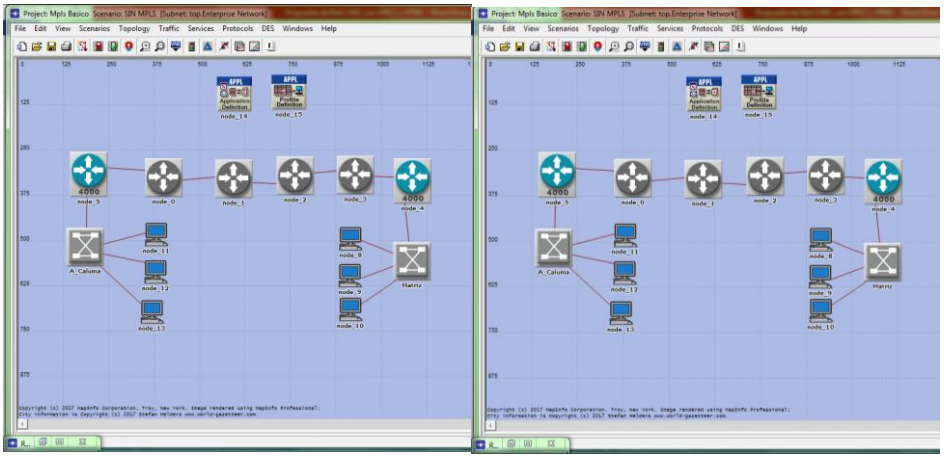


Figura 9-5: Escenarios de desempeño de la red
Elaborado por: Roberto Usca, 2017

5.4.5 Análisis de Trafico con Wireshark

A continuación, se presenta gráficamente cómo se comporta cada protocolo en la red CNEL BOLÍVAR, para estas pruebas se realizó un ping extendido desde las diferentes agencias hacia los servidores durante un lapso de tiempo de 22 minutos, debido a que e el tiempo recomendado para el análisis del tráfico de red. En los Gráficos 1-5 y 2-5, se muestra cómo se comporta las diferentes solicitudes hacia los servidores y como estos responden, mientras que en los Gráficos 5.3 y 5.4, se muestra como los diferentes protocolos se levantan y el tráfico que genera.

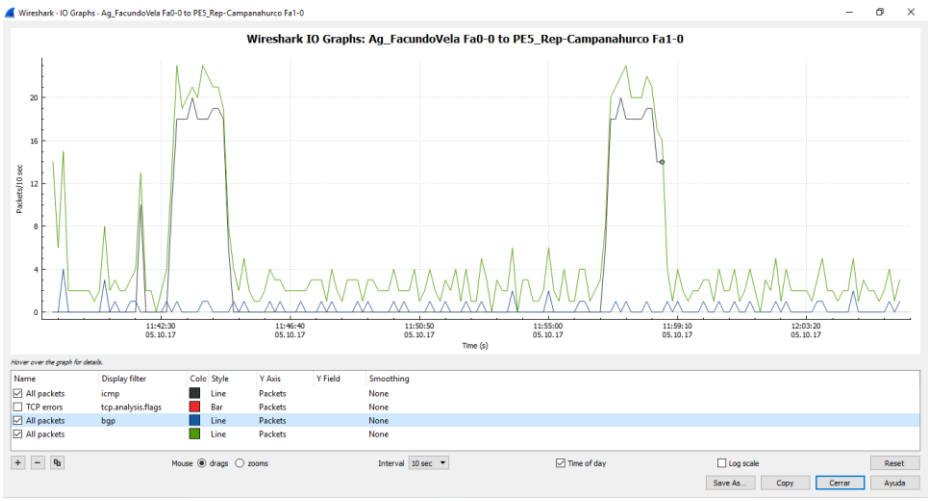


Gráfico 1-5: Tráfico de Datos, Voz, Video
Elaborado por: Roberto Usca, 2017

La representación de tráfico muestra cómo se comporta las solicitudes hacia los servidores desde la agencia Facundo Vela, indistintamente se procedió hacer un ping extendido a las direcciones, 192.168.1.1 que es la puerta de enlace de los servidores y a los servidores propiamente dicho 192.168.1.2-4 (servidores voz, datos y video). En el trafico tal generado en el enlace está incluido el tráfico generado por el protocolo BGP como se ve es mínimo a comparación del tráfico generado por parte de clientes hacia los servidores.

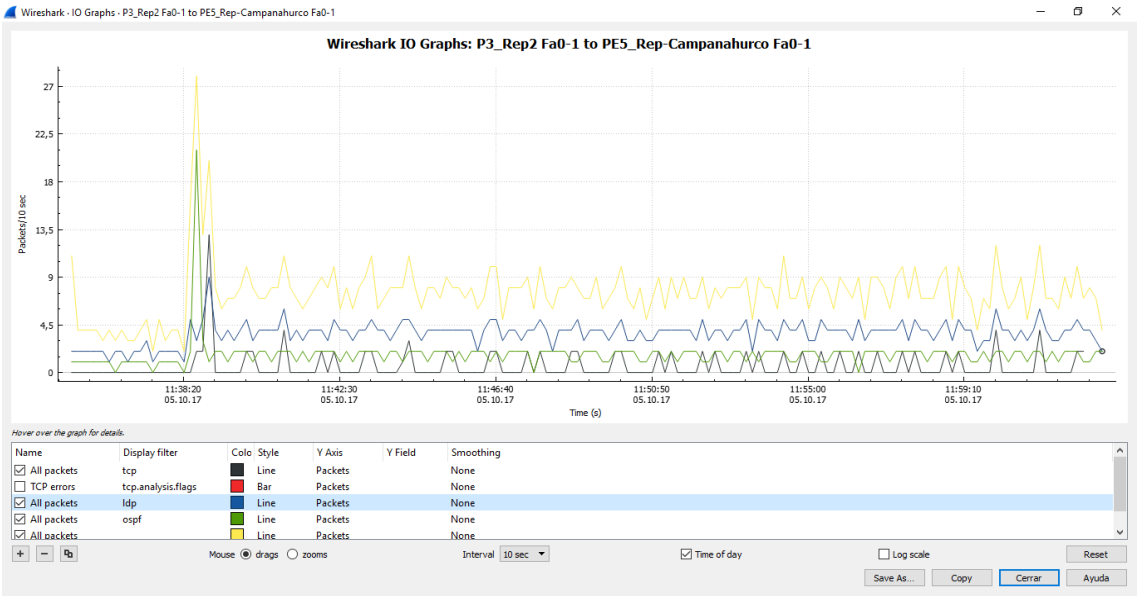


Gráfico 2-5: Protocolos OSPF, MPLS
Elaborado por: Roberto Usca, 2017

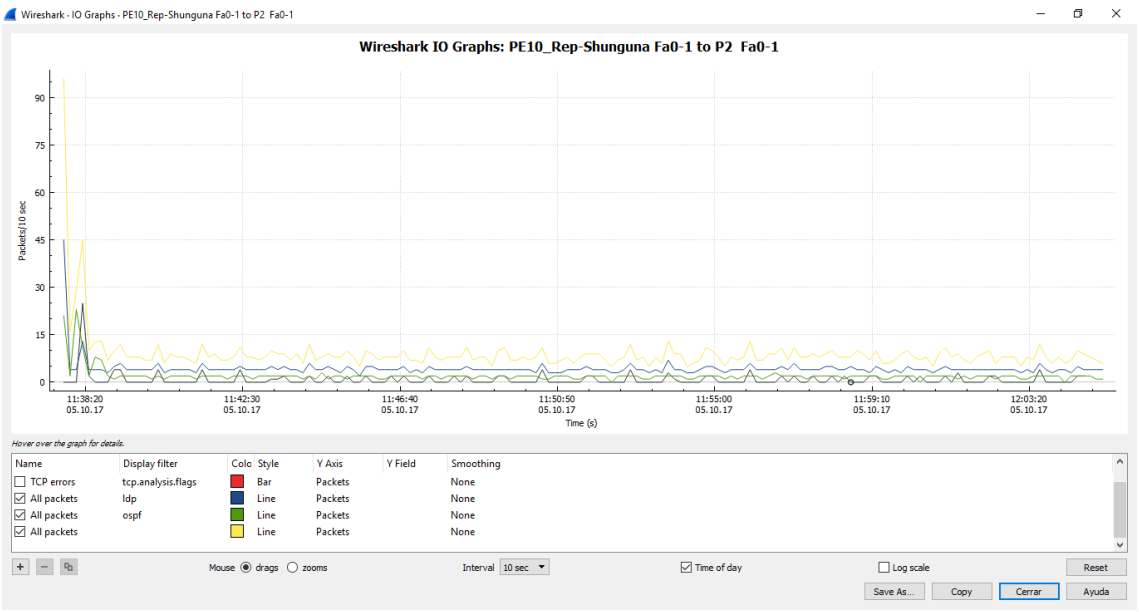


Gráfico 3-5: Protocolos OSPF, MPLS
Elaborado por: Roberto Usca, 2017

En los Gráficos 3-5 y 4-5 se presenta en mayor ponderación, los protocolos de enrutamiento en el core de MPLS, se verifica el tráfico total generado tanto por OSPF, BGP y MPLS, es notable que en los primeros minutos genera más tráfico que en el resto de tiempo, ya en primera instancia busca la ruta más corta por el protocolo OSPF, se genera el saludo de tres vías por parte del protocolo BGP para el intercambio de tablas de enrutamiento, y la distribución de etiquetas (ldp) por parte del protocolo que corre bajo MPLS,

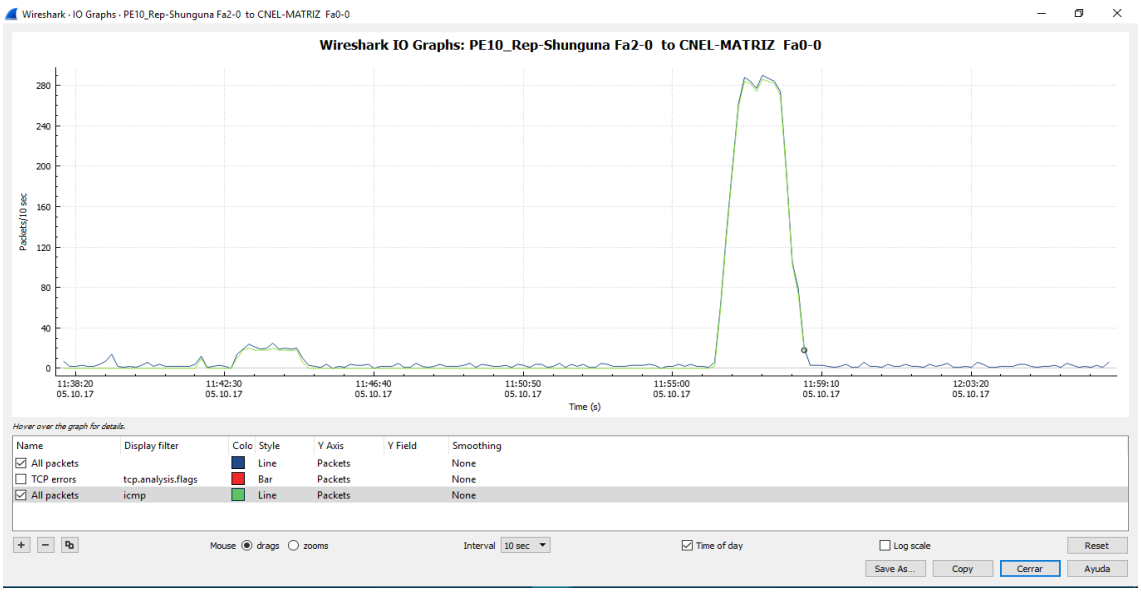


Gráfico 4-5: Tráfico en Servidores
Elaborado por: Roberto Usca, 2017

5.5 Identificación de parámetros de rendimiento del sistema de transmisión de datos.

A continuación, se realiza la comparación de los dos escenarios con medidas del “delay”, nivel de utilización del enlace y “throughput”. Los resultados se determinan con la utilización de GNS3 y la configuración de la topología de red propuesta.

Para cada una de las observaciones de los experimentos a realizarse se plantea un respectivo escenario.

- ✓ Para la observación 1, se analizó tres agencias accediendo a todos los servicios de voz, datos y video con carga baja a los servidores.
- ✓ Observación 2, se analizó tres agencias accediendo a todos los servicios de voz, datos y video con carga media a los servidores.
- ✓ Observación 3, se analizó tres agencias accediendo a todos los servicios de voz, datos y video con carga alta a los servidores.

- ✓ Observación 4, se analizó completamente la red con todas las agencias y subestaciones accediendo simultáneamente a los servicios de voz, datos y video con una carga baja a los servidores.

- ✓ Observación 5, se analizó completamente la red con todas las agencias y subestaciones accediendo simultáneamente a los servicios de voz, datos y video con una carga media a los servidores.

- ✓ Observación 6, se analizó completamente la red con todas las agencias y subestaciones accediendo simultáneamente a los servicios de voz, datos y video con una carga alta a los servidores.

A continuación, a partir de la Tabla 14-5, se presenta el resumen de la evaluación del rendimiento de red.

Tabla 14-5: Resumen de medición del rendimiento actual

	O. 1	**O. 2**	**O. 3**	**O. 4**	**O. 5**	**O. 6**
JITTER	0 s	3 ns	18 ns	2 ns	6ns	36 ns
LATENCIA	0.66 ms	6.4 ms	47 ms	8 ms	11.5 ms	0.09 s
THOGHPUT	28 bits/s	358 bits/s	24.7 kbits/s	800 bits/s	5.38 kbits/s	97 kbits/s
% DE UTILIZACIÓN	0.000028	0.00037	0.23	0.00038	0.00049	0.0128

Elaborado por: Roberto Usca, 2017

Tabla 15-5: Resumen de la medición del rendimiento propuesta MPLS

	O. 1	**O. 2**	**O. 3**	**O. 4**	**O. 5**	**O. 6**
JITTER	0 s	0 s	0 s	0.6 ns	3 ns	30 ns
LATENCIA	0.64 ms	6.3 ms	45 ms	7 ms	7 ms	0.5 s
THOGHPUT	360 bits/s	1.2 kbits/s	25 kbits/s	1.38 kbist/s	4.9 kbits/s	138 kbits/s
% DE UTILIZACIÓN	0.00036	0.0012	0.25	0.008	0.050	0.9

Elaborado por: Roberto Usca, 2017

5.6 Medición y comparación de resultados

5.6.1 Caraceristicas de la red con protocolo MPLS y sin MPLS

Como se muestra en el Gráfico 5-5, en color rojo se verifica la curva que presenta el delay SIN MPLS, y en azul el delay CON MPLS. Como se puede apreciar gráficamente se nota que MPLS mejora el rendimiento de la red. Se expresa gráficamente a continuación:

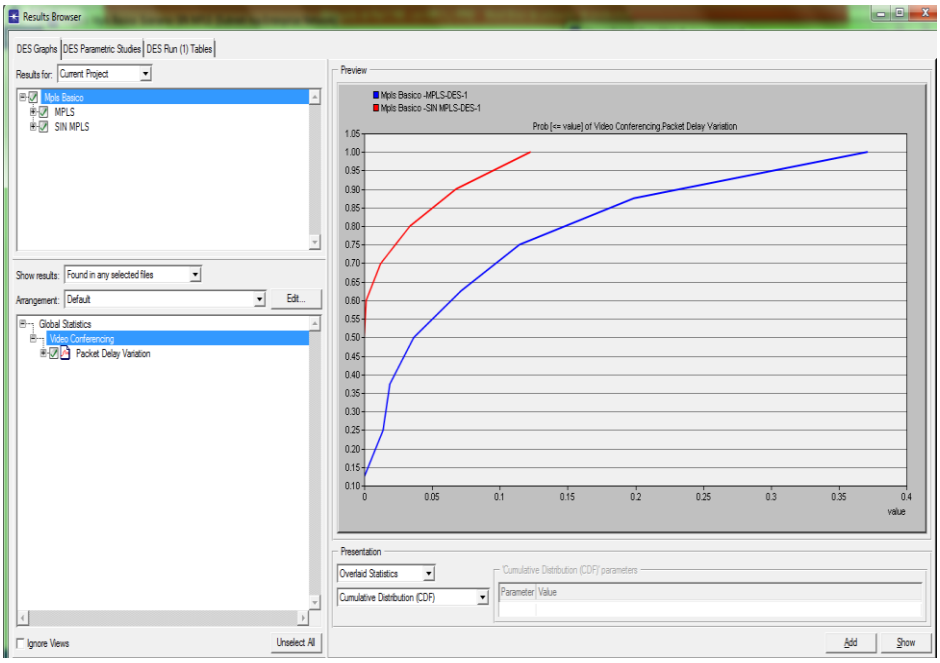


Gráfico 5-5: Delay comparativo de protocolo MPLS
Elaborado por: Roberto Usca, 2017

Analizando dentro del CORE, con el protocolo MPLS, simplemente se hace la conmutación de paquetes en función de etiquetas a comparación del uso de un protocolo de enrutamiento como es OSPF que para poder conmutar un paquete debe buscar en su tabla de enrutamiento para poder conmutar correctamente y enviar el paquete a su destino, la utilización de la red con sin MPLS es mayor se evidencia en la línea de color rojo de el Gráfico 5-6.

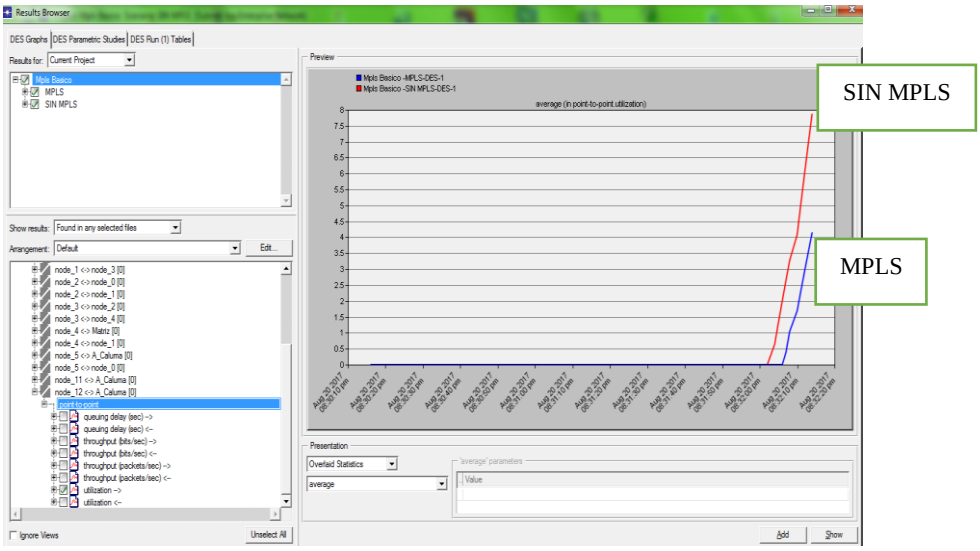


Gráfico 5-6: Utilización del enlace
Elaborado por: Roberto Usca, 2017

Lo mismo sucede con el throughput este nivel es menor en un entorno con MPLS, demuestra la línea azul. A comparación de un entorno sin MPLS que es muy alto. Como se verifica en el Gráfico 5-7.

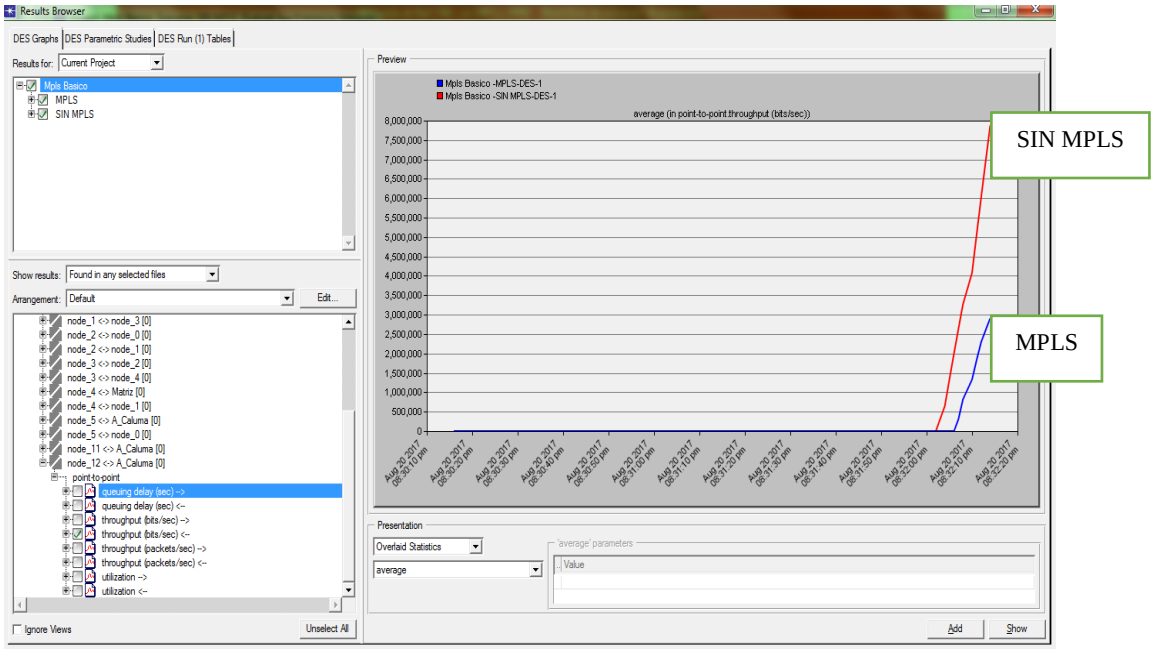


Gráfico 5-7: Comparación throughput con MPLS/sin MPLS
Elaborado por: Roberto Usca, 2017

En el diseño planteado es una mezcla de varios protocolos como son IGP, BGP, VRF Y VPNL3. Todos estos protocolos se juntan para mejorar el desempeño de red y lo más importante optimizar recursos de red además de brindarle seguridad.

Al hablar de redundancia de red se asegura la confiabilidad de red asegurar que los servicios de red no se caigan para eso se necesita monitorizar la red en todo momento para eso el uso de "CACTI" y "THE DUDE". Las políticas de seguridad son importantes porque evitan ataques informáticos internos y externos como es ataques DDOS, FISHING, MITM, entre otros.

Con estos resultados determinamos que la red propuesta de CNEL Bolívar con MPLS-VPN mejora el rendimiento de la red además de brindar seguridad al aplicar VPN-L3, la naturaleza de las VPN es una conexión punto a punto creando un túnel de tráfico dedicado, por lo cual se asegura servicios, un manejo del tráfico generado por aplicaciones y clientes; y mayor control de esta red.

5.6.2 Análisis evolutivo de la red

Para evaluar el aspecto evolutivo de los cambios de los ultimos años y comprobar el aporte del protocolo MPLS, se analiza en función del rendimiento de la red. Evidenciando la tabulacion de los datos en la Tabla 16-5.

Tabla 16-5: Resumen del rendimiento de red actual y con el protocolo MPLS.

JITTER	Actual	10,8333333	ns
LATENCIA	Actual	12,260015	ms
THOGHPUT	Actual	21,3776667	kbits/s
% DE UTILIZACION	Actual	0,040678	
JITTER	MPLS/VPN	5,6	ns
LATENCIA	MPLS/VPN	10,9900833	ms
THOGHPUT	MPLS/VPN	28,4733333	kbits/s
% DE UTILIZACION	MPLS/VPN	0,20159333	

Elaborado por: Roberto Usca, 2017

Asi el jitter se define como la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino, se puede notar que con la implementación del protocolo MPLS/VPN se reduce significativamente la congestión de la red, por ende es sistemas de transmisión de datos es mas eficiente con la utilización del protocolo MPLS.

Marco comparativo de latencia se identifica en el Gráfico 8-5.

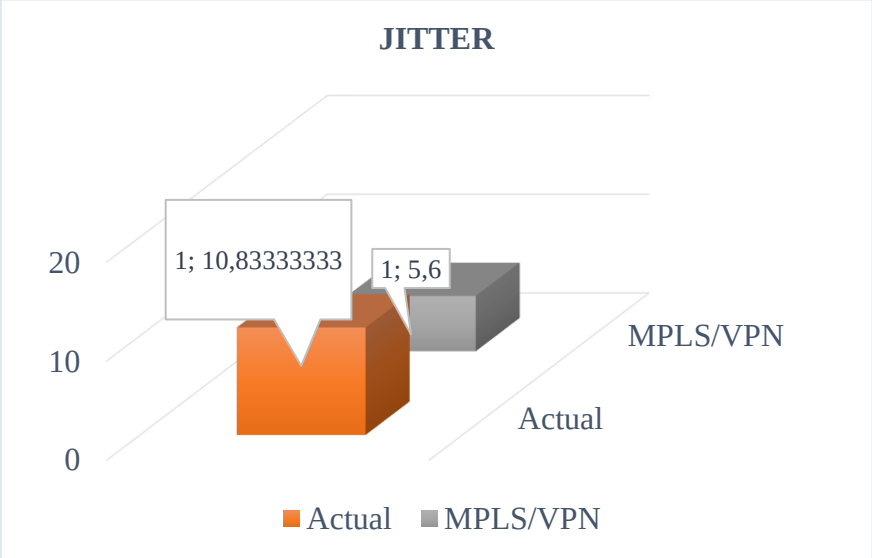


Gráfico 8-5: Análisis evolutivo jitter

Elaborado por: Roberto Usca, 2017

A la latencia se le conoce también como retardo, por ende, en el análisis comparativo de latencia se puede evidenciar que el retardo en la transmisión de datos en la red MPLS/VPN es mucho menor que en los utilizados actualmente por ende es útil y satisfactorio la utilización del protocolo

MPLS en la red CNEL Bolívar. La comparación de Latencia se puede evidenciar en el Gráfico 9-5.

