Pontificia Universidad Católica del Ecuador
FACULTAD DE INGENIERÍA
COORDINACIÓN DE POSGRADO

PUCE



PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

Trabajo de Titulación como requisito previo para la obtención del título de Magíster en Tecnologías de Información mención Gestión y Administración de TI

TEMA:

PRUEBA DE CONCEPTO DE VXLAN-EVPN EN INFRAESTRUCTURA OPENNETWORKING

Autor: CRISTHIAN PAUL LAGLA GALLARDO

Director: Dr. GUSTAVO DAVID SALAZAR CHACÓN. (PHD)

Quito, enero 2023

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

DECLARACIÓN Y AUTORIZACIÓN

Yo, CRISTHIAN PAUL LAGLA GALLARDO, con C.I 1720409471, autor del trabajo de graduación intitulado: "**PRUEBA DE CONCEPTO DE VXLAN-EVPN EN INFRAESTRUCTURA OPENNETWORKING**", previa a la obtención del grado académico de MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TI en la Facultad de INGENIERÍA:

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Quito, enero 2023



_____

CRISTHIAN PAUL LAGLA GALLARDO

C.I. 1720409471

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

APROBACIÓN DEL TUTOR

En mi carácter de Director del Trabajo de Posgrado Titulado: "**PRUEBA DE CONCEPTO DE VXLAN-EVPN EN INFRAESTRUCTURA OPENNETWORKING**", presentado por el maestrante CRISTHIAN PAUL LAGLA GALLARDO, titular de la Cédula de Identidad Nº 1720409471 para optar al Grado Magíster en Tecnologías de la Información mención en Gestión y Administración de TI, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ingeniería.

En la ciudad de Quito, a los 3 días de enero de 2023.

Firmado electrónicamente por:
GUSTAVO DAVID SALAZAR CHACON

GUSTAVO DAVID SALAZAR CHACÓN C.I. 1716104797

gsalazar787@puce.edu.ec

NOTA:

Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: 3 % índice de similitud con otras fuentes.

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

TURNITIN: HOJA DEL INFORME CON EL PORCENTAJE

Turnitin Informe de Originalidad

Procesado el: 02-ene.-2023 23:44 -05
Identificador: 1988115932
Número de palabras: 7619
Entregado: 1

TESIS FINAL CRISTHIAN LAGLA Por Cristhian Paul Lagla Gallardo

Índice de similitud	Similitud según fuente
3%	Internet Sources: 4% Publicaciones: 1% Trabajos del estudiante: 3%

1% match (trabajos de los estudiantes desde 30-abr.-2019)
Submitted to Universidad San Francisco de Quito on 2019-04-30

1% match (Internet desde 17-jun.-2021)
https://www.puce.edu.ec/wp-content/uploads/2021/02/Convocatoria-para-Intercambio-Virtual-U-Antonio-Ruiz-de-Montoya-2021-1-compressed.pdf

1% match (Internet desde 03-nov.-2022)
https://Es.Slideshare.Net/yenncy/t72591

FACULTAD DE INGENIERÍA COORDINACIÓN DE POSGRADO PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR FACULTAD DE INGENIERÍA Trabajo de Titulación como requisito previo para la obtención del título de Magíster en Tecnologías de Información mención Gestión y Administración de TI TEMA: PRUEBA DE CONCEPTO DE VXLAN-EVPN EN INFRAESTRUCTURA OPENNETWORKING Autor: CRISTHIAN PAUL LAGLA GALLARDO Director: Dr. GUSTAVO DAVID SALAZAR CHACÓN. (PHD) Quito, enero 2023 COORDINACIÓN DE POSGRADO PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR DECLARACIÓN Y AUTORIZACIÓN Yo, CRISTHIAN PAUL LAGLA GALLARDO, con C.I 1720409471, autor del trabajo de graduación intitulado: "PRUEBA DE CONCEPTO DE VXLAN-EVPN EN INFRAESTRUCTURA OPENNETWORKING", previa a la obtención del grado académico de MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TI en la Facultad de INGENIERÍA: 1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor. 2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad. Quito, enero 2023 _____ CRISTHIAN PAUL LAGLA GALLARDO C.I. 1720409471 ii COORDINACIÓN DE POSGRADO APROBACIÓN DEL TUTOR En mi carácter de Director del Trabajo de Posgrado Titulado: "PRUEBA DE CONCEPTO DE VXLAN-EVPN EN INFRAESTRUCTURA OPENNETWORKING", presentado por el maestrante CRISTHIAN PAUL LAGLA GALLARDO, titular de la Cédula de Identidad Nº 1720409471 para optar al Grado Magíster en Tecnologías de la Información mención en Gestión y Administración de TI, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ingeniería. En la ciudad de Quito, a los 3 días de enero de 2023. GUSTAVO DAVID SALAZAR CHACÓN C.I. 1716104797 gsalazar787@puce.edu.ec NOTA: Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: … % índice de similitud con otras fuentes. iii COORDINACIÓN DE POSGRADO TURNITIN: INCLUIR HOJA DEL INFORME CON EL PORCENTAJE iv COORDINACIÓN DE POSGRADO DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD Yo, Cristhian Paul Lagla Gallardo portador de la cédula de ciudadanía No.1720409471, declaro bajo juramento que la presente

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

JESUITAS ECUADOR

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Cristhian Paul Lagla Gallardo portador de la cédula de ciudadanía No.1720409471, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se ha respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.



CRISTHIAN PAUL LAGLA GALLARDO
C.I. 1720409471

DEDICATORIA

A mi amada esposa Marisela, a mi hija de 3 añitos Elaine y a mi bebe en camino por ser la mayor motivación de seguir superándome día a día, a mis padres por ser ese gran ejemplo de superación, lucha y humildad, este logro es dedicado a todos ustedes por siempre creer en mí.

AGRADECIMIENTOS

Culminada esta gran meta que me propuse hace un año atrás primero quiero agradecer a Dios por permitirme cumplirlo, por todas las veces que en oración le pedí que guíe mis pasos y tome control de mi mente para poder sacar adelante mi trabajo y mi maestría.

Agradezco a mi esposa Marisela por su amor, apoyo y paciencia en cada una de sus acciones, a mi pequeña hija Elaine por darme esa sonrisa cuando más lo necesite, y especialmente esta vez a mi bebe en camino por llegar a motivarme aún más para seguir adelante con mi trabajo y estudio.

Agradezco a mis padres por todas sus enseñanzas y valores inculcados que hoy en día me han hecho un profesional responsable, por no rendirse conmigo y siempre orientarme de la mejor manera siempre dar lo mejor de mí en todos los aspectos de mi vida.

A mis compañeros de trabajo por su apoyo y motivación para continuar estudiando.

A la Pontificia Universidad Católica del Ecuador haberme permitido continuar con mis estudios mediante su aprobación cuando me postule para la maestría, a cada uno de los docentes que me impartieron sus conocimientos y experiencias laborales que hoy en día son herramientas que uso en el diario en mi trabajo.

De manera especial agradezco a mi director de tesis Dr. Gustavo Salazar por su apertura desde el primer día, tuve la grata experiencia de ser su alumno anteriormente en la academia CISCO y en gran parte fue uno de los motivos que me motivaron a seguir la maestría, sin lugar a duda puedo decir que su manera de enseñar es motivante gracias a la claridad y pasión que demuestra en cada una de sus clases. ¡Por su gran apoyo, paciencia y guía muchas Gracias!

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN 12
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 13
1.1. Formulación del problema 13
1.2. Objetivos de la Investigación 13
Objetivo General 13
Objetivos Específicos 13
1.3. Justificación de la Investigación 13
CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA 15
2.1. Antecedentes de la Investigación 15
2.2. Bases Teóricas. 17
2.2.1. VXLAN 17
2.2.2. EVPN 18
2.2.3. Open Networking 19
CAPÍTULO III: METODOLOGÍA 21
3.1. Cumulus Linux 21
3.2. Topología de Red 23
3.3. Captura de Tráfico 23
CAPÍTULO IV: EMULACIÓN DE LA INFRAESTRUCTURA 24
4.1. Configuración de FRR 26
4.2. Configuración de Equipos Spines 27
4.3. Configuración Leafs 29
CAPÍTULO V: ANALISIS DE FACTIBILIDAD DE LA EMULACIÓN 31
CONCLUSIONES 35
RECOMENDACIONES 36
REFERENCIAS 37
ANEXOS 38

ÍNDICE DE TABLAS

Tabla 1 Cuadro Comparativo de Open Networking vs Tradicional Networking. 22
Tabla 2 Detalle de Comandos de Spine UIO 27
Tabla 3 Detalle de Comando Leaf UIO 29

ÍNDICE DE GRÁFICOS

Figura 1 Topología de 3 capas y Topología Spine-Leaf 15
Figura 2 Descripción general de la integración EVPN-VXLAN 17
Figura 3 Formato de Paquete VXLAN 18
Figura 4 Arquitectura de Cumulus Linux 21
Figura 5 Topología VXLAN-EVPN 23
Figura 6 Topología de Red UIO-GYE 24
Figura 7 VLAN entre Data Center UIO y Data Center GYE 24
Figura 8. Conexión en AD entre Data Center UIO y Data Center GYE. 25
Figura 9 Envió de Paquetes por VXLAN. 25
Figura 10 Habilitar zebra y bgpd. 26
Figura 11 Topología UIO-GYE 31
Figura 12 Ping PC1-PC2 31
Figura 13 Ping PC2- PC1 32
Figura 14 Actualización de versión de GNS3 en máquina virtual. 32
Figura 15 Exportación de Emulación VXLAN. 33
Figura 16 Captura de paquete XVLAN. 33
Figura 17 Validación de tráfico VXLAN. 34

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TI

Prueba de Concepto de VXLAN-EVPN en infraestructura OpenNetworking

Autor: Cristhian Paul Lagla Gallardo

Director -Tutor: Dr. Gustavo Salazar

Fecha: 3 de enero del 2023

RESUMEN

En este trabajo de fin de maestría se explica la evolución de las redes de datos, haciendo énfasis en el *Open Networking* y el diseño de topología *Spine Leaf*; en este escenario de red de datos se hace uso del emulador GNS3 para desplegar VXLAN-EVPN, una solución capaz de conectar dos datacenter ubicados en diferentes ciudades por medio de un túnel inteligente que se crea bajo petición, haciendo de esta manera que la comunicación entre ambos data centers sea mucho más sencilla y generando ventajas de ahorro de direccionamiento.

