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 Redes de Comunicaciones

ANÁLISIS DE FACTIBILIDAD DE UNA ARQUITECTURA DE DATA CENTER MODERNO PARA LA ADMINISTRACIÓN Y APROVISIONAMIENTO DE CLIENTES BASADO EN PROTOCOLOS VXLAN CON EVPN GARANTIZANDO LA CONECTIVIDAD SITE TO SITE.

Autor: Ingrid Elizabeth Falconí León

Director: PhD. Gustavo Salazar Chacón

Quito, octubre 2023

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

DECLARACIÓN Y AUTORIZACIÓN

Yo, INGRID ELIZABETH FALCONÍ LEÓN, con C.I 1003119094, autor del trabajo de graduación titulado: **"ANÁLISIS DE FACTIBILIDAD DE UNA ARQUITECTURA DE DATA CENTER MODERNO PARA LA ADMINISTRACIÓN Y APROVISIONAMIENTO DE CLIENTES BASADO EN PROTOCOLOS VXLAN CON EVPN GARANTIZANDO LA CONECTIVIDAD SITE TO SITE"**, previa a la obtención del grado académico de MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES 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, octubre 2023

_____

INGRID ELIZABETH FALCONÍ LEÓN

C.I. 1003119094

APROBACIÓN DEL TUTOR

En mi carácter de Director del Trabajo de Posgrado Titulado: **"ANÁLISIS DE FACTIBILIDAD DE UNA ARQUITECTURA DE DATA CENTER MODERNO PARA LA ADMINISTRACIÓN Y APROVISIONAMIENTO DE CLIENTES BASADO EN PROTOCOLOS VXLAN CON EVPN GARANTIZANDO LA CONECTIVIDAD SITE TO SITE"**, presentado por el maestrante INGRID ELIZABETH FALCONÍ LEÓN, titular de la Cédula de Identidad Nº 1003119094 para optar al Grado de Magíster Tecnologías de la Información mención Redes de Comunicaciones, 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 24 días de octubre de 2023.

GUSTAVO DAVID SALAZAR CHACÓN C.I. 1716104797

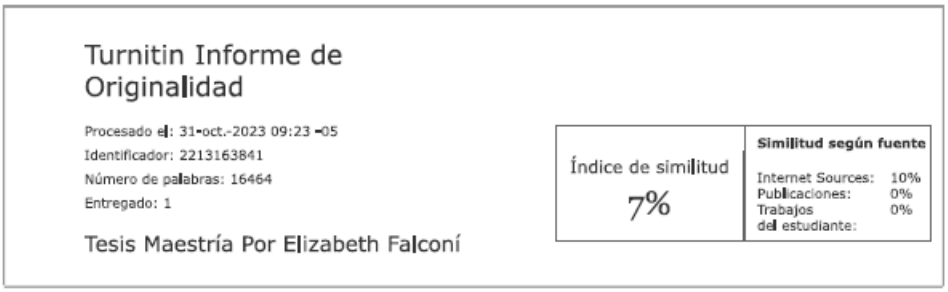
gsalazar787@puce.edu.ec

NOTA:

Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: 7% 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

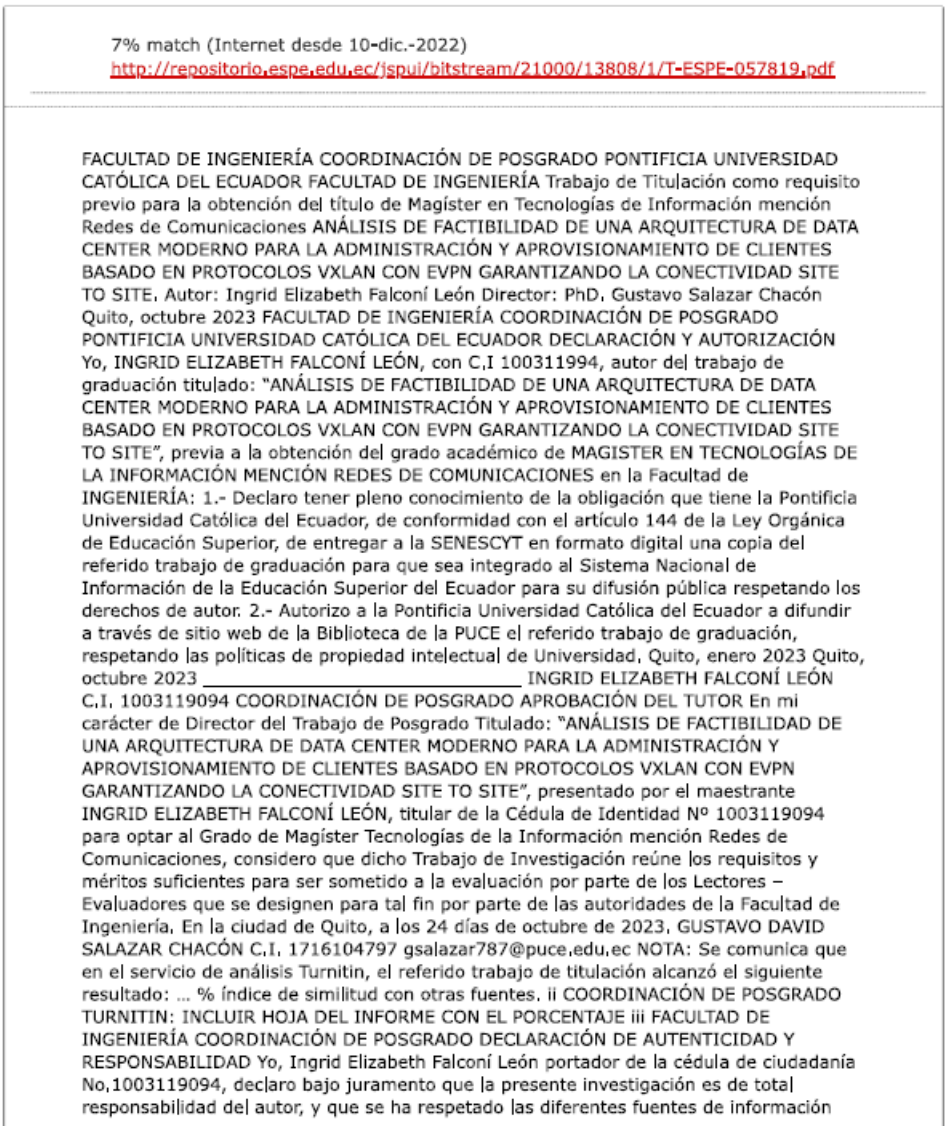


Turnitin Informe de Originalidad

Procesado el: 31-oct.-2023 09:23 -05
Identificador: 2213163841
Número de palabras: 16464
Entregado: 1

Tesis Maestría Por Elizabeth Falconí

Índice de similitud	Similitud según fuente	
7%	Internet Sources:	10%
	Publicaciones:	0%
	Trabajos del estudiante:	0%



7% match (Internet desde 10-dic.-2022)
http://repositorio.espe.edu.ec/jspui/bitstream/21000/13808/1/T-ESPE-057819.pdf

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 Redes de Comunicaciones ANÁLISIS DE FACTIBILIDAD DE UNA ARQUITECTURA DE DATA CENTER MODERNO PARA LA ADMINISTRACIÓN Y APROVISIONAMIENTO DE CLIENTES BASADO EN PROTOCOLOS VXLAN CON EVPN GARANTIZANDO LA CONECTIVIDAD SITE TO SITE. Autor: Ingrid Elizabeth Falconí León Director: PhD. Gustavo Salazar Chacón Quito, octubre 2023 FACULTAD DE INGENIERÍA COORDINACIÓN DE POSGRADO PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR DECLARACIÓN Y AUTORIZACIÓN Yo, INGRID ELIZABETH FALCONÍ LEÓN, con C.I 100311994, autor del trabajo de graduación titulado: "ANÁLISIS DE FACTIBILIDAD DE UNA ARQUITECTURA DE DATA CENTER MODERNO PARA LA ADMINISTRACIÓN Y APROVISIONAMIENTO DE CLIENTES BASADO EN PROTOCOLOS VXLAN CON EVPN GARANTIZANDO LA CONECTIVIDAD SITE TO SITE", previa a la obtención del grado académico de MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES 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 Quito, octubre 2023 _____ INGRID ELIZABETH FALCONÍ LEÓN C.I. 1003119094 COORDINACIÓN DE POSGRADO APROBACIÓN DEL TUTOR En mi carácter de Director del Trabajo de Posgrado Titulado: "ANÁLISIS DE FACTIBILIDAD DE UNA ARQUITECTURA DE DATA CENTER MODERNO PARA LA ADMINISTRACIÓN Y APROVISIONAMIENTO DE CLIENTES BASADO EN PROTOCOLOS VXLAN CON EVPN GARANTIZANDO LA CONECTIVIDAD SITE TO SITE", presentado por el maestrante INGRID ELIZABETH FALCONÍ LEÓN, titular de la Cédula de Identidad Nº 1003119094 para optar al Grado de Magíster Tecnologías de la Información mención Redes de Comunicaciones, 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 24 días de octubre 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. ii COORDINACIÓN DE POSGRADO TURNITIN: INCLUIR HOJA DEL INFORME CON EL PORCENTAJE iii FACULTAD DE INGENIERÍA COORDINACIÓN DE POSGRADO DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD Yo, Ingrid Elizabeth Falconí León portador de la cédula de ciudadanía No.1003119094, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se ha respetado las diferentes fuentes de información

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

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Ingrid Elizabeth Falconí León portador de la cédula de ciudadanía No.1003119094, 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.

_____

INGRID ELIZABETH FALCONÍ LEÓN
C.I. 1003119094

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

DEDICATORIA

A Dios, por ser mi fuerza, mi guía y mi soporte en cada etapa de mi vida. A mi familia, por el apoyo que me brindan en cada meta personal o profesional que me planteo. A mi padre Jorge por ser mi ejemplo de dedicación, superación y profesionalismo, por enseñarme a no rendirme y luchar por mis ideales, a mi hermano Ricardo por su apoyo constante en cada decisión, por ser la persona que me inspira a mejorar día con día y mi motor en los momentos difíciles; y especialmente quiero dedicar este momento de mi formación a mi madre Lorena, gracias por impulsarme a continuar preparándome académicamente y en mi crecimiento profesional, pero sobre todo gracias por tu bondad, humildad, amor y paciencia, gracias por ser el ángel que ilumina mi camino y por todo tu esfuerzo y dedicación, este título es totalmente tuyo.

AGRADECIMIENTOS

Agradezco A Dios por escuchar cada una de mis oraciones y permitirme llegar a este momento de mi formación profesional, porque mi fe en Él me reconforma y me permite lograr todo lo que me proponga.

A mi familia por brindarme siempre su apoyo, amor y paciencia, por el impulso que me dan para cumplir mis metas y por toda la ayuda que me brindan para hacer de cada momento más llevadero, gracias por ser mi fuerza y mi inspiración, por festejar cada uno de mis triunfos y por darme una mano en mis momentos difíciles, gracias por acompañarme en cada mala noche, por su constante preocupación y por la confianza que me dan día con día que hace que pueda alcanzar cada meta, cada sueño.

