
# UNIVERSIDAD TÉCNICA DE COTOPAXI

## FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

## CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

## PROYECTO DE INVESTIGACIÓN

ESTUDIO COMPARATIVO DEL RENDIMIENTO DE TECNOLOGÍAS EVPN Y VPLS EN UN AMBIENTE SIMULADO UTILIZANDO GNS3 EN LA UNIVERSIDAD TÉCNICA DE COTOPAXI

Proyecto de Investigación presentado previo a la obtención del Título de Ingeniero en Sistemas de Información

**Autores:**

Lituma Galarza Jonathan Paul

Yánez Arcos Bryan Fernando

**Tutor Académico:**

Ing. Rubio Peñaherrera Jorge Bladimir, Mgs

**Latacunga – Ecuador**

**2022**

# DECLARACION DE LA AUDITORIA

## DECLARACIÓN DE LA AUTORÍA

Nosotros, Jonathan Paul Lituma Galarza con C.I.: 1750766063 y Bryan Fernando Yanez Arcos con C.I.: 1726244583, ser los autores del presente proyecto de Investigación:

**" Estudio comparativo del rendimiento de tecnologías EVPN y VPLS en un ambiente simulado utilizando GNS3 en la Universidad Técnica de Cotopaxi",** siendo el Ing. Jorge Bladimir Rubio Peñaherrera, tutor del presente trabajo, eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certificamos que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de nuestra exclusiva responsabilidad.

Atentamente,

Lituma Galarza Jonathan Paul

CI: 1750766063

Yanez Arcos Bryan Fernando

CI: 1726244583

# AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título: **"Estudio comparativo del rendimiento de tecnologías EVPN y VPLS en un ambiente simulado utilizando GNS3 en la Universidad Técnica de Cotopaxi."**, de Lituma Galarza Jonathan Paul y Yánez Arcos Bryan Fernando , de la carrera de Ingeniería de Sistema de Información , considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la Facultad de Ciencias de la Ingeniería y Aplicada de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, 29 de agosto 2022

Firma:

Ing. Rubio Peñaherrera Jorge Bladimir

C.C.: 050222229-2

Tutor

# APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

## APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la FACULTAD de CIYA; por cuanto, el o los postulantes: Jonathan Paul Lituma Galarza, Bryan Fernando Yánez Arcos con el título de Proyecto de titulación: Estudio comparativo del rendimiento de tecnologías EVPN y VPLS en un ambiente simulado utilizando GNS3 en la Universidad Técnica de Cotopaxi han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, 29 de agosto del 2022

Para constancia firman:

**Lector 1 (Presidente)**
**Nombre:** MG. Manuel Villa
**CC:**180338695-0

**Lector 2**
**Nombre:** MG. Alex Llano
**CC:**050258986-4

**Lector 3**
**Nombre:** MG. Edwin Quinatoa
**CC:**050256337-2

## AGRADECIMIENTO

Quiero agradecer primeramente a mi papá: Charles Lituma, y a mi abuelita: Gradys Cabanilla por financiar mis estudios, por las conversaciones que me ayudaron a no rendirme, los valores que me inculcaron y a su amor incondicional que nunca me hizo falta.

A mis familiares y allegados que me apoyaron incondicionalmente en todo mi proceso universitario.

También quiero agradecer a mi tutor.Ing. Mg. Jorge Rubio quien me guió en la realización de esta investigación con su paciencia y rectitud como docente.

**Jonathan Lituma**

## DEDICATORIA

El presente trabajo de investigación le quiero dedicar a mi papá y a mi abuelita por su amor y sacrificios que me han dado todos estos años y que gracias a ellos he podido lograr a todas las personas que me han apoyado y han hecho qu

e el trabajo se realice con éxito y en especial compartieron su conocimiento.

**Jonathan Lituma**

## AGRADECIMIENTO

Agradezco primero a Dios por bendecirme cada día de mi vida, ser ese apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Quiero agradecer a mi padre Galo Yánez, a mi madre Marcia Arcos y mi hermano Jonathan Yánez que fueron mi motor que impulsa mis sueños y esperanzas quienes estuvieron siempre a mi lado en los días más difíciles dándome consejos durante toda la carrera por último pero muy importante también a mi abuelito Luis Arcos y a mis dos abuelitas que están en el cielo Mamá Laura y Mariana Aldaz.

Quiero agradecer a mi tutor.Ing. Mg. Jorge Rubio quien me guio en la realización de este proyecto de investigación con su paciencia, rectitud, sabiduría y conocimiento como docente

**Bryan Yánez**

## DEDICATORIA

Este proyecto de investigación está dedicado a mis padres, a mi hermano y a mis abuelitos por su amor y cariño que siempre me tuvieron a lo largo de mi vida, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy.

Quiero dedicarme a todas esas personas que me apoyaron a lo largo de mi vida estudiantil y han hecho que este proyecto de investigación se realice con éxito y conocimiento.

**Bryan Yánez**

# UNIVERSIDAD TÉCNICA DE COTOPAXI

## FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

**TÍTULO:** "Estudio comparativo del rendimiento de tecnologías EVPN y VPLS en un ambiente simulado utilizando GNS3 en la Universidad Técnica de Cotopaxi"

**Autores:**

Lituma Galarza Jonathan Paul

Yánez Arcos Bryan Fernando

**RESUMEN**

La necesidad que tenemos en la actualidad de tener redes seguras es casi indispensable tanto como para las personas naturales o como para una gran organización, ya que tenemos información importante que podría ser robada o cambiada. La resolución que llegaron los desarrolladores de infraestructura de redes , fue crear las redes virtuales privadas, en este proyecto de investigación pretendemos realizar una comparación de dos tecnológicas de las redes virtuales privadas, que son VPLS(Virtual private Lan Service) y EVPN(Ethernet VPN), las dos tecnologías están siendo utilizadas conjuntamente con el protocolo IP/MPLS que los ayuda a mejorar la calidad de servicio para las aplicaciones susceptibles al tiempo ,también con el propósito de evaluar el rendimiento del tráfico de datos y la seguridad , para así en un futuro determinar que opción es viable para implementar en la red de la Universidad técnica de Cotopaxi. La metodología del proyecto de investigación fue Top-Down Network Desing la cual tiene cuatro fases que son :análisis de negocios objetivos y limitaciones ,diseño lógico ,diseño físico y la fase de pruebas que nos permitió diseñar y elaborar la topología, el escenario de pruebas para comparar las dos tecnologías será el software de simulación GNS3, se utilizó entornos de virtualización como el VMWare Player y el GNS3 VM nos permitirá tener un mejor rendimiento en la simulación de todos los dispositivos de red integrados en la topología también se ejecutó tres escenarios de pruebas que son :convergencia de red, movilidad Mac y supresión de bum , para obtener un análisis de rendimiento y características de cada una de las herramientas tecnológicas.

**Palabras Claves**: Software Gns3, VPN (Red Virtual), VPLS Servicio, EVPN Servicio.

**TECHNICAL UNIVERSITY OF COTOPAXI**

**FACULTY OF ENGINEERING SCIENCESS AND APPLIED**

**THEME**: "Comparative study of the performance of EVPN and VPLS technologies in a simulated environment using GNS3 at the Technical University of Cotopaxi"

**AUTHORS:**

Lituma Galarza Jonathan Paul

Yánez Arcos Bryan Fernando

## ABSTRACT

The need that we currently have to have secure networks is almost essential both for individuals and for a large organization, since we have important information that could be stolen or changed. The resolution reached by the network infrastructure developers was to create virtual private networks, in this research project we intend to make a comparison of two technologies of virtual private networks, which are VPLS (Virtual private lan Service) and EVPN (Ethernet VPN ), the two technologies are being used in conjunction with the IP/MPLS protocol that helps them improve the quality of service for time-sensitive applications, also for the purpose of evaluating the performance of data traffic and security, in order to a future to determine which option is viable to implement in the network of the Technical University of Cotopaxi. The methodology of the research project was Top-Down Network Desing, which has four phases: objective business analysis and limitations, logical design, physical design and the testing phase that allowed us to design and develop the topology, the test scenario to compare the two technologies will be the GNS3 simulation software, virtualization environments such as VMWare Player and GNS3 VM will be used, it will allow us to have a better performance in the simulation of all the network devices integrated in the topology, three scenarios of tests that are: network convergence, Mac mobility and boom suppression, to obtain an analysis of the performance and characteristics of each of the technological tools.

**Key words**: Gns3 Software, Vpn (Virtual Network), VPLS Service, EVPN Service.

# AVAL DE TRADUCCIÓN

UNIVERSIDAD TÉCNICA DE COTOPAXI

CENTRO DE IDIOMAS

## *AVAL DE TRADUCCIÓN*

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que:

La traducción del resumen al idioma Inglés del trabajo de titulación cuyo título versa **"ESTUDIO COMPARATIVO DEL RENDIMIENTO DE TECNOLOGÍAS EVPN Y VPLS EN UN AMBIENTE SIMULADO UTILIZANDO GNS3 EN LA UNIVERSIDAD TÉCNICA DE COTOPAXI"**, presentado por: **Lituma Galarza Jonathan Paul y Yánez Arcos Bryan Fernando,** estudiantes de la Carrera de **Sistemas,** perteneciente a la **Facultad de Ciencias de la Ingeniería y Aplicadas,** lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a los peticionarios hacer uso del presente aval para los fines académicos legales.

Latacunga, septiembre del 2022

Atentamente,

Mg. Marco Beltrán

CENTRO DE IDIOMAS

**DOCENTE CENTRO DE IDIOMAS-UTC**
**CI:** 0502666514

# ÍNDICE GENERAL

DECLARACION DE LA AUDITORIA ..... ii
AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN ..... iii
APROBACIÓN DEL TRIBUNAL DE TITULACIÓN ..... iv
AGRADECIMIENTO ..... v
DEDICATORIA ..... vi
AGRADECIMIENTO ..... vii
DEDICATORIA ..... viii
RESUMEN ..... ix
ABSTRACT ..... x
AVAL DE TRADUCCIÓN ..... xi
ÍNDICE GENERAL ..... xii
1. INFORMACIÓN GENERAL ..... 1
2. INTRODUCCIÓN ..... 3
2.1. PROBLEMA ..... 3
2.1.1. Situación Problemática ..... 3
2.1.2. Formulación del problema ..... 4
2.2. REVISIÓN BIBLIOGRÁFICA Y DOCUMENTAL ..... 4
2.3. OBJETO Y CAMPO DE ACCIÓN ..... 5
2.3.1. Objeto de estudio ..... 5
2.4. BENEFICIARIOS ..... 5
2.5. JUSTIFICACIÓN ..... 6
2.6. HIPÓTESIS ..... 6
2.7. OBJETIVOS ..... 6
2.7.1. General ..... 6
2.7.2. Específicos ..... 6
2.8. SISTEMAS DE TAREAS ..... 7
3. FUNDAMENTACIÓN TEÓRICA ..... 8
3.1. Antecedentes ..... 8
3.1.1. MPLS Multiprotocolo Label Swithing ..... 8
3.1.2. Características Básicas y funcionamiento ..... 9
3.1.3. Arquitectura ..... 10
3.1.4. Protocolos utilizados ..... 10

3.2. VPN ..... 10
3.2.1. ¿Cómo funciona una VPN? ..... 11
3.2.2. Requerimientos básicos para una VPN ..... 11
3.2.3.1. TIPOS DE VPN ..... 12
3.3. VPLS Virtual Private LAN Service ..... 12
3.3.1. Terminología ..... 12
3.3.2. Plano de reenvío ..... 13
3.3.3. Plano de Control ..... 13
3.4. EVPN Ethernet Virtual Private Network ..... 14
3.4.1. Tipos de EVPN ..... 14
3.4.2. Limitaciones resueltas por EVPN ..... 14
3.4.2.1. Integración de servicios ..... 14
3.4.2.2. Eficiencia ..... 14
3.4.2.3. Flexibilidad ..... 15
3.4.3. ¿Qué son EVPN y BGP EVPN? ..... 15
3.4.4. ¿Cómo funciona EVPN? ..... 16
´3.4.4.1. ES ..... 16
3.4.4.2. ESI ..... 16
3.4.4.3. EVI ..... 16
3.4.5. Proceso de inicio de EVPN ..... 17
3.4.6. Aprendizaje de direcciones MAC ..... 18
3.4.6. ¿Cuáles son las aplicaciones típicas de EVPN? ..... 19
3.4.6.1. PBB ..... 19
3.4.6.1. VPWS EVPN ..... 19
3.5. ASPECTOS GENERALES ..... 20
3.5.1. Hardware ..... 20
3.5.2. Software ..... 21
3.5.2.1. IOS CISCO ..... 21
3.5.2.2. Componentes ..... 21
3.5.3. GNS3 ..... 22
3.5.3.1. Creación de una topología en GNS3 ..... 23
3.5.4. Motores de Simulación ..... 23
3.5.4.1. QEMU ..... 23
3.5.4.2. VMware player ..... 24
3.5.5. Herramientas de Análisis ..... 26

3.5.5.1. Ostinato ..... 26
3.5.5.2. Wirehark ..... 26
3.5.2.2.1. Donde realizar la captura de datos ..... 27
4. MATERIALES Y MÉTODOS ..... 27
4.1. Tipos de investigación ..... 28
4.1.1. Investigación bibliográfica ..... 28
4.1.2. Investigación de campo ..... 28
4.1.3. Investigación descriptiva ..... 28
4.2. Métodos Teóricos ..... 28
4.5. Población y muestra ..... 28
4.5.1. Población ..... 28
4.5.2. Muestra ..... 29
4.6. Variables ..... 29
4.6.1. Variable independiente ..... 29
4.6.2. Variable dependiente ..... 29
4.7. Metodología de la investigación ..... 29
5. ANÁLISIS Y DISCUSIÓN DE RESULTADOS ..... 29
5.1. Fase 1: Análisis de Negocios Objetivos y limitaciones ..... 30
5.2. Especificación de escenarios ..... 30
5.2.1. Instalación de GNS3 ..... 31
5.2.2. Configuración Básica ..... 33
5.2.2.1. Creación de loopback ..... 33
5.2.2.2. Configuración de Servidores ..... 36
5.2. Fase2: Diseño Lógico ..... 39
5.2.1. Topología de Red ..... 39
5.2.2. Direccionamiento Lógico ..... 41
5.2.3 Direccionamiento lógico VPLS ..... 41
El direccionamiento lógico de la tecnología VPLS es la siguiente: ..... 41
5.2.3. Direccionamiento lógico EVPN ..... 42
5.3. Fase 3: Diseño Físico ..... 42
5.3.1. Direccionamiento Físico VPLS ..... 42
5.3.2. Direccionamiento Físico EVPN ..... 43
5.4. Pruebas, Optimización y Documentación de la red ..... 44
5.4.1. Convergencia de la red total ..... 44
5.4.2. Movilidad MAC ..... 48

5.4.2.1 EVPN ..... 50
5.4.2.2 VPLS ..... 55
5.4.3 Supresión de Tráfico BUM ..... 58
5.4.3.1 EVPN ..... 59
5.4.3.2 VPLS ..... 60
5.5. Comparación de resultados de las tecnologías EVPN y VPLS ..... 62
5.6. Comparación de resultados de los informes de Expertos ..... 63
5.7. Análisis y Tabulación De La Encuestas ..... 63
6. CONCLUSIONES Y RECOMENDACIONES ..... 73
6.1. Conclusiones ..... 73
6.2. Recomendaciones ..... 74
7. BIBLIOGRAFÍA: ..... 74
8. ANEXOS ..... 77

# ÍNDICE DE TABLAS

Tabla 1. Beneficiario directos e indirectos ..... 6
Tabla 2. Planificación de actividades. ..... 7
Tabla 3. Papel de los Routers ..... 41
Tabla 4. Asignación de interfaces ..... 42
Tabla 5. Configuración de red de los clientes finales ..... 44
Tabla 6. Tabla comparativa de EVPN y VPLS ..... 62
Tabla 7. Comparación del informe los expertos ..... 63
Tabla 8. Frecuencia y porcentaje de la pregunta 1 de la encuesta realizada ..... 64
Tabla 9. Frecuencia y porcentaje de la pregunta 2 de la encuesta realizada. ..... 65
Tabla 10. Frecuencia y porcentaje de la pregunta 3 de la encuesta realizada ..... 67
Tabla 11. Frecuencia y porcentaje de la pregunta 4 de la encuesta realizada ..... 68
Tabla 12. Frecuencia y porcentaje de la pregunta 5 de la encuesta realizada ..... 69
Tabla 13. Frecuencia y porcentaje de la pregunta 6 de la encuesta realizada ..... 70
Tabla 14. Frecuencia y porcentaje de la pregunta 7 de la encuesta realizada ..... 71
Tabla 15. Frecuencia y porcentaje de la pregunta 8 de la encuesta realizada ..... 72

# ÍNDICE DE FIGURAS

Figura 1. Componentes de la red MPLS [1] ..... 9
Figura 2. Arquitectura de una VPN [4] ..... 11
Figura 3. Estructura de VPLS [5] ..... 13
Figura 4. redes EVPN [8] ..... 16
Figura 5. Topología de una red EVPN [8] ..... 17
Figura 6. Anuncio de ruta tipo 2 [8] ..... 18
Figura 7. Redes EVPN VPWS [8] ..... 19
Figura 8. Ordenador [7] ..... 20
Figura 9. logo Cisco IOS [17] ..... 21
Figura 10. Componentes [9] ..... 22
Figura 11. Logo de GNS3 [18] ..... 23
Figura 12. Logo de QEMU [19] ..... 24
Figura 13. Logo de VMware player [20] ..... 25
Figura 14. Logo de Ostinato [21] ..... 26
Figura 15. Logo de Wireshark [22] ..... 27
Figura 16. Instalación de GNS3(Paso 1) ..... 31
Figura 17. Instalación de GNS3(Paso 2) ..... 31
Figura 18. Instalación de GNS3(Paso 3) ..... 32
Figura 19. Instalación de GNS3(Paso 4) ..... 32
Figura 20. Instalación de GNS3 (Paso 5) ..... 33
Figura 21. Interfaz de Loopback (Paso 1) ..... 33
Figura 22. Interfaz de Loopback (Paso 2) ..... 34
Figura 23. Interfaz de Loopback (Paso 3) ..... 34
Figura 24. Interfaz de Loopback (Paso 4) ..... 35
Figura 25. Interfaz de Loopback (Paso 5) ..... 35
Figura 26. Interfaz de Loopback (Paso 6) ..... 35
Figura 27. Interfaz de Loopback (Paso 7) ..... 36
Figura 28. Preferencias de Servidores GNS3 ..... 36
Figura 29. Preferencias de GNS3 ..... 37
Figura 30. Archivo de GNS3 VM ..... 38
Figura 31. Importación de GNS3 VM en VMware ..... 38
Figura 32. Interfaz de VM en VMware ..... 39
Figura 33. Topología de Red ..... 40

Figura 34. Direccionamiento lógico VPLS ..... 41
Figura 35. Direccionamiento lógico EVPN ..... 42
Figura 36. Direccionamiento Físico VPLS ..... 43
Figura 37. Direccionamiento Físico EVPN ..... 44
Figura 38. Conectividad Ping PC-1 a PC-2 y PC-3 ..... 46
Figura 39. Conectividad Ping PC-2 a PC-3 y PC-1 ..... 46
Figura 40. Conectividad Ping PC-2 a PC-1 y PC-3 ..... 46
Figura 41. Conectividad Ping PC-2 a PC- 1 ..... 46
Figura 42. Conectividad Ping PC-1 a PC-2 ..... 47
Figura 43. Trazado PC-1 a PC-2 y PC-3 ..... 47
Figura 44. Trazado PC-2 a PC-1 y PC-3 ..... 47
Figura 45. Trazado PC-3 a PC-1 y PC-3 ..... 48
Figura 46. Trazado PC-1 a PC-2 ..... 48
Figura 47. Trazado PC-2 a PC- ..... 48
Figura 48. Escenario de Pruebas de Movilidad ..... 49
Figura 49. Movilidad MAC ..... 49
Figura 50. Tabla-MAC EVPN ..... 50
Figura 51. Capturas de Paquetes enlace PE1-P1 ..... 51
Figura 52. Mensaje de Actualización 162 ..... 52
Figura 53. Mensaje Actualización 251 ..... 53
Figura 54. Mensaje de Update 177 ..... 54
Figura 55. Mensaje Update 177 V2 ..... 54
Figura 56. Tabla de MAC VPLS ..... 55
Figura 57. Captura de paquetes enlace PE1-P1 ..... 56
Figura 58. Tabla MAC VPLS ..... 57
Figura 59. Configuración direcciones MAC e IP ..... 58
Figura 60. Configuración direcciones MAC e IP ..... 58
Figura 61. ARP antes ..... 59
Figura 62. Inundación ARP después ..... 59
Figura 63. Tabla EVPN MAC ..... 60
Figura. 64 inundación ARP antes ..... 61
Figura 65. Inundación ARP después ..... 61
Figura 66. Tabla MAC de VPLS ..... 62
Figura 67. Gráfico del porcentaje de la pregunta 1 de la encuesta realizada ..... 64
Figura 68. Gráfico del porcentaje de la pregunta 2 de la encuesta realizada ..... 65

Figura 69. Gráfico del porcentaje de la pregunta 3 de la encuesta realizada ..... 67
Figura 70. Gráfico del porcentaje de la pregunta 4 de la encuesta realizada ..... 68
Figura 71. Gráfico del porcentaje de la pregunta 5 de la encuesta realizada ..... 69
Figura 72. Gráfico del porcentaje de la pregunta 6 de la encuesta realizada ..... 70
Figura 73. Gráfico del porcentaje de la pregunta 7 de la encuesta realizada ..... 71
Figura 74. Gráfico del porcentaje de la pregunta 8 de la encuesta realizada ..... 72

## ÍNDICE DE ANEXO

Anexo 1. Informe de Urkund..... 77
Anexo 2. Formulario de encuesta..... 78
Anexo 3. Acuerdo de confidencialidad ..... 80
Anexo 4. Validación de Expertos..... 82

# 1. INFORMACIÓN GENERAL

**TITULO:** Estudio comparativo del rendimiento de tecnologías EVPN y VPLS en un ambiente simulado utilizando GNS3 en la Universidad Técnica de Cotopaxi.

**FECHA DE INICIO:** 25 de octubre del 2021

**FECHA DE FINALIZACIÓN:** 26 de agosto del 2022

**LUGAR DE EJECUCIÓN:**

- **Provincia:** Cotopaxi
- **Cantón:** Latacunga
- **Parroquia:** Eloy Alfaro
- **Instituto:** Universidad Técnica de Cotopaxi

**FACULTAD QUE AUSPICIA:**

Ciencias de la Ingeniería y Aplicadas

**CARRERA QUE AUSPICIA:**

Ingeniería en Sistemas de Información

**PROYECTO DE INVESTIGACIÓN VINCULADO:**

Proyecto generativo

**EQUIPO DE TRABAJO:**

**DOCENTE TUTOR**

**Nombre:** Ing. Jorge Bladimir Rubio Peñaherrera

**Nacionalidad:** ecuatoriano

**Estado Civil:** Casado

**Residencia:** Pujilí, calle Gabriel Álvarez 113 y Juan José Merizalde

**E-mail:** jorge.rubio@utc.edu.ec

**Teléfono:** 0995220308

**ESTUDIANTES**

**Primer Estudiante**

**Nombre:** Lituma Galarza Jonathan Paul

**Nacionalidad:** ecuatoriano

**Estado Civil:** Soltero

**Residencia:** Pichincha -Quito

**E-mail:** jonathan.lituma6063@utc.edu.ec

**Teléfono:** 0958994767

**Segundo Estudiante**

**Nombre:** Yánez Arcos Bryan Fernando

**Nacionalidad:** ecuatoriano

**Estado Civil:** Soltero

**Residencia:** Pichincha-Quito

**E-mail:** bryan.yanez4583@utc.edu.ec

**Teléfono:** 0984268448

**ÁREA DE CONOCIMIENTO:**

06 información y Comunicación (TIC) /061 Información y Comunicación (TIC) / 0611 El uso del ordenador

**LÍNEA DE INVESTIGACIÓN:**

Tecnologías de la información y comunicación (TICS)

**SUBLÍNEAS DE INVESTIGACIÓN DE LA CARRERA:**

Infraestructura de redes.

# 2. INTRODUCCIÓN

La técnica de las redes virtuales privadas fue concebida en un principio para las grandes empresas, pero en el presente la utilizamos para las actividades cotidianas que tienen las organizaciones pequeñas y medianas.

La necesidad que tenemos en la actualidad de tener redes seguras es casi indispensable ya que tenemos información importante que podría ser robada o cambiada. La resolución que llegaron fue las redes virtuales privadas.

Los ambientes virtuales de enrutamiento IP han ido evolucionando en los últimos tiempos es por ello que surgió el protocolo de MPLS, que puede mejorar los planes a corto mediano y largo plazo y poder extender las aplicaciones en una red, es de vital importancia hoy en día ya que las expectativas de los usuarios son cada vez mayores.

## 2.1. PROBLEMA

A partir del nacimiento del internet han sido creados nuevos espacios de interacción en la web es por ello que surgieron las redes que es la unión de varios equipos unidos entre sí mediante aparatos físicos que envían impulsos electrónicos y posteriormente para mayor seguridad se creó nuevos modos de interacción entre equipos como son las redes virtuales y privadas pero en la actualidad no hay mucho conocimiento acerca de la seguridad que debería tener las redes, es por ello que los piratas informáticos acceden con gran facilidad a los equipos, si no tenemos las correctas medidas de seguridad podría cualquier usuario acceder a información valiosa que tenemos en nuestros equipos, utilizamos las redes para realizar gran cantidad de actividades de nuestro diario vivir ya que se podría decir que no es un servicio sino una necesidad de la gran mayoría de personas que están en el mundo.

### 2.1.1. Situación Problemática

Las redes surgen para la comunicación entre individuos, que no necesariamente deben estar cerca, los motivos de la comunicación pueden ser diferentes ya sea esta amistad, parentesco o compartir información valiosa de una organización o empresa.

Los servicios de las redes virtuales privadas es una técnica conocida y ampliamente utilizada y se ha llegado a convertir en una manera fácil y económica de utilizar el internet con conexiones privadas y seguras.

El protocolo de MPLS es muy conocido en las empresas y organizaciones porque mejora el flujo de trabajo, así como una gran variedad de soportes y una escalable gama de servicios.

Las redes virtuales privadas pueden implementarse en cualquier tipo de circuito terminal tanto en tecnologías convencionales como en Frase Relay, una ventaja de este servicio es que permite que el usuario pueda gestionar su propio enrutamiento en su propia red virtual privada, lo que le proporciona una gran comprobación y seguridad en el flujo de datos.

### 2.1.2. Formulación del problema

¿Cuál es la tecnología más eficiente para el QoS (calidad de servicio) utilizando EVPN y VPLS en la Universidad Técnica de Cotopaxi?

## 2.2. REVISIÓN BIBLIOGRÁFICA Y DOCUMENTAL

Dentro de las investigaciones [1] encontramos, Calahorrano Vega Cesar Augusto de la Universidad de la ESPE realizó una evaluación del rendimiento de las tecnologías EVPN y VPLS en el ambiente simulado GSN3 y las mismas que se implementaran sobre una red IP/MLS gracias a las herramientas utilizadas dentro de la investigación y el análisis de la topología de la red aportan una confiable apreciación de los resultados obtenidos fueron favorables.

Por otro lado [2]el Ing. Fulvio Andrés Carrasco Cabrera de la Universidad Católica de Santiago de Guayaquil se diseñó y configuró mediante el Software GNS3 una red de accesos para medianas empresas en el Ecuador como CONSTELEC, utilizando la tecnología SD-WAN con equipos Fortigate, a fin de cumplir con sus requerimientos, necesidades y alternativas de servicio que requieren los administradores de la red. Se logró simular e implementar el diseño de la red para este proyecto de investigación a través del simulador GNS3 aplicando la tecnología SDWAN, el mismo que permite configurar de forma manual o gráfica los enrutamientos, gestión de equipos, tiempos de latencia, conmutación rápida, etc., y observar gráficamente mediante curvas el rendimiento del comportamiento parcial o total de la red.

Otra investigación que encontramos [3] Gabriel Marcelo Jiménez Macías de la Universidad Nacional de Loja el trabajo se enfoca en el estudio y diseño de una red de datos utilizando el protocolo múltiple de conmutación por etiquetas (MPLS, por sus siglas en inglés), para la interconexión de las dependencias externas de la Universidad Nacional de Loja (UNL) que se encuentran ubicadas en la región 7, este proyecto ha sido planteado por la Unidad de Telecomunicaciones e Información (UTI), departamento perteneciente a la UNL y los resultados obtenidos fueron El proceso de diseño de esta red MPLS VPN capa 3 planteado en este proyecto, puede ser tomado como referencia para la interconexión de más dependencias externas en otras regiones pertenecientes a la Universidad Nacional de Loja.

Otra Investigación [4] , Emileni Solange Castro Ullauri de la Universidad Politécnica Salesiana Sede Guayaquil realizó un diseño y simulación de una red MPLS para interconectar estaciones remotas utilizadas el en emulador GNS3 dentro una empresa X describiendo claramente las ventajas y desventajas que ofrece las mismas con la implementación se logró evidenciar que el protocolo MPLS permite realizar una mezcla entre el proceso de enrutamiento y reenvió de datos , además se verifico como pueden trabajar en conjunto con el protocolo BGP para permitir la superposición de rutas en la nube MPLS y también se identificó la manera de ahorrar recursos y puertos físicos a la hora de implementar MP-BGP.

## 2.3. OBJETO Y CAMPO DE ACCIÓN

### 2.3.1. Objeto de estudio

**Tecnología EVPN y VPLS**

EVPN (Ethernet VPN) Es un nivel de control BGP basado en estándares que le permite extender la comunicación de Capa 2 y Capa 3 entre diferentes centros de datos.