Palabras clave: Open Networking, Spine Leaf, GNS3, VXLAN, EVPN.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TI

Proof of Concept of VXLAN-EVPN in Open Networking infrastructure

Author: Cristhian Paul Lagla Gallardo

Director: Dr. Gustavo Salazar

Date: January 3rd, 2023

ABSTRACT

This research thesis explains the evolution of data networks, emphasizing Open Networking and Spine Leaf topology design. In this data network scenario, the GNS3 emulator is used to deploy VXLAN-EVPN, a solution capable of connecting two data centers located in different cities by the use of an intelligent tunnel that is created upon request, thus making communication between both data centers much easier and obtaining address savings advantages.

Keywords: Open Networking, Spine Leaf, GNS3, VXLAN, EVPN.

INTRODUCCIÓN

Hoy en día estamos en la Era de la Transformación Digital donde es necesario que existan protocolos mucho más robustos y con mejores prestaciones para transmitir información, uno de ellos es VXLAN, protocolo capaz de crear en hasta 16 millones de etiquetas en un dominio administrativo, esto facilita la migración de servidores virtuales que se encuentren en dominios independientes haciendo uso de la superposición de capa 2 por medio de una tunelización inteligente del tráfico a través de redes de capa 3, sin mencionar la ventaja de equilibrar la carga del tráfico y de esta manera dar un uso optimo del ancho de banda.

Con la virtualización, muchos data center cada vez buscan mejores prestaciones y por ende soluciones que les permitan eliminar limitantes como la distancia geográfica (EVPN-VXLAN), los diseños de red actuales ya no manejan un modelo jerárquico de 3 capas, sino que ahora las soluciones SDN tienen un diseño Spine-Leaf mismo que optimiza el tráfico este-oeste en una red de datos, con el fin de profundizar estos temas se analiza y se estructura la tesis de la siguiente manera:

Capítulo 1: PLANTEAMIENTO DEL PROBLEMA
Capítulo 2: FUNDAMENTACION TEORICA
Capítulo 3: METODOLOGIA
Capítulo 4: EMULACION DE LA INFRAESTRUCTURA
Capítulo 5: ANALISIS DE FACTIBILIDAD DE LA EMULACIÓN

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Formulación del problema

Existe la necesidad de comunicar dos sitios geográficos con una misma VLAN para mejorar el desempeño de aplicaciones de envío de tráfico y segmentación de red, por lo tanto, VXLAN uno de los protocolos más novedosos de *underlay-overlay* cumple con los requerimientos para solventar esa problemática.

1.2. Objetivos de la Investigación

Objetivo General

Desarrollar una prueba de concepto en GNS3 de VXLAN-EVPN dentro del ecosistema Open Networking para unir dos data centers geográficamente separados en una misma VLAN.

Objetivos Específicos

Definir el concepto de VXLAN-EVPN y su importancia para la transformación digital.

Describir a la topología *Spine Leaf* y su utilidad en data centers modernos.

Establecer la importancia de Cumulus Linux en el entorno Open Networking.

1.3. Justificación de la Investigación

La llamada transformación digital con el avance acelerado de la tecnología cada vez afecta más a todos los sectores económicos, esto se debe a los retos que afrontan las empresas hoy en día con tecnologías como el Internet de las Cosas, Big Data e Inteligencia artificial, todo indica una revolución que generará cambios importantes en el empleo, la producción, la economía y la sociedad. Con el avance de la tecnología el usuario cada vez busca mayor velocidad y mejores prestaciones tecnológicas, esto conlleva que detrás de estas soluciones modernas debe haber una infraestructura lo bastante robusta que garantice su funcionamiento.

Con la virtualización varios data centers se modernizaron e hicieron mucho más eficientes el uso de recursos de hardware que disponían, esto forma parte de una transformación digital al igual que la búsqueda de modernizar las redes de datos, en este punto existen protocolos

novedosos como VXLAN y el entorno SDN.

La modernización de la red no ha sido tan acelerada como el avance en servidores y almacenamiento, esto se ha logrado gracias a la virtualización, permitiendo de esta manera la desagregación del software y del hardware por medio de un hipervisor , el *open networking* es para la redes de datos el mismo concepto que se manejó en su momento para la virtualización y al momento es quien lidera la transformación digital en conectividad, permitiendo generar soluciones a la medida y con un pronto retorno de la inversión.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de la Investigación

Las redes tradicionales usan el modelo jerárquico de 3 capas mismos que son (Núcleo, distribución y Acceso), sin embargo, con el notable crecimiento de tráfico de este a oeste (entre Data Centers), el diseño ha evolucionado a uno denominado *Spine-Leaf*, este diseño está pensado para data centers modernos debido a su escalabilidad, fiabilidad y su mejor rendimiento.

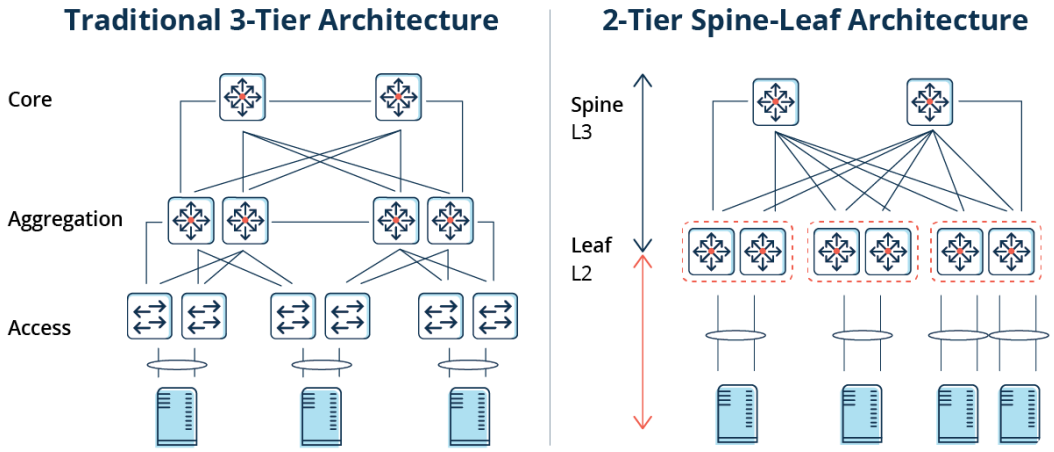


Figura 1 Topología de 3 capas y Topología Spine-Leaf
Fuente: (Aruba, 2022)

Con la digitalización en curso muchas organizaciones se encuentran migrando sus soluciones a la nube e incluso las orientan hacia las nuevas tendencias tecnológicas como IoT. Las nuevas tendencias exigen mayores prestaciones a la red de datos y su modelo tradicional no se adapta a las necesidades actuales de red.

La red definida por software (SDN) se enfoca en ser una solución con un enfoque en el cual las redes sean ágiles y agreguen simplicidad a los protocolos de red haciendo a su vez que el consumo de ancho de banda sea más eficiente y la administración de una red sea mucho más sencilla, independientemente de la cantidad de sedes que interconecte.

Una de sus soluciones más novedosas es la superposición (Underlay-Overlay) que no es más que un protocolo se ejecute más arriba o sobre otro en la red. VXLAN es una solución de superposición que permite generar un túnel a través de los enrutadores, de esta manera se puede

lograr eliminar limitaciones de distancia haciendo que una subred de capa 2 se extienda hacia otro data center.

VXLAN permite tener hasta 16 Millones de VNIs (VXLAN Network ID), a diferencia que con VLAN tradicionales únicamente podemos usar hasta 4000 ID (VIDs), a su vez permite extender la conectividad por capa 2 a cualquier lado de la red IP con un desborde optimizado.

EVPN permite la interconexión de centros de datos, extendiendo de esta manera la capa de enlace de datos L2 entre data centers que alojan y propagan varios servicios, de esta manera se genera un mejor rendimiento al momento de la transferencia de datos de cada aplicación a los usuarios finales. Entre las ventajas más importantes que tiene EVPN sobre tecnologías MPLS se puede mencionar el alias y la redundancia activa/activa.

VXLAN se integra con EVPN para propagar las direcciones MAC aprendidas del cliente a través del túnel inteligente de VXLAN en un protocolo muy importante para la interconectividad en Internet, BGP. En la Figura 2 se muestra cómo cada nodo PE (Provider Edge) aplica EVPN para propagar las direcciones MAC aprendidas del cliente a través del túnel bajo petición VXLAN en BGP. Los nodos PE encapsulan las tramas VXLAN o Ethernet con MPLS para el envío de los paquetes a través del núcleo MPLS y con el encabezado VXLAN para enviar los paquetes que pasan por la red VXLAN.

Cabe decir, que la red de interconexión en la WAN, no requiere necesariamente de MPLS, puede usarse enrutamiento tradicional bajo cualquier IGP (como OSPF), pero usando BGP como protocolo de transporte Overlay.

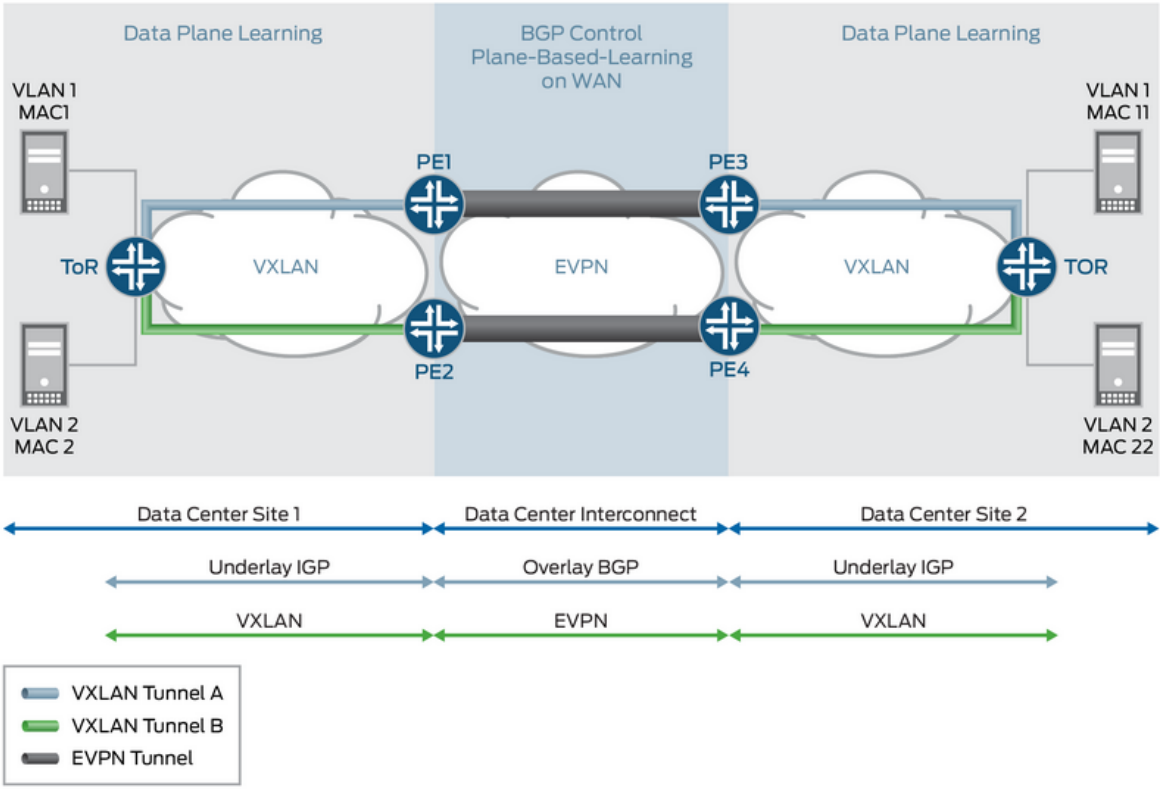


Figura 2 Descripción general de la integración EVPN-VXLAN
Fuente: (Juniper Networks, 2022)