Gracias a mi mejor amiga, mi hermana, Barbie, que a pesar de la distancia me apoya en cada momento, gracias por siempre creer en mi y estar en cada momento de mi vida, por ser una verdadera amiga y hablarme con la verdad cuando lo necesito y darme tu guía en los momentos en los cuales me siento perdida, gracias por el amor y cariño, porque cuando siento que no puedo estás tu para recordarme de todo lo que soy capaz.

Gracias a mis mejores amigas Mich y Yes, por ser luz en mi vida, por ser incondicionales en cada momento, bueno o malo, por enseñarme lo que es una amistad verdadera y porque puedo contar con ustedes siempre, gracias por celebrar mis triunfos y secar mis lágrimas en mis momentos difíciles, simplemente gracias por todo su apoyo durante este proceso y por ser ángeles en mi camino.

De manera especial agradezco a mi director de tesis Dr. Gustavo Salazar por su apertura desde el primer día para desarrollar el presente trabajo de titulación y porque su trayectoria me ha inspirado a continuar preparándome profesionalmente. Gracias por su apoyo y guía.

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

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES

ANÁLISIS DE FACTIBILIDAD DE UNA ARQUITECTURA DE DATA CENTER MODERNO PARA LA ADMINISTRACIÓN Y APROVISIONAMIENTO DE CLIENTES BASADO EN PROTOCOLOS VXLAN CON EVPN GARANTIZANDO LA CONECTIVIDAD SITE TO SITE

Autor: Ingrid Elizabeth Falconí León

Director -Tutor: PhD. Gustavo Salazar

Fecha: 24 de octubre del 2023

RESUMEN

El presente trabajo de titulación tiene dos componentes principales, los cuales se encuentran estrechamente ligados y que permiten tener una visión de la importancia de la investigación. En primer lugar, se llevará a cabo un análisis comparativo entre la arquitectura moderna y la arquitectura tradicional que ha sido previamente empleada en los centros de datos. Esta distinción entre las dos arquitecturas permitirá tomar decisiones adecuadas en la implementación, adaptándolas a las necesidades y recursos disponibles en los centros de datos. El segundo aspecto a considerar, se refiere a la tecnología utilizada en la configuración de la arquitectura de un centro de datos, con un enfoque en examinar su estructura y funcionamiento. En este caso, se prestará especial atención a VXLAN con EVPN, una tecnología que asegura la conectividad site to site.

Una emulación en un entorno virtualizado permitirá observar las ventajas de VXLAN con EVPN; y en base a los resultados obtenidos, el presente trabajo de titulación podrá abrir campo a futuras investigaciones y propuestas para la administración de clientes, proveedores de servicios, cloud computing en los centros de datos.

Palabras clave:
VXLAN, EVPN, Arquitectura, Centros de Datos.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES

FEASIBILITY ANALYSIS OF A MODERN DATA CENTER ARCHITECTURE FOR CUSTOMER MANAGEMENT AND PROVISIONING BASED ON VXLAN PROTOCOLS WITH EVPN GUARANTEING SITE TO SITE CONNECTIVITY

Autor: Ingrid Elizabeth Falconí León

Director -Tutor: PhD. Gustavo Salazar

Date: October 4th, 2023

ABSTRACT

This degree work has two main components, which are closely linked and allow us to have a vision of the importance of the research. Firstly, a comparative analysis will be carried out between modern architecture and the traditional architecture that has previously been used in data centers. This distinction between the two architectures will allow appropriate decisions to be made in the implementation, adapting them to the needs and resources available in the data centers.

The second aspect to consider refers to the technology used in configuring the architecture of a data center, with a focus on examining its structure and operation. In this case, special attention will be paid to VXLAN with EVPN, a technology that ensures site-to-site connectivity.

An emulation in a virtualized environment will allow the advantages of VXLAN with EVPN to be observed; and based on the results obtained, this degree work may open the field for future research and proposals for the administration of clients, service providers, cloud computing in data centers.

Keywords:

VXLAN, EVPN, Architecture, Data Centers.

INTRODUCCIÓN

Un data center o centro de procesamiento de datos, corresponde a la ubicación física donde se alojan ordenadores, redes, almacenamiento y otros equipos de TI, un agrupamiento de recursos necesarios para soportar cualquier entorno comercial. En la actualidad, la infraestructura informática y las implementaciones modernas en los centros de datos demandan una alta disponibilidad, capacidad de escalabilidad rápida y un rendimiento superior, sin comprometer la funcionalidad. Como resultado de esta necesidad, las redes de los centros de datos están experimentando una evolución en su diseño. Se están alejando de las estructuras jerárquicas tradicionales y están adoptando arquitecturas tipo "spine and leaf", donde los hosts y los servicios se distribuyen de manera más eficiente a través de la red.

Estas redes son capaces de soportar el incremento cada vez mayor del flujo de tráfico en las aplicaciones modernas buscando así soluciones de red definidas por software. El trabajo en red debe evolucionar desde el modelo estático a un modelo flexible para poder dar soporte a las comunicaciones entre las aplicaciones sin importar donde se encuentren, Es aquí donde las redes overlay entran en escena.
Una alternativa es VXLAN con plano de control EVPN, la cual provee una solución flexible, escalable y administrable que soporta la creciente demanda de ambientes basados en la nube. La superposición de EVPN-VXLAN se basa en la infraestructura IP existente y amplía la conectividad de capa 2 entre diversos centros de datos. Esto conlleva mejoras notables en el rendimiento de la entrega de tráfico a los usuarios finales y en la capacidad de recuperación en situaciones de desastre.

La presente investigación pretende analizar la estructura y operación de la tecnología VXLAN con EVPN, mediante una emulación en un entorno virtualizado para demostrar las ventajas de VXLAN, garantizando la conectividad site to site; y con base en los resultados obtenidos, esta investigación podría utilizarse como propuesta para la administración y aprovisionamiento de proveedores de servicios y clientes del centro de datos (DC) en el futuro.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Formulación del problema

Durante un largo período, los centros de procesamiento de datos se han construido siguiendo una arquitectura de tres niveles. Todos estos niveles se han diseñado con redundancia y considerando principalmente el tráfico de norte a sur, es decir, desde el cliente hacia el servidor. Sin embargo, cuando el tráfico entre servidores, es decir, el tráfico este-oeste, es significativo, los dispositivos finales conectados al mismo puerto del switch pueden competir por el ancho de banda disponible, lo que puede resultar en un tiempo de respuesta deficiente para los usuarios. Esta limitación se vuelve especialmente problemática en los centros de datos modernos, donde el almacenamiento y los servidores de cómputo no necesariamente se encuentran en el mismo lugar físico. En la actualidad, a medida que las empresas migran hacia la nube, es cada vez más común que sus servidores estén ubicados en diferentes lugares, lo que hace que el tráfico este-oeste sea igualmente relevante y, en muchos casos, en crecimiento constante.

Con el acrecentado número de clientes, servidores, máquinas virtuales, se generan problemas relacionados con el tamaño de tablas de direcciones MAC y con el número limitado de VLANs que se puede usar; adicionalmente teniendo en cuenta el problema que supone usar STP (Spanning Tree Protocol), el cual permite evitar bucles en la capa de enlace malgastando muchos recursos, ya que de todos los posibles caminos que puede haber, solo se utiliza uno, comprometiendo en los centros de datos la conexión site to site y ata disponibilidad que se oferta a al momento de aprovisionar clientes, surge la necesidad de realizar la conexión de red mediante nuevos protocolos que permitan mitigar los problemas descritos como lo es VXLAN con EVPN.

Al momento se ha visualizado gran número de emulaciones de centros de procesamientos de datos con arquitectura tradicional, y así mismo con protocolos que limitan la escalabilidad en entornos de nube virtualizados, creando la necesidad de contar con una infraestructura física adicional, generando aumento en los costos de implementación y problemas con duplicidad en direcciones MAC lo que puede ocasionar problemas en la conexión de clientes. El desconocimiento de las ventajas presentadas por nuevas arquitecturas y protocolos impide que los centros de datos evolucionen y se ajusten a las cambiantes necesidades de sus clientes. Esto les impide aprovechar los beneficios que estas nuevas soluciones pueden brindar.

Conforme lo discutido previamente se puede identificar el siguiente problema principal:

No se cuenta con un análisis de factibilidad de una arquitectura de data center moderno para la administración y aprovisionamiento de clientes basado en protocolos VXLAN con EVPN garantizando la conectividad site to site.

Y los siguientes problemas secundarios:

Se carece de un análisis de la estructura y conceptos de la tecnología VXLAN con EVPN
No se cuenta con un modelo de arquitectura de Data Center moderno mediante un emulador de infraestructura de red.
No se garantiza la conectividad site to site para el aprovisionamiento de clientes en Data Center mediante protocolos VXLAN en una arquitectura de Data Center moderno

1.2. Objetivos de la Investigación

Objetivo General

Diseñar una arquitectura de data center moderno para la administración y aprovisionamiento de clientes basado en protocolos VXLAN con EVPN garantizando la conectividad site to site.

Objetivos Específicos

Analizar la estructura y conceptos de la tecnología VXLAN con EVPN
Modelar la arquitectura de Data Center moderno mediante un emulador de infraestructura de red.
Garantizar conectividad site to site para el aprovisionamiento de clientes en Data Center

1.3. Justificación de la Investigación

Las TI están evolucionando hacia un modelo de consumo en la nube. Esta transición afecta la forma en que se están diseñando e implementado las aplicaciones, lo que conduce a una evolución en el diseño de la infraestructura de los centros de datos para satisfacer estos requerimientos. Como base de los data center modernos, la red también debe tomar parte en

esta evolución, al mismo tiempo que existe un incremento en la virtualización de servidores y arquitecturas basadas en microservicios.

La evolución de la demanda de usuarios y requisitos de las aplicaciones sugieren un enfoque diferente que es simple y más ágil. La facilidad de aprovisionamiento y la velocidad constituyen métricas críticas de rendimiento de la infraestructura de red de los data centers que soportan ambientes físicos, virtualizados y de cloud; sin comprometer la escalabilidad o seguridad.
Gracias a las plataformas de virtualización, el uso de los Data Center Multitenant se ha incrementado. Actualmente, no se encuentran solo en grandes proveedores de servicio, sino que también son utilizados internamente como parte de infraestructuras de red para asignar a cada departamento un tenant diferente y de esa manera proveer de los servicios IT de una manera controlada y segura. Una forma tradicional de aprovisionar redes virtuales ha sido empleando el despliegue de arquitecturas overlay, las cuales implementan redes superpuesta, en otras que ya han sido creada a través de túneles entre los enlaces de los nodos overlay sobre una infraestructura establecida llamada underlay y mediante la encapsulación de paquetes.

La justificación para realizar el presente trabajo de investigación, consiste en dar a conocer la ventaja de migrar hacia nuevas topologías en la infraestructura de centros de datos, que permitan tener ventajas como reducir la cantidad de switches necesarios, mejorar el tráfico este-oeste mejorando significativamente el rendimiento en entornos de servidores virtualizados, dando pie a la nueva era en la cual la empresas migran sus servicios a la nube y reducen costos en la implementación física de centros de datos. La implementación de la tecnología VXLAN permitirá la superposición de redes para el transporte de tráfico brindando una solución al número limitado de VLANS con las que se puede trabajar con otras tecnologías.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de la Investigación

(JONATHAN MORENO, 2019) menciona en su trabajo: "Actualmente vemos como las grandes y medianas organizaciones migran sus servicios e infraestructura a Data Centers, se realiza con el objetivo de disminuir costos y recibir grandes beneficios (Disponibilidad, atención 7 x 24 x 365, mayor eficiencia, menor costo de operación, velocidad del negocio, opción de crecimiento y escalabilidad), las empresas están migrando su infraestructura a la nube y es cada vez más común que tengan sus servidores lejos, por lo cual el tráfico este-oeste crece al mismo ritmo, haciendo que la arquitectura tradicional se vuelva ineficiente en cuanto a rendimiento, escalabilidad y flexibilidad."