VPLS (Servicio de red de área local privada virtual) es una tecnología de red para proporcionar servicios basados en Ethernet basados en conexiones multipunto a multipunto sobre redes IP/MPLS. Esto significa que con VPLS, la red local o red de área local llega a la sede de cada empresa a través de la interfaz del proveedor de servicios. Luego, la red del proveedor simula el comportamiento de un conmutador o puente mediante la creación de una LAN compartida en todos los sitios con un solo dominio de transmisión. Un caso muy común de este tipo de servicio es la comunicación entre dos oficinas mediante Ethernet, también conocida como línea Ethernet privada. Esta es una poderosa alternativa a las líneas dedicadas tradicionales de los operadores, que se proporciona localmente a través de Ethernet sin necesidad de un conmutador.

### 2.3.2. Campo de Acción

Rendimiento de las tecnologías EVPN y VPLS en la Universidad Técnica de Cotopaxi

## 2.4. BENEFICIARIOS

En la tabla 1, se puede evidenciar que los beneficiarios de este proyecto de investigación es principalmente la Universidad Técnica de Cotopaxi y los beneficiarios indirectos serían el grupo de investigación y personas externas.

Tabla 1. Beneficiario directos e indirectos

| Beneficiarios Directos | Beneficiarios Indirectos |
|---|---|
| TICS de la Universidad Técnica de Cotopaxi | Estudiantes de la carrera de sistemas de información (sexto, séptimo, octavo) |

## 2.5. JUSTIFICACIÓN

La fama del protocolo MPLS no es desinteresada para las organizaciones, ya que la utilización de la misma mejora el flujo de datos mediante una topología de muchos a muchos, es decir mejora la disponibilidad y efectividad, así como un soporte que nos brinda la amplia variedad de servicios.

Una red virtual privada es una técnica muy exitosa que puede ejecutarse encima de cualquier tipo de entrada o circuito terminal, también se puede utilizar con tecnologías que no son ethernet como son ATM o Frase Relay, además está en constante desarrollo, para los usuarios de internet y que es una excelente opción si quieren tener conexiones privadas y seguras.

Una propiedad del servicio es que permite al usuario administrar su propia distribución a través de una red virtual privada, lo que concede al usuario una sensación de control y seguridad.

## 2.6. HIPÓTESIS

El estudio comparativo del rendimiento de tecnologías EVPN y VPLS en un ambiente simulado GNS3 permitirá mejorar los niveles de seguridad en las Redes de la Universidad Técnica de Cotopaxi

## 2.7. OBJETIVOS

### 2.7.1. General

Experimentar una simulación mediante con el software GNS3 aplicando las tecnologías EVPN y VPLS en conjunto con el protocolo MPLS para cuantificar la eficiencia, eficacia de la seguridad y flujo de los datos en la red de la Universidad Técnica de Cotopaxi.

### 2.7.2. Específicos

- Revisar la literatura bibliográfica sobre las tecnologías de red virtual privada EVPN Y VPLS en conjunto con el protocolo IP/MPLS.
- Indagar las herramientas de software con las propiedades para la medición del rendimiento de la red con cada tecnología de red virtual privada.

- Cuantificar los resultados obtenidos de la simulación de las tecnologías EVPN Y VPLS sobre el entorno fingido para determinar cuál de las dos tecnologías es mejor en la red de la Universidad Técnica de Cotopaxi.

## 2.8. SISTEMAS DE TAREAS

Tabla 2. Planificación de actividades.

| OBJETIVOS ESPECÍFICOS | ACTIVIDADES | RESULTADOS DE LAS ACTIVIDADES | DESCRIPCIÓN (TÉCNICAS E INSTRUMENTOS) |
|---|---|---|---|
| Revisar la literatura bibliográfica sobre las tecnologías de red virtual EVPN Y VPLS | Comparación de fuentes bibliográficas. | -Conocimiento sobre las tecnologías EVPN y VPLS. | -Revistas científicas<br>-Proyectos de investigación<br>-Tesis |
| Indagar las herramientas de software con las propiedades para la medición del rendimiento de la red con cada tecnología de red virtual privada. | -Escoger el Escenario correcto | -Conocimiento del simulador GNS3 | -Revistas científicas<br>-Proyectos de investigación |
| Examinar los resultados de las tecnologías EVPN Y VPLS sobre el entorno fingido. | - Comparación de resultados con la simulación | - Ejecución de la simulación. | -Simulación en la herramienta llamada GNS3. |

| | | | |
|---|---|---|---|
| | | | |

# 3. FUNDAMENTACIÓN TEÓRICA

| Etapa inicial: | | |
|---|---|---|
| Actividad | Fecha de inicio | Fecha de cierre |
| Desarrollo del documento de titulación | 22/11/2021 | 15/08/2022 |
| Recolección de información: | | |
| Actividad | Fecha de inicio | Fecha de cierre |
| Configuración de equipos a utilizar. | 06/12/2021 | 05/05/2022 |
| Creación de una de EVPN y VPLS. | 13/12/2021 | 12/06/2022 |
| Simulación del envío de paquetes | 03/01/2022 | 05/07/2022 |
| Informe de resultados: | | |
| Actividad | Fecha de inicio | Fecha de cierre |
| Muestra de resultados de las simulaciones que realizamos | 04/08/2022 | 24/08/2022 |

## 3.1. Antecedentes

### 3.1.1. MPLS Multiprotocolo Label Swithing

El protocolo llamado MPLS se creó en la década de 1990, en un contexto donde la comunicación asincrónica era conocida por ser una tecnología de red de área amplia, posee varias ventajas, como son: multiservicio, transporte asíncrono, estado de envió reducido, clase

de servicio entre otros. Sin embargo, tenía algunos defectos y son: que no tenía ninguna complexión a la pérdida de los datos, una carga que de envío que lo hacía poco eficaz a las altas velocidades, la inexistente integración nativa con IP etc.

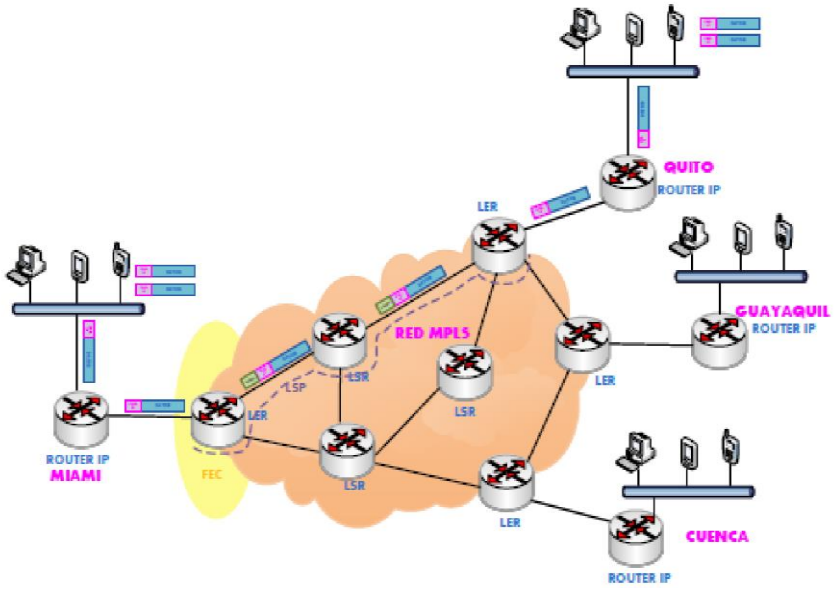



Figura 1. Componentes de la red MPLS [1]

El protocolo MPLS es una ciencia de envió asíncrono es decir que varios paquetes son enviados en el mismo momento, en contexto es parecido al protocolo de IP, pero la ciencia de MPLS es mucho más ligero y disminuye en volumen la cantidad de estado que es necesario ser señalado [1].

### 3.1.2. Características Básicas y funcionamiento

Un router de acceso a internet recibe un paquete del protocolo IP, este paquete tiene datos o información que no solo es la dirección IP de destino. No hay referencias de cómo el paquete debe ser tratado o enviado eso depende de cada router y la decisión que tome el router depende directamente del tipo de encabezado que tiene cada paquete, por lo consiguiente cada vez que un paquete llegue a un router debe de disponer donde enviar el paquete, y el router toma como referencia a tablas de enrutamiento complejas, este proceso se repite cada vez que sea necesario hasta que el paquete llegue a su destino.

Todas estas acciones que realiza el router hace que sea un proceso deficiente para aplicaciones que son dependientes al tiempo como: videoconferencias [1].

### 3.1.3. Arquitectura

El protocolo MPLS utiliza el protocolo IP heredado, mediante el cual el protocolo MPLS dispone de un conocimiento más exacto del estado de la red que vamos utilizar, son necesarios varios procesos de señalización, el empleo siempre va en conjunto con una comunicación de extremo a extremo, posteriormente vamos utilizar dos protocolos llamados LDP (Protocolo de distribución de etiquetas) y el protocolo RSVP (Protocolo de reserva de recursos), son los protocolos que elegimos.

Cada red se comunica por un camino lógico de extremo a extremo, ese camino es establecido según el estado de la red y las necesidades de las conexiones.

El proceso de defensa de la red llamado (Forward) no actúa sobre el contenido del paquete en el nivel 3, luego se añade al paquete una etiqueta y con el entendimiento de esta se añade el Forward, la sustitución de cada etiqueta se sobrescribe en un ámbito local, es decir que es en cada router. [1]

### 3.1.4. Protocolos utilizados

- LSR (Enrutadores conmutadores de etiquetas) Elemento que une etiquetas.
- LSP ((Ruta de cambio de etiqueta) El nombre inicial de la ruta MPLS especificada entre puntos finales.
- FEF (Clase Equivalencia de envió) Asignación que se da en el tráfico que va a la par con la etiqueta, conjunto de paquetes tratados del mismo modo por router. [1]

## 3.2. VPN

En el mundo se ha transformado últimamente ya no solo se trata de asuntos locales o internacionales ahora muchas organizaciones tienen que liderar con los mercados globales que existe por eso esas organizaciones necesitan una comunicación segura, confiable sin importar donde estén sus oficinas.

Los datos enviados a través de Internet son más vulnerables a los ataques porque viajan a través de la red interna de la empresa, son vulnerables a cualquier usuario malicioso. La solución a esta necesidad de una conexión confiable es conectar redes remotas a través de líneas dedicadas, sin embargo, este es un costo alto que la organización no está dispuesta a pagar.

### 3.2.1. ¿Cómo funciona una VPN?

VPN es una tecnología de red que permite la extensión segura de una red de área local (LAN) a través de una red pública encapsula y cifra paquetes de datos a varios puntos remotos. Mediante el uso de infraestructura de transporte público. Permite que las computadoras en una red envíen y reciban datos a través de una red compartida o pública como si fuera una red privada.

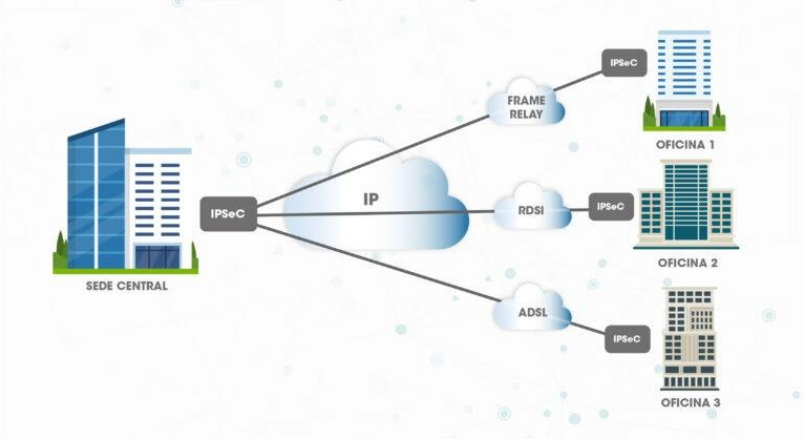



Figura 2. Arquitectura de una VPN [4]

VPN ofrece una solución de bajo costo para implementar la red a larga distancia al basarse sobre Internet, además de ofrecer autenticación de usuarios o equipos a través de cifrados, firmas digitales o claves de acceso para una identificación inequívoca; ofrece también integridad, garantizando que los datos enviados por el emisor sean exactos a los que se reciben, y confidencialidad, el cifrado hace posible que nada de lo transmitido sea interceptado o interpretada por nadie más que emisor y destino[5].

### 3.2.2. Requerimientos básicos para una VPN

Las VPN deben contar con algunos elementos básicos antes de que puedan implementarse, como un conjunto de políticas de seguridad para el cifrado de datos, ya que no están expuestos a clientes no autorizados en la red; Gestión de claves, para proporcionar cifrado entre el cliente y el servidor; compartir datos, aplicaciones y recursos; Servidor de acceso y autenticación, para que la red controle quién ingresa, verifique su identidad y tenga un registro estadístico de acceso; Gestión de direcciones, ya que la VPN debe generar una dirección para el cliente en la red privada y debe garantizar que estas direcciones permanezcan privadas finalmente soporta muchos protocolos, ya que tiene que gestionar los protocolos comunes de Internet, como IP.

Como podemos ver antes de implementar una VPN existe varias políticas de seguridad para la codificación de datos porque no debe ser visible por clientes no autorizados en una red o la administración de claves se debe asegurar la codificación entre los clientes y el servidor como la compartir los datos, aplicaciones o recursos también debe tener la debida autenticación y verificar su identidad para que la red tenga un control de quienes ingresan [5].

#### 3.2.3.1. TIPOS DE VPN

- Acceso VPN Remoto: Incluye usuarios que se conectan a una empresa desde ubicaciones remotas utilizando Internet como enlace de acceso. Una vez autenticados, tienen el mismo nivel de acceso que el nivel de acceso dentro de la red local.
- VPN Punto a Punto: Se utiliza para conectar diferentes oficinas de forma remota a una oficina central. Un servidor VPN está permanentemente conectado a Internet, acepta conexiones de sitios web y crea un túnel VPN. Se utiliza para eliminar la comunicación tradicional punto a punto.
- VPN interna (o Ver LAN): funciona como una VPN normal, excepto dentro de la misma LAN local en lugar de navegar por Internet. Se utiliza para aislar áreas y servicios de una misma red local. También se utiliza para mejorar las características de seguridad de las redes Wi-Fi inalámbricas.

## 3.3. VPLS Virtual Private LAN Service

### 3.3.1. Terminología

VPLS, también conocido como Servicio de red de área local transparente (TLS), es una capa VPN de punto a multipunto que permite que varios sitios de usuarios se comuniquen a través de una simulación de red de área local (LAN) de Ethernet. Todos los sitios de clientes que pertenecen a una entidad VPLS parecen estar en la misma red de área local, independientemente de su ubicación, como si estuvieran conectados entre sí a través de un solo conmutador Ethernet grande. VPLS se basa en la transmisión de tramas Ethernet. Como resultado, la red del proveedor de servicios puede transmitir información basándose únicamente en su dirección MAC, o teniendo en cuenta etiquetas LAN virtuales (Virtual LAN Tag, como su nombre en inglés).

Esta es la razón por la que los enrutadores PE deben admitir todas las características "clásicas" de Ethernet, como el aprendizaje de direcciones MAC, la derivación de tramas, etc. Esto se

llama un puente virtual (VB). La funcionalidad VB en PE se implementa asignando una VFT a cada entidad VPLS.

Los elementos necesarios para configurar una entidad VPLS son, como era de esperar, los mismos que componen una VPN MPLS L2 en general: backbone MPLS, enrutadores CE y PE, circuitos de interconexión (AC), puentes virtuales (VB, la palabra en inglés) y puente virtual) El túnel y el túnel imaginario. Los puentes virtuales no son diferentes de las tablas de relés virtuales (VFT) anteriores. Por otro lado, la definición de pseudocableado se usa para designar una entidad de comunicación bidireccional entre enrutadores PE que consta de dos circuitos virtuales unidireccionales (VC) o LSP en direcciones opuestas.

El resto de las designaciones siguen siendo las mismas. Esto simplifica el límite LAN/WAN y permite una prestación de servicios rápida y flexible [6].

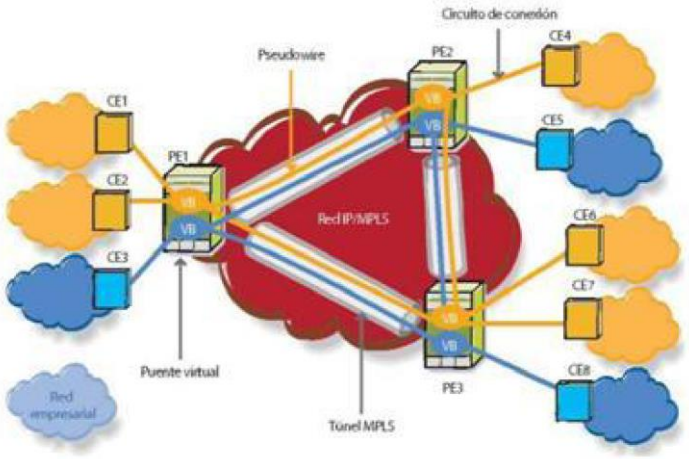



Figura 3. Estructura de VPLS [5]

### 3.3.2. Plano de reenvío

Encapsula, reenvía y decodifica tramas Ethernet desde el momento en que ingresan a la red del ISP hasta que salen del ISP.

### 3.3.3. Plano de Control

Detecta miembros de una entidad VPLS, lo que puede hacerse mediante configuración manual o automáticamente mediante el uso de ciertos protocolos. Además, dicho avión es responsable de la señal, a través de la cual establece, mantiene y elimina PWs entre los PE pertenecientes a la entidad VPLS. Estas funciones se pueden implementar mediante el uso de dos protocolos: BGP (Border Gateway Protocol) y LDP (Label Distribution Protocol). Estas variantes se

encuentran en IETF RFC 4761 y 4762, respectivamente, lo que da como resultado dos clasificaciones: VPLS Kompella y VPLS Martini. [6].

### 3.4. EVPN Ethernet Virtual Private Network

Este es un nuevo protocolo para conectar dominios L2 (Ethernet) sobre redes IP/MPLS. En el proceso de estandarización (borrador, RFC) a través de los distintos grupos de trabajo del "IETF Internet L2 Working Group". Algunos de los autores de la especificación EVPN son:

- Fabricantes: Juniper, Cisco, Alcatel-Lucent
- Proveedores de servicios: AT&T, Verizon, Bloomberg

Actualmente existen implementaciones comerciales basadas en proyectos: Juniper (EVPN), Cisco (PBB-EVPN), Alcatel-Lucent (EVPN, PBB-EVPN) [7].

#### 3.4.1. Tipos de EVPN

Existen tres tipos diferentes de tecnología según la solución implementada en el plano de datos: EVPN, PBB-EVPN y EVPN-VXLAN.

- Todos admiten aprendizaje de enrutamiento entre PE (nivel de control) a través de MP-BGP
- EVPN utiliza el protocolo MPLS/IP en el plano de datos. Esta es la solución EVPN original en la especificación de tecnología central.
- PBB-EVPN combina IEEE 802.1ah PBB y EVPN para aumentar la escalabilidad de MAC agregando C-MAC a B-MAC.
- Esta presentación versa sobre la primera de ellas: EVPN.

#### 3.4.2. Limitaciones resueltas por EVPN

##### 3.4.2.1. Integración de servicios

- Permite la provisión de servicios L2 y L3 en la misma interfaz de acceso, VLAN y VPN.
- La operación y entrega es similar a L3VPN, heredando sus características de escalabilidad y control.

##### 3.4.2.2. Eficiencia

- Habilita el equilibrio de carga por subproceso en un entorno de todos los múltiples sistemas activos (con todos los enlaces de acceso de servicio activo).
- Gestión mejorada de tráfico de difusión, unidifusión desconocida y multidifusión (BUM) [7].

#### 3.4.2.3. Flexibilidad

- Varias opciones de encapsulación de nivel de datos: MPLS, IP, VXLAN.
- Admite los servicios E-LAN, E-Line y E-TREE existentes.
- Simplificar la prestación de servicios y la operación con una única tecnología VPN [7].

### 3.4.3. ¿Qué son EVPN y BGP EVPN?

EVPN es una solución VPN portadora de servicio completo de próxima generación. Subvierte el mecanismo tradicional de L2VPN de aprender direcciones MAC en el plano de reenvío, introduce el plano de control y utiliza extensiones BGP para transmitir información de direcciones MAC. Basado en MP-BGP, EVPN define una serie de nuevos tipos de ruta BGP EVPN que permiten que diferentes sitios aprendan las direcciones MAC entre sí [8].

Las rutas BGP EVPN se clasifican en los siguientes tipos:

- Una ruta de descubrimiento automático de Ethernet anuncia la accesibilidad del PE local a las direcciones MAC de sus sitios conectados. Esta ruta se usa principalmente en escenarios de convergencia rápida, protección de redundancia, creación de alias y horizonte dividido para implementar el balanceo de carga en una red de conexión múltiple.
- Una ruta EVPN MAC/IP anuncia la dirección MAC, la dirección IP y otra información de los sitios. Esto elimina la necesidad de inundar las solicitudes ARP en la red, lo que reduce el volumen de tráfico de transmisión en la red y ahorra recursos de ancho de banda.
- Una ruta de multidifusión inclusiva anuncia la accesibilidad de la dirección del tráfico de difusión, unidifusión desconocida y multidifusión (BUM) para implementar el descubrimiento mutuo de vecinos en un dominio de difusión. Esto permite que el PE local envíe el tráfico BUM recibido de los CE al PE remoto. Dicha ruta también contiene atributos de túnel que permiten a los PE establecer un túnel entre ellos para transmitir tráfico de plano de datos [7].
- Una ruta de segmento Ethernet permite que los PE conectados al mismo CE se descubran entre sí. Esta ruta se utiliza principalmente para la elección del transitario designado (DF). Para evitar que un CE con conexión múltiple a varios PE reciba tráfico duplicado, solo se requiere un PE para reenviar el tráfico BUM al CE. Tal PE se elige entre todos los PE en el mismo segmento Ethernet (ES) a través de la elección de DF.

- Una ruta de prefijo IP permite que una EVPN acceda a la red externa. EVPN anuncia rutas externas importadas como rutas de prefijo IP.

### 3.4.4. ¿Cómo funciona EVPN?

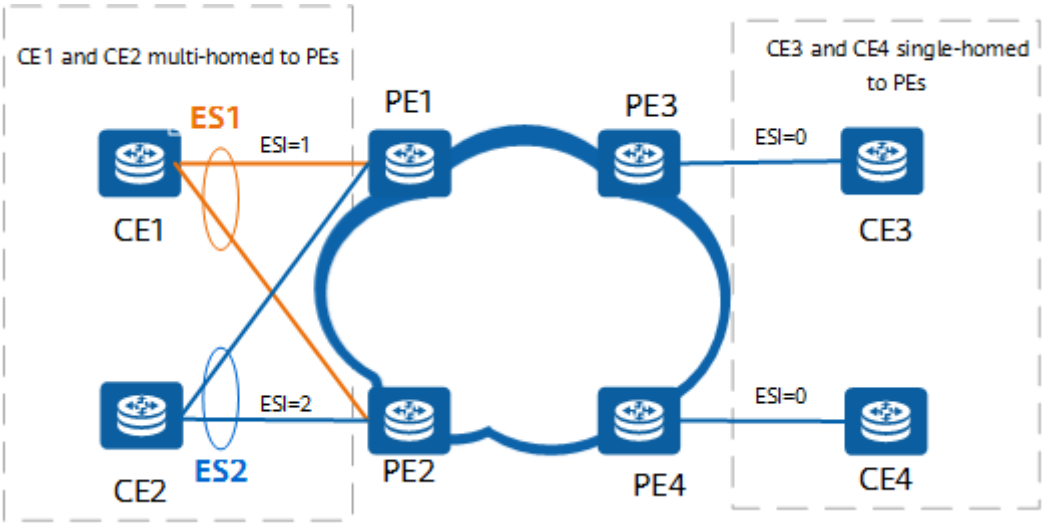



Figura 4. redes EVPN [8]

#### ´3.4.4.1. ES

Si un CE es multidireccional a dos o más PE, los enlaces Ethernet que conectan el CE a diferentes PE forman un ES. En la red que se muestra en la figura anterior, CE1 tiene conexión dual a PE1 y PE2, y los dos enlaces Ethernet entre CE1 y PE1 y entre CE1 y PE2 forman un ES.

#### 3.4.4.2. ESI

Un identificador de segmento de Ethernet (ESI) identifica de forma única un ES. En la red que se muestra en la siguiente figura, las interfaces de diferentes PE conectadas al mismo CE deben tener el mismo ESI. Si el ESI es 0, el CE se une al PE.

#### 3.4.4.3. EVI

Se utiliza una instancia de EVPN (EVI), similar a la instancia de conmutador virtual (VSI) de VPLS, para identificar a un cliente de VPN. Debido a que EVPN es un tipo de VPN, un PE puede tener múltiples EVI.

MAC-VRF

Un MAC-VRF almacena direcciones MAC aprendidas por un EVI a través de extensiones BGP. Cada EVI tiene un MAC-VRF independiente [8].

### 3.4.5. Proceso de inicio de EVPN

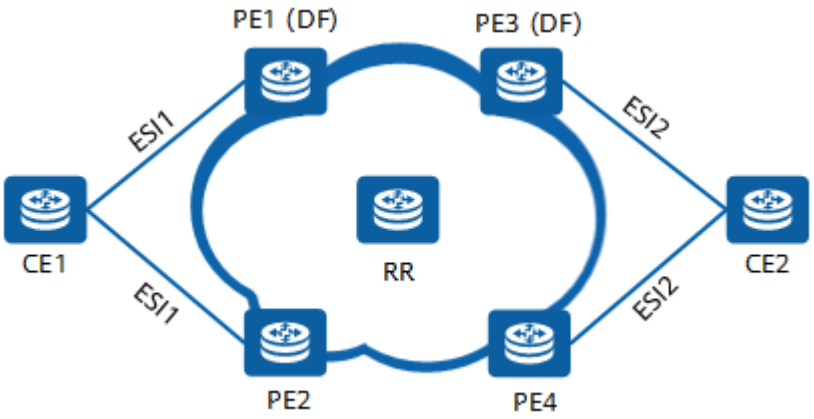



Figura 5. Topología de una red EVPN [8]

Como se muestra en la figura anterior, el proceso de inicio de EVPN consta de los siguientes pasos:

- Cree un EVI para cada PE y configure los atributos RD y RT de cada EVI.
- Configure pares BGP y habilite EVPN.

Cada PE envía una ruta de Tipo 3 a sus pares. Una ruta de Tipo 3 contiene la información de RD y etiqueta (asignada por MPLS).

Cuando un par recibe el paquete, agrega la información de ruta a su tabla de reenvío de tráfico BUM local para guiar el reenvío de paquetes BUM.

- Enlace el ESI generado al EVI.

Luego, cada PE comienza a enviar una ruta Tipo 4 a sus pares. Una ruta de tipo 4 transporta la información de dirección de origen de RD, ESI y PE.

Los compañeros guardan la información de ESI recibida en la tabla de información de miembros de ESI.

- Los PE intercambian rutas de Tipo 1 para actualizar las etiquetas ESI.

Una vez completada la elección de DF, los PE anuncian rutas de tipo 1 entre sí. Estas rutas llevan ESI y etiquetas asignadas para los ESI correspondientes.

Después de recibir una ruta Tipo 1 de un par, un PE verifica si el ESI transportado en la ruta es el mismo que el ESI local. Si los ESI son los mismos, el PE agrega el ESI a su lista de miembros de ES locales [8].

### 3.4.6. Aprendizaje de direcciones MAC

Suponga que CE1 envía una solicitud ARP a PE1.

PE1 aprende la dirección MAC mac1 de CE1 a través del plano de reenvío y guarda la dirección MAC en su MAC-VRF local.

Luego, PE1 genera una ruta Tipo 2 para anunciar mac1 a otros PE. La ruta Tipo 2 transporta el RD de la etiqueta EVI, ESI, mac1 y MPLS asignada a mac1.

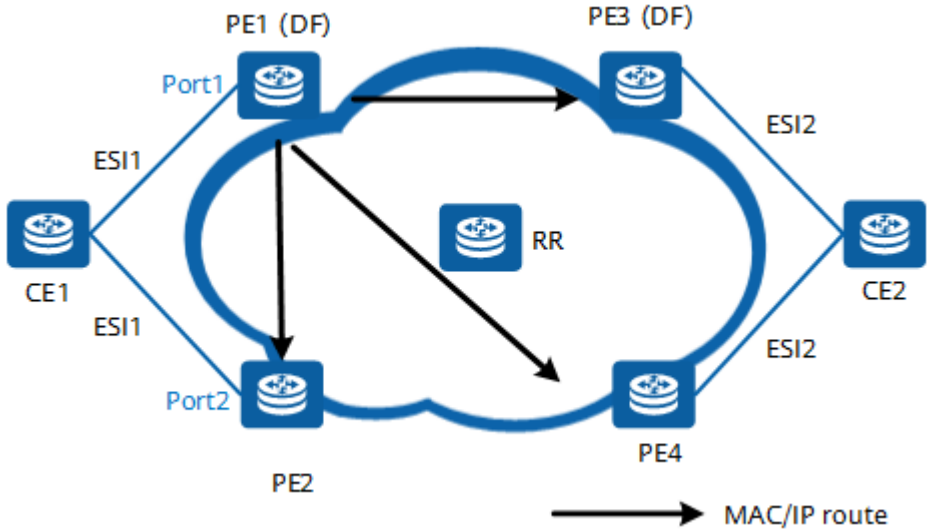



Figura 6. Anuncio de ruta tipo 2 [8]

En la red que se muestra en la figura anterior, después de recibir una ruta de tipo 2 de PE1, PE3 y PE4 actualizan sus MAC-VRF locales. De esta forma, PE3 y PE4 aprenden la dirección MAC de CE1 a través del plano de control. PE2, después de recibir la ruta, encuentra que lleva el mismo ESI que el ESI local.