2.2. Bases Teóricas.

2.2.1. VXLAN

Es una red de área local extensible (de ahí sus siglas) utilizada para crear una estructura de capa 2 en centros de datos y entornos de múltiples nubes. Se puede también hacer uso de VXLAN para aislar tráfico que pertenece a múltiples inquilinos alojados en un entorno en nube, incluso permite unir aplicaciones distribuidas en entornos de múltiples nubes.

Los dispositivos que admiten VXLAN se consideran como puntos de conexión de túnel virtual (VTEP), en estos dispositivos se encapsula el tráfico VXLAN y a su vez se desencapsula ese tráfico cuando abandonan el túnel VXLAN.
Cada VTEP agrega varios campos para encapsular una trama Ethernet, entre los ellos se encuentran los siguientes:

- Dirección MAC del punto de conexión del túnel VTEP
- Dirección MAC del origen del túnel VTEP
- Dirección IP del punto de conexión del VTEP

- Dirección IP del origen del túnel VTEP
- Encabezado UDP externo

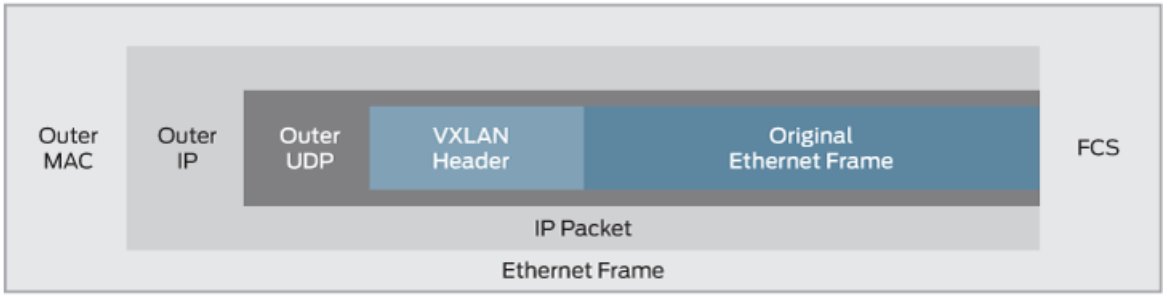


Figura 3 Formato de Paquete VXLAN
Fuente: (Juniper Networks, 2022)

Un encabezado VXLAN contiene un campo de 24 bits que permite identificar la red VXLAN (VNI), este campo permite identificar de forma exclusiva las VXLAN. El VNI es conceptualmente como un ID de VLAN, pero al tener 24 bits tolera la creación de muchas más VXLANs que VLAN (Juniper Networks, 2021).

2.2.2. EVPN

Es una extensión del Protocolo de puerta de enlace fronteriza (BGP) que permite a la red transferir información de accesibilidad del punto final. Esta tecnología de plano de control usa MP-BGP (MultiProtocol BGP) para propagar las direcciones MAC e IP de puntos finales, donde las direcciones MAC se manejan como rutas (Juniper Networks) .

EVPN concede una redundancia y reenvío de múltiples rutas con un modelo de hospedaje múltiple totalmente activo. Un dispositivo tiene la facilidad de conectarse a dos o más dispositivos ascendentes y utilizar todos los enlaces para reenviar el tráfico, esto origina un comportamiento de alta disponibilidad en el cual si un determinado enlace o dispositivo falla, el tráfico sigue siendo enviado por medio de los enlaces activos restantes.

La inundación típica de las redes de capa 2 son evitadas debido al aprendizaje de MAC que ahora se manejan en el plano de control. Con las arquitecturas EVPN-VXLAN, VXLAN proporciona una encapsulación del plano de datos superpuesto y EVPN admite que los dispositivos que generan el túnel inteligente de VXLAN (VTEP) intercambien información de accesibilidad entre sí sobre sus terminales.

El cambio de paradigma hacia la nube ha incluido la adopción de un grado cada vez mayor de virtualización, donde una matriz de servidores físicos y dispositivos pueden albergar varios servidores virtuales que pueden compartir la misma red lógica a pesar de estar en lugares geográficos remotos. A diferencia de la dirección tradicional norte-sur del tráfico de datos entre clientes y servidores, la virtualización ha facilitado un mayor tráfico de datos este-oeste dentro del centro de datos.

El tráfico este-oeste describe las comunicaciones de datos entre servidores y/o varias aplicaciones, todas contenidas dentro del centro de datos. Debido a que muchos de los datos requeridos por el usuario final en una red corporativa o en Internet involucran datos más complejos, se requieren ciertas actividades de preprocesamiento. Como medio para demostrar esta necesidad de preprocesamiento, un ejemplo de tráfico este-oeste implica el acceso desde un servidor web (a través de un servidor de aplicaciones) a la base de datos.

La representación dinámica de sitios web y/o aplicaciones comerciales a menudo utiliza una arquitectura de servidor de dos o tres niveles, donde un nivel debe comunicarse con un segundo nivel antes de entregar los datos solicitados al usuario final. Cuando estos niveles se comunican entre sí o necesitan acceso al almacenamiento de datos u otros datos que residen en el mismo centro de datos, se usa el término tráfico este-oeste porque representa un perfil de ruta más horizontal. Otro ejemplo de tráfico este-oeste se da cuando un usuario que realiza una solicitud a un sitio de redes sociales (como www.facebook.com), lo que da como resultado un conjunto rápido de intercambios entre los servidores que se encuentran en el *backend* del centro de datos y que devuelven una página web. que tiene mucha información sobre el usuario, los *feeds* de sus amigos, los anuncios asociados que pueden coincidir con las preferencias del usuario, etc.

2.2.3. Open Networking

Las redes de datos tradicionales se adaptaron al crecimiento y la redundancia creando varios niveles, esto generaba arquitecturas costosas con varias desventajas como ancho de banda no utilizado, convergencia lenta y una mayor complejidad en la gestión. Las redes actuales no están encaminadas únicamente para tráfico vertical, sino que se adaptan a las nuevas tendencias como es el tráfico este-oeste y de esta manera eliminando bucles de red.

El modelo te topología de las nuevas redes es *Spine-Leaf* y al momento son utilizadas por centros de datos como Google, Facebook y Amazon, su diseño es cada vez más popular para

las empresas debido a sus propiedades de escalamiento horizontal.

El enfoque abierto permite a las empresas manejar un nuevo panorama con la desagregación del sistema operativo del Hardware y la red virtual de la física.

Las soluciones de Open Networking permiten diseñar soluciones a medida del requerimiento de la empresa, esto a su vez estimula la innovación en búsqueda de nuevas soluciones que permitan a los clientes alcanzar mejores niveles de flexibilidad y eficiencia.

Al comparar una solución Open Networking con una solución de Networking propietario podemos encontrar las siguientes ventajas del uso de Open Networking:

- Menor uso de espacio en Data Center.
- Menor consumo de Energía
- Menor gasto en enfriamiento.
- Menor costo
- Un solo punto de administración.

CAPÍTULO III: METODOLOGÍA

En este capítulo se presenta un análisis de la prueba de concepto diseñada para la comprender el funcionamiento y factibilidad de VXLAN-EVPN en *Open Networking* antes de su emulación.

3.1. Cumulus Linux

Cumulus Linux es un potente sistema operativo de networking con base Debian, este sistema operativo está diseñado para la automatización, escalabilidad y flexibilidad que se demanda actualmente en las redes de campus a nivel mundial.

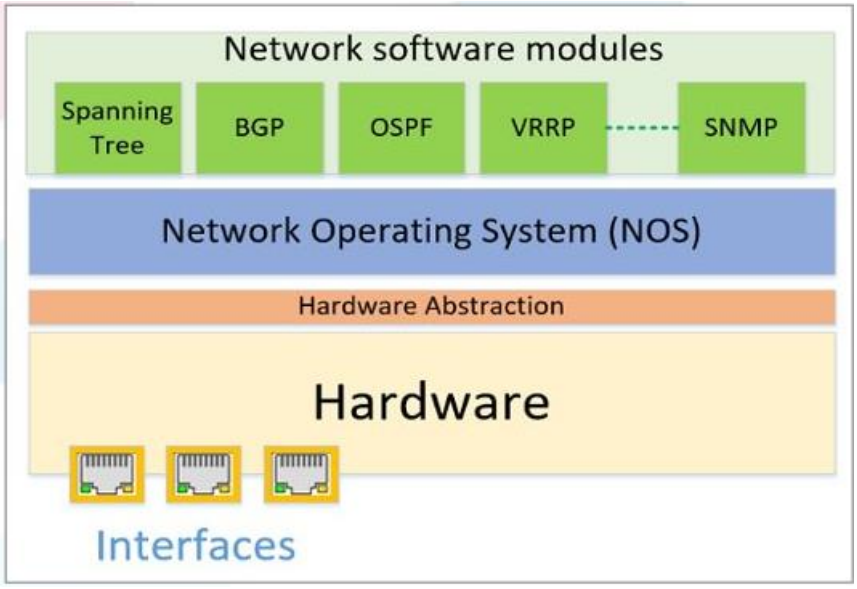


Figura 4 Arquitectura de Cumulus Linux

Permite generar soluciones SDN personalizadas y escalables a un menor costo que soluciones licenciadas o propietarias y a su vez nos brinda una pronta recuperación de la inversión. Como solución CAPEX, reduce el coste y como solución OPEX, permite un aprovechamiento del talento existente.

