



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería Electrónica y Eléctrica

Escuela Profesional de Ingeniería Electrónica

**Implementación de una red privada virtual
L2TP/IPSEC sobre la red LTE para interconectar dos
repetidores de radio digital de dos vías en los
almacenes de Ate y Huachipa del grupo Molicom**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero Electrónico

AUTOR

Alejandro Adar CASTILLO QUISPE

ASESOR

Otto Leoncio CASTILLO GONZALES

Lima, Perú

2021



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

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

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

Referencia bibliográfica

Castillo, A. (2021). *Implementación de una red privada virtual L2TP/IPSEC sobre la red LTE para interconectar dos repetidores de radio digital de dos vías en los almacenes de Ate y Huachipa del grupo Molicom*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Alejandro Adar Castillo Quispe
Tipo de documento de identidad	DNI
Número de documento de identidad	46906702
URL de ORCID	https://orcid.org/0000-0002-7009-2970
Datos de asesor	
Nombres y apellidos	Otto Leoncio Castillo Gonzales
Tipo de documento de identidad	DNI
Número de documento de identidad	25488983
URL de ORCID	https://orcid.org/0000-0001-6799-8758
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Luis Ernesto Cruzado Montañez
Tipo de documento	DNI
Número de documento de identidad	32920395
Miembro del jurado 1	
Nombres y apellidos	Wilbert Chávez Irazabal
Tipo de documento	DNI
Número de documento de identidad	08121733
Miembro del jurado 2	
Nombres y apellidos	Rejis Renato Paredes Peñafiel
Tipo de documento	DNI
Número de documento de identidad	06758404

Datos de investigación	
Línea de investigación	No aplica.
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Lince Urbanización: San Eugenio Calle: Los Geranios Latitud: -12.090079264713513 Longitud: -77.02649607090002
Año o rango de años en que se realizó la investigación	2019-2021
URL de disciplinas OCDE	Ingeniería eléctrica, Ingeniería electrónica https://purl.org/pe-repo/ocde/ford#2.02.01



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



UNMSM

Firmado digitalmente por PAREDES
PENAFIEL Rejis Renato FAU
20148092282 soft
Motivo: Soy el autor del documento
Fecha: 22.09.2021 14:04:15 -05:00



ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL Nº 045/FIEE-EPIE/2021

Los suscritos Miembros del Jurado, nombrados por la Comisión Ejecutiva del Programa de Perfeccionamiento Profesional de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha, bajo La Presidencia Del **Ing. Cruzado Montañez, Luis Ernesto** integrado por **Ing. Castillo Gonzales, Otto Leoncio** y **Mg. Chavez Irazabal, Wilbert**.

Después de escuchar la Sustentación de Trabajo de Suficiencia Profesional del **Bach. CASTILLO QUISPE, ALEJANDRO ADAR** con código **Nº10190061** que para optar el Título Profesional de Ingeniero Electrónico sustentó el Trabajo de Suficiencia Profesional titulada **IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL L2TP/IPSEC SOBRE LA RED LTE PARA INTERCONECTAR DOS REPETIDORES DE RADIO DIGITAL DE DOS VIAS EN LOS ALMACENES DE ATE Y HUACHIPA DEL GRUPO MOLICOM.**

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

Ciudad Universitaria, 18 de setiembre del 2021

Ing. Cruzado Montañez, Luis Ernesto
Presidente de Jurado

Ing. Castillo Gonzales, Otto Leoncio
Miembro de Jurado

Mg. Chavez Irazabal, Wilbert
Miembro de Jurado

Mg. Paredes Peñañiel, Rejis Renato
Miembro Jurado

DEDICATORIA

Para mi madre Neri Quispe Fernández, por su apoyo constante en los buenos y malos momentos de mi vida. Para ella, mi gratitud por siempre.

AGRADECIMIENTOS

A la Lic. Neri Quispe Fernández, mi madre, pues sin su apoyo no hubiese sido posible este trabajo.

A mi asesor Ing. Otto Castillo Gonzales, por su paciencia y apoyo en la realización del presente trabajo.

Al Lic. César Jiménez Wong, Gerente General de Centauro Comunicaciones, por su apoyo total en el desarrollo e implementación de la investigación.

A mi amigo Eduardo Valencia Luque, quien me apoyó durante la realización de la investigación brindándome sus opiniones y aportes.

Y a todas las personas que me apoyaron de muchas maneras en el transcurso de este trabajo de investigación: Ing. Javier, Ing. Jaime, Lic. Jhoysy, Vidi, Cindy, Margot y todos los amigos que en alguna oportunidad les pedí una opinión.

RESUMEN

El diseño de una red privada virtual L2TP/IPSec permite interconectar las repetidoras de radio digital de dos vías de forma segura, encriptando la información (voz) de los dos almacenes a través del protocolo IPSec bajo el tipo de red privada virtual de acceso remoto. Las repetidoras serán conectadas a una unidad de interface de red capaz de convertir la señal de radio digital de dos vías a los paquetes IP que serán enrutados estáticamente al servidor de enrutamiento y así se logrará interconectar las comunicaciones de los dos los almacenes en tiempo real.

La red LTE presenta baja latencia de acceso a Internet y gran ancho de banda, por lo cual se propone como medio de enlace entre las repetidoras de radio digital de dos vías, de tal manera que la solución no dependerá de la arquitectura de red ethernet de la empresa.

Finalmente, el diseño de la red privada virtual L2TP/IPSec sobre la red LTE se realizó aplicando la metodología de diseño Top-Down propuesta por Cisco Press & Priscilla Oppenheimer, comprobándose el funcionamiento de la solución propuesta con los siguientes valores medidos: latencia promedio 92ms, jitter 68.5ms y 15 kbps de ancho de banda en la comunicación half dúplex.

PALABRAS CLAVES: Servidor de enrutamiento Mikrotik, Enrutamiento estático, Radio móvil digital, Radio sobre el protocolo de Internet, Telefonía celular de cuarta generación.

ABSTRAC

The design of a L2TP / IPSec virtual private network allows interconnection of the two-way digital radio repeaters in a secure way, encrypting the information (voice) of the two stores through the IPSec protocol under the type of remote access virtual private network. The repeaters will be connected to a network interface unit capable of converting the bidirectional digital radio signal into IP packets that will be routed statically to the routing server and thus the communications of the two stores will be interconnected in real time.

The LTE network has low Internet access latency and high bandwidth, which is why it is proposed as a means of link between two-way digital radio repeaters, in such a way that the solution will not depend on the architecture. Ethernet network.

Finally, the design of the L2TP / IPSec virtual private network over the LTE network was carried out by applying the Top-Down design methodology proposed by Cisco Press & Priscilla Oppenheimer, verifying the operation of the proposed solution with the following measured values: average latency 92 ms, 68.5 ms of jitter and 15 kbps of bandwidth in half duplex communication.

KEYWORDS: Mikrotik Routing Server, Static Routing, Digital Mobile Radio, Radio over Internet Protocol, Fourth Generation Cellular Telephony.

TABLA DE CONTENIDO

DEDICATORIA	II
AGRADECIMIENTOS	III
RESUMEN	IV
ABSTRAC	V
TABLA DE CONTENIDO	VI
LISTA DE TABLAS	IX
LISTA DE FIGURAS	X
CAPÍTULO I	1
INTRODUCCIÓN	1
1.1 OBJETIVO DEL INFORME	1
1.2 ESTRUCTURA DEL INFORME	1
CAPITULO II	2
INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	2
2.1 INSTITUCIÓN DONDE SE DESARROLLÓ LA ACTIVIDAD	2
2.2 PERIODO DE DURACIÓN DE LA ACTIVIDAD	2
2.3.FINALIDAD Y OBJETIVOS DE LA ENTIDAD	2
2.4 RAZÓN SOCIAL	3
2.5 DIRECCIÓN POSTAL	3
2.6 CORREO ELECTRÓNICO DEL PROFESIONAL A CARGO	3
CAPITULO III	4
DESCRIPCIÓN DE LA ACTIVIDAD	4
3.1 ORGANIZACIÓN DE LA ACTIVIDAD	4
3.2 FINALIDAD Y OBJETIVOS DE LA ACTIVIDAD	5
3.2.1 Finalidad	5
3.2.2 Objetivos	5
3.3 PROBLEMÁTICA	5
3.3.1 Problema general	5

3.3.2 Problemas específicos	6
3.3.3 Justificación e importancia de la investigación	6
3.4 METODOLOGÍA	7
3.4.1 Bases teóricas	11
3.4.1.1 Red privada virtual.	11
3.4.1.2 Protocolo de túnel L2TP	11
3.4.1.3 Protocolo de encriptación IPSEC	12
3.4.1.4 Protocolo EoIP.	13
3.4.1.5 Latencia en LTE.	14
3.4.1.6 Radio móvil digital DMR.	14
3.4.1.7 Unidad de interface de red.	15
3.4.1.8 Estándar de interfaz de aplicación (AIS)	16
3.4.2 Marco conceptual	16
3.4.3 Variable Interconexión	17
3.5 PROCEDIMIENTO	17
3.5.1 Tipo de investigación	17
3.5.2 Enfoque de investigación	17
3.5.3 Alcance de la investigación	18
3.5.4 Diseño de la investigación	18
3.5.5 Población y muestra	19
3.5.6 Técnica e instrumento:	19
3.5.7 Método y sus fases para el diseño:	22
3.6 RESULTADOS DE LA ACTIVIDAD	23
CAPITULO IV	31
CONCLUSIONES	31
4.1 JUSTIFICACIÓN	31
4.2 METODOLOGÍA APLICADA	32
4.2.1 FASE I: Identificación de necesidades y objetivos de los clientes	32
4.2.2 FASE II: Diseño lógico	38
4.2.3 FASE III: Diseño físico	41
4.2.4 FASE IV: Fase de prueba, optimización y documentación	43
4.3 DESCRIPCIÓN DE LA IMPLEMENTACIÓN	48
4.4 CONCLUSIONES	50

CAPITULO V	51
RECOMENDACIONES	51
CAPITULO VI	52
BIBLIOGRAFIA	52
CAPITULO VII	57
ANEXOS	57
7.1 ANEXO N°01: CONFIGURACIÓN INICIAL DEL SERVIDOR VPN L2TP/IPSEC EN MIKROTIK	57
7.2 ANEXO N°02: SEGURIDAD BÁSICA EN EL SERVIDOR VPN L2TP/IPSEC MIKROTIK	60
7.3 ANEXO N°03: CONFIGURACIÓN DE MODEM ROUTER MIKROTIK REP_1	67
7.4 ANEXO N°04: CONFIGURACIÓN DEL MODEM HUAWIE	71

LISTA DE TABLAS

TABLA 1	VELOCIDADES DE DESCARGA Y CARGA DE LOS PRINCIPALES OPERADORES DEL PERÚ 2019-2020	21
TABLA 2	<i>JITTER EN LA RED IP. FUENTE. TOMADO DE SUIN (2016). DISEÑO E IMPLEMENTACIÓN DE UNA RED ROIP DE DOS VÍAS PARA LA EMPRESA MAXIGROUP. TRABAJO DE TITULACIÓN PARA OBTENER EL TÍTULO DE INGENIERO ELECTRÓNICO. ECUADOR – QUITO. UNIVERSIDAD POLITÉCNICA SALESIANA. (P.50)</i>	32
TABLA 3	<i>PAQUETE DE ROIP. FUENTE. TOMADO DE BLANCO (2018). EVALUACIÓN DE LOS MODELOS UTILIZADOS PARA LA MEDICIÓN DE LOS PARÁMETROS DE CALIDAD DE SERVICIO EN LA TELEFONÍA IP. TESIS PRESENTADA COMO REQUISITO PARCIAL PARA OPTAR EL TÍTULO DE MAGISTER EN INGENIERÍA – TELECOMUNICACIONES. BOGOTÁ – COLOMBIA. UNIVERSIDAD NACIONAL DE COLOMBIA. (P.66)</i> ³⁴	34
TABLA 4	<i>CAPACIDAD DE LOS PERFILES DE TRÁFICO ESTÁNDAR DE VOZ. FUENTE. TOMADO MODULO 2 DISEÑO DEL SISTEMA: TOPOLOGÍAS, PLANIFICACIÓN DE LA CAPACIDAD Y CONFIGURACIONES. MOTOROLA 2018. (P.97)</i>	37
TABLA 5	<i>NIVEL DE CALIDAD DE AUDIO ENTREGADO. FUENTE. TOMADO DE MODULO 1 INFORMACIÓN DEL PRODUCTO Y SISTEMA MOTOTRBO, 2018. (P.77).</i>	38
TABLA 6	<i>DIRECCIÓN IP DE LA RED IP DEL SISTEMA ROIP. FUENTE. PROPIA</i>	40
TABLA 7	<i>ENRUTAMIENTO DE RED PARA LOS ALMACENES DE ATE Y HUACHIPA. FUENTE. PROPIA</i>	41

LISTA DE FIGURAS

<i>FIGURA 1.</i> EOIP TÚNEL. FUENTE. TÚNELES L2TP Y EOIP PARA GESTIÓN Y CONEXIÓN L2.	13
<i>FIGURA 2.</i> VISIÓN GENERAL DE ALTO NIVEL DE LA COMUNICACIÓN DE VOZ DE RADIO DIGITAL. FUENTE. ANÁLISIS Y DISEÑO DE UN SISTEMA DE COMUNICACIÓN ROIP A TRAVÉS DE LA RED DE DATOS PARA EL MODELO DE RADIOS MOTOROLA DGM 8000. TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGISTER EN TELECOMUNICACIONES. ECUADOR- GUAYAQUIL. UNIVERSIDAD DE SANTIAGO DE GUAYAQUIL	15
<i>FIGURA 3.</i> MEDICIÓN DE LA RED LTE BITEL PARA EL ALMACÉN DE HUACHIPA. FUENTE. PROPIA, SETIEMBRE 2020	20
<i>FIGURA 4.</i> MEDICIÓN DE LA RED LTE BITEL PARA EL ALMACÉN DE ATE. FUENTE. PROPIA, SETIEMBRE 2020	20
<i>FIGURA 5.</i> VELOCIDADES DE DESCARGA, CARGA GARANTIZADA POR EL OPERADOR BITEL EN LA RED LTE FUENTE. TOMADO DE LA PÁGINA WEB HTTPS://TIENDA.BITEL.COM.PE/PLAN_ICHIP.PHP , SETIEMBRE 2020	22
<i>FIGURA 6.</i> NIVEL DE INTENSIDAD DE LA RED LTE PARA REP_2. FUENTE. PROPIA	23
<i>FIGURA 7.</i> PARÁMETROS DEL ANCHO DE BANDA DE LA RED LTE PARA REP_2. FUENTE. PROPIA	23
<i>FIGURA 8.</i> NIVEL DE INTENSIDAD DE LA RED LTE PARA REP_1. FUENTE. PROPIA	24
<i>FIGURA 9.</i> PARÁMETROS DEL ANCHO DE BANDA DE LA RED LTE PARA REP_1. FUENTE. PROPIA	24
<i>FIGURA 10.</i> LATENCIA DESDE EL SERVER VPN L2TP/IPSEC A LAS REP_1 Y REP_2 DESDE ROUTEROS. FUENTE. PROPIA	25
<i>FIGURA 11.</i> PING DE UNIDAD DE INTERFACE REP_1 A LA UNIDAD DE INTERFACE REP_2 DESDE INTERPRETE DE COMANDOS DE WINDOWS. FUENTE. PROPIA	26

<i>FIGURA 12.</i> PING DE UNIDAD DE INTERFACE REP_2 A LA UNIDAD DE INTERFACE REP_1 DESDE INTERPRETE DE COMANDOS DE WINDOWS. FUENTE. PROPIA	26
<i>FIGURA 13.</i> MEDICIÓN DE JITTER EN EL SISTEMA PARA REP_1 IP:192.168.1.10/24. FUENTE. PROPIA	27
<i>FIGURA 14.</i> MEDICIÓN DEL ANCHO DE BANDA CONSUMIDO PARA LLEGAR A LA REP_1. FUENTE. PROPIA	27
<i>FIGURA 15.</i> MEDICIÓN DE JITTER EN EL SISTEMA PARA REP_2 IP:192.168.1.20/24. FUENTE. PROPIA	28
<i>FIGURA 16.</i> MEDICIÓN DEL ANCHO DE BANDA CONSUMIDO PARA LLEGAR A LA REP_2. FUENTE. PROPIA	28
<i>FIGURA 17.</i> PERCEPCIÓN DE LA CALIDAD DE AUDIO DEL SISTEMA, PUNTUACIÓN 4/5. FUENTE. PROPIA	29
<i>FIGURA 18.</i> PERCEPCIÓN DE LA CALIDAD DE AUDIO DEL SISTEMA, PUNTUACIÓN 5/5. FUENTE. PROPIA	29
<i>FIGURA 19.</i> TIEMPO DE ESTABLECIMIENTO DE LA CONEXIÓN ENTRE LAS REPETIDORAS, INTENTO NÚMERO 01. FUENTE. PROPIA	30
<i>FIGURA 20.</i> TIEMPO DE ESTABLECIMIENTO DE LA CONEXIÓN ENTRE LAS REPETIDORAS, INTENTO NÚMERO 02. FUENTE. PROPIA	30
<i>FIGURA 21.</i> TIEMPO DE ESTABLECIMIENTO DE LA CONEXIÓN ENTRE LAS REPETIDORAS, INTENTO NÚMERO 03. FUENTE. PROPIA	30
<i>FIGURA 22.</i> PLAN DE DATOS DEL OPERADOR BITEL. FUENTE. PÁGINA WEB DE BITEL – PLAN ÚNICO, SETIEMBRE 2020	37
<i>FIGURA 23.</i> TOPOLOGÍA LÓGICA DE RED. FUENTE. PROPIA	39
<i>FIGURA 24.</i> TOPOLOGÍA FÍSICA DE RED. FUENTE. PROPIA	42
<i>FIGURA 25.</i> HABILITACIÓN DEL SERVIDOR L2TP/IPSEC. FUENTE. PROPIA	43
<i>FIGURA 26.</i> CONFIGURACIÓN DEL CLIENTE L2TP/IPSEC DEL ALMACÉN DE ATE REP_1. FUENTE. PROPIA	44
<i>FIGURA 27.</i> CONFIGURACIÓN DE TÚNEL EOIP. FUENTE. PROPIA	45
<i>FIGURA 28.</i> ASIGNACIÓN DE LAS DIRECCIONES SEGÚN LA TABLA: DIRECCIÓN IP DE LA RED IP DEL SISTEMA	45
<i>FIGURA 29.</i> CONFIGURACIÓN DEL VPN L2TP/IPSEC DE REP_2. FUENTE. PROPIA	46
<i>FIGURA 30.</i> TÚNEL EOIP PARA REP_2. FUENTE. PROPIA	47