Por lo tanto, PE2 selecciona preferentemente la ruta con el siguiente salto local siendo Port2.De manera similar, PE2 genera una ruta de tipo 2 que anuncia mac1 en función de la dirección MAC local y anuncia la ruta a sus pares.

El proceso anterior permite que todos los PE aprendan la dirección MAC de CE1.

### 3.4.6. ¿Cuáles son las aplicaciones típicas de EVPN?

#### 3.4.6.1. PBB

PBB-EVPN es una tecnología L2VPN de próxima generación basada en tecnologías MPLS y Ethernet. PBB-EVPN usa BGP para intercambiar información de direcciones MAC entre PE en el plano de control y controla el intercambio de paquetes de datos entre diferentes sitios a través de la red MPLS.

Un servicio PBB-EVPN consta de dos partes: I-EVPN y B-EVPN. La interfaz conectada a un CE está vinculada a la instancia de I-EVPN para brindar acceso al servicio, y la instancia de B-EVPN se conecta a la red troncal para administrar las rutas EVPN enviadas desde otros PE.

#### 3.4.6.1. VPWS EVPN

Al igual que el servicio de cable privado virtual tradicional (VPWS), EVPN VPWS proporciona servicios de punto a punto (P2P). Esta solución aprovecha una versión simplificada de la tecnología EVPN original y utiliza túneles MPLS para atravesar la red troncal sin necesidad de aprender la dirección MAC.

En la red que se muestra en la siguiente figura, se establece una conexión VPWS utilizando ID de circuito adjunto (AC). El ACID local en un PE debe ser el mismo que el remoto en el PE del mismo nivel. De manera similar, el ACID remoto en el PE local debe ser el mismo que el local en el PE del mismo nivel [8].

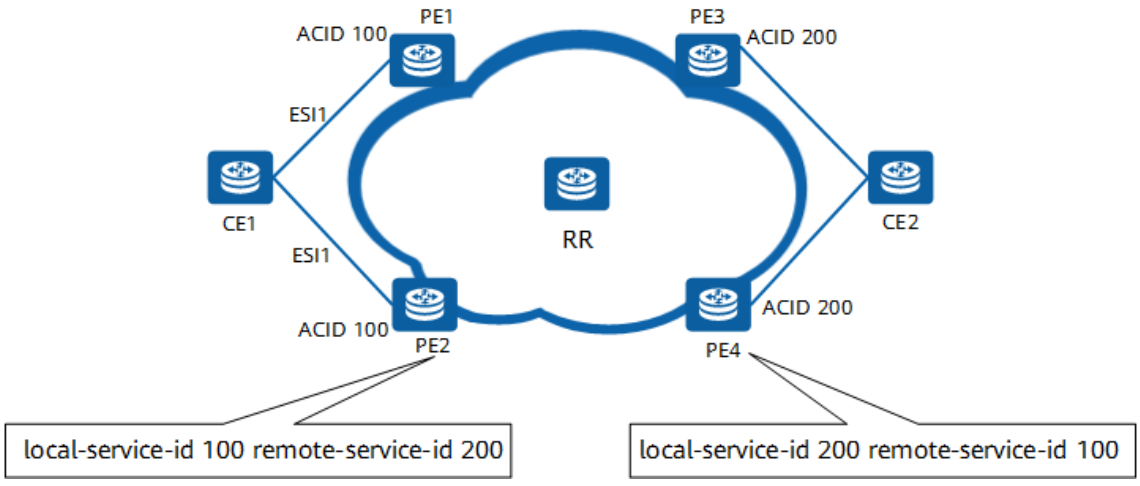



Figura 7. Redes EVPN VPWS [8]

## 3.5. ASPECTOS GENERALES

En este estudio es necesario combinar hardware y software para simular la topología de una red MPLS en un ambiente adecuado.

### 3.5.1. Hardware

Para poder realizar la simulación dentro del entorno de GNS3 es necesario conocer las características del hardware como los dispositivos de red que se eligieron para esta investigación son los siguientes:

- Ordenador: Acer con procesador AMD A12-9720P RADEON R7, disco sólido de 256GB y tiene una memoria de 8GB RAM DDR3.


Figura 8. Ordenador [7]

- **Router CRV 1000V:** Es de la marca Cisco utiliza el nuevo sistema operativo IOS XE tienes todas las funciones, que permite a los departamentos de TI implementar servicios de red de la clase empresarial en la nube de Azure cabe recalcar que soporta la tecnología EVPN.
- **Router 7200:** Es de la marca Cisco utiliza el sistema operativo IOS tienes características muy interesantes, proporciona un enrutamiento de alto rendimiento y un rendimiento de procesamiento además soporta el protocolo MPLS, BGP es fundamental para la tecnología VPLS.

### 3.5.2. Software

#### 3.5.2.1. IOS CISCO

IOS es el sistema operativo de conexión a Internet. Creado por Cisco Systems para programar y mantener dispositivos de red como conmutadores y enrutadores.

Para configurar un conmutador o enrutador Cisco, debe acceder a la interfaz de usuario de su computadora mediante un terminal o acceder de forma remota a través de telnet o ssh. Al acceder al dispositivo, debe registrarse antes de ingresar cualquier pedido [9].


Figura 9. logo Cisco IOS [17]

#### 3.5.2.2. Componentes

La arquitectura interna del enrutador/conmutador de Cisco admite componentes que son críticos para el proceso de inicio, como se muestra en la Figura 10. Las partes internas son las siguientes:

- RAM / RAM: almacena la tabla de enrutamiento, caché ARP, caché de intercambio en caliente, caché de paquetes (RAM compartida), cola de paquetes. La RAM también proporciona memoria temporal y/o activa para el archivo de configuración del enrutador cuando el enrutador está encendido. El contenido de la memoria RAM se pierde si se corta la alimentación o se reinicia la computadora. • NVRAM: la RAM no volátil almacena una copia de respaldo del archivo de configuración/configuración de inicio del enrutador. El contenido de la NVRAM se conserva durante un corte de energía o si se reinicia la computadora. • Flash: ROM borrable y reprogramable que almacena firmware e imágenes para el sistema operativo.
- La memoria flash permite actualizaciones de software sin quitar o reemplazar el chip del procesador. El contenido flash se conserva en caso de un corte de energía o un reinicio. La unidad flash puede almacenar múltiples versiones del software IOS

- ROM: contiene diagnósticos de arranque, gestor de arranque y software del sistema operativo. • Las actualizaciones de software en ROM requieren la eliminación y el reemplazo de chips conectados al procesador
- • Interfaz: conexiones de red, ya sea en la placa base o en unidades de interfaz separadas, a través de las cuales los paquetes entran y salen de la computadora [9].

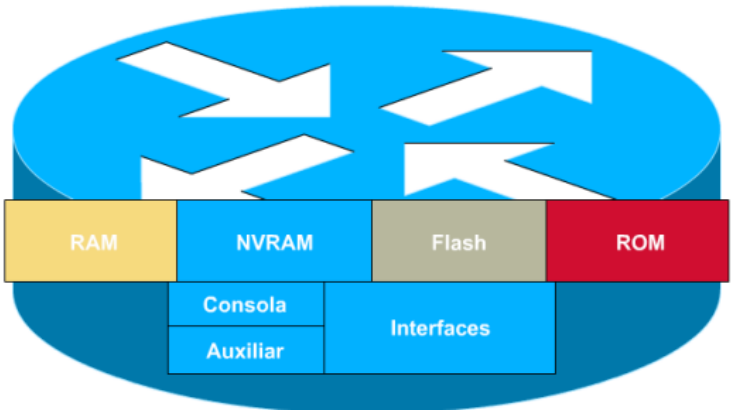



Figura 10. Componentes [9]

### 3.5.3. GNS3

Gns3 es una herramienta de virtualización de redes que utilizamos como fuente de ejecución la plataforma Dynamips/Dynagen, Dynamips es un software capaz de simular las arquitecturas de hardware de muchos modelos de routers de cisco, que es una marca de predominantes en el mercado de los elementos de redes ,Dynamips complementa toda la lógica que es necesario para virtualizar las diferentes topologías que existen en la actualidad , con el propósito de hacer fácil esta tarea y obtener los detalles del usuario de particulares de configuración del habitad de simulación , fue desarrollada la interfaz de comandos Dynagen .Desde un fichero de configuración donde se puede especificar las topologías que utilizaremos en la red (routers, conexiones, configuraciones, etc.), Dynagen instruye a Dynamips para realizar la correcta virtualización del escenario. El programa llamado GNS3 simplifica mucho más el proceso de configuración de topologías de red virtuales. Con la ayuda de una sencilla e intuitiva interfaz gráfica para los usuarios, este programa ofrece una interfaz muy fácil de utilizar para cualquier usuario.[10]


Figura 11. Logo de GNS3 [18]

#### 3.5.3.1. Creación de una topología en GNS3

La creación de una topología de red se organiza en tres pasos fundamentales:

- Primero, considere el escenario del cambio de enrutador. Con un sistema de elementos de arrastrar y soltar, el usuario elige el tipo de conexión y la distribuye en el área de trabajo de nuestra elección.
- A continuación, se modifica cada enrutador introducido anteriormente. A través del panel de configuración, puede especificar las características del enrutador, como la cantidad de interfaces y el tipo de cada una.
- El último paso para completar la construcción de la arquitectura es establecer conexiones entre los diferentes enrutadores del escenario. Para esto, la herramienta GNS3 proporciona un proceso de configuración de nodo simple donde se definen los puntos finales de los nodos.[10]

### 3.5.4. Motores de Simulación

#### 3.5.4.1. QEMU

QEMU es una aplicación de simulación de máquinas virtuales multiplataforma, emplea un traductor binario dinámico que tiene el propósito de convertir en tiempo de ejecución las instrucciones de la arquitectura imitando las características de la arquitectura sobre la cual ejecuta el emulador. Este código binario que se genera es procesado en una caché de traducción para ser utilizado nuevamente por el usuario.

Figura 12. Logo de QEMU [19]

QEMU es compatible con la mayoría de las arquitecturas de hardware, para diferentes patrones de usuario, como el modo de máquina virtual, donde: i386, x86_64, Alpha, arm, cry, lm32, m68k, microblaze, microblazeel, mips, mipsel, mips64, mips64el, or32, ppc, ppcemb, ppc64, sh4, sh4eb, sparc, sparc64, s390x, xtensa, xtensaeb, unicore32.

El soporte para una amplia gama de arquitecturas de hardware ha convertido a QEMU en uno de los emuladores más utilizados para el desarrollo de software en sistemas integrados. Aunque QEMU es un motor virtual, no proporciona un VMM. Esto requiere el uso de un módulo KVM (máquina virtual basada en el kernel) en el kernel de Linux. El KVM actúa como un controlador para controlar las máquinas virtuales proporcionadas por QEMU.

Con KVM, cada máquina virtual del sistema se trata como un proceso, independientemente de ciertas restricciones de seguridad, pero interactúa con los recursos del sistema como cualquier otro proceso del sistema. QEMU ha sido ampliamente utilizado en procesos de desarrollo de software tanto básicos como genéricos. Este es el estado del SDK de Android usando una versión personalizada de QEMU. También ha sido portado para ser empleado como herramienta de emulación/virtualización sobre otras plataformas, como ocurre en Plan9 y en Minix3 Las principales deficiencias o críticas hacia QEMU están dadas en que no posee una interfaz gráfica para la creación y configuración de máquinas virtuales como provee VirtualBox. Para tratar de enmendar este problema han surgido varias alternativas en los diferentes sistemas operativos como es el caso de QEMU Launcher en GNU/Linux, QEMU Manager en Windows y Q en MacOS, pero aún no se define una interfaz estándar [11].

#### 3.5.4.2. VMware player

VMware Player es un paquete de software de virtualización proporcionado de forma gratuita por VMware Inc., empresa que antes era una división y cuyo mayor accionista sigue siendo EMC Corporation. VMware Player puede ejecutar máquinas virtuales existentes y crear sus propias máquinas virtuales (requiere la instalación del sistema operativo para funcionar).

Utiliza el mismo kernel de virtualización que VMware Workstation, un programa con más funciones, pero no gratuito. VMware Player se proporciona para uso personal, no comercial, distribución u otro uso con consentimiento por escrito. VMWare no brinda soporte, pero hay un sitio comunitario activo para discusión y solución de problemas.[12]

Figura 13. Logo de VMware player [20]

VMware afirma que el Player ofrece mejores gráficos, un rendimiento más rápido y un diseño más ajustado, integración para ejecutar Windows XP bajo Windows Vista o Windows 7 que El modo Windows XP de Microsoft se ejecuta en Windows Virtual PC, que es gratuito para todos los efectos.[12]

Las versiones de VMware Player anteriores a la versión 3 no pueden crear una máquina virtual (VM), que debe ser creada por una aplicación compatible o manualmente siguiendo las instrucciones almacenadas en un archivo de texto con una extensión “. vmx"; las versiones posteriores pueden crear máquinas virtuales.

Las características de Workstation que no están disponibles en Player son "características centradas en el desarrollador, como Equipos, varias instantáneas y clones, y funciones de administración de derechos virtuales para la seguridad de puntos finales", y soporte de VMWare. El lanzador permite clonar una máquina virtual completa en cualquier momento copiando un directorio; Aunque no es una funcionalidad de instantánea completa, le permite almacenar una copia del dispositivo en un estado específico y volver a él más tarde si lo desea. VMware Player también se incluye en la distribución de VMware Workstation, para uso en instalaciones donde no todos los usuarios del cliente están autorizados a usar la versión completa de VMware Workstation. En un entorno donde se ejecutan algunas máquinas sin licencias de VMware Workstation VMWare Player, una máquina virtual creada por

Workstation se puede distribuir a computadoras que ejecutan Player sin pagar licencias de estaciones de trabajo adicionales si no se usan comercialmente [12].

### 3.5.5. Herramientas de Análisis

#### 3.5.5.1. Ostinato

Ostinato es un generador y analizador de tráfico de paquetes de red de comunicaciones con una interfaz gráfica de usuario fácil de usar. Tiene la capacidad de crear paquetes personalizados con la edición de cualquier campo para diferentes protocolos: Ethernet, 802.3, LLC SNAP, VLAN (con Q-in-Q), ARP, IPv4, IPv6, IP-in-IP, también conocido como IP Tunneling, TCP, UDP, ICMPv4, ICMPv6, HTTP, SIP, RTSP, NNTP, etc. Es útil para pruebas funcionales y de rendimiento. (Austin, 2010). Funciona en Windows y Linux [13].

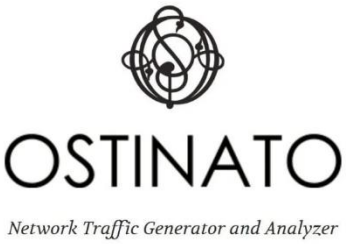



Figura 14. Logo de Ostinato [21]

#### 3.5.5.2. Wirehark

Wireshark es una herramienta de estudio de protocolos gratis creada por Gerald Combs, y hoy en día se utiliza para diferentes plataformas como son: Windows y Unix.

Su principal función es el estudio de tráfico en la red y puede ser una muy buena aplicación de apoyo didáctico para el análisis de las comunicaciones y para la solución de problemas de la red que se pueden suscitar [14].


Figura 15. Logo de Wireshark [22]

Wireshark es una herramienta que implementa una gran gama de procesos que facilitan la búsqueda de los varios protocolos que hay en la actualidad, y todo ello con una interfaz fácil de utilizar e intuitiva que permite dividir por capas cada uno de los paquetes obtenidos [14].

Gracias a la interfaz de Wireshark facilita el entendimiento de los diferentes protocolos que existen, podemos observar los campos de cada una de las diferentes cabeceras y capas que forman los paquetes automatizados, la herramienta da una gran gama de funcionalidades al administrador de redes para analizar el análisis de trafico de la red [14].

#### 3.5.2.2.1. Donde realizar la captura de datos

Para estudiar la red será de vital importancia en que capa analizar el tráfico de red. Supongamos un hábitat común. Nos encontramos en un alrededor comunicado compuesto por varios routers, varios equipos y un servidor de ficheros. Toda red debe tener una IDS detección de intrusiones: que es una funcionalidad usada para detectar accesos autorizados a una computadora un servidor [14].

La primera inquietud que hay es donde podemos instalarlo. Podría ser lógico instalar Wireshark en el mismo servidor de ficheros para estudiar el tráfico que hay en un fragmento de red, nos vamos encontrar con elementos en los cuales no podemos tener acceso físico al servicio o tan solo por seguridad [15].

# 4. MATERIALES Y MÉTODOS

El enfoque de la investigación es cuantitativo, por consiguiente, se pretende analizar el flujo de datos con las tecnologías EVPN y VPLS con el software Ostinato de una manera que facilite la investigación a corto mediano y largo plazo en el tiempo, con el propósito de entender de una manera más global el objeto de estudio sobre el rendimiento de la red de la Universidad Técnica de Cotopaxi.

## 4.1. Tipos de investigación

### 4.1.1. Investigación bibliográfica

La investigación bibliográfica permitirá obtener información relevante de artículos, libros, sitios web autorizados que tengan contenido verídico sobre las tecnologías EVPN y VPLS. La investigación se hará por medio de buscadores autorizados y repositorios bibliográficos que nos permitan la obtención de información.

### 4.1.2. Investigación de campo

La recolección de la información se llevará a cabo con el departamento de las TIC de la Universidad Técnica de Cotopaxi para saber las características e infraestructura que tiene la red.

### 4.1.3. Investigación descriptiva

La investigación tiene como propósito analizar las tecnologías de tráfico de datos que son: EVPN y VPLS para distinguir el rendimiento de la red de la Universidad Técnica de Cotopaxi y dar un informe con los resultados obtenidos al departamento de TICS.

## 4.2. Métodos Teóricos

## 4.3. Método Analítico

En esta investigación con la utilización de este método se diferenció los campos de estudio para así obtener la información por diferentes fuentes bibliográficas.

## 4.4. Método Hipotético

Mediante este método se planteó la hipótesis y a partir de ella se pudo expresar el tema que se investigó, realizando deducciones que nos ayudaron a comprobar la exactitud d o falsedad del problema a solucionar.

## 4.5. Población y muestra

### 4.5.1. Población

La población de alumnos corresponde a la carrera de Sistemas de Información, de toda esta comunidad estudiantil se extrajo información correspondiente de los cursos (sexto, séptimo y octavo), cuya cantidad de estudiantes aproximadamente 80, debido a que tienen un conocimiento avanzado.

### 4.5.2. Muestra

Hay dos fórmulas de la muestra finita e infinita para nuestro proyecto escogimos finita calculamos a una cierta cantidad de población.

$$\boldsymbol{n = \frac{N * Z_a^2 * p * q}{e^2 * (N-1) + Z_a^2 * p * q}}$$

$$\boldsymbol{n = \frac{70 * 1.960_a^2 * 0.4 * 0.5}{0.3^2 * (70-1) + 1.960_a^2 * 0.4 * 0.5}}$$

$$\boldsymbol{n = 64.77}$$

| Parámetro | Significado |
|---|---|
| N | Tamaño de la población |
| Z | Nivel de confianza |
| q | probalidad a favor |
| p | probalidad en contra |
| e | Error de muestra |

## 4.6. Variables

### 4.6.1. Variable independiente

Las tecnologías EVPN y VPLS.

### 4.6.2. Variable dependiente

Rendimiento del tráfico de datos de la red de la Universidad Técnica de Cotopaxi.

## 4.7. Metodología de la investigación

Para la elaboración del prototipo de la investigación se propuso la utilización de la metodología Top-Down Network Design.

# 5. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Para la elaboración del prototipo de la investigación se propuso la utilización de la metodología Top-Down Network Design.

Esta metodología tiene cuatro Fases, para el diseño de redes como:

### 5.1. Fase 1: Análisis de Negocios Objetivos y limitaciones

La Simulación tendrá una configuración con los dispositivos de red de marca Cisco para poder realizar la simulación de redes GNS3 es el más conveniente para el proyecto que estamos realizando, esta plataforma permite una simulación directa e indirectamente de las imágenes de router o swith. La versión de GNS3 que utilizaremos o se va implementar el prototipo de red es:

- GNS3 versión 2.2.3

Como se mencionó anteriormente sobre la plataforma de GNS3 es necesario la emulación directa e indirectamente a continuación se detallará:

- Emulación en vivo: Gns3 incluye un emulador de IOS (Cisco) que permite ejecutar binarios/imágenes sin configuración adicional.
- Emulación indirecta: GNS3 no cuenta con emuladores para todos los sistemas operativos, por lo que agrega funcionalidad para el uso de máquinas virtuales, habilitando herramientas de virtualización como VMware, VirtualBox, etc.

Los motores de virtualización que se utilizaran en esta investigación son las siguiente:

- VMware Player: esta herramienta de virtualización permitirá la optimización del hardware.
- GNS3 VM: Esta máquina virtual tiene el sistema operativo Ubuntu 14.04.5 LTS y es compatible con KVM (Kernel-Virtual Machine). Esta característica permite el mapeo de recursos de hardware como RAM, cantidad de procesadores y memoria ROM para un mejor rendimiento en la simulación de todos los dispositivos de red integrados en la topología.

### 5.2. Especificación de escenarios

La topología de VPN de capa 2 permite que sitios geográficamente dispares se conecten mediante puentes virtuales. Esto incluye dispositivos periféricos (servidores, enrutadores y conmutadores), que están conectados a uno o más enrutadores periféricos (PE), y también pueden incluir un conmutador de borde MPLS (MES) que opera en el borde de la infraestructura MPLS.

### 5.2.1. Instalación de GNS3

Para obtener el archivo de instalación se debe descargar desde la página oficial y seguir los pasos del asistente de instalación:

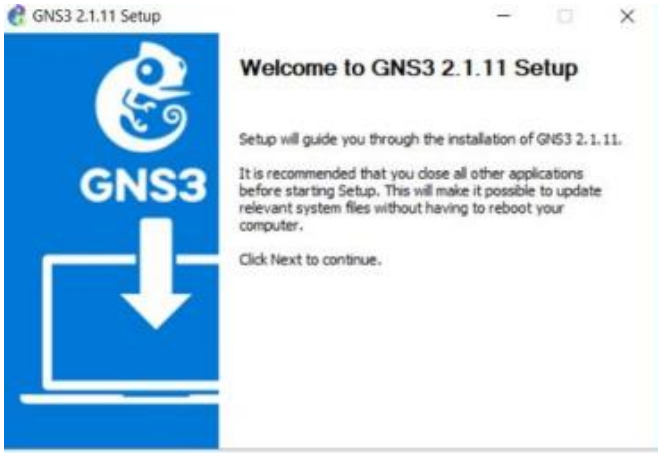



Figura 16. Instalación de GNS3(Paso 1)

Haga clic en el botón Acepto para continuar con la instalación de GNS3:


Figura 17. Instalación de GNS3(Paso 2)

Seleccione la carpeta de Menú de Inicio para el acceso directo GNS3, haga clic en Siguiente para continuar con la Instalación:

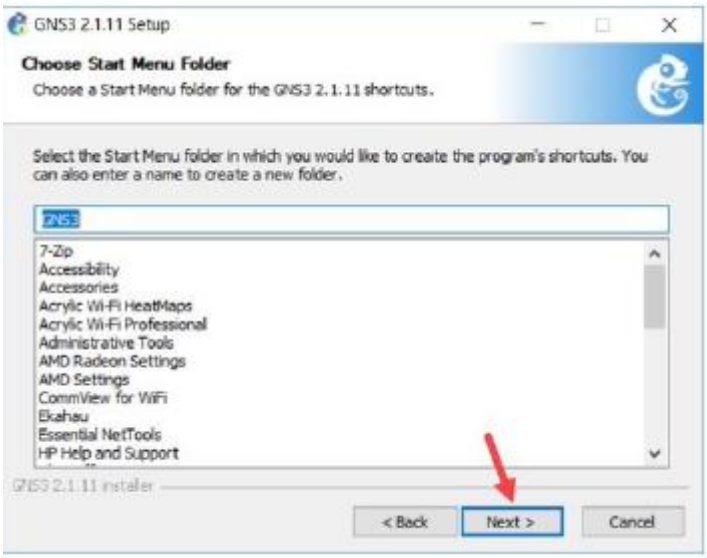



Figura 18. Instalación de GNS3(Paso 3)

En esta parte dejamos como predeterminado estas opciones y damos clic en siguiente:

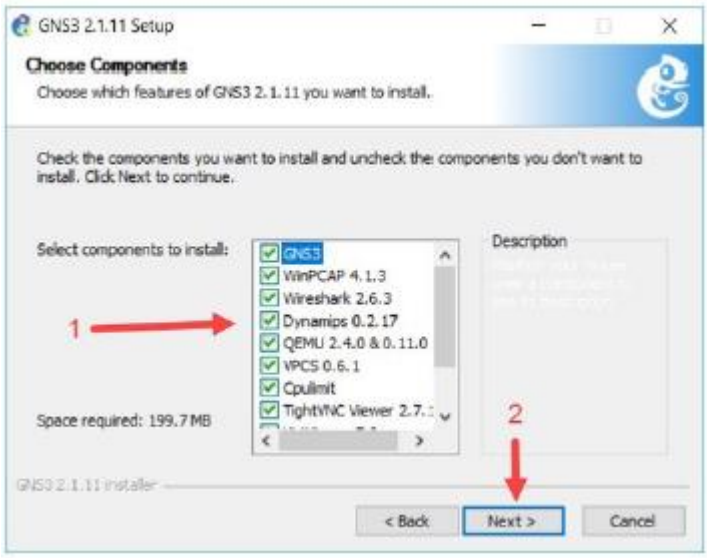



Figura 19. Instalación de GNS3(Paso 4)

Se elige la ubicación de instalación. La ubicación predeterminada es C: / Archivos de programa / GNS3 y luego haga clic en instalar:

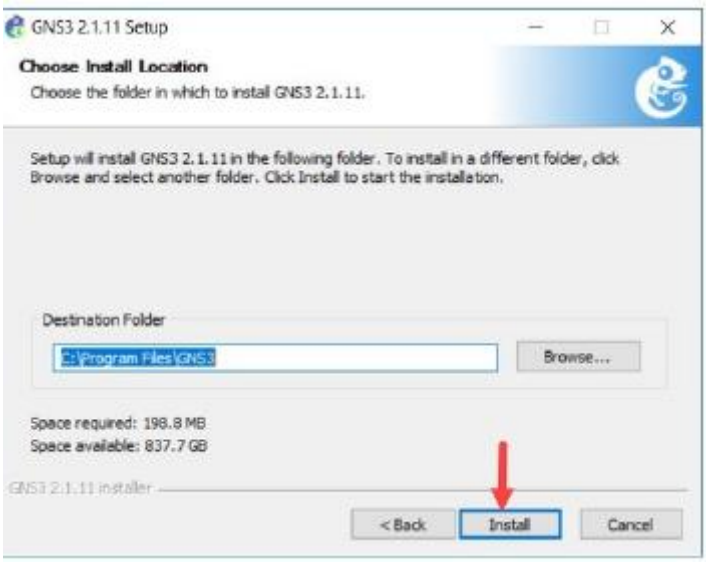



Figura 20. Instalación de GNS3 (Paso 5)

### 5.2.2. Configuración Básica

GNS3 tiene la ventaja de utilizar el servidor local o remoto para mejorar el rendimiento del hardware, por lo que es necesario crear un adaptador de red tipo anillo, de esta forma en las preferencias del servidor GNS3 se reenvía a la dirección IP del adaptador de loopback, se deben tomar los siguientes pasos:

#### 5.2.2.1. Creación de loopback

Es necesario ir al administrador de dispositivos para crear el loopback tenemos que ir en propiedades del sistema, luego agregar hardware como se muestra a continuación.