Cumulus Linux permite arquitecturas de centros de datos modernos, al tiempo que proporciona una ruta de transición para las arquitecturas de centros de datos tradicionales, con soporte para redes de capa 2, capa 3 y superpuestas. Este enfoque abierto permite una amplia gama de soluciones. La administración remota y centralizada de las implementaciones de Inteligencia Artificial permite actualizaciones de software inalámbricas, depuración remota y monitoreo del sistema, así como otras características como sistemas de recuperación automática. Estas funciones de administración remota facilitan el mantenimiento, la Inteligencia Artificial, y

hacen que la IA sea más accesible y práctica para ubicaciones de difícil acceso o lejos de una sede. Esto da como resultado una información más rápida y completa con conocimientos que pueden impulsar decisiones en tiempo real. (NVIDIA, 2022)

Tabla 1 Cuadro Comparativo de Open Networking vs Tradicional Networking.

Open Networking	**Característica**	**Networking Tradicional**
Agilidad altamente automatizada y aumentada.	Compra	Intervención manual y falta de agilidad.
Libertad de la cadena de suministros.	Modelo de Negocio	Bloqueo de proveedores con complejidad inherente.
Mas control y flexibilidad.	Arquitectura	Mayor mantenimiento e inflexible.
1 administrador para 200 conmutadores.	Ventaja Operativa	Administrador de Habilidades especialidades 1: 50 conmutadores.
Hasta 45% de ahorro en gastos de capital.	Costo	Alto gasto de capital.

Las características de Cumulus Linux más relevantes son:

- Uso de interfaces no numeradas.
- Redistribución de vecinos.
- Permite hacer VRFs y EVPN
- Soportado por NVIDIA
- Es un sistema operativo Abierto.

Para comprobar la teoría con una emulación previa a llevarlo a la práctica, para esta emulación se utilizará GNS3, herramienta que facilita crear una topologías con los sistemas operativos reales, pero a una menor escala, que conste de solo unos pocos dispositivos, a su vez permite configurar, probar y plantear una solución de problemas de redes virtuales y reales.

Los ingenieros de redes siempre buscan herramientas que permitan emular una solución de red y en la búsqueda de estas soluciones, GNS3 ha permitido virtualizar dispositivos de hardware reales, en un comienzo solo permitía emular dispositivos de una marca determinada mediante un proceso llamado *Dynamips*, en la actualidad es compatible con muchos dispositivos de

múltiples proveedores de redes, incluidos conmutadores virtuales de Cisco, Cisco ASA, Brocade, vRouters, conmutadores Cumulus Linux, instancias Docker, HPE, Huawei, VSR, varios dispositivos Linux y muchos otros. (gns3, 2021)

3.2. Topología de Red

La topología planteada está formada por 2 equipos Spine y 2 equipos Leaf que representan cada uno un data center diferente, pero que a su vez se encuentran conectados en alta disponibilidad y se comunican en capa 2.

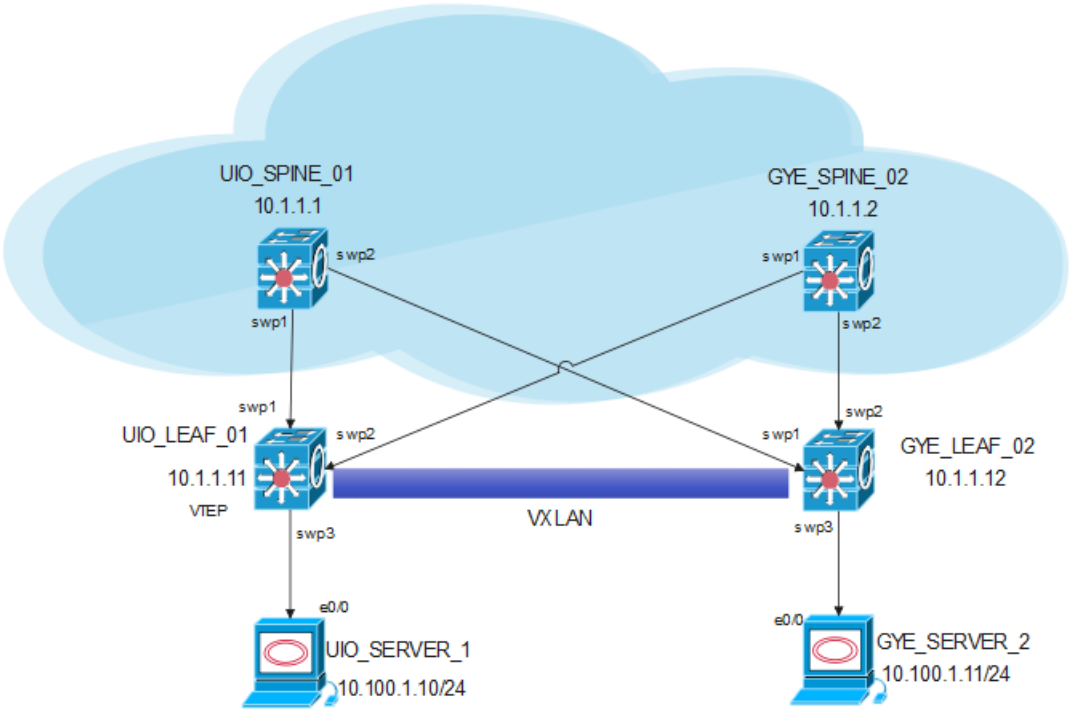


Figura 5 Topología VXLAN-EVPN
Fuente: Autor

3.3. Captura de Tráfico

Con el uso de Wireshark se realizará la captura de los datos, esto permitirá evidenciar la comunicación y encapsulación de VXLAN por medio un túnel inteligente bajo petición, al tener la validación de este tráfico por medio del túnel se podrá evidenciar ventajas para las aplicaciones por medio de una alta disponibilidad y a su vez un mejor uso del ancho banda junto con el ahorro de direccionamiento IPv4.

CAPÍTULO IV: EMULACIÓN DE LA INFRAESTRUCTURA

En la emulación a continuación propuesta se busca tener comunicación entre dos Data centers ampliamente separados geográficamente, uno de ellos ubicado en Quito y el otro de Guayaquil, para poder lograr esta comunicación se plantea el diagrama de red detallado en la Figura 6.

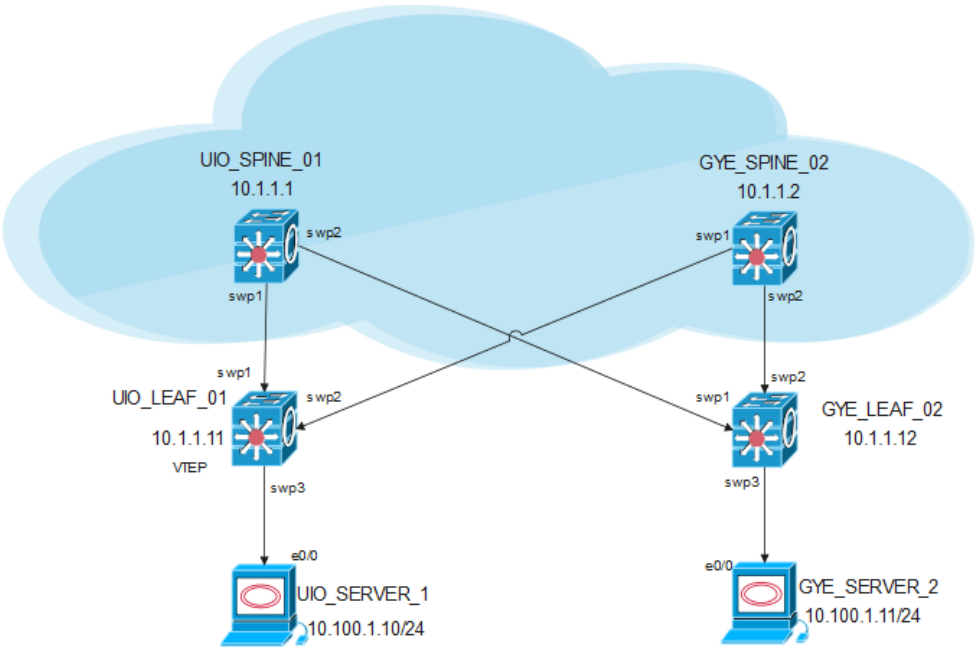


Figura 6 Topología de Red UIO-GYE
Fuente: Autor

En la topología propuesta se tiene dos equipos en la misma VLAN y no es necesario que se configure una dirección de Gateway (de forma lógica están en la misma subred), en la Figura 7 se detalla la VLAN de conexión entre ambos Data Centers.



Figura 7 VLAN entre Data Center UIO y Data Center GYE
Fuente: Autor

Sin embargo, a nivel de topología física, ambos equipos se comunican por medio de una red pública o privada WAN, misma que se encuentra formada por los equipos UIO_SPINES_01 y

GYE_SPINES_02, de igual manera se encuentran conectados en alta disponibilidad con los Leafs de cada Data Center como se puede observar en la Figura 8.

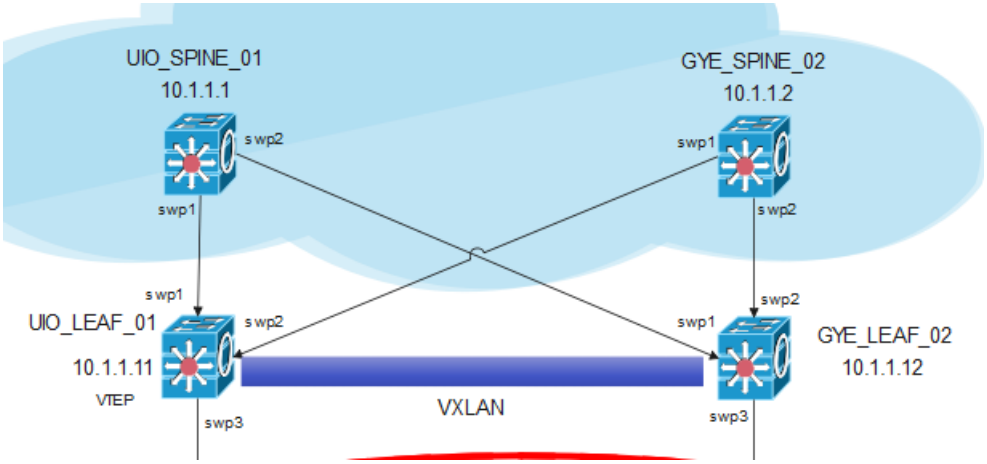


Figura 8. Conexión en AD entre Data Center UIO y Data Center GYE.
Fuente: Autor

Cuando un equipo de cualquiera de los dos data center envía información hacia un equipo ubicado en el otro data center, los datos llegan al Leaf que a su vez se convierte en un VTEP que genera un túnel de comunicación virtual entre los dos puntos (VXLAN), es decir de manera física el tráfico va hacia los Leafs y los Spines, pero lógicamente es como si ambos equipos estuvieran conectados por medio un solo switch (Figura 8). Esto genera ventajas de hiperconvergencia, las aplicaciones funcionan mucho más rápido, existe disminución de latencia de procesamiento y ahorro de direccionamiento IP.