<i>FIGURA 31.</i> BRIDGE DE LAS INTERFACES ETHER 2, ETHER 3 Y EL TÚNEL EOIP. FUENTE. PROPIA	47
<i>FIGURA 32.</i> IMPLEMENTACIÓN DEL SISTEMA DE REPETIDORA REP_1 CON ENLACE LTE, PARTE FRONTAL. FUENTE. PROPIA	48
<i>FIGURA 33.</i> IMPLEMENTACIÓN DEL SISTEMA DE REPETIDORA REP_1 CON ENLACE LTE, PARTE POSTERIOR. FUENTE. PROPIA	48
<i>FIGURA 34.</i> IMPLEMENTACIÓN DEL SISTEMA DE REPETIDORA REP_2 CON ENLACE LTE, PARTE FRONTAL. FUENTE. PROPIA	49
<i>FIGURA 35.</i> IMPLEMENTACIÓN DEL SISTEMA DE REPETIDORA REP_2 CON ENLACE LTE, PARTE POSTERIOR. FUENTE. PROPIA	49
<i>FIGURA 36.</i> INGRESO A ROUTEROS POR WINBOX. FUENTE. PROPIA	57
<i>FIGURA 37.</i> ACTUALIZACIÓN DE ROUTEROS v6.47.4. FUENTE. PROPIA.	58
<i>FIGURA 38.</i> CONFIGURACIÓN DE SNTP CLIENT. FUENTE. PROPIA	59
<i>FIGURA 39.</i> CONFIGURACIÓN DE LA HORA. FUENTE. PROPIA	59
<i>FIGURA 40.</i> CREACIÓN DE USUARIO. FUENTE. PROPIA	60
<i>FIGURA 41</i> DESHABILITACIÓN DE SERVICIOS IP. FUENTE. PROPIA	61
<i>FIGURA 42.</i> ATAQUE SYN FLOOD. FUENTE. CANÓ ACADEMY, SEMINARIO ONLINE DE FIREWALLS CON MIKROTIK, 2018	61
<i>FIGURA 43.</i> FILTRO SYN FLOOD. FUENTE. CANÓ ACADEMY, SEMINARIO ONLINE DE FIREWALLS CON MIKROTIK, 2018	62
<i>FIGURA 44.</i> ATAQUE DoS. FUENTE. CANÓ ACADEMY, SEMINARIO ONLINE DE FIREWALLS CON MIKROTIK, 2018	63
<i>FIGURA 45.</i> FILTRO DoS. FUENTE. CANÓ ACADEMY, SEMINARIO ONLINE DE FIREWALLS CON MIKROTIK, 2018	64
<i>FIGURA 46.</i> ATAQUE DNS RELAY ATTACK. FUENTE. CANÓ ACADEMY, SEMINARIO ONLINE DE FIREWALLS CON MIKROTIK, 2018	65
<i>FIGURA 47.</i> FILTRO DNS RELAY ATTACK. FUENTE. CANÓ ACADEMY, SEMINARIO ONLINE DE FIREWALLS CON MIKROTIK, 2018	66
<i>FIGURA 48.</i> INGRESO A ROUTEROS. FUENTE. PROPIA	67
<i>FIGURA 49</i> CONFIGURACIÓN DE APN. FUENTE. PROPIA	68
<i>FIGURA 50.</i> CONFIGURACIÓN DE LA INTERFAZ LTE. FUENTE. PROPIA	69
<i>FIGURA 51.</i> CONEXIÓN A LA RED LTE. FUENTE. PROPIA	70
<i>FIGURA 52.</i> MARCA Y MODELO DEL MODEM. FUENTE. PROPIA	71
<i>FIGURA 53.</i> INTERFAZ DE CONFIGURACIÓN HUAWEI. FUENTE. PROPIA	71

<i>FIGURA 54. MODO DE RED PREFERIDO. FUENTE. PROPIA</i>	72
<i>FIGURA 55. CONFIGURACIÓN DEL APN BITEL. FUENTE. PROPIA</i>	72
<i>FIGURA 56. CONFIGURACIÓN DEL DNS BITEL. FUENTE. PROPIA</i>	73
<i>FIGURA 57. CONFIGURACIÓN DHCP. FUENTE. PROPIA</i>	73

CAPÍTULO I

INTRODUCCIÓN

1.1 Objetivo del informe

El presente informe tiene como objetivo buscar una solución para interconectar las comunicaciones de radio digital de dos vías por Internet sin disponer una dirección IP pública en los almacenes de Ate y Huachipa, así como explicar brevemente los protocolos de comunicación.

1.2 Estructura del Informe

El presente informe, tomará una estructura de análisis guiada por un profundo estudio de la interacción entre factores técnicos y factores económicos propios del presente trabajo:

- Análisis técnico, se realizará usando las recomendaciones del curso de certificación de Motorola “Información del producto y sistema Mototrbo” del 2018 tales como: una dirección IP pública estática, ancho de banda de 40kbps por enlace, latencia de red menor de 90ms y jitter menor de 60ms.
- Análisis económico se llevará a cabo utilizando información del consumo de ancho de banda para contratar un plan de datos y se seleccionará al operador de telefonía móvil que brinde una baja latencia de acceso a Internet en 4G LTE.

CAPITULO II

INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución donde se desarrolló la actividad

Las actividades vistas en el presente trabajo se realizaron en la empresa CENTAURO COMUNICACIONES.

2.2 Periodo de duración de la actividad

Las actividades que se tocan en el presente trabajo, se desarrollaron durante los años 2019 a 2021.

2.3. Finalidad y objetivos de la entidad

La visión corporativa de Centauro Comunicaciones es “convertirse en una de las empresas líderes en integración de soluciones tecnológicas orientadas a las industrias aportando recursos y servicios de alta calidad”.

Y en lo relacionado a la misión:

“Ofrecer innovación en soluciones tecnológicas certificadas para procesos industriales, de protección, prevención y seguridad, garantizando un alto grado de confiabilidad y calidad de los producto y servicios que brindan”.

2.4 Razón social

CENTAURO COMUNICACIONES SRL

2.5 Dirección postal

15046

2.6 Correo electrónico del profesional a cargo

jtipula@centaurocomunicaciones.com

CAPITULO III

DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

El profesional a cargo durante las actividades realizadas fue Jaime Típula Pérez y la organización de las actividades llevadas a cabo en el presente trabajo, se tomaron en cuenta las realidades observadas en proyectos desarrollados

Local:

Dentro del diseño de una red de comunicaciones de una empresa se encuentra el diseño de un sistema de radiocomunicación de dos vías; se observó específicamente que, a nivel local, los sistemas mayormente implementados son TIER 1. El sistema TIER 1 cumple con las características básicas de cobertura, capacidad y calidad que el cliente solicita.

Nacional:

Las empresas mineras, petroleras, centrales hidroeléctricas, y otras grandes empresas a nivel nacional cuentan un sistema de radiocomunicación de dos vías TIER 2 o TIER 3, en estos sistemas el análisis realizado que se toma en cuenta para el diseño es principalmente la calidad y disponibilidad de las comunicaciones por cada canal requerido.

3.2 Finalidad y objetivos de la actividad

3.2.1 Finalidad

Proponer una alternativa de solución para interconectar dos repetidores de radio digital de dos vías en los almacenes de Ate y Huachipa del Grupo Molicom sin IP pública fija y sin utilizar la red ethernet de la empresa.

3.2.2 Objetivos

Implementar una red privada virtual sobre la red LTE para interconectar dos repetidoras de radio digital de dos vías en los almacenes de Ate y Huachipa del Grupo Molicom

Implementar una red privada virtual sobre la red LTE con el protocolo de túnel L2TP/IPSEC para interconectar dos repetidoras de radio digital de dos vías en los almacenes de Ate y Huachipa del Grupo Molicom

Implementar una red privada virtual sobre la red LTE con el tipo de acceso remoto para interconectar dos repetidoras de radio digital de dos vías en los almacenes de Ate y Huachipa del Grupo Molicom

3.3 Problemática

3.3.1 Problema general

¿Cómo diseñar una red privada virtual sobre la red LTE para interconectar repetidoras de radio digital de dos vías en los almacenes de Ate y Huachipa del Grupo Molicom?

3.3.2 Problemas específicos

¿Cómo diseñar una red privada virtual sobre la red LTE con el protocolo de túnel L2TP/IPSEC para interconectar repetidoras de radio digital de dos vías en los almacenes de Ate y Huachipa del Grupo Molicom?

¿Cómo diseñar una red privada virtual sobre la red LTE con el tipo de acceso remoto para interconectar repetidoras de radio digital de dos vías en los almacenes de Ate y Huachipa del Grupo Molicom?

3.3.3 Justificación e importancia de la investigación

La radio sobre el protocolo de Internet (RoIP), aplicada en este trabajo, no solo ofrece una mayor confiabilidad que las redes de radiocomunicaciones existentes, sino que mejora y agrega valor gracias a características adicionales que anteriormente no eran posibles a través de puertas de enlace habilitadas para transceptores digitales de dos vías para redes ethernet. Estos beneficios surgen de la capacidad de la tecnología digital para utilizar la infraestructura ethernet existente.

Este trabajo es importante porque al interconectar dos repetidores de radio digital de dos vías de los almacenes de Ate y Huachipa se podrá monitorear, supervisar y reportar cualquier actividad directamente a la oficina central.

Utilizando los conceptos y la idea del presente trabajo, se podrá integrar al sistema de radiocomunicación soluciones industriales como circuito cerrado de televisión, sistemas de alerta temprana y otros más según la necesidad del mercado industrial peruano.

Asimismo, el presente trabajo proporcionará una fuente a la que acudir cuando se requiera interconectar dos dispositivos de red por Internet sin disponer de una IP pública fija.

3.4 Metodología

Suin (2016) en su trabajo de titulación previo a la obtención del título de Ingeniero Electrónico presento el trabajo “Diseño e implementación de una red RoIP de dos vías para la empresa MaxiGroup” donde expone como objetivos general: buscar la convergencia entre los sistemas de radiofrecuencia con redes de voz y datos y como objetivos específicos: realizar la convergencia de los sistemas de comunicaciones de la empresa MaxiGroup a través de las redes de datos; transmitir las redes de radio sobre Internet (RoIP); la red RoIP diseñada logre un ahorro del 39% con respecto a sistemas de radiocomunicaciones analógicas convencionales; diseñar la red RoIP con un jitter máximo del 129 ms para permitir la una comunicación de voz sin problemas entre usuarios con distinta ubicación geográfica; medir el funcionamiento de la red RoIP: BER, ancho de banda, velocidad de transmisión y capacidad de canal. Para llevar a cabo el estudio emplea un método descriptivo, analítico y comparativo donde se investigó los fundamentos teóricos necesarios del sistema RoIP, sus protocolos de señalización y requisitos mínimos para su funcionamiento, para el levantamiento de datos se empleó como técnica de investigación la observación directa constando la situación actual. Los instrumentos para registrar la información obtenida fueron: Wireshark para la medición del jitter en la red RoIP, tasa de errores de bits es una medida de la calidad física de la transmisión y símbolo del sistema de Windows para las pruebas de conectividad. La tesis llego a las siguientes conclusiones: la red RoIP posee un Jitter de 129.10 ms siendo aceptable para las comunicaciones de voz; el parámetro capacidad de canal de la red RoIP para un paquete de 64 Kbyte en un intervalo de 10 segundos tiene un ancho de banda de 94.9Mbps, el ancho de banda necesario para una llamada es de 120 kbps multiplicado por 10

usuarios y con un crecimiento de 10% se necesita 1.32Mbps de ancho de banda, el cual representa solo el 1.39% de la red RoIP.

Zhingre y Patricio (2018), en su tesis de maestría para obtener el grado académico de Magister en Telecomunicaciones de la Universidad Católica de Santiago de Guayaquil titulada “Análisis y diseño de un sistema de comunicación RoIP a través de la red de datos para el modelo de radios Motorola DGM 8000”, plantearon como objetivo general: analizar y diseñar un sistema de comunicación RoIP a través de la red de datos para el modelo de radios Motorola DGM8000, objetivos específicos: analizar el sistema de comunicación mediante la red troncalizada, identificar soluciones de integración para la radio comunicación, analizar un sistema de comunicación mediante la tecnología RoIP para el modelo de radios Motorola DGM8000, diseñar un sistema de comunicación mediante la tecnología RoIP para el modelo de radios Motorola DGM8000; la tesina tiene el enfoque de investigación científica cuantitativa, descriptiva transversal, para el levantamiento de datos se empleó como técnica de investigación la observación directa al revisar el sistema actual de comunicaciones que utilizan los modelos de radio Motorola DGM800 evidenciándose algunas limitantes en el sistema de comunicación. Los instrumentos para registrar la información obtenida fueron: controlador del sistema de radio troncalizado el cual permite tener el control de los receptores como los transmisores, servidor Elastix para la interconexión entre el terminal de radio en el origen y los destinos que pueden ser otros terminales de radio o un usuario que se conecte al servidor mediante una aplicación. La tesis llegó a las siguientes conclusiones: el sistema de radio comunicación mediante la red troncalizada permite utilizar el canal de comunicación por varios usuarios formando grupos de conversación y optimizando los recursos, existen equipos de integración como son RoIP(102,302), ACU1000 y Zepron 6300, los cuales permiten establecer la comunicación entre radiofrecuencia y sistemas bajo RoIP, el dispositivo RoIP 102 permite que los sistemas de comunicación convencionales de radio Motorola DGM8000 puedan integrarse a través de Internet optimizando de esta forma el uso del espectro radioeléctrico.

Martel (2019), en su trabajo de titulación previo a la obtención del título de Ingeniero de Redes y Comunicaciones de la Universidad Peruana de Ciencias Aplicadas titulada “Diseño de una red de comunicación VPN sobre internet para un distribuidor autorizado de Claro basado en el RFC 2764”, plantea como objetivo principal: diseñar una red de comunicación VPN sobre internet que permita comunicación en tiempo real para agilizar los procesos de negocio mediante un eficiente uso de los recursos TI basado en el RFC 2764 para un distribuidor autorizado de Claro; y como objetivos específicos: establecer una segmentación de red escalable para las sucursales mediante el cálculo VLSM bajo el cumplimiento del RFC 1878; desarrollar una configuración VPN que brinde seguridad de datos en el flujo de sus comunicaciones mediante el uso del protocolo L2TP/IPSec bajo el cumplimiento del RFC 3193; presentar una topología de red lógica centralizada que permita proponer medidas de optimización de recursos TI para la disponibilidad de la información. La tesina tiene el enfoque cuantitativo experimental, la investigación del tipo aplicativo ya que consiste en el empleo práctico del conocimiento de las redes que deben utilizarse en las instituciones para una comunicación en tiempo real; descriptiva porque estas se observan y se describen tal como se presentan en la realidad; la población es: las oficinas de los centros de distribución; utiliza la técnica de observación. La tesis tiene como conclusión general que las redes privadas virtuales son al fin y al cabo redes de comunicación y en consecuencia su análisis y estudio no crea la necesidad de reinventar la red, o de introducir paradigma completamente nuevos que no tengan un análogo directo con las redes físicas existentes; las redes privadas virtuales son sin duda una solución muy flexible y sobre todo económica para las organizaciones que necesiten tener una comunicación segura con sus proveedores, clientes, y/o sucursales, prescindiendo así de la implementación de costosas redes dedicadas de comunicación que permitirían conseguir el mismo fin; de acuerdo al RFC1878 se pudo concluir que efectivamente la red de clase B nos brinda hasta 2048 redes disponibles de 30 host lo cual nos permite tener un amplio margen de direcciones IP para futuros locales; la configuración VPN nos brinda de manera directa confidencialidad e integridad en el flujo de la información entre sucursales la misma que permitirá tomar buenas decisiones en base a

información real integra y segura; las VPN son una gran solución que permite una topología de red centralizada entre sucursales donde es posible tener acceso a los recursos TI en tiempo real permitiendo así la disponibilidad de la información, logrando un nivel de disponibilidad mayor al 90% mensual.

Pimentel (2019), en su trabajo de titulación previo a la obtención del grado académico de magister de Ingeniería de las Telecomunicaciones de la Pontificia Universidad Católica del Perú titulada “Diseño para la evolución de la red de voz de control de tránsito aéreo de la Fuerza Aérea utilizando tecnología Radio sobre IP”, tiene como objetivo principal mejorar las capacidades de la red de voz de control de tránsito aéreo de la Fuerza Aérea del Perú, con el fin de optimizar su funcionamiento y gestión; y como objetivos específicos: posibilitar la convergencia de las comunicaciones de voz de control de tránsito aéreo a nivel nacional, en centros y torre de control, empleando para ello tecnología de Radio sobre IP; optimizar la actualmente limitada capacidad de grabación de las comunicaciones que acontecen en un torre de control, de acuerdo a las normas establecidas, a fin de centralizarlas y almacenarlas en un servidor común. La tesina tiene el enfoque cuantitativo experimental, la investigación exploratoria porque se examina un tema o problema de investigación poco estudiado: correlacional porque tiene como propósito medir el grado de relación entre las variables de la hipótesis; estas se observan y se describen tal como se presentan en la realidad; la población es la Fuerza Aérea del Perú; utiliza la técnica de observación y como instrumento utilizo la guía de observación de campo. La tesis tiene como conclusiones: por la diversidad de medios de comunicaciones y la ausencia de tecnologías que permitan interoperabilidad y convergencia entre ellos, actualmente las funciones de Control de Tránsito Aéreo (ATC) en la Fuerza Aérea del Perú presentan una limitada capacidad de gestión principalmente en periodos de alta densidad de tráfico; el uso de la RoIP e IP ha permitido en los diferentes ambientes donde se ha implementado alcanzar la convergencia e interoperabilidad a través de una mejor gestión de las redes de comunicaciones; existe infraestructura de redes adecuadas para realizar la implementación de RoIP en la red de ATC, haciéndola factible y viable; el diseño la solución se ha ceñido al estándar internacional de EUROCAE,

asegurando confiabilidad y seguridad; la solución planteada tendrá vigencia en el tiempo a alguna migración tecnológica que pudiera decidir la Fuerza Aérea en lo que concierne a las radios que emplean para el ATC.

3.4.1 Bases teóricas

3.4.1.1 Red privada virtual. Ariganello (2014, p.305 de “*Redes Cisco Guía de estudio para la certificación CCNA Security*”, primera edición); define la red privada virtual:

Una VPN es una red privada que se crea mediante el uso de túneles sobre una red pública, usualmente Internet. En lugar de utilizar conexiones físicas dedicadas, una VPN utiliza conexiones virtuales enrutadas a través de Internet, desde la organización hasta sitio remoto. En el sentido más amplio, una VPN conecta dos extremos sobre una red pública para formar una conexión lógica (Ariganello, 2014, p. 305).

Delgado, Cáceres, Jorquera y Esquivel (2014, p.3 de “*Redes privadas virtuales (VPN)*”. Colombia: Universidad Técnica Federico Santa María); define una red privada virtual como:

VPN es una tecnología de red que permite una extensión segura de red local (LAN) sobre una red pública o no controlada como Internet, mediante un proceso de encapsulación y de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada. (Delgado, Cáceres, Jorquera y Esquivel, 2014, p.3).

3.4.1.2 Protocolo de túnel L2TP. Martel (2019, p.31, “*Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764*”. Tesis para la obtención del grado de

Ingeniero de Redes y Comunicaciones. Lima – Perú. Universidad Peruana de Ciencias Aplicadas) indica:

L2TP (Layer 2 Tunneling Protocol) fue diseñado por un grupo de trabajo de IETF conformado por las mismas compañías creadoras de los protocolos PPTP y L2F, con el fin de corregir las deficiencias de estos protocolos, así que L2TP heredo de PPTP y de L2F las mejores funciones y características. L2TP es un protocolo que crea un túnel entre un cliente y servidor (ambos L2TP) donde encapsula las tramas PPP para su envío a través de redes como IP, X.25, Frame Relay o ATM. Una vez establecido el túnel se configura un mecanismo de autenticación de usuarios con el fin de establecer su identidad. A través de las redes internas IP, L2TP utiliza el Protocolo de Datagramas de Usuarios (UDP) y una serie de mensajes L2TP con el fin de crear, mantener y optimizar los túneles por donde se transmiten los datos³⁰(Martel, 2019, p.31).

3.4.1.3 Protocolo de encriptación IPSEC. Ariganello (2014, p.309, de “Redes Cisco Guía de estudio para la certificación CCNA Security”, primera edición) define:

IPsec es un conjunto de características que protegen los datos IP cuando estos viajan desde una entidad a otra (...). Es importante recordar que solamente IPsec puede proteger la capa de red, la capa IP y superiores, transporte y usuario. IPsec no puede brindar servicio a la capa de enlace. Si fuese necesario la protección de dicha capa, habrá que buscar entonces otro tipo de encriptación para el enlace.