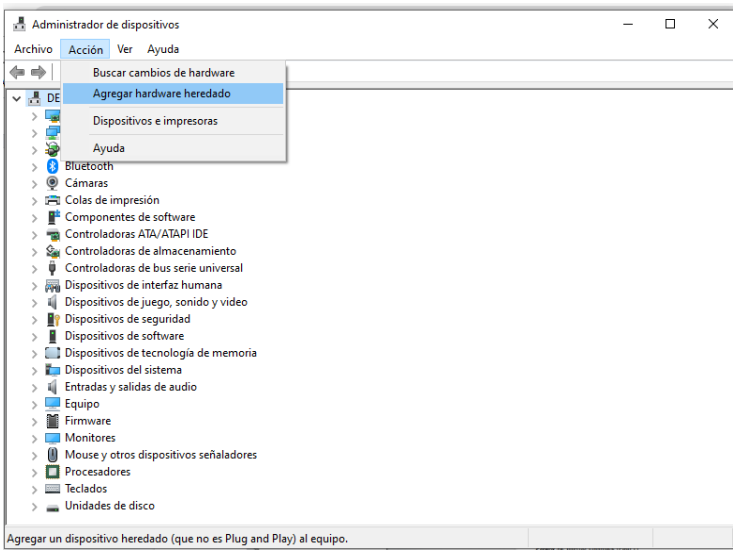



Figura 21. Interfaz de Loopback (Paso 1)

Solo damos en siguiente para crear el loopback como se muestra desde la figura 22 hasta la figura 27:

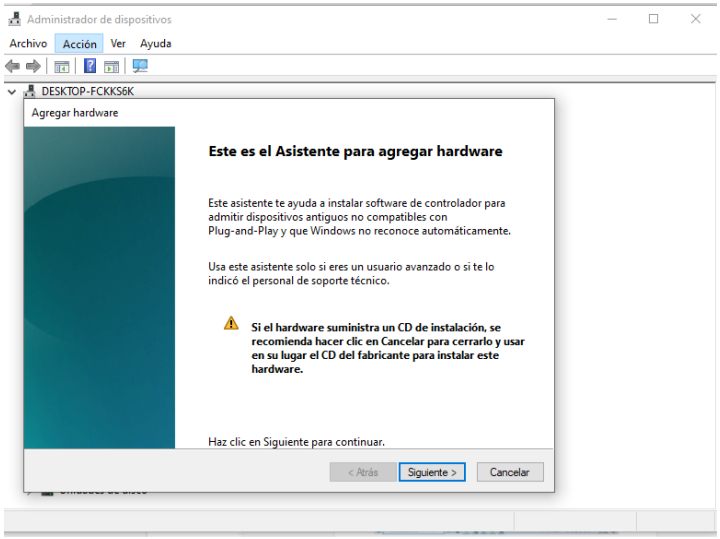



Figura 22. Interfaz de Loopback (Paso 2)

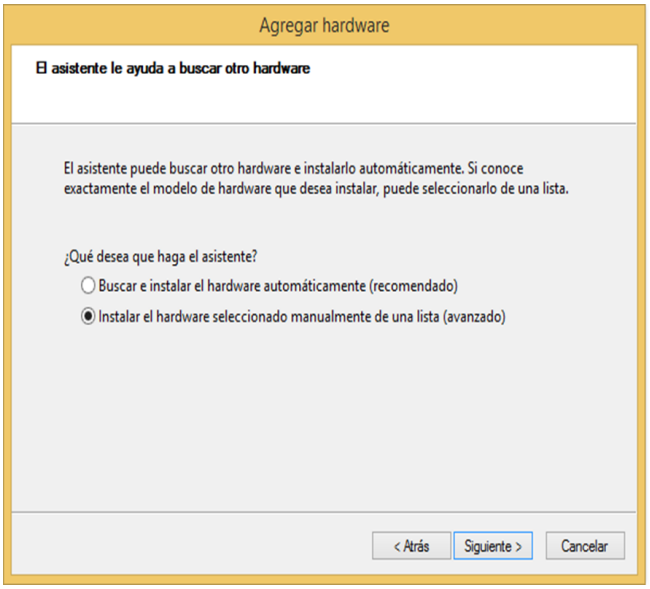



Figura 23. Interfaz de Loopback (Paso 3)

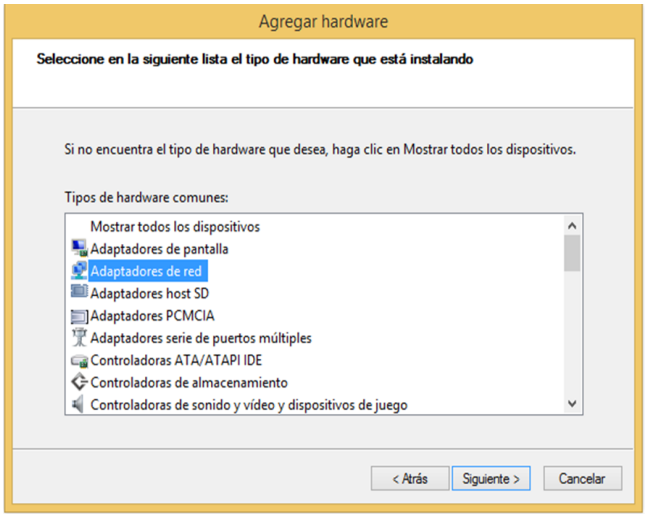



Figura 24. Interfaz de Loopback (Paso 4)

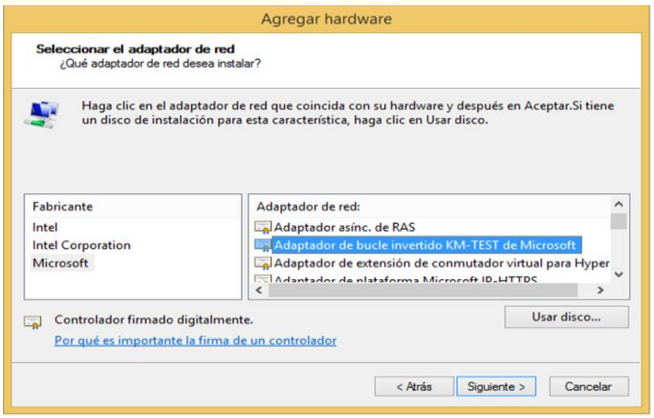



Figura 25. Interfaz de Loopback (Paso 5)

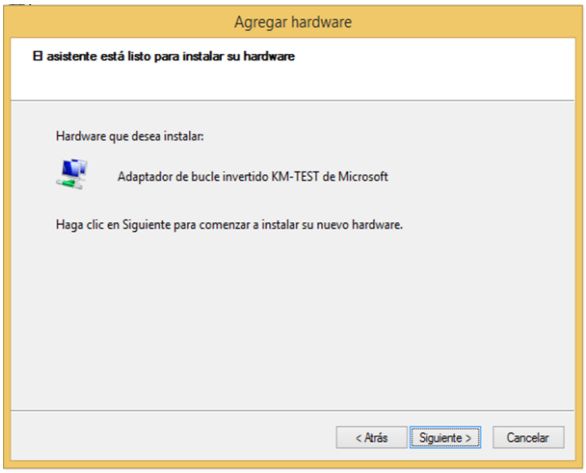



Figura 26. Interfaz de Loopback (Paso 6)

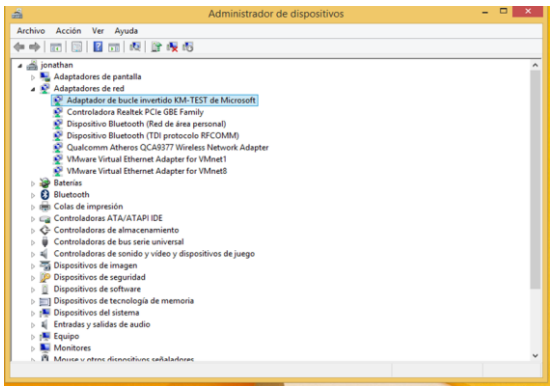



Figura 27. Interfaz de Loopback (Paso 7)

### 5.2.2.2. Configuración de Servidores

- VMware Player: esta herramienta de virtualización permitirá la optimización del hardware.
- GNS3 VM: Esta máquina virtual tiene el sistema operativo Ubuntu 14.04.5 LTS y es compatible con KVM (Kernel-Virtual Machine). Esta característica permite el mapeo de recursos hardware como RAM, cantidad de procesadores y memoria ROM para un mejor rendimiento en la simulación de todos los dispositivos de red integrados en la topología.

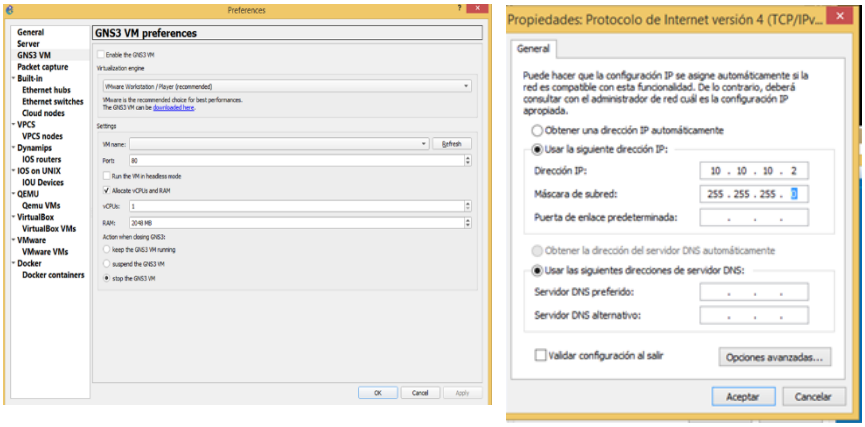



Figura 28. Preferencias de Servidores GNS3

### 5.2.3. Software de virtualización

Los motores de virtualización que utilizamos en esta investigación son:

- VMWARE

#### 5.2.3.1 VMware

Esta herramienta de virtualización nos permite lanzar un plugin para mejorar el rendimiento del hardware.

Desde las opciones de GNS3 en la sección GNS3VM, existe un enlace que nos ayudará a descargar esta herramienta de virtualización lista para ser instalada en la arquitectura de simulación, como se muestra en la Figura 29.

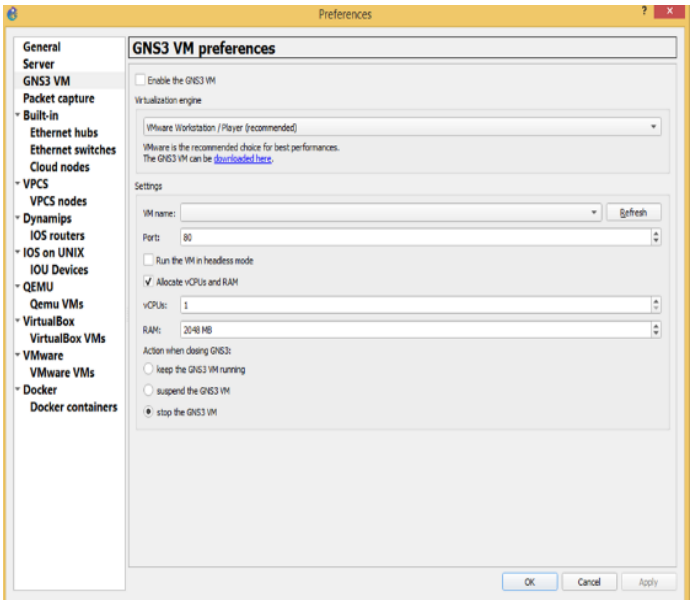



Figura 29. Preferencias de GNS3

El archivo descargado es el siguiente:

- GNS3 VM.ova

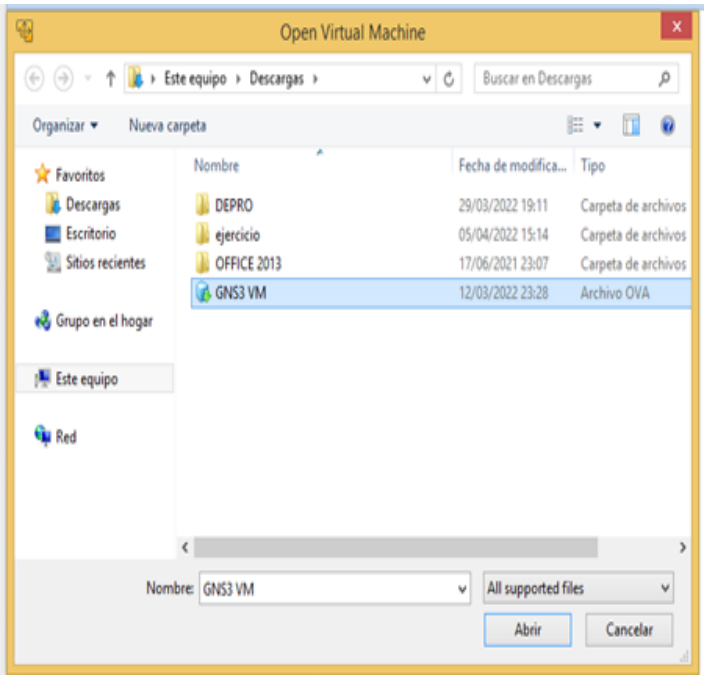



Figura 30. Archivo de GNS3 VM

Este archivo lo importamos en VMware y realizaremos lo siguiente:

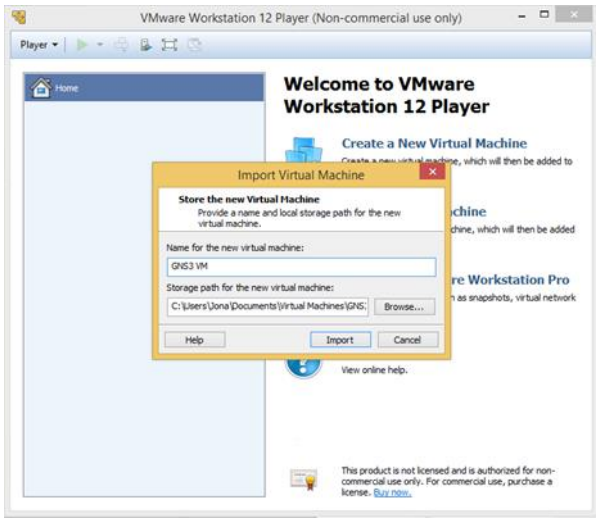



Figura 31. Importación de GNS3 VM en VMware

Solo damos en Siguiente y automáticamente se instala GNS3 VM en VMware.

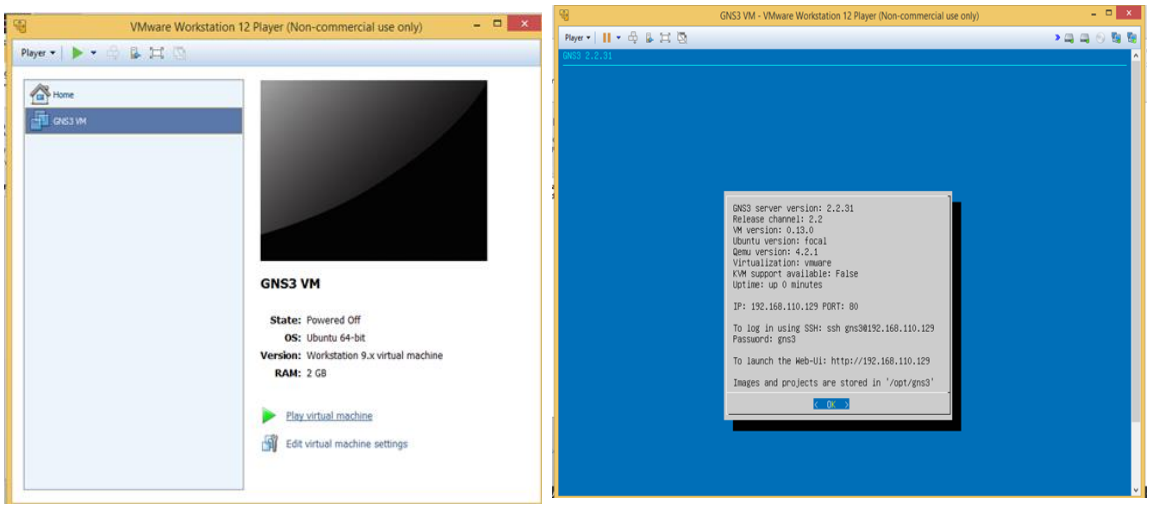



Figura 32. Interfaz de VM en VMware

## 5.2. Fase2: Diseño Lógico

### 5.2.1. Topología de Red

El caso de prueba para evaluar el rendimiento de la tecnología EVPN/VPLS incluye enrutadores que admiten VPN de capa 2 y permiten la convergencia de MPLS, BGP y protocolos de enrutamiento de información de acceso como LDP. y OSPF y RSVP.

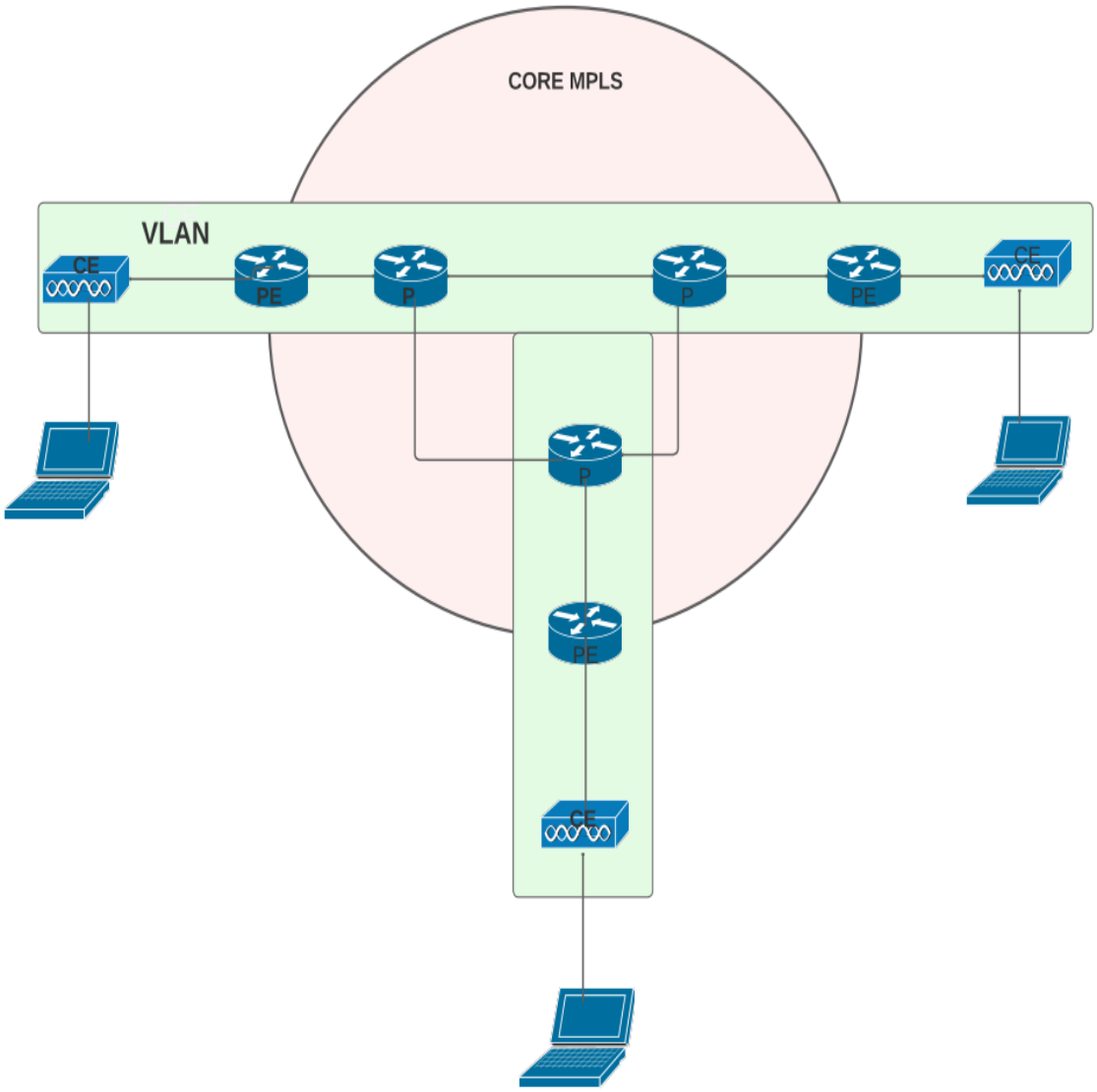



Figura 33. Topología de Red

Para este proyecto de investigación, la estructura que se muestra en la figura 33, se cuenta con tres routers que forman un anillo los cuales a su vez forman parte del core de la red MPLS conocido como el Router Provisionado (P.), además de formar parte otros tres routers del core PE Provider Edge, que se denomina enrutador de borde, es responsable de todas las tecnologías que hacen posible el acceso de extremo a extremo.

Los enrutadores de borde solo intercambian información de accesibilidad a través de BGP, por lo que se requieren dispositivos de acceso para conectarse a los clientes finales, y estos dispositivos se denominan "Customer Edge (CE)". Este dispositivo no necesita un diseño de VPNs y solo funciona en base a VLANs. La siguiente tabla muestra el enrutador y su función en la topología.

Tabla 3. Papel de los Routers

| Router | Función |
|---|---|
| CE | Acceso |
| PE | Router de Borde |
| P | Core |

### 5.2.2. Direccionamiento Lógico

El direccionamiento lógico será el mismo para ambas tecnologías VPN en la red central, excepto por los cambios de direccionamiento lógico a nivel de acceso, que se detallan en las siguientes secciones.

### 5.2.3 Direccionamiento lógico VPLS

El direccionamiento lógico de la tecnología VPLS es la siguiente:

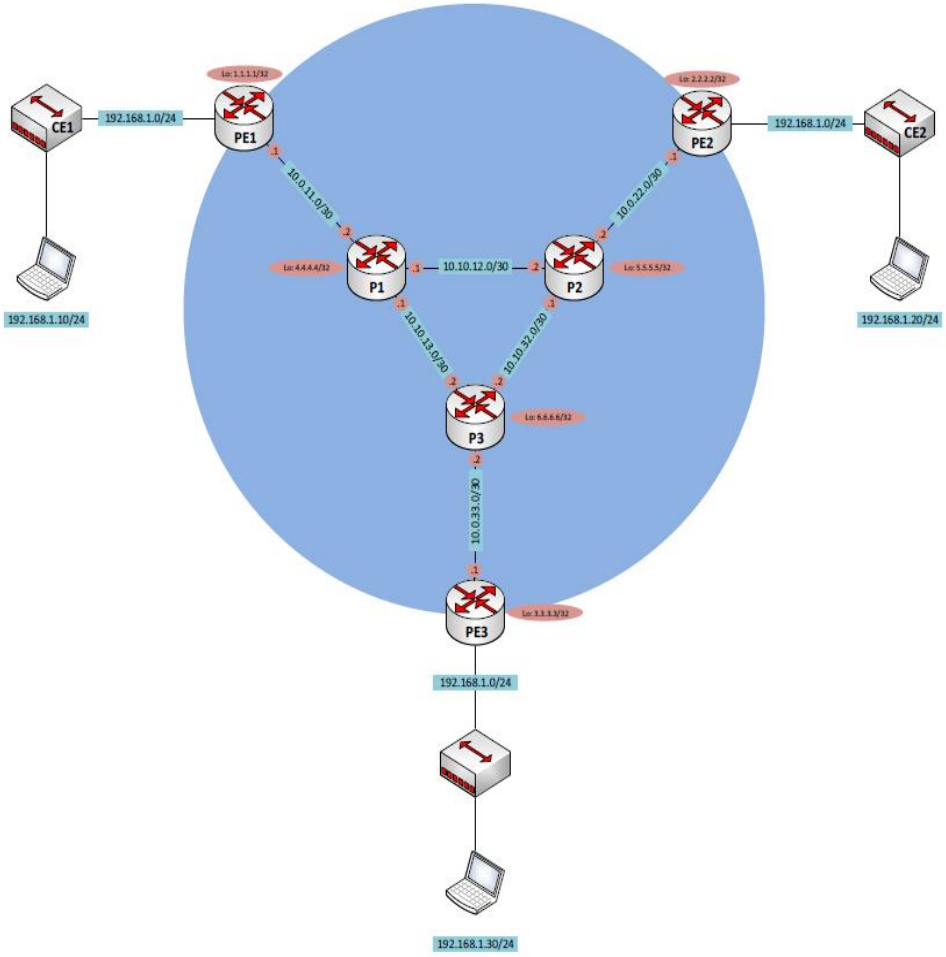



Figura 34. Direccionamiento lógico VPLS

### 5.2.3. Direccionamiento lógico EVPN

El direccionamiento lógico de la tecnología EVPN es la siguiente:


Figura 35. Direccionamiento lógico EVPN

## 5.3. Fase 3: Diseño Físico

### 5.3.1. Direccionamiento Físico VPLS

La nomenclatura de asignación de interfaz de red, para esto y con la ayuda de la simulación de algunos escenarios, se determinó que el modelo Qemu generado debería tener un número de cinco interfaces; La disposición y nomenclatura de las interfaces de red es como se muestra en la Tabla 4:

Tabla 4. Asignación de interfaces

| Interfaz Física | Interfaz Lógica |
|---|---|
| e0/0 | N/A |
| e1/0 | N/A |
| e2/0 | ge0/0/0 |
| e3/0 | ge/0/0/1 |
| e4/0 | ge0/0/2 |

Dado de la tabla 3, el prototipo físico para el escenario en el que se evaluará la tecnología VPLS es la siguiente:

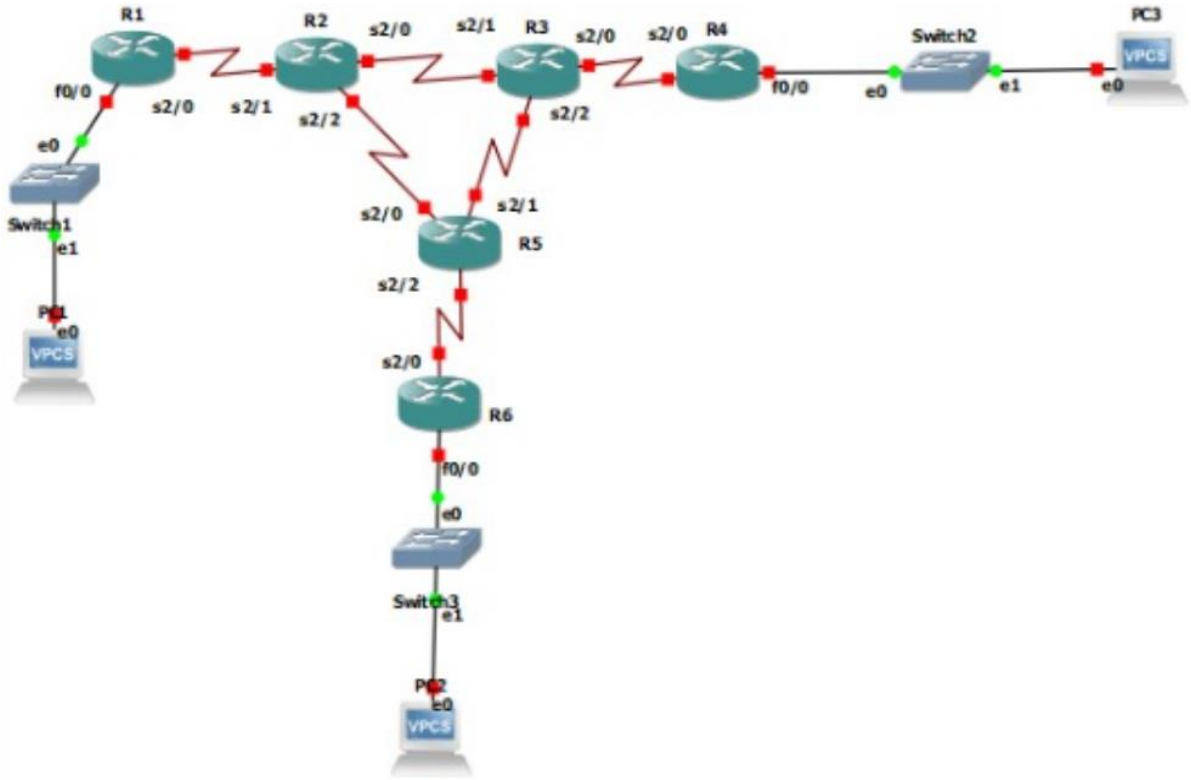



Figura 36. Direccionamiento Físico VPLS

### 5.3.2. Direccionamiento Físico EVPN

El prototipo físico para el escenario en el que se evaluará la tecnología EVPN es la siguiente:

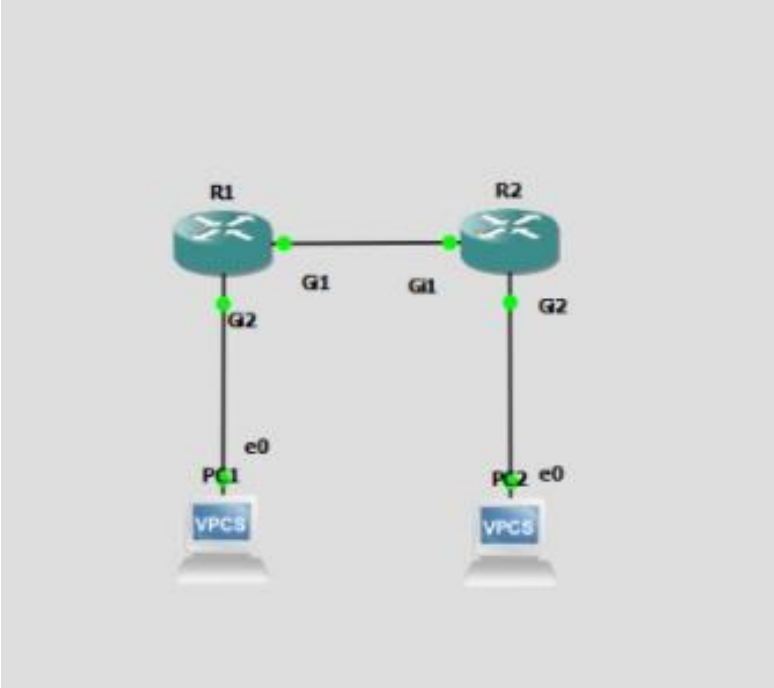



Figura 37. Direccionamiento Físico EVPN

### 5.4. Pruebas, Optimización y Documentación de la red

La topología está diseñada para ejecutar tres escenarios de pruebas, y el mismo escenario determina qué tecnología funciona mejor según estos parámetros:

- Convergencia de la red total
- Aprendizaje Mac
- Supresión de tráfico BUM

#### 5.4.1. Convergencia de la red total

Una vez configurada la red, existe una conexión de extremo a extremo PE1, PE2.PE3 por direccionamiento físico como se muestra en la Figura 36 para VPLS/EVPN. El cliente final se configura según la siguiente tabla para verificar la conexión.