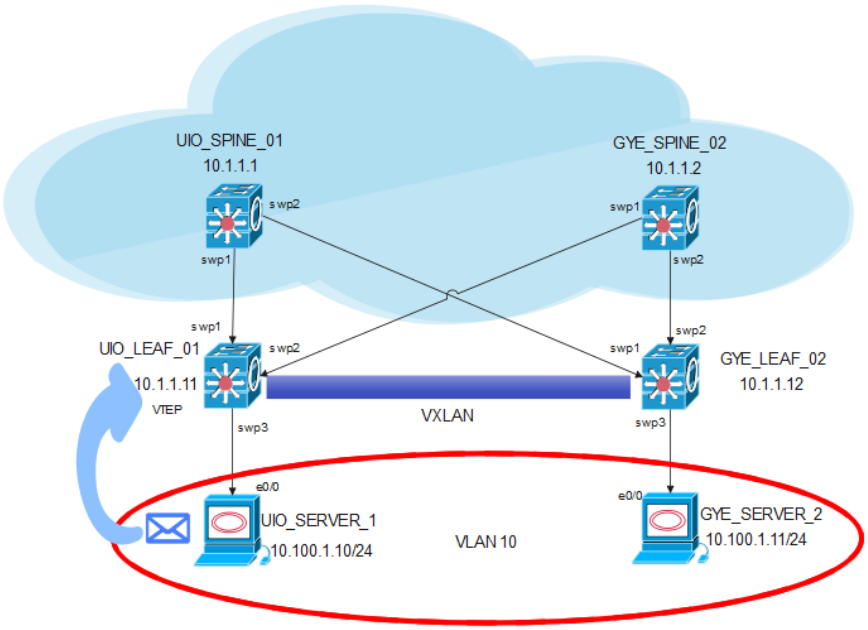


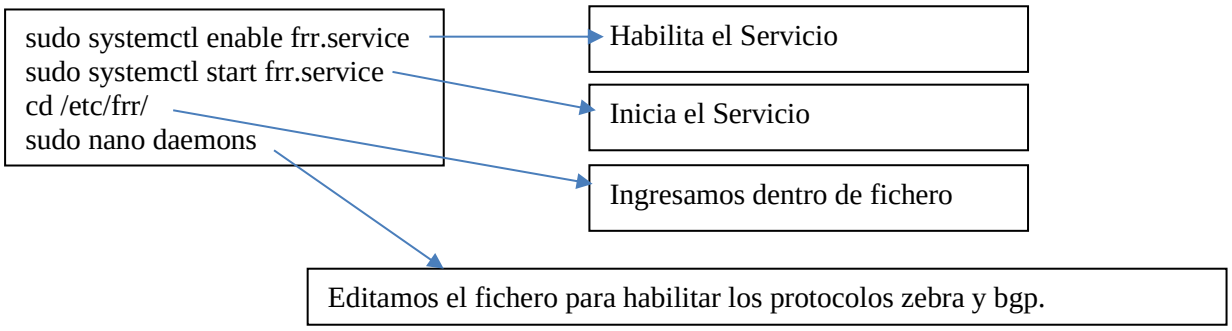
Figura 9 Envió de Paquetes por VXLAN.
Fuente: Autor

Al llegar de un VTEP hacia el otro VTEP, se desencapsula el tráfico quitando el encabezado de VXLAN y llegan los datos de un Data Center hacia otro.

4.1. Configuración de FRR (Free Range Routing)

Habilitar Servicio FRR para poder usar protocolos de enrutamiento. Esta es una característica típica de enrutamiento bajo equipos de Software Libre.

Para habilitar el servicio es necesario usar los siguientes comandos:



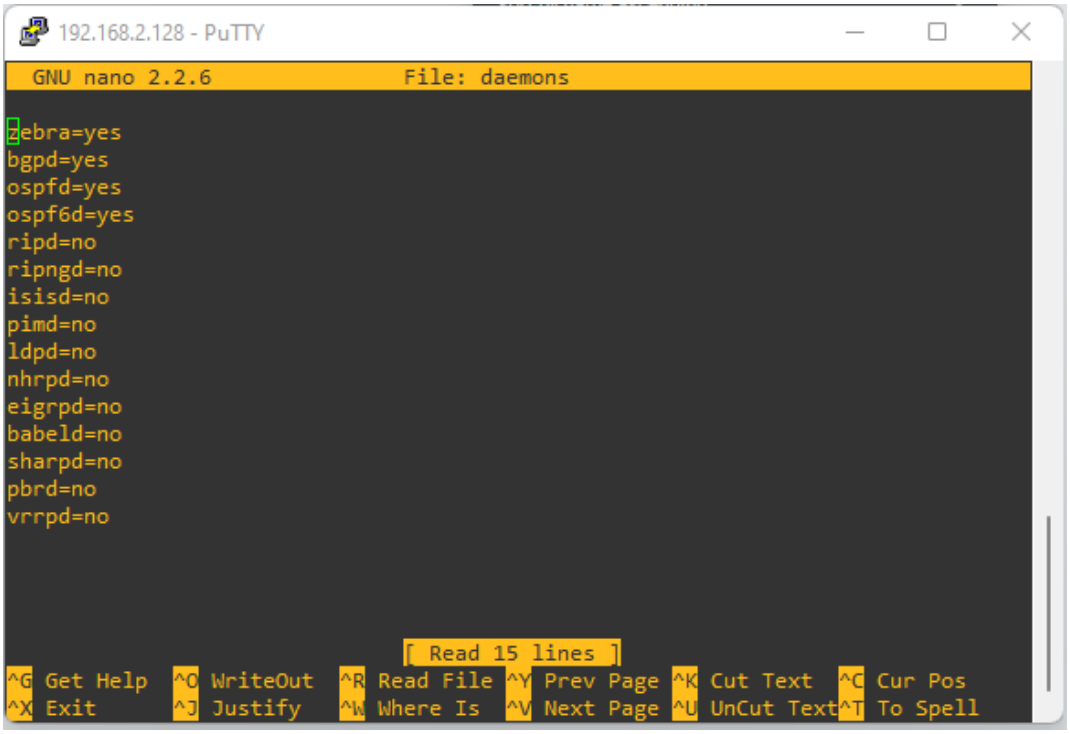


Figura 10 Habilitar zebra y bgpd.
Fuente: Autor

4.2. Configuración de Equipos Spines

UIO-SPINE01

```
net add hostname uio-spine01
net add interface swp1 ipv6 nd ra-interval 5
net del interface swp1 ipv6 nd suppress-ra
net add interface swp2 ipv6 nd ra-interval 5
net del interface swp2 ipv6 nd suppress-ra
net add loopback lo ip address 10.1.1.1/32
net add bgp autonomous-system 65000
net add bgp router-id 10.1.1.1
net add bgp bestpath as-path multipath-relax
net add bgp bestpath compare-routerid
net add bgp neighbor fabric peer-group
net add bgp neighbor fabric remote-as external
net add bgp neighbor fabric description Internal Fabric Network
net add bgp neighbor fabric capability extended-nexthop
net add bgp neighbor swp1 interface peer-group fabric
net add bgp neighbor swp2 interface peer-group fabric
net add bgp ipv4 unicast network 10.1.1.1/32
net add bgp ipv6 unicast neighbor fabric activate
net add bgp l2vpn evpn neighbor fabric activate
net add bgp l2vpn evpn advertise-all-vni
net commit
```

Código basado en (Davidson, 2019).

Tabla 2 Detalle de Comandos de Spine UIO

Comandos	Descripción
net add hostname uio-spine01	Comando para asignar nombre al equipo.
net add interface swp1 ipv6 nd ra-interval 5	Prepara la interfaz swp1 ipv6 nd
net del interface swp1 ipv6 nd suppress-ra	Elimina de la interfaz swp1 nd suppress-ra
net add loopback lo ip address 10.1.1.1/32	Asignamos dirección ip de loopback al equipo
net add bgp autonomous-system 65000	Asigna el valor de sistema autónomo de bgp
net add bgp router-id 10.1.1.1	Asigna id para el bgp
net add bgp bestpath as-path multipath-relax	Permite que tanto las rutas BGP como en la tabla de enrutamiento aparecen como las mejores.
net add bgp bestpath compare-routerid	Obliga a bgp a comparar por id de router
net add bgp neighbor fabric peer-group	Crea el grupo de vecinos fabric
net add bgp neighbor fabric remote-as external	Permisos de conexión remota o externa para el grupo fabric
net add bgp neighbor fabric description Internal Fabric Network	Asigna descripción al grupo fabric
net add bgp neighbor fabric capability extended-nexthop	Agrega capacidad de próximo salto extendido al grupo fabric
net add bgp neighbor swp1 interface peer-group fabric	Agrega la interfaz swp1 al grupo fabric

net add bgp neighbor swp2 interface peer-group fabric	Agrega la interfaz swp2 al grupo fabric
net add bgp ipv4 unicast network 10.1.1.1/32	Asigna dirección unicast ipv4
net add bgp ipv6 unicast neighbor fabric actívate	Activa el dirección unicast ipv6 para el grupo fabric
net add bgp l2vpn evpn neighbor fabric actívate	Active distribución de EVPN entre vecinos del grupo fabric
net add bgp l2vpn evpn advertise-all-vni	Habilita evpn para todos los VNI
net commit	Graba las configuraciones

GYE-SPINE02

```
net add hostname gye-spine02
net add interface swp1 ipv6 nd ra-interval 5
net del interface swp1 ipv6 nd suppress-ra
net add interface swp2 ipv6 nd ra-interval 5
net del interface swp2 ipv6 nd suppress-ra
net add loopback lo ip address 10.1.1.2/32
net add bgp autonomous-system 65000
net add bgp router-id 10.1.1.2
net add bgp bestpath as-path multipath-relax
net add bgp bestpath compare-routerid
net add bgp neighbor fabric peer-group
net add bgp neighbor fabric remote-as external
net add bgp neighbor fabric description Internal Fabric Network
net add bgp neighbor fabric capability extended-nexthop
net add bgp neighbor swp1 interface peer-group fabric
net add bgp neighbor swp2 interface peer-group fabric
net add bgp ipv4 unicast network 10.1.1.2/32
net add bgp ipv6 unicast neighbor fabric activate
net add bgp l2vpn evpn neighbor fabric activate
net add bgp l2vpn evpn advertise-all-vni
net commit
```

Código basado en (Davidson, 2019).