(T. Singh, V. Jain and G. S. Babu,2017) mencionan en su trabajo: "Con la evolución de la tecnología en la nube y el gran beneficio de la multitenencia, el requisito básico de la arquitectura de red ha cambiado por completo desde una perspectiva de Data Center único a múltiples Data Center en todas las ubicaciones para lograr una continuidad comercial perfecta. Esto ha requerido mejorar las tecnologías existentes y también implementar nuevas tecnologías con muchas características nuevas. Las tendencias que impulsan a los DC a rediseñar la red tienen tres objetivos en mente: Escalabilidad: la mayor dependencia del aislamiento de la red en un entorno de múltiples inquilinos ha previsto la necesidad de escalar las VLAN y la implementación de la nube en los DC geográficamente separados requirió tecnologías como VXLAN. Eficiencia operativa: a medida que la empresa expande sus operaciones en todo el mundo, deben abordarse los problemas que surgen debido a la distancia física entre los centros de distribución. La red DC debe soportar la movilidad de aplicaciones; las aplicaciones deben migrar sin problemas dentro de DC y entre DC para la continuidad del negocio. Las nuevas tecnologías como EVPN reducen la carga en los planos de datos y control y mejoran la eficiencia mediante la implementación de funciones como el aprendizaje remoto de MAC, lo que aumenta la eficiencia operativa y proporciona una continuidad comercial efectiva. Alto rendimiento: la adopción de la nube ha hecho que los DC reconsideren su arquitectura de red tanto a nivel intra como inter-DC. Requiere una convergencia y una agregación más rápidas de los enlaces que están disponibles mediante el uso de una capa subyacente basada en IP de capa 3 junto con una superposición VXLAN-EVPN."

(A. -E. Rădoi and C. -I. Rincu,2022) “La implementación de overlays en la red, como la red de área local extensible virtual (VXLAN) como plano de datos y el protocolo de puerta de enlace fronteriza/VPN Ethernet (BGP/EVPN) como plano de control para la distribución de red virtual, juega un papel importante en la integración de tecnologías VXLAN BGP EVPN en modernos Centros de Datos, permitiendo un mejor control de flujo sobre la red. En este sentido, se ha logrado la mejora de las redes dedicadas y, además, de las capacidades de conmutación y enrutamiento, reduciendo así los costes de implementación y gestión dispositivo a dispositivo hacia un sistema más centralizado e integrado. La nueva arquitectura de red, junto con sus protocolos relacionados, no solo para el plano de control, sino también para el plano de datos, ha demostrado la necesidad de reemplazar las arquitecturas y protocolos de red tradicionales, como el protocolo Spanning Tree y vPC.”

2.2. Bases Teóricas

2.2.1. Data Center

Un Data Center o centro de datos, es una instalación que proporciona acceso compartido a aplicaciones y datos mediante una infraestructura compleja de red, computación y almacenamiento. (Checkpoint, 2021)

Dichas instalaciones necesitan contar con los recursos necesarios para su correcto funcionamiento, como son: energía, ventilación y sistemas de seguridad avanzados para evitar fugas de datos u otros riesgos.

Así mismo, un centro de datos puede ofrecer alojamiento a empresas, esto con el fin de ahorrar recursos, equipos, y construcción de Centros de Datos. El housing ayudará a compilar, guardar y proteger toda su información e interconectarse con otros proveedores, manteniendo la seguridad y garantizando la continuidad del negocio. (TkmE Enviromental and Power Monitoring., 2017)

Las empresas especializadas que se dedican a brindar los servicios mencionados, deben contar con el espacio, equipo y almacenamiento necesario para poder resguardar la gran cantidad de data que pueden llegar a recibir, brindando además seguridad, confidencialidad y disponibilidad en la información.

Los principales beneficios de contratar un Data Center externo son:

- Reducción de costos: debido a que el centro de datos proveerá la infraestructura y equipamiento necesario para el correcto funcionamiento
- Tecnología: infraestructura moderna al alcance de pocas empresas, brindando mejor acceso a la data y mayor capacidad de procesamiento.
- Monitoreo: personal especializado para hacer frente ante una incidencia con soporte 24x7
- Conectividad: permitiendo acceso permanente a la data y alta disponibilidad a grandes velocidades
- Seguridad: garantizando la fiabilidad y confiabilidad de la data.
- Flexibilidad: al tener el servicio externalizado, no se realiza la inversión inicial en infraestructura y adicionalmente se pagará únicamente por los servicios que sean usado por la empresa.

2.2.2. Red de Data Center

Una red de Data Center es la infraestructura de comunicación utilizada en el Centro de Datos, y se describe por equipos de switching/routing, topologías de red y el uso de protocolos.

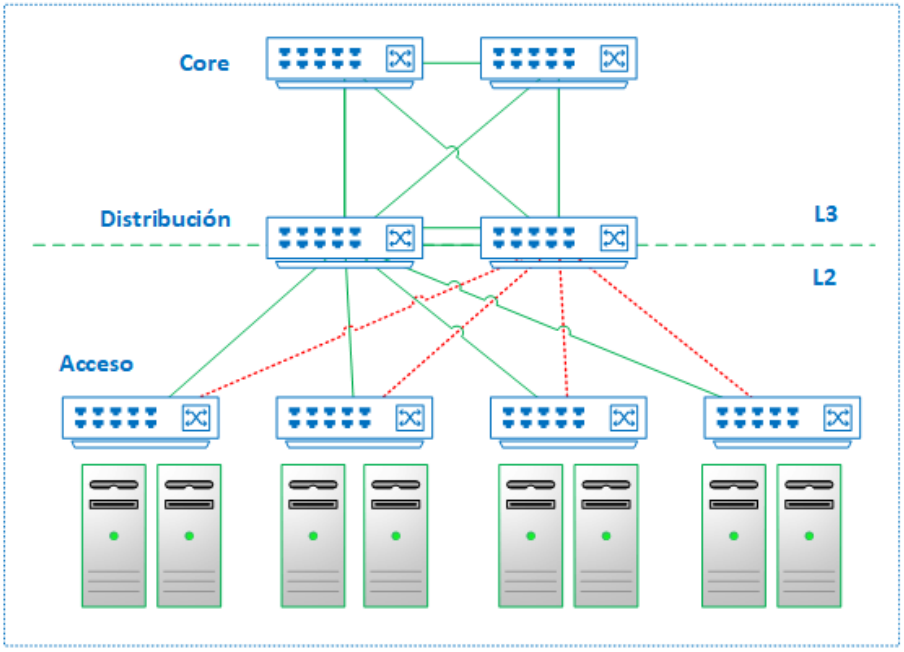


FIGURA 1 Topología común de una red de Data Center
Fuente: (Hernández, 2020)

Las arquitecturas típicas de Data Center, pueden consistir en dos o tres niveles constituidos por routers o switches. Un diseño de tres niveles está constituido por el nivel de core, agregación y Edge. En un diseño de dos niveles tienes solo la capa de core y Edge. Se desplegará mayor detalle de los tipos de arquitectura en los siguientes párrafos.

Durante muchos años la arquitectura Three-Tier fue fuertemente considerada en la implementación de los Centros de Datos, sin embargo, las limitaciones como su pobre escalabilidad y el alto costo en los equipos que conforman la misma, hicieron necesario buscar nuevas alternativas en la implementación de los nuevos y modernos Centros de Datos.

Los avances tecnológicos en la transmisión y almacenamiento de datos, el Cloud Computing, Big Data, IoT, han provocado que el tráfico entre los servidores (conocido como este - oeste) alcance alrededor de una 70% del total del tráfico generado en un Data Center, y el restante 30% corresponde al tráfico que entra y/o sale desde el Centro de Datos hacia Internet u otras WANs (conocido como norte - sur), tomando en cuenta lo antes mencionado, las arquitecturas han ido evolucionando para proveer mayor escalabilidad y eficiencia. (Zárate, 2017)

2.2.3. Arquitectura de Data Center

2.2.3.1. Arquitectura de 3 niveles

La arquitectura de tres niveles, ha sido la pionera y una de las más usadas en Centros de Datos debido a su robustez, diseño modular y buen rendimiento. Con los avances tecnológicos y debido a crecimiento exponencial que se ha tenido en los Data Center, el surgimiento de Cloud Computing, este tipo de arquitectura ya no es viable para grandes DC, por las implicaciones en costes altos y baja eficiencia y escalabilidad. En la actualidad, el almacenamiento y los servidores de cómputo no tienen por qué estar en el mismo lugar. Las empresas hoy en día están migrando su infraestructura a la nube y es cada vez más común que sus servidores se encuentren a mayor distancia geográfica, por lo cual el tráfico este – oeste crece al mismo ritmo. Los niveles que conforman esta arquitectura son la capa de CORE, distribución y acceso.

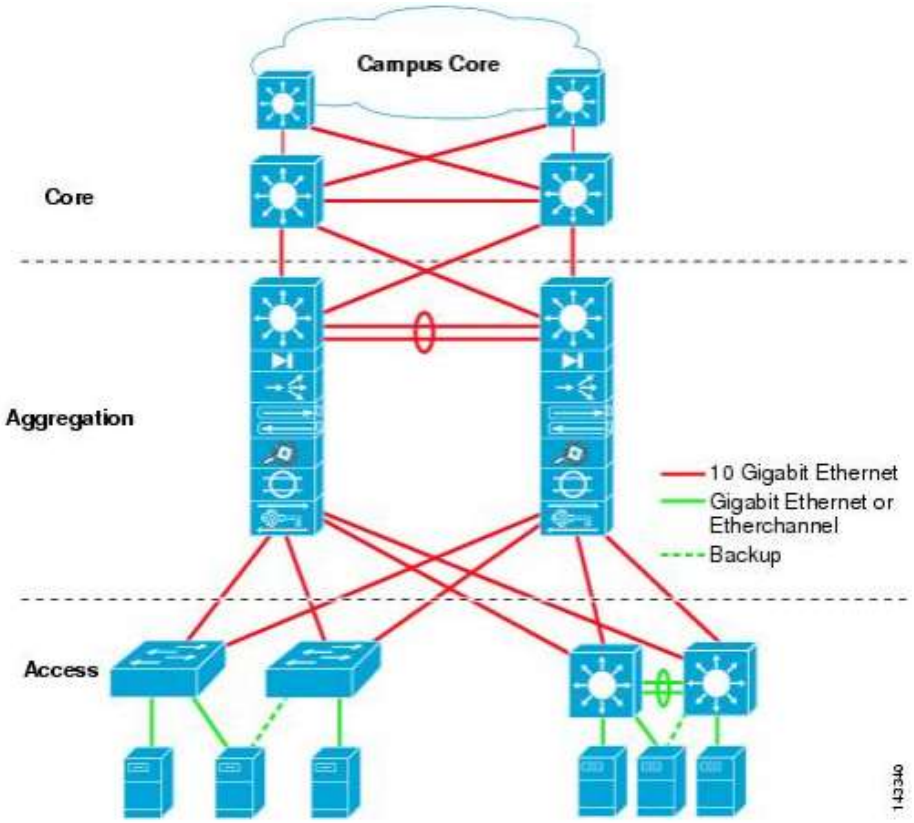


FIGURA 2 Arquitectura de 3 niveles
Fuente: (CISCO, s.f.)