Es importante comprender que estos protocolos están basados en estándares abiertos, IPsec los utiliza para autenticación, encriptación, generación de llaves y establecimiento de asociaciones de seguridad. IPsec es utilizado para proteger el flujo de los datos a través de una VPN, pero una VPN no necesariamente tiene que requerir que estos contenidos estén

protegidos. Una VPN puede ser simplemente un túnel o un enlace entre dos puntos finales; por lo tanto, la cabecera o etiqueta es identificada como tal, pero el contenido interno está disponible para cualquiera que lo quiera inspeccionar entre dichos extremos finales. Entonces una VPN IPsec puede ser considerada segura y protegida mientras que otro tipo de VPN no comparte este tipo de características (Ariganello, 2014, p.309).

3.4.1.4 Protocolo EoIP. Muñoz (2020, p.27, de *Túneles L2Tp y EoIP para gestión y conexión L2.*) indica:

El túnel Ethernet sobre IP (EoIP) es un protocolo Mikrotik RouterOS que crea un túnel Ethernet entre dos enrutadores en la parte superior de una conexión IP [Figura 1]

El túnel EoIP puede ejecutarse sobre el túnel L2TP, el túnel PPTP o cualquier otra conexión capaz de transportar IP.

Cuando la función de puente del enrutador está habilitada, todo el tráfico de Ethernet (todos los protocolos de Ethernet) se puentearán como si hubiera una interfaz Ethernet física y un cable entre los dos enrutadores. Este protocolo hace posible múltiples esquemas de red.

El protocolo EoIP encapsula las tramas de Ethernet en paquetes GRE (número de protocolo IP 47) (al igual que PPTP) y las envía al lado remoto del túnel EoIP (Muñoz, 2020, p.27).

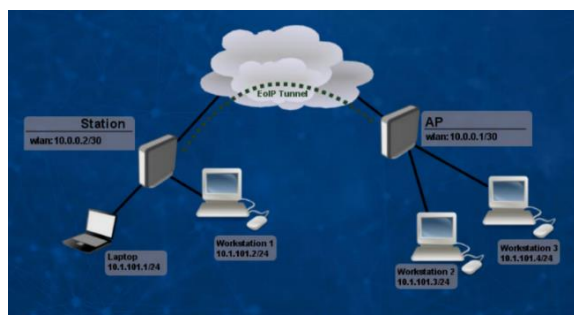


Figura 1. EoIP Túnel. Fuente. Túneles L2TP y EoIP para gestión y conexión L2.

3.4.1.5 Latencia en LTE. SoftwareLab (2020, tomado de Diferencias entre el 3G y el 4G) nos indica sobre la latencia lo siguiente:

La diferencia entre el 3G y el 4G es la velocidad de navegación y descarga de datos en Internet. La cuarta generación es entre cinco y diez veces más rápido que la tercera y, asimismo, su tiempo de respuesta es entre tres y cuatro veces menor que en el 3G. La estabilidad de la red es mayor en la cuarta generación, ya que resulta menos probable que se caiga la conexión a Internet en comparación con el 3G. Los protocolos de funcionamiento son otra diferencia entre ambas redes, pues el 4G tan solo hace uso del protocolo IP, mientras que el 3G se basa en UMTS (SoftwareLab, 2020).

3.4.1.6 Radio móvil digital DMR. Elsa Jiménez (2018, p.24, de Diseño y dimensionamiento de un sistema de telecomunicaciones optimizado para el nuevo hospital de la provincia Espinar en Cusco. Tesis para optar el título de Ingeniera de las Telecomunicaciones. Lima – Perú. Pontificia Universidad Católica del Perú), define la radio móvil digital:

Es un estándar que mejora la calidad de la voz, información de la ubicación, eficiencia del canal y seguridad por medio de la autenticación y encriptación. Actualmente, es el más usado en el mercado y se encuentran repuesto y servicios técnicos fácilmente (Elsa Jiménez, 2018, p.24).

López (2019, p.8-10, de Análisis y diseño de un sistema de comunicación ROIP a través de la red de datos para el modelo de radios Motorola DGM 8000. Tesis para optar el grado académico de Magister en Telecomunicaciones. Ecuador- Guayaquil. Universidad de Santiago de Guayaquil), nos presenta la siguiente definición de radio móvil digital:

Los sistemas de radio móviles digitales toman señales analógicas y las convierten en digitales a través de un proceso llamado muestreo. La señal analógica (voz humana) se convierte a través del micrófono en voltaje y (López, 2019, p8)

del voltaje a número binarios 0 o 1. La información binaria (ceros “0” y unos “1”) se transmite por el aire en comparación con la información analógica (voltaje continuo). La idea de utilizar señales digitales en lugar de analógica es aumentar el número de canales de radio en un espectro de frecuencia dado (reduce el ancho de banda necesario por canal), mejorar la calidad de audio, eliminar problemas de desvanecimiento en el entorno móvil, proporcionar capacidades adicionales de transferencia de datos y mantener la cobertura de radio con menor potencia transmitida. Para lograr una mejora eficiencia del espectro (reducir el ancho de banda) se han utilizado algoritmos de codificación de voz. La figura 2.3 [Figura 2] muestra un diagrama de bloques del sistema de radio digital (López, 2019, p9-10).

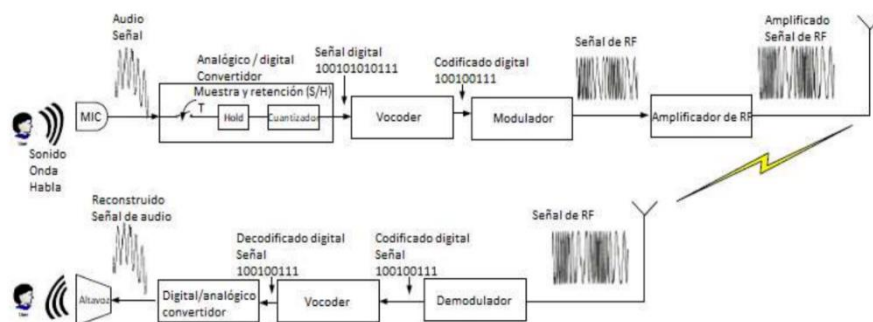


Figura 2. Visión general de alto nivel de la comunicación de voz de radio digital. Fuente. Análisis y diseño de un sistema de comunicación ROIP a través de la red de datos para el modelo de radios Motorola DGM 8000. Tesis para optar el grado académico de Magister en Telecomunicaciones. Ecuador-Guayaquil. Universidad de Santiago de Guayaquil

3.4.1.7 Unidad de interface de red. Suin (2016, p.7, de Diseño e implementación de una red RoIP de dos vías para la Empresa Maxigroup. Trabajo de titulación para obtener el título de Ingeniero

Electrónico. Ecuador – Quito. Universidad Politécnica Salesiana) define una unidad de interface de red como:

La interconexión de los sistemas de RoIP con redes IP se realiza mediante un Gateway el cual posee un puerto ethernet, esto permite que los dispositivos analógicos y digitales interactúen entre sí, la comunicación entre el emisor y transmisor se realiza mediante una señalización en forma de tonos o pulsos. Los sistemas de integración de RoIP realizan tres principales funciones sincronización, temporización y conmutación (Suin, 2016, p.7).

3.4.1.8 Estándar de interfaz de aplicación (AIS). La empresa TaitNet (2015, p.68, de DMR Introduction Training Manual) nos explica sobre la interfaz AIS:

El DMR AIS es una interconexión basada en SIP para comunicaciones de voz y datos de redes de radio DMR Tier II y Tier III. Es adecuado para consolas de despacho, grabación de voz, aplicaciones de datos como texto y ubicación LIP e interconexión entre DMR y otras redes de radio.

3.4.2 Marco conceptual

ms	Milisegundos
s	Segundos
dBm	Decibelio por milivatio
b	bits
B	Byte
kbps	Kilobits por segundo
Mbps	Megabits por segundo
PPS	Paquetes por segundo
Mb	Megabit
GB	Gigabyte
RSRP	Potencia recibida de la señal de referencia

3.4.3 *Variable Interconexión*

Una red informática es una red digital de telecomunicaciones que permite que los nodos compartan información. Los protocolos y estándares son los que hacen que las redes funcionen juntas, logrando que los diversos componentes de una red se comuniquen entre sí. La interconexión es el despliegue de puntos de intercambio de tráfico que integran conexiones directas y privadas entre participantes. La conexión “inter”, habla de una conectividad que involucra varias partes a la vez. La interconexión vincula numerosas entidades, capaces de conectarse como una unidad contra entidades individuales.

3.5 Procedimiento

3.5.1 *Tipo de investigación*

La investigación es de tipo aplicativo; consiste en el empleo práctico del conocimiento de la red privada virtual L2TP/IPSEC, túnel EoIP, la red LTE y repetidor de radio digital de dos vías que deben utilizarse con la finalidad de resolver un problema en concreto, interconectar dos repetidoras de radio digital de dos vías. La investigación aplicada se basa fundamentalmente en los hallazgos tecnológicos de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto.

3.5.2 *Enfoque de investigación*

La investigación tiene la intención de describir, explicar, comprobar o confirmar y predecir los fenómenos, es decir establecer una causalidad entre las variables. La lógica del proceso es deductiva porque partiremos de lo

general a lo particular, se transita de las leyes y la teoría a los datos y resultados. La teoría se produce a partir de comparar los resultados de la investigación con los resultados de estudios previos. Se adopta una posición personal neutral e imparcial al hacer a un lado las creencias y valores propios. Presenta tipo de datos numéricos con instrumentos de recolección estandarizados para describir las variables y sus relaciones, así como explicar sus cambios, por ello se adopta el enfoque cuantitativo (Roberto Hernández y Christian Mendoza,2018)

3.5.3 Alcance de la investigación

Según el estado del conocimiento previo sobre el problema de investigación mostrado por la revisión de la literatura y el propósito de tipo aplicativo que se pretende dar a la investigación, se ha optado por elegir un alcance descriptivo, es decir, se miden o recolectan datos y reportan información sobre diversos conceptos, variables, aspectos, dimensiones o componentes del fenómeno o problema a investigar (Roberto Hernández y Christian Mendoza,2018, pág. 106), que es interconectar las repetidoras de radio digital de dos vías utilizando la red privada virtual L2TP/IPSEC sobre red LTE.

3.5.4 Diseño de la investigación

Para la presente tesina utiliza el diseño experimental de tipo transversal, la cual se realiza al manipular la variable independiente, es decir se trata de estudios en los que se hace variar en forma intencional la variable independiente (red privada virtual L2TP/IPSEC sobre la red LTE) para ver su efecto sobre las otras variables (interconexión de dos repetidoras de radio digital de dos vías). Los diseños transeccionales o transversales recolectan datos en un solo momento, en un tiempo único cuyo propósito es determinar cuál es el nivel o modalidad de las variables en un momento dado, se realiza

la captura de datos en el mes de octubre del 2020 (Roberto Hernández y Christian Mendoza, 2018, págs. 174-179).

3.5.5 Población y muestra

Una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones, en nuestro caso los almacenes del Grupo Molicom: Ate, Huachipa, Pisco, Paíta, Trujillo y Matarani, no cuentan con un sistema de radiocomunicación integrado, pero sí cuentan con cobertura parcial de telefonía móvil LTE.

Debido al objetivo de la investigación que es implementar una red privada virtual L2TP/IPSEC sobre la red LTE para interconectar repetidoras de radio digital de dos vías, el tipo de muestra es no probabilística, donde la elección de las unidades no depende de la probabilidad, sino de razones relacionadas con las características y contexto de la investigación (Roberto Hernández y Christian Mendoza, 2018). La muestra que se ha utilizado en la investigación son los almacenes de Huachipa y Ate.

3.5.6 Técnica e instrumento:

Recolectar los datos significa aplicar uno o varios instrumentos de medición para recabar la información pertinente de las variables del estudio en la muestra o casos seleccionados, los datos obtenidos son la base del análisis (Roberto Hernández y Christian Mendoza, 2018).

Para la investigación se utiliza la técnica de la observación, la técnica de observación es un método de recolección de datos que consiste en el registro sistemático, válido y confiable de comportamientos y situaciones observables, a través de un conjunto de categorías y subcategorías (Roberto Hernández y Christian Mendoza, 2018, págs. 290-291).

La técnica de la observación se realiza con el software Speedtest y el celular Pocophone F1 para recolectar los siguientes datos: la velocidad de bajada, subida, latencia, jitter y nivel de señal de la red LTE para el operador Bitel en banda 900 MHz, lo que nos permitirá determinar la latencia total y ancho de banda del enlace para interconectar dos repetidoras de radio digital de dos vías.

Se identifica las ubicaciones exactas de los almacenes:

- ✓ Dirección del almacén de Ate: Av. Los Ingenieros 154 Urb. Sta. Raquel, 2da Etapa, Ate. Figura 3.
- ✓ Dirección del almacén de Huachipa: Calle Archipiélago Mza C Lote 12-13, La Capitana, Huachipa. Figura 4.



Figura 3. Medición de la red LTE Bitel para el Almacén de Huachipa. Fuente. Propia, setiembre 2020



Figura 4. Medición de la red LTE Bitel para el Almacén de Ate. Fuente. Propia, setiembre 2020

Las máximas velocidades de conexión que pueden alcanzar los dispositivos, según el reporte del diario La República del 15 de mayo del 2020, en el Perú la velocidad alcanza los 19.01 Mbps, alcanzando el puesto 96 a nivel mundial. Otros países tienen una velocidad de conexión a Internet de: Uruguay 30.80 Mbps, Argentina 24.69 Mbps, Brasil 24.21 Mbps, Surinam 24.17 Mbps, Ecuador 19.97 Mbps y por debajo de Perú están Colombia, Chile, Bolivia, Paraguay y Venezuela.

Asimismo, la velocidad cambia en cada lugar medido y la variación de velocidades puede variar de 50Mbps a 5Mbps, ello se representa en la siguiente Tabla 1:

Tabla 1

Velocidades de descarga y carga de los principales operadores del Perú 2019-2020 de la red móvil LTE. Fuente. Tomado de Ookla -Speed Score, mayo 2020

Operador/Periodo -Año	Segundo y tercer trimestre 2019	Cuarto trimestre 2019 y primer trimestre 2020
Claro	33.49 Mbps	27.47 Mbps / 12.18 Mbps
Entel	23.00 Mbps	20.56 Mbps / 17.95Mbps
Movistar	22.39 Mbps	20.30 Mbps / 14.34 Mbps
Bitel	10.52 Mbps	10.20 Mbps / 9.84Mbps

En la página web de Bitel encontramos las velocidades mínimas garantizadas, Figura 5, 240 kbps (0.24Mbps) de subida y 1200 kbps (1.2 Mbps) de bajada para la implementación se requiere 30 kbps de subida y baja.

Las Velocidad de Transmision contratadas son las siguientes :

Tecnología	Velocidad	Minina garantizada	Máxima	Tecnología	Minina garantizada	Máxima
4G - LTE	Bajada	1.2 Mbps	3 Mbps	3G	0.4 Mbps	1 Mbps
	Subida	0.24 Mbps	0.6 Mbps		0.08 Mbps	0.2 Mbps

Figura 5. Velocidades de descarga, carga garantizada por el operador Bitel en la red LTE Fuente. Tomado de la página web https://tienda.bitel.com.pe/plan_ichip.php, setiembre 2020

3.5.7 Método y sus fases para el diseño:

Ortega (2017. p.23-33, de *Diseño de un cableado estructurado bajo la metodología top down network design aplicando políticas de seguridad para el colegio el Pinar de La ciudad de Huaraz 2017*. Tesis para optar el título profesional de Ingeniero de Sistemas. Perú – Huaraz. Universidad Católica Los Ángeles Chimbote), define la metodología de diseño de redes Top Down, la cual se trabajará en nuestra investigación:

La metodología Top-Down propuesta por Cisco Press & Priscilla Oppenheimer se basa en las necesidades de análisis de requerimientos y diseño arquitectónico de las redes de comunicación, que debe realizarse ante de la selección de determinados componentes específicos para construir la red física. Un proceso Top-Down describe las múltiples fases por las que una red atraviesa utilizando el llamado ciclo de vida de redes PDIOO (planificación – diseño – implementación – operación – optimización) (23) (p.33).

3.6 Resultados de la Actividad

Se mide la intensidad de señal LTE para el router REP_2 con el aplicativo G-NetTrack Lite utilizando el celular Pocophone F1, obteniendo una intensidad RSRP de -86 dBm, siendo óptima para la red propuesta, Figura 6



Figura 6. Nivel de intensidad de la red LTE para REP_2. Fuente. Propia

Se mide el ancho de banda para la REP_2 con el aplicativo Speedtest, obteniendo 14.7 Mbps de bajada y 9.01Mbps de subida, latencia de 17 ms y un jitter de 4ms, Figura 7.



Figura 7. Parámetros del ancho de banda de la red LTE para REP_2.

Fuente. Propia

De la misma forma se mide la intensidad de señal LTE para el router REP_1 con el aplicativo G-NetTrack Lite utilizando el celular Pocophone F1, obteniendo una intensidad RSRP de -81 dBm, siendo óptima para la red propuesta, Figura 8.

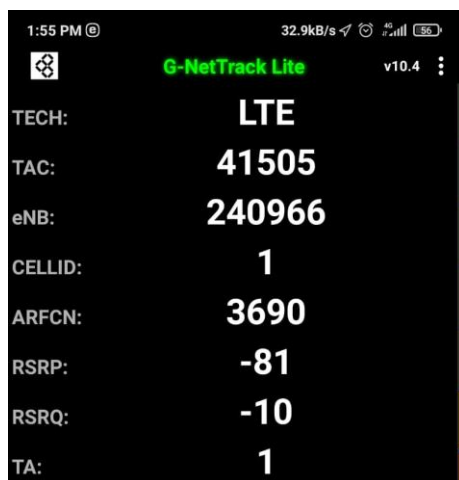


Figura 8. Nivel de intensidad de la red LTE para REP_1. Fuente. Propia

Se mide el ancho de banda para la REP_1 con el aplicativo Speedtest, obteniendo 14.0 Mbps de bajada y 12.9Mbps de subida, latencia de 16 ms y un jitter de 8ms, Figura 9.



Figura 9. Parámetros del ancho de banda de la red LTE para REP_1.
Fuente. Propia

Desde el SERVIDOR VPN L2TP/IPSEC se monitorea las conexiones hacia los MODEM ROUTER MIKROTIK REP_2 y ROUTER MIKROTIK REP_1, obteniendo como resultado 42 ms para el enlace hacia REP_1 y 44 ms para el enlace de REP_2 desde el servidor, Figura 10.