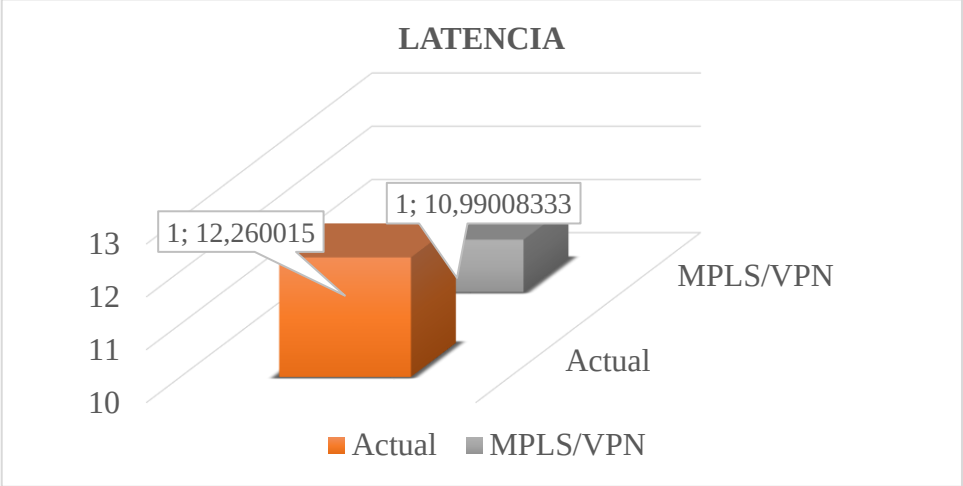


Gráfico 9-5: Análisis evolutivo de latencia
Elaborado por: Roberto Usca, 2017

En el gráfico 10-5 el throughput es definido como la velocidad real de transporte de datos a través de una red telemática, por ende se puede analizar que la comparación del throughput de la red actual y la propuesta de implementación de protocolo MPLS/VPN se incrementa significativamente la velocidad real de la transmision de datos y se demuestra que la propuesta es realativamente eficiente.

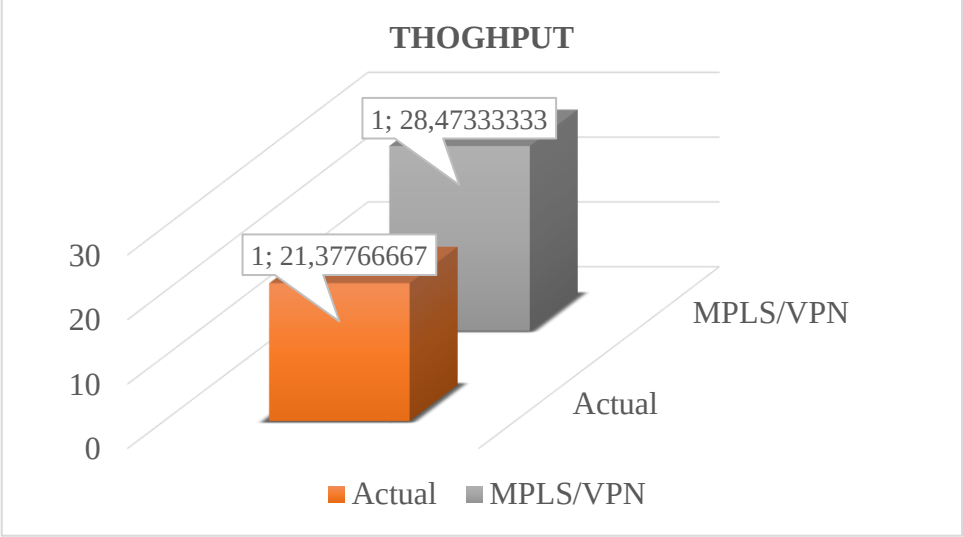


Gráfico 10-5: Analisis evolutivo thoghput
Elaborado por: Roberto Usca, 2017

El Gráfico 11-5 demuestra que en los datos de MPLS se nota favorablemente el rendimiento de la red, por la explicación en la teoría de MPLS y su conmutación de paquetes permite que la red sea más rápida y segura en los delay de red, obviamente el porcentaje de utilización de enlaces es mayor en la red cuando se aplica MPLS puesto que aparte de la información que se transmite

también se envía paquetes ldp, ello, etc., que hace que el nivel de utilización del enlace suba, esos porcentajes son mínimos, pero no despreciables.

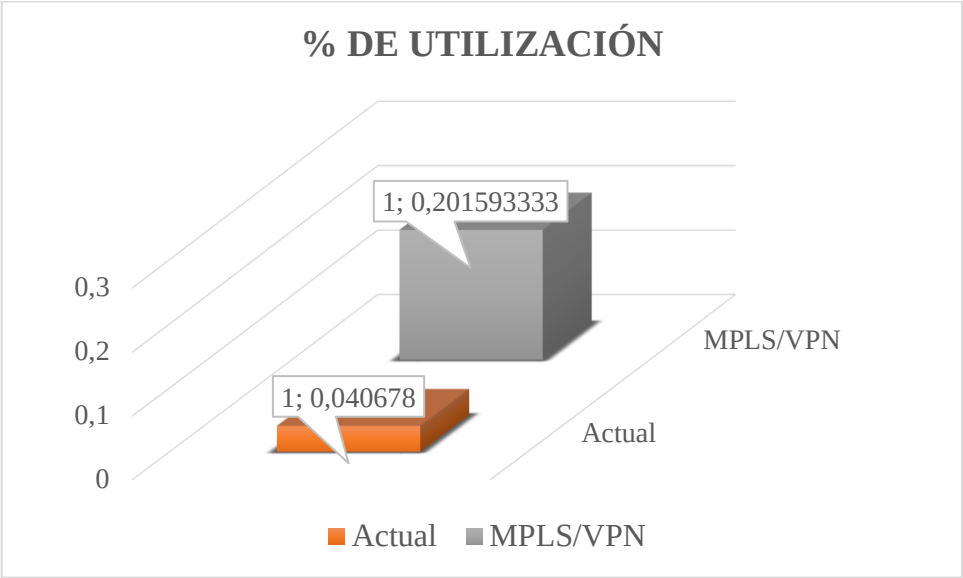


Gráfico 11-5: Analisis evolutivo del porcentaje de utilizacion de red.
Elaborado por: Roberto Usca, 2017

5.7 Análisis de la influencia del protocolo MPLS/VPN en el rendimiento de la red

Para el análisis de los resultados de la evaluación del rendimiento de la implementación del Protocolo MPLS con la aplicación de VPN, de CNEL Regional Bolívar, en lo relacionado con la seguridad de transmisión de información, se ha procedido en la presente investigación a aplicar un diseño experimental de la evaluación del rendimiento del protocolo MPLS a la entidad matriz y las sucursales correspondientes. El resultado obtenido en la mencionada experimentación se presenta en un cuadro en el cual se realiza la validación de sus datos mediante un diseño experimental completamente al azar, para posteriormente realizar un análisis e interpretación de los datos que este contiene.

Los principios estadísticos son los agrupados con la recolección de aquellas observaciones que provean la mayor cantidad de información para el estudio de investigación de forma eficiente, la misma que incluye el diseño de tratamientos, el control local de la variabilidad, el número de réplicas, la aleatorización y la eficiencia de los experimentos realizados.

La réplica de un experimento proporciona los suficientes datos para estimar la varianza del error experimental. La bloquización facilita un medio para reducir el error experimental (Kuehl, 2001, pág. 21).

Fisher (1926) señaló que la “aleatorización proporciona estimaciones válidas de la varianza del error para los métodos de inferencia estadística justificados para la estimación y pruebas de

hipótesis en el experimento. La aleatorización es la asignación aleatoria de tratamientos a las unidades experimentales".

5.7.1 Numero de observaciones en la investigación

La rigurosidad del experimento y la representatividad de las pruebas en una investigación, están claramente asociadas, no sólo con la calidad, de la misma manera con la cantidad de observaciones que deben realizarse, con el total de muestras que debe ser tomado o con el número de repeticiones que debe efectuarse para recopilar y confrontar la información que puede falsar la hipótesis nula y ratificar el planteamiento o hipótesis del investigador. Contandriopoulos, ed. al (1991)

Para determinar el número mínimo de muestras, observaciones o réplicas que deben efectuarse en el presente estudio se calcula con la siguiente formula:

$$n = \frac{W - W^2 * Z_\beta + 1.4{Z_\alpha}^2}{W^2} \qquad (1)$$

Donde:

n = Número mínimo de muestras, observaciones o réplicas que deben efectuarse en el estudio.

*Z*α = Valor correspondiente al nivel de confianza asignado (Riesgo de cometer un error tipo I).

*Z*β = Valor correspondiente al poder estadístico o potencia asignada a la prueba (Riesgo de cometer un error tipo II).

W = Rendimiento mínimo esperado, eficiencia mínima esperada o diferencia mínima observable.

Se plantea que los resultados del experimento deben tener una significación (α) de 0,05 (5%) que corresponde a un nivel de confianza (1-α) del 95% (0.95). En la Tabla 1, (anexo C), se observa que, para este nivel de confianza, Zα tiene un valor de 1,96.

También, en la Tabla 2 (Anexo C), para un valor estadístico β igual a 0,10 (90%), existe un Zβ de 1,282. El rendimiento mínimo que se espera (W) es del 30%; es decir, se espera una remoción mínima de 30% respecto a los resultados del rendimiento de la red de la Corporación Nacional de Electricidad Regional Bolívar.

.

Datos:

*Z*α = 1,96

$Z\beta = 1{,}282$

W = 30%(0,3)

$$n = \frac{W - W^2 * Z_\beta + 1.4{Z_\alpha}^2}{W^2} \qquad (1)$$

$$n = \frac{0{,}3 - 0{,}3^2 * (1{,}282) + 1.4(1{,}96)^2}{0{,}3^2}$$

$$n = \frac{0{,}3 - 0{,}12 + 5{,}38}{0{,}9}$$

$$n = 6{,}18$$

El número de observaciones experimentales que se solicitan realizar de acuerdo al riesgo de error y rendimiento esperado es de 6 observaciones por cada tratamiento es decir por cada escenario planteado.

Debido a la congestión de datos de la Corporación Electrica Regional de Bolivar; con un diseño totalmente aleatorizado, este se puede utilizar porque existe homogeneidad entre las unidades experimentales, los datos se analizan en base al rendimiento de la red que se evidencia en la Tabla 16-5.

Tabla 16-5: Resumen de la medición del rendimiento propuesta MPLS

	O. 1	**O. 2**	**O. 3**	**O. 4**	**O. 5**	**O. 6**
JITTER	0 s	0 s	0 s	0.6 ns	3 ns	30 ns
LATENCIA	0.64 ms	6.3 ms	45 ms	7 ms	7 ms	0.5 s
THOGHPUT	360 bits/s	1.2 kbits/s	25 kbits/s	1.38 kbist/s	4.9 kbits/s	138 kbits/s
% DE UTILIZACIÓN	0.00036	0.0012	0.25	0.008	0.050	0.9

Elaborado por: Roberto Usca, 2017

Para la verificación de la Hipótesis planteada en la presente investigación se utiliza la prueba de bloques aleatorizados, de la teoría estadística, se sabe que las sumas de los cuadrados de variables aleatorias con distribución normal se relacionan con la distribución F de Fisher. (F) para el 95.00% de confianza, con un 5% de error de muestreo y con GL= (n-1) grados de libertad, dependiendo ello de los tratamientos o de los bloques.

En el presente caso para la verificación de la influencia del protocolo MPLS en el rendimiento de la red de la Corporación Nacional de Electricidad de Bolívar es necesario identificar que si el valor de (Fc) calculado es igual o mayor a (FT) tabulado, se acepta la influencia del protocolo MPLS en el rendimiento de la red, y los datos analizados demuestran validéz.

5.7.2 Comprobación de datos

En un diseño de bloques completamente al azar se presenta el siguiente modelo estadístico:

$$y_e = \mu + r_i + B_j + e_{ij} \begin{cases} i = 1,2,\dots,a \\ j = 1,2,..b \end{cases} \qquad (2)$$

Donde: μ: Media global

r_i: Efecto del tratamiento

B_j: Efecto del boque

e_{ij}: Termino del error

El modelo de comprobación de Hipótesis por un diseño de bloques completamente aleatorizados se resume en la Tabla 17-5:

Tabla 17-5: Modelo de diseño de bloques completamente aleatorizados

Fuente de variación	**Suma de cuadrados**	**Grados de libertad**	**Cuadrado medio (MS)**	F_0
Tratamientos	$SS_{Tratamientos}$	n_T-1	$\frac{SS_{Tratamientos}}{n_T - 1}$	$\frac{MS_{Tratamientos}}{MS_E}$
Bloques	$SS_{Bloques}$	n_B-1	$\frac{SS_{Bloques}}{n_B - 1}$	
Error	SS_E	$(n_T$-1)(n_B-1)	$\frac{SS_E}{(n_T - 1)(\, n_B - 1)}$	
Total	SS_T	N-1		

Fuente: (Montgomery, 2004)

Las fórmulas para el respectivo cálculo de suma de cuadrados y cuadrado medio se muestran a continuación:

Suma de cuadrados del tratamiento

$$SS_T = \sum_{i=1}^{a}\sum_{j=1}^{b} {Y_{ij}}^2 - \frac{y^2}{N} \qquad (3)$$

$$SS_{Tratamiwntos} = \frac{1}{b}\sum_{i=1}^{a} {Y_i}^2 - \frac{y^2}{N} \qquad (4)$$

$$SS_{Bloques} = \frac{1}{a}\sum_{j=1}^{b} {Y_j}^2 - \frac{y^2}{N} \qquad (5)$$

$$SS_E = SS_T - SS_{Tratamiento} - SS_{Bloques} \qquad (6)$$

Los experimentos realizados de la situación actual y el protocolo MPLS se consideran en la tabla 18-5.

Tabla 18-5: Resultados de experimentos realizados con la implementación de MPLS(C) y sin la implementación MPLS (S/N)

	O.1		O.2		O.3		O.4		O.5		O.6	
	C	S/N	C	S/N	C	S/N	C	S/N	C	S/N	C	S/N
1		0		3		18		2		6		36
	0		0		0		0,6		3		30	36
2		0,66		6,4		47		8		11,5		0,00009
	0,64		6,3		45		7		7		0,0005	
3		0,028		0,358		24,7		0,8		5,38		97
	0,36		1,2		25		1,38		4,9		138	
4		0,000028		0,00057		0,23		0,00038		0,00049		0,0128
	0,00036		0,0012		0,25		0,08		0,05		0,9	

Elaborado por: Roberto Usca, 2017

Tabla 19-5: Resumen de observaciones experimentales Tratamientos Vs Bloques

		Bloques						
Tratamiento		1	2	3	4	5	6	$\sum T$
	1	0	1,5	9	1,3	4,5	33	49,3
	2	0,65	6,35	46	7,5	9,25	0,000295	69,750295
	3	0,194	1,558	24,85	1,09	5,14	117,5	150,332
	4	0,000194	0,000785	0,24	0,00419	0,02525	0,4564	0,723048
$\sum B$		0,844194	9,408785	80,09	9,890419	18,91525	150,956695	270,105343

Elaborado por: Roberto Usca, 2017

- Sumatoria de los cuadrados totales

$$SS_T = \sum_{i=1}^{a}\sum_{j=1}^{b} {Y_{ij}}^2 - \frac{y^2}{N}$$

$$SS_T = 17946{,}86 - \frac{(270{,}11)^2}{48}$$

$$SS_T = 17946{,}86 - 1519{,}99$$

$$SS_T = 16426{,}87$$

- Sumatoria de los cuadrados de los tratamientos

$$SS_{Tratamiwntos} = \frac{1}{b}\sum_{i=1}^{a} {Y_i}^2 - \frac{y^2}{N}$$

$$SS_{Tratamiwntos} = \frac{1}{4}(49{,}3^2 + 69{,}75^2 + 150{,}33^2 + 0{,}723^2) - 1519{,}99$$

$$SS_{Tratamiwntos} = 5953{,}81$$

- Sumatoria de los cuadrados de los bloques

$$SS_{Bloques} = \frac{1}{a}\sum_{j=1}^{b} {Y_j}^2 - \frac{y^2}{N}$$

$$SS_{Bloques} = \frac{1}{6}(0{,}844^2 + 9{,}409^2 + 80{,}09^2 + 9{,}89^2 + 18{,}915^2 + 150{,}957^2) - \ 1519{,}99$$

$$SS_{Bloques} = 3437{,}89$$

- Sumatoria de los cuadrados del error

$$SS_E = SS_T - SS_{Tratamiento} - SS_{Bloques}$$

$$SS_E = 16426{,}87 - 5953{,}81 - 3437{,}89$$

$$SS_E = 7035{,}17$$

Los resultados del análisis de suma de cuadrados y cuadrados medios para determinar el F_0**,** o F calculado se resumen en la Tabla 20-5:

Tabla 20-5: Determinación de Fo calculado

Fuente de variación	**Suma de cuadrados**	**Grados de libertad**	**Cuadrado medio (MS)**	F_0
Tratamientos	5953,81	3	1984,60	4,23
Bloques	3437,89	5	687,58	
Error	7035,17	15	469,01	
Total	16426,87	23		

Elaborado por: Roberto Usca, 2017

El F de tabla se determina con los grados de libertad del tratamiento y del error respectivamente, identificados en el Anexo F, el mismo que asciende 3,29.

Si F $\mathbf{Fc = 4.23}$ > F $\mathbf{Ft = 3.29,}$ por ende La implementación del protocolo MPLS con la aplicación de VPN influye significativamente en el rendimiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar.

CONCLUSIONES

- El uso de simuladores adecuados para el diseño de redes y evaluación de los mismos, permite verificar el rendimiento del sistema de transmisión de datos de una manera didáctica y eficiente, posterior a la evaluación es necesario el análisis de confiabilidad de datos mediante un método experimental en el cual se evidencia una gran influencia del rendimiento de la red y la eficiencia de la implementación del protocolo MPLS con la aplicación de VPN. Siendo el tiempo en la llegada de los paquetes mas rapido con el protocolo MPLS de 5,6, a diferencia del valor Sin MPLS que es de 10,83 ns. La latencia también muestra una reducción de 12,26 sin MPLS a 10,99 ms. La velocidad real de transporte de datos(throughput) se incrementa de 21,48 sin MPLS a 28,47 con la utilización de MPLS.

- Con el diseño de un esquema topológico en el software GNS3 basado en el protocolo MPLS con la aplicación de VPN, permite conocer el comportamiento de la red diseñada conjuntamente con las pruebas de conectividad entre agencias de la Corporacion Nacional de Electricidad Bolívar.

- Los valores recomendados de latencia o retardo entre el punto de inicio y fin de la comunicación lo ideal es menor a 150 ms, el jitter entre el punto inicial y final de la comunicación debiera ser inferior a 100 ms, datos según, (Brognara, 2016), comparando con la propuesta de implementación del protocolo MPLS se cumplen dichos parámetros, los valores analizados en la red CNEL Bolívar son inferiores a los recomendados por lo que el sistema de transmisión de datos es más eficiente y muestra mejor resultados de rendimiento.

- La utilizacion del protocolo MPLS con la Aplicación de VPN permite operar sobre varias tecnologías de transporte proporcionando gran flexibilidad, escalabilidad, capacidad y beneficios de ingeniería en tráfico de datos en comparación con las redes VPN tradicionales basadas en IP.

RECOMENDACIONES

Mediante el estudio técnico realizado en la Corporación Nacional de Electricidad Regional Bolívar, se puede citar algunas recomendaciones que ayudan a mejorar las condiciones de rendimiento de la red; y se mencionan a continuación:

- Se recomienda implementar sistema MPLS con VPN porque mejora el rendimiento de la red brindando seguridad al aplicar VPN-L3, y a su vez creando un túnel de tráfico dedicado, con lo que se asegura servicios, un manejo del tráfico generado por aplicaciones y clientes con mayor control de la red.

- Se recomienda la aplicación de redes flexibles (MPLS) y sobretodo escalable permitiendo un incremento en el desempeño y estabilidad de la red. Incluyendo ingeniería de tráfico y soporte de VPN, ofreciendo la calidad de servicio QoS pertinente en la red, como lo presenta el protocolo MPLS.

- Permitir la transmisión de datos mediante el establecimiento o asignación de etiquetas, en lugar de realizar búsquedas complejas basada en direccionamiento IP destino. Esta técnica permite optener muchos beneficios en comparación a redes basadas en IP como la aplicación de VPN, Ingenieria de tráfico y calidad de servicio QoS.

- Se recomienda combinar IGP, BGP, VRF Y VPNL3, debido a que estos protocolos se juntan para mejorar el desempeño de red y lo más importante optimizar recursos de red además de brindarle seguridad.

BIBLIOGRAFÍA

Aguilar, L. J. (2010). *Ciberseguridad. retos y amenazas a la seguridad nacional en el ciberespacio.* España: Imprenta del Ministerio de Defensa. Obtenido de chrome-extension://ihgdgpjankaehldoaimdlekdidkjfghe/viewer.html#https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

Ahmed, F., Butt, Z. U., & Siddiqui, U. A. (2016). *MPLS based VPN Implementation in a Corporate Environment* (Vol. 6:5). Pakistan: OMICS International. doi:10.4172/2165-7866.1000193

Biblioteca de la Universidad de Cornell Departamento de Investigación. (2003). Digitalizacion de imagenes. *Universidad de Cornell*, 6. Obtenido de http://preservationtutorial.library.cornell.edu/tutorial-spanish/technical/technicalA-01.html

Buettrich, S. (2007). Cálculo de Radioenlace. *Asociación Civil Nodo TAU*. Obtenido de chromeextension://ihgdgpjankaehldoaimdlekdidkjfghe/viewer.html#http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/06_es_calculo-de-radioenlace_guia_v02.pdf

Camacho, T. H. (2015). *Estudio De La Ingenieria De Tráfico En Redes Mpls Mediante Casos De Uso Practico Con La Herramienta Vnx* (Vol. 1). Madrid, España: Universidad Politecnica de Madrid. Obtenido de chrome-extension://ihgdgpjankaehldoaimdlekdidkjfghe/viewer.html#http://www.dit.upm.es/~posgrado/doc/TFM/TFMs20142015/TFM_Tatiana_Hernandez_Camacho_2015.pdf

Chavez, N. (2007). *Introducción a la investigación Educativa.* Venezuela: Editorial Universal.

Contandriopoulos, A., Champagne, F., Potvin, L., Denis, J., & Boyle, P. (1991). *Preparar un proyecto de investigación.* Barcelona, España: SG Editores.

Cordoba, C. (2017). MPLS. *SCRIBD*, 62. Obtenido de https://es.scribd.com/document/213931807/MPLS-pdf

Cure, E., & González, J. L. (2014). Análisis de la arquitectura MPLS (MULTI-PROTOCOL LABEL SWITCHING). *slideplayer*, 55. Obtenido de http://slideplayer.es/slide/1846859/

Delgado, D. Á., Cáceres, C. J., Jorquera, G. S., & Esquivel, C. Z. (2014). *Redes Privadas Virtuales (VPN).* Chile: Universidad Técnico Federico Santa María .

Díaz, M. (15 de 05 de 2014). *APOGEE*. Obtenido de Knowledgebase: http://www.apogeedigital.com/knowledgebase/spanish/que-es-jitter/

Espinosa, B. M., Salcedo, P. O., & Gómez, V. R. (2013). Análisis de Redes MPLS/BGP/VPN en el Rendimiento de los Anuncios del Algoritmo de Enrutamiento BGP. . *Tecno Lógicas*, 425-435.

Filippis, C. D. (2012). *La importancia de la latencia en las redes de datos.*

Fisher, R. A. (1926). *The Arrangement of Field Experiments.* California: Springer Series in Statistics.

Frenkel, A. S. (2017). Diferentes tipos de VPN y cuándo usarlas. *VPN Mentor*, 5. Obtenido de https://es.vpnmentor.com/blog/diferentes-tipos-de-vpn-y-cuando-usarlas/

Kuehl, R. O. (2001). *Principios estadisticos para el diseño y analisis de investigaciones* (2 ed.). Mexico: Thomson Learning.

Kuehl, R. O. (2001). *Principios estadisticos para el diseño y analisis de investigaciones* (2 ed.). Mexico: Thomson Learning.

Montgomery, D. (2004). *Diseño y analisis de experimentos* (Edicion 2 ed.). Arizona: Limusa Wiley.

Morales, L. (2017). *Multiprotocolo de conmutacion de etiquetas (MPLS).* Mexico: catarina-UDLAP. Obtenido de catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo2.pdf

Pacheco, H. J. (2008). Redes de comunicacion. *Monografias.com*. Obtenido de http://www.monografias.com/trabajos58/redes-comunicaciones/redes-comunicaciones.shtml

Pino, O. A. (2009). Creacion de una red MPLS. *sdm3.blogspot.com*, 1. Obtenido de http://sdm3.blogspot.com/2009/08/creacion-de-una-red-mpls.html

Revelo, F. G. (2014). *Impacto de túneles MPLS en la topología de internet.* Buenos Aires, Argentina: Universidad de Buenos Aires Argentina. Obtenido de chrome-extension://ihgdgpjankaehldoaimdlekdidkjfghe/viewer.html#http://cnet.fi.uba.ar/fernando_davila/Tesis_Fernando_Davila.pdf

Ríos, R. (2009). Anáisis de tráfico de una red local universitaria. *Telematique, 8*(2), 7.

Rodríguez, J. R., & Vazquez, J. (2015). *Manual practico de trasmision de datos* (Vol. 1). México: UNAM. Obtenido de https://es.slideshare.net/pcuadradosbalderas/transmision-datos-2015-2

Romero, M. (2004). *Seguridad en redes y protocolos asociados.* España: Creative commons. Obtenido de chrome-extension://ihgdgpjankaehldoaimdlekdidkjfghe/viewer.html#http://www.dte.us.es/personal/mcromero/docs/ip/tema-seguridad-IP.pdf

Salcedo, O., Pedraza, L. F., & Espinosa, M. (2012). Evaluación de redes MPLS/VPN/BGP con rutas reflejadas. *Tecnura*, 107-116.

Shahzad, A., & Hussain, M. (2013). IP Backbone Security: MPLS VPN Technology. *ScienceDirect*, 16.

Solsona, A. B., Moya, J. M., & Calero, J. J. (2016). *Anministracion de sistemas informaticos redes de area local* (2 ed.). España: Editorial Paraninfo.

St-Pierre, A., & Stéphanos, W. (2005). *Redes locales e internet. Introducción a la comunicación de datos.* (2 ed.). Mexico: WorldCat.

System, C. (2006). *Cisco MPLS Fundamentals.* Indianapolis, USA: Cisco Press.

Tamayo, M., & Tamayo. (2004). *El proceso de la investigación científica* (4 ed.). Mexico: Limusa.

Tigridae. (3 de Junio de 2017). *Rlinx.* Obtenido de Rlinx: https://es.wikipedia.org/wiki/Conmutaci%C3%B3n_(redes_de_comunicaci%C3%B3n)

Torres, D., Lewis, J., & Hernández, P. (2015). Multi Protocol Label Switching (MPLS). *Coup Scient*, 23. Obtenido de chrome-extension://ihgdgpjankaehldoaimdlekdidkjfghe/viewer.html#https://supportforums.cisco.com/sites/default/files/presentacion_mpls.pdf

Ullauri, E. S. (2015). *Diseño y simulación de una red mpls para interconectar estaciones remotas utilizando el emulador GNS3* (Vol. 1). Guayaquil, Ecuador: Universidad Politecnica Salesiana. Obtenido de chrome-extension://ihgdgpjankaehldoaimdlekdidkjfghe/viewer.html#

http://dspace.ups.edu.ec/bitstream/123456789/10297/1/UPS-GT001192.pdf

Valdivia, J. R., & Peña, C. M. (2015). MPLS y su aplicación en redes privadas virtuales. *Advances in Engineering and Technology: A Global Perspective*, 10. Obtenido de chromeextension://ihgdgpjankaehldoaimdlekdidkjfghe/viewer.html#http://www.laccei.org/LACCEI2005-Cartagena/Papers _MolinerPena.pdf

Valladares, D. R. (2014). *Diseño y evaluación de nivel de seguridad del protocolo getvpn en una red de datos para un entorno multipunto que utiliza MPLS para su comunicación WAN* (Vol. 1). Quito, Ecuador: ESPE.