- **Capa de CORE**

La capa de núcleo o CORE, funciona como la puerta de enlace para el resto de la red, conectándose a DCs remotos, campus universitarios, o resto de internet. Está diseñada para el transporte de una gran cantidad de datos y para balancear la carga entre switches de la capa de distribución, mediante enlaces de alta velocidad, priorizando disminuir la latencia y maximizar throughput. Los switches de esta capa se conectan a través de enlaces Ethernet Channel, esta tecnología permite la agregación de múltiples enlaces Ethernet en un gran enlace lógico, permitiendo mayor throughput. La capa de CORE es una de las más importantes, si un problema se presenta en alguno de los equipos que confirman esta capa, podría causar cortes de servicio en múltiples servidores dentro del DC y de esta forma paralizar por completo las operaciones; es por esto que es necesario enlaces y equipos altamente redundantes

- **Capa de Distribución - (Aggregation Layer)**

La capa de distribución tiene como función principal llevar a cabo el enrutamiento y el filtrado de paquetes. Esto se logra mediante el uso de firewalls y balanceadores de carga. Además, esta capa proporciona acceso a redes WAN (Wide Area Network) desde la capa de acceso a través de enlaces redundantes. En la capa de distribución, es posible implementar políticas de priorización de paquetes conocidas como QoS (Quality of Service).
Esta capa, al igual que la capa CORE, manejan switches multicapa, trabajando de esta manera en capa 2 y capa 3 del modelo OSI, manejando protocolos IP y MAC.

- **Capa de Acceso**

Esta capa es la encargada de establecer la conexión entre los switches de la capa de acceso y los servidores que se encuentran en los racks del centro de datos. Estos servidores pueden pertenecer a instituciones, empresas, clientes externos o ser utilizados internamente dentro del centro de datos.
Dado que se requiere que los enlaces entre los switches de la capa de acceso y la capa de distribución sean completamente redundantes, se hace necesario implementar el protocolo Spanning Tree para prevenir la formación de bucles en las tramas Ethernet., por lo cual, en este tipo de arquitecturas, se tiene un manejo pobre del ancho de banda por el bloqueo de gran cantidad de enlaces debido a STP.

2.2.3.2. Spine and Leaf

La topología Spine and Leaf consta de dos capas como una solución a los problemas presentados con la arquitectura de 3 – Tier o 3 capas, siendo una arquitectura altamente escalable, una mejora en la latencia, mayor ancho de banda disponible y reducción en cuellos de banda.

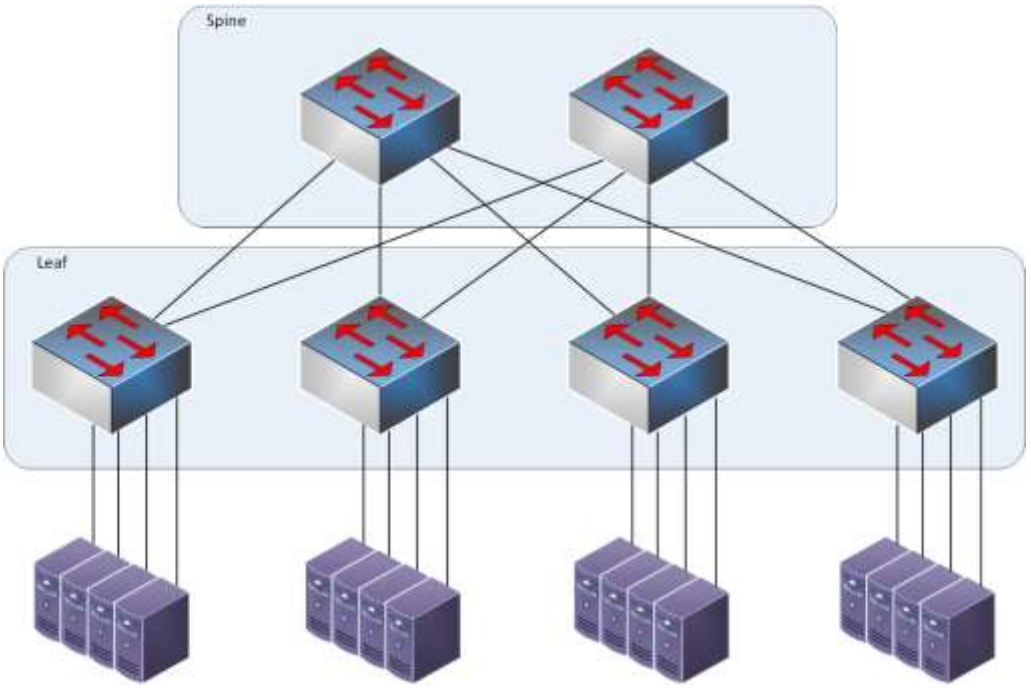


FIGURA 3 Arquitectura Spine and Leaf
Fuente: (Salinero, 2019)

Esta solución de dos capas optimiza la utilización de todos los enlaces de conexión al asegurar que cada dispositivo "leaf" esté conectado a todos los dispositivos "spine". Esto crea una estructura de red con menos intermediarios, lo que resulta en una arquitectura más eficiente y directa.

Una de las principales características de usar Spine and Leaf es que ya no se requiere del protocolo STP, los switches dejan de procesar tramas de la capa 2 del modelo OSI, procesando únicamente paquetes de la capa 3 OSI. Al no existir tramas entre switches, no es necesario bloquear enlaces usando STP y aunque existen rutas redundantes, las mismas son enrutadas por otros protocolos, para equilibrar el tráfico de carga en todas las rutas disponibles y evitar bucles de red.

Una de las ventajas de Spine and Leaf es su tolerancia a fallas, como se había mencionado en la arquitectura 3 – Tier, si el CORE falla, podría generarse cortes importantes en toda la red, pero si un Spine falla, se tendría una leve degradación en los servicios debido a que siempre habrá un Switch Spine disponible para mover datos en la misma cantidad de saltos.

2.2.3.2.1. Roles de la arquitectura Spine and Leaf

SPINE

- Interconecta a los LEAFS
- Reenvía tráfico entre los LEAFs
- Si no es un dispositivo de borde, no es necesario ser configurado como VTEP

LAEF

- Dispositivo de borde en una interconexión VXLAN
- Interconecta dispositivos finales
- Encapsula y des encapsula paquetes VXLAN

LEAF DE BORDE

- Intercambia información de protocolos de enrutamiento (IGP/EGP) con redes externas

SPINE DE BORDE

- Cumple las funciones de un SPINE y de un LEAF de borde
- Requiere ser configurado como VTEP
- Provee conectividad con redes externas. (Naranjo E. , 2018)

2.2.3.3. Comparación de la arquitectura 3 – Tier y Spine and Leaf

Se ha realizado una breve comparativa sobre los beneficios que ofrece Spine and Leaf sobre la arquitectura tradicional 3 – Tier

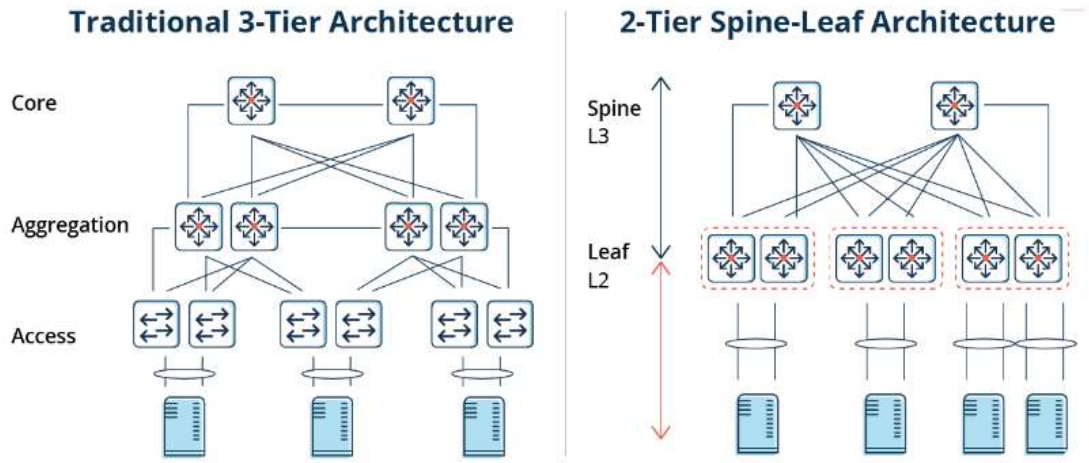


FIGURA 4 Comparativo entre redes tradicionales y Spine and Leaf
Fuente: (HUAWEI, 2022)

- Alta utilización del ancho de banda: Los enlaces ascendentes de cada switch "leaf" operan en modo de balanceo de carga, lo que permite aprovechar al máximo el ancho de banda disponible.

- Latencia de red predecible: al determinar el número de rutas de conexión entre los switches "leaf" que pasan exclusivamente a través de un "spine", es posible anticipar y predecir la latencia de la red en la dirección este-oeste.

- Buena escalabilidad: para aumentar el ancho de banda, basta con aumentar el número de switches spine. Cuando el número de servidores aumenta, el número de switches spine también puede ampliar la escala del centro de datos, de esta forma se aprecia que la planificación y expansión son muy convenientes.

- Reducción en los requisitos de los switches: para salida del tráfico norte – sur, el mismo puede realizarse desde el nodo leaf o el nodo spine, eliminando la necesidad de costosos switches de alto rendimiento y gran ancho de banda.

- Alta seguridad y disponibilidad: al no ser necesario el uso del protocolo STP, cuando un dispositivo falla no es necesaria la re-convergencia y el tráfico sigue pasando por otras rutas normales. La conectividad de la red no se ve afectada y el ancho de banda se reduce en una sola ruta reduciendo al mínimo el impacto en el rendimiento.

2.2.4. Protocolos de Enrutamiento

Los protocolos de enrutamiento son un conjunto de reglas que establecen cómo los dispositivos, como los enrutadores, identifican y dirigen los paquetes a lo largo de una ruta de red. Estos protocolos de enrutamiento se dividen en dos categorías: los protocolos de puerta de enlace interior (IGP, por sus siglas en inglés) y los protocolos de puerta de enlace exterior (EGP, por sus siglas en inglés).

- **Protocolos de puerta de enlace interior:** evalúan el sistema autónomo y toman decisiones de enrutamiento en función de diferentes métricas como recuentos de saltos, cantidad de enrutadores entre el origen y destino, capacidad del enlace, entre otros.
- **Protocolos de puerta de enlace externa:** conocido como BGP, es un protocolo de puerta de enlace fronterizo. Defina la comunicación a través de internet.

2.2.4.1. Spine and Leaf

La topología Spine and Leaf consta de dos capas como una solución a los problemas presentados con la arquitectura de 3 – Tier o 3 capas, siendo una arquitectura altamente escalable, una mejora en la latencia, mayor ancho de banda disponible y reducción en cuellos de banda.