Tabla 5. Configuración de red de los clientes finales

| | VPLS | EVPN |
|---|---|---|
| PC-1 | 192.168.1.10/24 | 10.40.40.1/24 |
| PC-2 | 192.168.1.20/24 | 10.40.40.2/24 |

| | | |
|---|---|---|
| PC-3 | 192.168.1.30/24 | |

Las comunicaciones entre clientes se muestran en las siguientes figuras utilizando la herramienta PING con el siguiente comando para VPLS:

- PC-1 ping PC-2
- PC-1 ping PC-3
- PC-2 ping PC-1
- PC-2 ping PC-3
- PC-3 ping PC-1
- PC-2 ping PC-2

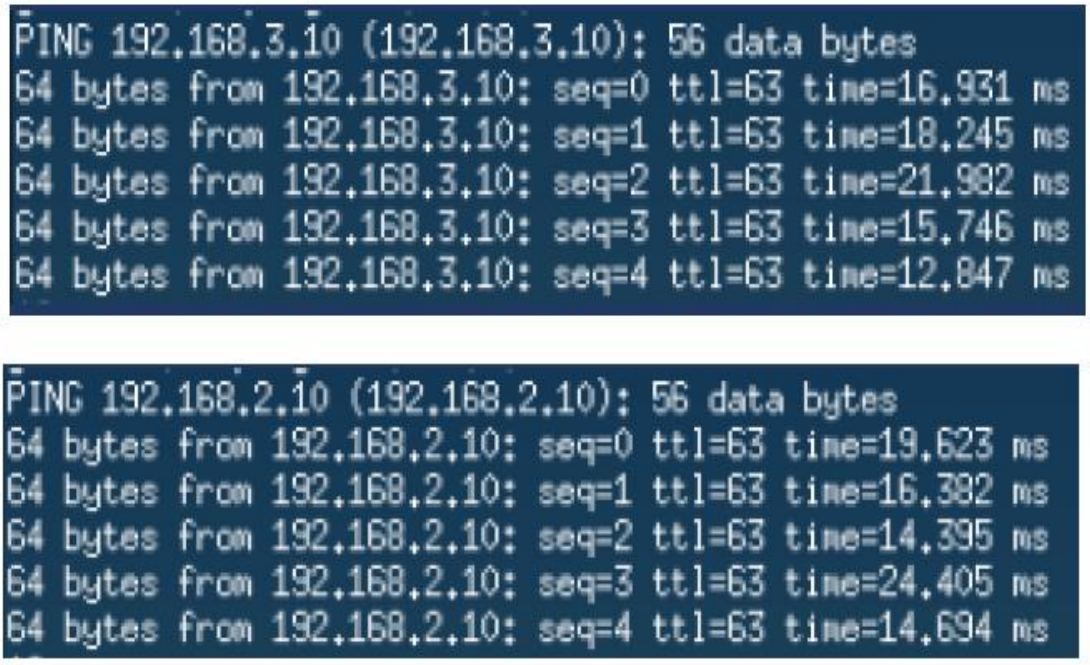



Figura 38. Conectividad Ping PC-1 a PC-2 y PC-3

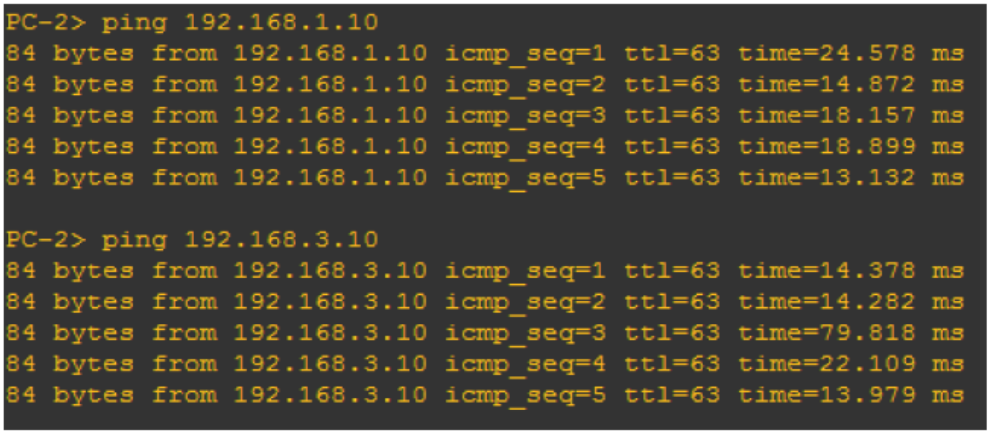



Figura 39. Conectividad Ping PC-2 a PC-3 y PC-1

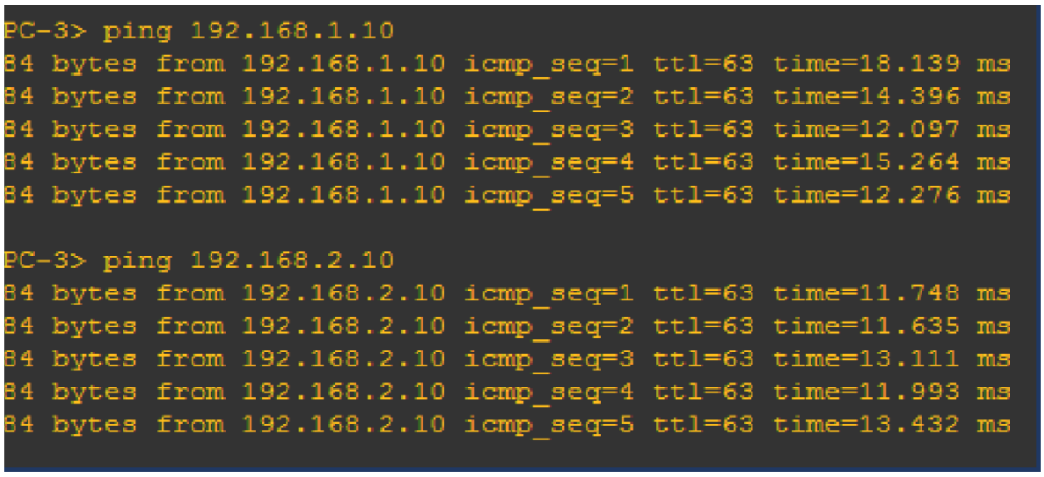



Figura 40. Conectividad Ping PC-2 a PC-1 y PC-3

Las comunicaciones entre clientes se muestran en las siguientes figuras utilizando la herramienta PING con el siguiente comando para EVPN:

- PC-1 ping PC-2
- PC-2 ping PC-1

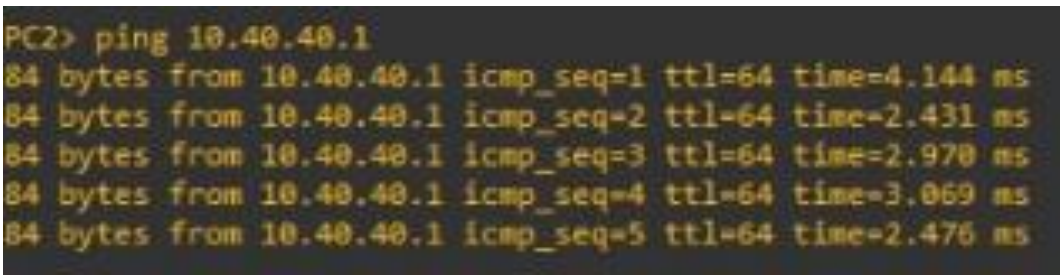



Figura 41. Conectividad Ping PC-2 a PC- 1

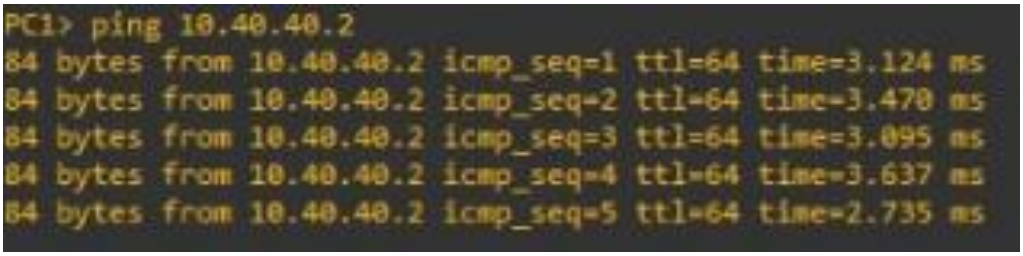



Figura 42. Conectividad Ping PC-1 a PC-2

La información de accesibilidad es completamente transparente desde el punto de vista del cliente, lo que se evidencia creando un rastreo de un cliente a otro utilizando la siguiente guía, con la ayuda de la herramienta tracerauter para VPLS.

- PC-1 tracert PC-2
- PC-1 tracert PC-3
- PC-2 tracert PC-1
- PC-2 tracert PC-3
- PC-3 tracert PC-1
- PC-3 tracert PC-1

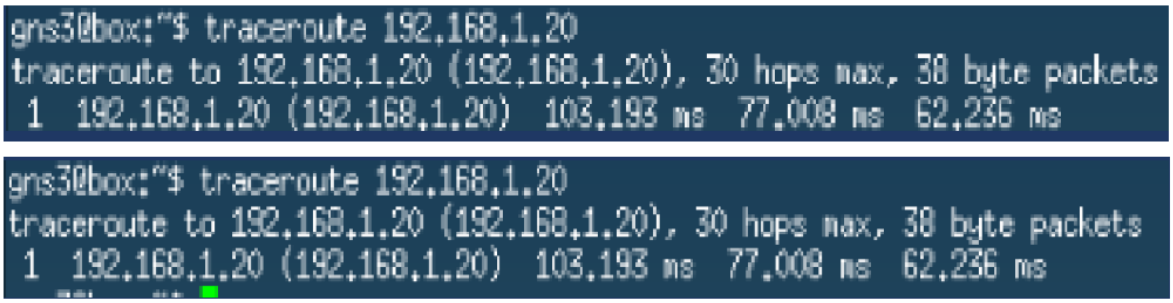



Figura 43. Trazado PC-1 a PC-2 y PC-3

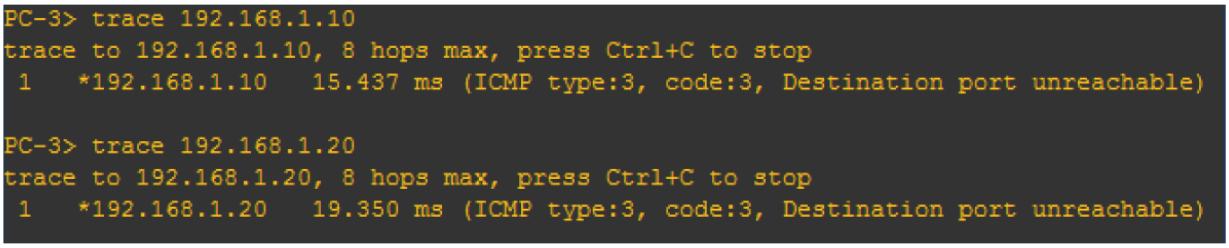



Figura 44. Trazado PC-2 a PC-1 y PC-3

```
PC-2> trace 192.168.1.10
trace to 192.168.1.10, 8 hops max, press Ctrl+C to stop
 1   *192.168.1.10   25.630 ms (ICMP type:3, code:3, Destination port unreachable)

PC-2> trace 192.168.1.30
trace to 192.168.1.30, 8 hops max, press Ctrl+C to stop
 1   *192.168.1.30   41.571 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figura 45. Trazado PC-3 a PC-1 y PC-3

La información de accesibilidad es completamente transparente desde el punto de vista del cliente, lo que se evidencia creando un rastreo de un cliente a otro utilizando la siguiente guía, con la ayuda de la herramienta tracerauter para EVPN.

- PC-1 tracert PC-2
- PC-2 tracert PC-1

```
PC1> trace 10.40.40.2
trace to 10.40.40.2, 8 hops max, press Ctrl+C to stop
 1   *10.40.40.2   2.324 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figura 46. Trazado PC-1 a PC-2

```
PC2> trace 10.40.40.1
trace to 10.40.40.1, 8 hops max, press Ctrl+C to stop
 1   *10.40.40.1   5.806 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figura 47. Trazado PC-2 a PC-

### 5.4.2. Movilidad MAC

El caso de prueba para VPLS y EVPN es el siguiente:

Comenzará con tres clientes PC-3, PC-4 y PC-5, en CE y PE respectivamente.

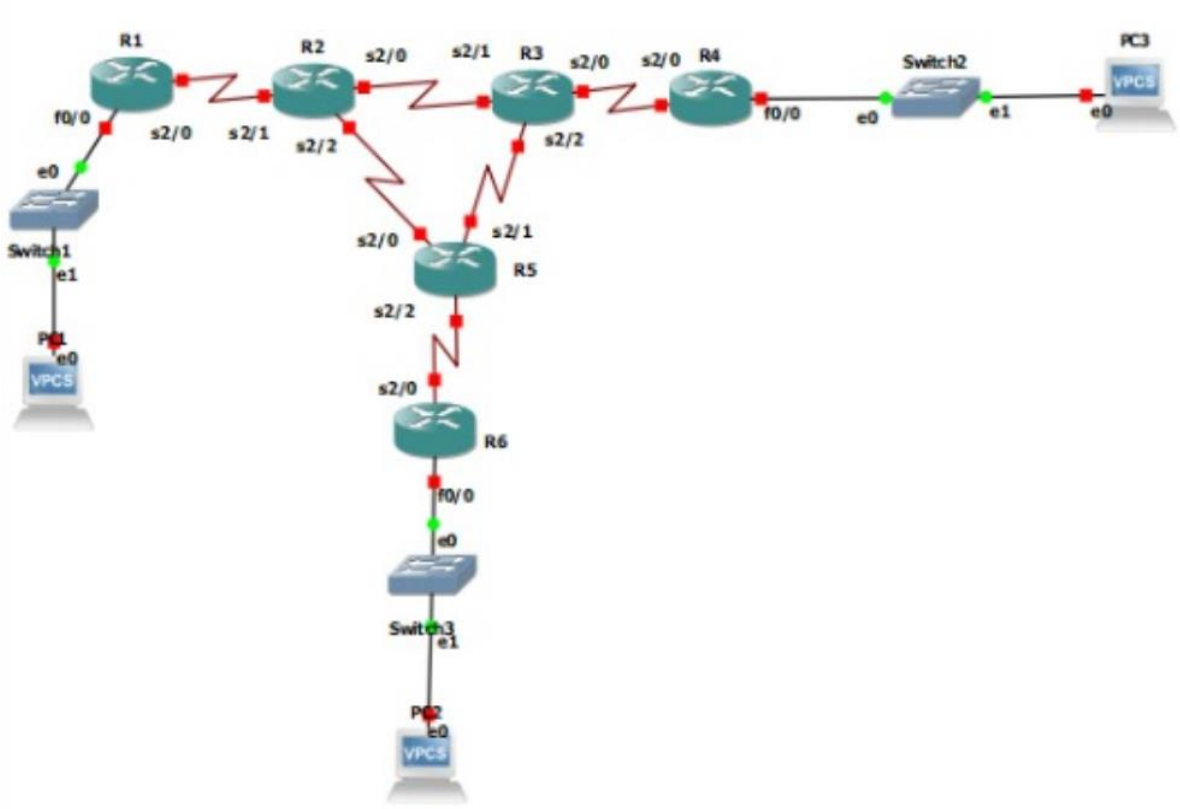



Figura 48. Escenario de Pruebas de Movilidad

Para verificar si la migración MAC ocurre o no en VPLS/EVPN, la PC-1 se desconectará y la PC-2 se moverá a CE1, dejando a CE2 sin una PC, como se muestra.

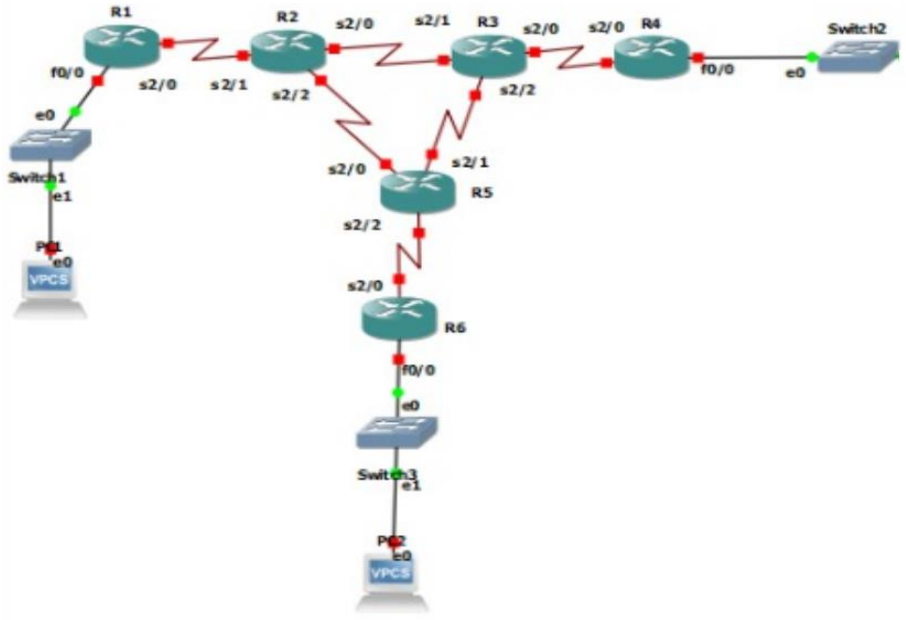



Figura 49. Movilidad MAC

#### 5.4.2.1 EVPN

La dirección MAC de cada PC se ha asignado a cada PE, por lo que tenemos:

- PC-1 00:50:79: 66:68:01
- PC-2 00:50:79: 66:68:00

```
root@R1-PE1> show evpn mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : evpna
 Bridging domain : __evpna__, VLAN : 10
   MAC                 MAC      Logical          NH     RTR
   address             flags    interface        Index  ID
   00:50:79:66:68:00   DC
   00:50:79:66:68:01   D        ge-0/0/0.0
   00:50:79:66:68:02   DC
   c0:01:06:91:f1:00   DC
   c0:03:08:a5:00:00   DC