Usca, R. B. (2013). *Auditoria operativa de la red para el mejoramiento del sistema de transmisión de datos en la Corporación Nacional de Electricidad Regional Bolívar*. Amabato: UTA.

VoipForo. (2017). QoS QualityOf sevice VoIP. *VoipForo*, 1. Obtenido de http://www.voipforo.com/QoS/QoS_Latencia.php

Anexo A. Análisis de la situación actual de los radioenlaces

Enlace Rep.Shunguna-CNEL Matriz (Proxim 5.8 Ghz)

Tabla 1A: Ubicación geográfica CNEL Matriz

NOMBRE	LATITUD	LONGITUD
Rep.Shunguna(Tx)	1°35'52.80"S	79° 1'8.00"O
Matriz CNEL Bolivar(Rx)	1°35'2.96"S	78°59'54.13"O

Elaborado por: Roberto Usca, 2017

Tabla 2A: Descripción de Antenas (Tx-Rx) CNEL Matriz

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	50dBm	30dBi	21 m	2.75 Km	PTP
Rx	-115dBm	30dBi	7 m	2.75 Km	PTP

Elaborado por: Roberto Usca, 2017

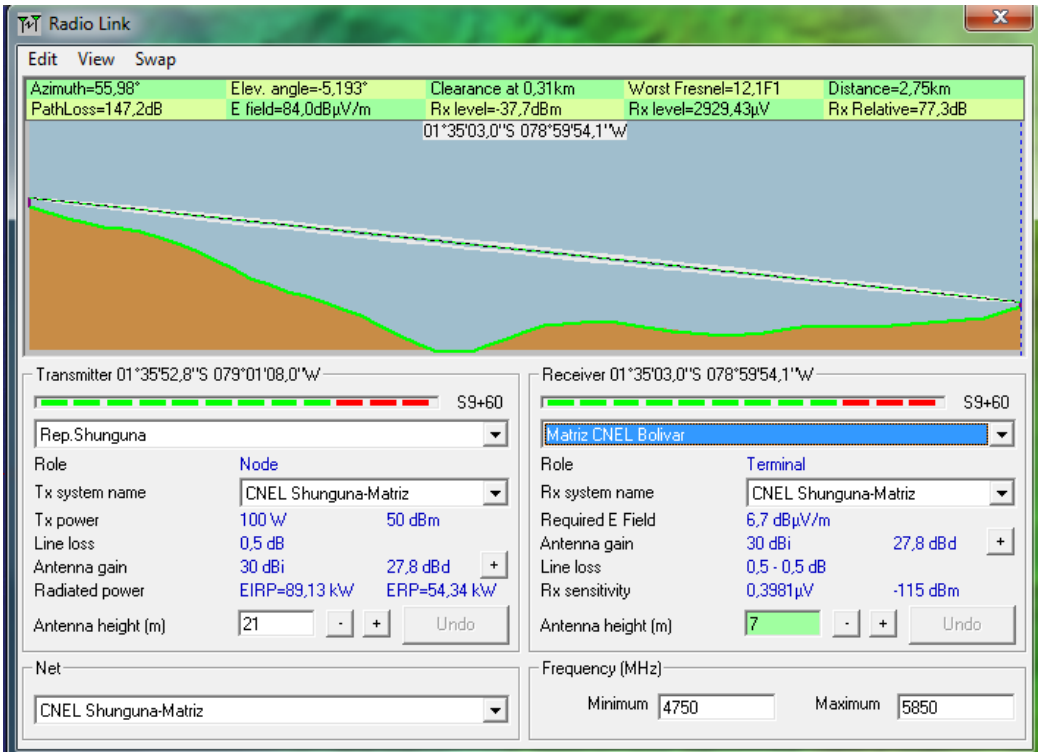


Figura 1A: Enlace Rep.Shunguna-CNEL Matriz

Elaborado por: Roberto Usca, 2017

Enlace Rep. Shunguna-Sub.Guaranda(5.8Ghz Mikrotik)

Tabla 3A: Ubicación Geográfica Shunguna

NOMBRE	LATITUD	LONGITUD
Rep. Shunguna(Tx)	1°35'52.80"S	79° 1'8.00"O
Sub. Guaranda (Rx)	1°35'45.54"S	78°59'45.96"O

Elaborado por: Roberto Usca, 2017

Tabla 4A: Descripción de Antenas (Tx-Rx) Shunguna

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	21 m	2.54 Km	PTP
Rx	-115dBm	16dBi	3 m	2.54 Km	PTP

Elaborado por: Roberto Usca, 2017

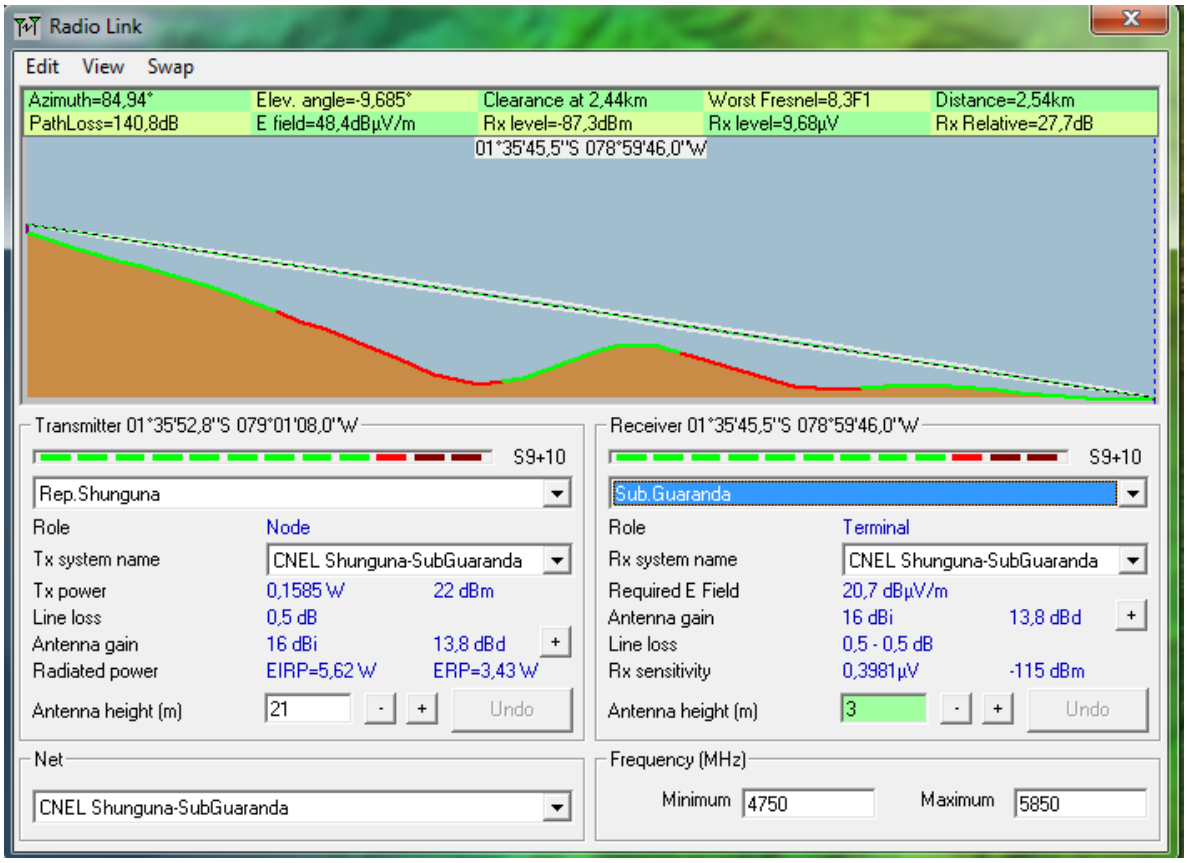


Figura 2A: Enlace Rep.Shunguna-Sub.Guaranda

Elaborado por: Roberto Usca, 2017

Enlace Rep. Shunguna-Sub. Guanujo (5.8Ghz Mikrotik)

Tabla 5A: Ubicación Geográfica Sub. Guanujo

NOMBRE	LATITUD	LONGITUD
Rep. Shunguna(Tx)	1°35'52.80"S	79° 1'8.00"O
Sub. Guanujo (Rx)	1°35'45.54"S	78°59'45.96"O

Elaborado por: Roberto Usca, 2017

Tabla 6A: Descripción de Antenas (Tx-Rx) Sub. Guanujo

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	21 m	5.10 Km	PTP
Rx	-115dBm	16dBi	3 m	5.10 Km	PTP

Elaborado por: Roberto Usca, 2017

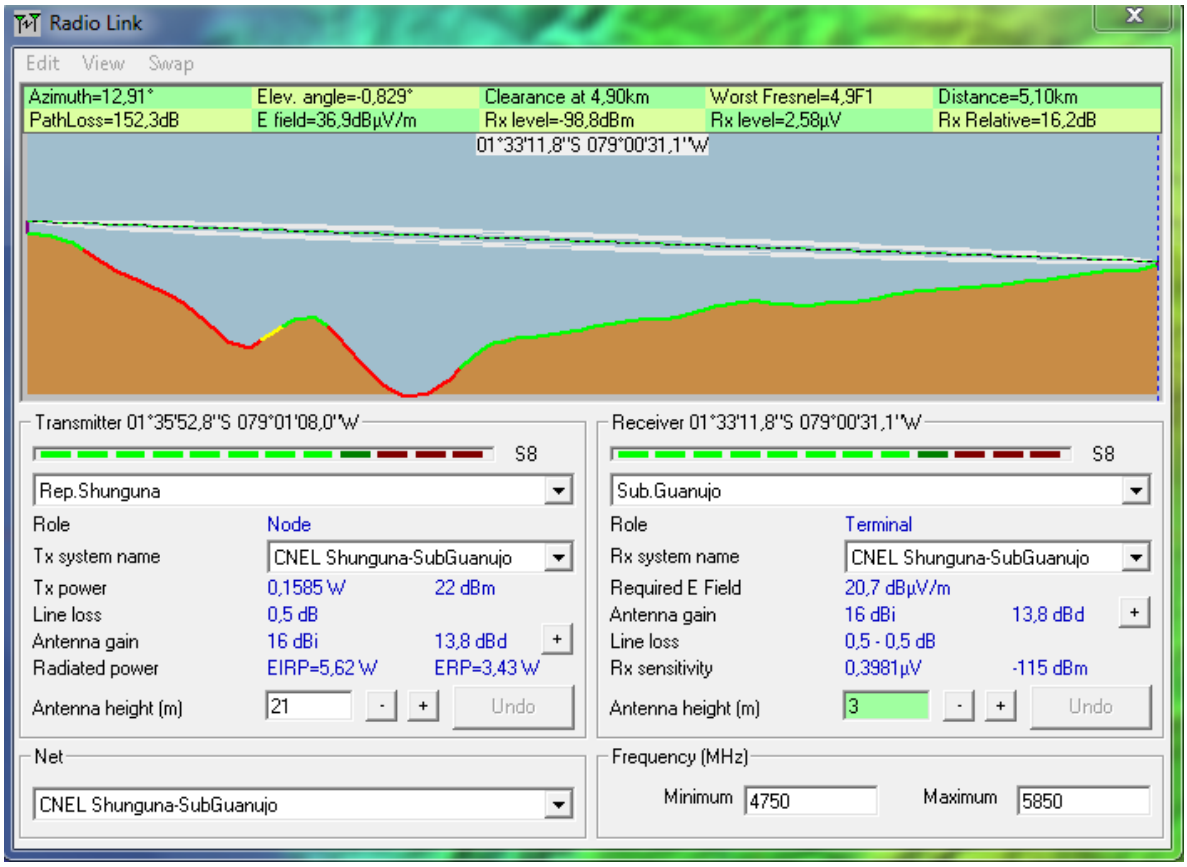


Figura 3A: Enlace Rep.Shunguna-Sub.Guanujo

Elaborado por: Roberto Usca, 2017

Enlace Rep. Shunguna-Rep. Susanga(2.4Ghz Mikrotik)

Tabla 7 A: Ubicación Geográfica Rep.Shunguna

NOMBRE	LATITUD	LONGITUD
Rep. Shunguna(Tx)	1°35'52.80"S	79° 1'8.00"O
Rep. Susanga (Rx)	1°40'26.90"S	79° 1'18.18"O

Elaborado por: Roberto Usca, 2017

Tabla 8A: Descripción de Antenas (Tx-Rx) Rep.Shunguna

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	27dBm	10dBi	21 m	8.47 Km	PTP
Rx	-115dBm	10dBi	21 m	8.47 Km	PTP

Elaborado por: Roberto Usca, 2017

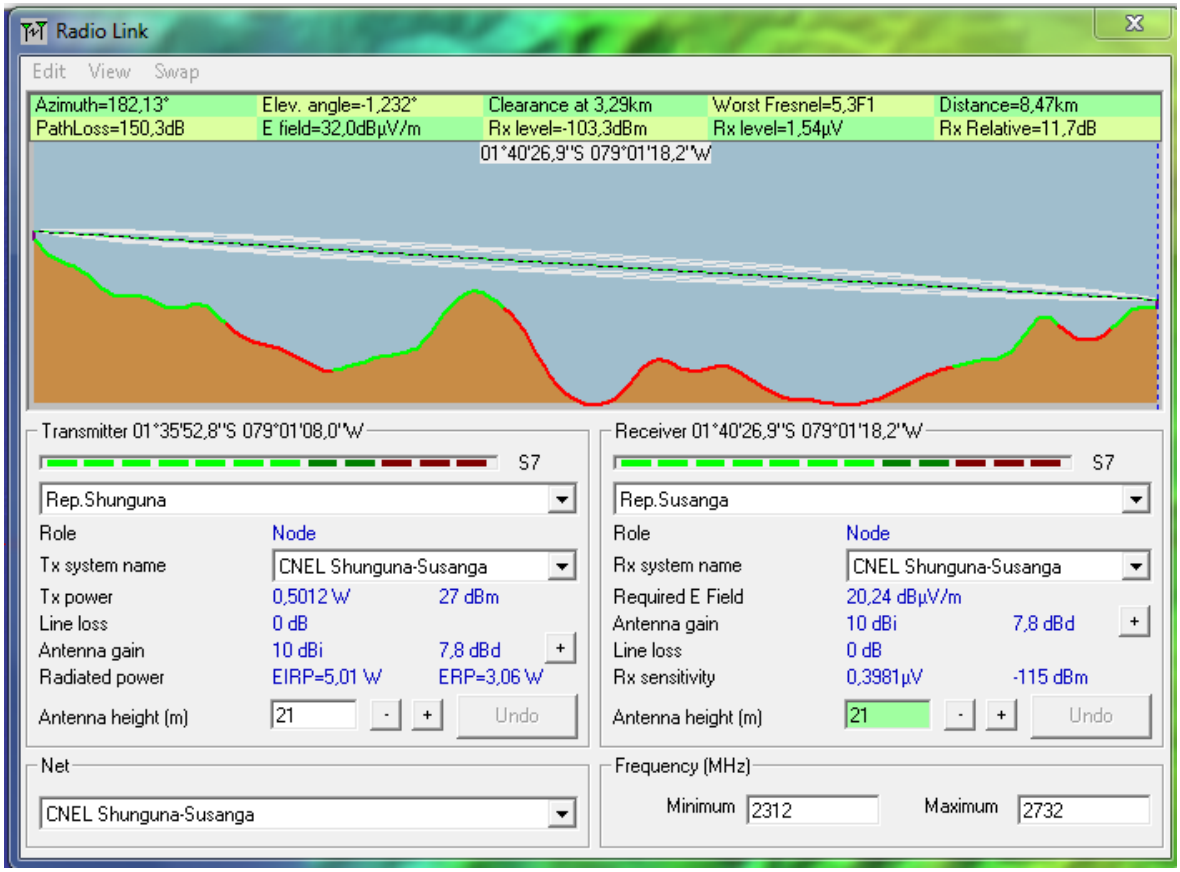


Figura 4A: Enlace Rep.Shunguna-Rep.Susanga

Elaborado por: Roberto Usca, 2017

Enlace Rep.Shunguna-Rep.Piscoquero(5.8Ghz Mikrotik)

Tabla 9A: Ubicación Geográfica Rep.Shunguna-Rep.Susanga

NOMBRE	LATITUD	LONGITUD
Rep. Shunguna(Tx)	1°35'52.80"S	79° 1'8.00"O
Rep. Piscoquero (Rx)	1°28'14.30"S	79° 3'43.10"O

Elaborado por: Roberto Usca, 2017

Tabla 10A: Descripción de Antenas (Tx-Rx) Rep.Shunguna-Rep.Susanga

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	16.5 m	14.94 Km	PTP
Rx	-115dBm	16dBi	24 m	14.94 Km	PTP

Elaborado por: Roberto Usca, 2017

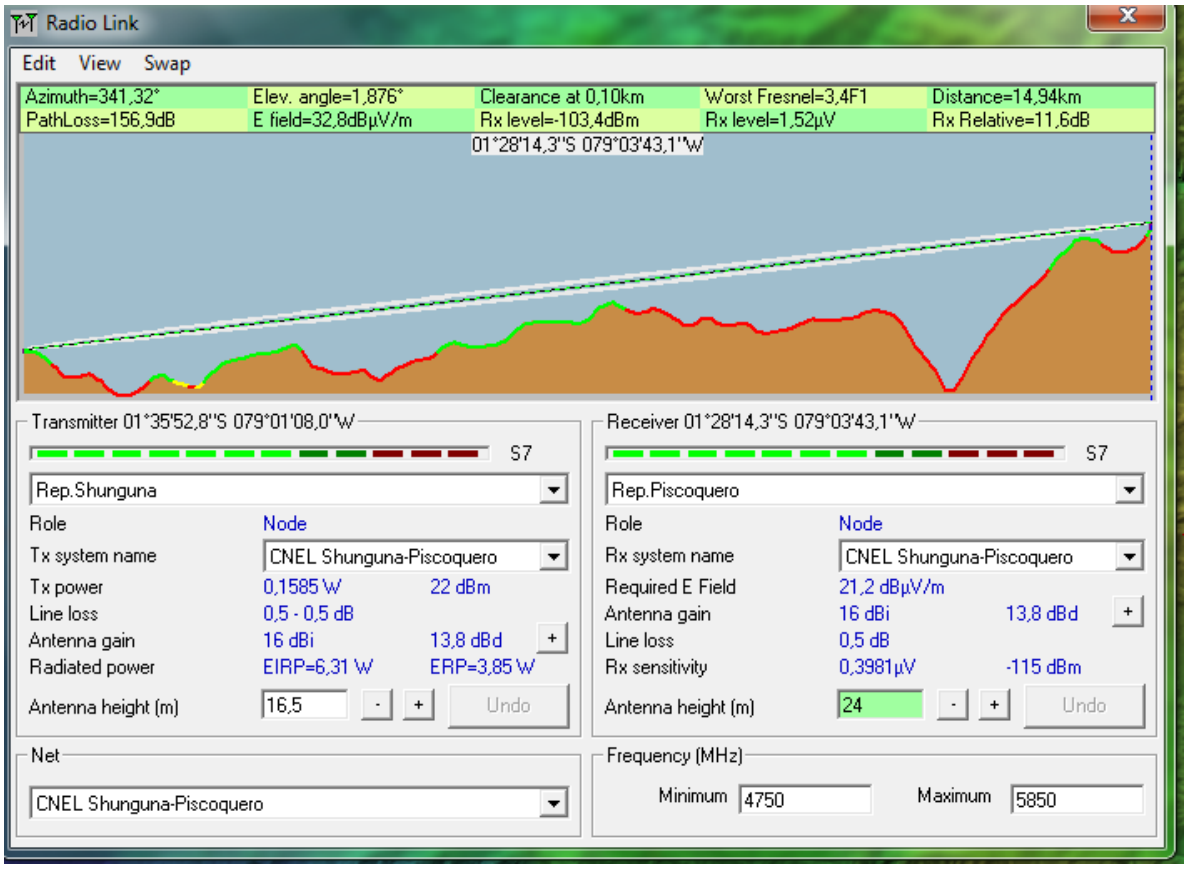


Figura 5A: Rep.Shunguna-Rep.Piscoquero

Elaborado por: Roberto Usca, 2017

Enlace Rep. Shunguna-Rep. Lourdes (5.8Ghz Promix)

Tabla 11 A: Ubicación Geográfica Rep. Shunguna-Rep. Lourdes

NOMBRE	LATITUD	LONGITUD
Rep.Shunguna(Tx)	1°35'52.80"S	79° 1'8.00"O
Rep. Lourdes (Rx)	1°42'19.74"S	79° 4'46.40"O

Elaborado por: Roberto Usca, 2017

Tabla 12A: Descripción de Antenas (Tx-Rx) Rep. Shunguna-Rep. Lourdes

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	50dBm	30dBi	21 m	13.71 Km	PTP
Rx	-115dBm	16dBi	21 m	13.71 Km	PTP

Elaborado por: Roberto Usca, 2017

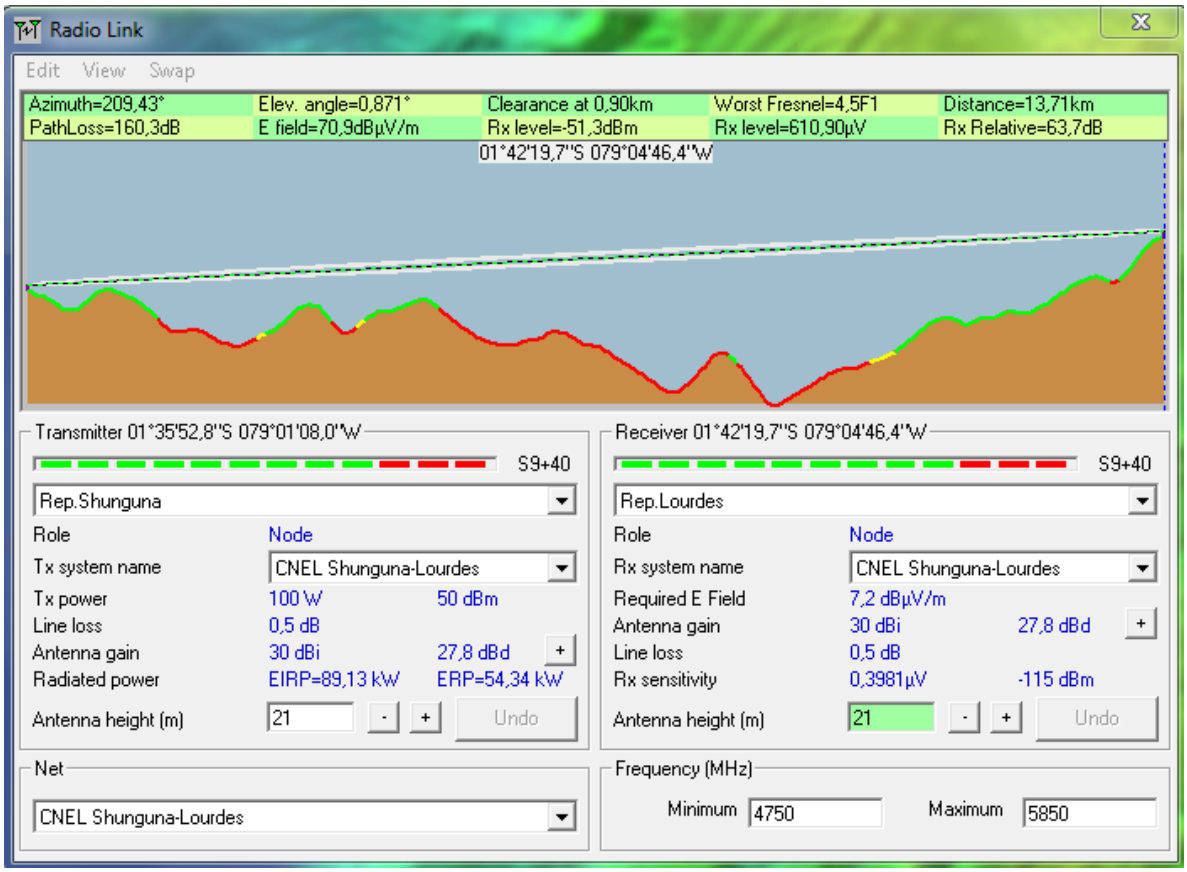


Figura 6A: Enlace Rep.Shunguna-Rep.Lourdes

Elaborado por: Roberto Usca, 2017

Enlace Rep. Susanga-Ag. Chimbo (5.8Ghz UBNT)

Tabla 13A: Ubicación Geográfica Rep. Susanga-Ag. Chimbo

NOMBRE	LATITUD	LONGITUD
Rep. Susanga (Tx)	1°40'26.90"S	79° 1'18.18"O
Ag. Chimbo(Rx)	1°41'1.92"S	79° 1'27.06"O

Elaborado por: Roberto Usca, 2017

Tabla 14A: Descripción de Antenas (Tx-Rx) Rep. Susanga-Ag. Chimbo

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	26dBm	34dBi	21 m	1.12 Km	PTP
Rx	-115dBm	34dBi	3 m	1.12 Km	PTP