4.3. Configuración Leafs

UIO-LEAF01

```
net add hostname uio-leaf01
net add interface swp1 ipv6 nd ra-interval 5
net del interface swp1 ipv6 nd suppress-ra
net add interface swp2 ipv6 nd ra-interval 5
net del interface swp2 ipv6 nd suppress-ra
net add loopback lo ip address 10.1.1.11/32
net add interface swp3 bridge access 10
net add bgp autonomous-system 65010
net add bgp router-id 10.1.1.11
net add bgp bestpath as-path multipath-relax
net add bgp bestpath compare-routerid
net add bgp neighbor fabric peer-group
net add bgp neighbor fabric remote-as external
net add bgp neighbor fabric description Internal Fabric Network
net add bgp neighbor fabric capability extended-nexthop
net add bgp neighbor swp1 interface peer-group fabric
net add bgp neighbor swp2 interface peer-group fabric
net add bgp ipv4 unicast network 10.1.1.11/32
net add bgp ipv6 unicast neighbor fabric activate
net add bgp l2vpn evpn neighbor fabric activate
net add bgp l2vpn evpn advertise-all-vni
net add vxlan vni-10 vxlan id 10
net add vxlan vni-10 vxlan local-tunnelip 10.1.1.11
net add vxlan vni-10 bridge access 10
net commit
```

Código basado en (Davidson, 2019).

Tabla 3 Detalle de Comando Leaf UIO

Comandos	Descripción
net add hostname uio-leaf01	Asigna el nombre al host hoja
net add interface swp1 ipv6 nd ra-interval 5	Prepara la interfaz swp1 ipv6 nd
net del interface swp1 ipv6 nd suppress-ra	Elimina de la interfaz swp1 nd suppress-ra
net add interface swp2 ipv6 nd ra-interval 5	Prepara la interfaz swp2 ipv6 nd
net del interface swp2 ipv6 nd suppress-ra	Elimina de la interfaz swp2 nd suppress-ra
net add loopback lo ip address 10.1.1.11/32	Crea una dirección de loopback
net add interface swp3 bridge access 10	Propaga la VLAN 10 por la interfaz swp3
net add bgp autonomous-system 65010	Asigna el sistema autónomo para bgp
net add bgp router-id 10.1.1.11	Asigna el id para bgp
net add bgp bestpath as-path multipath-relax	Permite que tanto las rutas BGP como en la tabla de enrutamiento aparecen como las mejores.
net add bgp bestpath compare-routerid	Obliga a bgp a comparar por id de router
net add bgp neighbor fabric peer-group	Agrega el grupo de vecinos fabric
net add bgp neighbor fabric remote-as external	Permisos de conexión remota o externa para el grupo fabric

net add bgp neighbor fabric description Internal Fabric Network	Asigna descripción al grupo fabric
net add bgp neighbor fabric capability extended-nexthop	Agrega capacidad de próximo salto extendido al grupo fabric
net add bgp neighbor swp1 interface peer-group fabric	Agrega la interfaz swp1 al grupo fabric
net add bgp neighbor swp2 interface peer-group fabric	Agrega la interfaz swp2 al grupo fabric
net add bgp ipv4 unicast network 10.1.1.11/32	Asigna dirección unicast ipv4
net add bgp ipv6 unicast neighbor fabric activate	Activa el dirección unicast ipv6 para el grupo fabric
net add bgp l2vpn evpn neighbor fabric activate	Active distribución de EVPN entre vecinos del grupo fabric
net add bgp l2vpn evpn advertise-all-vni	Habilita EVPN para todos los VNI
net add vxlan vni-10 vxlan id 10	Se crea VXLAN con VNI-10 y el id 10
net add vxlan vni-10 vxlan local-tunnelip 10.1.1.11	Asigna la dirección ip de loopback del túnel para el envió de VXLAN
net add vxlan vni-10 bridge access 10	Asigna el túnel VXLAN para el id 10
net commit	Graba las configuraciones

GYE-LEAF02

```
net add hostname gye-leaf02
net add interface swp1 ipv6 nd ra-interval 5
net del interface swp1 ipv6 nd suppress-ra
net add interface swp2 ipv6 nd ra-interval 5
net del interface swp2 ipv6 nd suppress-ra
net add loopback lo ip address 10.1.1.12/32
net add interface swp3 bridge access 11
net add bgp autonomous-system 65011
net add bgp router-id 10.1.1.12
net add bgp bestpath as-path multipath-relax
net add bgp bestpath compare-routerid
net add bgp neighbor fabric peer-group
net add bgp neighbor fabric remote-as external
net add bgp neighbor fabric description Internal Fabric Network
net add bgp neighbor fabric capability extended-nexthop
net add bgp neighbor swp1 interface peer-group fabric
net add bgp neighbor swp2 interface peer-group fabric
net add bgp ipv4 unicast network 10.1.1.12/32
net add bgp ipv6 unicast neighbor fabric activate
net add bgp l2vpn evpn neighbor fabric activate
net add bgp l2vpn evpn advertise-all-vni
net add vxlan vni-10 vxlan id 10
net add vxlan vni-10 vxlan local-tunnelip 10.1.1.12
net add vxlan vni-10 bridge access 11
net commit
```

Código basado en (Davidson, 2019).

CAPÍTULO V: ANALISIS DE FACTIBILIDAD DE LA EMULACIÓN

En este capítulo se comprueba la teoría de VXLAN usando el emulador GNS3-VM con la solución de Open Networking Cumulus Linux. Se genera la topología para comunicar las agencias de Quito y Guayaquil (separación geográfica de los Datacenters) con un diseño de red Spine-Leaf, donde los Spines y los Leafs deben estar conectados en alta disponibilidad como lo muestra la Figura 9. Los Spines no se deben conectar entre sí, evitando así bucles físicos.

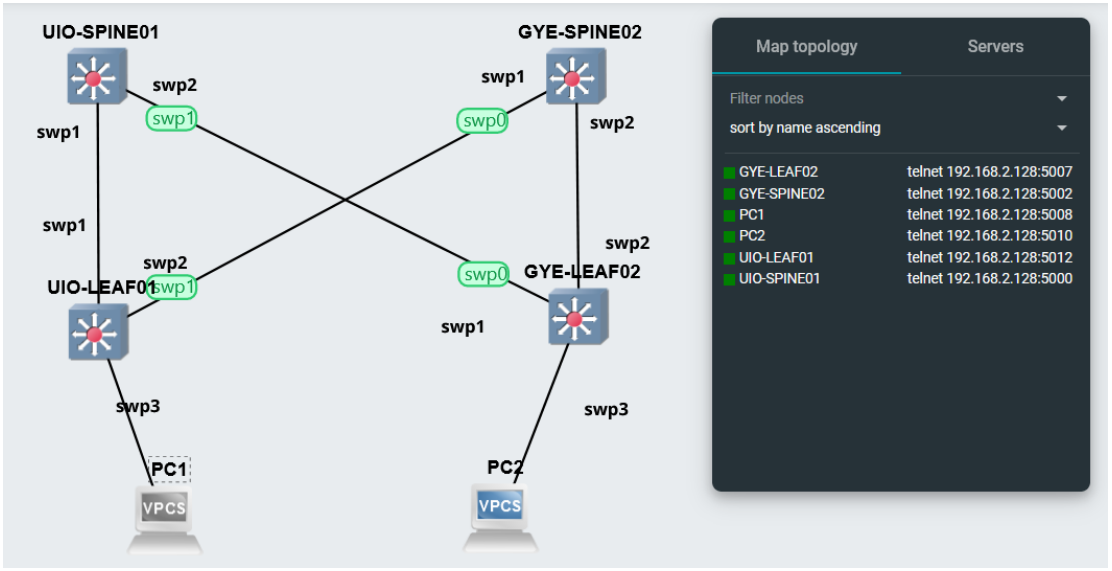


Figura 11 Topología UIO-GYE
Fuente: Autor

Con la topología generada y realizada la configuración en los Spines y los Leafs se evidencia el envío del tráfico desde PC1 a PC2 (Figura 10) y de PC2 a PC1 (Figura 11).