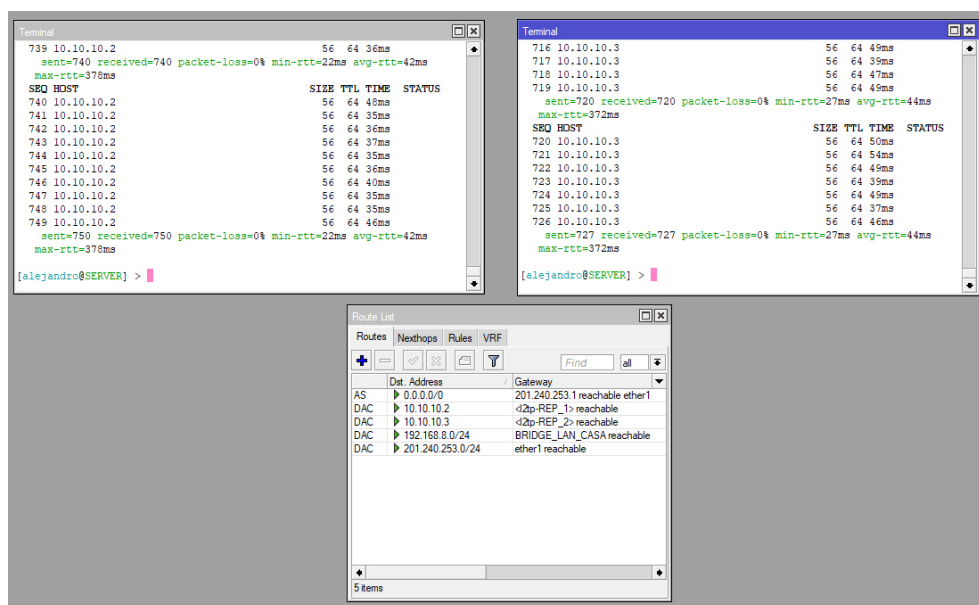


Figura 10. Latencia desde el SERVER VPN L2TP/IPSEC a las REP_1 y REP_2 desde RouterOS. Fuente. Propia

Se prueba la conectividad del diseño de red lógico realizando ping desde la unidad de interface de REP_1 a la unidad de interface de REP_2, la medición se realizó conectado en el Mikrotik RB930-2nD de REP_1, Figura 11.

```

Administrador: C:\WINDOWS\system32\cmd.exe
Respuesta desde 192.168.1.20: bytes=32 tiempo=87ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=85ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=89ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=90ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=97ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=81ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=150ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=98ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=87ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=79ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=81ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=88ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=102ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=97ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=82ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=89ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=91ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=87ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=102ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=80ms TTL=64
Respuesta desde 192.168.1.20: bytes=32 tiempo=97ms TTL=64

Estadísticas de ping para 192.168.1.20:
    Paquetes: enviados = 75, recibidos = 75, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 71ms, Máximo = 183ms, Media = 99ms
Control-C
^C
C:\Users\Usuario>

```

Figura 11. Ping de unidad de interface REP_1 a la unidad de interface REP_2 desde Interprete de Comandos de Windows. Fuente. Propia

De la misma forma se prueba la conectividad desde la unidad de interface de REP_2 a la unidad de interface de REP_1, la medición se realizó conectado en el Mikrotik RB930-2nD de REP_2. Se comprueba que está dentro de los rangos recomendados según Rendon (2017) en la paginas 62 al 65 y 74 de su investigación, Figura 12.

```

Administrador: C:\WINDOWS\system32\cmd.exe
Respuesta desde 192.168.1.10: bytes=32 tiempo=90ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=84ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=75ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=68ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=78ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=98ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=94ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=91ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=72ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=87ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=79ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=78ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=75ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=97ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=85ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=85ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=93ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=84ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=83ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=95ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=82ms TTL=64

Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 140, recibidos = 140, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 59ms, Máximo = 112ms, Media = 84ms
Control-C
^C
C:\Users\Usuario>

```

Figura 12. Ping de unidad de interface REP_2 a la unidad de interface REP_1 desde Interprete de Comandos de Windows. Fuente. Propia

Se procede a realizar las mediciones de los paquetes en el sistema RoIP, iniciamos con la medición del Jitter para REP_1. Se obtiene un jitter de variación máxima de 68.48 ms con 0% de paquetes perdidos, Figura 13.

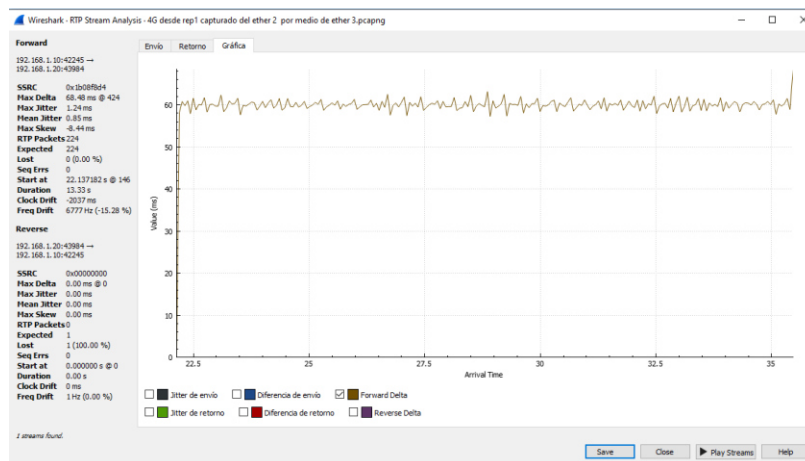


Figura 13. Medición de Jitter de variación máxima en el sistema para REP_1 IP:192.168.1.10/24. Fuente. Propia

Se mide el ancho de banda consumido por la REP_1 para transmitir información hasta la REP_2. Se observa que consume 15 kbps. Figura 14.



Figura 14. Medición del ancho de banda consumido para llegar a la REP_1. Fuente. Propia

Se procede a realizar las mediciones de los paquetes en el sistema RoIP para REP_2. Se obtiene un jitter de variación máxima de 68.53 ms con 0% de paquetes perdidos, Figura 15.

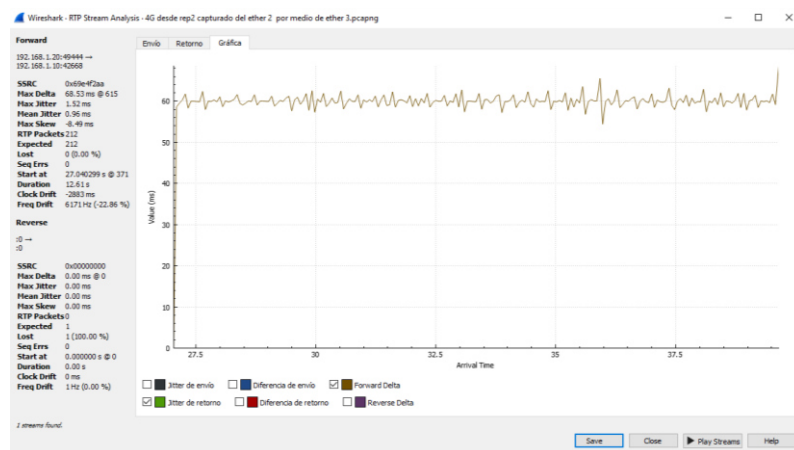


Figura 15. Medición de Jitter de variación máxima en el sistema para REP_2
IP:192.168.1.20/24. Fuente. Propia

Se mide el ancho de banda consumido por la REP_2 para transmitir información hasta la REP_1. Se observa que consume 15 kbps, Figura 16.

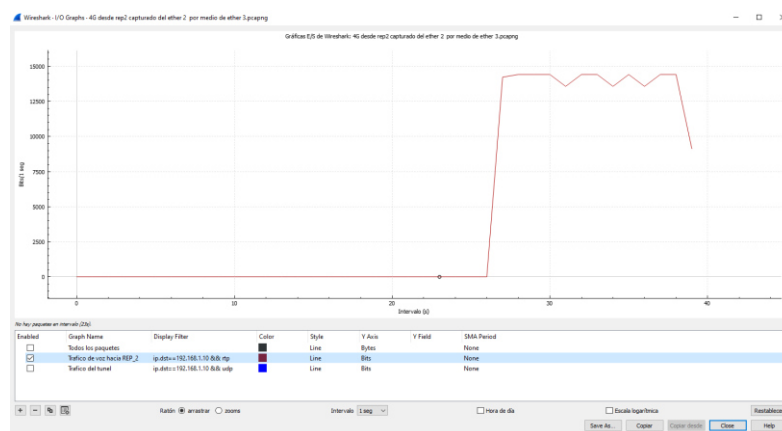


Figura 16. Medición del ancho de banda consumido para llegar a la REP_2.
Fuente. Propia

Se realiza la prueba de calidad de audio con el personal de Centauro Comunicaciones, valorando la calidad del audio del 1 al 5 indicados con su mano, siendo 5 una calidad audio perfecto, Figura 17 y Figura 18.



Figura 17. Percepción de la calidad de audio del sistema, puntuación 4/5.

Fuente. Propia



Figura 18. Percepción de la calidad de audio del sistema, puntuación 5/5.

Fuente. Propia

Por último, se mide el tiempo de establecimiento de conexión, el energizar todos los equipos a la vez, Figura 19, Figura 20 y Figura 21.



01:29.69

Figura 19. Tiempo de establecimiento de la conexión entre las repetidoras, intento número 01. Fuente. Propia



01:24.95

Figura 20. Tiempo de establecimiento de la conexión entre las repetidoras, intento número 02. Fuente. Propia



01:10.39

Figura 21. Tiempo de establecimiento de la conexión entre las repetidoras, intento número 03. Fuente. Propia

CAPITULO IV

CONCLUSIONES

4.1 Justificación

Se verifica los objetivos:

- ✓ La red privada virtual sobre la red LTE interconecta las repetidoras de radio digital de dos vías.

Al tener conectividad menor a 100ms entre las dos interfaces de red para los dos almacenes se comprueba que las dos repetidoras de radio digital de dos vías se interconectan cumpliendo los requisitos de Motorola a través de la red privada virtual sobre la red LTE. Asimismo, la red LTE como medio de transporte es indispensable por tener bajas latencias de acceso al SERVIDOR VPN L2TP/IPSEC junto con su gran ancho de banda.

- ✓ La red privada virtual sobre la red LTE con el protocolo de túnel L2TP/IPSEC interconecta las repetidoras de radio digital de dos vías.

Se verifica que el protocolo de túnel L2TP/IPSEC permite conectar dos interfaces de radio, con tiempo de conexión en promedio de 81 segundos. Utiliza el protocolo UDP en la capa de transporte, siendo el recomendado para transmitir voz, a ello se suma el protocolo de seguridad IPSEC el cual encripta la información que fluye por el túnel L2TP.

- ✓ La red privada virtual sobre la red LTE con el tipo de acceso remoto interconecta las repetidoras de radio digital de dos vías.

La tecnología de red privada virtual presenta el tipo de acceso remoto, el cual permite conectar a las dos repetidoras de radio digital de dos vías, debido a que en los Modem – Router 4G-LTE los operadores de telecomunicaciones

no asignan IP pública y los repetidores pueden estar ubicados en todo el Perú dentro de la cobertura de señal celular 4G-LTE.

4.2 Metodología aplicada

4.2.1 FASE I: Identificación de necesidades y objetivos de los clientes

Para la interconexión de la repetidora de radio digital de dos vías se utiliza las recomendaciones de la marca Motorola tomado del Módulo 1 Información del producto y sistema Mototrbo 2018 (p.14) para el correcto funcionamiento sobre una red interna o una red LAN:

IP Site Connect necesita:

- Al menos una dirección IP estática por red
- Aproximadamente 40 kbps por enlace del repetidor
- Latencia de red menor que 90 ms
- Jitter de red menor que 60 ms

Suin (2016. p.50, de *Diseño e implementación de una red RoIP de dos vías para la Empresa Maxigroup*. Trabajo de titulación para obtener el título de Ingeniero Electrónico. Ecuador – Quito. Universidad Politécnica Salesiana), establece una escala del jitter para una llamada de 2 minutos sobre una red LAN, Tabla 2:

Tabla 2

Jitter en la red IP. Fuente. Tomado de Suin (2016). Diseño e implementación de una red RoIP de dos vías para la Empresa Maxigroup. Trabajo de titulación para obtener el título de Ingeniero Electrónico. Ecuador – Quito. Universidad Politécnica Salesiana. (p.50)

Variabilidad del retardo	
Excelente	0 ms – 150 ms
Bueno	150 ms – 300 ms
Pobre	300 ms – 400 ms

Rendón (2017.p.62-65,74, de *Evaluación de métodos para realizar mediciones de calidad de servicio VoIP en redes móviles de cuarta generación (LTE) en ambientes urbanos de la ciudad de Guayaquil*. Tesis para optar el título de Magister en Telecomunicaciones. Ecuador – Guayaquil. Escuela Superior Politécnica del Litoral), describe las principales afectaciones o problemas que ocurren en una red IP durante una llamada de VoIP sobre la red LTE, las cuales tomaremos en cuenta para nuestro diseño:

- Jitter UDP de hasta 60ms
- Retraso [latencia] de hasta 150 ms
- Pérdida de datagramas debería ser cero
- Paquetes con errores
- Entrega desordenada de datagramas
- Eco

Las limitaciones de la red LTE en general abarcan un campo de estudio completo y pueden ser tema de futuras investigaciones y desarrollos de temas de grado. Específicamente las limitaciones de LTE para VoIP estarían relacionadas principalmente a cobertura y calidad de señal LTE

Blanco (2018, p.65, de *Evaluación de los modelos utilizados para la medición de los parámetros de calidad de servicio en la telefonía IP*. Tesis presentada como requisito parcial para optar el título de Magister en Ingeniería – Telecomunicaciones. Bogotá – Colombia. Universidad Nacional de Colombia) para calcular el ancho de banda de una comunicación RoIP por canal utilizaremos la guía de cálculo de VOIP de Blanco.

1.- Tamaño de los encabezados de los protocolos utilizados en la transmisión de la llamada.

IP: 20 bytes

UDP: 8 bytes

RTP: 12 bytes

Ethernet: 26 bytes

Dependiendo del tipo de protocolo de Capa 2 el encabezado puede cambiar, para el caso de Ethernet son 18 octetos, pero se pueden utilizar otros protocolos y de acuerdo a esto cambiar el ancho de banda requerido para una comunicación. En la Tabla 3 se aprecia los octetos de los encabezados de los paquetes:

Tabla 3

Paquete de RoIP. Fuente. Tomado de Blanco (2018). Evaluación de los modelos utilizados para la medición de los parámetros de calidad de servicio en la telefonía IP. Tesis presentada como requisito parcial para optar el título de Magister en Ingeniería – Telecomunicaciones. Bogotá – Colombia. Universidad Nacional de Colombia. (p.66)

Encabezados				Carga útil de la voz
Ethernet (26 bytes)	IP (20 bytes)	UDP (8 bytes)	RTP (12 bytes)	

2.- El Códec utilizado y la velocidad de bits por segundo.

El ancho de banda requerido para transportar la voz durante una llamada está definido como:

$$\text{Ancho de banda por llamada} = (\text{tamaño del paquete de voz}) * \text{PPS}$$

Siendo PPS: Paquetes por segundo.

El procedimiento para calcular el ancho de banda requerido para transportar la voz utiliza el Códec AMBE +2, cuya calidad de servicios es MOS=4.0 es el siguiente:

Tamaño total del paquete:

$$\text{Tamaño total del paquete (bytes)} = (\text{encabezado Capa 2}) + (\text{encabezado IP, UDP, RTP}) + (\text{carga útil de voz})$$

$$\text{Tamaño total del paquete (bytes)} = 26 \text{ bytes} + 40 \text{ bytes} + 9 \text{ bytes}$$

$$\text{Tamaño total del paquete (byte)} = 75 \text{ bytes}$$

$$\text{Tamaño total del paquete (bits)} = 75 \text{ bytes} * 8 \text{ bits por byte}$$

$$\text{Tamaño total del paquete (bits)} = 600 \text{ bits}$$

PPS (Paquetes por segundo):

$$PPS = \frac{(\text{Velocidad de transmision del codec})}{(\text{Tamaño de la carga util de la voz})}$$

Donde:

$$\text{Tamaño de la carga útil de la voz (bits)} = \text{Tamaño de la carga útil de la voz (bytes)} * 8 \text{ bits por byte}$$

Para el códec AMBE +2, el tamaño de carga útil de la voz (bytes) es de 9 bytes con una duración del paquete de 20 ms y la velocidad de bits del códec es de 3.6 kbps.

$$\text{Tamaño de la carga útil de la voz (bits)} = 9 \text{ bytes} * 8 \text{ bits por byte}$$

$$\text{Tamaño de la carga útil de la voz (bits)} = 72 \text{ bits}$$

$$PPS = \frac{(\text{Velocidad de transmision del codec})}{(\text{Tamaño de la carga util de la voz})}$$

$$PPS = \frac{3.6 \text{ kbps}}{72 \text{ bits}}$$

$$PPS = 50 \text{ pps}$$

Entonces:

$$\text{Ancho de banda por llamada} = (\text{tamaño del paquete de voz}) * PPS$$

$$\text{Ancho de banda por llamada} = 600 \text{ bits} * 50 \text{ pps}$$

$$\text{Ancho de banda por llamada} = 30 \text{ kbps}$$

Las comunicaciones de radio digital de dos vías utilizan la mitad del ancho de banda por ser una comunicación half dúplex por canal:

$$\text{Ancho de banda requerido RoIP por canal} = 15 \text{ kbps}$$

Se calcula los datos consumidos para 8 horas por día de comunicación fluida según el ancho de banda requerido:

$$\text{Datos por dia} = \text{Ancho de banda} * \text{tiempo}$$

$$\text{Datos por dia} = 15 \text{ kbps} * 28800 \text{ s}$$

$$\text{Datos por dia} = 432000 \text{ kb}$$

$$\text{Datos por dia} = 54000 \text{ KB}$$

$$\text{Datos por dia} = 54 \text{ MB}$$

$$\text{Datos por dia} = 0.054 \text{ GB}$$

Calculamos para 31 días:

$$\text{Datos al mes} = 1.674 \text{ GB}$$

Se requiere una conexión a internet por telefonía celular que nos proporcione un ancho de banda de 15 kbps, siendo factibles UMTS, HSPA y HSDPA, pero estas tecnologías presentan latencia de acceso a internet superiores a los 100 ms, por lo cual no son factibles para la solución que requiere en total 100 ms. Se utiliza la tecnología 4G-LTE al poseer una latencia de acceso promedio de 50ms, se requiere un plan de datos para 31 días de 1.674 GB. El operador Bitel nos presenta el Plan Único, Figura 22, 1 GB por día, superando nuestro requerimiento.

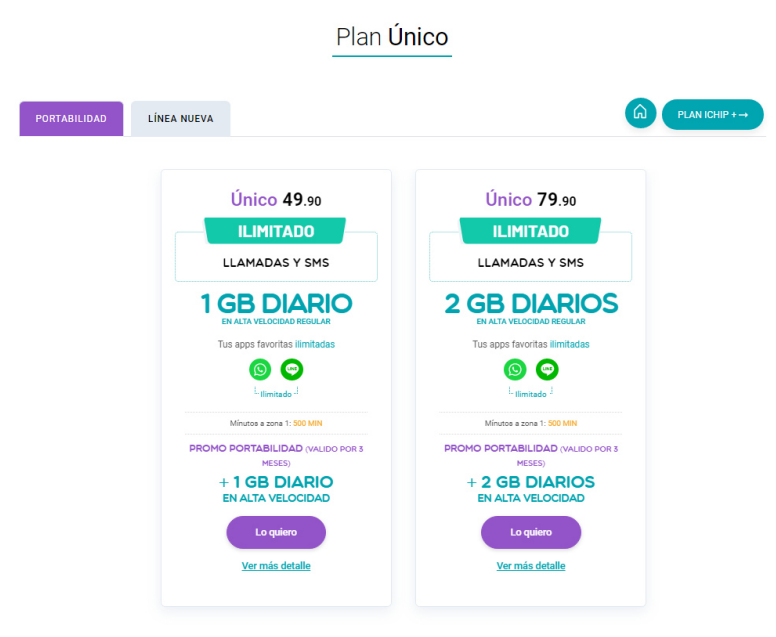


Figura 22. Plan de datos del operador Bitel. Fuente. Página web de Bitel – Plan Único, setiembre 2020

Con respecto a la calidad del audio entregado, tomaremos las recomendaciones de Motorola:

Consideraciones acerca de la capacidad de los perfiles de tráfico estándar de voz se resumen en la siguiente Tabla 4:

Tabla 4

Capacidad de los perfiles de tráfico estándar de voz. Fuente. Tomado Modulo 2 Diseño del sistema: topologías, planificación de la capacidad y configuraciones. Motorola 2018. (p.97)

Nombre de perfil	Tipo de tráfico	Descripción de llamada	Tráfico por usuario por hora	
Voz alta	Llamada de voz grupal	Llamada de 10 segundos, 2 transmisiones por llamada	3,0 llamadas por usuario por hora	90 %
	Llamada de voz individual	Llamada de 20 segundos, 4 transmisiones por llamada		10 %
Voz baja	Llamada de voz grupal	Llamada de 10 segundos, 2 transmisiones por llamada	1,0 llamadas por usuario por hora	90 %
	Llamada de voz individual	Llamada de 20 segundos, 4 transmisiones por llamada		10 %

El DAQ “Delivered Audio Quality” (Calidad de audio entregado) mide la inteligibilidad y calidad de la voz transmitida a través de un sistema de comunicaciones. La calidad del audio se mide en una escala de 5 puntos y normalmente los clientes buscan DAQ 3 como mínimo, [Tabla 5]. (p.76)

Tabla 5

Nivel de calidad de audio entregado. Fuente. Tomado de Modulo 1 Información del producto y sistema Mototrbo,2018. (p.77).