Elaborado por: Roberto Usca, 2017

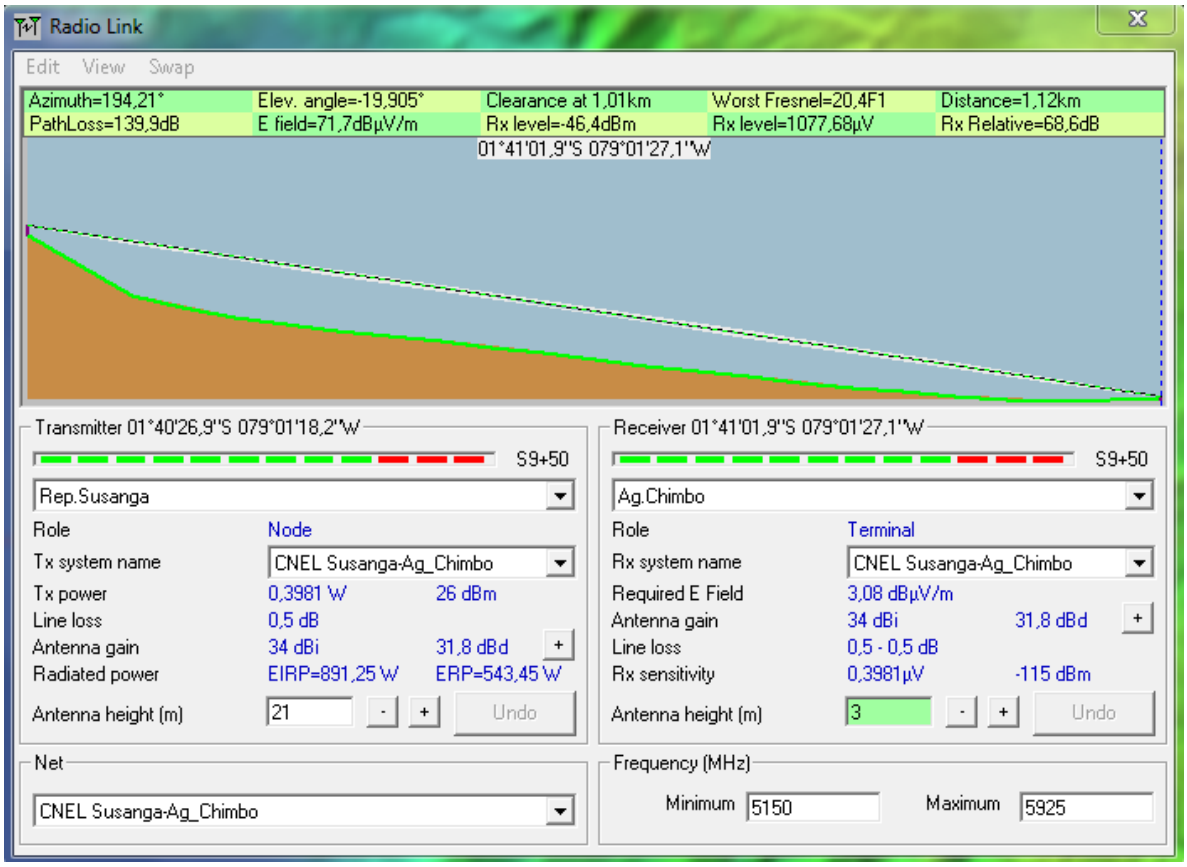


Figura 7A: Enlace Rep.Susanga-Ag. Chimbo

Elaborado por: Roberto Usca, 2017

Enlace Rep. Lourdes -Ag. San Miguel (2.4Ghz Mikrotik)

Tabla 15A: Ubicación Geográfica Rep. Lourdes -Ag. San Miguel

NOMBRE	LATITUD	LONGITUD
Rep. Lourdes(Tx)	1°42'19.74"S	79° 4'46.40"O
Ag. San Miguel(Rx)	1°42'27.24"S	79° 2'27.72"O

Elaborado por: Roberto Usca, 2017

Tabla 16A: Descripción de Antenas (Tx-Rx) Rep. Lourdes -Ag. San Miguel

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	27dBm	10dBi	21 m	4.29 Km	PTP
Rx	-115dBm	10dBi	4 m	4.29 Km	PTP

Elaborado por: Roberto Usca, 2017

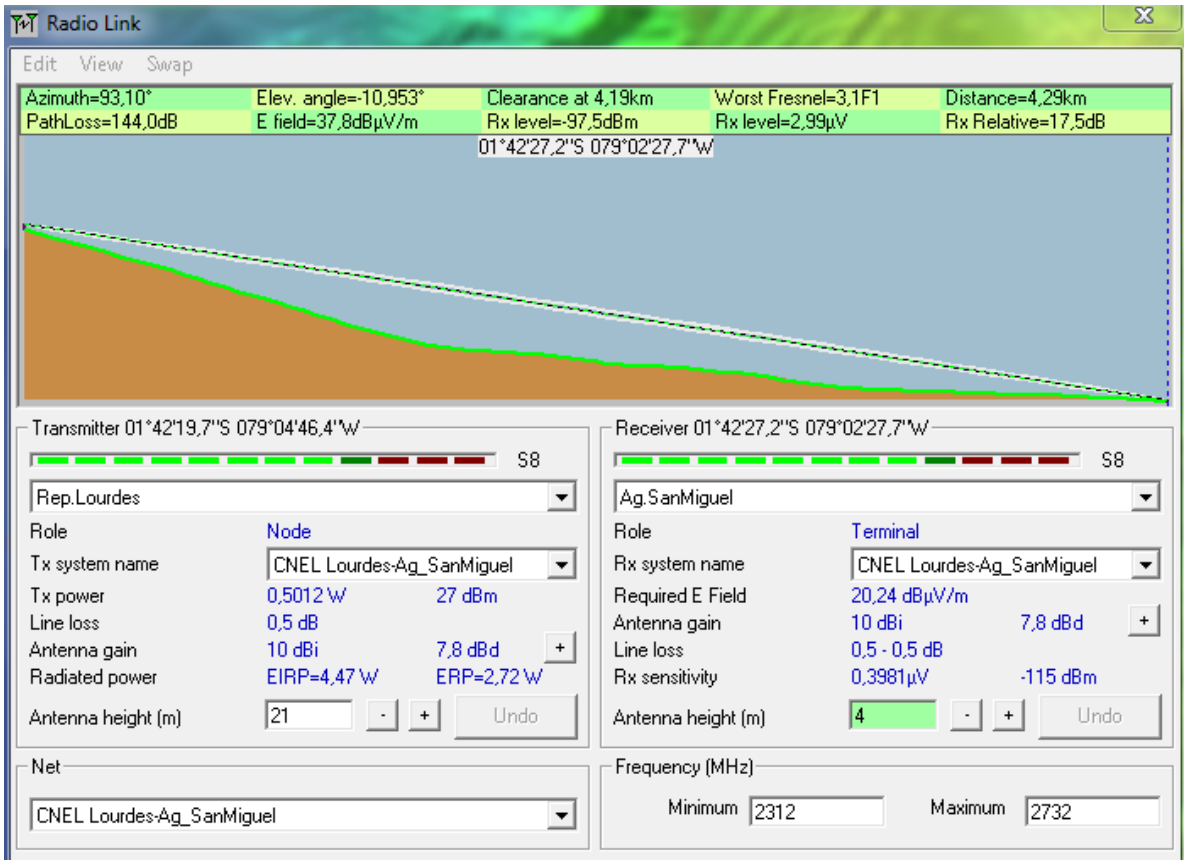


Figura 8A: Enlace Rep.Lourdes -Ag. San Miguel

Elaborado por: Roberto Usca, 2017

Enlace Rep. Lourdes – Sub. Cochabamba (5.8Ghz Mikrotik)

Tabla 17A: Ubicación Geográfica Rep. Lourdes – Sub. Cochabamba

NOMBRE	LATITUD	LONGITUD
Rep. Lourdes(Tx)	1°42'19.74"S	79° 4'46.40"O
Sub. Cochabamba(Rx)	1°41'35.30"S	79° 6'28.20"O

Elaborado por: Roberto Usca, 2017

Tabla 18A: Descripción de Antenas (Tx-Rx) Rep. Lourdes – Sub. Cochabamba

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	24 m	3.43 Km	PTP
Rx	-115dBm	16dBi	4 m	3.43 Km	PTP

Elaborado por: Roberto Usca, 2017

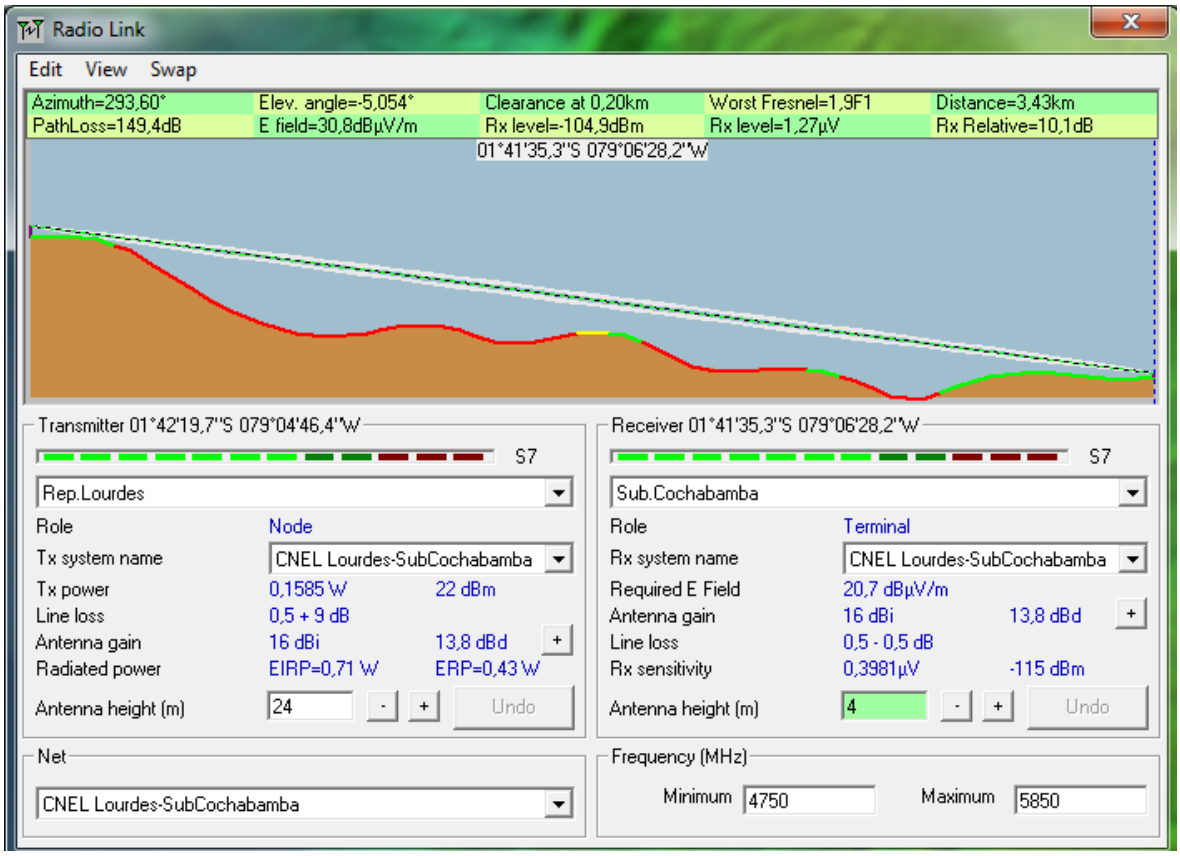


Figura 9A: Enlace Rep.Lourdes – Sub.Cochabamba

Elaborado por: Roberto Usca, 2017

Enlace Rep. Lourdes – Rep. Willoloma (5.8Ghz Mikrotik)

Tabla 19 A: Ubicación Geográfica Rep. Lourdes – Rep. Willoloma

NOMBRE	LATITUD	LONGITUD
Rep. Lourdes(Tx)	1°42'19.74"S	79° 4'46.40"O
Rep.Willoloma (Rx)	1°43'58.62"S	79°10'33.78"O

Elaborado por: Roberto Usca, 2017

Tabla 20A: Descripción de Antenas (Tx-Rx) Rep. Lourdes – Rep. Willoloma

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	24 m	11.14 Km	PTP
Rx	-115dBm	16dBi	23.5 m	11.14 Km	PTP

Elaborado por: Roberto Usca, 2017

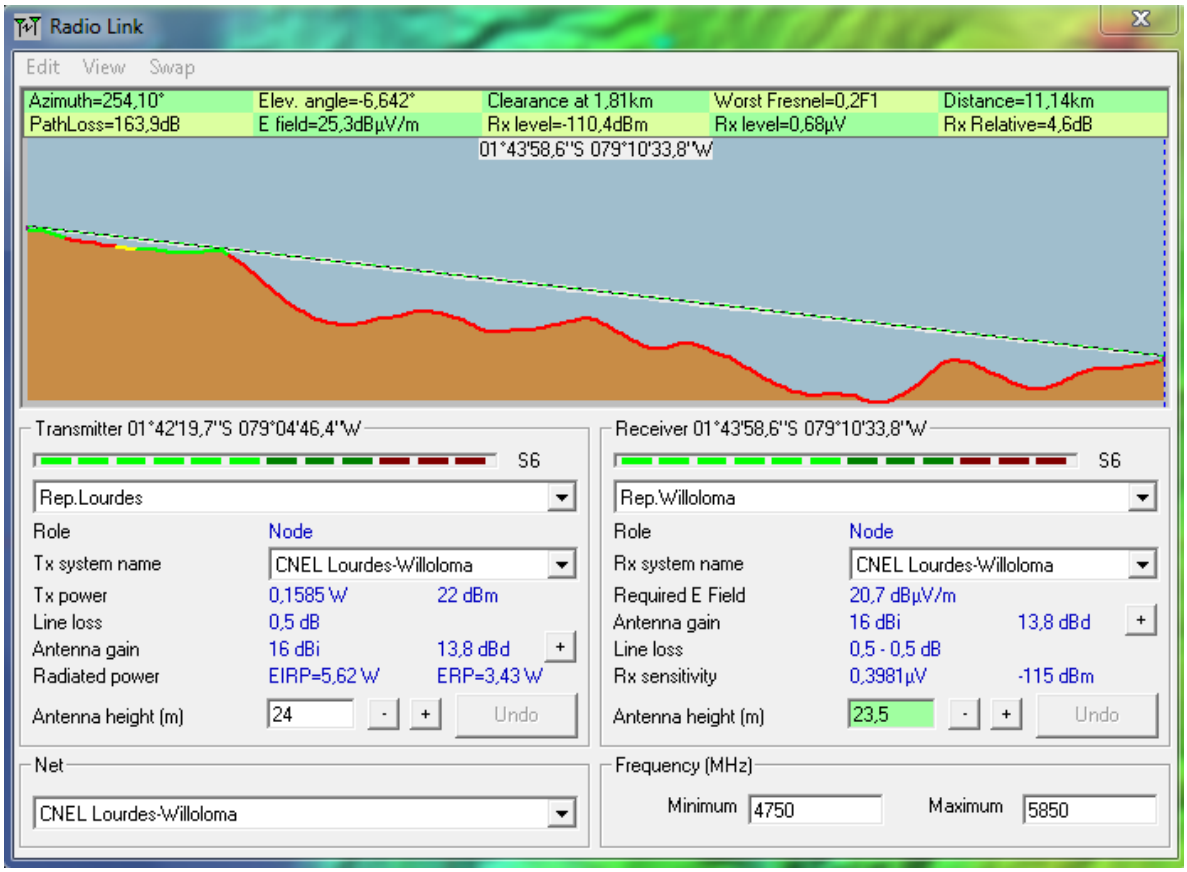


***Figura 10A**:* Enlace Rep.Lourdes – Rep.Willoloma

Elaborado por: Roberto Usca, 2017

Enlace Rep. Lourdes – Rep. Cuchicahua (2.4Ghz Mikrotik)

Tabla 21A: Ubicación Geográfica Rep. Lourdes – Rep. Cuchicahua

NOMBRE	LATITUD	LONGITUD
Rep. Lourdes(Tx)	1°42'19.74"S	79° 4'46.40"O
Rep. Cuchicahua (Rx)	1°55'44.00"S	79° 4'51.00"O

Elaborado por: Roberto Usca, 2017

Tabla 22A: Descripción de Antenas (Tx-Rx) Rep. Lourdes – Rep. Cuchicahua

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	27dBm	10dBi	24 m	24.83 Km	PTP
Rx	-115dBm	10dBi	24 m	24.83 Km	PTP

Elaborado por: Roberto Usca, 2017

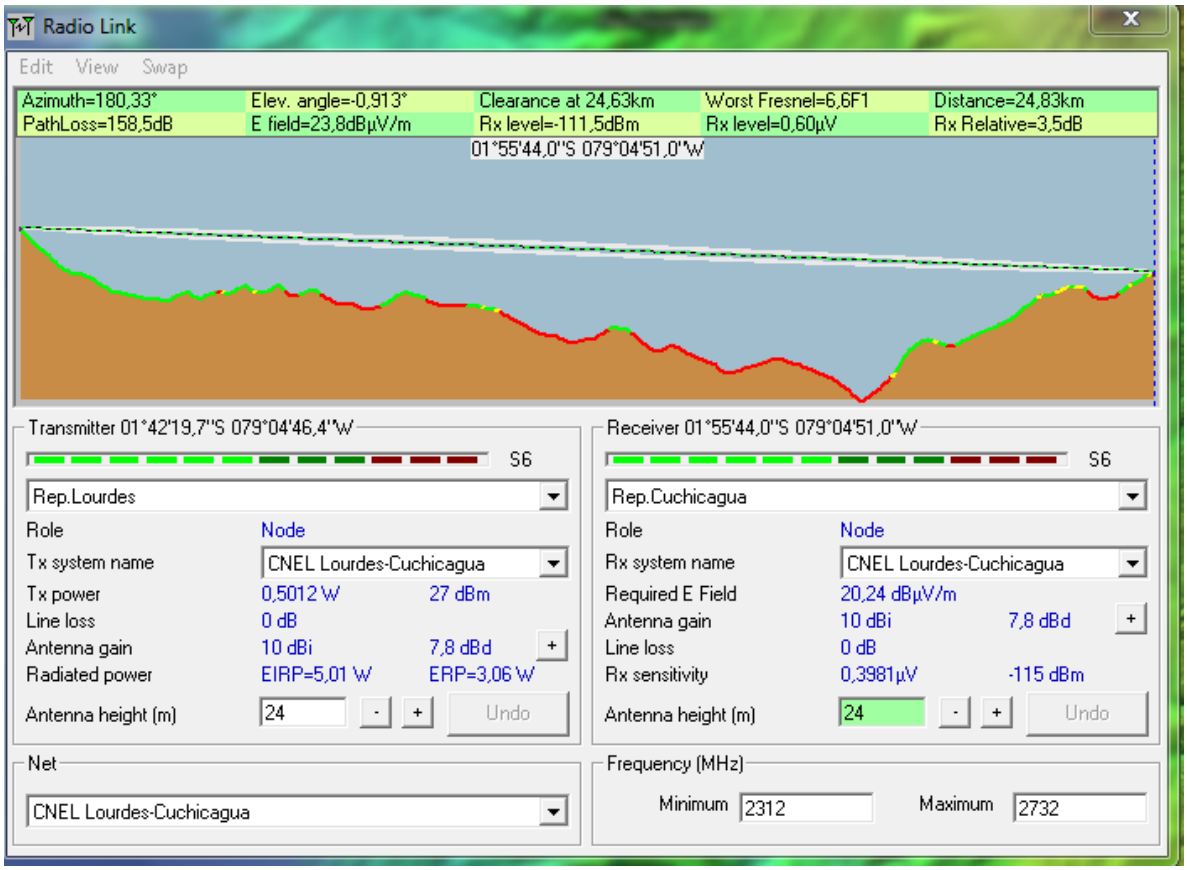


Figura 11A: Enlace Rep.Lourdes – Rep.Cuchicahua

Elaborado por: Roberto Usca, 2017

Enlace Rep. Willoloma – Ag. Balsapamba (5.8Ghz Mikrotik)

Tabla 23A: Ubicación Geográfica Rep. Willoloma – Ag. Balsapamba

NOMBRE	LATITUD	LONGITUD
Rep. Willoloma (Tx)	1°42'19.74"S	79° 4'46.40"O
Ag. Balsapamba (Rx)	1°46'1.01"S	79°10'44.06"O

Elaborado por: Roberto Usca, 2017

Tabla 24A: Descripción de Antenas (Tx-Rx) Rep. Willoloma – Ag. Balsapamba

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	23.5 m	3.79 Km	PTP
Rx	-115dBm	16dBi	15 m	3.79 Km	PTP

Elaborado por: Roberto Usca, 2017

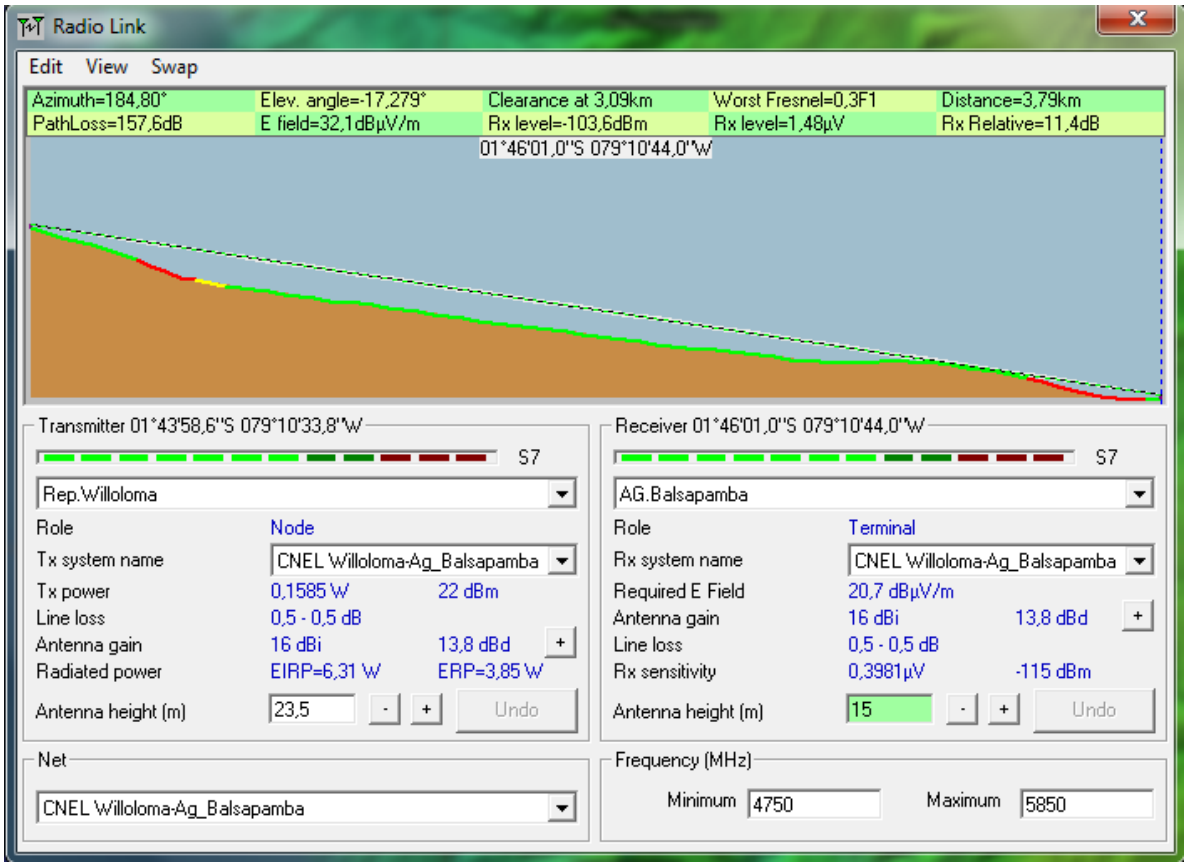


***Figura 12A**:* Enlace Rep.Willoloma – Ag. Balsapamba

Elaborado por: Roberto Usca, 2017

Enlace Rep.Cuchicahua – Sub.Sicoto (5.8Ghz Mikrotik)

Tabla 25A: Ubicación Geográfica Rep.Cuchicahua – Sub.Sicoto

NOMBRE	LATITUD	LONGITUD
Rep. Cuchicahua (Tx)	1°55'44.00"S	79° 4'51.00"O
Sub. Sicoto (Rx)	1°51'19.80"S	79° 3'52.92"O

Elaborado por: Roberto Usca, 2017

Tabla 26A: Descripción de Antenas (Tx-Rx) Rep.Cuchicahua – Sub.Sicoto

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	24 m	24.83 Km	PTP
Rx	-115dBm	16dBi	6 m	24.83 Km	PTP

Elaborado por: Roberto Usca, 2017

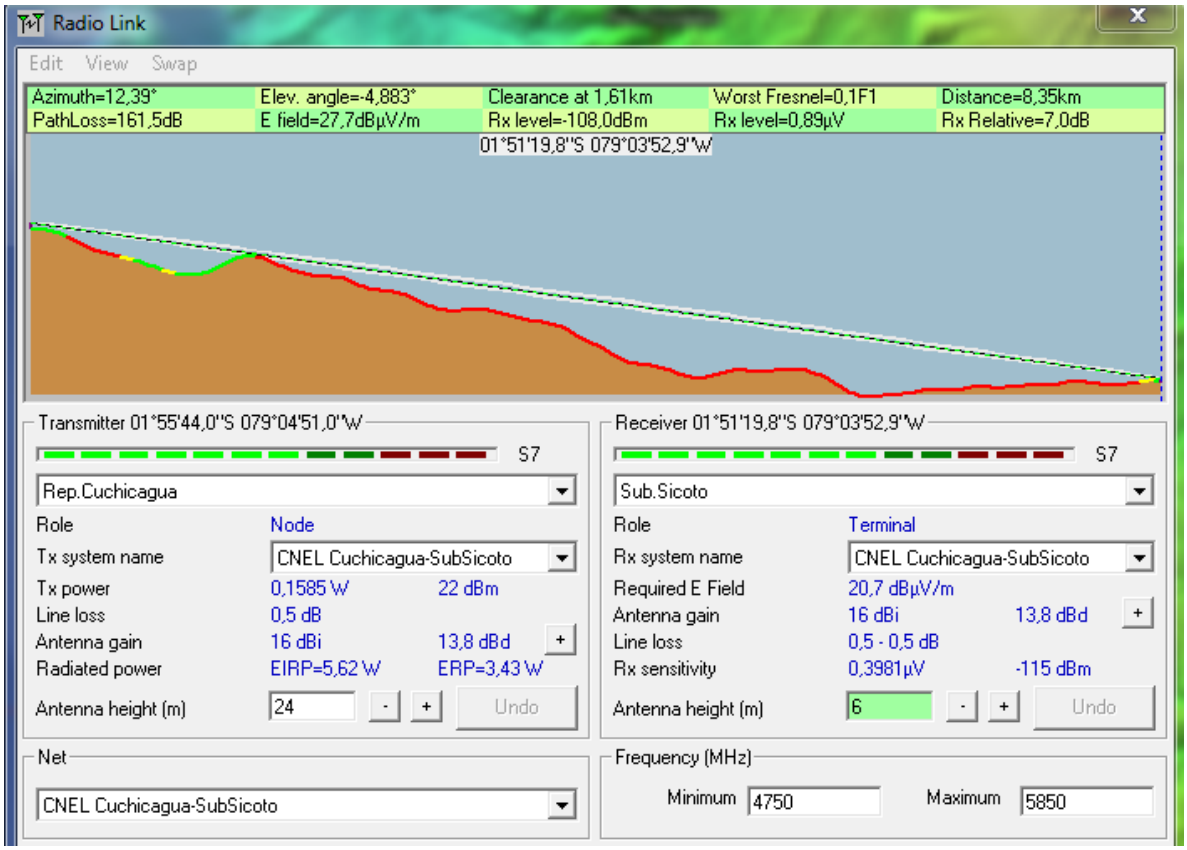


Figura 13A: Enlace Rep.Cuchicahua – Sub.Sicoto

Elaborado por: Roberto Usca, 2017

Enlace Rep. Cuchicahua – Ag. Chillanes (5.8Ghz Mikrotik)