root@R2-PE2> show evpn mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : evpna
 Bridging domain : __evpna__, VLAN : 10
   MAC                 MAC      Logical          NH     RTR
   address             flags    interface        Index  ID
   00:50:79:66:68:00   D        ge-0/0/0.0
   00:50:79:66:68:01   DC
   00:50:79:66:68:02   DC
   c0:01:06:91:f1:00   D        ge-0/0/0.0
   c0:03:08:a5:00:00   DC
```

Figura 50. Tabla-MAC EVPN

Una vez que se determina la dirección MAC, volvemos a colocar la PC 2 y tomamos los paquetes con Wireshark snnifer en el enlace entre PE1-P1, y obtenemos los siguientes resultados:

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 50 | 02:47:01,535151 | 2.2.2.2 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 68 | 02:47:12,125088 | 3.3.3.3 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 95 | 02:47:26,720220 | 1.1.1.1 | 2.2.2.2 | BGP | 85 | KEEPALIVE Message |
| 96 | 02:47:26,721211 | 1.1.1.1 | 3.3.3.3 | BGP | 85 | KEEPALIVE Message |
| 104 | 02:47:29,608664 | 2.2.2.2 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 123 | 02:47:37,276944 | 3.3.3.3 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 158 | 02:47:55,260790 | 1.1.1.1 | 2.2.2.2 | BGP | 85 | KEEPALIVE Message |
| 159 | 02:47:55,262989 | 1.1.1.1 | 3.3.3.3 | BGP | 85 | KEEPALIVE Message |
| 164 | 02:47:56,834972 | 2.2.2.2 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 181 | 02:48:02,313313 | 3.3.3.3 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 214 | 02:48:22,380076 | 1.1.1.1 | 2.2.2.2 | BGP | 85 | KEEPALIVE Message |
| 218 | 02:48:22,719175 | 1.1.1.1 | 3.3.3.3 | BGP | 85 | KEEPALIVE Message |
| 231 | 02:48:27,455135 | 2.2.2.2 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 237 | 02:48:29,993329 | 3.3.3.3 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 248 | 02:48:33,679724 | 2.2.2.2 | 1.1.1.1 | BGP | 162 | UPDATE Message |
| 250 | 02:48:33,797630 | 2.2.2.2 | 1.1.1.1 | BGP | 251 | UPDATE Message, UPDATE Message |
| 270 | 02:48:38,501764 | 1.1.1.1 | 2.2.2.2 | BGP | 135 | UPDATE Message |
| 271 | 02:48:38,506799 | 1.1.1.1 | 3.3.3.3 | BGP | 135 | UPDATE Message |
| 275 | 02:48:38,638074 | 1.1.1.1 | 2.2.2.2 | BGP | 177 | UPDATE Message, UPDATE Message |
| 278 | 02:48:38,759554 | 1.1.1.1 | 3.3.3.3 | BGP | 177 | UPDATE Message, UPDATE Message |
| 294 | 02:48:46,750959 | 1.1.1.1 | 2.2.2.2 | BGP | 85 | KEEPALIVE Message |
| 305 | 02:48:51,689028 | 1.1.1.1 | 3.3.3.3 | BGP | 85 | KEEPALIVE Message |
| 309 | 02:48:54,268356 | 2.2.2.2 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 317 | 02:48:54,740615 | 3.3.3.3 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 351 | 02:49:15,667453 | 1.1.1.1 | 2.2.2.2 | BGP | 85 | KEEPALIVE Message |
| 359 | 02:49:19,692202 | 3.3.3.3 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |
| 361 | 02:49:20,482841 | 1.1.1.1 | 3.3.3.3 | BGP | 85 | KEEPALIVE Message |
| 365 | 02:49:21,082984 | 2.2.2.2 | 1.1.1.1 | BGP | 85 | KEEPALIVE Message |

Figura 51. Capturas de Paquetes enlace PE1-P1

La Figura 46 ilustra el proceso de captura de paquetes donde la señalización se realiza antes, durante y después de la transferencia PC-2. Así tenemos en los paquetes del 50 al 237 no se realiza la transferencia, y en los paquetes del 248 al 278 se transfiere PC-2 y del paquete 294 se ensambla el capacitor de transferencia. Esta actualización está encapsulada en los mensajes de ACTUALIZACIÓN que se muestran en la Figura 47. En este contexto, se procede a descifrar el mensaje de ACTUALIZACIÓN, para comprobar la portabilidad de la MAC.

Este mensaje se envía de PE1 a PE2 indicando la dirección MAC que tenía incluso antes de mover la computadora, y el NLRI contiene la información del enrutador privado PE2 cuya dirección MAC se indica.

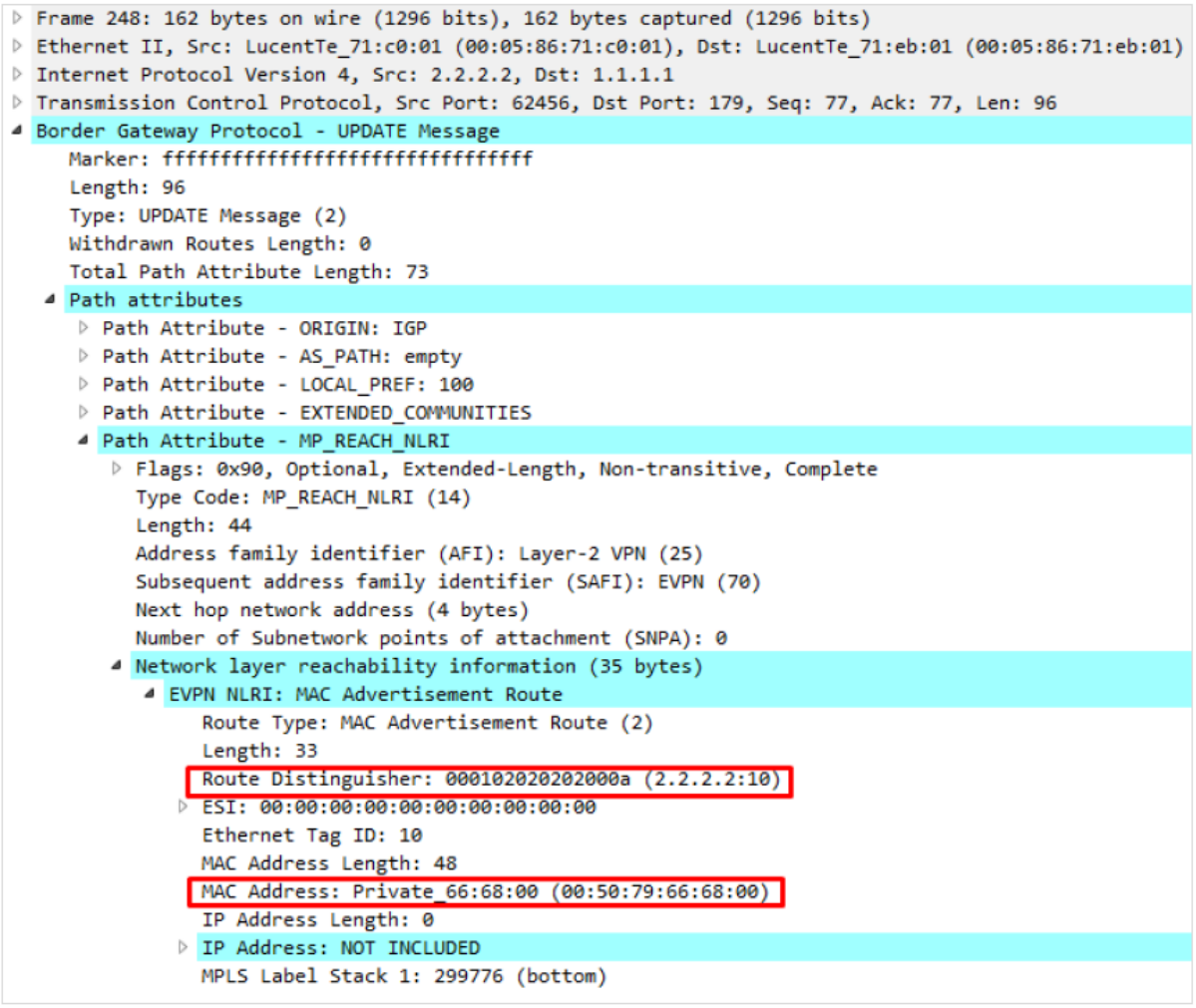



Figura 52. Mensaje de Actualización 162

En este mensaje se agrega información sobre la dirección IP que posee el PC reubicado, esta información es para el aprendizaje MAC no es de mucha utilidad informativo.

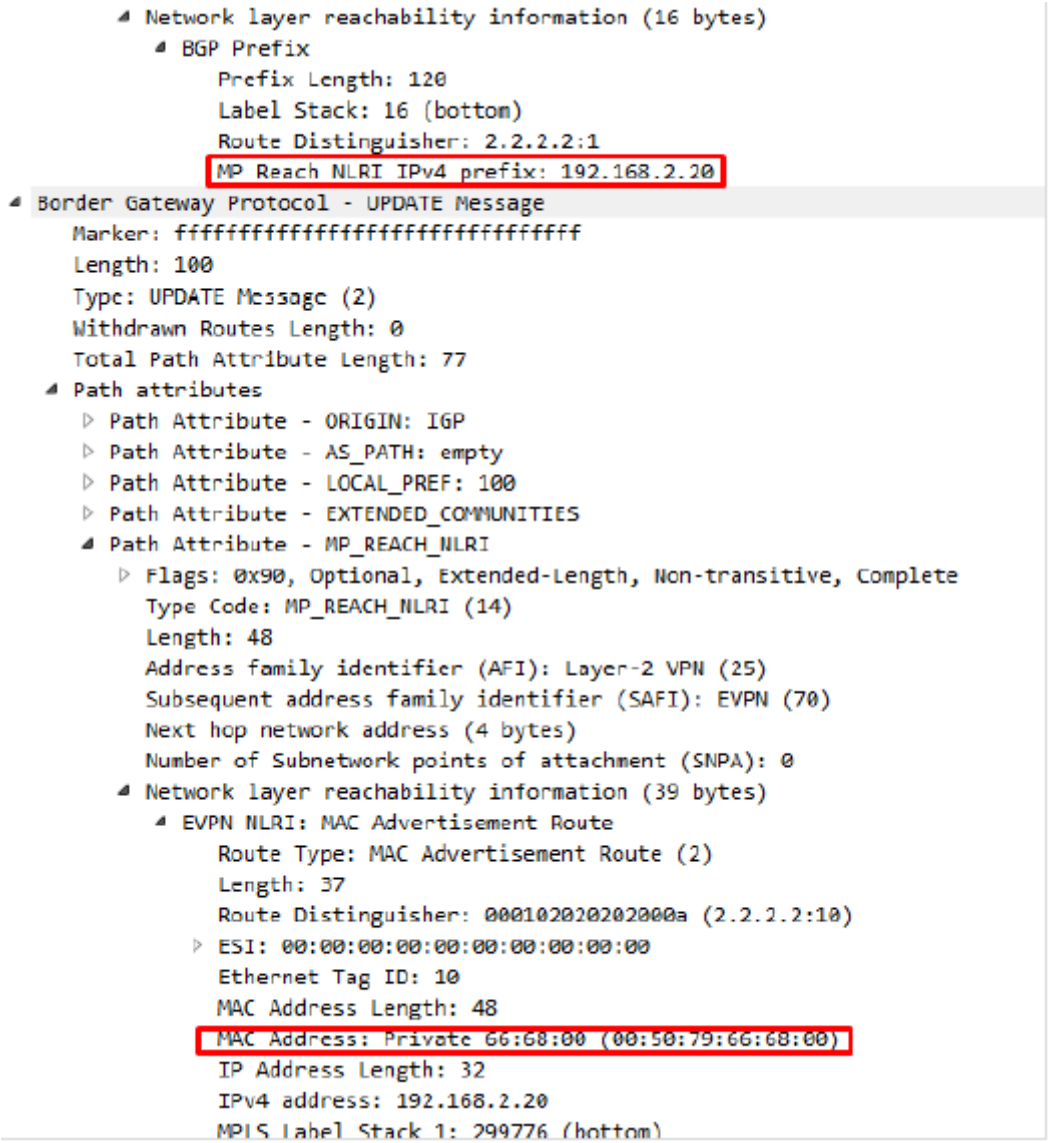



Figura 53. Mensaje Actualización 251

En este mensaje, la dirección MAC se registra en el enrutador PE1 y se envía a los enrutadores PE2 y PE1 para que se actualicen las tablas MAC respectivas.

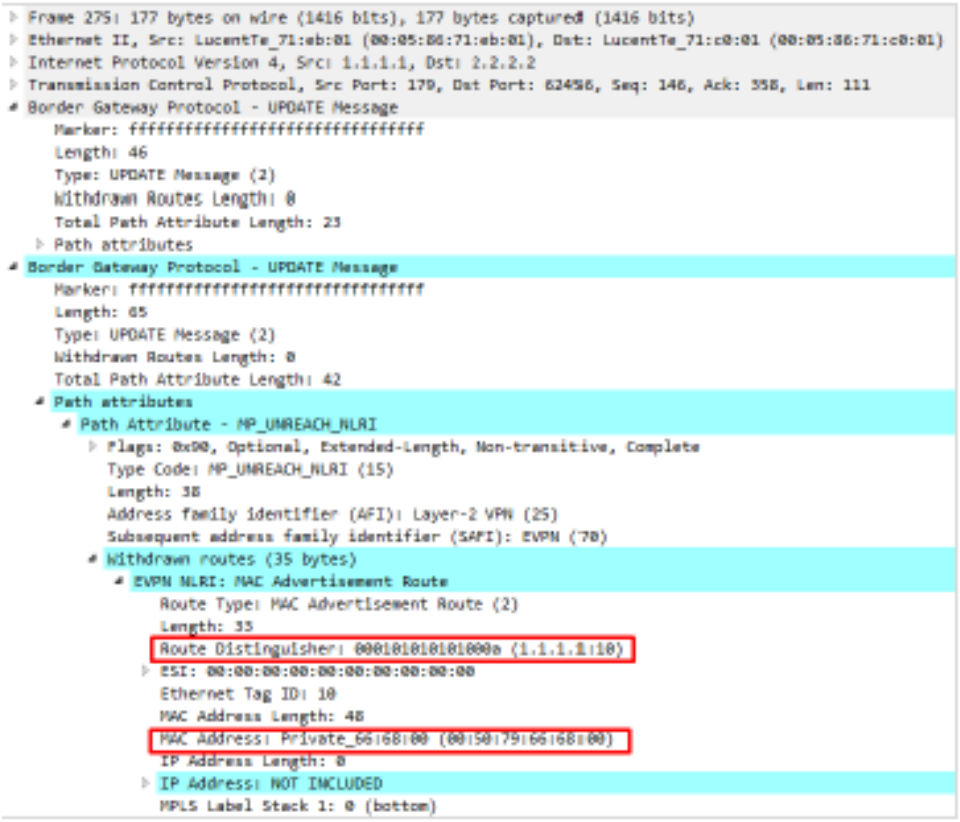



Figura 54. Mensaje de Update 177

Por lo tanto, EVPN respeta la actualización de las tablas de MAC desde el momento en que cambias el terminal de una CE a otra. Los resultados de esta operación realizada por EVPN a través del intercambio NLRI se reflejan en las tablas MAC de EVPN.

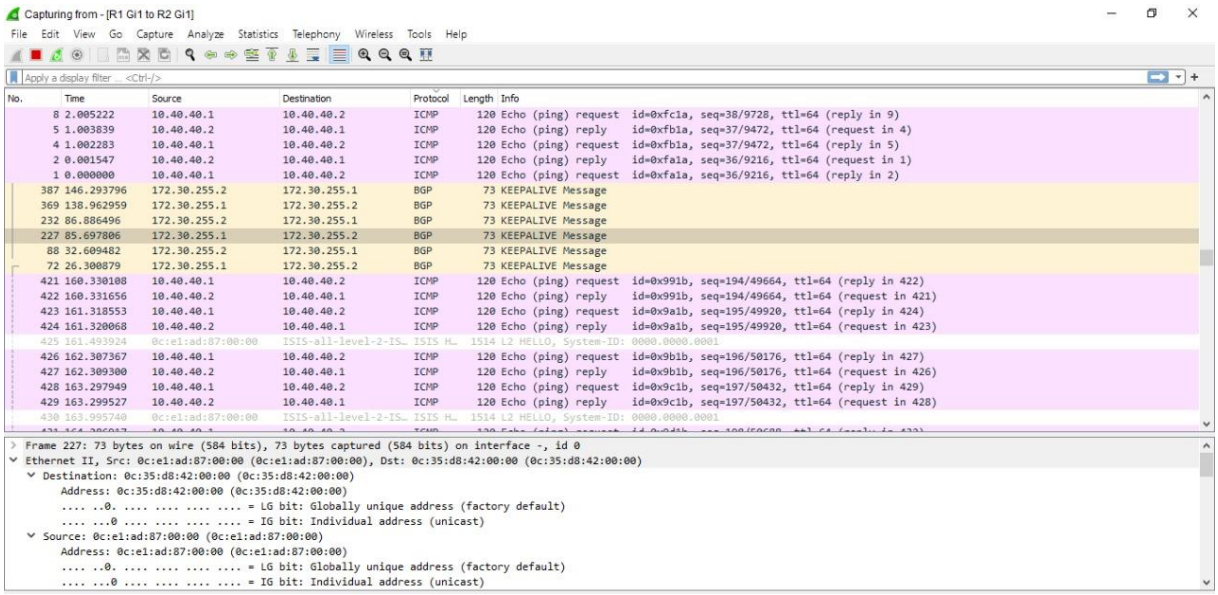



Figura 55. Mensaje Update 177 V2

Este proceso indica que el enrutador PE3 sabe exactamente a qué enrutador de borde enviar paquetes porque su programación se ha actualizado, es decir, la PC-3 puede enviar paquetes a la PC-2 sin perderla ni perder su conexión, gracias al aprendizaje de MAC.

#### 5.4.2.2 VPLS

La dirección MAC de cada PC se especifica en cada PE, por lo que tenemos:

- PC-1 00:50:79: 66:68:01
- PC-2 00:50:79: 66:68:00
- PC-3 00:50:79: 66:68:02

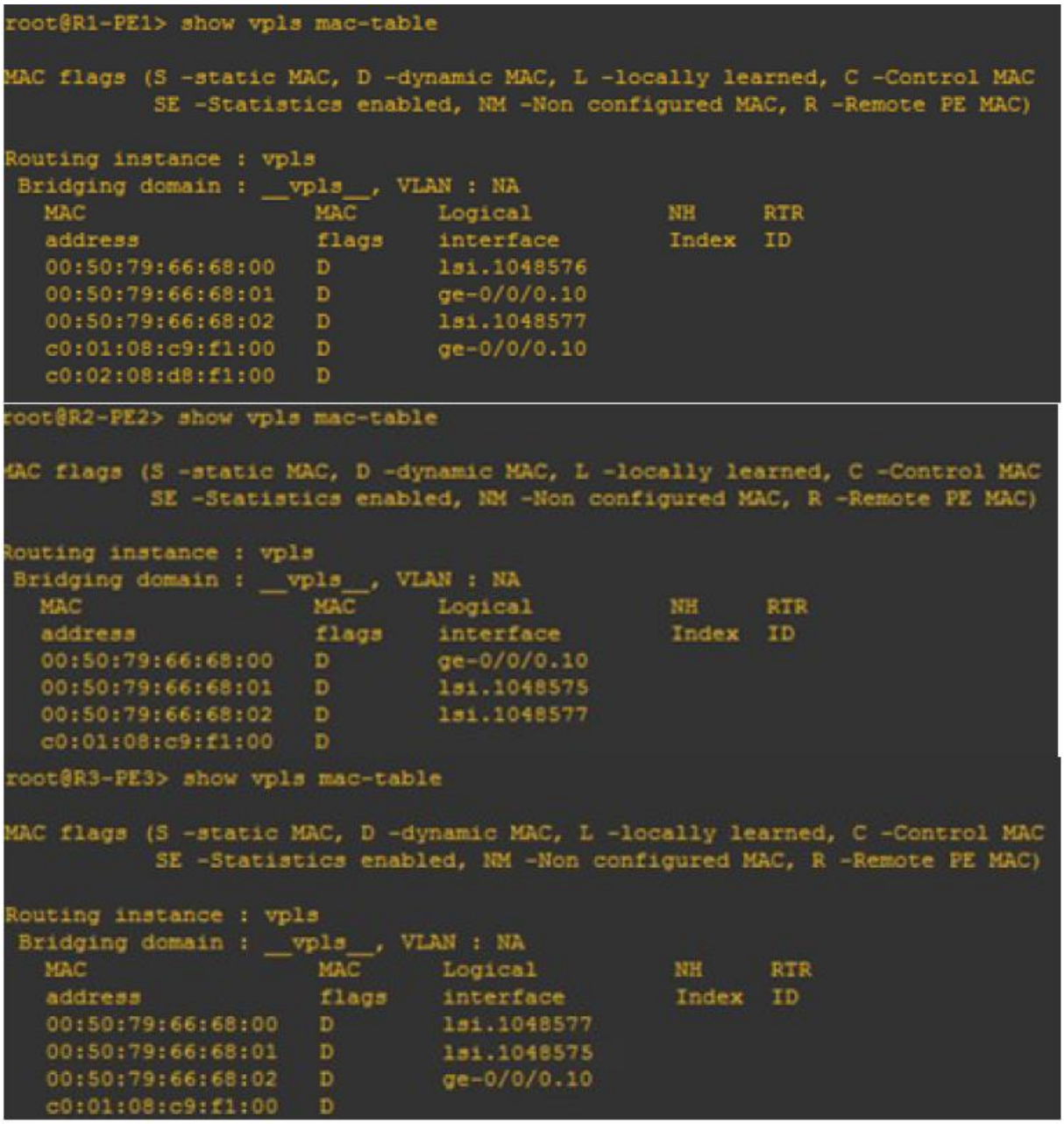



Figura 56. Tabla de MAC VPLS

Después de determinar las direcciones MAC, reubicamos el cliente PC-2 y capturamos los paquetes usando el detector Wireshark en el enlace entre PE1-P1 y obtenemos algunos resultados.

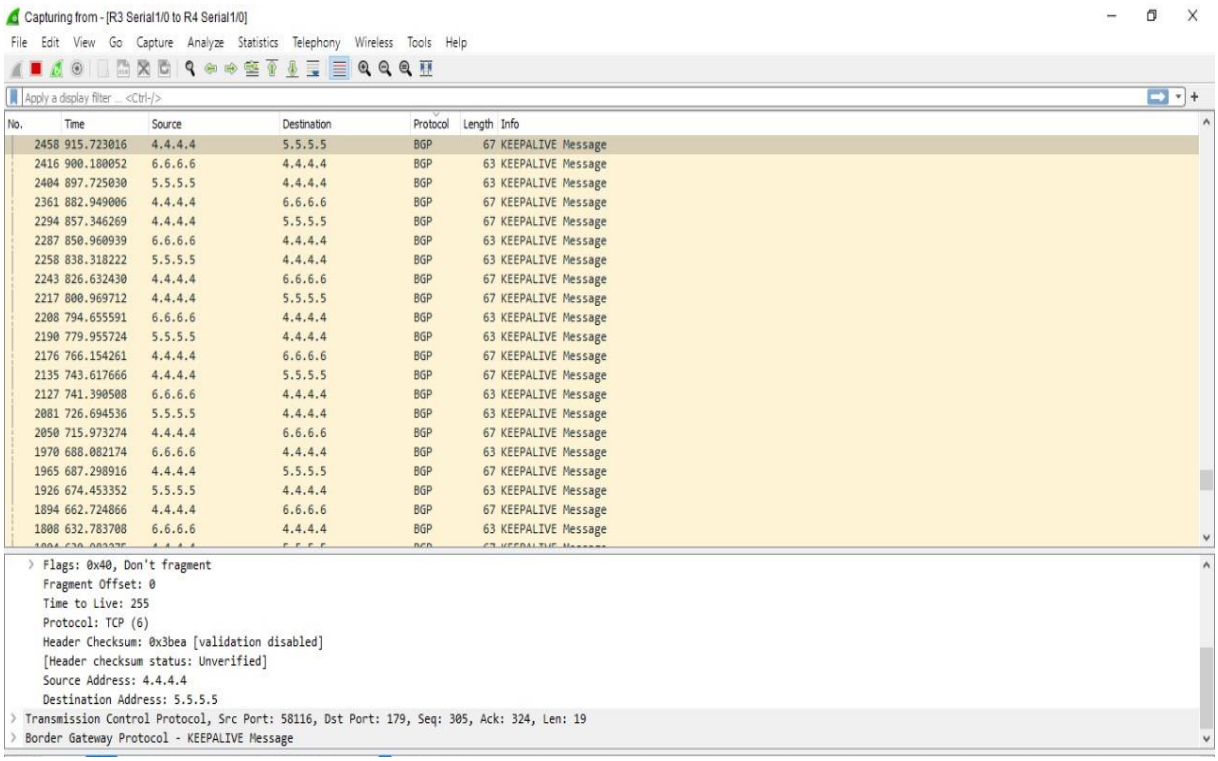



Figura 57. Captura de paquetes enlace PE1-P1

La Figura 52 muestra que no hay ningún tipo de mensaje BGP asociado al aprendizaje de MAC, lo que significa que la tabla MAC no sufrirá ningún tipo de cambio, excepto por dispositivos eliminados de la red como podemos ver a continuación.

```
root@R1-PE1> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : vpls
 Bridging domain : __vpls__, VLAN : NA
   MAC                 MAC      Logical          NH     RTR
   address             flags    interface        Index  ID
   00:50:79:66:68:00   D        ge-0/0/0.10
   00:50:79:66:68:02   D        lsi.1048577
   c0:01:08:c9:f1:00   D        ge-0/0/0.10
root@R2-PE2> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : vpls
 Bridging domain : __vpls__, VLAN : NA
   MAC                 MAC      Logical          NH     RTR
   address             flags    interface        Index  ID
   00:50:79:66:68:00   D        lsi.1048576
   c0:01:08:c9:f1:00   D        lsi.1048576

root@R3-PE3> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : vpls
 Bridging domain : __vpls__, VLAN : NA
   MAC                 MAC      Logical          NH     RTR
   address             flags    interface        Index  ID
   00:50:79:66:68:00   D        lsi.1048576
   00:50:79:66:68:02   D        ge-0/0/0.10
   c0:01:08:c9:f1:00   D        lsi.1048576
```

Figura 58. Tabla MAC VPLS

Después de determinar las direcciones MAC, reubicamos el cliente PC-2 y capturamos los paquetes usando el detector Wireshark en el enlace entre PE1-P1 y obtenemos los siguientes resultados. La Figura 52 muestra que no hay ningún tipo de mensaje BGP asociado al aprendizaje de MAC, lo que significa que la tabla MAC no sufrirá ningún tipo de cambio, excepto por dispositivos eliminados de la red como podemos ver a continuación la tabla MAC.

### 5.4.3 Supresión de Tráfico BUM

Para comprobar el comportamiento de cada tecnología en respuesta a inundaciones de tráfico, el caso de prueba es el siguiente:

En Ostinato, configuramos una nueva transmisión en el puerto 0 ether1 como se muestra;

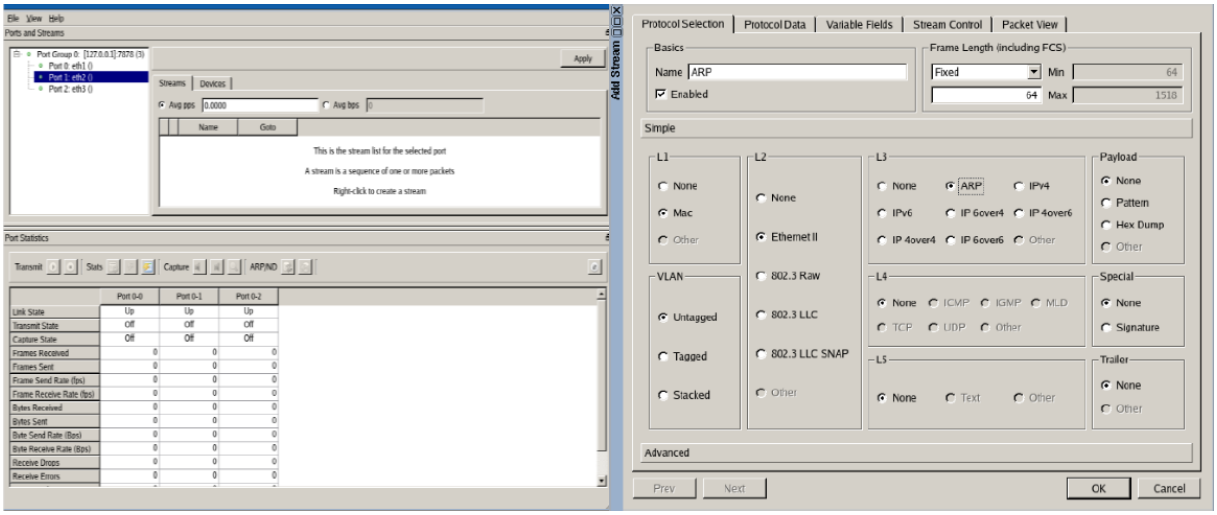



Figura 59. Configuración direcciones MAC e IP

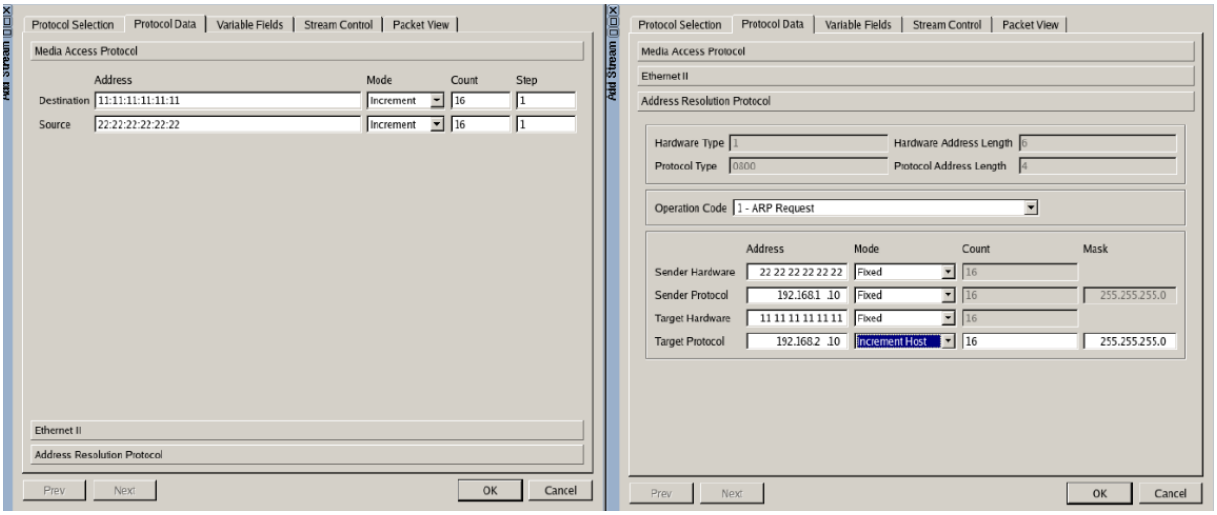



Figura 60. Configuración direcciones MAC e IP

Ahora, con el escenario configurado, el tráfico ARP se inunda dos veces para verificar qué sucede con el aprendizaje de MAC; En un enlace PE1-PE, el tráfico se registra mediante Wireshark.

### 5.4.3.1 EVPN

Durante la primera inundación de tráfico de ARP, se obtuvieron estos resultados:

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 138 | 22:43:29,563568 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.20? Tell 192.168.1.10 |
| 139 | 22:43:30,563939 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.21? Tell 192.168.1.10 |
| 143 | 22:43:31,566624 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.22? Tell 192.168.1.10 |
| 145 | 22:43:32,565444 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.23? Tell 192.168.1.10 |
| 146 | 22:43:33,566713 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.24? Tell 192.168.1.10 |
| 147 | 22:43:34,580873 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.25? Tell 192.168.1.10 |
| 151 | 22:43:35,576509 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.26? Tell 192.168.1.10 |
| 152 | 22:43:36,576804 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.27? Tell 192.168.1.10 |
| 153 | 22:43:37,577436 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.28? Tell 192.168.1.10 |
| 157 | 22:43:38,577686 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.29? Tell 192.168.1.10 |
| 372 | 22:47:23,856368 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.20? Tell 192.168.1.10 |
| 376 | 22:47:24,857224 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.21? Tell 192.168.1.10 |
| 377 | 22:47:25,857343 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.22? Tell 192.168.1.10 |
| 378 | 22:47:26,858372 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.23? Tell 192.168.1.10 |
| 382 | 22:47:27,858211 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.24? Tell 192.168.1.10 |
| 383 | 22:47:28,858128 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.25? Tell 192.168.1.10 |
| 384 | 22:47:29,858716 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.26? Tell 192.168.1.10 |
| 385 | 22:47:30,859036 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.27? Tell 192.168.1.10 |
| 389 | 22:47:31,860008 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.28? Tell 192.168.1.10 |
| 390 | 22:47:32,860254 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.29? Tell 192.168.1.10 |
| 391 | 22:47:33,860668 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.30? Tell 192.168.1.10 |
| 395 | 22:47:34,863837 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.31? Tell 192.168.1.10 |
| 396 | 22:47:35,863565 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.32? Tell 192.168.1.10 |
| 397 | 22:47:36,863947 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.33? Tell 192.168.1.10 |
| 401 | 22:47:37,864649 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.34? Tell 192.168.1.10 |
| 402 | 22:47:38,865470 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.35? Tell 192.168.1.10 |
| 403 | 22:47:39,866474 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.2.20? Tell 192.168.1.10 |

Figura 61. ARP antes

En la segunda inundación se obtiene los siguientes resultados:

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1256 | 22:47:21,408907 | f1:00:81:00:00:0a | cc:cd:c0:01:0a:a4 | STP | 86 | Conf. Root = 32768/0/c0:01:08:46:00:01  Cost = 0  Port = 0x8029 |