Nivel de DAQ	Calidad de voz
DAQ 1	No se puede utilizar. Hay voz pero no es comprensible.
DAQ 2	Voz comprensible con considerable esfuerzo. Requiere repeticiones frecuentes debido al ruido o la distorsión.
DAQ 3	Voz comprensible con un pequeño esfuerzo. Requiere repeticiones ocasionales debido al ruido o la distorsión.
DAQ 3,4	Voz comprensible sin repeticiones. Hay un poco de ruido o distorsión.
DAQ 4	Voz fácilmente comprensible. Poco ruido o distorsión.
DAQ 5	Perfecto. No se distingue distorsión ni ruido.

4.2.2 FASE II: Diseño lógico

En la Figura 23 se observa la topología lógica de red que se implementará. Se utiliza direcciones IP de mascara 24 para la red LAN de voz y disponer de direcciones IP según la siguiente Tabla 6:

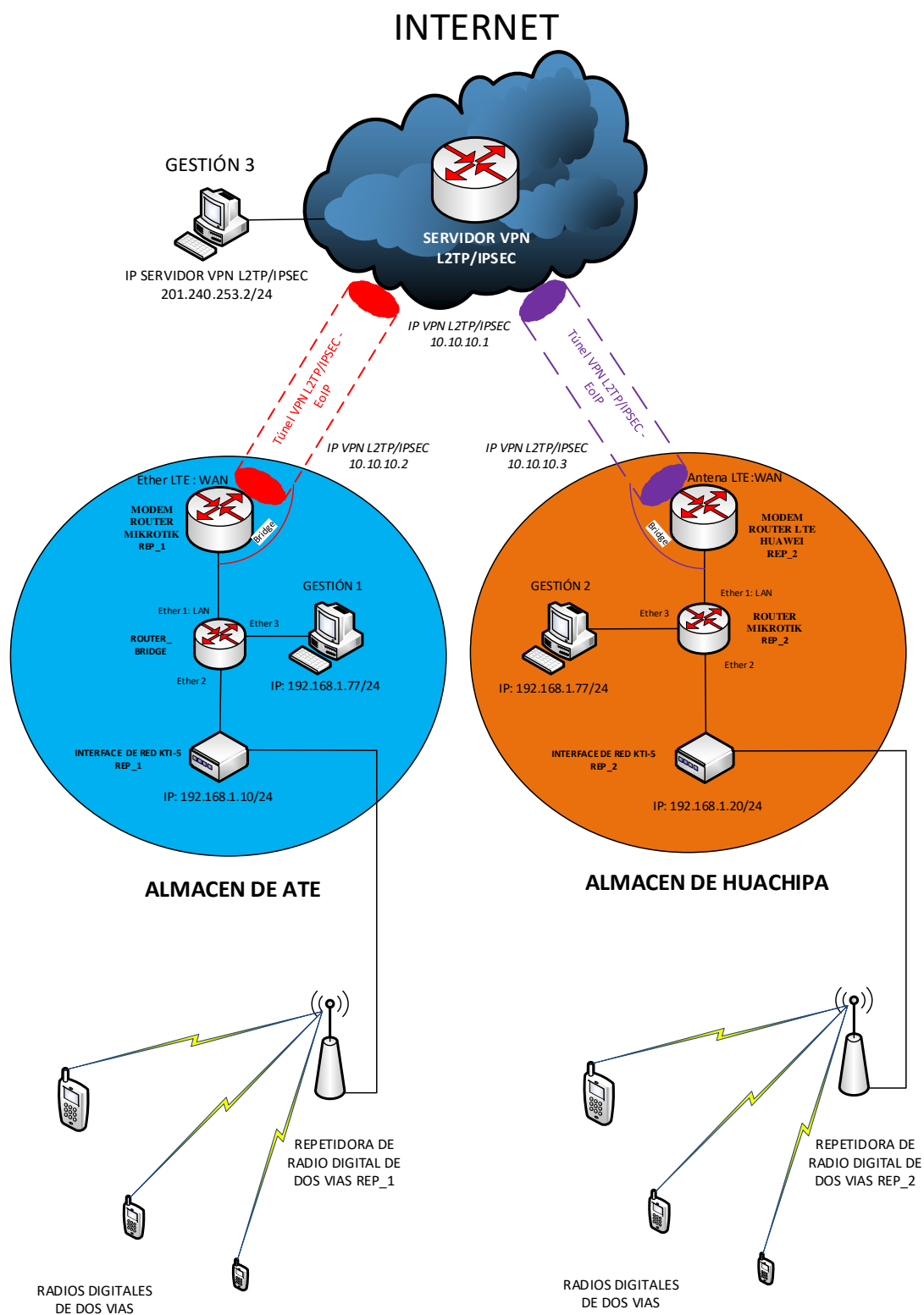


Figura 23. Topología lógica de red. Fuente. Propia

Tabla 6

Dirección IP de la red IP del sistema RoIP. Fuente. Propia

NOMBRE	DIRECCIÓN IP
Red LAN	192.168.1.0/24
Gateway	192.168.1.254/24
Broadcast	192.168.1.255/24
Interface de Red KTI-5 REP_1	192.168.1.10/24
Interface de Red KTI-5 REP_2	192.168.1.20/24
Gestión REP_1 o REP_2	192.168.1.77/224

La red IP de los almacenes de Ate y Huachipa tendrán una dirección IP en su interfaz WAN, a la cual se realiza un nateo para la red, lo cual permite salir de la red la dirección privada que esta asignada a la Interface de Red del Repetidor de radio digital de dos vías.

Para interconectar las dos redes: Ate y Huachipa, se realiza el enrutamiento estático hacia el SERVIDOR VPN L2TP/IPSEC en la nube, mediante túneles de red privada virtual L2TP/IPSEC tipo de acceso remoto, de tal manera que los datos de la red de Ate irán primero al SERVIDOR VPN L2TP/IPSEC y desde ahí se enruta a la red de Huachipa. Se muestra la Tabla 7 que enrutará los paquetes de la red de Ate con la de Huachipa.

Tabla 7

Enrutamiento de red para los almacenes de Ate y Huachipa. Fuente. Propia

DISPOSITIVO	RED A ALCANZAR	PUERTA DE ENLACE PREDETERMINADO
MODEM ROUTER MIKROTIK REP_1	10.10.10.3/24	10.10.10.1/24
ROUTER MIKROTIK REP_2	10.10.10.2/24	10.10.10.1/24
SERVIDOR VPN L2TP/IPSEC	10.10.10.2/24	<l2tp-REP_1>
SERVIDOR VPN L2TP/IPSEC	10.10.10.3/24	<l2tp-REP_2>

En el ámbito de seguridad para la red LAN será cubierta por la red privada virtual L2TP/IPSEC que permitirá un viaje seguro de los datos mediante el túnel L2TP encriptando la información con protocolo IPSEC. El ingreso de los usuarios a la red LAN estará permitido a la IP llamada Gestión, para prevenir el acceso a la configuración de los dispositivos de red se definirán nuevos usuarios y contraseñas y para los ataques a la red WAN como Syn Flood, Denial os Services y DNS Relay Attack se implementarán medidas de seguridad que bloquearán dichos ataques.

4.2.3 FASE III: Diseño físico

Los equipos necesarios para cumplir con el diseño lógico lo podemos apreciar en la Figura 24.

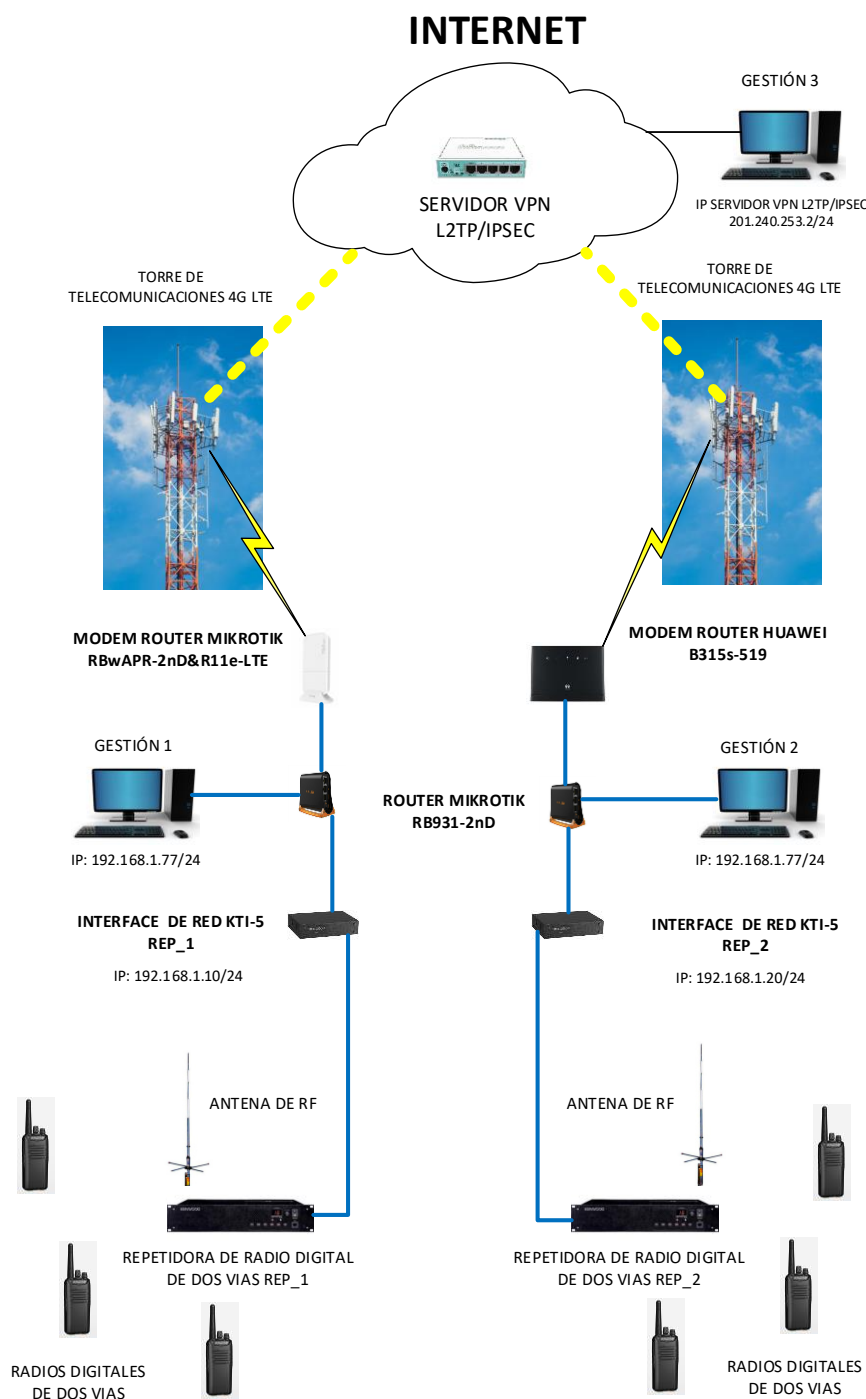


Figura 24. Topología física de red. Fuente. Propia

4.2.4 FASE IV: Fase de prueba, optimización y documentación

Para obtener la interconexión de la repetidora digital de radio de dos vías de Ate con la de Huachipa según la topología lógica, Figura 23, y física, Figura 24, se necesita realizar la configuración en el equipamiento seleccionado en la Fase III.

Las redes privadas virtuales son el mecanismo ideal para conectarse a la red interna, logrando desde un punto externo acceder a los diferentes servicios internos que se ofrecen. Se ha seleccionado la red privada virtual basado en hardware (Mikrotik) y de tipo acceso remoto para los clientes: almacenes de Ate y Huachipa. Se utiliza la tecnología L2TP/IPSEC porque utiliza para el transporte de paquetes IP el protocolo UDP, además presenta una rápida conexión del enlace y tiene una elevada seguridad gracias el protocolo IPSEC.

Se inicia con la configuración del SERVIDOR VPN L2TP/IPSEC, para ello, se activa la casilla L2TP Server, se selecciona Profile L2TP/IPSEC, utilizando autenticación Chap - Pap, y una contraseña a IPsec, Figura 25.

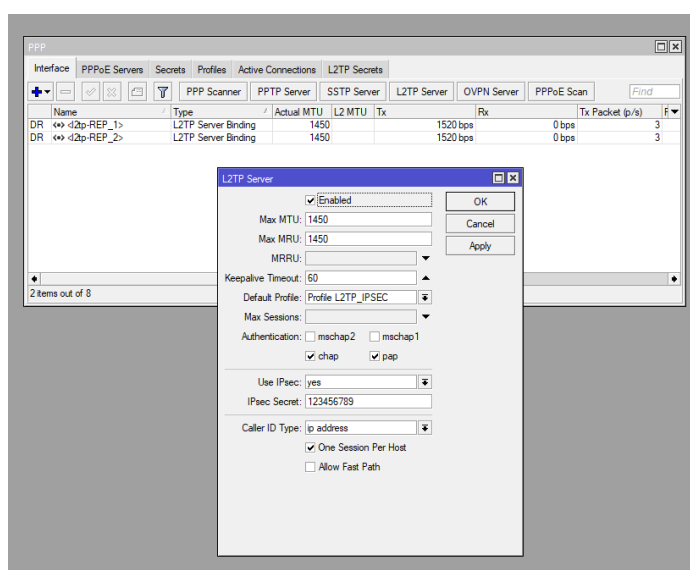


Figura 25. Habilitación del servidor L2TP/IPSEC. Fuente. Propia

Se realiza la configuración del cliente de la red privada virtual L2TP/IPSEC, para ello se configura el Dial-Out, ingresando la dirección IP pública del SERVIDOR VPN L2TP/IPSEC: 201.240.253.2/24, usuario y contraseña de Secret, habilitaremos Use IPsec y la contraseña, se utiliza la misma autenticación que la del SERVIDOR VPN L2TP/IPSEC, Figura 26.

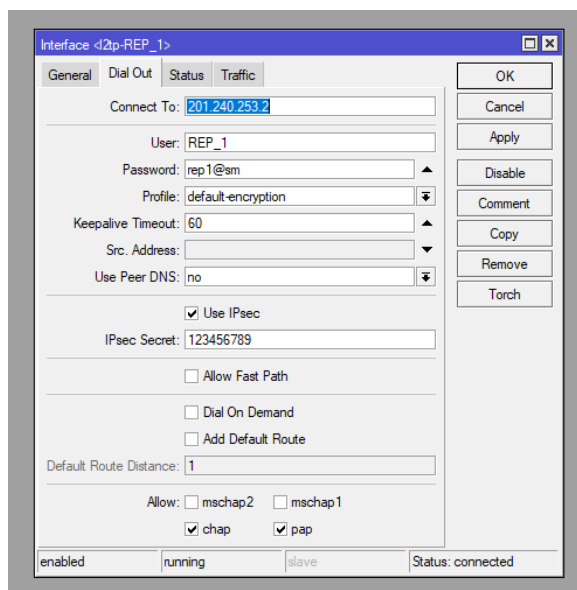


Figura 26. Configuración del Cliente L2TP/IPSEC del almacén de Ate REP_1. Fuente. Propia

Se agrega la interfaz EoIP Túnel para REP_1, con el direccionamiento según la IP local 10.10.10.2 y IP destino 10.10.10.3 creados por el túnel L2TP/IPSEC. Se asigna un ID de túnel 10, Figura 27.

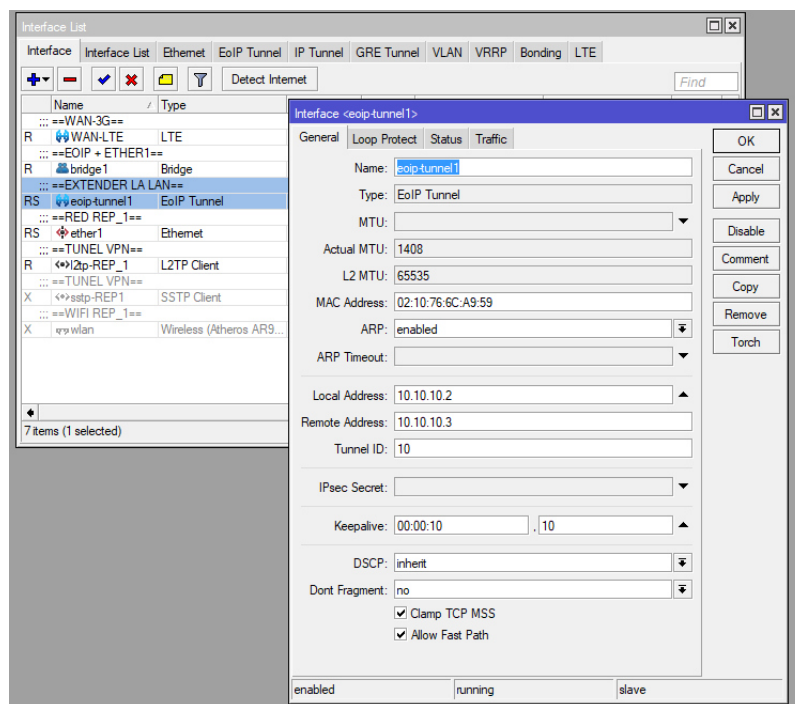


Figura 27. Configuración de Túnel EoIP. Fuente. Propia

Se asigna la dirección IP según el diagrama lógico al bridge1, Tabla 6: Dirección IP de la red IP del sistema RoIP, Figura. 28.

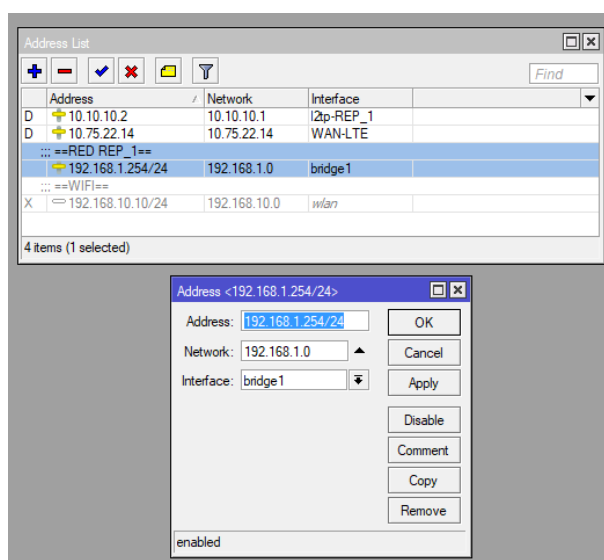


Figura 28. Asignación de las direcciones según la tabla: Dirección IP de la red IP del sistema RoIP. Fuente. Propia

Se realiza el mismo procedimiento para el ROUTER MIKROTIK REP_2 respetando la Figura 23 diseño lógico, la Tabla 6 Dirección IP de la red IP del Almacén Huachipa y Tabla 7 Enrutamiento de red para los almacenes de Ate y Huachipa

Se configura la VPN L2TP/IPSEC hacia el servidor VPN L2TP/IPSEC, se ingresa la dirección IP:201.240.253.2, user: REP_2, contraseña: rep2@sm, contraseña IPSEC: 123456789, Figura 29.