Tabla 27 A: Ubicación Geográfica Rep. Cuchicahua – Ag. Chillanes

NOMBRE	LATITUD	LONGITUD
Rep. Cuchicahua (Tx)	1°55'44.00"S	79° 4'51.00"O
Ag. Chillanes (Rx)	1°56'30.12"S	79° 4'0.54"O

Elaborado por: Roberto Usca, 2017

Tabla 28A: Descripción de Antenas (Tx-Rx) Rep. Cuchicahua – Ag. Chillanes

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	24 m	2.11 Km	PTP
Rx	-115dBm	16dBi	3 m	2.11 Km	PTP

Elaborado por: Roberto Usca, 2017

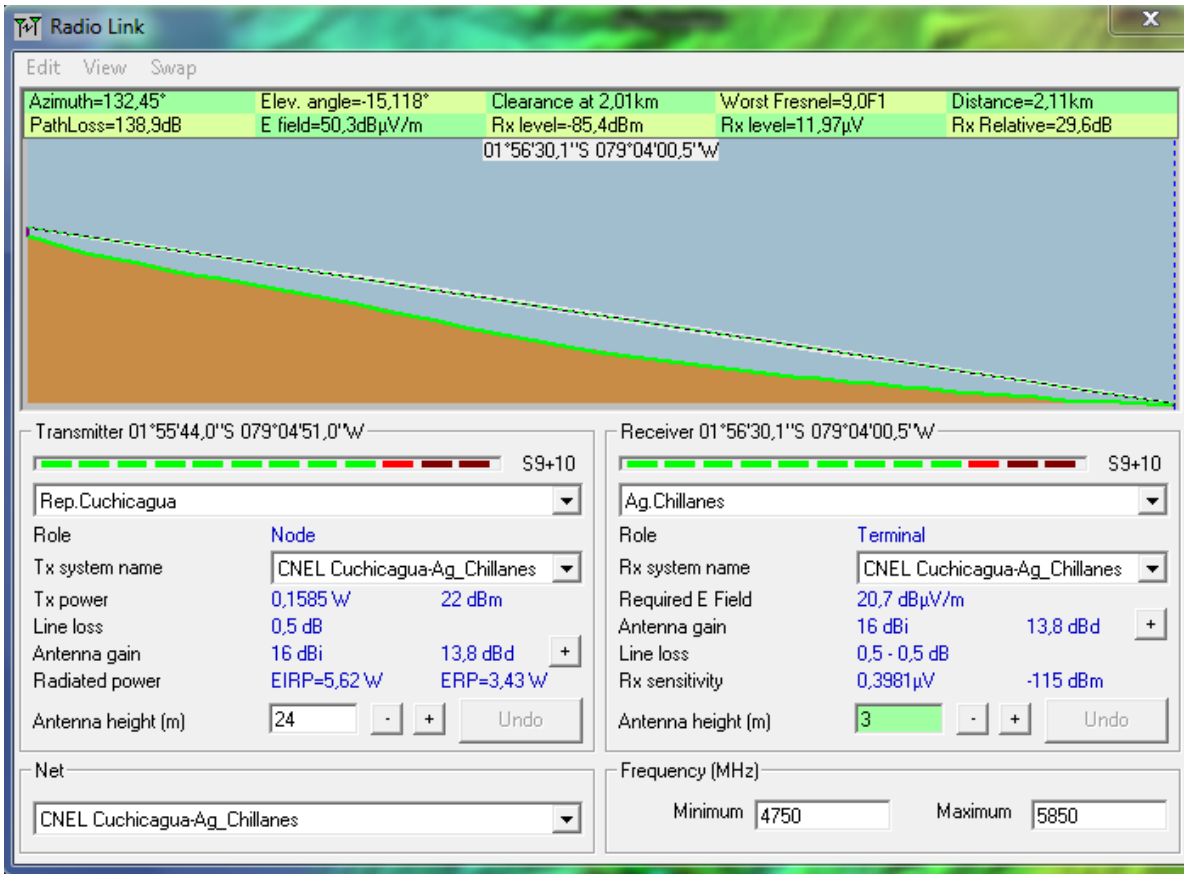


Figura 14A: Enlace Rep.Cuchicahua – Ag.Chillanes

Elaborado por: Roberto Usca, 2017

Enlace Rep. Cuchicahua – Ag. El Tambo (5.8Ghz UBNT)

Tabla 29A: Ubicación Geográfica Rep. Cuchicahua – Ag. El Tambo

NOMBRE	LATITUD	LONGITUD
Rep. Cuchicahua (Tx)	1°55'44.00"S	79° 4'51.00"O
Ag. El Tambo (Rx)	1°57'25.00"S	79°14'1.00"O

Elaborado por: Roberto Usca, 2017

Tabla 30A: Descripción de Antenas (Tx-Rx) Rep. Cuchicahua – Ag. El Tambo

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	26dBm	34dBi	24 m	17.25 Km	PTP
Rx	-115dBm	34dBi	3 m	17.25 Km	PTP

Elaborado por: Roberto Usca, 2017

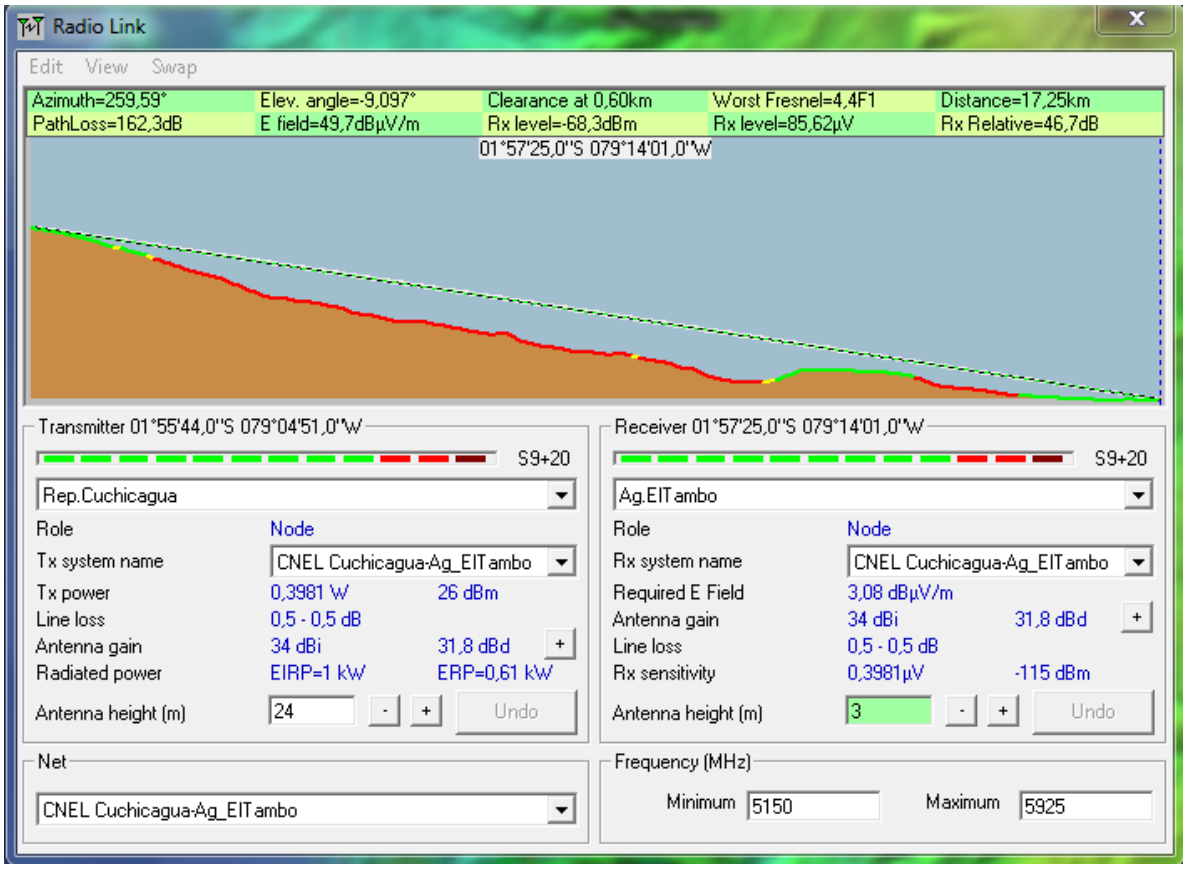


Figura 15A: Enlace Rep.Cuchicahua – Ag. El Tambo

Elaborado por: Roberto Usca, 2017

Enlace Rep. Piscoquero – Ag. Caluma (2.4Ghz Mikrotik)

Tabla 31A: Ubicación Geográfica Enlace Rep. Piscoquero – Ag. Caluma

NOMBRE	LATITUD	LONGITUD
Rep. Piscoquero (Tx)	1°28'14.30"S	79° 3'43.10"O
Ag. Caluma (Rx)	1°37'48.72"S	79°15'7.10"O

Elaborado por: Roberto Usca, 2017

Tabla 32A: Descripción de Antenas (Tx-Rx) Enlace Rep. Piscoquero – Ag. Caluma

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	27dBm	10dBi	24 m	27.57 Km	PTP
Rx	-115dBm	10dBi	3 m	27.57 Km	PTP

Elaborado por: Roberto Usca, 2017

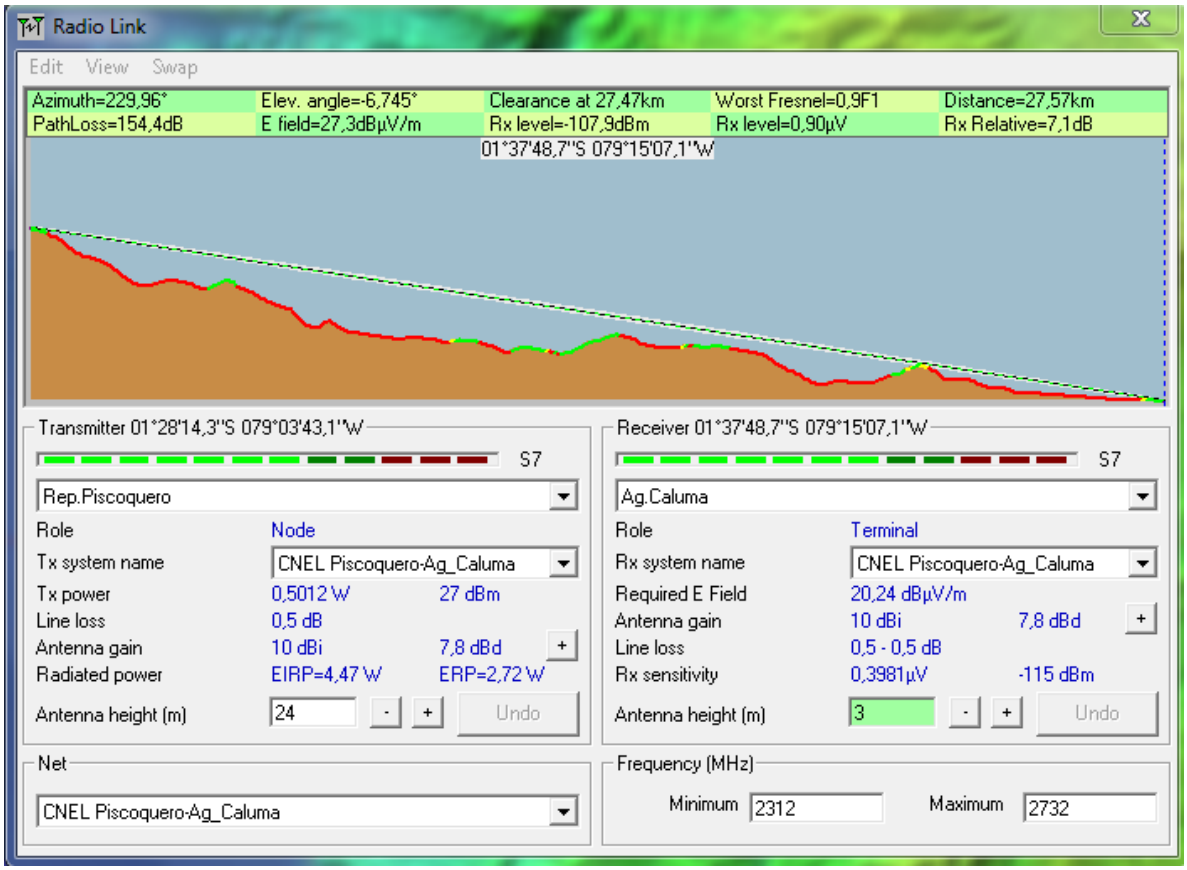


Figura 16A: Enlace Rep.Piscoquero – Ag.Caluma

Elaborado por: Roberto Usca, 2017

Enlace Rep. Piscoquero – Ag. Echeandia (2.4Ghz Mikrotik)

Tabla 33A: Ubicación Geográfica Rep. Piscoquero – Ag. Echeandia

NOMBRE	LATITUD	LONGITUD
Rep. Piscoquero (Tx)	1°28'14.30"S	79° 3'43.10"O
Ag. Echeandia (Rx)	1°25'51.42"S	79°16'58.32"O

Elaborado por: Roberto Usca, 2017

Tabla 34A: Descripción de Antenas (Tx-Rx) Rep. Piscoquero – Ag. Echeandia

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	27dBm	10dBi	24 m	24.93 Km	PTP
Rx	-115dBm	10dBi	12.5 m	24.93 Km	PTP

Elaborado por: Roberto Usca, 2017

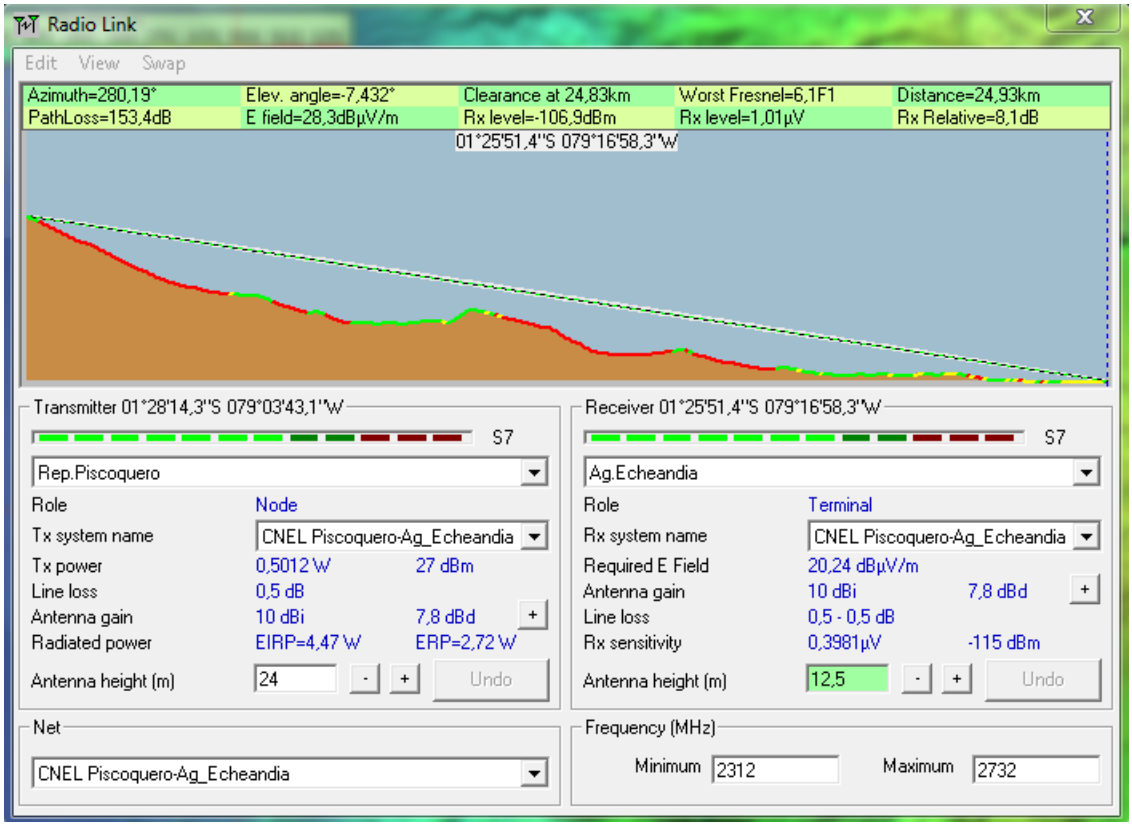


Figura 17A: Enlace Rep.Piscoquero – Ag.Echeandia

Elaborado por: Roberto Usca, 2017

Enlace Rep. Piscoquero – Rep. Jerusalen (2.4Ghz Mikrotik)

Tabla 35A: Ubicación Geográfica Rep. Piscoquero – Rep. Jerusalen

NOMBRE	LATITUD	LONGITUD
Rep. Piscoquero (Tx)	1°28'14.30"S	79° 3'43.10"O
Rep. Jerusalen (Rx)	1°19'42.14"S	79°16'22.09"O

Elaborado por: Roberto Usca, 2017

Tabla 36A: Descripción de Antenas (Tx-Rx) Rep. Piscoquero – Rep. Jerusalen

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	27dBm	10dBi	23.5 m	28.24 Km	PTP
Rx	-115dBm	10dBi	23.5 m	28.24 Km	PTP

Elaborado por: Roberto Usca, 2017

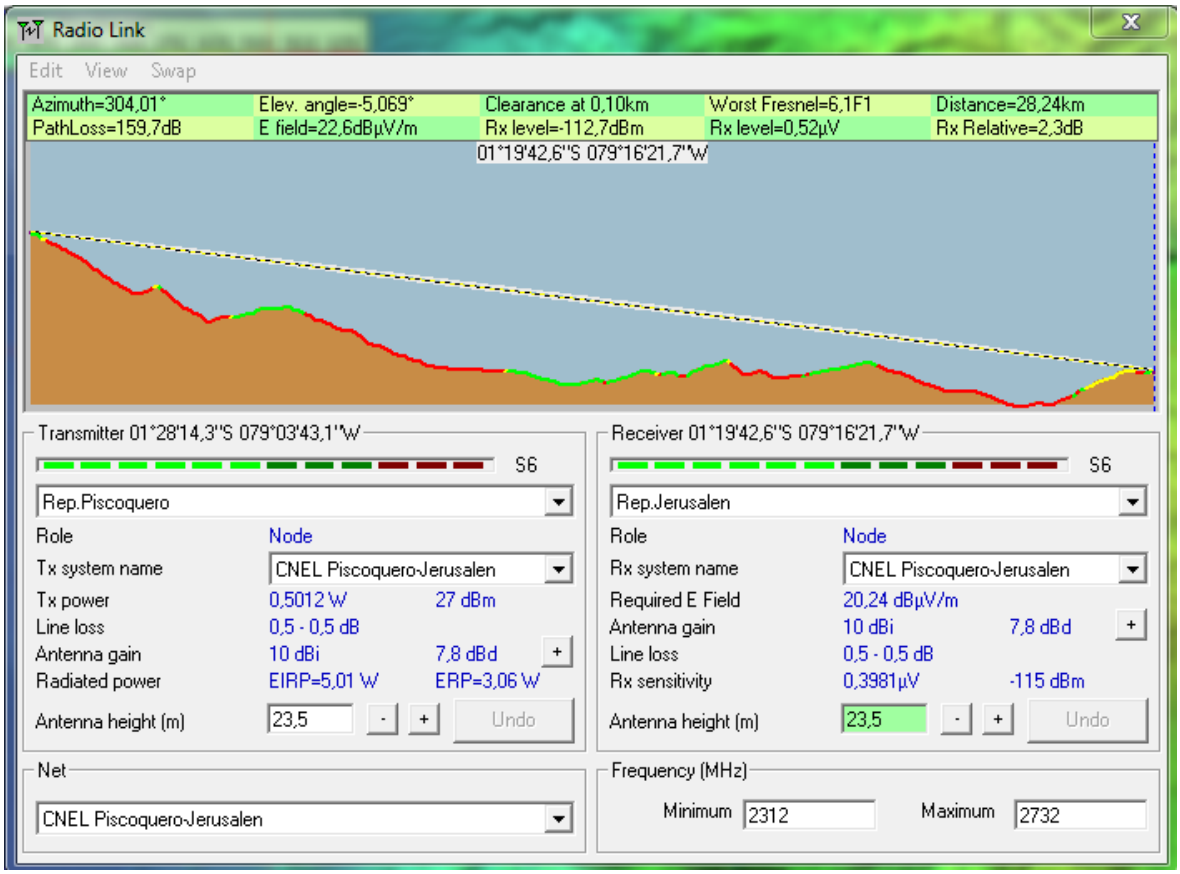


Figura 18A: Enlace Rep.Piscoquero – Rep.Jerusalen

Elaborado por: Roberto Usca, 2017

Enlace Rep. Jerusalen – Ag. San Luis de Pambil (5.8Ghz Mikrotik)

Tabla 37A: Ubicación Geográfica Rep. Jerusalen – Ag. San Luis de Pambil

NOMBRE	LATITUD	LONGITUD
Rep. Jerusalen (Tx)	1°19'42.14"S	79°16'22.09"O
Ag. San Luis de Pambil (Rx)	1°14'3.16"S	79°14'20.56"O

Elaborado por: Roberto Usca, 2017

Tabla 38A: Descripción de Antenas (Tx-Rx) Rep. Jerusalen – Ag. San Luis de Pambil

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	24 m	11.16 Km	PTP
Rx	-115dBm	16dBi	3 m	11.16 Km	PTP

Elaborado por: Roberto Usca, 2017

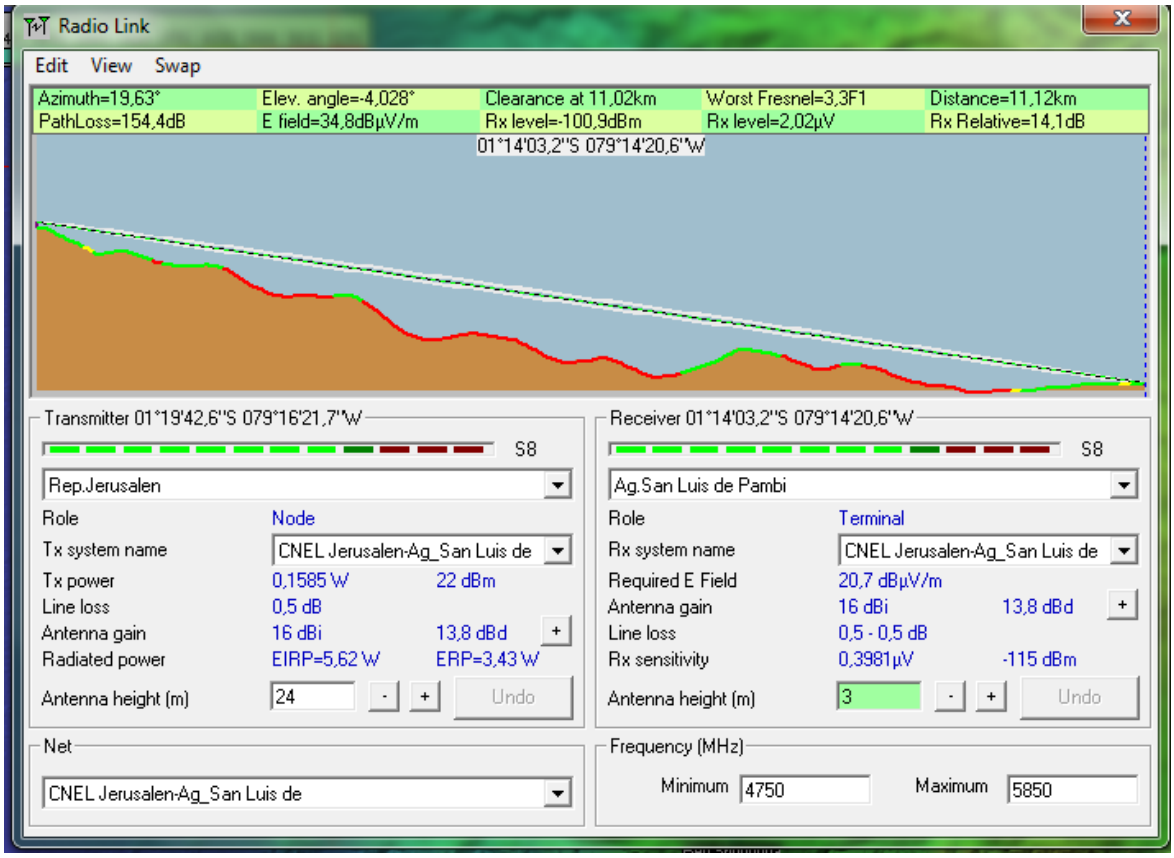


Figura 19A: Enlace Rep.Jerusalen – Ag. San Luis de Pambil

Elaborado por: Roberto Usca, 2017

Enlace Rep. Jerusalen – Ag. Las Naves (5.8Ghz Mikrotik)

Tabla 39A: Ubicación Geográfica Rep.Jerusalen – Ag. Las Naves

NOMBRE	LATITUD	LONGITUD
Rep. Jerusalen (Tx)	1°19'42.14"S	79°16'22.09"O
Ag. Las Naves (Rx)	1°17'12.22"S	79°18'47.99"O

Elaborado por: Roberto Usca, 2017

Tabla 40A: Descripción de Antenas (Tx-Rx) Rep.Jerusalen – Ag. Las Naves

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	24 m	6.48 Km	PTP
Rx	-115dBm	16dBi	3 m	6.48 Km	PTP