2.2.5. Virtual Extensible LAN (VXLAN)

VXLAN es una tecnología overlay diseñada para proporcionar conectividad de capa 2 y capa 3 sobre una red IP tradicional. VXLAN realiza el entunelamiento de tramas de capa 2 dentro de paquetes IP. VXLAN solo requiere conectividad IP entre los dispositivos de borde que manejan VXLAN (VTEP), la cual es obtenida mediante protocolos de enrutamiento. De esta forman VXLAN mantiene las características de una red IP en cuanto a escalabilidad, balanceo de carga y recuperación predecible contra fallos. En resumen, VXLAN es una tecnología de capa 2 que posibilita la creación de una red de capa 2 sobre una infraestructura de red de capa 3. Esto ofrece un mayor nivel de aislamiento de red. En un entorno de nube, la asignación de recursos no se limita a una única red física de capa 2. Los servidores físicos pueden formar parte de una red VXLAN siempre que estén interconectados mediante redes IPv4 o IPv6. (ORACLE, 2014)

La terminología al describir los componentes claves de la tecnología VXLAN se describe a continuación:

- **VTEP:** conocido también como Leaf, es el encargado de la encapsulación y des encapsulación de VXLAN e instanciar el entunelamiento.

- **VNI:** (Virtual Network Instance), instancia de red lógica que provee servicios de capa 2 o de capa 3 y define un dominio de broadcast de capa 2.

- **VNID:** (Virtual Network Identifier), Identificador de 24 bits que permite direccionar alrededor de 16 millones de redes lógicas.

- **Bridge - Domain:** conjunto de puertos físicos y lógicos que comparten el mismo dominio de broadcast.

- **SPINE:** Capa que interconecta los dispositivos LEAF. (Naranjo E. , 2018)

2.2.5.1. Formato del paquete VXLAN

VXLAN es una técnica de virtualización de red que utiliza la encapsulación MAC-in-UDP agregando un encabezado UDP y un encabezado VXLAN antes de un paquete Ethernet original.

El estándar VXLAN define el paquete como se ilustra en la Figura 5.

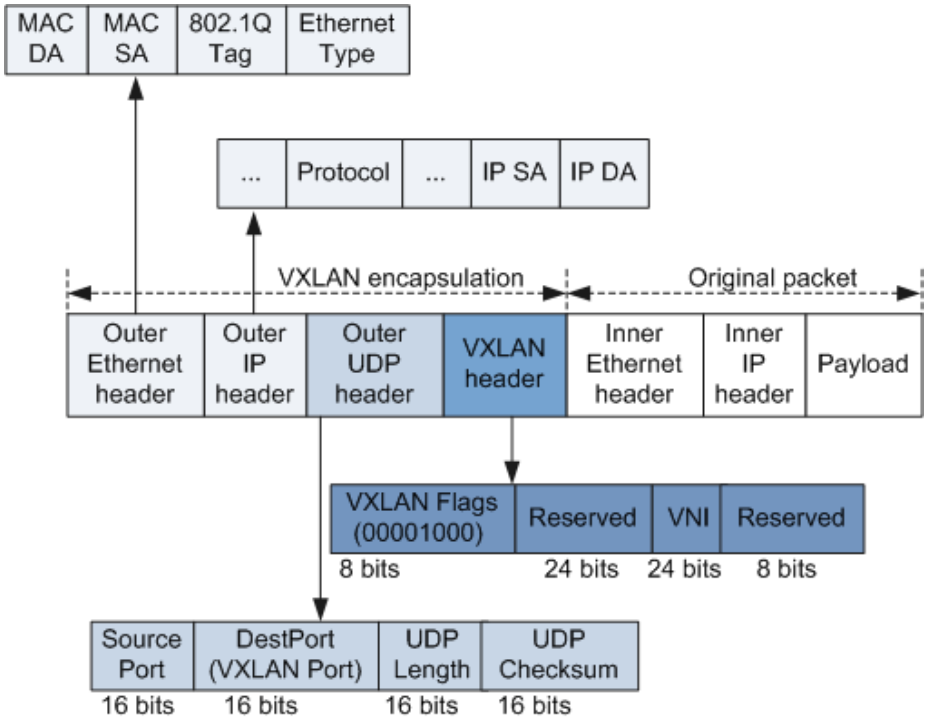


FIGURA 5 Comparativo entre redes tradicionales y Spine and Leaf
Fuente: (HUAWEI, 2020)

Descripción de los campos en el paquete VXLAN, especificados en la Figura 5.:

TABLA 1 Descripción de los campos del paquete VXLAN

CAMPO	**DESCRIPCIÓN**
VXLAN header	• VXLAN Flags (8 bits): el valor es 00001000. • VNI (24 bits): ID de segmento de VXLAN o identificador de red de VXLAN utilizado para identificar un segmento de VXLAN. • Campos reservados (24 bits y 8 bits): deben establecerse en 0.
Outer UDP header	• DestPort: número de puerto de destino, que es 4789 para UDP. • Source Port: número de puerto de origen, que se calcula realizando la operación hash en los paquetes internos.

Outer IP header	• IP SA: dirección IP de origen, que es la dirección IP del VTEP local de un túnel VXLAN. • IP DA: dirección IP de destino, que es la dirección IP del VTEP remoto de un túnel VXLAN.
Outer Ethernet header	• MAC DA: dirección MAC de destino, que es la dirección MAC asignada a la dirección IP del siguiente salto en función de la dirección VTEP de destino en la tabla de enrutamiento del VTEP en la que reside la VM que envía paquetes. • MAC SA: dirección MAC de origen, que es la dirección MAC del VTEP en el que reside la VM que envía el paquete. • Etiqueta 802.1Q: etiqueta VLAN transportada en paquetes. Este campo es opcional. • Tipo de Ethernet: tipo de paquete de Ethernet.

FUENTE: (HUAWEI, 2020)

2.2.5.2. Funcionamiento de VXLAN

- **Plano de Datos**

VXLAN requiere de una infraestructura de red (underlay) para llevar a cabo el data plane forwarding

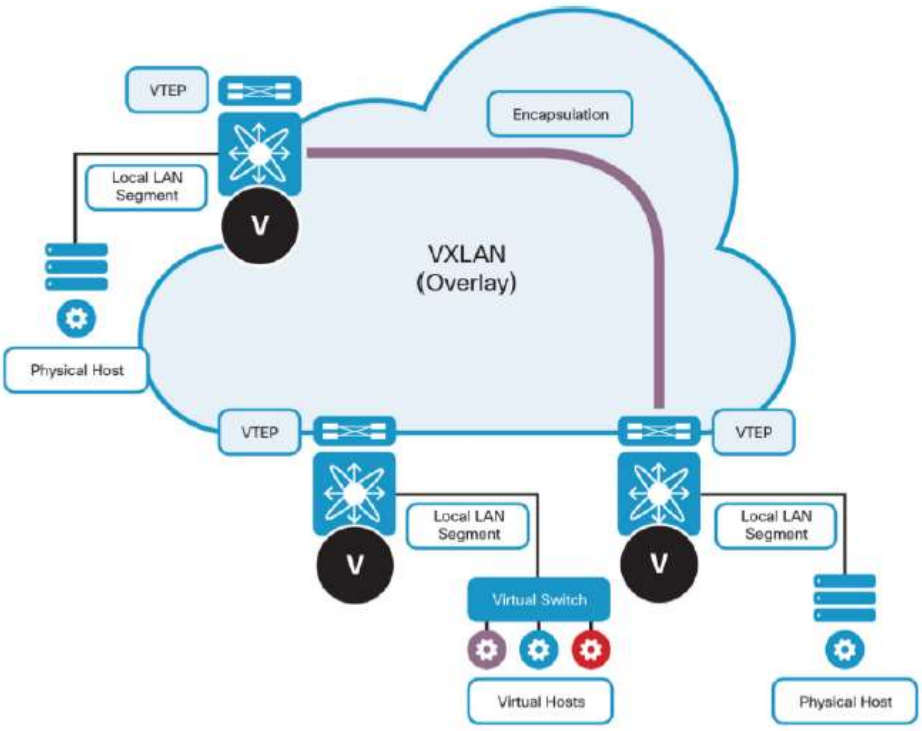


FIGURA 6 VXLAN Tunnel Endpoint
Fuente: (Jansen, 2017)

El data plane forwarding es requerido para proporcionar comunicación unicast entre los dispositivos finales conectados a la VXLAN Fabric. La infraestructura de red puede usarse para enviar tráfico multidestino a dispositivos finales conectados a un dominio de broadcast común en capa 2 en la red overlay. Con frecuencia, este tráfico es conocido como BUM, el cual incluye tráfico de broadcast, unknown unicast y multicast.

Los segmentos VXLAN se crean entre los puntos finales del túnel VXLAN (VTEP). Los VTEP admiten el protocolo VXLAN y realizan encapsulación y des encapsulación VXLAN. Un segmento VXLAN se puede analizar como un túnel entre dos VTEP, donde un VTEP encapsula una trama de capa 2 con un encabezado UDP y un encabezado IP y lo envía a través del túnel. El otro VTEP recibe y des encapsula el paquete para obtener el marco de capa 2.
Cada segmento VXLAN tiene un identificador llamado VNI (VXLAN Network Identifier). Este campo tiene 24 bits de longitud, brindando aproximadamente 16 millones de redes lógicas. Una VNI se mantiene separada con otra VNI, para lograr la comunicación entre ellas, se deberá enrutar el tráfico como se realiza con los dispositivos de diferentes VLAN. VXLAN es una tecnología que encapsula toda la trama original de capa 2 en un paquete UDP, por lo que se le

conoce como una tecnología "MAC-in-UDP" (MAC dentro de UDP). Esta encapsulación permite que VXLAN funcione como un túnel sobre redes de capa 3, lo que facilita la creación de redes virtuales y el aislamiento de tráfico en entornos de red más amplios.

- **Superposiciones y subposiciones**

VXLAN creará redes virtuales sobre la infraestructura existente, haciendo que VXLAN sea una red superpuesta y que la infraestructura existente sea la red subyacente (capa 3).

Todos los puertos de la red subyacente están enrutados, por lo que no es necesario STP, para este enrutamiento se puede usar OSPF, IS-IS y BGP. En la Figura 6. se puede visualizar la red superpuesta y subyacente.