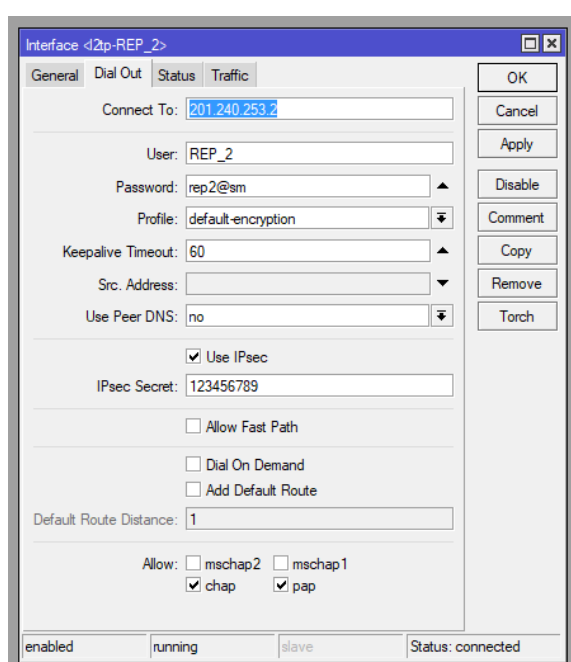


Figura 29. Configuración del VPN L2TP/IPSEC de REP_2. Fuente. Propia

Se agrega el túnel EoIP, para ello se configura la dirección IP local 10.10.10.3 y dirección IP remota 10.10.10.2, con ID de túnel 10, Figura 30.

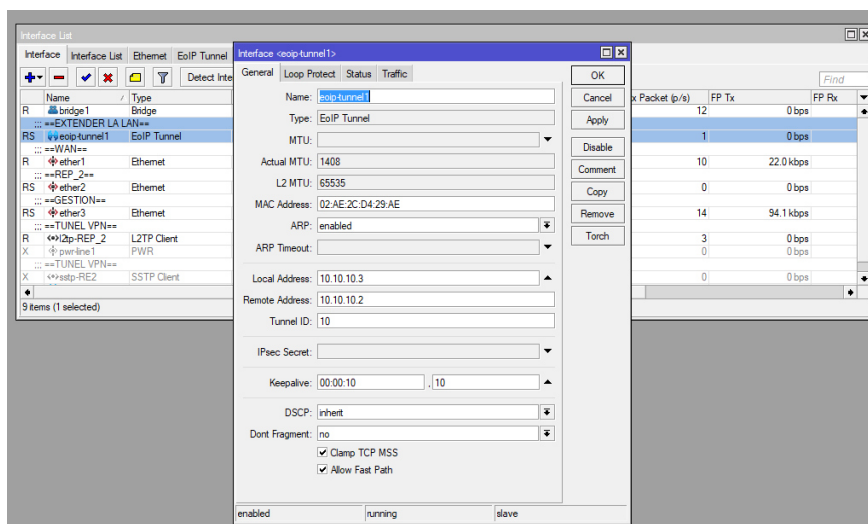


Figura 30. Túnel EoIP para REP_2. Fuente. Propia

Para utilizar los dos puertos (Ether 2 y Ether 3) dentro de la misma red, se realiza un Bridge con nombre bridge1 en el cual se agrega las dos interfaces. Para extender la red LAN de REP_1 a REP_2, se agrega al bridge1 el túnel EoIP, Figura 31.

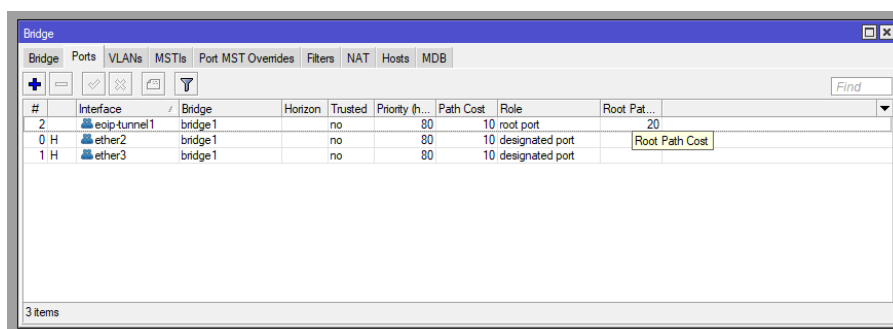


Figura 31. Bridge de las interfaces Ether 2, Ether 3 y el Túnel EoIP. Fuente. Propia

La optimización de la red física se podría llevar a cabo al replicar la red del almacén de Ate en el almacén de Huachipa y reemplazar el Modem HUAWEI B315S-519, RBwAPR-2nD&R11e-LTE por RBLHGR&R11e-LTE y Router RB931-2nD por el Switch TL-SF1005D.

4.3 Descripción de la implementación

La implementación se lleva a cabo en el laboratorio de Centauro Comunicaciones, como lo muestra las siguientes imágenes, Figura 32 hasta la Figura 35:



Figura 32. Implementación del sistema de repetidora REP_1 con enlace LTE, parte frontal. Fuente. Propia



Figura 33. Implementación del sistema de repetidora REP_1 con enlace LTE, parte posterior. Fuente. Propia



Figura 34. Implementación del sistema de repetidora REP_2 con enlace LTE, parte frontal. Fuente. Propia



Figura 35. Implementación del sistema de repetidora REP_2 con enlace LTE, parte posterior. Fuente. Propia

4.4 Conclusiones

- Se puede interconectar dos hosts (repetidoras de radio digital de dos vías) con IP/CGNAT a través de un servidor de enrutamiento.
- La tecnología LTE de telefonía móvil, permite crear nuevos servicios por Internet al tener una baja latencia de acceso y un gran ancho de banda.
- Debido al rápido crecimiento tecnológico a nivel mundial es posible contratar servidores privados virtuales, permitiéndonos implementar cualquier servidor a precios muy competitivos.
- Se puede interconectar dos repetidores de radio sin importar la modulación digital, frecuencia de operación y lugar geográfico dentro de la cobertura de la red LTE, a través de una interface de red.
- El Router servidor de VPN Mikrotik se gestiona por Web y APP desarrollado por la marca
- Los operadores de telefonía móvil brindan una IP pública con IP/CGNAT con DHCP de 24 horas y su tiempo de reconexión demora aproximadamente 30 segundos.
- Se denomina solución plug and play, transparente para el usuario final.

CAPITULO V

RECOMENDACIONES

- Seleccionar enrutadores con dos o tres interfaces de telefonía móvil para poder contar enlaces backup's ante la caída de una estación base o la renovación de la IP publica por DHCP.
- Seleccionar equipos para uso externo con IP54 y así obtener intensidad de señal de telefonía móvil superior a los -85 dBm (4/5 barras de la señal de telefonía móvil LTE).
- Contratar un servicio de almacenamiento en la nube a nivel local para implementar el servidor de enrutamiento y obtener una disponibilidad del 99% en caso que no se pueda implementar el servidor en la empresa o localmente.
- Para la medición con WireShark se recomienda utilizar un switch administrable para poder capturar la información a través de Port Mirroring.

CAPITULO VI

BIBLIOGRAFIA

American Psychological Association, & Association, A. P. (2010). *Manual de publicaciones de la APA*. Taylor & Francis.

Ariganello, E. (2014). Redes Cisco Guía de estudio para la certificación CCNA Security (1.a ed.). RA-MA.

Atencio y Mamani (2017). *Diseño e implementación de un prototipo de red privada virtual en capa 3 utilizando Cisco IOS para la Universidad Nacional del Altiplano*. Tesis para la obtención del grado de Ingeniero Electrónico. Puno -Perú. Universidad Nacional del Altiplano.

Blanco (2018). *Evaluación de los modelos utilizados para la medición de los parámetros de calidad de servicio en la telefonía IP*. Tesis presentada como requisito parcial para optar el título de Magister en Ingeniería – Telecomunicaciones. Bogotá – Colombia. Universidad Nacional de Colombia.

Caldera, Suazo y Ramírez (2010). *Modulo III: Telefonía IP*, Universidad Nacional de Ingeniería Nicaragua.

Canó Academy (2020), *Seminario web VPN para voz*. República Dominicana.

Choque (2012). *Implementación de una repetidora en la banda VHF para la ampliación de cobertura en la ciudad de la Paz*. Trabajo de aplicación para obtener el título de Ingeniero Electrónico y Telecomunicaciones- Bolivia – La Paz. Universidad Mayor de San Andrés.

Comms 2014 Connect (2014). Presentation Title: *Advanced Radio Over IP Speaker: Paul Whitfield*. Omnitronics.

- Córdova (2020). *Diseño de una red LTE escalable para la transmisión de video IP aplicado a la seguridad ciudadana*. Tesis para optar el título profesional de Ingeniero de Redes y Comunicaciones. Lima – Perú. Universidad Peruana de Ciencias Aplicadas.
- Delgado, Cáceres, Jorquera y Esquivel (2014). *Redes privadas virtuales (VPN)*. Colombia: Universidad Técnica Federico Santa María.
- De La Cruz y Vera (2019). *Implementación de una VPN con open Source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo*. Tesis para optar el título profesional de Ingeniero en Computación e Informática. Perú – Lambayeque. Universidad Nacional “Pedro Ruíz Gallo”.
- Elsa Jiménez (2018). *Diseño y dimensionamiento de un sistema de telecomunicaciones optimizado para el nuevo hospital de la provincia Espinar en Cusco*. Tesis para optar el título de Ingeniera de las Telecomunicaciones. Lima – Perú. Pontificia Universidad Católica del Perú.
- Excera AIS-DMR Settings*. (s. f.). Walkiefleet. Recuperado 25 de octubre de 2020, de <http://walkiefleet.com/aisdmrguide>.
- Huidobro Moya, J. M. (2014). *Comunicaciones Móviles Sistemas GSM, UMTS y LTE* (1.^a ed.). RA-MA.
- Jairo Restrepo Ángulo Cuaderno No. 2 Compendio de Telecomunicaciones, L. C. R. S. U. M. P. (2007). *Análisis de los procesos básicos de un sistema de comunicaciones*. Universidad de Medellín.
- Jiménez y Ochovo (2017). *Evaluación comparativa de redes móviles*. Proyecto de fin de carrera. Universidad Politécnica de Madrid.
- López (2018). *Análisis y diseño de un sistema de comunicación ROIP a través de la red de datos para el modelo de radios Motorola DGM 8000*. Tesis para optar el grado académico de Magister en Telecomunicaciones. Ecuador- Guayaquil. Universidad de Santiago de Guayaquil.

L2TP – MUM Mikrotik (2020). *Túneles L2Tp y EoIP para gestión y conexión L2*.

Mar (2016). *Propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco INEI CASO: Servidor de Correos*. Tesis para la obtención del grado de Ingeniero de Sistemas. Cusco – Perú. Universidad Andina del Cusco.

Martel (2019). *Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764*. Tesis para la obtención del grado de Ingeniero de Redes y Comunicaciones. Lima – Perú. Universidad Peruana de Ciencias Aplicadas.

Mimenza, O. C., & Castillero Mimenza, O. (2020, 25 noviembre). *Los 15 tipos de investigación (y características)*. Psicología y Mente. <https://psicologiaymente.com/miscelanea/tipos-de-investigacion>.

Minango y Valenzuela (2017). *Diseño de un sistema de comunicaciones digital para la empresa Dataradio Telecomunicaciones C.A. entre Ibarra y Tulcán*. Trabajo de titulación para la obtención del título de Ingenieros Electrónicos. Ecuador – Quito. Universidad Politécnica Salesiana.

Motorola (2018). Modulo 1 Información del producto y sistema Mototrbo.

Motorola (2018). Modulo 2 Diseño del sistema: topologías, planificación de la capacidad y configuraciones.

Municipalidad Distrital de Lurigancho (2020). *Plan de Acción Distrital de Seguridad Ciudadana 2020*.

Rábanos, J. M. H., Tomás, L. M., & Salis, J. M. R. (2013). *Transmisión por radio*. Centro de Estudios Ramón Areces.

Rendón (2017). *Evaluación de métodos para realizar mediciones de calidad de servicio VoIP en redes móviles de cuarta generación (LTE) en ambientes urbanos de la ciudad de Guayaquil*. Tesis para optar el título

de Magister en Telecomunicaciones. Ecuador – Guayaquil. Escuela Superior Politécnica del Litoral.

Omnitronics (2020). *VoIP for Radio Networks* Revisión 1. 1.

Pimentel (2019). *Diseño para la evolución de la red de voz de control de tránsito aéreo de la Fuerza Aérea utilizando tecnologías Radio sobre IP*. Tesis para optar el grado académico de Magister en Ingeniería de las Telecomunicaciones. Perú – Lima. Pontificia Universidad Católica del Perú.

Peru's Mobile and Broadband Internet Speeds. (s. f.). Speedtest Global Index. Recuperado 10 de octubre de 2020, de <https://www.speedtest.net/global-index/peru#mobile>.

Puga, N. (2017, 12 octubre). *La Tecnología de Compresión de Voz Más Avanzada del Mundo*. Syscom. <https://www.syscomblog.com/2017/10/la-tecnologia-de-compresion-de-voz-mas.html>.

¿Qué significa 3G y 4G? Definición y diferencias //. (2020, 30 agosto). SoftwareLab. <https://softwarelab.org/es/3g-4g-definicion-diferencias>.

República, L. (2020, 15 mayo). *Internet: Perú tiene un 93% de disponibilidad de 4G, pero velocidad aún es inconsistente*. La República. <https://larepublica.pe/economia/2020/05/15/internet-peru-tiene-un-93-de-disponibilidad-de-4g-pero-velocidad-aun-es-inconsistente/>.

Sevilla (2017). *Sistema de radiocomunicaciones para los centros de control del parque nacional Llanganates*. Proyecto de investigación para la obtención del título de Ingeniero en Electrónica y Comunicaciones. Ecuador – Ambato. Universidad Técnica de Ambato.

Scribbr. (2018, 18 diciembre). *Scribbr - Revisión académica a tu medida*. <https://www.scribbr.es/>.

Suin (2016). *Diseño e implementación de una red RoIP de dos vías para la Empresa Maxigroup*. Trabajo de titulación para obtener el título de Ingeniero Electrónico. Ecuador – Quito. Universidad Politécnica Salesiana.

TaitNet DMR (2015). DMR Introduction Training Manual.

Tipos de investigación. (2019, 10 diciembre). Significados. <https://www.significados.com/tipos-de-investigacion/>.

Toro (2020). *Implementación de algoritmos de medición de QoS para redes LTE utilizando el simulador OMNeT++*. Trabajo de titulación para obtener el título de Ingeniero en Telecomunicaciones. Ecuador – Guayaquil. Universidad Católica de Santiago de Guayaquil.

Understanding AIS – the DMR Application Interface Specification. (2016, 24 diciembre). The Dispatch Blog. <https://blog.catcomtec.com/2016/12/23/understanding-ais-the-dmr-application-interface-specification/>.

Voz sobre IP – Consumo de Ancho de Banda por Llamada. (2020, 17 enero). Cisco. https://www.cisco.com/c/es_mx/support/docs/voice/voice-quality/7934-bwidth-consume.html#anc1.

CAPITULO VII

ANEXOS

7.1 Anexo N°01: Configuración inicial del SERVIDOR VPN L2TP/IPSEC en Mikrotik

Ingresamos al SERVIDOR VPN L2TP/IPSEC por Winbox a través de la IP: 201.240.253.2 login: alejandro y password, Figura 36.

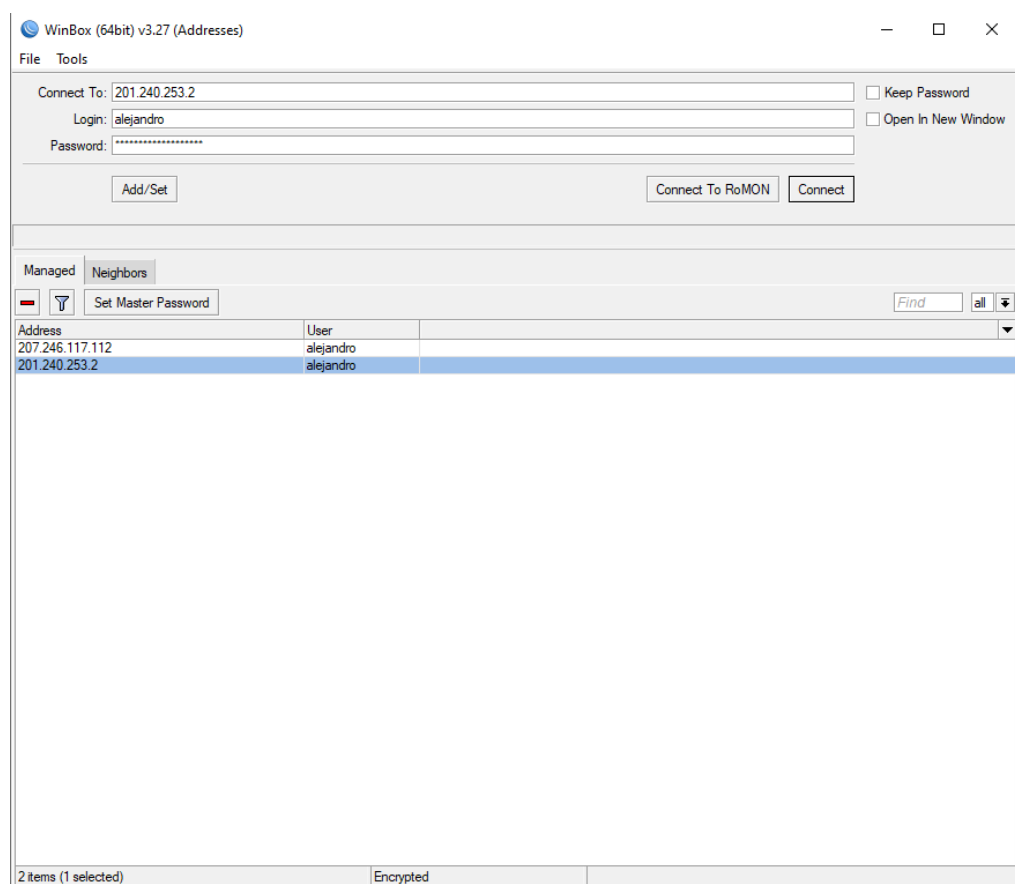


Figura 36. Ingreso a RouterOS por Winbox. Fuente. Propia

Actualizamos el software RouterOS desde System, Package, Figura 37.

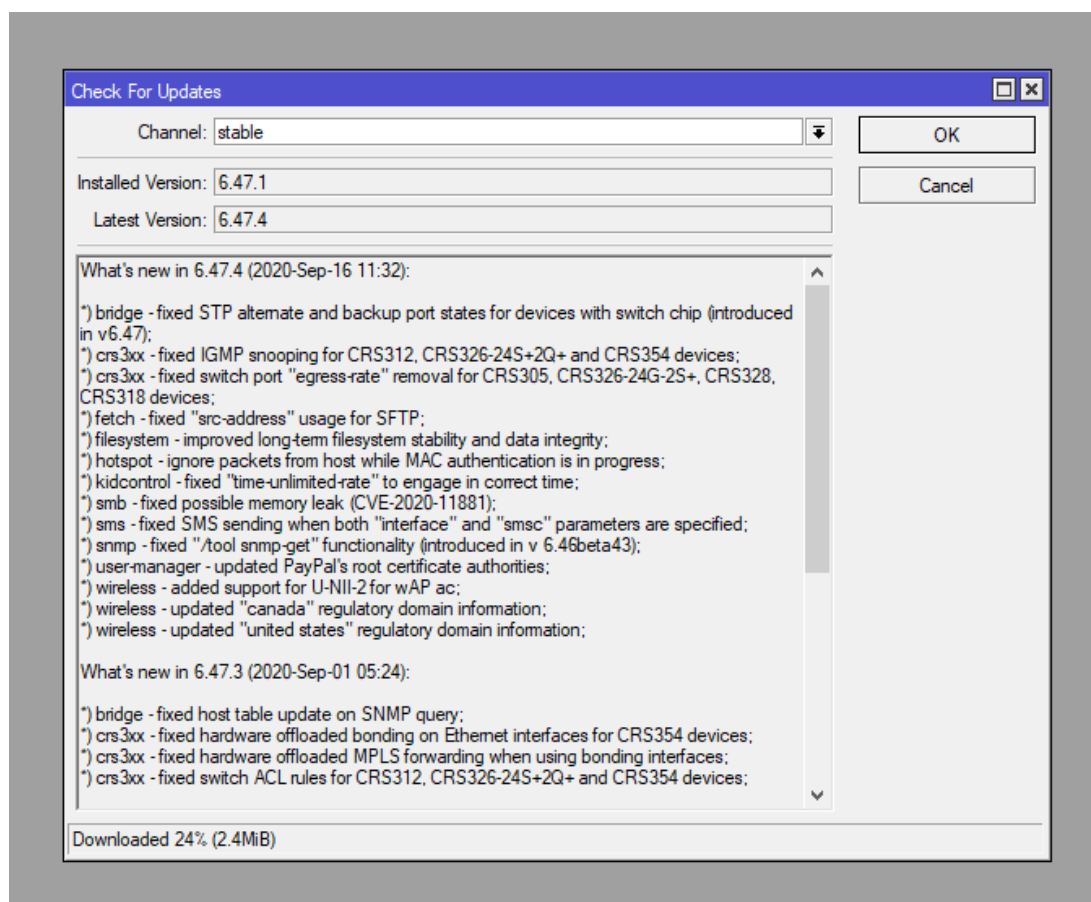


Figura 37. Actualización de RouterOS v6.47.4. Fuente. Propia.