| 1259 | 22:47:23,876929 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1260 | 22:47:24,648541 | f1:00:81:00:00:0a | cc:cd:c0:01:0a:a4 | STP | 86 | Conf. Root = 32768/0/c0:01:08:46:00:01  Cost = 0  Port = 0x8029 |
| 1262 | 22:47:24,867822 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1263 | 22:47:25,885889 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1266 | 22:47:26,869680 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1271 | 22:47:27,785095 | f1:00:81:00:00:0a | cc:cd:c0:01:0a:a4 | STP | 86 | Conf. Root = 32768/0/c0:01:08:46:00:01  Cost = 0  Port = 0x8029 |
| 1272 | 22:47:27,872059 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1273 | 22:47:28,873790 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1274 | 22:47:29,866313 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1276 | 22:47:30,872338 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1278 | 22:47:30,946619 | f1:00:81:00:00:0a | cc:cd:c0:01:0a:a4 | STP | 86 | Conf. Root = 32768/0/c0:01:08:46:00:01  Cost = 0  Port = 0x8029 |
| 1281 | 22:47:31,877567 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1283 | 22:47:32,893762 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1284 | 22:47:33,872686 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1285 | 22:47:34,068294 | f1:00:81:00:00:0a | cc:cd:c0:01:0a:a4 | STP | 86 | Conf. Root = 32768/0/c0:01:08:46:00:01  Cost = 0  Port = 0x8029 |
| 1288 | 22:47:34,879415 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1290 | 22:47:35,878217 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1292 | 22:47:36,886777 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1294 | 22:47:37,282781 | f1:00:81:00:00:0a | cc:cd:c0:01:0a:a4 | STP | 86 | Conf. Root = 32768/0/c0:01:08:46:00:01  Cost = 0  Port = 0x8029 |
| 1296 | 22:47:37,886234 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1299 | 22:47:38,880938 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1301 | 22:47:39,884772 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1305 | 22:47:40,475636 | f1:00:81:00:00:0a | cc:cd:c0:01:0a:a4 | STP | 86 | Conf. Root = 32768/0/c0:01:08:46:00:01  Cost = 0  Port = 0x8029 |
| 1306 | 22:47:40,899967 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1307 | 22:47:41,888234 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1308 | 22:47:42,878946 | LucentTe_71:a2:01 | LucentTe_71:33:01 | MPLS | 82 | MPLS Label Switched Packet |
| 1310 | 22:47:43,573133 | f1:00:81:00:00:0a | cc:cd:c0:01:0a:a4 | STP | 86 | Conf. Root = 32768/0/c0:01:08:46:00:01  Cost = 0  Port = 0x8029 |

Figura 62. Inundación ARP después

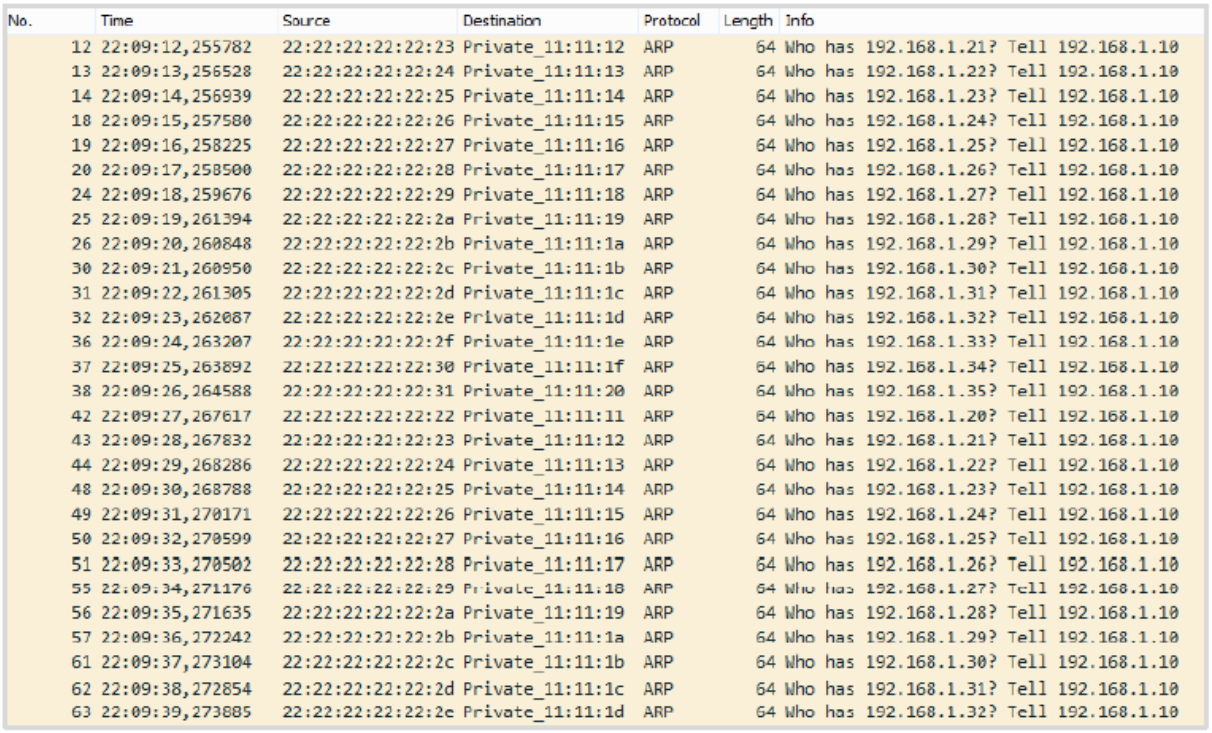
```
root@R1-PE1> show evpn mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : evpna
 Bridging domain : __evpna__, VLAN : 10
   MAC                 MAC      Logical          NH     RTR
   address             flags    interface        Index  ID
   22:22:22:22:22:22   D        ge-0/0/0.0
   22:22:22:22:22:23   D        ge-0/0/0.0
   22:22:22:22:22:24   D        ge-0/0/0.0
   22:22:22:22:22:25   D        ge-0/0/0.0
   22:22:22:22:22:26   D        ge-0/0/0.0
   22:22:22:22:22:27   D        ge-0/0/0.0
   22:22:22:22:22:28   D        ge-0/0/0.0
   22:22:22:22:22:29   D        ge-0/0/0.0
   22:22:22:22:22:2a   D        ge-0/0/0.0
   22:22:22:22:22:2b   D        ge-0/0/0.0
   22:22:22:22:22:2c   D        ge-0/0/0.0
   22:22:22:22:22:2d   D        ge-0/0/0.0
   22:22:22:22:22:2e   D        ge-0/0/0.0
   22:22:22:22:22:2f   D        ge-0/0/0.0
   22:22:22:22:22:30   D        ge-0/0/0.0
   22:22:22:22:22:31   D        ge-0/0/0.0
   c0:01:11:25:f1:00   D        ge-0/0/0.0
   c0:02:11:34:f1:00   DC                        1048578 1048578
```

Figura 63. Tabla EVPN MAC

EVPN opera en un plano de control, lo que significa que aprende el MAC usando MP-BGP y declara las rutas de la Capa 2, como las rutas del servidor MAC/IP que representan a cada cliente. Tenemos que tener en cuenta que cada vez que un router recibe una nueva dirección MAC. La próxima vez que un cliente envié la solicitud del protocolo ARP a la dirección MAC, esta solicitud no genere una inundación a la principal red, el enrutador de bode actuara como servidor proxy para que responda a la solicitud y no genere una inundación. Con su dirección MAC el tráfico BUM ha disminuido en la red EVPN.

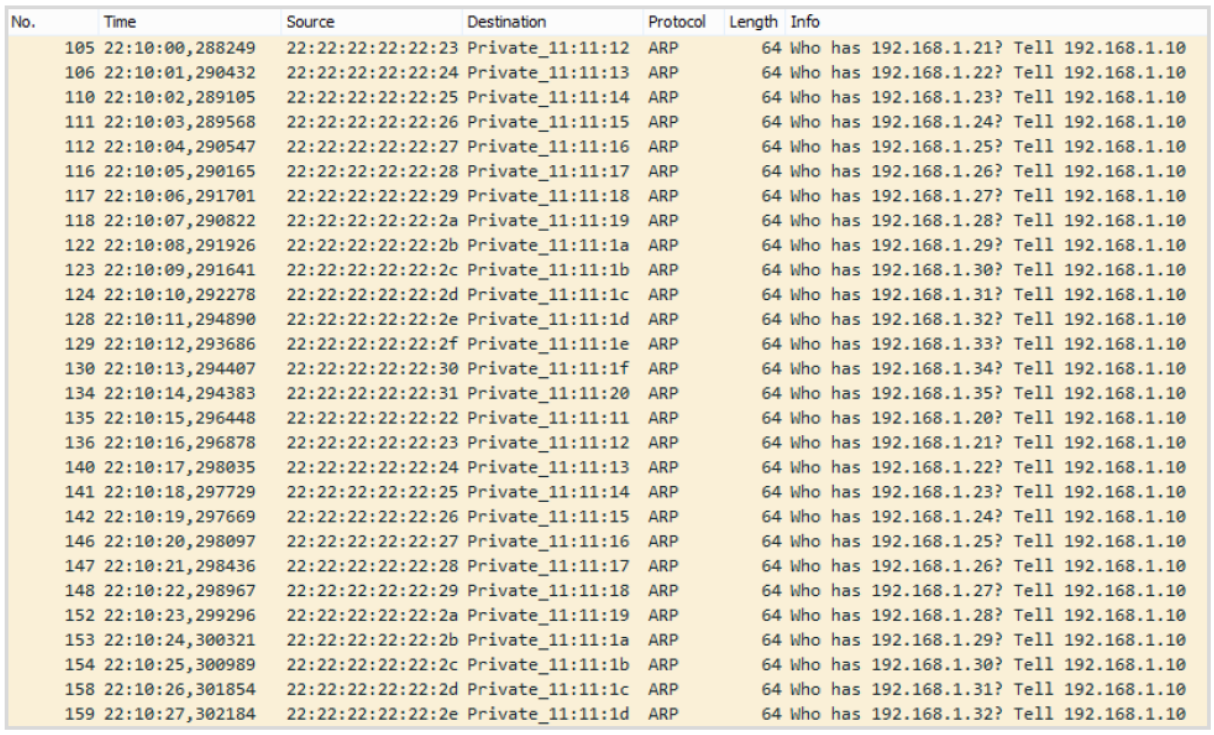
#### 5.4.3.2 VPLS

La primera inundación de tráfico para la tecnología VPLS, se obtuvieron los siguientes resultados:



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 12 | 22:09:12,255782 | 22:22:22:22:22:23 | Private_11:11:12 | ARP | 64 | Who has 192.168.1.21? Tell 192.168.1.10 |
| 13 | 22:09:13,256528 | 22:22:22:22:22:24 | Private_11:11:13 | ARP | 64 | Who has 192.168.1.22? Tell 192.168.1.10 |
| 14 | 22:09:14,256939 | 22:22:22:22:22:25 | Private_11:11:14 | ARP | 64 | Who has 192.168.1.23? Tell 192.168.1.10 |
| 18 | 22:09:15,257580 | 22:22:22:22:22:26 | Private_11:11:15 | ARP | 64 | Who has 192.168.1.24? Tell 192.168.1.10 |
| 19 | 22:09:16,258225 | 22:22:22:22:22:27 | Private_11:11:16 | ARP | 64 | Who has 192.168.1.25? Tell 192.168.1.10 |
| 20 | 22:09:17,258500 | 22:22:22:22:22:28 | Private_11:11:17 | ARP | 64 | Who has 192.168.1.26? Tell 192.168.1.10 |
| 24 | 22:09:18,259676 | 22:22:22:22:22:29 | Private_11:11:18 | ARP | 64 | Who has 192.168.1.27? Tell 192.168.1.10 |
| 25 | 22:09:19,261394 | 22:22:22:22:22:2a | Private_11:11:19 | ARP | 64 | Who has 192.168.1.28? Tell 192.168.1.10 |
| 26 | 22:09:20,260848 | 22:22:22:22:22:2b | Private_11:11:1a | ARP | 64 | Who has 192.168.1.29? Tell 192.168.1.10 |
| 30 | 22:09:21,260950 | 22:22:22:22:22:2c | Private_11:11:1b | ARP | 64 | Who has 192.168.1.30? Tell 192.168.1.10 |
| 31 | 22:09:22,261305 | 22:22:22:22:22:2d | Private_11:11:1c | ARP | 64 | Who has 192.168.1.31? Tell 192.168.1.10 |
| 32 | 22:09:23,262087 | 22:22:22:22:22:2e | Private_11:11:1d | ARP | 64 | Who has 192.168.1.32? Tell 192.168.1.10 |
| 36 | 22:09:24,263207 | 22:22:22:22:22:2f | Private_11:11:1e | ARP | 64 | Who has 192.168.1.33? Tell 192.168.1.10 |
| 37 | 22:09:25,263892 | 22:22:22:22:22:30 | Private_11:11:1f | ARP | 64 | Who has 192.168.1.34? Tell 192.168.1.10 |
| 38 | 22:09:26,264588 | 22:22:22:22:22:31 | Private_11:11:20 | ARP | 64 | Who has 192.168.1.35? Tell 192.168.1.10 |
| 42 | 22:09:27,267617 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.1.20? Tell 192.168.1.10 |
| 43 | 22:09:28,267832 | 22:22:22:22:22:23 | Private_11:11:12 | ARP | 64 | Who has 192.168.1.21? Tell 192.168.1.10 |
| 44 | 22:09:29,268286 | 22:22:22:22:22:24 | Private_11:11:13 | ARP | 64 | Who has 192.168.1.22? Tell 192.168.1.10 |
| 48 | 22:09:30,268788 | 22:22:22:22:22:25 | Private_11:11:14 | ARP | 64 | Who has 192.168.1.23? Tell 192.168.1.10 |
| 49 | 22:09:31,270171 | 22:22:22:22:22:26 | Private_11:11:15 | ARP | 64 | Who has 192.168.1.24? Tell 192.168.1.10 |
| 50 | 22:09:32,270599 | 22:22:22:22:22:27 | Private_11:11:16 | ARP | 64 | Who has 192.168.1.25? Tell 192.168.1.10 |
| 51 | 22:09:33,270502 | 22:22:22:22:22:28 | Private_11:11:17 | ARP | 64 | Who has 192.168.1.26? Tell 192.168.1.10 |
| 55 | 22:09:34,271176 | 22:22:22:22:22:29 | Private_11:11:18 | ARP | 64 | Who has 192.168.1.27? Tell 192.168.1.10 |
| 56 | 22:09:35,271635 | 22:22:22:22:22:2a | Private_11:11:19 | ARP | 64 | Who has 192.168.1.28? Tell 192.168.1.10 |
| 57 | 22:09:36,272242 | 22:22:22:22:22:2b | Private_11:11:1a | ARP | 64 | Who has 192.168.1.29? Tell 192.168.1.10 |
| 61 | 22:09:37,273104 | 22:22:22:22:22:2c | Private_11:11:1b | ARP | 64 | Who has 192.168.1.30? Tell 192.168.1.10 |
| 62 | 22:09:38,272854 | 22:22:22:22:22:2d | Private_11:11:1c | ARP | 64 | Who has 192.168.1.31? Tell 192.168.1.10 |
| 63 | 22:09:39,273885 | 22:22:22:22:22:2e | Private_11:11:1d | ARP | 64 | Who has 192.168.1.32? Tell 192.168.1.10 |

Figura. 64 inundación ARP antes



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 105 | 22:10:00,288249 | 22:22:22:22:22:23 | Private_11:11:12 | ARP | 64 | Who has 192.168.1.21? Tell 192.168.1.10 |
| 106 | 22:10:01,290432 | 22:22:22:22:22:24 | Private_11:11:13 | ARP | 64 | Who has 192.168.1.22? Tell 192.168.1.10 |
| 110 | 22:10:02,289105 | 22:22:22:22:22:25 | Private_11:11:14 | ARP | 64 | Who has 192.168.1.23? Tell 192.168.1.10 |
| 111 | 22:10:03,289568 | 22:22:22:22:22:26 | Private_11:11:15 | ARP | 64 | Who has 192.168.1.24? Tell 192.168.1.10 |
| 112 | 22:10:04,290547 | 22:22:22:22:22:27 | Private_11:11:16 | ARP | 64 | Who has 192.168.1.25? Tell 192.168.1.10 |
| 116 | 22:10:05,290165 | 22:22:22:22:22:28 | Private_11:11:17 | ARP | 64 | Who has 192.168.1.26? Tell 192.168.1.10 |
| 117 | 22:10:06,291701 | 22:22:22:22:22:29 | Private_11:11:18 | ARP | 64 | Who has 192.168.1.27? Tell 192.168.1.10 |
| 118 | 22:10:07,290822 | 22:22:22:22:22:2a | Private_11:11:19 | ARP | 64 | Who has 192.168.1.28? Tell 192.168.1.10 |
| 122 | 22:10:08,291926 | 22:22:22:22:22:2b | Private_11:11:1a | ARP | 64 | Who has 192.168.1.29? Tell 192.168.1.10 |
| 123 | 22:10:09,291641 | 22:22:22:22:22:2c | Private_11:11:1b | ARP | 64 | Who has 192.168.1.30? Tell 192.168.1.10 |
| 124 | 22:10:10,292278 | 22:22:22:22:22:2d | Private_11:11:1c | ARP | 64 | Who has 192.168.1.31? Tell 192.168.1.10 |
| 128 | 22:10:11,294890 | 22:22:22:22:22:2e | Private_11:11:1d | ARP | 64 | Who has 192.168.1.32? Tell 192.168.1.10 |
| 129 | 22:10:12,293686 | 22:22:22:22:22:2f | Private_11:11:1e | ARP | 64 | Who has 192.168.1.33? Tell 192.168.1.10 |
| 130 | 22:10:13,294407 | 22:22:22:22:22:30 | Private_11:11:1f | ARP | 64 | Who has 192.168.1.34? Tell 192.168.1.10 |
| 134 | 22:10:14,294383 | 22:22:22:22:22:31 | Private_11:11:20 | ARP | 64 | Who has 192.168.1.35? Tell 192.168.1.10 |
| 135 | 22:10:15,296448 | 22:22:22:22:22:22 | Private_11:11:11 | ARP | 64 | Who has 192.168.1.20? Tell 192.168.1.10 |
| 136 | 22:10:16,296878 | 22:22:22:22:22:23 | Private_11:11:12 | ARP | 64 | Who has 192.168.1.21? Tell 192.168.1.10 |
| 140 | 22:10:17,298035 | 22:22:22:22:22:24 | Private_11:11:13 | ARP | 64 | Who has 192.168.1.22? Tell 192.168.1.10 |
| 141 | 22:10:18,297729 | 22:22:22:22:22:25 | Private_11:11:14 | ARP | 64 | Who has 192.168.1.23? Tell 192.168.1.10 |
| 142 | 22:10:19,297669 | 22:22:22:22:22:26 | Private_11:11:15 | ARP | 64 | Who has 192.168.1.24? Tell 192.168.1.10 |
| 146 | 22:10:20,298097 | 22:22:22:22:22:27 | Private_11:11:16 | ARP | 64 | Who has 192.168.1.25? Tell 192.168.1.10 |
| 147 | 22:10:21,298436 | 22:22:22:22:22:28 | Private_11:11:17 | ARP | 64 | Who has 192.168.1.26? Tell 192.168.1.10 |
| 148 | 22:10:22,298967 | 22:22:22:22:22:29 | Private_11:11:18 | ARP | 64 | Who has 192.168.1.27? Tell 192.168.1.10 |
| 152 | 22:10:23,299296 | 22:22:22:22:22:2a | Private_11:11:19 | ARP | 64 | Who has 192.168.1.28? Tell 192.168.1.10 |
| 153 | 22:10:24,300321 | 22:22:22:22:22:2b | Private_11:11:1a | ARP | 64 | Who has 192.168.1.29? Tell 192.168.1.10 |
| 154 | 22:10:25,300989 | 22:22:22:22:22:2c | Private_11:11:1b | ARP | 64 | Who has 192.168.1.30? Tell 192.168.1.10 |
| 158 | 22:10:26,301854 | 22:22:22:22:22:2d | Private_11:11:1c | ARP | 64 | Who has 192.168.1.31? Tell 192.168.1.10 |
| 159 | 22:10:27,302184 | 22:22:22:22:22:2e | Private_11:11:1d | ARP | 64 | Who has 192.168.1.32? Tell 192.168.1.10 |

Figura 65. Inundación ARP después