Elaborado por: Roberto Usca, 2017

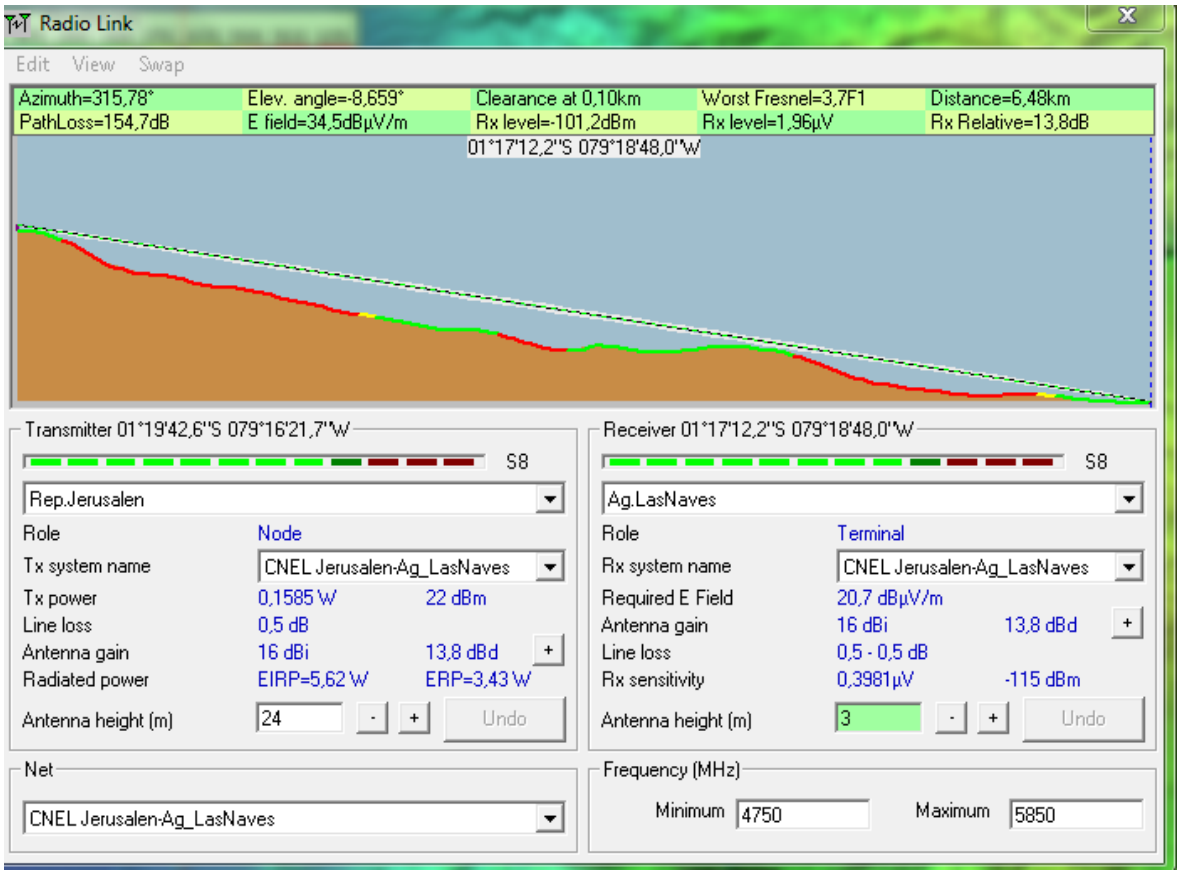


Figura 20A: Enlace Rep.Jerusalen – Ag. Las Naves

Elaborado por: Roberto Usca, 2017

Enlace Rep. Jerusalen – Rep. Campanahurco (5.8 GHz Mikrotik)

Tabla 41A: Ubicación Geográfica Rep.Jerusalen – Rep. Campanahurco

NOMBRE	LATITUD	LONGITUD
Rep. Jerusalen (Tx)	1°19'42.14"S	79°16'22.09"O
Rep. Campanahurco (Rx)	1°16'32.49"S	79° 1'38.79"O

Elaborado por: Roberto Usca, 2017

Tabla 42A: Descripción de Antenas (Tx-Rx) Rep.Jerusalen – Rep. Campanahurco

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	21 m	27.87 Km	PTP
Rx	-115dBm	16dBi	21 m	27.87 Km	PTP

Elaborado por: Roberto Usca, 2017

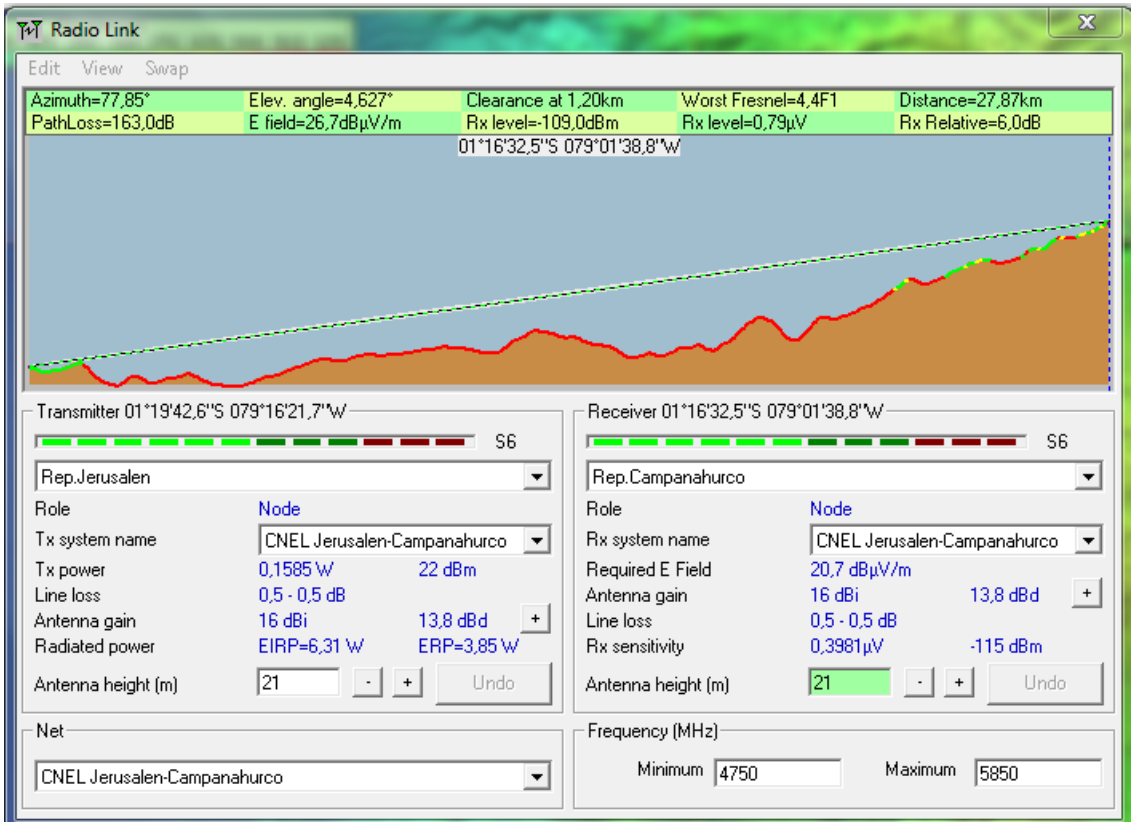


Figura 21A: Enlace Rep.Jerusalen – Rep. Campanahurco

Elaborado por: Roberto Usca, 2017

Enlace Rep. Campanahurco – Ag. Facundo Vela (5.8 GHz Mikrotik)

Tabla 43 A: Ubicación Geográfica Rep. Campanahurco – Ag. Facundo Vela

NOMBRE	LATITUD	LONGITUD
Rep. Campanahurco (Tx)	1°16'32.49"S	79° 1'38.79"O
Ag. Facundo Vela (Rx)	1°11'49.76"S	79° 3'21.84"O

Elaborado por: Roberto Usca, 2017

Tabla 44A: Descripción de Antenas (Tx-Rx) Rep. Campanahurco – Ag. Facundo Vela

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	24 m	9.29 Km	PTP
Rx	-115dBm	16dBi	13 m	9.29 Km	PTP

Elaborado por: Roberto Usca, 2017

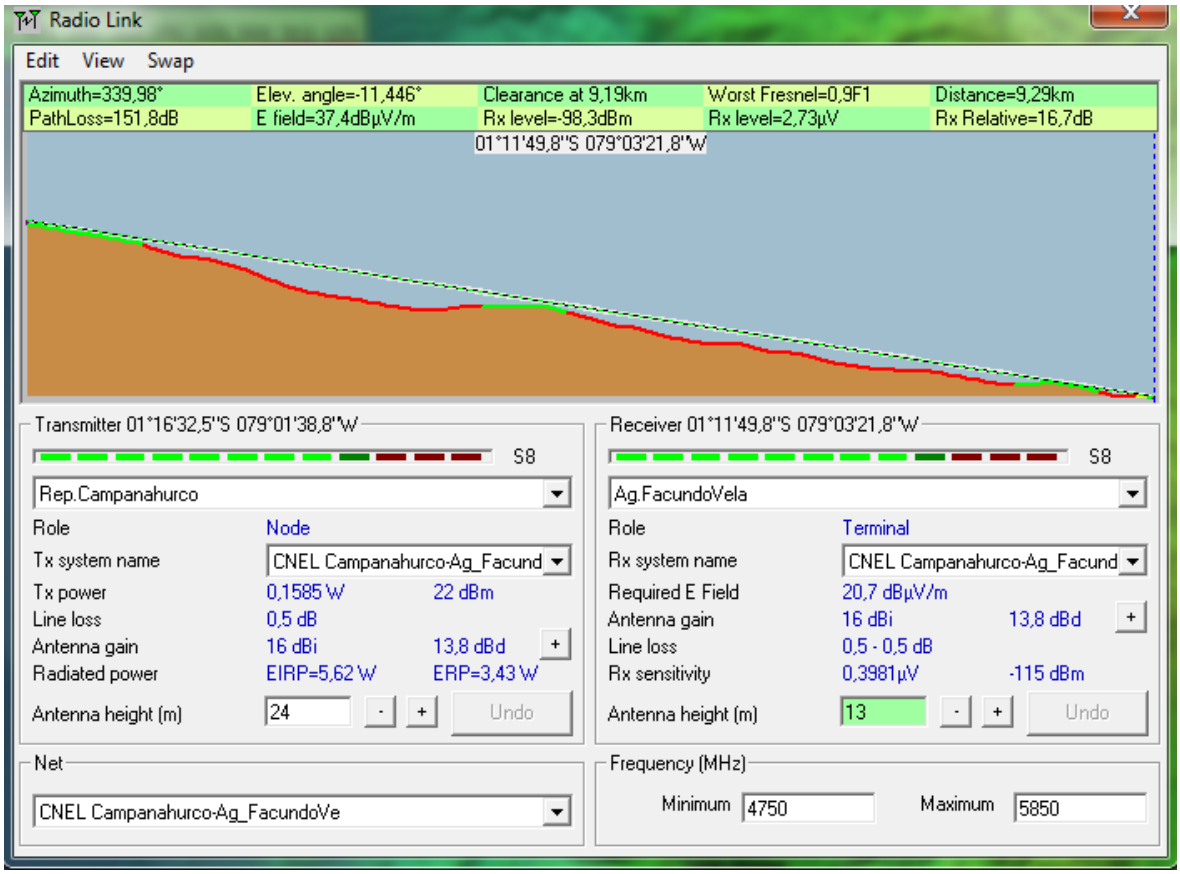


***Figura 22A**:* Enlace Rep. Campanahurco – Ag. Facundo Vela

Elaborado por: Roberto Usca, 2017

Enlace Rep. Campanahurco – Rep. Pimbalo (5.8 GHz Mikrotik)

Tabla 45A: Ubicación Geográfica Rep. Campanahurco – Rep. Pimbalo

NOMBRE	LATITUD	LONGITUD
Rep. Campanahurco (Tx)	1°16'32.49"S	79° 1'38.79"O
Rep. Pimbalo (Rx)	1°17'0.57"S	78°58'10.64"O

Elaborado por: Roberto Usca, 2017

Tabla 46A: Descripción de Antenas (Tx-Rx) Rep. Campanahurco – Rep. Pimbalo

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	24 m	6.48 Km	PTP
Rx	-115dBm	16dBi	24 m	6.48 Km	PTP

Elaborado por: Roberto Usca, 2017

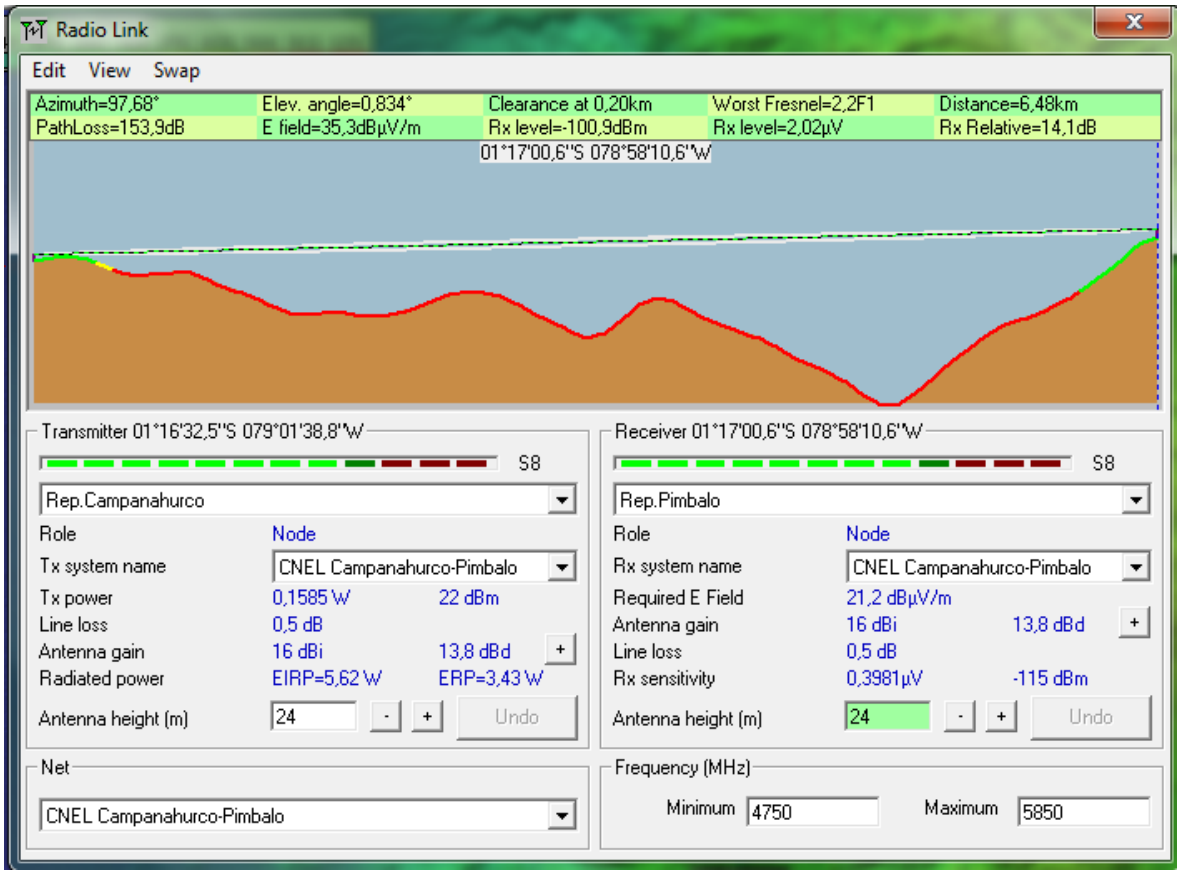


Figura 23A: Enlace Rep. Campanahurco – Rep. Pimbalo

Elaborado por: Roberto Usca, 2017

Enlace Rep. Pimbalo – Ag. Simiatug (5.8 GHz Mikrotik)

Tabla 47A: Ubicación Geográfica Rep. Pimbalo – Ag. Simiatug

NOMBRE	LATITUD	LONGITUD
Rep. Pimbalo (Tx)	1°17'0.57"S	78°58'10.64"O
Ag. Simiatug(Rx)	1°18'0.69"S	78°54'52.34"O

Elaborado por: Roberto Usca, 2017

Tabla 48A: Descripción de Antenas (Tx-Rx) Rep. Pimbalo – Ag. Simiatug

Antena	Potencia	Ganancia	Altura de Antena	Distancia de Enlace	Tipo de Enlace
Tx	22dBm	16dBi	24 m	6.39 Km	PTP
Rx	-115dBm	16dBi	3 m	6.39 Km	PTP