Configuramos el servidor SNTP protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variables, para ello usamos dos de los servidores con la IP 201.217.3.85, Figura 38.

- ✓ 0.south-america.pool.ntp.org
- ✓ 1.south-america.pool.ntp.org
- ✓ 2.south-america.pool.ntp.org
- ✓ 3.south-america.pool.ntp.org

Figura 38. Configuración de SNTP Client. Fuente. Propia

Configuramos la hora del Mikrotik con la zona horaria -05 GTM Offset y Time Zone Name: América / Lima, Figura 39.

Figura 39. Configuración de la hora. Fuente. Propia

7.2 Anexo N°02: Seguridad básica en el SERVIDOR VPN

L2TP/IPSEC Mikrotik

Eliminamos el usuario y contraseña por defecto e ingresamos un nuevo usuario llamado alejandro con su contraseña, Figura 40.

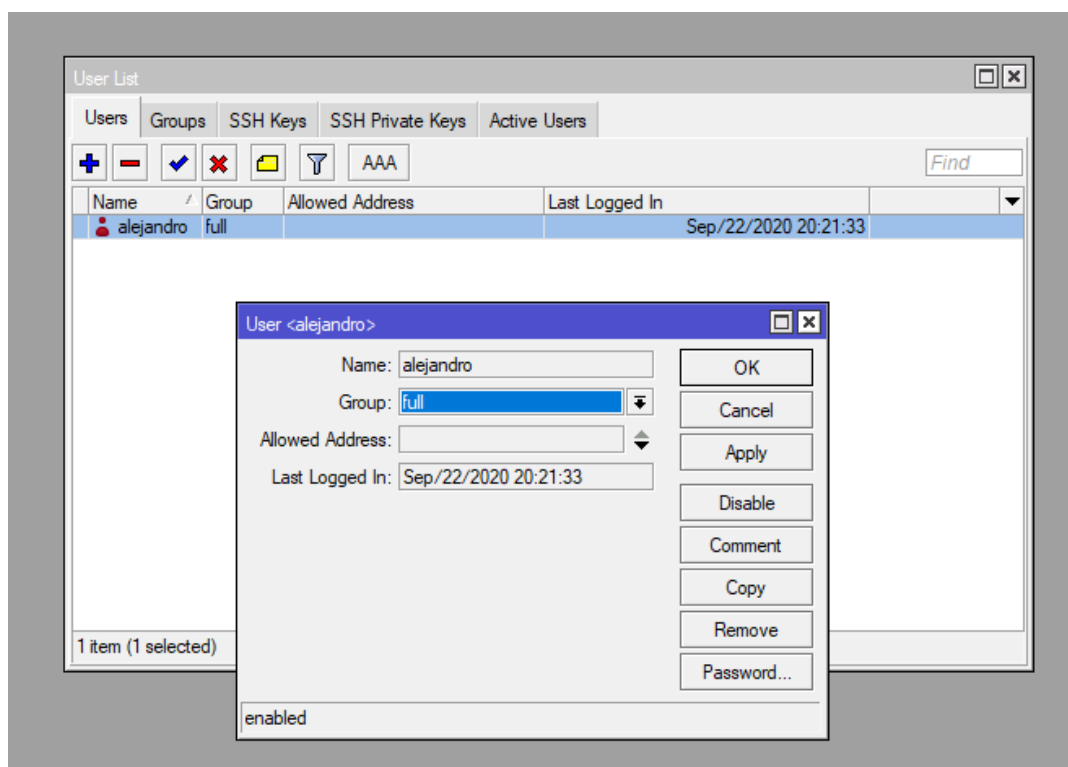


Figura 40. Creación de usuario. Fuente. Propia

Deshabilitamos los servicios IP que no usaremos, Figura 41:

- ✓ ftp
- ✓ ssh
- ✓ telnet
- ✓ api
- ✓ api-ssl
- ✓ www

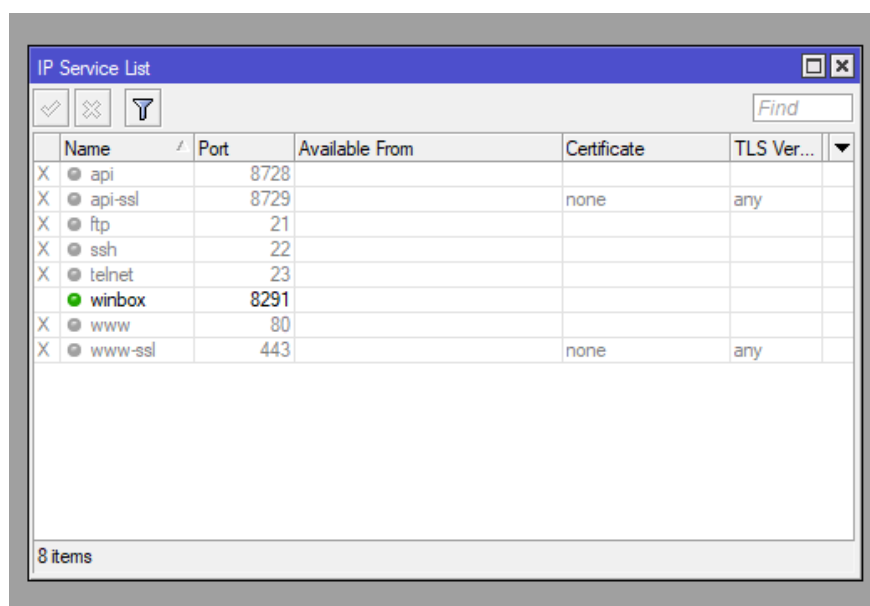


Figura 41 Deshabilitación de servicios IP. Fuente. Propia

Protección contra Syn Flood, es una forma de ataque de denegación de servicio en el que un atacante envía una sucesión de solicitudes al sistema del objetivo en un intento de consumir suficientes recursos del servidor para que el sistema no responda al tráfico legítimo (<https://www.youtube.com/watch?v=fzrNxwquV4M>, 2020), Figura 42.

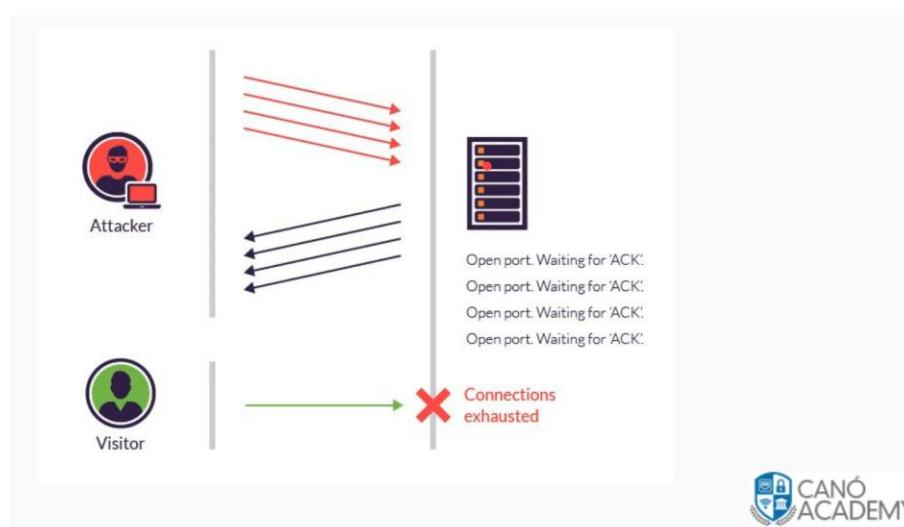


Figura 42. Ataque Syn Flood. Fuente. Canó Academy, Seminario Online de firewalls con Mikrotik, 2018

Limitamos a 30 conexiones por segundo desde una red de mascara 32, lo que implica que el acceso es fuera de nuestra red. En promedio un hacker puede llegar a realizar 500 conexiones por segundo por lo cual haremos un drop de eso paquetes IP, Figura 43.

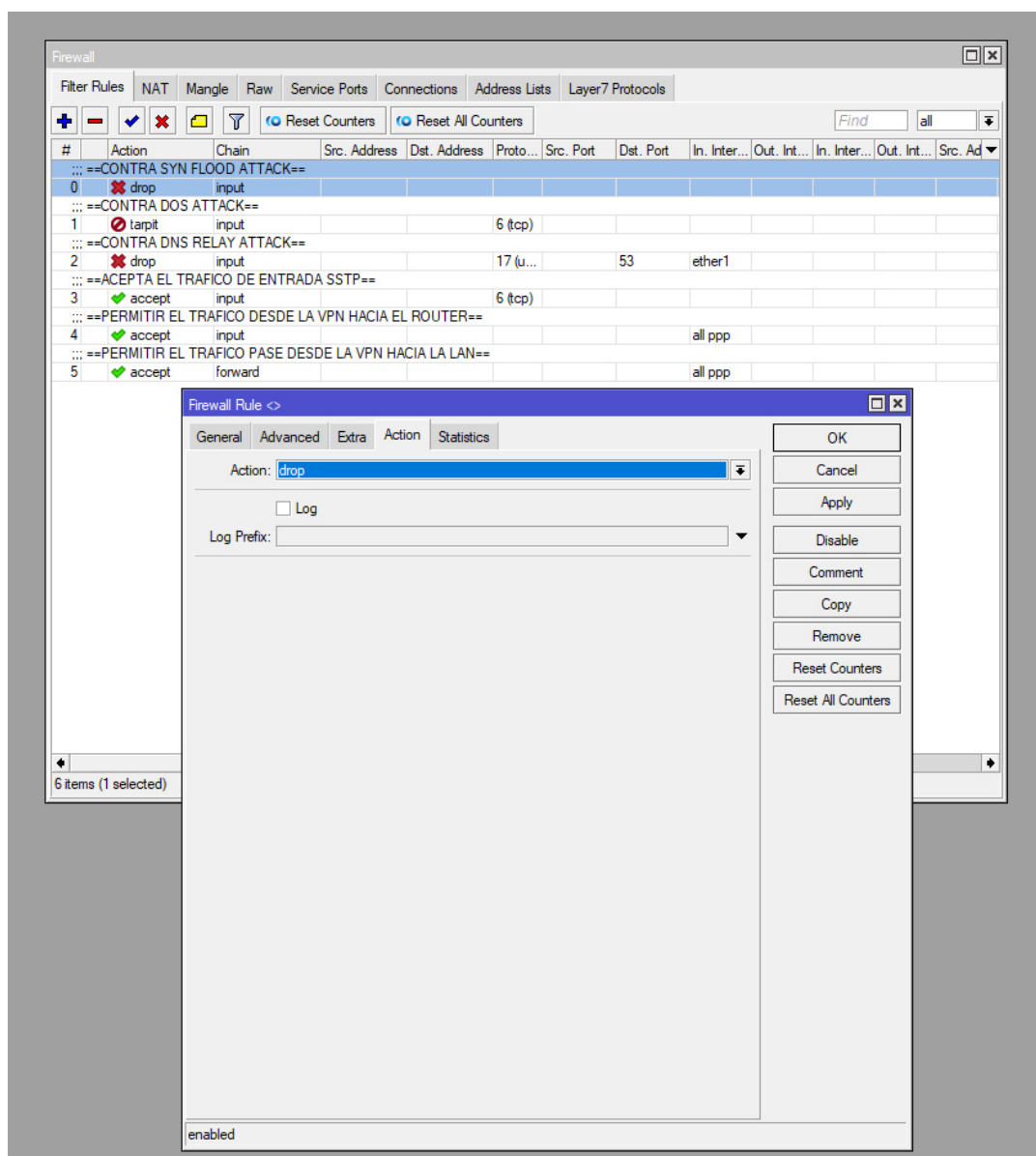


Figura 43. Filtro Syn Flood. Fuente. Canó Academy, Seminario Online de firewalls con Mikrotik, 2018

Protección contra Denial of Services (DOS), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos (<https://www.youtube.com/watch?v=fzrNxwquV4M>, 2020), Figura 44.

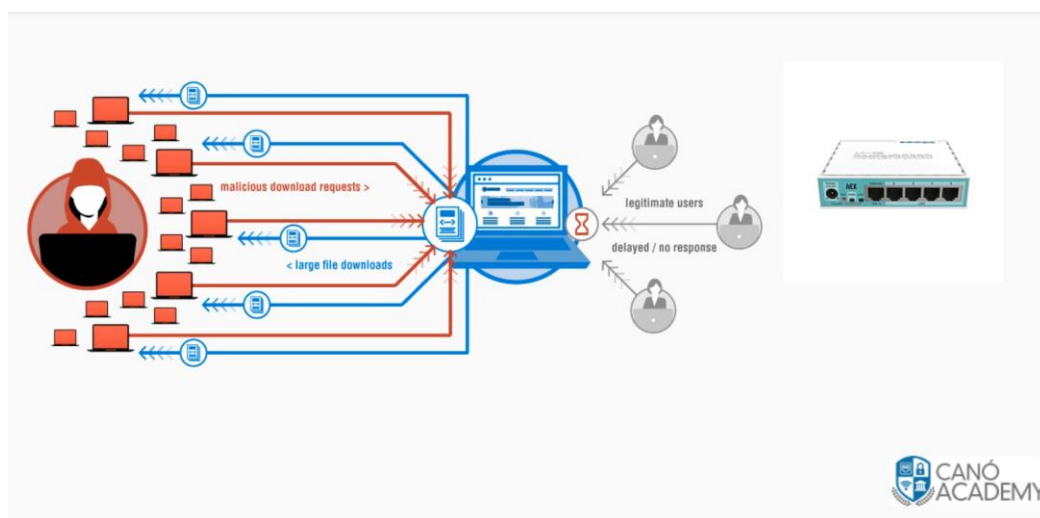


Figura 44. Ataque DoS. Fuente. Canó Academy, Seminario Online de firewalls con Mikrotik, 2018

Capturamos el tráfico dirigido al SERVIDOR VPN L2TP/IPSEC Mikrotik por el protocolo TCP y limitamos a 3 conexiones por segundo desde una red de mascara 32, lo que implica que el acceso es fuera de nuestra red. Realizamos un Tarptit para capturar y retener paquetes y así evitamos que se genere el “Three way handshake” que es el procedimiento por el cual dos dispositivos intercambian una serie de mensajes a fin de poder establecer una sesión y sincronizar sus "Sequence Numbers", Figura 45.

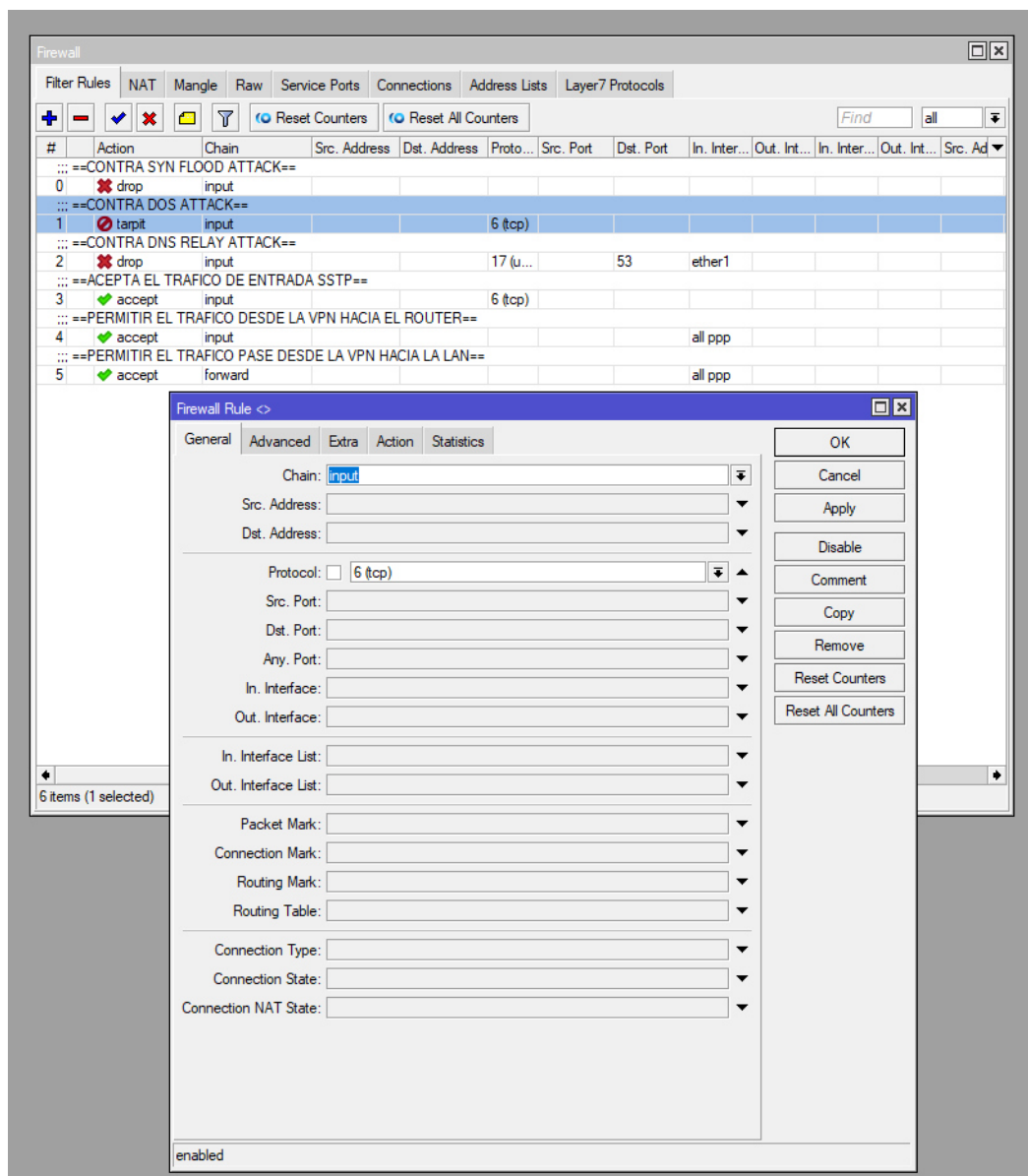


Figura 45. Filtro DoS. Fuente. Canó Academy, Seminario Online de firewalls con Mikrotik, 2018

DNS Relay Attack, un ataque DNS es un exploit en el que un atacante aprovecha las vulnerabilidades en el sistema de nombres de dominio (<https://www.youtube.com/watch?v=fzrNxwguV4M>, 2020), Figura 46.