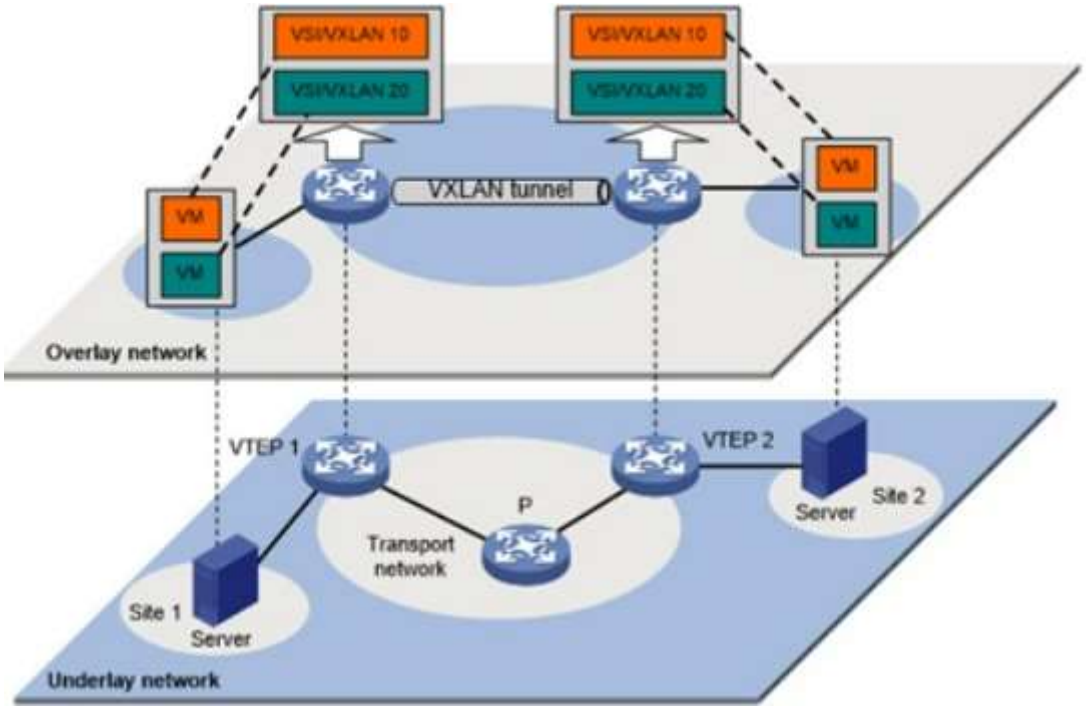


FIGURA 7 Redes superpuestas y subyacentes
Fuente: (HUAWEI, 2022)

Cada VNI es una red separada que se ejecuta sobre la capa subyacente, estos VNI son denominados dominio puente. Para la creación de la red virtual, el tráfico es encapsulado con UDP e IP antes enviado, al llegar al destino se des encapsula. Mientras haya conectividad IP

entre los dispositivos que componen la capa subyacente, la capa superpuesta no tendrá problemas

- **VTEPs y Encapsulación**

El VTEP proporciona la conexión entre la capa superpuesta y la capa subyacente. Cada VTEP tiene una dirección IP en la red subyacente. Cada uno de ellos tiene también una o más VNIs. Para entregar el tráfico de un host a otro, un VTEP de origen y destino creará un túnel sin estado. Estos túneles establecerán solo el tiempo suficiente para entregar el paquete VXLAN. Los dispositivos que establecen este túnel se denominan NVE (Network Virtualization Edges). El túnel VXLAN puede terminar en dispositivos de red o incluso en el vSwitch que reside en un servidor. (HUAWEI, 2022)

2.2.5.3. Beneficios de VXLAN en el aprovisionamiento de un Centro de Datos

- **Multi-tenancy:** intrínsecamente soportado por VXLAN, tanto para capa 2 (VNI capa 2 separados) como para capa 3 (definiendo diferentes VRF para cada cliente)

- **Movilidad:** despliegue flexible y movilidad a estaciones de trabajo tanto físicas como virtualizadas por la capacidad overlay ofrecida por VXLAN, brindando una extensión de servicios de capa 2 en los Centros de Datos.

- **Incremento de la escalabilidad a nivel de capa 2:** VXLAN introduce el VNID de 24 bits, lo que teóricamente permite admitir más de 16 millones de segmentos de capa 2. Esto contrasta con el diseño tradicional que utiliza VLANs y está limitado a un máximo de 4096 segmentos de capa 2 debido a los 12 bits correspondientes al VLAN ID. Gracias a esta mayor capacidad de segmentación, VXLAN ofrece una escalabilidad significativamente superior en comparación con las VLANs convencionales.

- **Soporte multi-path en capa 2:** VXLAN hace uso de una red subyacente de capa 3 (underlay network) para el uso de varios caminos activo (multi-path). Las redes de capa 2 tradicionales soportan un camino (path) activo debido a que el protocolo Spanning Tree STP forza a una topología libre de lazos bloqueando caminos redundantes. (Naranjo E. , 2018)

2.2.6. EVPN (Ethernet VPN)

EVPN es una tecnología basada en estándares que proporciona conectividad multipunto con puente virtual entre distintos dominios de capa 2 a través de una red IP o IP/MPLS troncal. Las instancias de EVPN se configuran en enrutadores perimetrales de proveedor (PE) para mantener la separación de los servicios lógicos entre los clientes. Los enrutadores de PE se conectan a los dispositivos de borde de la red del cliente (CE), los cuales pueden ser enrutadores, conmutadores o hosts.

Los enrutadores PE intercambiarán información de accesibilidad mediante multiprotocolo, Protocolo de puerta de enlace de borde (MP-BGP) y el tráfico encapsulado se reenviará entre enrutadores PE. EVPN tiene el beneficio de introducirse e integrarse en arquitecturas tradicionales, debido a que estas arquitecturas tienen elementos comunes de la tecnología VPN. (Juniper, 2020)

2.2.6.1. EVPN - VXLAN

EVPN-VXLAN es una estructura de red que extiende la conectividad de capa 2 como una superposición sobre una infraestructura de red física preexistente. Esta tecnología, basada en estándares abiertos, tiene como objetivo principal la creación de redes en centros de datos que sean más ágiles, seguras y escalables. EVPN – VXLAN consta de:

- **Ethernet VPN (EVPN):** que se utiliza como el plano de control de superposición y proporciona conectividad virtual entre diferentes dominios de capa 2 y capa 3 a través de una red IP o MPLS
- **LAN extensible virtual LAN (VXLAN):** un protocolo común de superposición de virtualización de red que amplía el espacio de direcciones de red de capa 2 de 4000 a 16 millones

2.2.6.2. Funcionamiento de EVPN – VXLAN

Mediante la implementación de EVPN-VXLAN se pueden conectar ubicaciones dispersas geográficamente a través de puentes virtuales de capa 2. EVPN-VXLAN proporciona la escala que necesitan los proveedores de servicios de nube y a menudo es la tecnología elegida para la interconexión de los Centros de Datos.

EVPN, como superposición, es altamente versátil y extensible, lo que le permite admitir multiusuarios y, con frecuencia, integrar recursos de diversos centros de datos para ofrecer un servicio unificado. Puede habilitar la conectividad de capa 2 a través de una infraestructura física para dispositivos dentro de una red virtual o permitir el enrutamiento de capa 3 según sea necesario, brindando flexibilidad para satisfacer diversas necesidades de conectividad y servicios en la red.

Puesto que sirve como plano de control de detección de direcciones MAC para redes de superposición, EVPN puede admitir diferentes tecnologías de encapsulación de plano de datos. Esta flexibilidad es especialmente atractiva para estructuras de red que no se basan estrictamente en MPLS.

VXLAN encapsula las tramas Ethernet de capa 2 en paquetes UDP de capa 3, lo que permite que las subredes virtuales de capa 2 abarquen las redes de capa 3 subyacentes. Esto se logra mediante el uso de un identificador de red de VXLAN (VNI), que se utiliza para segmentar cada subred de capa 2 de manera similar a como se emplean los identificadores de VLAN tradicionales. De esta manera, VXLAN permite una mayor flexibilidad y escalabilidad en la creación y gestión de redes virtuales.

Un extremo de túnel de VXLAN (VTEP) es un dispositivo con capacidad de VXLAN que encapsula y desencapsula paquetes. En la red física, normalmente un switch funciona como gateway de VXLAN de capa 2 o capa 3 y se considera un VTEP de hardware. Los equivalentes en redes virtuales se conocen como VTEP de software, que se alojan en hipervisores como VMware ESXi o vSphere.

2.2.6.3. Ventajas de EVPN-VXLAN

- **Flexibilidad:** EVPN-VXLAN admite varios protocolos y comparte elementos arquitectónicos comunes con otros servicios de red comunes como VPN, por lo que es fácil de integrar en las redes existentes.

- **Mayor escalabilidad:** una arquitectura basada en EVPN-VXLAN permite a las empresas añadir con facilidad nuevos switches sin necesidad de rediseños de la red subyacente.

- **Seguridad mejorada:** la segmentación más precisa permite a TI restringir los flujos de tráfico entre todos los elementos conectados de la red, para endurecer posiciones de seguridad y limitar el radio de afectación de los ataques.

- **Mejor rendimiento y resiliencia:** la latencia entre los dispositivos de red es más predecible, sobre todo en arquitecturas "spine-leaf", y el fallo de un solo "spine" o "leaf" no tiene un impacto tan grande en el rendimiento de la estructura general. (ARUBA, 2022)

CAPÍTULO III: METODOLOGÍA

En el presente capítulo se presenta el análisis de la prueba de concepto diseñada para validar el comportamiento, funcionamiento y factibilidad de VXLAN-EVPN usando Open Networking para la emulación

3.1. Open Networking

Open Networking es el concepto de desarrollar redes desagregadas, separando la plataforma de hardware de la plataforma de software o del sistema operativo de red. Esta estrategia permite desarrollar soluciones "abiertas", capaces de responder a la necesidad de usuarios, instituciones o clientes de negocio, mediante la integración de soluciones de red con el resto de plataformas IT que componen sus servicios, ya sean dentro de sus instalaciones o en la nube.

Open Networking da la posibilidad de seleccionar el hardware más adecuado en lo cuanto a puertos, capacidad, alta disponibilidad o funcionalidades especializadas gracias a ASICs programables, así como poder elegir que funcionalidades de software, incluyendo capacidades SDN, son las más adecuadas para cubrir la integración con servicios y proporcionarles la escalabilidad, flexibilidad y automatización que requieren los flujos de trabajo actuales en servicios como Big Data. IA o IoT.

TABLA 2 Cuadro comparativo de Open Networking vs Tradicional Networking

OPEN NETWORKING	CARACTERÍSTICAS	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

FUENTE: (GALLARDO, 2023)

3.2. Cumulus Linux

Cumulus Linux se ha desarrollado para proporcionar software de red para diseñar, ejecutar y operar centros de datos modernos. Este diseño de software permite construir y operar de manera eficaz la red de los usuarios de los Centros de Datos.

El desarrollo de Cumulus Linux ofrece la posibilidad de crear centros de datos que son abiertos, escalables, ágiles, resistentes y eficientes. Es una solución única que permite construir y operar redes de manera efectiva y asequible, de manera similar a los centros de datos más grandes del mundo.