Elaborado por: Roberto Usca, 2017

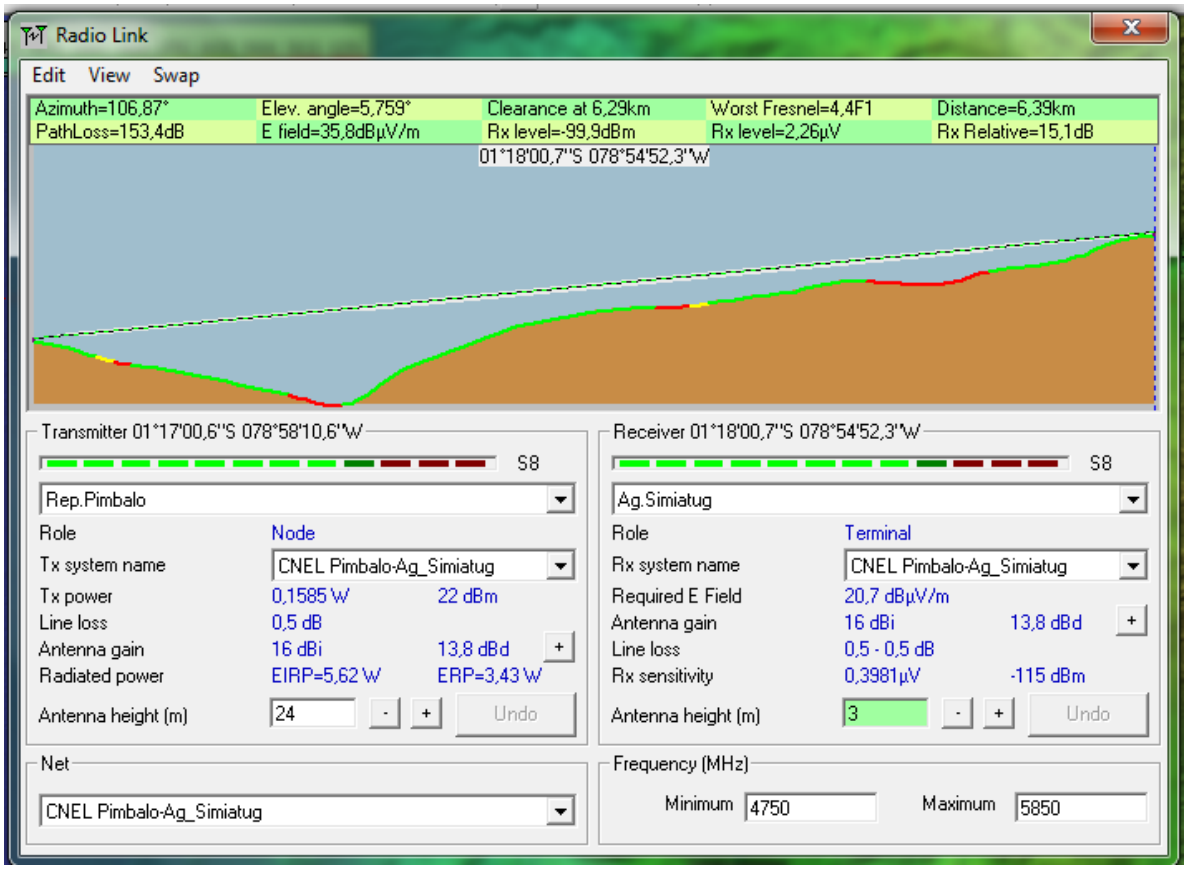


Figura 24A: Enlace Rep. Pimbalo – Ag. Simiatug

Elaborado por: Roberto Usca, 2017

Anexo B. Análisis de radio enlaces on el protocolo MPLS

Enlace Repetidor2-Rep.Campanahurco

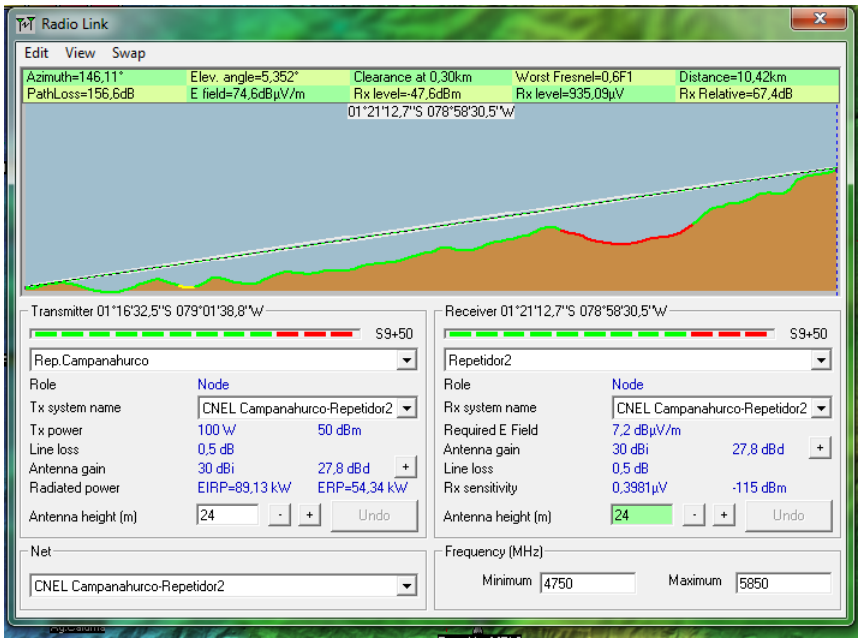


Figura 25A: Enlace Repetidor2-Rep.Campanahurco

Elaborado por: Roberto Usca, 2017

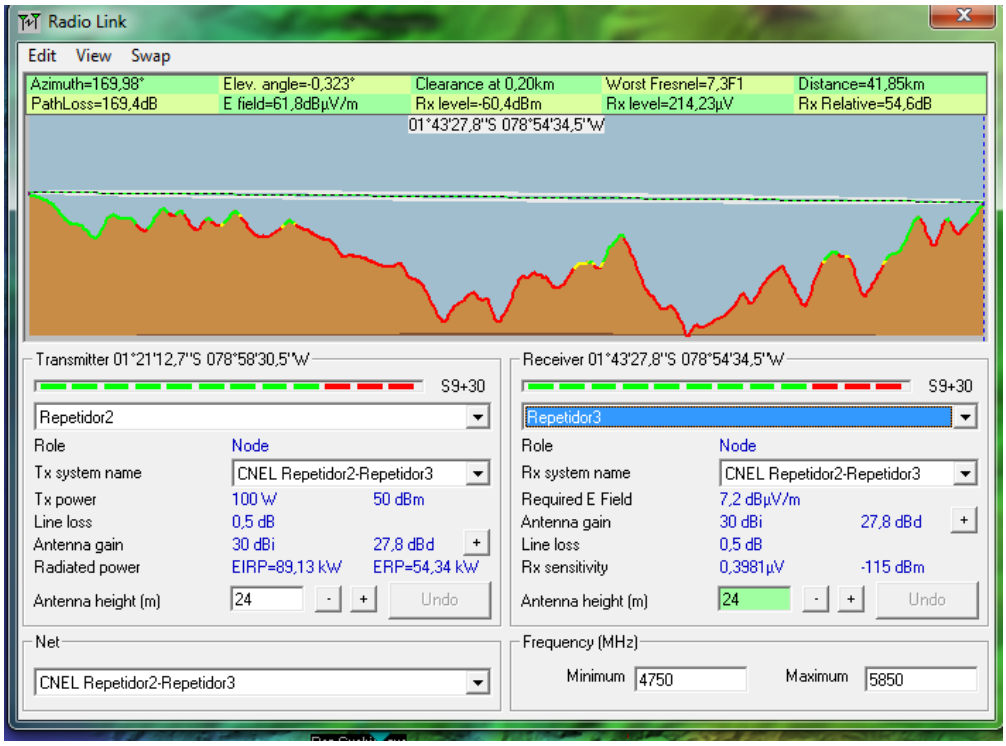


Figura 26A: Enlace Repetidor2-Repetidor3

Elaborado por: Roberto Usca, 2017

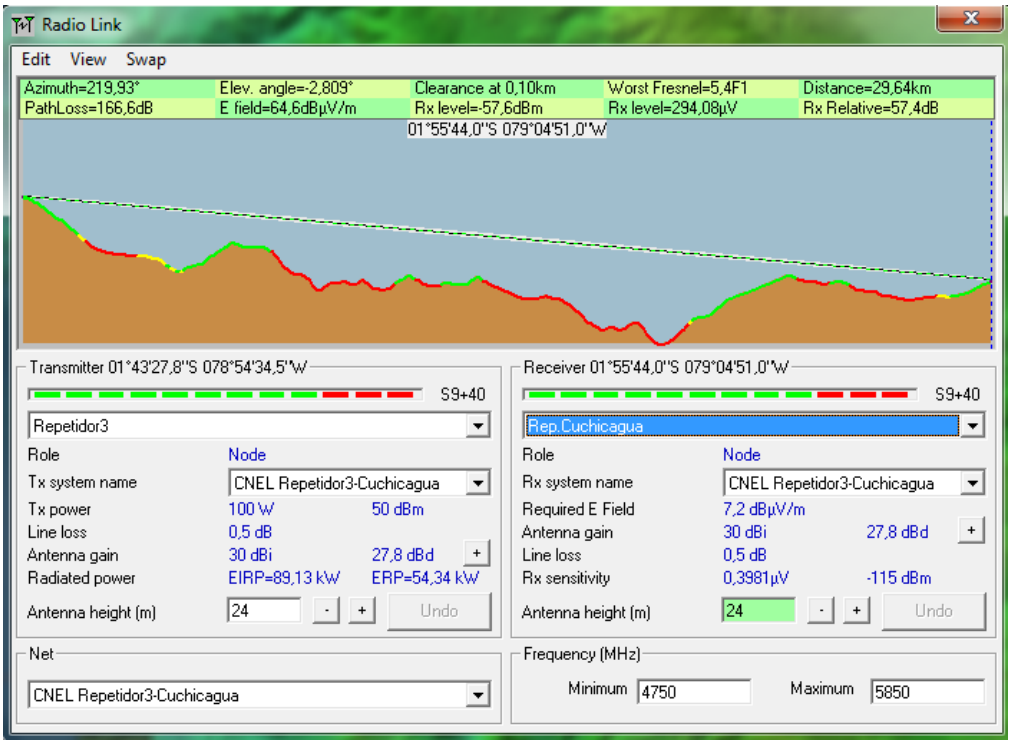


Figura 27A: Enlace Repetidor3-Rep.Cuchicagua

Elaborado por: Roberto Usca, 2017

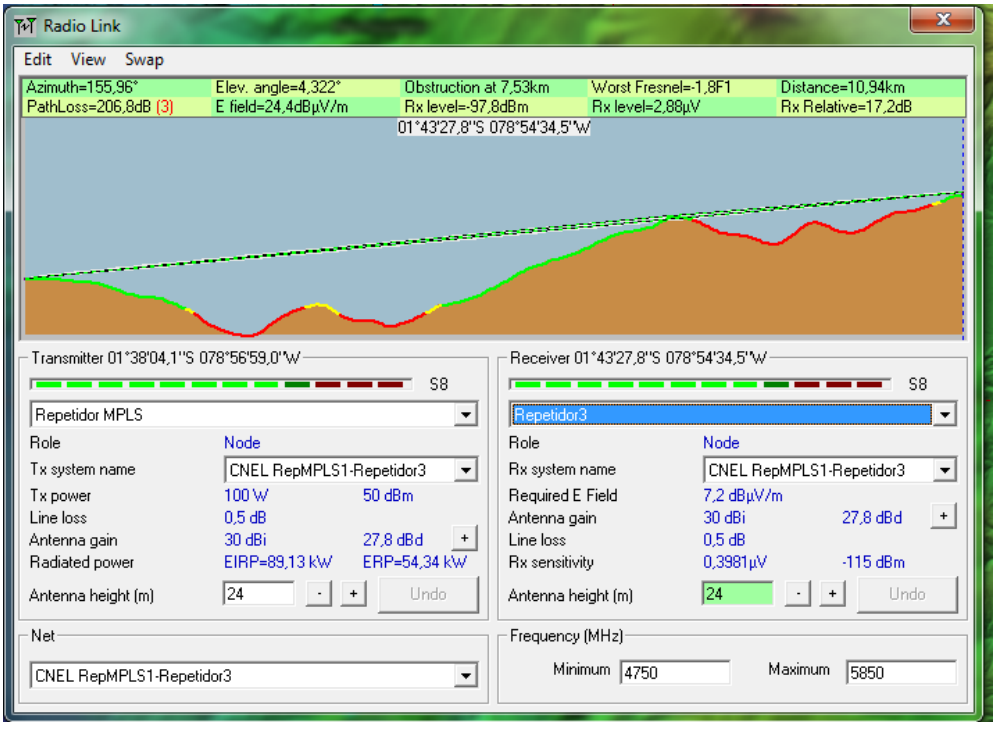


Figura 28A: Enlace Repetidor MPLS-Repetidor3

Elaborado por: Roberto Usca, 2017

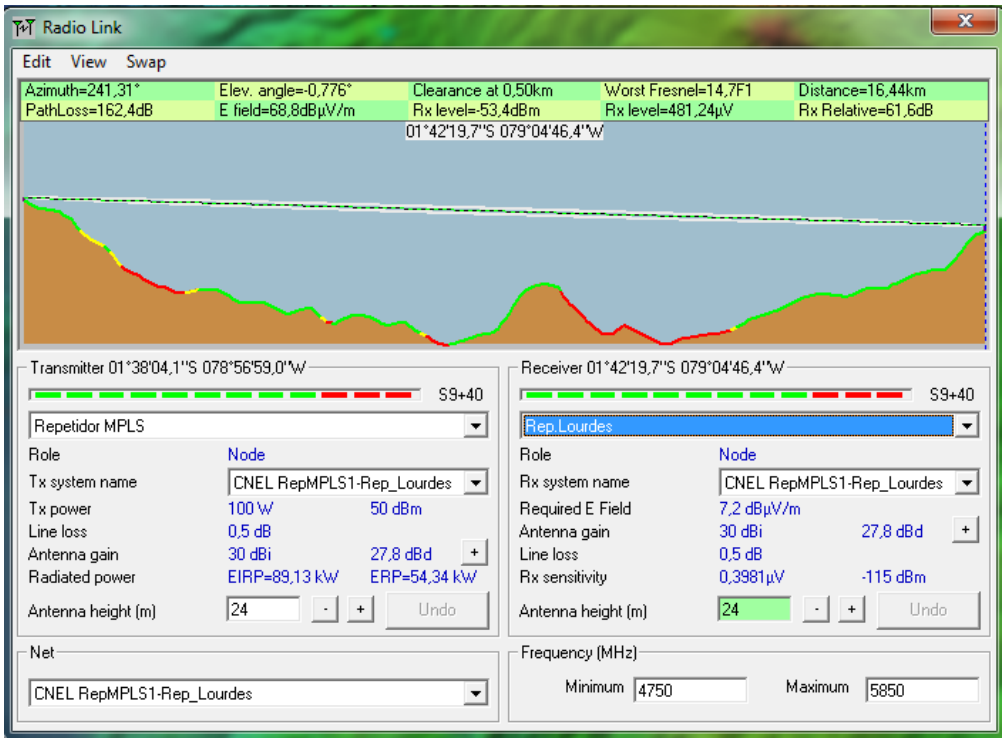


Figura 29A: Enlace repetidor MPLS- Rep. Lourdes

Elaborado por: Roberto Usca, 2017

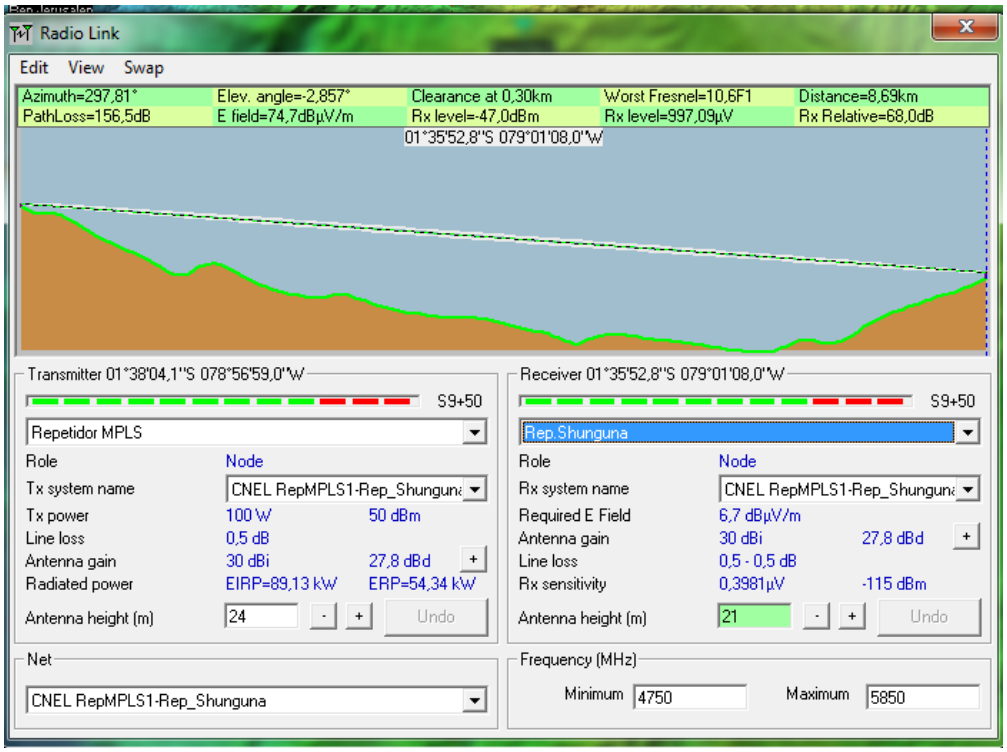


Figura 30A: Enlace Repetidor MPLS-Rep. Shunguna

Elaborado por: Roberto Usca, 2017

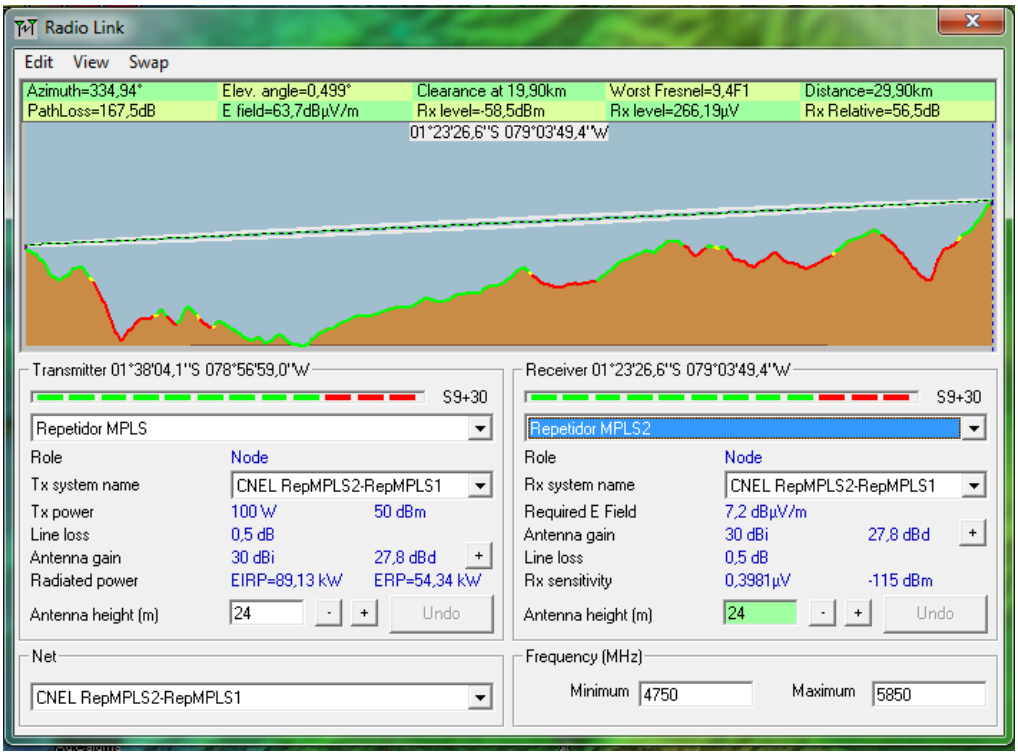


Figura 31A: Enlace Repetidor MPLS-Repetidor MPLS2

Elaborado por: Roberto Usca, 2017

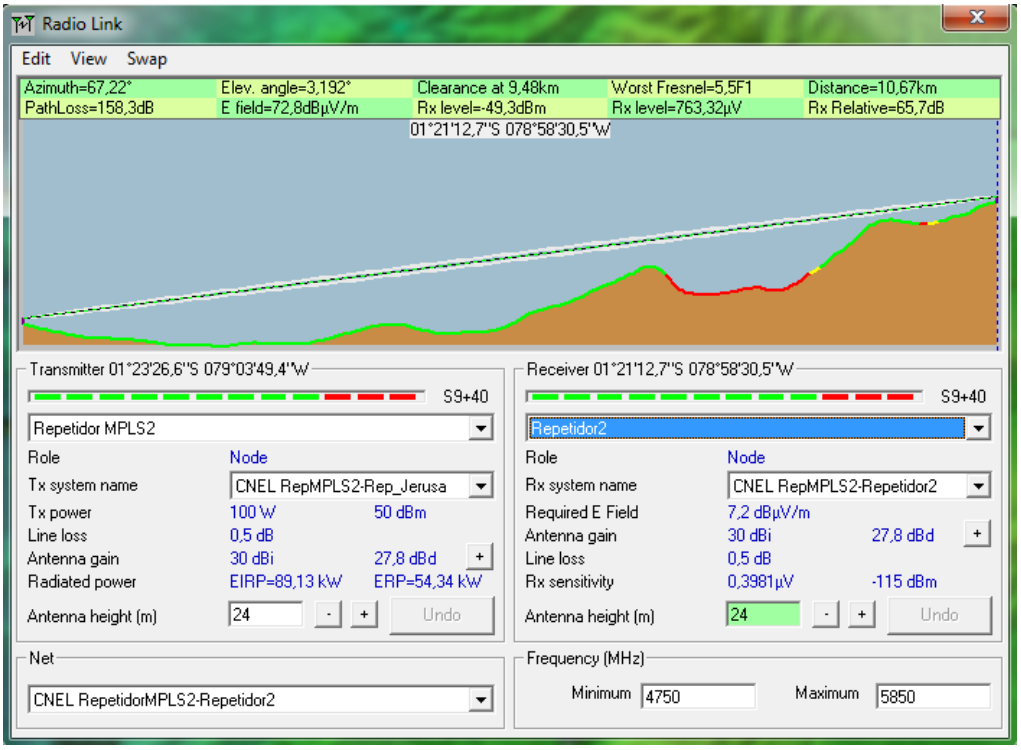


Figura 32A: Enlace Repetidor MPLS2-Repetidor2

Elaborado por: Roberto Usca, 2017

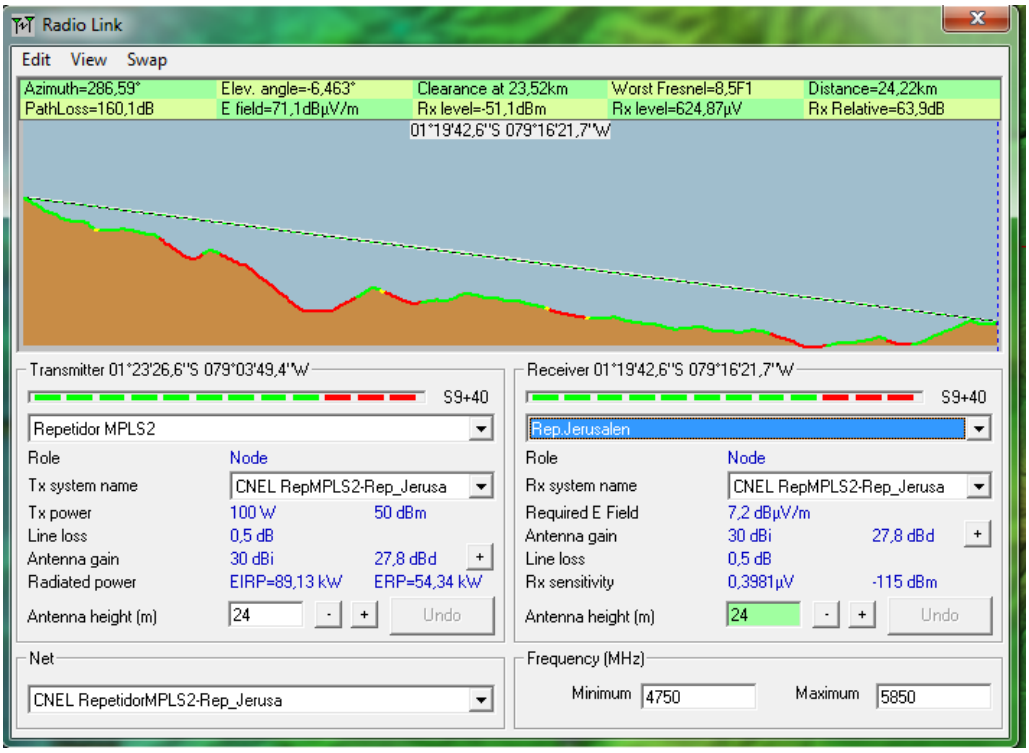


Figura 33A: Enlace Repetidor MPLS2-Rep.Jerusalen

Elaborado por: Roberto Usca, 2017

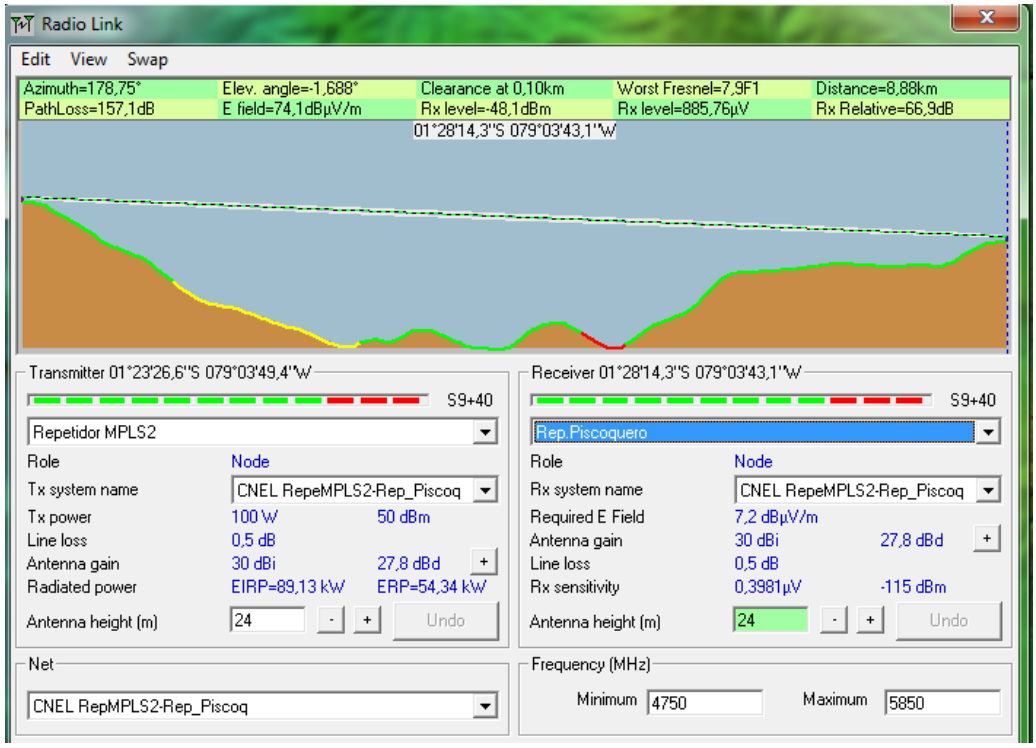


Figura 34A: Enlace Repetidor MPLS2-Rep.Piscoquero

Elaborado por: Roberto Usca, 2017

Anexo C. Valores del nivel de confianza.

Valores de Z nivel de confianza para realizar análisis estadístico con un nivel de 95% de confiabilidad.

Tabla 1. Valores de Z_α para diferentes niveles de confianza

α	Nivel de Confianza (1-α) (%)	Z_α
0,050	95,0	**1,960**
0,025	97,5	**2,240**
0,010	99,0	**2,576**

Tabla 2. Valores de Z_β para diferentes niveles de poder estadístico

β	Poder estadístico (1-β) (%)	Z_β
0,20	80,0	**0,842**
0,15	85,0	**1,036**
0,10	90,0	**1,282**

Anexo D. Direccionamiento de la red

Direccionamiento de la Red

Router	Interfaces	Direccionamiento	Protocolo de enrutamiento	Router Distinguer
P1	Fa1/1	10.10.13.1/24	OSPF 1 AREA 0 MPLS	
	Fa0/0	10.10.12.1/24	OSPF 1 AREA 0 MPLS	
	Fa0/1	10.10.17.1/24	OSPF 1 AREA 0 MPLS	
	Fa1/0	10.10.19.1/24	OSPF 1 AREA 0 MPLS	
	Lookback 0	1.1.1.1/32	OSPF 1 AREA 0 MPLS	
P2	Fa1/1	10.10.24.2/24	OSPF 1 AREA 0 MPLS	
	Fa0/0	10.10.12.2/24	OSPF 1 AREA 0 MPLS	
	Fa0/1	10.10.102.2/24	OSPF 1 AREA 0 MPLS	
	Fa1/0	10.10.28.1/24	OSPF 1 AREA 0 MPLS	
	Lookback 0	2.2.2.2/32	OSPF 1 AREA 0 MPLS	
P3_Rep2	Fa1/1	10.10.13.3/24	OSPF 1 AREA 0 MPLS	
	Fa0/0	10.10.34.3/24	OSPF 1 AREA 0 MPLS	
	Fa0/1	10.10.35.3/24	OSPF 1 AREA 0 MPLS	
	Lookback 0	3.3.3.3/32	OSPF 1 AREA 0 MPLS	
P4_Rep3	Fa1/1	10.10.24.4/24	OSPF 1 AREA 0	

			MPLS	
	Fa0/0	10.10.34.4/24	OSPF 1 AREA 0 MPLS	
	Fa0/1	10.10.36.4/24	OSPF 1 AREA 0 MPLS	
	Lookback 0	4.4.4.4/32	OSPF 1 AREA 0 MPLS	
P5_Rep-Campanahurco	Fa0/0	10.10.57.5/24	OSPF 1 AREA 0 MPLS	
	Fa0/1	10.10.35.5/24	OSPF 1 AREA 0 MPLS	
	Fa1/0	172.17.191.53/30 VRF AgFacundoVela		300:14
	Fa1/1	172.17.191.57/30 VRF AgSimiatug		300:15
	Lookback 0	5.5.5.5/32	OSPF 1 AREA 0 MPLS BGP 100	
P6_Rep-Cuchicagua	Fa0/0	10.10.68.6/24	OSPF 1 AREA 0 MPLS	
	Fa0/1	10.10.36.6/24	OSPF 1 AREA 0 MPLS	
	Fa1/0	172.17.191.25/30 VRF SubSicoto		300:7
	Fa1/1	172.17.191.29/30 VRF AgChillanes		300:8
	Lookback 0	6.6.6.6/32	OSPF 1 AREA 0 MPLS BGP 100	
P7_Rep-Jerusalen	Fa0/0	10.10.57.7/24	OSPF 1 AREA 0 MPLS	
	Fa0/1	10.10.17.7/24	OSPF 1 AREA 0 MPLS	

	Fa1/1	10.10.79.7/24	OSPF 1 AREA 0 MPLS	
	Fa2/0	172.17.191.45/30 VRF AgLasNaves		300:12
	Fa2/1	172.17.191.49/30 VRF AgSLPambil		300:13
	Lookback 0	7.7.7.7/32	OSPF 1 AREA 0 MPLS BGP 100	
P8_Rep-Lourdes	Fa0/0	10.10.68.8/24	OSPF 1 AREA 0 MPLS	
	Fa1/0	10.10.28.8/24	OSPF 1 AREA 0 MPLS	
	Fa1/1	10.10.108.8/24	OSPF 1 AREA 0 MPLS	
	Fa2/0	172.17.191.13/30 VRF AgSanMiguel		300:4
	Fa2/1	172.17.191.17/30 VRF AgBalsapamba		300:5
	Fa3/0	172.17.191.21/30 VRF SubCochabamba		300:6
	Lookback 0	8.8.8.8/32	OSPF 1 AREA 0 MPLS BGP 100	
P9_Rep-Piscoquero	Fa0/0	10.10.109.9/24	OSPF 1 AREA 0 MPLS	
	Fa1/0	10.10.19.9/24	OSPF 1 AREA 0 MPLS	
	Fa1/1	10.10.79.9/24	OSPF 1 AREA 0 MPLS	
	Fa2/0	172.17.191.37/30 VRF AgEcheandia		300:10

	Fa2/1	172.17.191.41/30 VRF AgCaluma		300:11
	Lookback 0	9.9.9.9/32	OSPF 1 AREA 0 MPLS BGP 100	
P10_Rep-Shunguna	Fa0/0	10.10.109.10/24	OSPF 1 AREA 0 MPLS	
	Fa0/1	10.10.102.10/24	OSPF 1 AREA 0 MPLS	
	Fa1/1	10.10.108.10/24	OSPF 1 AREA 0 MPLS	
	Fa2/0	172.17.191.1/30 VRF CNEL-MATRIZ		300:1
	Fa2/1	172.17.191.5/30 VRF AgChimbo		300:2
	Fa3/0	172.17.191.9/30 VRF SubGuaranda		300:3
	Fa3/1	172.17.191.61/30 VRF SubGuanujo		300:16
	Lookback 0	10.10.10.10/32	OSPF 1 AREA 0 MPLS BGP 100	
Ag_SanMiguel	Fa0/0	172.17.191.14/30		
	Fa1/0	192.168.4.1/24	BGP 104	
Ag_Balsapamba	Fa0/0	172.17.191.18/30		
	Fa1/0	192.168.5.1/24	BGP 105	
Ag_Cochabamba	Fa0/0	172.17.191.22/30		
	Fa1/0	192.168.6.1/24	BGP 106	
Sub_Sicoto	Fa0/0	172.17.191.26/30		
	Fa1/0	192.168.7.1/24	BGP 107	
Ag_Chillanes	Fa0/0	172.17.191.30/30		
	Fa1/0	192.168.8.1/24	BGP 108	

Ag_ElTambo	Fa0/0	172.17.191.34/30		
	Fa1/0	192.168.9.1/24	BGP 109	
Ag_Echeandia	Fa0/0	172.17.191.38/30		
	Fa1/0	192.168.10.1/24	BGP 110	
Ag_Caluma	Fa0/0	172.17.191.42/30		
	Fa1/0	192.168.11.1/24	BGP 111	
Ag_LasNaves	Fa0/0	172.17.191.46/30		
	Fa1/0	192.168.12.1/24	BGP 112	
Ag_SLPambil	Fa0/0	172.17.191.50/30		
	Fa1/0	192.168.13.1/24	BGP 113	
Ag_FacundoVela	Fa0/0	172.17.191.54/30		
	Fa1/0	192.168.14.1/24	BGP 114	
Ag_Simiatug	Fa0/0	172.17.191.58/30		
	Fa1/0	192.168.15.1/24	BGP 115	
CNEL_MATRIZ	Fa0/0	172.17.191.2/30		
	Fa1/0	192.168.1.1/24	BGP 101	
Ag_Chimbo	Fa0/0	172.17.191.6/30		
	Fa1/0	192.168.2.1/24	BGP 102	
Sub_Guaranda	Fa0/0	172.17.191.10/30		
	Fa1/0	192.168.3.1/24	BGP 103	
Sub_Guanujo	Fa0/0	172.17.191.62/30		
	Fa1/0	192.168.16.1/24	BGP 116	
Servidor Datos	Ethernet 0	192.168.1.2/24		
Servidor Video	Ethernet 0	192.168.1.3/24		
Servidor Voz	Ethernet 0	192.168.1.4/24		
PC	Ethernet 0	192.168.2.2/24 192.168.3.2/24 192.168.4.2/24 192.168.5.2/24 192.168.6.2/24 192.168.7.2/24 192.168.8.2/24 192.168.9.2/24		

		192.168.10.2/24 192.168.11.2/24 192.168.12.2/24 192.168.13.2/24 192.168.14.2/24 192.168.15.2/24 192.168.16.2/24		

Anexo E. Configuración de P1, P2 CORE MPLS

----------Configuracion de CNEL-MPLS----------

P1(Antena uno)

---

config t

int f1/1

ip add 10.10.13.1 255.255.255.0

no shut

int f0/0

ip add 10.10.12.1 255.255.255.0

no shut

int f0/1

ip add 10.10.17.1 255.255.255.0

no shut

int f1/0

ip add 10.10.19.1 255.255.255.0

no shut

int lo 0

ip add 1.1.1.1 255.255.255.255

no shut

router ospf 1

router-id 1.1.1.1

network 10.10.0.0 0.0.255.255 area 0

network 1.1.1.1 0.0.0.0 area 0

mpls ip

mpls ldp router-id loopback 0

router ospf 1

mpls ldp autoconfig

P2 (Antena dos)