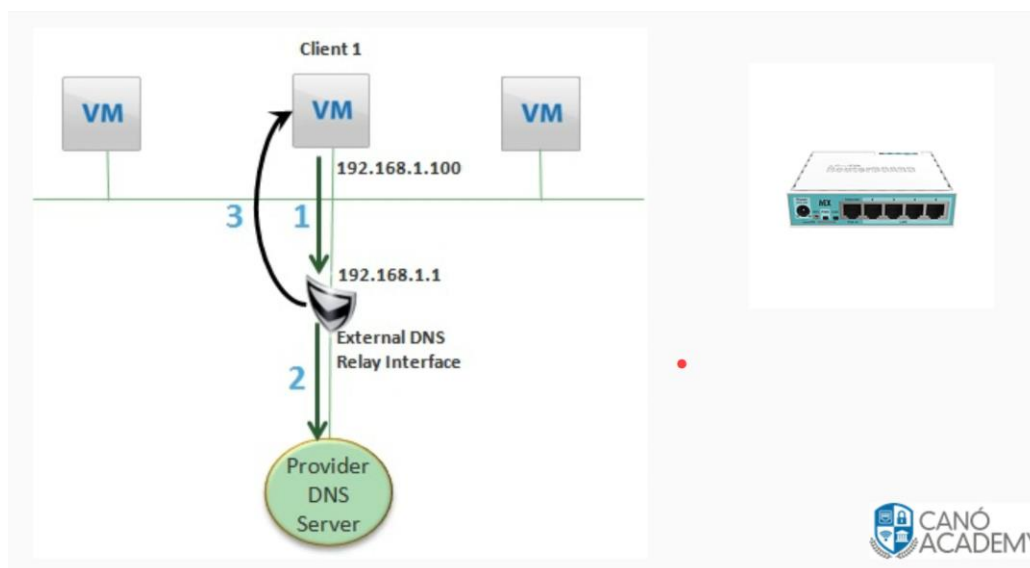


Figura 46. Ataque DNS Relay Attack. Fuente. Canó Academy, Seminario Online de firewalls con Mikrotik, 2018

Capturamos el tráfico dirigido al SERVIDOR VPN L2TP/IPSEC Mikrotik con protocolo UDP 53 que ingrese por la interfaz Ether 1: WAN y realizamos el drop de paquetes, Figura 47.

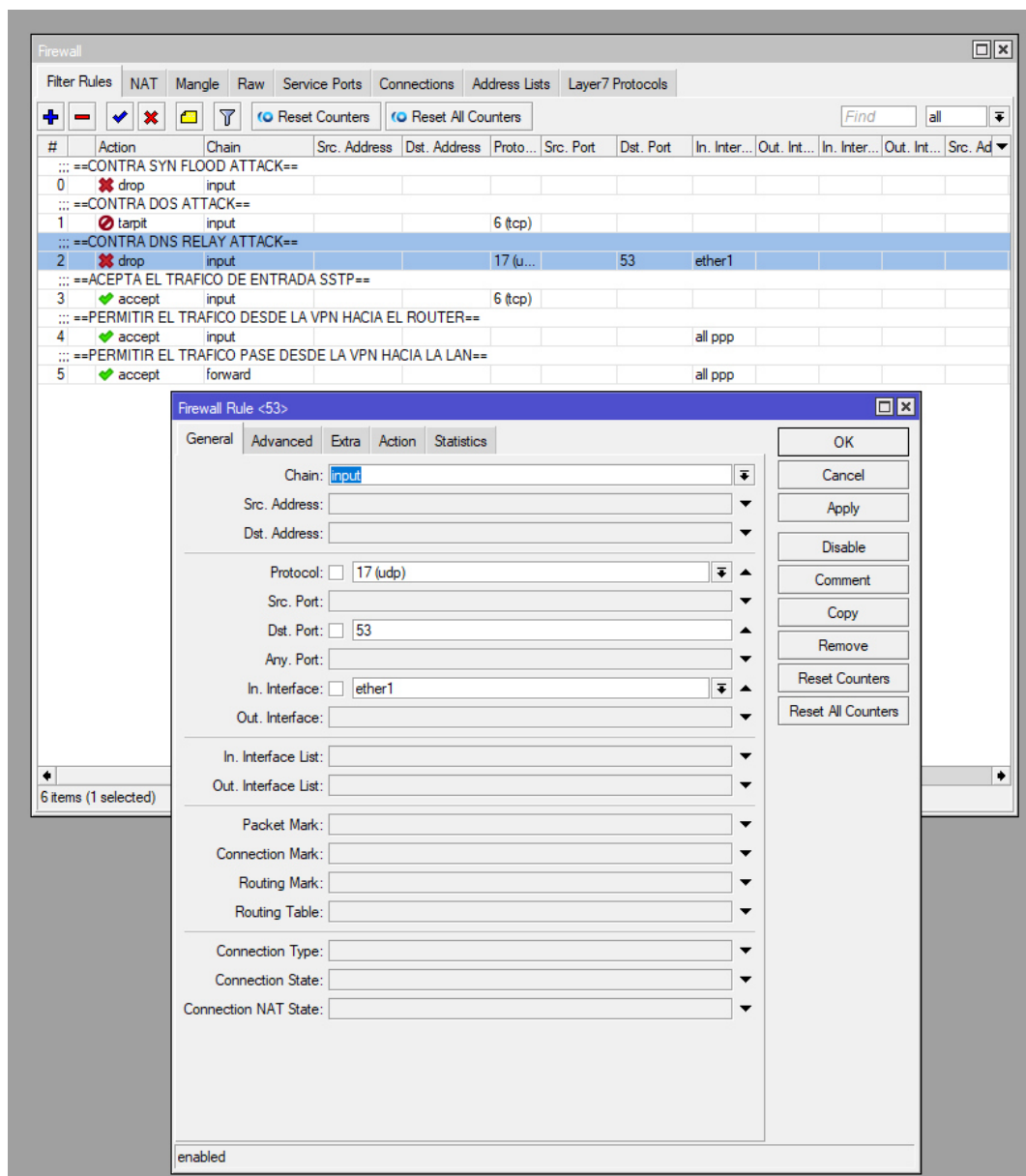


Figura 47. Filtro DNS Relay Attack. Fuente. Canó Academy, Seminario Online de firewalls con Mikrotik, 2018

7.3 Anexo N°03: Configuración de MODEM ROUTER MIKROTIK

REP_1

Ingresamos al equipo por Winbox a través de la MAC, Figura 48.

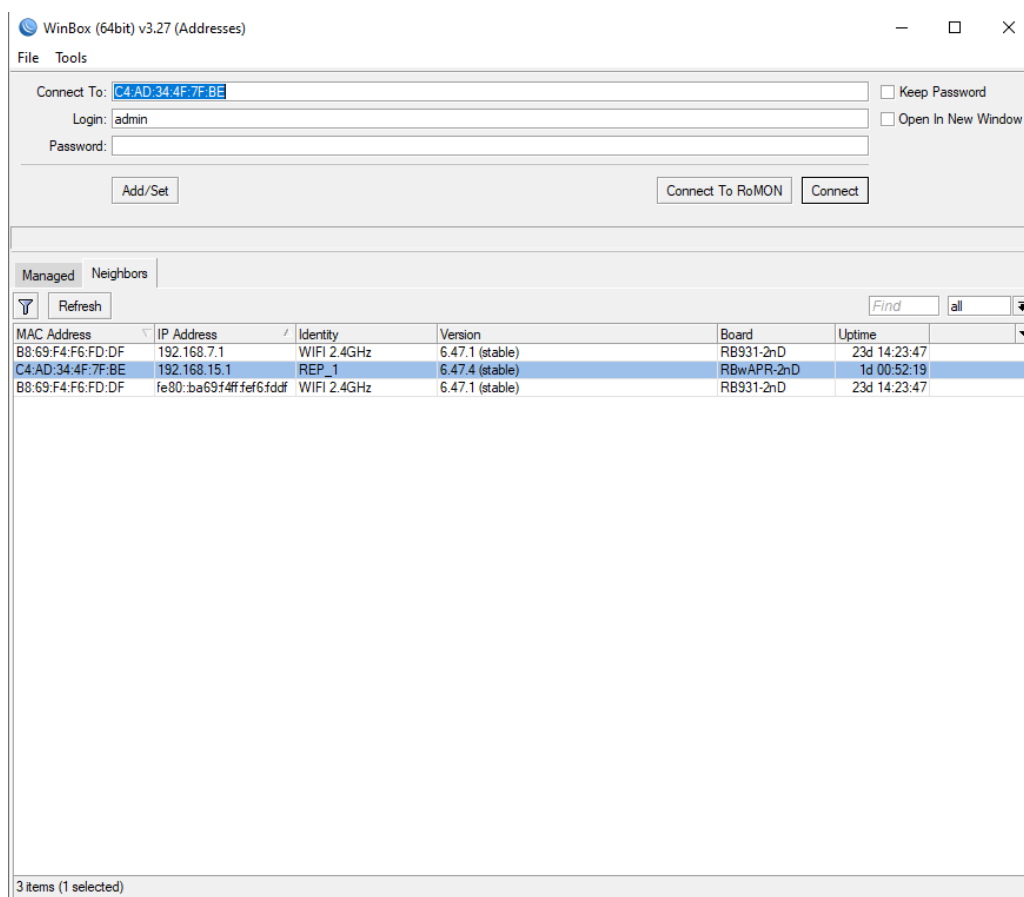


Figura 48. Ingreso a RouterOS. Fuente. Propia

Configuramos la interfaz LTE e ingresamos APN Bitel Internet, seleccionamos User Peer DNS y Add Default Route, Figura 49.

- ✓ Name: Bitel Internet
- ✓ APN: bitel.pe

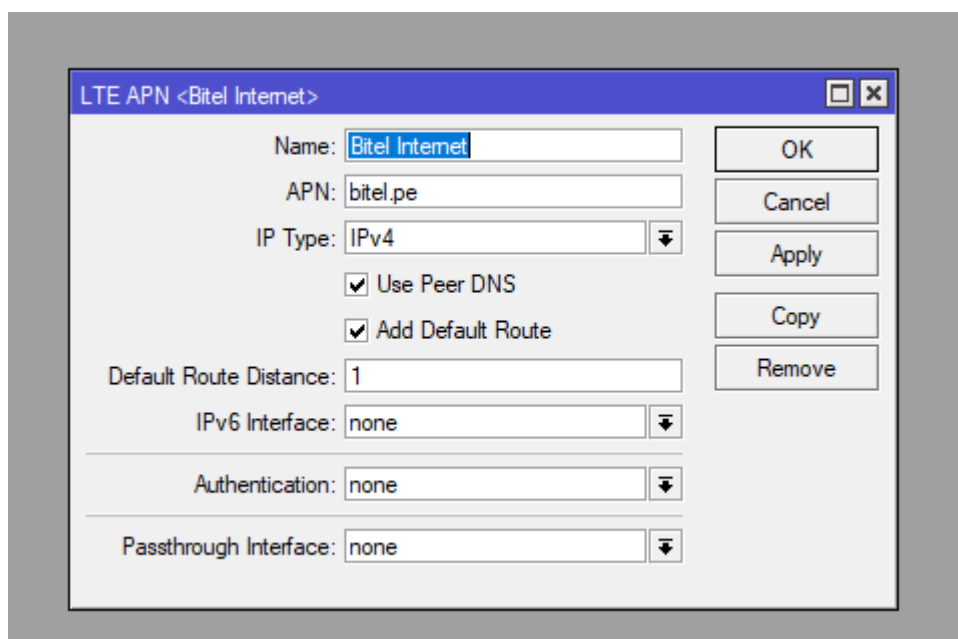


Figura 49 Configuración de APN. Fuente. Propia

Nombraremos la interfaz LTE como WAN-LTE, seleccionaremos Network Mode LTE y en APN Profile Bitel Internet, Figura 50.

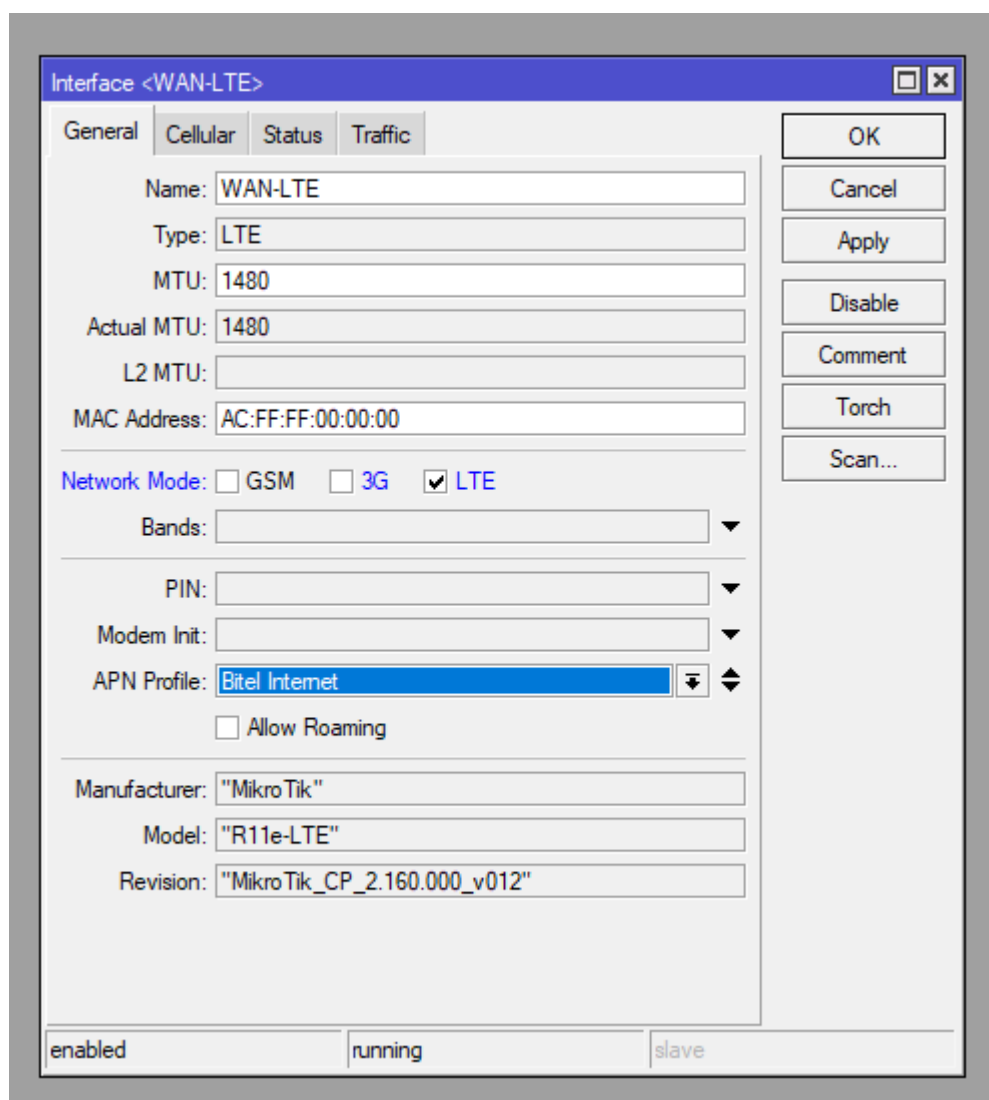


Figura 50. Configuración de la interfaz LTE. Fuente. Propia

Verificamos que se haya registrado nuestro IMSI e IMEI y estemos registrados a la red de Bitel. Hacemos doble click en la interface WAN-LTE y verificamos la pestaña Status, Figura 51.

Interface <WAN-LTE>

General Cellular Status Traffic

Last Link Down Time: Sep/21/2020 23:11:25

Last Link Up Time: Sep/21/2020 23:11:44

Link Downs: 3

Registration Status: registered

PIN Status: ok

Functionality: full

OK

Cancel

Apply

Disable

Comment

Torch

Scan...

enabled running slave

Figura 51. Conexión a la red LTE. Fuente. Propia

7.4 Anexo N°04: Configuración del Modem HUAWEI

Ingresamos al Modem Router Huawei a través de la IP por defecto 192.168.8.1, usuario admin y contraseña admin, Figura 52 y Figura 53.



Figura 52. Marca y modelo del modem. Fuente. Propia

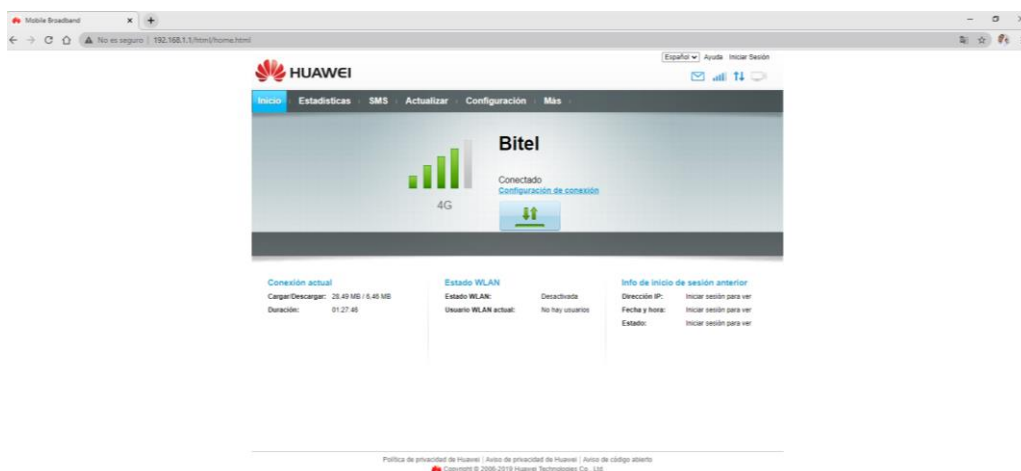


Figura 53. Interfaz de configuración Huawei. Fuente. Propia

Ingresamos la preferencia a la red que se va a conectar, en nuestro caso seleccionamos Solo 4G y en modo de búsqueda de red seleccionamos automático, Figura 54.



Figura 54. Modo de red preferido. Fuente. Propia

El modem viene por defecto con el APN de Bitel y DNS, Figura 55 y Figura 56.



Figura 55. Configuración del APN Bitel. Fuente. Propia

HUAWEI Español Ayuda admin Cerrar sesión

Inicio Estadísticas SMS Actualizar **Configuración** Más

Configuración rápida
Dial-up
Ethernet
→ Configuración de Ethernet
Estado de Ethernet
Clonación de MAC
VPN
WLAN
DHCP
Seguridad
Sistema

Configuración de Ethernet

Nota: Si el producto no cuenta con un puerto Ethernet, se deberá adquirir un adaptador USB-LAN.

Modo de conexión: IP dinámica

El sistema obtiene la dirección IP automáticamente. Cuando el puerto de red se configura en modo WAN, no podrá acceder a la IU web en la PC.

Tamaño de la MTU: 1500 Predeterminado: 1500
Si no es necesario, no edite.

☒ Configurar el servidor DNS manualmente

Servidor DNS primario: 181.176.242.138

Servidor DNS secundario: 181.176.242.34 (Opcional)

Aplicar

Política de privacidad de Huawei | Aviso de privacidad de Huawei | Aviso de código abierto
Copyright © 2006-2019 Huawei Technologies Co., Ltd.

Figura 56. Configuración del DNS Bitel. Fuente. Propia

Configuramos DHCP Server desde la IP 192.168.1.3 hasta 192.168.1.5, Figura 57.

HUAWEI Español Ayuda admin Cerrar sesión

Inicio Estadísticas SMS Actualizar **Configuración** Más

Configuración rápida
Dial-up
Ethernet
VPN
WLAN
DHCP
Seguridad
Sistema

DHCP

Dirección IP: 192.168.1.1

Servidor DHCP: ☒ Habilitar ☐ Deshabilitar

Rango IP DHCP: 3 a 5
192.168.1.3 a 192.168.1.5

Duración de alquiler de DHCP (s): 604800

Aplicar

Política de privacidad de Huawei | Aviso de privacidad de Huawei | Aviso de código abierto
Copyright © 2006-2019 Huawei Technologies Co., Ltd.

Figura 57. Configuración DHCP. Fuente. Propia