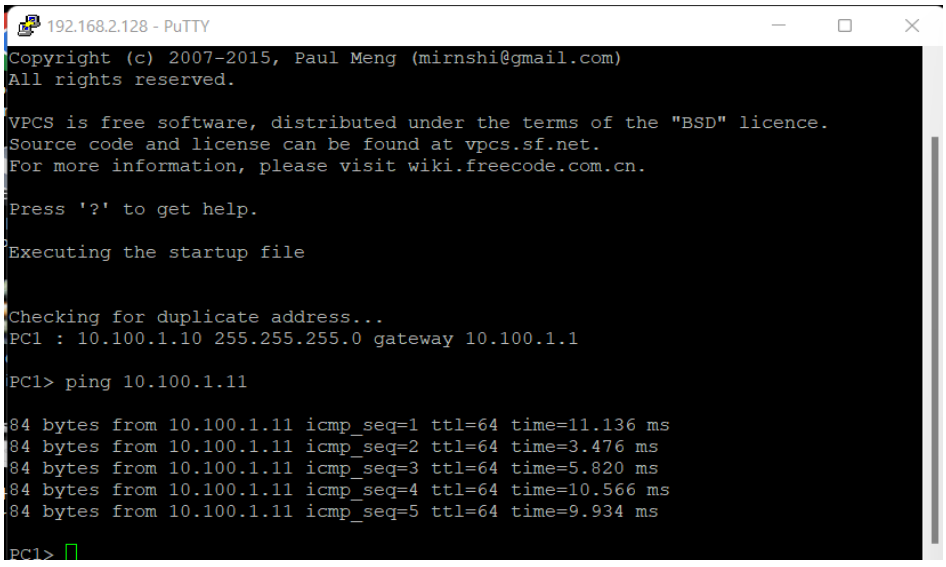


Figura 12 Ping PC1-PC2
Fuente: Autor

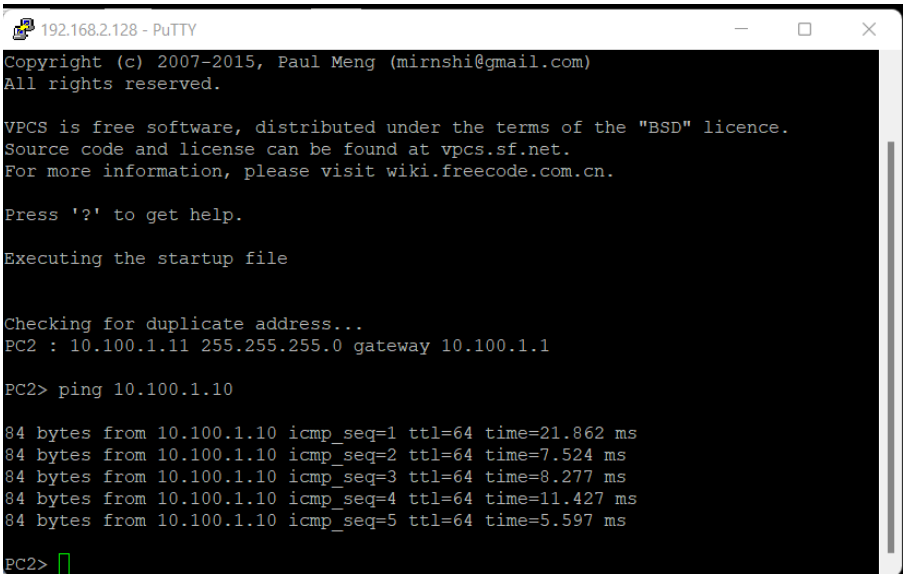


Figura 13 Ping PC2- PC1
Fuente: Autor

Prueba de Wireshark

Para validar el encapsulamiento de VXLAN, es necesario el uso de Wireshark, sin embargo, para hacer esta captura de paquetes es necesario la descarga de GNS3 (a nivel de software) y a su vez que tanto la versión de la máquina virtual de GNS3 como la aplicación GNS3-VM instalada sean la misma.

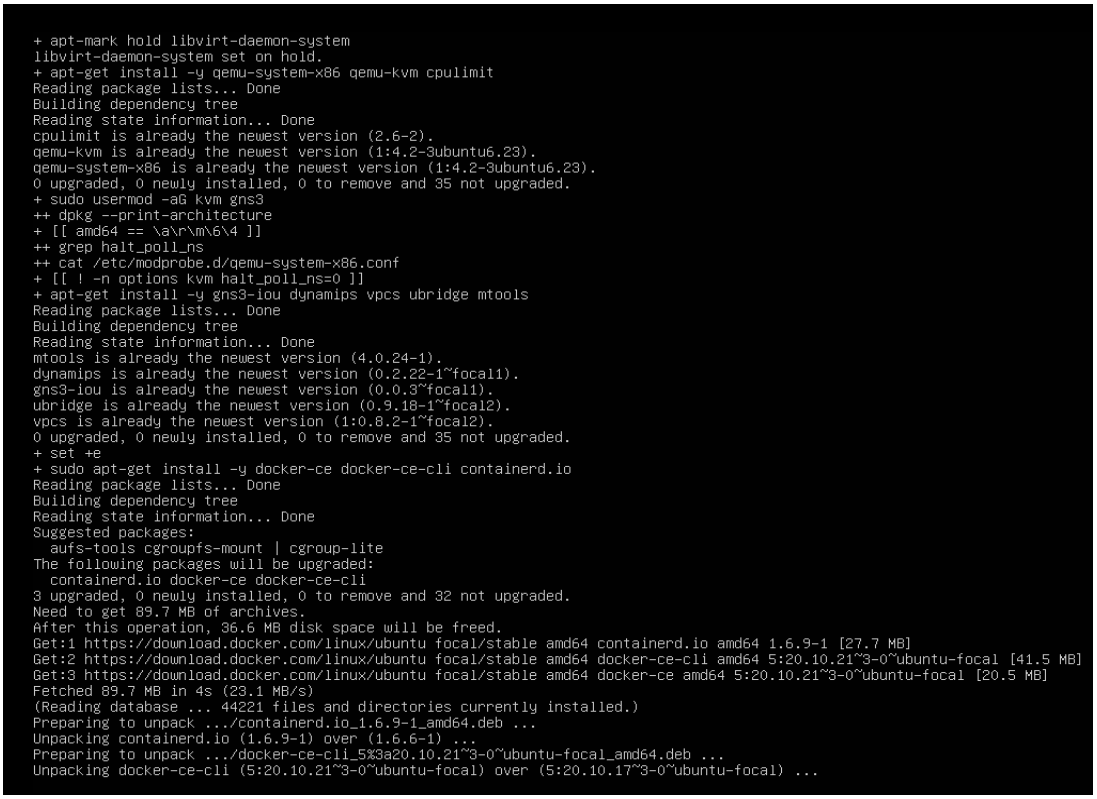


Figura 14 Actualización de versión de GNS3 en máquina virtual.
Fuente: Autor

Una vez que ambos GNS3 estén en la misma versión podemos exportar la topología configurada desde el terminal de la máquina virtual de GNS3 VM como se muestra en la Figura 13.

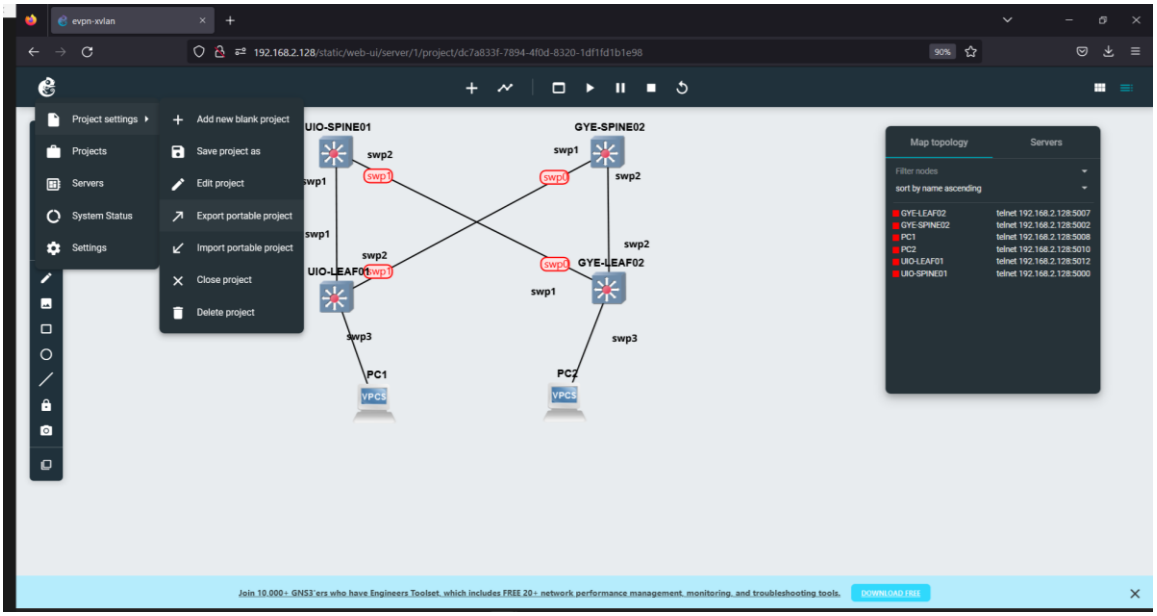


Figura 15 Exportación de Emulación VXLAN.
Fuente: Autor

Una vez levantada la emulación en GNS3 realizamos una captura de ping para poder validar el tráfico VXLAN como se evidencia en la Figura 15 donde se evidencia el VNI 10.

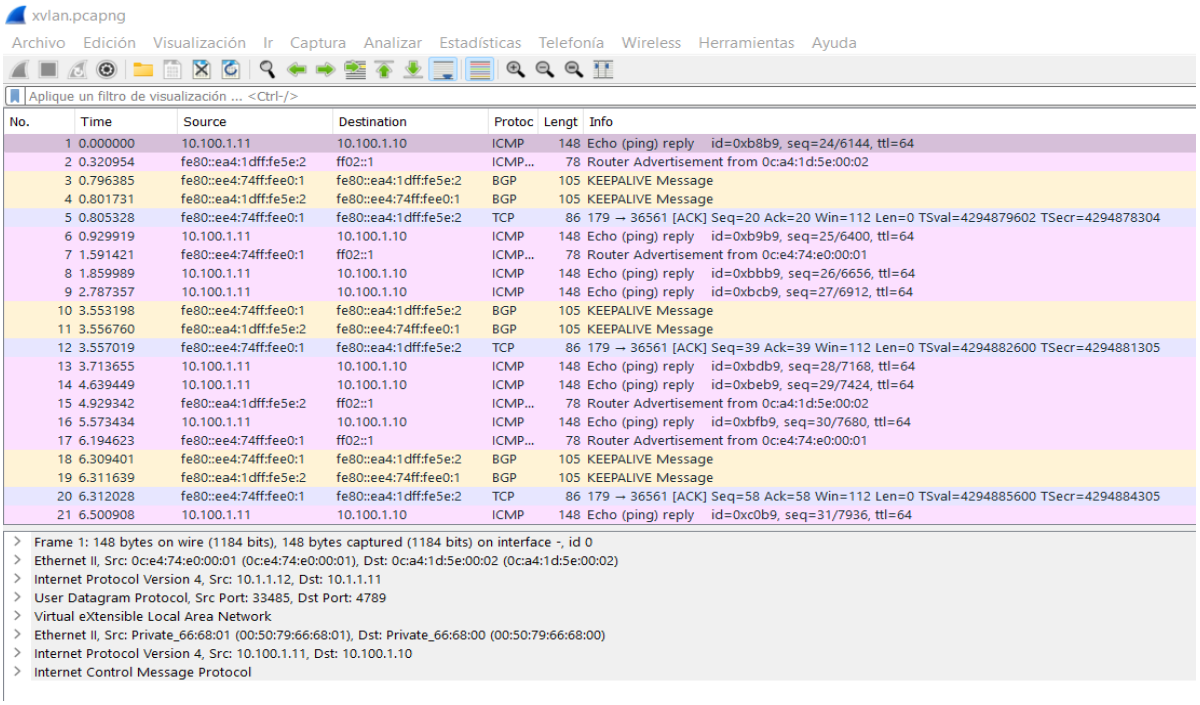


Figura 16 Captura de paquete XVLAN.
Fuente: Autor

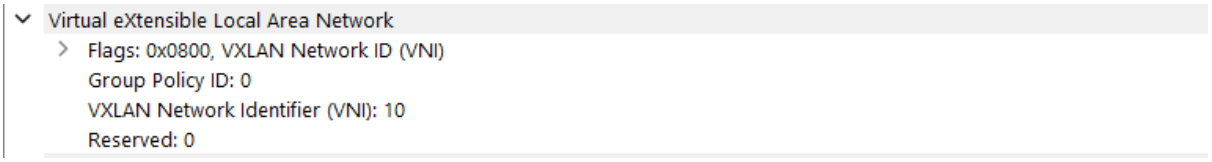


Figura 17 Validación de tráfico VXLAN.
Fuente: Autor

CONCLUSIONES

Luego de un análisis se puede concluir que VXLAN-EVPN es una solución que permite a una organización comunicar sus redes (data centers) generando ventajas considerables, tomando en cuenta que es un túnel inteligente que se crea bajo petición generando ventajas considerables que le permiten generar soluciones hiperconvergentes de bajo consumo de recursos.