```
root@R1-PE1> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
          SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : vpls
 Bridging domain : __vpls__, VLAN : NA
   MAC                 MAC      Logical          NH     RTR
   address             flags    interface        Index  ID
   22:22:22:22:22:22   D        ge-0/0/0.10
   22:22:22:22:22:23   D        ge-0/0/0.10
   22:22:22:22:22:24   D        ge-0/0/0.10
   22:22:22:22:22:25   D        ge-0/0/0.10
   22:22:22:22:22:26   D        ge-0/0/0.10
   22:22:22:22:22:27   D        ge-0/0/0.10
   22:22:22:22:22:28   D        ge-0/0/0.10
   22:22:22:22:22:29   D        ge-0/0/0.10
   22:22:22:22:22:2a   D        ge-0/0/0.10
   22:22:22:22:22:2b   D        ge-0/0/0.10
   22:22:22:22:22:2c   D        ge-0/0/0.10
   22:22:22:22:22:2d   D        ge-0/0/0.10
   22:22:22:22:22:2e   D        ge-0/0/0.10
   22:22:22:22:22:2f   D        ge-0/0/0.10
   22:22:22:22:22:30   D        ge-0/0/0.10
   22:22:22:22:22:31   D        ge-0/0/0.10
   c0:01:08:c9:f1:00   D        ge-0/0/0.10
```

Figura 66. Tabla MAC de VPLS

### 5.5. Comparación de resultados de las tecnologías EVPN y VPLS

Con los resultados obtenidos de los tres escenarios de prueba se puedo determinar que la tecnología EVPN es mejor a continuación se observa una pequeña comparación de las dos tecnologías.

Tabla 6. Tabla comparativa de EVPN y VPLS

| Escenarios de Pruebas | VPLS | EVPN |
|---|---|---|
| Convergencia de red total | la tecnología VPLS tarda 44.5 segundos en media para que la red converja. | la tecnología EVPN tarda 7.7 segundos en media para que la red converja. |
| Movilidad MAC | Este escenario de movilidad MAC de la tecnología VPLS al rato que cambiamos de lugar las PCs el Router no actualiza su programación, es decir, la PC-3 no puede enviar paquetes a la PC-2 pierde conexión. | Este escenario de movilidad MAC de la tecnología EVPN puede enviar paquetes al Router porque su programación se ha actualizado, es decir, la PC-3 puede enviar paquetes a la PC-2 sin perderla ni perder su conexión ni perdida de |

| | | |
|---|---|---|
| | | paquetes, gracias al aprendizaje de MAC. |
| Trafico de BUM | Esta tecnología VPLS opera principalmente en el plano de datos, aprende los patrones de transmisión comunes como Unicast y Multicast, por lo que el tráfico BUM que pasa por el núcleo principal de la red es inevitable y se produce una inundación. | EVPN opera en un plano de control, lo que significa que aprende el MAC. La próxima vez que un cliente envié la solicitud del protocolo ARP a la dirección MAC, por lo cual no inunda la red. |

### 5.6. Comparación de resultados de los informes de Expertos

Con los resultados obtenidos del informe de expertos a continuación se observa una pequeña comparación.

Tabla 7. Comparación del informe los expertos

| Indicadores de Evaluación | PhD. Gustavo Rodríguez Bárcenas | MG. Christian Andres Morales Robalino |
|---|---|---|
| **1.** Claridad de la investigación | Obtuvimos una calificación de bueno (4) | Obtuvimos una calificación de bueno (5) |
| **2.** Objetividad de la Investigación | Obtuvimos una calificación de bueno (4) | Obtuvimos una calificación de bueno (5) |
| **3.** Consistencia de la Investigación | Obtuvimos una calificación de bueno (4) | Obtuvimos una calificación de bueno (4) |
| **4.** Coherencia de la Investigación | Obtuvimos una calificación de bueno (4) | Obtuvimos una calificación de bueno (4) |
| **5.** Pertinencia de la Investigación | Dentro de este indicador hay sub indicadores por lo cual sumando obtuvimos una calificación de bueno (19) | Dentro de este indicador hay sub indicadores por lo cual sumando obtuvimos una calificación de bueno (16) |
| SUMA TOTAL | 35 | 34 |

### 5.7. Análisis y Tabulación De La Encuestas

**Pregunta 1.** ¿Usted ha oído hablar de las VPNs?

Tabla 8. Frecuencia y porcentaje de la pregunta 1 de la encuesta realizada

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| Si | 43 | 71.7 |
| No | 17 | 28.3 |
| Total | 60 | 100 |

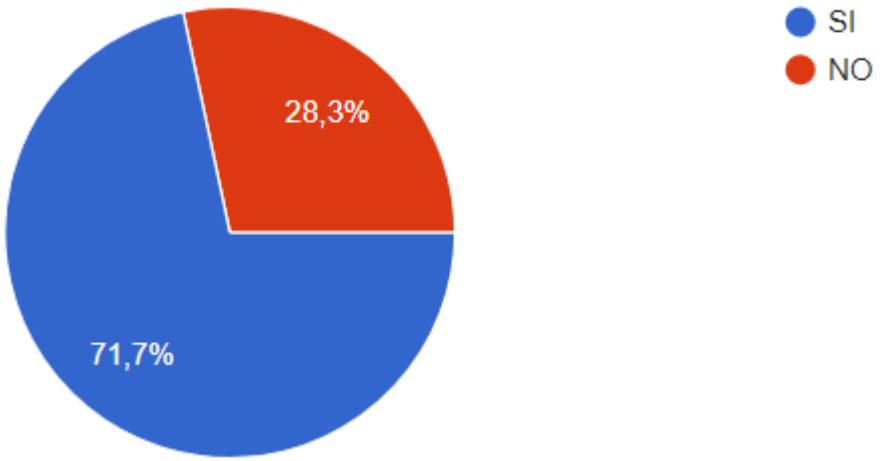



Figura 67. Gráfico del porcentaje de la pregunta 1 de la encuesta realizada

**Fuente:** Grupo Investigativo

**Análisis e Interpretación**

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 28.3% no han oído hablar sobre las VPNs y que un 71.7% tiene un conocimiento sobre las VPNs.

**Conclusión**

Con los resultados obtenidos de la primera pregunta se puede evidenciar que la mayoría de estudiantes de los ciclos sexto, séptimo y octavo de la Universidad Técnica de Cotopaxi conocen la tecnología VPN.

**Pregunta 2.** ¿Para qué usas o usarías una VPN?

Tabla 9. Frecuencia y porcentaje de la pregunta 2 de la encuesta realizada.

| | OPCIONES | PORCENTAJE |
|---|---|---|
| Evitar censuras y bloqueos geográficos de contenido | 5 | 8.3 |
| Esconder mi IP y falsear mi ubicación | 20 | 31.7 |
| Evitar que mi proveedor de Internet sepa lo que hago | 5 | 8.3 |
| Descargar películas, series, música…(p2p) | 7 | 11.7 |
| Conexión a internet segura incluso en WI-FI públicas | 12 | 20 |
| Evitar que comercialicen mis datos de navegación | 4 | 6.7 |
| Otros | 7 | 13.3 |
| Total | 60 | 100 |


Figura 68. Gráfico del porcentaje de la pregunta 2 de la encuesta realizada

**Fuente:** Grupo Investigativo

**Análisis e Interpretación**

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que la mayoría de encuestados es el 31.7% utilizan las VPN para esconder su IP y falsear su ubicación, 20% utilizan para los WIFI públicas para tener una conexión segura, 11% utiliza para descargar música o películas, 8.3% utilizan para evitar las censuras y bloqueos geográficos de contenido y también utilizan para evitar que el proveedor de Internet sepa lo que hagan y por ultimo 13.3% son otros como juegos, no saben y no han utilizado.

**Conclusión**

Con los resultados obtenidos de la segunda pregunta se puede evidenciar que la mayoría de estudiantes de los ciclos sexto, séptimo y octavo de la Universidad Técnica de Cotopaxi prefieren esconder su dirección IP para mejorar la red que utilizan.

**Pregunta 3.** ¿Conoce usted la tecnología de redes privadas virtuales VPLS?

Tabla 10. Frecuencia y porcentaje de la pregunta 3 de la encuesta realizada

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| Si | 19 | 31.7 |
| No | 41 | 68.3 |
| Total | 60 | 100 |

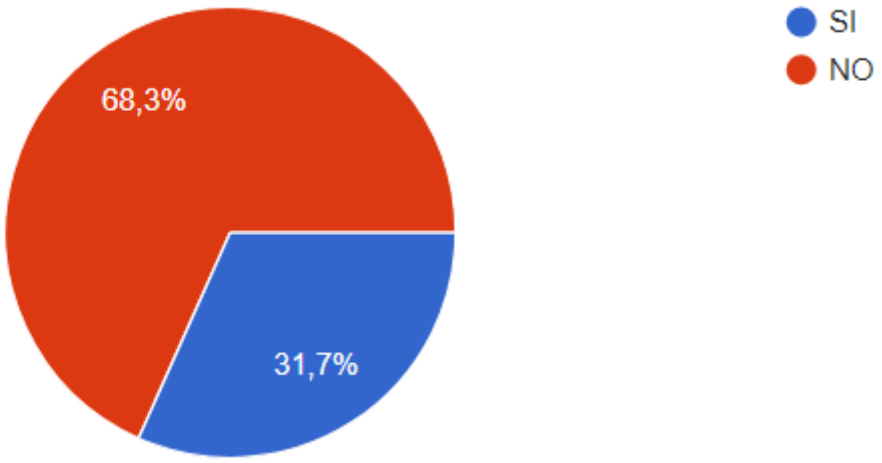



Figura 69. Gráfico del porcentaje de la pregunta 3 de la encuesta realizada

**Fuente:** Grupo Investigativo

### Análisis e Interpretación

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 68.3% se, expresaron no tienen conocimiento sobre la tecnología VPLS y un 31.7 tienen un conocimiento sobre VPLS la mayoría no han escuchado hablar sobre esta tecnología.

### Conclusión

Con los resultados obtenidos de la tercera pregunta se puede evidenciar que la mayoría de estudiantes de los ciclos sexto, séptimo y octavo de la Universidad Técnica de Cotopaxi no conocen la tecnología VPLS.

**Pregunta 4.** ¿Conoce usted la tecnología de redes privadas virtuales EVPN?

Tabla 11. Frecuencia y porcentaje de la pregunta 4 de la encuesta realizada

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| Si | 15 | 25 |
| No | 45 | 75 |
| Total | 60 | 100 |

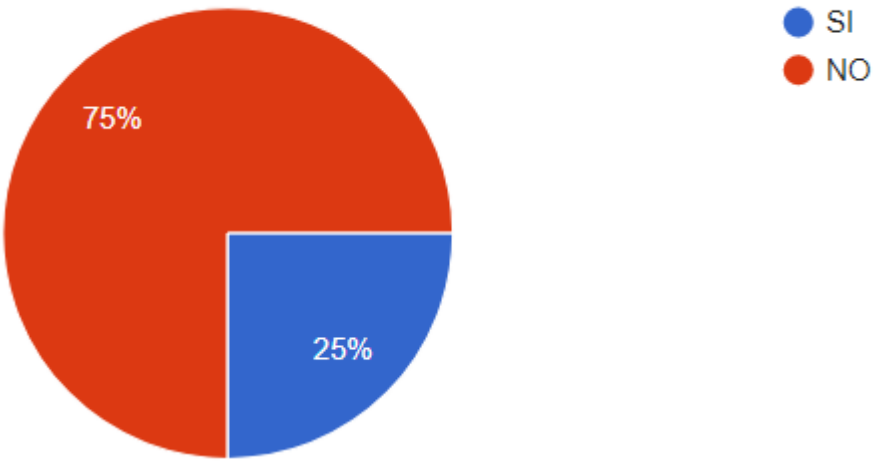



Figura 70. Gráfico del porcentaje de la pregunta 4 de la encuesta realizada

**Fuente:** Grupo Investigativo

**Análisis e Interpretación**

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 25% se, expresaron que, si tiene un conocimiento sobre la tecnología EVPN, mientras que el 75% indicó que no tienen un conocimiento sobre la tecnología EVPN.

**Conclusión**

Con los resultados obtenidos de la cuarta pregunta se puede evidenciar que la mayoría de estudiantes de los ciclos sexto, séptimo y octavo de la Universidad Técnica de Cotopaxi no conocen la tecnología EVPN.

**Pregunta 5.** ¿Considera usted que tiene seguridad la red la Universidad Técnica de Cotopaxi?

Tabla 12. Frecuencia y porcentaje de la pregunta 5 de la encuesta realizada

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| Si | 24 | 40 |
| No | 36 | 60 |
| Total | 60 | 100 |

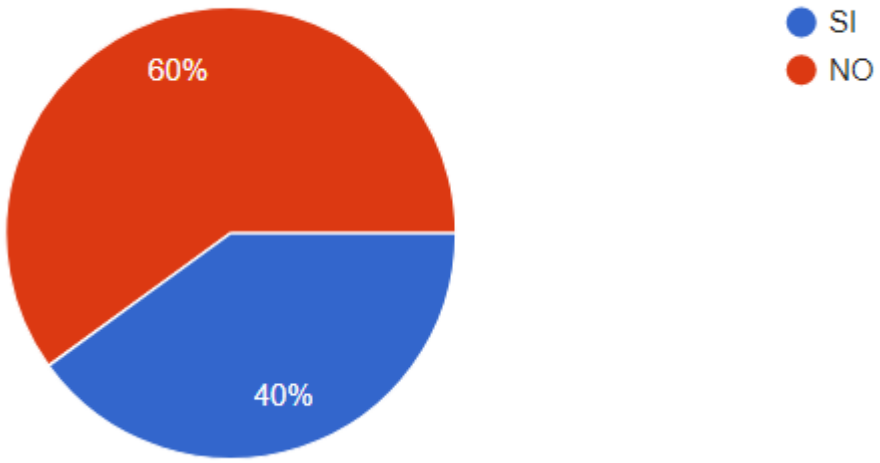



Figura 71. Gráfico del porcentaje de la pregunta 5 de la encuesta realizada

**Fuente:** Grupo Investigativo

**Análisis e Interpretación**

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 40% se, expresaron que, si la red de la universidad tiene seguridad, mientras que el 60% determinó que no que la red de la de la universidad no tiene seguridad.

**Conclusión**

Con los resultados obtenidos de la quinta pregunta se puede evidenciar que la mayoría de estudiantes de los ciclos sexto, séptimo y octavo de la Universidad Técnica de Cotopaxi determino que la red de la Universidad Técnica de Cotopaxi es insegura.

**Pregunta 6.** ¿Tiene calidad de servicio la red de la Universidad Técnica de Cotopaxi?

Tabla 13. Frecuencia y porcentaje de la pregunta 6 de la encuesta realizada

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| Si | 24 | 40 |
| No | 36 | 60 |
| Total | 60 | 100 |

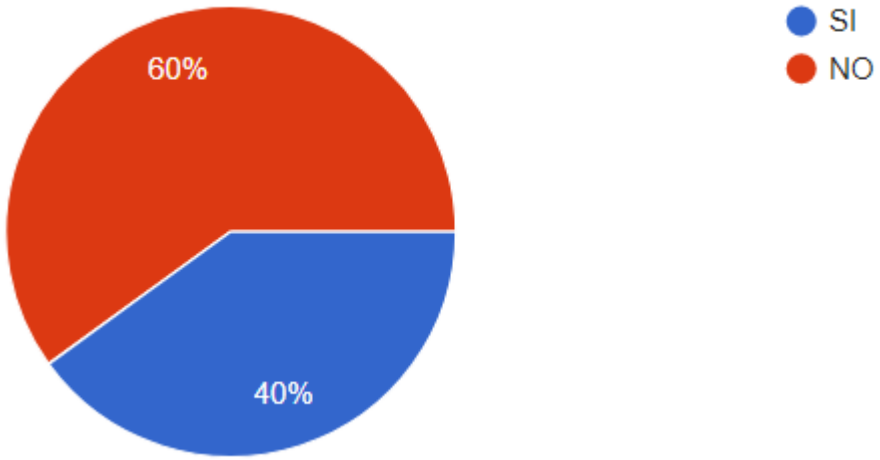



Figura 72. Gráfico del porcentaje de la pregunta 6 de la encuesta realizada

**Fuente:** Grupo Investigativo

**Análisis e Interpretación**

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 40% se, expresaron que, si la red de la universidad tiene calidad de servicios, mientras que el 60% determinó que no la red de la de la universidad no tiene calidad de servicio.

**Conclusión**

Con los resultados obtenidos de la sexto pregunta se puede evidenciar que la mayoría de estudiantes de los ciclos sexto, séptimo y octavo de la Universidad Técnica de Cotopaxi determino que la red de la Universidad Técnica de Cotopaxi no tiene calidad de servicios.

**Pregunta 7.** ¿Considera eficaz la red de la Universidad Técnica de Cotopaxi?

Tabla 14. Frecuencia y porcentaje de la pregunta 7 de la encuesta realizada

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| Si | 24 | 40 |
| No | 36 | 60 |
| Total | 60 | 100 |

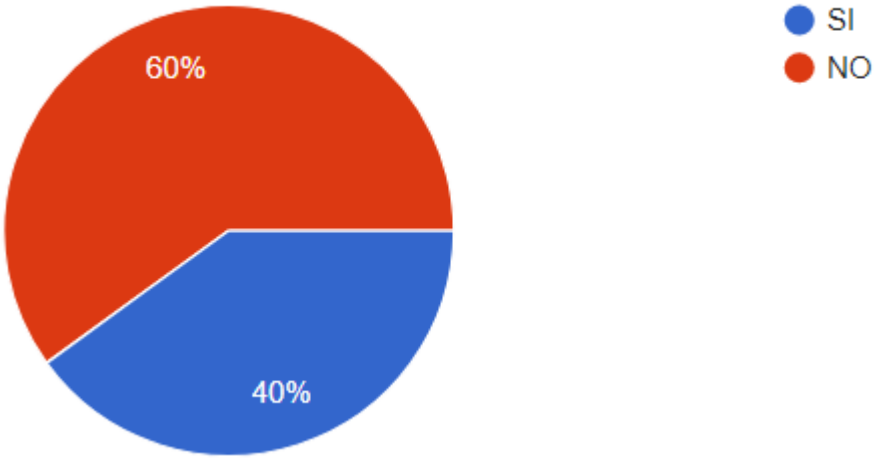



Figura 73. Gráfico del porcentaje de la pregunta 7 de la encuesta realizada

**Fuente:** Grupo Investigativo

### Análisis e Interpretación

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 40% se, expresaron que, si es eficaz la red de la universidad, mientras que el 60% determino que no la red de la de la universidad no es eficaz.

### Conclusión

Con los resultados obtenidos de la séptima pregunta se puede evidenciar que la mayoría de estudiantes de los ciclos sexto, séptimo y octavo de la Universidad Técnica de Cotopaxi determino que la red de la Universidad Técnica de Cotopaxi no es eficaz.

**Pregunta 8.** ¿Considera usted que la Universidad Técnica de Cotopaxi debe implementar alguna de estas tecnologías de VPNs para mejorar la seguridad de la red?

Tabla 15. Frecuencia y porcentaje de la pregunta 8 de la encuesta realizada

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| Si | 43 | 71.7 |
| No | 17 | 28.3 |
| Total | 60 | 100 |

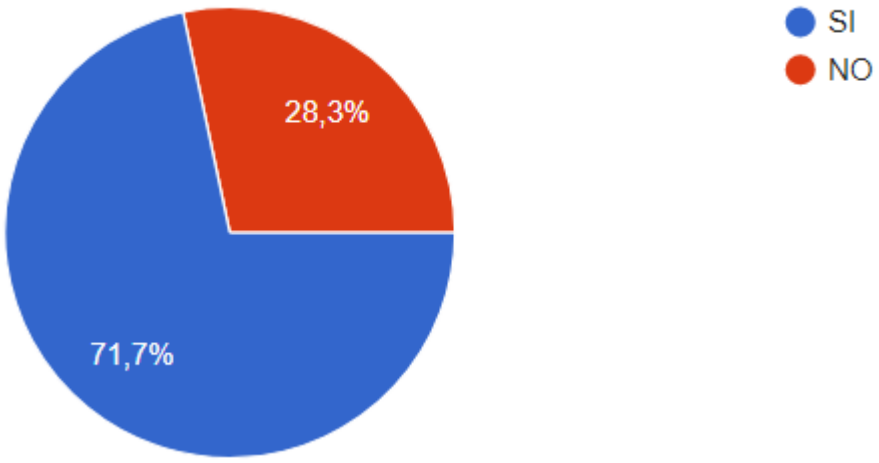



Figura 74. Gráfico del porcentaje de la pregunta 8 de la encuesta realizada

**Fuente:** Grupo Investigativo

**Análisis e Interpretación**

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 71.37% se, expresaron que, si deben implementar algunas de estas tecnologías para mejorar la seguridad en la Universidad Técnica de Cotopaxi, mientras que el 28.3% determino que no factible implementar estas tecnologías en la universidad.

**Conclusión**

Con los resultados obtenidos de la octava pregunta se puede evidenciar que la mayoría de estudiantes de los ciclos sexto, séptimo y octavo de la Universidad Técnica de Cotopaxi determino que la red de la Universidad Técnica de Cotopaxi no cuenta con la seguridad que debería.

# 6. CONCLUSIONES Y RECOMENDACIONES

## 6.1. Conclusiones

- La revisión bibliográfica de las tecnologías EVPN (Ethernet Vpn) y VPLS (Virtual Private Lan Service) fortalecen la seguridad de la red de la Universidad Técnica de Cotopaxi, en la capa 2 y capa 3 de acuerdo al modelo OSI y mejora la calidad de servicio del tráfico de datos.
- El siguiente proyecto de investigación hemos utilizado herramientas tecnológicas para la simulación y posterior análisis del rendimiento, la utilización del software GNS3 para la simulación y el motor llamado VMware apoyara a un desempeño eficaz del hardware para una red mixta es decir con varias topologías en cuanto a equipos de networking, lo cual hara un ambiente más real en el ambiente de pruebas y configuraciones, las pruebas realizadas se basan en la infraestructura de la red de la Universidad Técnica de Cotopaxi sobre la que es posible implementar las herramientas tecnológicas bajo las mismas restricciones y condiciones para que los resultados sean confiables.
- En el rendimiento se pudo validar que el tiempo de confluencia en la tecnología de VPLS es de 44.5 segundos en media, en caso contrario la tecnología EVPN tarda 8.0 segundos en media para que la red converja, la red de la Universidad técnica de Cotopaxi comprende en el núcleo 3 enrutadores son importantes en un rango de 6 a 1 .por lo tanto cuando brindamos un servicio es de vital importancia ya que el tiempo de tolerancia a fallos debe ser bajo ,otro aspecto relevante en esta investigación es la capacidad de las dos tecnologías en la movilidad Mac , la investigación se basa en una persona con una computadora moviéndose de un enrutador a otro ,pero en la realidad en un centro de datos ,obtendremos la capacidad de tener redundancia en un problema en fallo de datos y tiempo en la actualización de la tabla de alcanzabilidad.

### 6.2. Recomendaciones

- De la revisión bibliográfica realizada se sugiere revisar las plataformas estandarizadas en la infraestructura de redes, como son la plataforma de cisco
- La red de la Universidad Técnica de Cotopaxi debe tener mayor autonomía sobre el hardware, con un número considerable de enrutadores se podría realizar más pruebas de las realizadas y de esta manera profundizar el aprendizaje de comunicación de datos.
- Con los resultados obtenidos del proyecto de investigación de las herramientas tecnológicas EVPN (Ethernet Vpn) y VPLS (Virtual Private Lan Service) se recomienda la utilización la tecnología EVPN (Ethernet Vpn) en la red de la Universidad Técnica de Cotopaxi ya que mejora el tráfico de datos y da seguridad para entornos virtualizados.

## 7. BIBLIOGRAFÍA:


[1] Calahorrano Vega, Cesar Augusto, "LAS TECNOLOGIAS DE EVPN Y VPLS SOBRE UNA RED MPLS. (2019)"

[2] Ing. Fulvio Andrés Carrasco Cabrera, "DISEÑO Y SIMULACIÓN DE UNA RED DE ACCESOS EN GNS3 UTILIZANDO LA TECNOLOGÍA SD-WAN PARA MEDIANAS EMPRESAS EN EL ECUADOR. (2020)"

[3] Gabriel García Moreno, "ESTUDIO Y DISEÑO DE UNA RED MPLS PARA LAS DEPENDENCIAS EXTERNAS UBICADAS EN LA REGIÓN 7 DE LA UNIVERSIDAD NACIONAL DE LOJA. (2017)"

[4] Emileni Solange Castro Ullauri, "UN DISEÑO Y SIMULACIÓN DE UNA RED MPLS PARA INTERCONECTAR ESTACIONES REMOTAS UTILIZADAS EL EN EMULADOR GNS3. (2016)"

[5] -Diego Álvarez Delgado -Carolina Jorquera Cáceres -Gabriel Sepúlveda Jorquera -Camila Zamora Esquivel, "Redes Privadas Virtuales (VPN), (2017)."

[6] O. B. Prieto, "VPLS: alternativa de interconexión a través del backbone IP/MPLS de ETECSA VPLS: alternative of interconnection through ETECSA´s IP/MPLS backbone," *Revista Cubana de Ciencias Informáticas*, vol. 7, no. 1, pp. 32–43, 2017, [Online]. Available: http://rcci.uci.cu

[7] "ETHERNET VPN (EVPN) Interconexión L2-Ethernet sobre redes WAN de última generación_ E-VPN - PDF Free Download" (2016).

[8] "What Is EVPN? Why Do We Need EVPN? - Huawei." https://info.support.huawei.com/info-finder/encyclopedia/en/EVPN.html (accessed jun. 14, 2022).

[9] A. Valdés Jiménez, "Cisco IOS", 2018.

[10] F. García and López Rafael, “Gns3 en el desarrollo de laboratorios de redes virtuales”, (2017).

[11] A. Fajardo-Moya, “QEMU, una alternativa libre para la emulación de arquitecturas de hardware,” 2016. [Online]. Available: https://www.researchgate.net/publication/283506874

[12] A. B. Mailewa, A. Mailewa, and J. Herath, “Operating Systems Learning Environment with VMware,” 2018. [Online]. Available: https://www.researchgate.net/publication/322343230

[13] Castaño Andres, Ocampo Lina, and Orozco Michael, “Fundamentación teórica y exploración de generadores de tráfico multiplataforma.” (2018).

[14] “ANÁLISIS DE TRÁFICO CON WIRESHARK INTECO-CERT,” 2018. [Online]. Available: http://www.inteco.es.

[15] Aguirre L, F. González, and Mejía D, “Aplicaciones de MPLS, Transición de IPv4 a IPv6 y Mejores Prácticas de Seguridad para el ISP Telconet,” 2018.

[16] “5 MOTIVOS POR LOS QUE UTILIZAR UNA VPN - Tecsens - Consulting.” https://www.tecsens.com/5-motivos-por-los-que-utilizar-una-vpn/ (accessed Aug. 05, 2022).

[17] “Cisco IOS se actualiza reparando diez vulnerabilidades de denegación de servicio - ChannelBiz.” https://www.channelbiz.es/2013/09/30/cisco-ios-actualiza-diez-vulnerabilidades-denegacion-servicio/amp/ (accessed Aug. 18, 2022).

[18] “GNS3 lanza la versión 1.4 con importantes mejoras incluyendo GNS3 VM.” https://www.redeszone.net/2016/01/17/gns3-lanza-la-version-1-4-con-importantes-mejoras-incluyendo-gns3-vm/ (accessed Aug. 20, 2022).

[19] “QEMU 6.2: RISC-V, SGX, Apple Silicon (M1) y más... | Linux Adictos.” https://www.linuxadictos.com/qemu-6-2-mejoras-version.html (accessed Aug. 19, 2022).

[20] “Instalar VMware Workstation Player en Ubuntu - SomeBooks.es.” http://somebooks.es/instalar-vmware-workstation-player-ubuntu/ (accessed Aug. 20, 2022).

[21] “Overview - Ostinato Guides.” https://userguide.ostinato.org/ (accessed Aug. 20, 2022).

[22] “El nuevo Wireshark 2.2.2 con varias vulnerabilidades corregidas.” https://www.redeszone.net/2016/11/17/disponible-nuevo-wireshark-2-2-2-varias-vulnerabilidades-corregidas/ (accessed Aug. 20, 2022).

[23] K. Alam Singh and J. Noonari, “EVPN basado en BGP MPLS EVPN basado en BGP MPLS Y su implementación y casos de uso.2017”.

[24] Lesserre M, & Kompella, “V. Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP)” (2019).

[25] Sanchez, A, & Grzegorz, K. “MPLS in the SDN Era.O’Relly” (2016).

[26] K. Alam Singh and J. Noonari, “BGP MPLS based EVPN BGP MPLS based EVPN And its implementation and use cases,” 2019.

[27] Y. Nurdiansyah, N. Pratama, M. I. Putra, and M. A. Sya'roni, "Analisis Perbandingan Metode Interior Gateway Protocol RIP Dengan OSPF Pada Jaringan MPLS-VPLS," 2020.

[28] Dr. Y. K. Sharma* and C. Kaur, "The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World," International Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 6, pp. 2336–2339, Mar. 2020, doi: 10.35940/ijrte.F8335.038620.

[29] S. Plug and L. Engels, "Using EVPN to minimize ARP traffic in anIXP environment," 2019.

[30] S. Dadi Riskiono, "ANALISIS DAN DESAIN JALUR TRANSMISI JARINGAN ALTERNATIF MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN)," 2019.

[31] D. Pucci and G. Casoni, "Monitoring an EVPN-VxLAN fabric with BGP Monitoring Protocol," 2020.

[32] Valencia Marin Jonh Jaime, Valencia Patino Alejandro, and Acevedo Bedoya Juan Camilo, "Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS," pp. 84–99, 2020.

[33] F. Rosenbaum, G. Rosenbaum, W. Lau, and S. Jha, "An Analysis of Virtual Private Network Solutions Cell-Hopping Networks View project LoRa network View project An Analysis of Virtual Private Network Solutions," 2020. [Online]. Available: https://www.researchgate.net/publication/2899089

# 8. ANEXOS

## Anexo 1. Informe de Urkund

Ouriginal by Turnitin

### Document Information

| | |
|---|---|
| **Analyzed document** | Lituma_Yanez.docx (D143368477) |
| **Submitted** | 8/29/2022 9:16:00 PM |
| **Submitted by** | |
| **Submitter email** | jorge.rubio@utc.edu.ec |
| **Similarity** | 1% |
| **Analysis address** | jorge.rubio.utc@analysis.urkund.com |

Firmado electrónicamente por:
JORGE BLADIMIR RUBIO PENAHERRERA

### Sources included in the report

| | | |
|---|---|---|
| SA | **GABRIELTORRESTESIS.docx**<br>Document GABRIELTORRESTESIS.docx (D23798883) | 1 |
| SA | **Tesis Laboratorios virtuales para cursos de Tx de Datos..docx**<br>Document Tesis Laboratorios virtuales para cursos de Tx de Datos..docx (D11056299) | 1 |
| W | URL: https://www.channelbiz.es/2013/09/30/cisco-ios-actualiza-diez-vulnerabilidades-denegacion-servicio/amp/<br>Fetched: 8/29/2022 9:18:00 PM | 1 |
| SA | **TT GIAN BANCHON.docx**<br>Document TT GIAN BANCHON.docx (D85985355) | 1 |
| W | URL: https://www.linuxadictos.com/qemu-6-2-mejoras-version.html<br>Fetched: 8/29/2022 9:18:00 PM | 1 |
| W | URL: https://www.redeszone.net/2016/11/17/disponible-nuevo-wireshark-2-2-2-varias-vulnerabilidades-corregidas/<br>Fetched: 8/29/2022 9:18:00 PM | 1 |

### Entire Document

1. INTRODUCCIÓN La técnica de las redes virtuales privadas fue concebida en un principio para las grandes empresas, pero en el presente la utilizamos para las actividades cotidianas que tienen las organizaciones pequeñas y medianas. La necesidad que tenemos en la actualidad de tener redes seguras es casi indispensable ya que tenemos información importante que podría ser robada o cambiada. La resolución que llegaron fue las redes virtuales privadas.
Los ambientes virtuales de enrutamiento IP han ido evolucionando en los últimos tiempos es por ello que surgió el protocolo de MPLS, que puede mejorar los planes a corto mediano y largo plazo y poder extender las aplicaciones en una red, es de vital importancia hoy en día ya que las expectativas de los usuarios son cada vez mayores.
1.1. PROBLEMA

**Anexo 2. Formulario de encuesta**

**UNIVERSIDAD TÉCNICA DE COTOPAXI**

**FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS**

**CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACION**

**TEMA:** "Estudio comparativo del rendimiento de tecnologías EVPN y VPLS en un ambiente simulado utilizando GNS3 en la Universidad Técnica de Cotopaxi."

**INSTRUCCIONES:** Sus respuestas serán tratadas de forma confidencial y serán utilizadas únicamente para un proyecto de investigación.

**DIRIGIDO:** Estudiantes de la Carrera de sistemas (sexto, séptimo, octavo).

1. **¿Has oído hablar de las VPNs?**
   - SI
   - NO

2. **¿Para qué usas o usarías una VPN?**
   - Evitar censuras y bloqueos geográficos de contenido
   - Esconder mi IP y falsear mi ubicación
   - Evitar que mi proveedor de Internet sepa lo que hago
   - Descargar películas, series, música…(p2p)
   - Conexión a internet segura incluso en WI-FI públicas
   - Evitar que comercialicen mis datos de navegación
   - Otros: (Por favor escribe una breve descripción)

3. **¿Conoce usted la tecnología de redes privadas virtuales VPLS?**
   - SI
   - NO

4. **¿Conoce usted la tecnología de redes privadas virtuales EVPN?**
   - SI

- NO

**5. ¿Tiene seguridad la red la Universidad Técnica de Cotopaxi?**

- SI
- NO

**6. ¿Tiene calidad de servicio la red de la Universidad Técnica de Cotopaxi?**

- SI
- NO

**7. ¿Considera eficaz la red de la Universidad Técnica de Cotopaxi?**

- SI
- NO

**8. ¿Considera usted que la Universidad Técnica de Cotopaxi debe implementar alguna de estas tecnologías de VPNs?**

- SI
- NO

## Anexo 3. Acuerdo de confidencialidad

Universidad Técnica de Cotopaxi

DIRECCION DE ASESORIA JURIDICA

**ACUERDO DE CONFIDENCIALIDAD**

- Comparece a la suscripción del presente acuerdo de confidencialidad y responsabilidad de la información, Bryan Fernando Yánez Arcos,1726244583, y Jonathan Paul Lituma Galarza, 1750766063, en calidad de estudiantes (en lo adelante *LOS ESTUDIANTES*) investigador del Proyecto" Estudio comparativo del rendimiento de tecnologías Evpn y Vpls en un ambiente simulado utilizando gns3 en la Universidad Técnica de Cotopaxi"; y, por otra parte, el PhD. Cristian Tinajero, en calidad de Rector de la Universidad Técnica de Cotopaxi, de conformidad con las siguientes cláusulas:

**CLÁUSULA PRIMERA: ANTECEDENTES.-**

**1.1** De conformidad a lo señalado en bases legales de la Universidad Técnica de Cotopaxi relacionado a la ***PROPIEDAD Y CONFIDENCIALIDAD DE LOS DOCUMENTOS.-*** *Todos los informes, documentos y en general toda la información que resultaren conocidas por los colaboradores (LOS ESTUDIANTES), serán de propiedad exclusiva de LA UNIVERSIDAD; así mismo, LOS ESTUDIANTES tendrán la obligación de mantener la más estricta confidencialidad de la información técnica, comercial y financiera perteneciente a LA UNIVERSIDAD, ya sea por venir inscrita en cualquier material físico, o en el sentido de resultar conocida por LOS ESTUDIANTES como consecuencia, directa o indirecta, de los servicios objeto de la presente colaboración, consecuentemente se obliga a no hacer, no divulgar de las actividades materia de LA INVESTIGACIÓN a terceras personas que puedan afectar la estructura de los proyectos su ejecución o administración.*

**1.2** El artículo 116 del Código Orgánico de la Economía Social de los Conocimientos señala: ***Art. 116.- Derechos Patrimoniales del Sector Público.-*** *La titularidad de los derechos sobre las obras creadas por servidores públicos en el desempeño de sus cargos, corresponderá a los organismos, entidades, dependencias del sector público respectivamente.*

**1.3** Los estudiantes Bryan Fernando Yánez Arcos,1726244583, y Jonathan Paul Lituma Galarza, 1750766063, estudiantes de la carrera de Sistemas de Información, fueron designados como Estudiantes Investigadores del proyecto Estudio comparativo del rendimiento de tecnologías Evpn y Vpls en un ambiente simulado utilizando gns3 en la Universidad Técnica de Cotopaxi, *para realizar su proyecto de titulación* cuyo objetivo es:

**General:** Realizar el estudio comparativo del rendimiento de tecnologías Evpn y Vpls en un ambiente simulado utilizando gns3 en la Universidad Técnica de Cotopaxi

**CLÁUSULA SEGUNDA: OBJETO. -**

El objeto del presente acuerdo es determinar las prohibiciones de divulgación, uso y explotación de los resultados y toda la información inherente al desarrollo, ejecución y culminación del proyecto, "Estudio comparativo del rendimiento de tecnologías Evpn y Vpls en un ambiente simulado utilizando gns3 en la Universidad Técnica de Cotopaxi", términos y condiciones con los cuales los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063, en calidad de Estudiantes Investigadores, mantendrán la confidencialidad de todos los datos que maneje y la información institucional que por motivo de su actividad, funciones y servicios llegaren a conocer, tener acceso, hacer uso o manejo de ella.

**CLÁUSULA TERCERA: ACUERDO.-**

Las partes acuerdan que cualquier información relacionada con el proyecto "Estudio comparativo del rendimiento de tecnologías Evpn y Vpls en un ambiente simulado utilizando gns3 en la Universidad Técnica de Cotopaxi", es de propiedad patrimonial de la Universidad Técnica de Cotopaxi y que fuera facilitada de sus archivos o creada en relación a la propiedad intelectual bajo los parámetros del Código Orgánico de la Economía Social de los Conocimientos, y que por motivo de la actividad, funciones y servicio, o que por cualquier otra circunstancia o medio llegue a conocimiento de los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063, se regirá por este Acuerdo.

**CLÁUSULA CUARTA: USO Y SU PROTECCIÓN.-**

En lo relativo al uso y protección de la información institucional, los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063, deberán considerar los siguientes aspectos:

**4.1** La información institucional que reciban, conozcan, accedan, manejen o hagan uso los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063, será mantenida y protegida como confidencial, incluyendo información relativa a derechos de autor, investigaciones técnicas, programas, modelos, estrategias, utiliza para cumplir con su objeto y funciones.

**4.2** Toda la información institucional incluida la digital y física (archivos) es de propiedad de la Universidad Técnica de Cotopaxi, por lo que los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063, son conscientes en que la información que reciban, conozcan, accedan, manejen o hagan uso es confidencial y su utilización será exclusiva de sus funciones.

1

**4.3** Los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063, suscriben este documento comprometiéndose a cuidar la información entregada en relación al proyecto "Estudio comparativo del rendimiento de tecnologías Evpn y Vpls en un ambiente simulado utilizando gns3 en la Universidad Técnica de Cotopaxi" es de propiedad exclusiva de la Universidad Técnica de Cotopaxi y no revelársela a terceras personas sin previa autorización de la institución.

En la Universidad Técnica de Cotopaxi se gestionará el consentimiento escrito del señor Rector para la divulgación de la información, exceptuando los casos en que sea requerida legalmente por la autoridad competente. En aquellos casos en que la información sea requerida legalmente por autoridad competente, los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063, previo a la entrega de la información, notificarán inmediatamente a la Universidad Técnica de Cotopaxi, al respecto.

**4.4** los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063 del Proyecto "Estudio comparativo del rendimiento de tecnologías Evpn y Vpls en un ambiente simulado utilizando gns3 en la Universidad Técnica de Cotopaxi, suscriben este documento obligándose a guardar y mantener la reserva para la no reproducción de la información institucional confiada en virtud de la ejecución y cumplimiento del presente Acuerdo. La inobservancia de lo manifestado generará responsabilidad y dará lugar a que la Universidad Técnica de Cotopaxi, ejerza las acciones legales civiles, penales y/o administrativas correspondientes.

**4.5** los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063 _están obligados a devolver al personal responsable de la Universidad Técnica de Cotopaxi, la información, grabación, y/o productos resultantes del proyecto "Estudio comparativo del rendimiento de tecnologías Evpn y Vpls en un ambiente simulado utilizando gns3 en la Universidad Técnica de Cotopaxi",a los que se tuvieren acceso, sin autorización expresa y evidenciada por parte del Director de Tecnologías de Información y Comunicación poniendo en riesgo la información confidencial obtenida.

**CLÁUSULA QUINTA: ACLARATORIA.-** Este acuerdo, únicamente regula la confidencialidad y la información institucional de la Universidad Técnica de Cotopaxi por lo que no constituye o implica la promesa de entrar en una relación contractual o de negocios entre las partes.

**CLÁUSULA SEXTA: SOLUCIÓN DE CONTROVERSIAS.-** De producirse controversias, discrepancias o reclamos, derivados o relacionados con la interpretación, aplicación, cumplimiento o ejecución del presente Acuerdo, en casos pertinentes y luego de la decisión de la Máxima Autoridad de la Universidad Técnica de Cotopaxi se procederá a un arreglo directo, con justicia y equidad. Si no fuere posible solucionar las controversias en el término de cinco (5) días desde que se originaron, serán sometidas a decisión de un mediador del Centro de Mediación de la Procuraduría General del Estado, con sede en la ciudad de Quito. Si las partes no llegaren a un acuerdo, se someterán al procedimiento determinado en el Código Orgánico de la Economía Social del Conocimiento; para lo cual, renuncian fuero y domicilio y se someterán a la decisión y fallo de la autoridad competente en materia de derechos intelectuales.

**CLÁUSULA SÉPTIMA:** Los estudiantes Bryan Fernando Yánez Arcos,1726244583 y Jonathan Paul Lituma Galarza, 1750766063, aceptan el contenido de acuerdo de confidencialidad y de responsabilidad, para lo cual suscribe el documento en tres originales de igual contenido y valor.

Dado en la ciudad de Latacunga, a los 11 días del mes de mayo de 2022.

Bryan Fernando Yánez Arcos
1726244583

Dr. Cristian Fabricio Tinajero Jiménez
RECTOR

UNIDAD TÉCNICA DE COTOPAXI RECTORADO

Jonathan Paul Lituma Galarza
1750766063

## Anexo 4. Validación de Expertos

### INFORME DE OPINIÓN DE EXPERTOS

**1. DATOS GENERALES:**

- Nombres del Experto: Gustavo Rodríguez Bárcenas
- Grado Académico: PhD. En Ciencias de la Información
- Profesión: Sistemas
- Institución donde labora: Universidad Técnica de Cotopaxi
- Cargo que desempeña: Director de TIC

**2. TEMA DE INVESTIGACIÓN A VALIDAR**

Estudio comparativo del rendimiento de tecnologías EVPN y VPLS en un ambiente simulado utilizando GNS3 en la Universidad Técnica de Cotopaxi.

**3. TABLA DE VALIDACIÓN**

| INDICADORES DE EVALUACIÓN | CRITERIOS | Muy Malo | Malo | Regular | Bueno | Muy Bueno |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 1. Claridad de la investigación | Está formulada con un lenguaje apropiado que facilita su comprensión. | | | | x | |
| 2. Objetividad de la Investigación | Está expresada en conductas observables y medibles. | | | | x | |
| 3. Consistencia de la Investigación | Existe una organización lógica en los contenidos y relación con la teoría | | | | x | |
| 4. Coherencia de la Investigación | Existe relación de los contenidos con las metodologías de investigación | | | | x | |

1

| | | | | | | |
|---|---|---|---|---|---|---|
| 5. Pertinencia de la Investigación | Existe pertinencia de la investigación con la utilización de GNS3. | | | | | x |
| | La Investigación proporciona acceso a la tecnología actual | | | | x | |
| | La Investigación proporciona nuevos conocimientos en lo referente a Redes e Infraestructura | | | | x | |
| | La Investigación permite la implementación de modelos y técnicas de nuevas tecnologías de red | | | | x | |
| SUMATORIA PARCIAL | | | | | 7 | 1 |
| SUMATORIA TOTAL | | | | | | |

**RESULTADOS DE LA VALIDACIÓN**

Valoración total cuantitativa:

Opinión: FAVORABLE _____ DEBE MEJORAR _____

NO FAVORABLE _____

**Observaciones:**

---

---

**Firma:**


PhD. Gustavo Rodríguez Bárcenas

C.C: 1757001357

**Validación de expertos**

# INFORME DE OPINIÓN DE EXPERTOS

**1. DATOS GENERALES:**

- Nombres del Experto: Christian Andrés Morales Robalino
- Grado Académico: Master en Tecnologías de la información con mención en gestión y administración de las tecnologías
- Profesión: Administrador de la infraestructura
- Institución donde labora: Ferrero del Ecuador
- Cargo que desempeña: Administrador de la infraestructura

**2. TEMA DE INVESTIGACIÓN A VALIDAR**

Estudio comparativo del rendimiento de tecnologías EVPN y VPLS en un ambiente simulado utilizando GNS3 en la Universidad Técnica de Cotopaxi.

**3. TABLA DE VALIDACIÓN**

| INDICADORES DE EVALUACIÓN | CRITERIOS | Muy Malo | Malo | Regular | Bueno | Muy Bueno |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 1. Claridad de la investigación | Está formulada con un lenguaje apropiado que facilita su comprensión. | | | | | x |
| 2. Objetividad de la Investigación | Está expresada en conductas observables y medibles. | | | | | x |
| 3. Consistencia de la Investigación | Existe una organización lógica en los contenidos y relación con la teoría | | | | x | |
| 4. Coherencia de la Investigación | Existe relación de los contenidos con las | | | | x | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | metodologías de investigación | | | | | |
| 5. Pertinencia de la Investigación | Existe pertinencia de la investigación con la utilización de GNS3. | | | | | x |
| | La Investigación proporciona acceso a la tecnología actual | | | | x | |
| | La Investigación proporciona nuevos conocimientos en lo referente a Redes e Infraestructura | | | | x | |
| | La Investigación permite la implementación de modelos y técnicas de nuevas tecnologías de red | | | x | | |
| SUMATORIA PARCIAL | | | | 1 | 4 | 3 |
| SUMATORIA TOTAL | | 34 | | | | |

**RESULTADOS DE LA VALIDACIÓN**

Valoración total cuantitativa:

Opinión: FAVORABLE ____X_____ DEBE MEJORAR _____

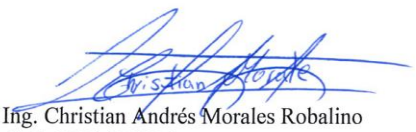
NO FAVORABLE _____

**Observaciones:**

---

---

**Firma:**



Ing. Christian Andrés Morales Robalino
C.C: 1721602884