---

config t

int f1/1

ip add 10.10.24.2 255.255.255.0

no shut

int f0/0

ip add 10.10.12.2 255.255.255.0

no shut

int f0/1

ip add 10.10.102.2 255.255.255.0

no shut

int f1/0

ip add 10.10.28.2 255.255.255.0

no shut

int lo 0

ip add 2.2.2.2 255.255.255.255

no shut

```
router ospf 1
router-id 2.2.2.2
network 10.10.0.0 0.0.255.255 area 0
network 2.2.2.2 0.0.0.0 area 0

mpls ip
mpls ldp router-id loopback 0
router ospf 1
mpls ldp autoconfig
```

```
router ospf 1
router-id 3.3.3.3
network 10.10.0.0 0.0.255.255 area 0
network 3.3.3.3 0.0.0.0 area 0

mpls ip
mpls ldp router-id loopback 0
router ospf 1
mpls ldp autoconfig
```

P3_Rep2

```
config t
int f1/1
ip add 10.10.13.3 255.255.255.0
no shut

int f0/0
ip add 10.10.34.3 255.255.255.0
no shut

int f0/1
ip add 10.10.35.3 255.255.255.0
no shut

int lo 0
ip add 3.3.3.3 255.255.255.255
no shut
```

P4_Rep3

```
config t
int f1/1
ip add 10.10.24.4 255.255.255.0
no shut

int f0/0
ip add 10.10.34.4 255.255.255.0
no shut

int f0/1
ip add 10.10.36.4 255.255.255.0
no shut

int lo 0
ip add 4.4.4.4 255.255.255.255
no shut
```

router ospf 1
router-id 4.4.4.4
network 10.10.0.0 0.0.255.255 area 0
network 4.4.4.4 0.0.0.0 area 0

mpls ip
mpls ldp router-id loopback 0
router ospf 1
mpls ldp autoconfig

P5_Rep-Campanahurco

---

config t

int f0/0
ip add 10.10.57.5 255.255.255.0
no shut

int f0/1
ip add 10.10.35.5 255.255.255.0
no shut

int lo 0
ip add 5.5.5.5 255.255.255.255
no shut

router ospf 1
router-id 5.5.5.5
network 10.10.0.0 0.0.255.255 area 0
network 5.5.5.5 0.0.0.0 area 0

mpls ip
mpls ldp router-id loopback 0
router ospf 1
mpls ldp autoconfig

ip vrf AgFacundoVela
rd 300:14
route-target export 1:1
route-target import 2:2
exit

ip vrf AgSimiatug
rd 300:15
route-target export 1:1
route-target import 2:2
exit

int fa1/0
ip vrf forwarding AgFacundoVela
ip add 172.17.191.53 255.255.255.252
no shut
exit

int fa1/1
ip vrf forwarding AgSimiatug
ip add 172.17.191.57 255.255.255.252
no shut

exit

router bgp 100

bgp router-id 5.5.5.5

neighbor 10.10.10.10 remote-as 100

neighbor 10.10.10.10 update-source Loopback0

exit

router bgp 100

address-family vpnv4 unicast

neighbor 10.10.10.10 activate

exit

router bgp 100

address-family ipv4 unicast vrf AgFacundoVela

neighbor 172.17.191.54 remote-as 114

neighbor 172.17.191.54 activate

exit

address-family ipv4 unicast vrf AgSimiatug

neighbor 172.17.191.58 remote-as 115

neighbor 172.17.191.58 activate

exit

P6_Rep-Cuchicagua

---

config t

int f0/0

ip add 10.10.68.6 255.255.255.0

no shut

int f0/1

ip add 10.10.36.6 255.255.255.0

no shut

int lo 0

ip add 6.6.6.6 255.255.255.255

no shut

router ospf 1

router-id 6.6.6.6

network 10.10.0.0 0.0.255.255 area 0

network 6.6.6.6 0.0.0.0 area 0

mpls ip

mpls ldp router-id loopback 0

router ospf 1

mpls ldp autoconfig

ip vrf SubSicoto

rd 300:7

route-target export 1:1

route-target import 2:2

exit

ip vrf AgChillanes

rd 300:8

route-target export 1:1

route-target import 2:2

exit

ip vrf AgElTambo

rd 300:9

route-target export 1:1

route-target import 2:2

exit

int f1/0

ip vrf forwarding SubSicoto

ip add 172.17.191.25 255.255.255.252

no shut

int f1/1

ip vrf forwarding AgChillanes

ip add 172.17.191.29 255.255.255.252

no shut

int f2/0

ip vrf forwarding AgElTambo

ip add 172.17.191.33 255.255.255.252

no shut

router bgp 100

bgp router-id 6.6.6.6

neighbor 10.10.10.10 remote-as 100

neighbor 10.10.10.10 update-source Loopback0

exit

router bgp 100

address-family vpnv4 unicast

neighbor 10.10.10.10 activate

exit

router bgp 100

address-family ipv4 unicast vrf SubSicoto

neighbor 172.17.191.26 remote-as 107

neighbor 172.17.191.26 activate

exit

address-family ipv4 unicast vrf AgChillanes

neighbor 172.17.191.30 remote-as 108

neighbor 172.17.191.30 activate

exit

address-family ipv4 unicast vrf AgElTambo

neighbor 172.17.191.34 remote-as 109

neighbor 172.17.191.34 activate

exit

P7_Rep-Jerusalen

---

config t

int f0/0

ip add 10.10.57.7 255.255.255.0

no shut

```
int f0/1
ip add 10.10.17.7 255.255.255.0
no shut

int f1/1
ip add 10.10.79.7 255.255.255.0
no shut

int lo 0
ip add 7.7.7.7 255.255.255.255
no shut

router ospf 1
router-id 7.7.7.7
network 10.10.0.0 0.0.255.255 area 0
network 7.7.7.7 0.0.0.0 area 0

mpls ip
mpls ldp router-id loopback 0
router ospf 1
mpls ldp autoconfig

ip vrf AgLasNaves
rd 300:12
route-target export 1:1
route-target import 2:2
exit

ip vrf AgSLPambil
rd 300:13
route-target export 1:1
route-target import 2:2
exit

int fa2/0
ip vrf forwarding AgLasNaves
ip add 172.17.191.45 255.255.255.252
no shut
exit

int fa2/1
ip vrf forwarding AgSLPambil
ip add 172.17.191.49 255.255.255.252
no shut
exit

router bgp 100
 bgp router-id 7.7.7.7
 neighbor 10.10.10.10 remote-as 100
 neighbor 10.10.10.10 update-source Loopback0
exit

router bgp 100
address-family vpnv4 unicast
neighbor 10.10.10.10 activate
exit

router bgp 100
```

address-family ipv4 unicast vrf AgLasNaves

neighbor 172.17.191.46 remote-as 112

neighbor 172.17.191.46 activate

exit

address-family ipv4 unicast vrf AgSLPambil

neighbor 172.17.191.50 remote-as 113

neighbor 172.17.191.50 activate

exit

P8_Rep-Lourdes

---

config t

int f0/0

ip add 10.10.68.8 255.255.255.0

no shut

int f1/0

ip add 10.10.28.8 255.255.255.0

no shut

int f1/1

ip add 10.10.108.8 255.255.255.0

no shut

int lo 0

ip add 8.8.8.8 255.255.255.255

no shut

router ospf 1

router-id 8.8.8.8

network 10.10.0.0 0.0.255.255 area 0

network 8.8.8.8 0.0.0.0 area 0

mpls ip

mpls ldp router-id loopback 0

router ospf 1

mpls ldp autoconfig

ip vrf AgSanMiguel

rd 300:4

route-target export 1:1

route-target import 2:2

exit

ip vrf AgBalsapamba

rd 300:5

route-target export 1:1

route-target import 2:2

exit

ip vrf SubCochabamba

rd 300:6

route-target export 1:1

route-target import 2:2

exit

int fa2/0

ip vrf forwarding AgSanMiguel

ip add 172.17.191.13 255.255.255.252

no shut

exit

int fa2/1

ip vrf forwarding AgBalsapamba

ip add 172.17.191.17 255.255.255.252

no shut

exit

int fa3/0

ip vrf forwarding SubCochabamba

ip add 172.17.191.21 255.255.255.252

no shut

exit

router bgp 100

bgp router-id 8.8.8.8

neighbor 10.10.10.10 remote-as 100

neighbor 10.10.10.10 update-source Loopback0

exit

router bgp 100

address-family vpnv4 unicast

neighbor 10.10.10.10 activate

exit

router bgp 100

address-family ipv4 unicast vrf AgSanMiguel

neighbor 172.17.191.14 remote-as 104

neighbor 172.17.191.14 activate

exit

address-family ipv4 unicast vrf AgBalsapamba

neighbor 172.17.191.18 remote-as 105

neighbor 172.17.191.18 activate

exit

address-family ipv4 unicast vrf SubCochabamba

neighbor 172.17.191.22 remote-as 106

neighbor 172.17.191.22 activate

exit

P9_Rep-Piscoquero

---

config t

int f0/0

ip add 10.10.109.9 255.255.255.0

no shut

int f1/0

ip add 10.10.19.9 255.255.255.0

no shut

int f1/1

ip add 10.10.79.9 255.255.255.0

no shut

```
int lo 0
ip add 9.9.9.9 255.255.255.255
no shut

router ospf 1
router-id 9.9.9.9
network 10.10.0.0 0.0.255.255 area 0
network 9.9.9.9 0.0.0.0 area 0

mpls ip
mpls ldp router-id loopback 0
router ospf 1
mpls ldp autoconfig

ip vrf AgEcheandia
rd 300:10
route-target export 1:1
route-target import 2:2
exit

ip vrf AgCaluma
rd 300:11
route-target export 1:1
route-target import 2:2
exit

int fa2/0
ip vrf forwarding AgEcheandia
ip add 172.17.191.37 255.255.255.252
no shut
exit

int fa2/1
ip vrf forwarding AgCaluma
ip add 172.17.191.41 255.255.255.252
no shut
exit

router bgp 100
 bgp router-id 9.9.9.9
 neighbor 10.10.10.10 remote-as 100
 neighbor 10.10.10.10 update-source Loopback0
exit

router bgp 100
address-family vpnv4 unicast
neighbor 10.10.10.10 activate
exit

router bgp 100
address-family ipv4 unicast vrf AgEcheandia
neighbor 172.17.191.38 remote-as 110
neighbor 172.17.191.38 activate
exit

address-family ipv4 unicast vrf AgCaluma
neighbor 172.17.191.42 remote-as 111
neighbor 172.17.191.42 activate
```

exit

mpls ldp autoconfig

P10_Rep-Shunguna

---

config t

int f0/0

ip add 10.10.109.10 255.255.255.0

no shut

int f0/1

ip add 10.10.102.10 255.255.255.0

no shut

int f1/1

ip add 10.10.108.10 255.255.255.0

no shut

int lo 0

ip add 10.10.10.10 255.255.255.255

no shut

router ospf 1

router-id 10.10.10.10

network 10.10.0.0 0.0.255.255 area 0

network 10.10.10.10 0.0.0.0 area 0

mpls ip

mpls ldp router-id loopback 0

router ospf 1

ip vrf CNEL-MATRIZ

rd 300:1

route-target export 2:2

route-target import 1:1

exit

ip vrf AgChimbo

rd 300:2

route-target export 1:1

route-target import 2:2

exit

ip vrf SubGuaranda

rd 300:3

route-target export 1:1

route-target import 2:2

exit

ip vrf SubGuanujo

rd 300:16

route-target export 1:1

route-target import 2:2

exit

int f2/0

ip vrf forwarding CNEL-MATRIZ

ip add 172.17.191.1 255.255.255.252

```
no shut
exit

int f2/1
ip vrf forwarding AgChimbo
ip add 172.17.191.5 255.255.255.252
no shut
exit

int f3/0
ip vrf forwarding SubGuaranda
ip add 172.17.191.9 255.255.255.252
no shut
exit

int f3/1
ip vrf forwarding SubGuanujo
ip add 172.17.191.61 255.255.255.252
no shut
exit

router bgp 100
 bgp router-id 10.10.10.10
 neighbor 5.5.5.5 remote-as 100
 neighbor 5.5.5.5 update-source Loopback0

 neighbor 6.6.6.6 remote-as 100
 neighbor 6.6.6.6 update-source Loopback0

 neighbor 7.7.7.7 remote-as 100
 neighbor 7.7.7.7 update-source Loopback0

 neighbor 8.8.8.8 remote-as 100
 neighbor 8.8.8.8 update-source Loopback0

 neighbor 9.9.9.9 remote-as 100
 neighbor 9.9.9.9 update-source Loopback0

 exit

router bgp 100

 address-family vpnv4 unicast
 neighbor 5.5.5.5 activate

 address-family vpnv4 unicast
 neighbor 6.6.6.6 activate

 address-family vpnv4 unicast
 neighbor 7.7.7.7 activate

 address-family vpnv4 unicast
 neighbor 8.8.8.8 activate

 address-family vpnv4 unicast
 neighbor 9.9.9.9 activate
 exit
```

router bgp 100

address-family ipv4 unicast vrf CNEL-MATRIZ

neighbor 172.17.191.2 remote-as 101

neighbor 172.17.191.2 activate

exit

router bgp 100

address-family ipv4 unicast vrf AgChimbo

neighbor 172.17.191.6 remote-as 102

neighbor 172.17.191.6 activate

exit

router bgp 100

address-family ipv4 unicast vrf SubGuaranda

neighbor 172.17.191.10 remote-as 103

neighbor 172.17.191.10 activate

exit

router bgp 100

address-family ipv4 unicast vrf SubGuanujo

neighbor 172.17.191.62 remote-as 116

neighbor 172.17.191.62 activate

exit

---------Ag_SanMiguel----------

config t

int f0/0

ip add 172.17.191.14 255.255.255.252

no shut

exit

int fa1/0

ip add 192.168.4.1 255.255.255.0

no shut

exit

router bgp 104

neighbor 172.17.191.13 remote-as 100

network 192.168.4.0 mask 255.255.255.0

exit

---------Ag_Balsapamba----------

config t

int f0/0

ip add 172.17.191.18 255.255.255.252

no shut

exit

int fa1/0

ip add 192.168.5.1 255.255.255.0

no shut

exit

router bgp 105

neighbor 172.17.191.17 remote-as 100

network 192.168.5.0 mask 255.255.255.0

exit

---------Ag_Cochabamba----------
-
config t
int f0/0
ip add 172.17.191.22 255.255.255.252
no shut
exit

int fa1/0
ip add 192.168.6.1 255.255.255.0
no shut
exit

router bgp 106
neighbor 172.17.191.21 remote-as 100
network 192.168.6.0 mask
255.255.255.0
exit

---------Sub_Sicoto----------
config t
int f0/0
ip add 172.17.191.26 255.255.255.252
no shut
exit

int fa1/0
ip add 192.168.7.1 255.255.255.0
no shut
exit

router bgp 107
neighbor 172.17.191.25 remote-as 100
network 192.168.7.0 mask
255.255.255.0
exit

---------Ag_Chillanes----------
config t
int f0/0
ip add 172.17.191.30 255.255.255.252
no shut
exit

int fa1/0
ip add 192.168.8.1 255.255.255.0
no shut
exit

router bgp 108
neighbor 172.17.191.29 remote-as 100
network 192.168.8.0 mask
255.255.255.0
exit

---------Ag_ElTambo----------
config t
int f0/0
ip add 172.17.191.34 255.255.255.252
no shut

exit

int fa1/0

ip add 192.168.9.1 255.255.255.0

no shut

exit

router bgp 109

neighbor 172.17.191.33 remote-as 100

network 192.168.9.0 mask 255.255.255.0

exit

---------Ag_Echeandia----------

config t

int f0/0

ip add 172.17.191.38 255.255.255.252

no shut

exit

int f1/0

ip add 192.168.10.1 255.255.255.0

no shut

exit

router bgp 110

neighbor 172.17.191.37 remote-as 100

network 192.168.10.0 mask 255.255.255.0

exit

---------Ag_Caluma----------

config t

int f0/0

ip add 172.17.191.42 255.255.255.252

no shut

exit

int f1/0

ip add 192.168.11.1 255.255.255.0

no shut

exit

router bgp 111

neighbor 172.17.191.41 remote-as 100

network 192.168.11.0 mask 255.255.255.0

exit

---------Ag_LasNaves----------

config t

int f0/0

ip add 172.17.191.46 255.255.255.252

no shut

exit

int f1/0

ip add 192.168.12.1 255.255.255.0

no shut

exit

router bgp 112

neighbor 172.17.191.45 remote-as 100

network 192.168.12.0 mask 255.255.255.0

exit

---------Ag_SLPambil----------

config t

int f0/0

ip add 172.17.191.50 255.255.255.252

no shut

exit

int f1/0

ip add 192.168.13.1 255.255.255.0

no shut

exit

router bgp 113

neighbor 172.17.191.49 remote-as 100

network 192.168.13.0 mask 255.255.255.0

exit

---------Ag_FacundoVela----------

config t

int f0/0

ip add 172.17.191.54 255.255.255.252

no shut

exit

int fa1/0

ip add 192.168.14.1 255.255.255.0

no shut

exit

router bgp 114

neighbor 172.17.191.53 remote-as 100

network 192.168.14.0 mask 255.255.255.0

exit

---------Ag_Simiatug----------

config t

int f0/0

ip add 172.17.191.58 255.255.255.252

no shut

exit

int fa1/0

ip add 192.168.15.1 255.255.255.0

no shut

exit

router bgp 115

neighbor 172.17.191.57 remote-as 100

network 192.168.15.0 mask 255.255.255.0

exit

---------CNEL_MATRIZ----------

config t

int f0/0

ip add 172.17.191.2 255.255.255.252

no shut

exit

int fa1/0

ip add 192.168.1.1 255.255.255.0

no shut

exit

router bgp 101

neighbor 172.17.191.1 remote-as 100

network 192.168.1.0 mask 255.255.255.0

exit

---------Ag_Chimbo----------

config t

int f0/0

ip add 172.17.191.6 255.255.255.252

no shut

exit

int fa1/0

ip add 192.168.2.1 255.255.255.0

no shut

exit

router bgp 102

neighbor 172.17.191.5 remote-as 100

network 192.168.2.0 mask 255.255.255.0

exit

---------Sub_Guaranda----------

config t

int f0/0

ip add 172.17.191.10 255.255.255.252

no shut

exit

int fa1/0

ip add 192.168.3.1 255.255.255.0

no shut

exit

router bgp 103

neighbor 172.17.191.9 remote-as 100

network 192.168.3.0 mask 255.255.255.0

exit

---------Sub_Guanujo----------

config t

int f0/0

ip add 172.17.191.62 255.255.255.252

no shut

exit

int fa1/0

```
ip add 192.168.16.1 255.255.255.0
no shut
exit
```

```
router bgp 116
neighbor 172.17.191.61 remote-as 100
network 192.168.16.0 mask 255.255.255.0
exit
```

Anexo F. Tabla de valor F de Fisher 95% de confianza

IV. Puntos porcentuales de la distribución F (*continuación*)

$F_{0.05,\nu_1,\nu_2}$

ν_2 \ ν_1	Grados de libertad del numerador (ν_1)																		
Grados de libertad del denominador (ν_2)	1	2	3	4	5	6	7	8	9	10	12	15	20	24	30	40	60	120	∞
	161.4	199.5	215.7	224.6	230.2	234.0	236.8	238.9	240.5	241.9	243.9	245.9	248.0	249.1	250.1	251.1	252.2	253.3	254.3
2	18.51	19.00	19.16	19.25	19.30	19.33	19.35	19.37	19.38	19.40	19.41	19.43	19.45	19.45	19.46	19.47	19.48	19.49	19.50
3	10.13	9.55	9.28	9.12	9.01	8.94	8.89	8.85	8.81	8.79	8.74	8.70	8.66	8.64	8.62	8.59	8.57	8.55	8.53
4	7.71	6.94	6.59	6.39	6.26	6.16	6.09	6.04	6.00	5.96	5.91	5.86	5.80	5.77	5.75	5.72	5.69	5.66	5.63
5	6.61	5.79	5.41	5.19	5.05	4.95	4.88	4.82	4.77	4.74	4.68	4.62	4.56	4.53	4.50	4.46	4.43	4.40	4.36
6	5.99	5.14	4.76	4.53	4.39	4.28	4.21	4.15	4.10	4.06	4.00	3.94	3.87	3.84	3.81	3.77	3.74	3.70	3.67
7	5.59	4.74	4.35	4.12	3.97	3.87	3.79	3.73	3.68	3.64	3.57	3.51	3.44	3.41	3.38	3.34	3.30	3.27	3.23
8	5.32	4.46	4.07	3.84	3.69	3.58	3.50	3.44	3.39	3.35	3.28	3.22	3.15	3.12	3.08	3.04	3.01	2.97	2.93
9	5.12	4.26	3.86	3.63	3.48	3.37	3.29	3.23	3.18	3.14	3.07	3.01	2.94	2.90	2.86	2.83	2.79	2.75	2.71
10	4.96	4.10	3.71	3.48	3.33	3.22	3.14	3.07	3.02	2.98	2.91	2.85	2.77	2.74	2.70	2.66	2.62	2.58	2.54
11	4.84	3.98	3.59	3.36	3.20	3.09	3.01	2.95	2.90	2.85	2.79	2.72	2.65	2.61	2.57	2.53	2.49	2.45	2.40
12	4.75	3.89	3.49	3.26	3.11	3.00	2.91	2.85	2.80	2.75	2.69	2.62	2.54	2.51	2.47	2.43	2.38	2.34	2.30
13	4.67	3.81	3.41	3.18	3.03	2.92	2.83	2.77	2.71	2.67	2.60	2.53	2.46	2.42	2.38	2.34	2.30	2.25	2.21
14	4.60	3.74	3.34	3.11	2.96	2.85	2.76	2.70	2.65	2.60	2.53	2.46	2.39	2.35	2.31	2.27	2.22	2.18	2.13
15	4.54	3.68	3.29	3.06	2.90	2.79	2.71	2.64	2.59	2.54	2.48	2.40	2.33	2.29	2.25	2.20	2.16	2.11	2.07
16	4.49	3.63	3.24	3.01	2.85	2.74	2.66	2.59	2.54	2.49	2.42	2.35	2.28	2.24	2.19	2.15	2.11	2.06	2.01
17	4.45	3.59	3.20	2.96	2.81	2.70	2.61	2.55	2.49	2.45	2.38	2.31	2.23	2.19	2.15	2.10	2.06	2.01	1.96
18	4.41	3.55	3.16	2.93	2.77	2.66	2.58	2.51	2.46	2.41	2.34	2.27	2.19	2.15	2.11	2.06	2.02	1.97	1.92
19	4.38	3.52	3.13	2.90	2.74	2.63	2.54	2.48	2.42	2.38	2.31	2.23	2.16	2.11	2.07	2.03	1.98	1.93	1.88
20	4.35	3.49	3.10	2.87	2.71	2.60	2.51	2.45	2.39	2.35	2.28	2.20	2.12	2.08	2.04	1.99	1.95	1.90	1.84
21	4.32	3.47	3.07	2.84	2.68	2.57	2.49	2.42	2.37	2.32	2.25	2.18	2.10	2.05	2.01	1.96	1.92	1.87	1.81
22	4.30	3.44	3.05	2.82	2.66	2.55	2.46	2.40	2.34	2.30	2.23	2.15	2.07	2.03	1.98	1.94	1.89	1.84	1.78
23	4.28	3.42	3.03	2.80	2.64	2.53	2.44	2.37	2.32	2.27	2.20	2.13	2.05	2.01	1.96	1.91	1.86	1.81	1.76
24	4.26	3.40	3.01	2.78	2.62	2.51	2.42	2.36	2.30	2.25	2.18	2.11	2.03	1.98	1.94	1.89	1.84	1.79	1.73
25	4.24	3.39	2.99	2.76	2.60	2.49	2.40	2.34	2.28	2.24	2.16	2.09	2.01	1.96	1.92	1.87	1.82	1.77	1.71
26	4.23	3.37	2.98	2.74	2.59	2.47	2.39	2.32	2.27	2.22	2.15	2.07	1.99	1.95	1.90	1.85	1.80	1.75	1.69
27	4.21	3.35	2.96	2.73	2.57	2.46	2.37	2.31	2.25	2.20	2.13	2.06	1.97	1.93	1.88	1.84	1.79	1.73	1.67
28	4.20	3.34	2.95	2.71	2.56	2.45	2.36	2.29	2.24	2.19	2.12	2.04	1.96	1.91	1.87	1.82	1.77	1.71	1.65
29	4.18	3.33	2.93	2.70	2.55	2.43	2.35	2.28	2.22	2.18	2.10	2.03	1.94	1.90	1.85	1.81	1.75	1.70	1.64
30	4.17	3.32	2.92	2.69	2.53	2.42	2.33	2.27	2.21	2.16	2.09	2.01	1.93	1.89	1.84	1.79	1.74	1.68	1.62
40	4.08	3.23	2.84	2.61	2.45	2.34	2.25	2.18	2.12	2.08	2.00	1.92	1.84	1.79	1.74	1.69	1.64	1.58	1.51
60	4.00	3.15	2.76	2.53	2.37	2.25	2.17	2.10	2.04	1.99	1.92	1.84	1.75	1.70	1.65	1.59	1.53	1.47	1.39
120	3.92	3.07	2.68	2.45	2.29	2.17	2.09	2.02	1.96	1.91	1.83	1.75	1.66	1.61	1.55	1.55	1.43	1.35	1.25
∞	3.84	3.00	2.60	2.37	2.21	2.10	2.01	1.94	1.88	1.83	1.75	1.67	1.57	1.52	1.46	1.39	1.32	1.22	1.00

Anexo G. Presupuesto

Se trata de una predicción cuantitativa, de los recursos necesarios para llevar a cabo un supuesto de implementación del protocolo MPLS con VPN en la Corporación Nacional de Electricidad Regional Bolívar.

Tabla 49A. Presupuesto de equipos

Cantidad	Equipo	Precio por Unidad	Total
20	Antena parabólica 5,8 Ghz	$149,52	$2990,40
16	Protectores de cable	$32,00	$512,00
20	Fuentes POE	$20,00	$400,00
8	Baterías	$1.130,00	$9040,00
4	Torre 24m	$900,00	$3600,00
26	Routers	$2.960,00	$76960,00
		Subtotal	$93502,40
		Imprevistos 3%	$2805,72
		Reajuste 2%	$1870,05
		Total	**$98178,00**

Fuente: Roberto Usca, 2017

Basado en el análisis de costos de los equipos se evidencia que los mismos hacienden a 98178,00 dólares.