Mediante la emulación se evidencia que topología Spine Leaf está diseñada para soluciones de tráfico este-oeste permitiendo una alta disponibilidad para los aplicativos de una organización, los data center modernos necesitan soportar aplicaciones con alta demanda de usuarios y que a su vez permitan una hiperconvergencia que le permita al usuario un acceso rápido y seguro.

Podemos concluir que Cumulus Linux es una solución de Open Networking que permite generar soluciones de Networking robustas y modernas a un menor costo, con un recupero de inversión a corto plazo, adicional a esto se encuentra respaldada por NVIDIA lo que genera una mayor confianza al momento de diseñar una red en un ambiente de Open Networking.

La emulación generada permite verificar todas las ventajas del uso de VXLAN-EVPN, al mismo tiempo evidencia con el uso de Cumulus Linux que con Open Networking se puede dar soluciones potentes y modernas capaces de soportar incluso una interconexión entre dos data centers ubicados en diferentes localidades y por una misma VLAN, ahorrando de esa manera direccionamiento IP, mejora en el desempeño de las aplicaciones y mayor control del tráfico.

RECOMENDACIONES

Para la instalación de la máquina virtual de GNS3 es necesario primero habilitar la virtualización en la BIOS del equipo, tomando en cuenta también que es necesario mantener habilitada la opción *Virtualize Intel VT-x/EPT* para poder hacer uso de las imágenes de los equipos a configurar.

Al momento de configurar los equipos para no hacer la configuración línea por línea es recomendable el uso de Putty haciendo el uso de la dirección IP y puerto que se detalla en el mapa de la topología.

Se recomienda al momento de emplear el Software de Interfaz gráfica de GNS3 junto con GNS3-VM, que tanto el software como la Máquina Virtual tengan la misma versión para que al integrarse no existan conflictos.

REFERENCIAS

Aruba. (2022). Obtenido de https://www.arubanetworks.com/faq/what-is-spine-leaf-architecture/

Ch, G. D. S., Naranjo, E. F., & Marrone, L. (2018). SDN-Ready WAN networks: Segment Routing in MPLS-Based Environments. In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)(pp. 173-178)

Davidson, J. (05 de 10 de 2019). *JD NETWORKS*. Obtenido de https://jdnetworks.co.uk/blog/2019/10/05/labbing-a-modern-datacentre/gns3. (2021).

Juniper Networks. (2021). *Guía de usuario EVPN*. Obtenido de https://www.juniper.net/documentation/mx/es/software/junos/evpn-vxlan/topics/topic-map/sdn-vxlan.html

Juniper Networks. (2022). *Juniper*. Obtenido de https://www.juniper.net/documentation/mx/es/software/junos/evpnvxlan/topics/concept/evpn-vxlan-data-plane-encapsulation.html

Juniper Networks. (2022). *Juniper*. Obtenido de https://www.juniper.net/documentation/mx/es/software/junos/evpn-vxlan/topics/topic map/sdn-vxlan.html

Juniper Networks. (s.f.). *What is EVPN-VXLAN?* Obtenido de https://www.juniper.net/us/en/research-topics/what-is-evpn-vxlan.html

Naranjo, E. F., & Ch, G. D. S. (2017, October). Underlay and overlay networks: The approach to solve addressing and segmentation problems in the new networking era: VXLAN encapsulation with Cisco and open source networks. In *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)* (pp. 1-6). IEEE

NVIDIA. (2022). *The World's Most Flexible Network Operating System.* Obtenido de https://nvdam.widen.net/s/sbkdzsrtpv/ethernet-switches-data-sheet-cumulus-linux-updates-2279601

Salazar-Chacon, G., & Marrone, L. (2022, October). Open Networking for Modern Data Centers Infrastructures: VXLAN Proof-of-Concept Emulation using LNV and EVPN under Cumulus Linux. In *2022 IEEE Sixth Ecuador Technical Chapters Meeting (ETCM)* (pp. 1-6). IEEE

Salazar Chacón, G. D. (2021). *Hybrid Networking SDN y SD-WAN: Interoperabilidad de arquitecturas de redes tradicionales y redes definidas por software en la era de la digitalización* (Doctoral dissertation, Universidad Nacional de La Plata).

Salazar-Chacón, G., Naranjo, E., & Marrone, L. (2020). Open networking programmability for VXLAN Data Centre infrastructures: Ansible and Cumulus Linux feasibility study. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E32), 469-482.

Salazar-Chacón, G. D. (2020, October). VXLAN-IPSec Dual-Overlay as a Security Technique in Virtualized Datacenter Environments. In *2020 IEEE ANDESCON* (pp. 1-6). IEEE

Salazar-Chacón, G. D., & Marrone, L. (2020, November). OpenSDN Southbound Traffic Characterization: Proof-of-Concept Virtualized SDN-Infrastructure. In *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 0282-0287). IEEE

ANEXOS

Configuraciones completas de Equipos de Red.

UIO-SPINE01

```
net add hostname uio-spine01
net add interface swp1 ipv6 nd ra-interval 5
net del interface swp1 ipv6 nd suppress-ra
net add interface swp2 ipv6 nd ra-interval 5
net del interface swp2 ipv6 nd suppress-ra
net add loopback lo ip address 10.1.1.1/32
net add bgp autonomous-system 65000
net add bgp router-id 10.1.1.1
net add bgp bestpath as-path multipath-relax
net add bgp bestpath compare-routerid
net add bgp neighbor fabric peer-group
net add bgp neighbor fabric remote-as external
net add bgp neighbor fabric description Internal Fabric Network
net add bgp neighbor fabric capability extended-nexthop
net add bgp neighbor swp1 interface peer-group fabric
net add bgp neighbor swp2 interface peer-group fabric
net add bgp ipv4 unicast network 10.1.1.1/32
net add bgp ipv6 unicast neighbor fabric activate
net add bgp l2vpn evpn neighbor fabric activate
net add bgp l2vpn evpn advertise-all-vni
net commit
```

GYE-SPINE02

```
net add hostname gye-spine02
net add interface swp1 ipv6 nd ra-interval 5
net del interface swp1 ipv6 nd suppress-ra
net add interface swp2 ipv6 nd ra-interval 5
net del interface swp2 ipv6 nd suppress-ra
net add loopback lo ip address 10.1.1.2/32
net add bgp autonomous-system 65000
net add bgp router-id 10.1.1.2
net add bgp bestpath as-path multipath-relax
net add bgp bestpath compare-routerid
net add bgp neighbor fabric peer-group
net add bgp neighbor fabric remote-as external
net add bgp neighbor fabric description Internal Fabric Network
net add bgp neighbor fabric capability extended-nexthop
net add bgp neighbor swp1 interface peer-group fabric
net add bgp neighbor swp2 interface peer-group fabric
net add bgp ipv4 unicast network 10.1.1.2/32
net add bgp ipv6 unicast neighbor fabric activate
net add bgp l2vpn evpn neighbor fabric activate
net add bgp l2vpn evpn advertise-all-vni
net commit
```

UIO-LEAF01

```
net add hostname uio-leaf01
net add interface swp1 ipv6 nd ra-interval 5
net del interface swp1 ipv6 nd suppress-ra
net add interface swp2 ipv6 nd ra-interval 5
net del interface swp2 ipv6 nd suppress-ra
net add loopback lo ip address 10.1.1.11/32
```

net add interface swp3 bridge access 10
net add bgp autonomous-system 65010
net add bgp router-id 10.1.1.11
net add bgp bestpath as-path multipath-relax
net add bgp bestpath compare-routerid
net add bgp neighbor fabric peer-group
net add bgp neighbor fabric remote-as external
net add bgp neighbor fabric description Internal Fabric Network
net add bgp neighbor fabric capability extended-nexthop
net add bgp neighbor swp1 interface peer-group fabric
net add bgp neighbor swp2 interface peer-group fabric
net add bgp ipv4 unicast network 10.1.1.11/32
net add bgp ipv6 unicast neighbor fabric activate
net add bgp l2vpn evpn neighbor fabric activate
net add bgp l2vpn evpn advertise-all-vni
net add vxlan vni-10 vxlan id 10
net add vxlan vni-10 vxlan local-tunnelip 10.1.1.11
net add vxlan vni-10 bridge access 10
net commit

GYE-LEAF02

net add hostname gye-leaf02
net add interface swp1 ipv6 nd ra-interval 5
net del interface swp1 ipv6 nd suppress-ra
net add interface swp2 ipv6 nd ra-interval 5
net del interface swp2 ipv6 nd suppress-ra
net add loopback lo ip address 10.1.1.12/32
net add interface swp3 bridge access 11
net add bgp autonomous-system 65011
net add bgp router-id 10.1.1.12
net add bgp bestpath as-path multipath-relax
net add bgp bestpath compare-routerid
net add bgp neighbor fabric peer-group
net add bgp neighbor fabric remote-as external
net add bgp neighbor fabric description Internal Fabric Network
net add bgp neighbor fabric capability extended-nexthop
net add bgp neighbor swp1 interface peer-group fabric
net add bgp neighbor swp2 interface peer-group fabric
net add bgp ipv4 unicast network 10.1.1.12/32
net add bgp ipv6 unicast neighbor fabric activate
net add bgp l2vpn evpn neighbor fabric activate
net add bgp l2vpn evpn advertise-all-vni
net add vxlan vni-10 vxlan id 10
net add vxlan vni-10 vxlan local-tunnelip 10.1.1.12
net add vxlan vni-10 bridge access 11
net commit