El enfoque abierto de Cumulus Linux permite elegir arquitecturas de red con el mejor hardware, software y aplicación, sin depender de un solo proveedor

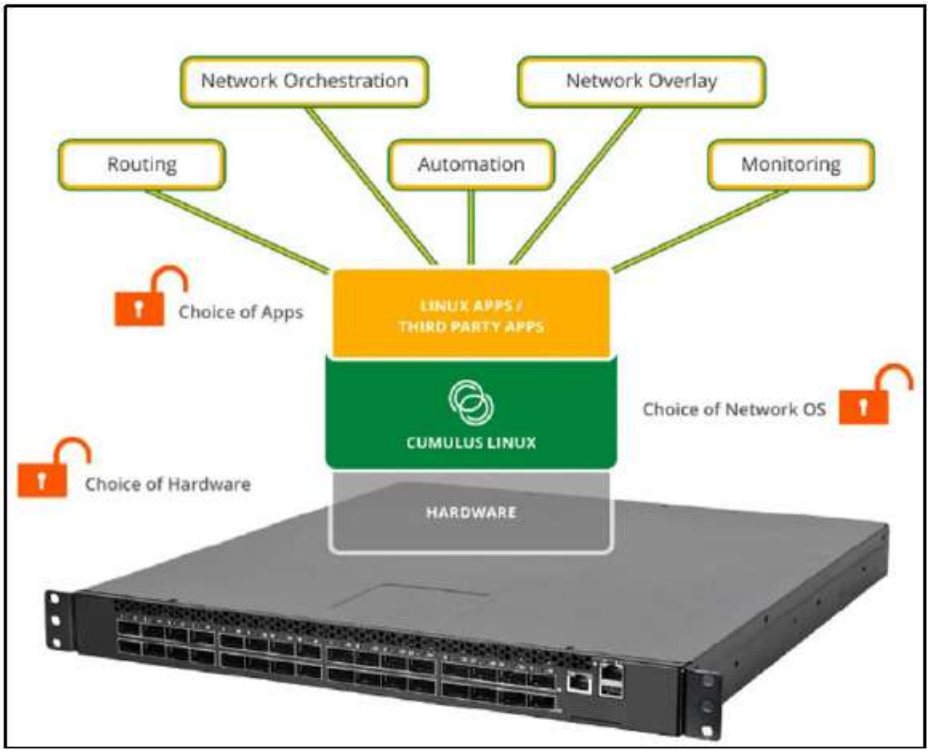


FIGURA 8 Enfoque Cumulus Linux
Fuente: (Salazar-Chacón & Marcillo Parra, 2023)

Cumulus Linux permite implementar arquitecturas de Data Center modernos, permitiendo la transición para las arquitecturas tradicionales, soportando redes de capa 2, capa 3 y superpuestas.

Las principales características de Cumulus Linux son:

- Permite usar protocolos VXLAN y EVPN
- Soportado por NVIDIA
- Sistema Operativo abierto
- No depende de un solo proveedor
- Redistribución de vecinos

3.3. Diseño de Investigación

Para poder realizar la prueba de concepto y comprobar lo mencionado teóricamente, se realizará una emulación de un Data Center con arquitectura moderna, aplicado los protocolos EVPN con VXLAN para su interconexión mediante la herramienta EVE, este emulador permite crear y configurar topologías de red acorde a las necesidades del usuario, así como realizar pruebas, troubleshooting o plantear soluciones a problemas de redes virtuales y reales.

CAPÍTULO IV: EMULACIÓN DE LA INFRAESTRUCTURA

4.1. Topología de la Red

La topología planteada está formada por dos centros de datos separados geográficamente, Quito y Guayaquil, cada uno de estos centros de datos está formado por dos equipos Spine, dos equipos Leaf y dos DCI para la interconexión entre ellos:

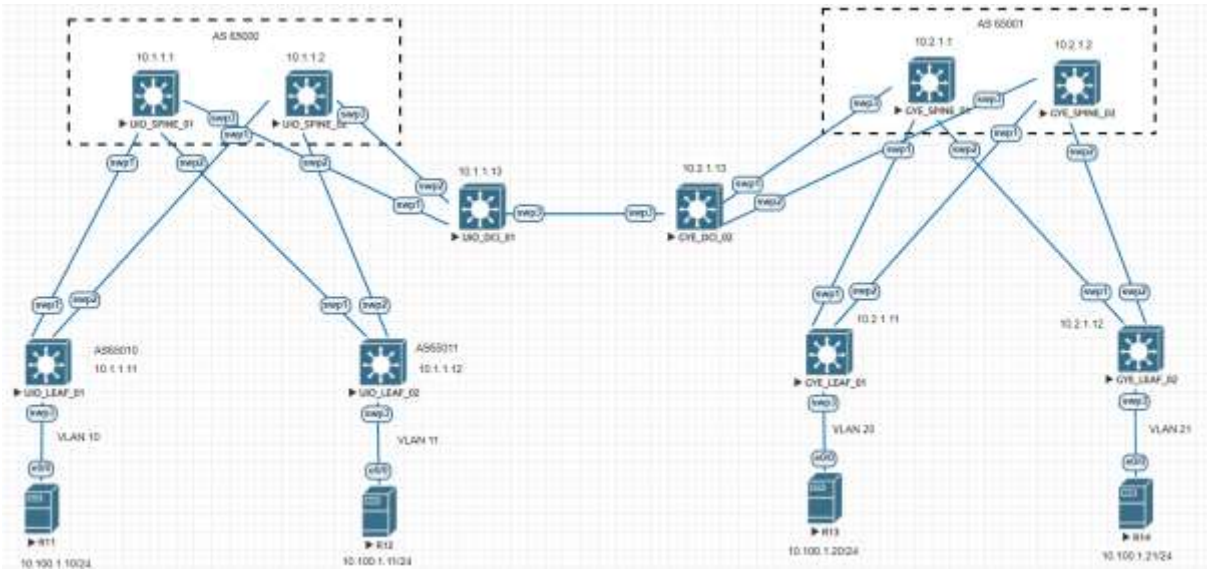


FIGURA 9 Topología de Centros de Datos con VXLAN-EVPN

Para los fines del presente trabajo, no es necesario configurar una dirección Gateway, se puede identificar que, en cada uno de los servidores separados geográficamente, se usan vlans distintas, pero compartiendo un mismo segmento de red:

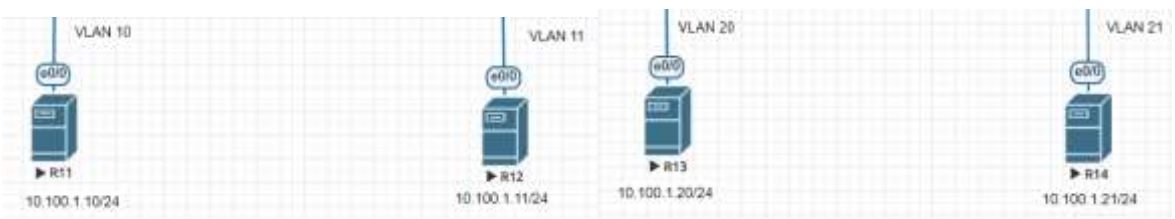


FIGURA 10 Topología de servidores de Centros de Datos

A pesar de que ninguno de los servidores se encuentra configurado con la misma VLAN o tienen una misma ubicación geográfica, todos tienen conectividad entre sí. Esto es posible gracias al túnel VXLAN que ha sido generado. La VNI 10 se ha asignado a cada VLAN en los leafs de la topología propuesta y son anunciados a través de EVPN por BGP.

Como se puede observar a continuación en cada uno de los leafs de la topología, se despliegan los tres VTEP remotos para el VNI 10 que ha sido descubiertos a través de EVPN y BGP:

- **UIO-LEAF-01**

```
cumulus@UIO-LEAF-01:~$ net show evpn vni 10
VNI: 10
 Type: L2
 Tenant VRF: default
 VxLAN interface: vni-10
 VxLAN ifIndex: 10
 Local VTEP IP: 10.1.1.11
 Remote VTEPs for this VNI:
  10.1.1.12
  10.2.1.12
  10.2.1.11
 Number of MACs (local and remote) known for this VNI: 4
 Number of ARPs (IPv4 and IPv6, local and remote) known for this VNI: 0
```

FIGURA 11 VTEP remotos UIO-LEAF-01

- **UIO-LEAF-02**

```
cumulus@UIO-LEAF-02:~$ net show evpn vni 10
VNI: 10
 Type: L2
 Tenant VRF: default
 VxLAN interface: vni-10
 VxLAN ifIndex: 10
 Local VTEP IP: 10.1.1.12
 Remote VTEPs for this VNI:
  10.1.1.11
  10.2.1.12
  10.2.1.11
 Number of MACs (local and remote) known for this VNI: 4
 Number of ARPs (IPv4 and IPv6, local and remote) known for this VNI: 0
```

FIGURA 12 VTEP remotos UIO-LEAF-02

- **GYE-LEAF-01**

```
cumulus@GYE-LEAF-01:~$ net show evpn vni 10
VNI: 10
 Type: L2
 Tenant VRF: default
 VxLAN interface: vni-10
 VxLAN ifIndex: 10
 Local VTEP IP: 10.2.1.11
 Remote VTEPs for this VNI:
  10.1.1.12
  10.1.1.11
  10.2.1.12
 Number of MACs (local and remote) known for this VNI: 4
 Number of ARPs (IPv4 and IPv6, local and remote) known for this VNI: 0
```

FIGURA 13 VTEP remotos GYE-LEAF-01

- **GYE-LEAF-02**

```
cumulus@GYE-LEAF-02:~$ net show evpn vni 10
VNI: 10
 Type: L2
 Tenant VRF: default
 VxLAN interface: vni-10
 VxLAN ifIndex: 10
 Local VTEP IP: 10.2.1.12
 Remote VTEPs for this VNI:
  10.1.1.12
  10.1.1.11
  10.2.1.11
 Number of MACs (local and remote) known for this VNI: 4
 Number of ARPs (IPv4 and IPv6, local and remote) known for this VNI: 0
```

FIGURA 14 VTEP remotos GYE-LEAF-02

Los VTEP remotos que han sido descubiertos, eliminan totalmente la necesidad de mapear manualmente desde y hacia donde se desea asignar los túneles VXLAN. Esto permite que ubicaciones geográficamente separadas puedan compartir IPs en una misma red, como si los servidores se encontraran uno a continuación del otro, de esta forma se logra extender un dominio L2 sobre conexiones L3.

Cuando los servidores del Data Center UIO envían información hacia el Data Center GYE, los datos son transportados hacia la capa “Leaf”, quienes son los encargados de convertir la data en VTEP que genera el túnel virtual (VXLAN). Esto brinda la ventaja de que a pesar que los servidores se encuentran separados geográficamente, simula estar conectados a través de un único switch, lo que brinda las ventajas de menos tiempos de latencia, rapidez en

hiperconvergencia y tiempos de respuesta.

Cuando el VTEP del Data Center UIO llega hacia el VTEP del Data Center GYE, desencapsula el tráfico quitando el encabezado VXLAN y entregando la data enviada.

Cabe mencionar que los centros de datos propuestos tienen alta disponibilidad y su redundancia funciona como un “full mesh”, garantizando la operatividad de los clientes ante incidentes.

4.2. Configuración de Equipos Spines

UIO-SPINE-01

```
cumulus@UIO-SPINE-01:~$ net show configuration commands
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65000
net add interface swp1-3 ipv6 nd ra-interval 5
net del interface swp1-3 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
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 neighbor swp3 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 add dns nameserver ipv4 10.0.2.3
        net add ptp global slave-only no
        net add ptp global priority1 255
        net add ptp global priority2 255
        net add ptp global domain-number 0
        net add ptp global logging-level 5
        net add ptp global path-trace-enabled no
        net add ptp global use-syslog yes
        net add ptp global verbose no
        net add ptp global summary-interval 0
        net add ptp global time-stamping
        net add interface swp1-3
        net add loopback lo ip address 10.1.1.1/32
        net add hostname UIO-SPINE-01
        net add dot1x radius accounting-port 1813
        net add dot1x radius authentication-port 1812
        net add dot1x eap-reauth-period 0
        net add dot1x mab-activation-delay 30
       net commit
```

Código referenciado de (Davidson, 2019)

- **Descripción de comandos representativos**

TABLA 3 Detalle de comandos UIO-SPINE-01

Comando	Descripción
`net add bgp autonomous-system 65000`	El comando establece el número de sistema autónomo usado para la comunicación mediante el protocolo BGP. Un ASN es un identificador único que define un grupo de uno o mas prefijos de IP que mantienen una política de enrutamiento única y claramente definida.
`net add bgp router-id 10.1.1.1`	Comando que define el router ID para el protocolo BGP. El router-id se utiliza en el algoritmo BGP para determinar la mejor ruta a un destino donde la preferencia es el enrutador BGP con la ID de enrutador más baja.

net add bgp bestpath as-path multipath-relax	Comando que permite equilibrar la carga entre múltiple ruta recibidas de diferente AS vecinos.
net add bgp bestpath compare-routerid	Este comando permite comparar rutas idénticas recibidas durante el proceso de selección de la mejor ruta y da prioridad a la ruta con el ID mas bajo.
net add bgp neighbor fabric peer-group	Comando para creación del grupo de vecinos fabric
net add bgp neighbor fabric remote-as external	Brinda los permisos para conexión remota o externa del grupo fabric
net add bgp neighbor swp1 interface peer-group fabric	Agrega interfaces swp al grupo fabric
net add bgp ipv4 unicast network 10.1.1.1/32	Asignación de una IPv4
net add bgp l2vpn evpn neighbor fabric activate	Activa el protocol EVPN para la distribución entre vecinos del grupo fabric
net add bgp l2vpn evpn advertise-all-vni	Activación del EVPN para todos los VNI
net add loopback lo ip address 10.1.1.1/32	Agrega una interfaz loopback
net add hostname UIO-SPINE-01	Añade el nombre/idetificativo del equipo

4.3. Configuración de Equipos Leafs

UIO-LEAF-01

```
cumulus@UIO-LEAF-01:~$ net show  configuration commands
net del all
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65010
net add interface swp1-2 ipv6 nd ra-interval 5
net del interface swp1-2 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
```

```
net add routing log syslog informational
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 dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
net add vxlan vni-10 vxlan id 10
net add bridge bridge ports swp3,vni-10
net add bridge bridge vids 10
net add bridge bridge vlan-aware
net add interface swp1-2
net add interface swp3 bridge access 10
net add loopback lo ip address 10.1.1.11/32
net add vxlan vni-10 bridge access 10
net add vxlan vni-10 stp bpduguard
net add vxlan vni-10 stp portbpdufilter
net add vxlan vni-10 vxlan local-tunnelip 10.1.1.11
net add hostname UIO-LEAF-01
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
net commit
```

Código referenciado de (Davidson, 2019)

- **Descripción de comandos representativos**

TABLA 4 Detalle de comandos UIO-LEAF-01

Comando	Descripción
`net add bgp autonomous-system 65010`	Comando que permite agregar el sistema autónomo para establecer la sesión BGP
`net add bgp router-id 10.1.1.11`	Agrega la router-id del BGP
`net add bgp bestpath as-path multipath-relax`	Comando que permite equilibrar la carga entre múltiple ruta recibidas de diferente AS vecinos.
`net add bgp bestpath compare-routerid`	Este comando permite comparar rutas idénticas recibidas durante el proceso de selección de la mejor ruta y da prioridad a la ruta con el ID mas bajo.
`net add bgp neighbor fabric peer-group`	Comando para creación del grupo de vecinos fabric
`net add bgp neighbor fabric remote-as external`	Brinda los permisos para conexión remota o externa del grupo fabric
`net add bgp neighbor fabric capability extended-nexthop`	Agrega la capacidad extendida-nexthop a las declaraciones de vecindades globales en cada extremo de las sesiones BGP.
`net add bgp neighbor swp1 interface peer-group fabric`	Agrega interfaces swp al grupo fabric
`net add bgp ipv4 unicast network 10.1.1.11/32`	Asignación de una IPv4
`net add bgp ipv6 unicast neighbor fabric activate`	Activa la dirección unicast ipv6 para el grupo fabric
`net add bgp l2vpn evpn  neighbor fabric activate`	Activación de la distribución BGP mediante EVPN entre las vecindades del grupo fabric
`net add bgp l2vpn evpn  advertise-all-vni`	Habilitación EVPN para todos los VNI
`net add vxlan vni-10 vxlan id 10`	Creación del VNI-10 con el ID10 para VXLAN
`net add loopback lo ip address 10.1.1.11/32`	Asignación de la IP loopback
`net add vxlan vni-10 bridge access 10`	Asigna el túnel VXLAN para el ID 10
`net add vxlan vni-10 stp bpduguard`	Habilitación del STP BPDU en las interfaces del VXLAN

`net add vxlan vni-10 vxlan local-tunnelip 10.1.1.11`	Establece la IP local para el túnel VXLAN
`net add hostname UIO-LEAF-01`	Añade el nombre/idetificativo del equipo

4.4. Configuración de Equipos DCI

UIO-DCI-01

```
cumulus@UIO-DCI-01:~$ net show configuration commands
net del all
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65012
net add interface swp1-3 ipv6 nd ra-interval 5
net del interface swp1-2 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
net add bgp router-id 10.1.1.13
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 neighbor swp3 interface peer-group fabric
net add bgp ipv4 unicast network 10.1.1.13/32
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 dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
```

```
        net add ptp global logging-level 5
        net add ptp global path-trace-enabled no
        net add ptp global use-syslog yes
        net add ptp global verbose no
        net add ptp global summary-interval 0
        net add ptp global time-stamping
        net add interface swp1-3
        net add loopback lo ip address 10.1.1.13/32
        net add hostname UIO-DCI-01
        net add dot1x radius accounting-port 1813
        net add dot1x radius authentication-port 1812
        net add dot1x eap-reauth-period 0
        net add dot1x mab-activation-delay 30
net commit
```

Código referenciado de (Davidson, 2019)

- **Descripción de comandos representativos**

TABLA 5 Detalle de comandos UIO-DCI-01

Comando	Descripción
`net add bgp autonomous-system 65012`	Comando que permite agregar el sistema autónomo para establecer la sesión BGP
`net add bgp router-id 10.1.1.13`	Agrega la router-id del BGP
`net add bgp bestpath as-path multipath-relax`	Comando que permite equilibrar la carga entre múltiple ruta recibidas de diferente AS vecinos.
`net add bgp bestpath compare-routerid`	Este comando permite comparar rutas idénticas recibidas durante el proceso de selección de la mejor ruta y da prioridad a la ruta con el ID mas bajo.
`net add bgp neighbor fabric peer-group`	Comando para creación del grupo de vecinos fabric
`net add bgp neighbor fabric capability extended-nexthop`	Agrega la capacidad extendida-nexthop a las declaraciones de vecindades globales en cada extremo de las sesiones BGP.
`net add bgp neighbor swp1 interface peer-group fabric`	Agrega interfaces swp al grupo fabric
`net add bgp ipv4 unicast network 10.1.1.13/32`	Asignación de una IPv4

`net add bgp ipv6 unicast neighbor fabric activate`	Activa la dirección unicast ipv6 para el grupo fabric
`net add bgp l2vpn evpn  neighbor fabric activate`	Activación de la distribución BGP mediante EVPN entre las vecindades del grupo fabric
`net add bgp l2vpn evpn  advertise-all-vni`	Habilitación EVPN para todos los VNI
`net add loopback lo ip address 10.1.1.13/32`	Asignación de la IP loopback
`net add hostname UIO-DCI-01`	Añade el nombre/idetificativo del equipo

CAPÍTULO V: PRESENTACIÓN Y ANÁLISIS DE RESULTADOS DE LA EMULACIÓN

En la presente emulación se puede comprobar el correcto funcionamiento de VXLAN con EVPN para la comunicación de dos Data Center alejados geográficamente, donde los clientes (servidores) comparten red en su configuración a pesar de que ninguno se encuentra configurado con la misma VLAN, todos tienen conectividad entre sí. Adicionalmente se validará una topología en alta disponibilidad para brindar continuidad en los servicios de Data Center ante desastres.

5.1. Pruebas de conectividad

Se valida que existe conectividad entre los servidores de Data Center UIO y Data Center GYE sin inconvenientes:

- **Desde el Centro de Datos UIO**

SERVER_01 hacia el Centro de Datos GYE SERVER_01

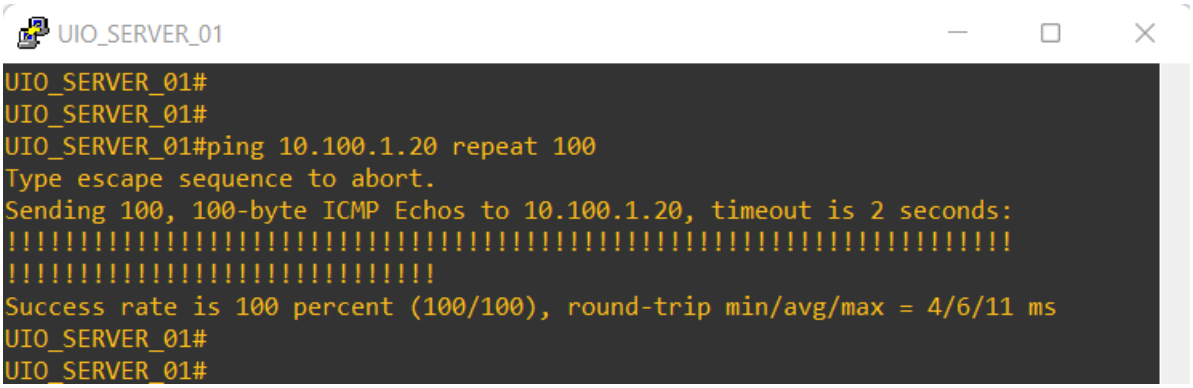


FIGURA 15 Conectividad desde SERVER_01 hacia GYE SERVER_01

SERVER_01 hacia el Centro de Datos GYE SERVER_02

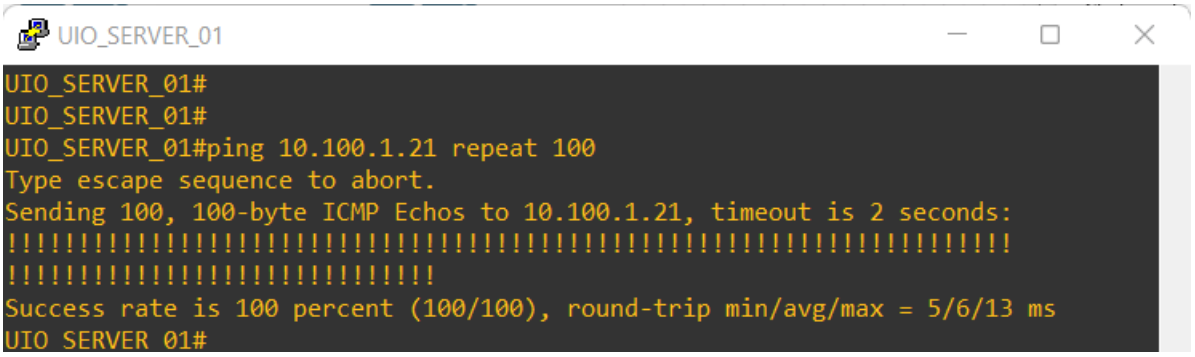


FIGURA 16 Conectividad desde SERVER_01 hacia GYE SERVER_02

SERVER_02 hacia el Centro de Datos GYE SERVER_01

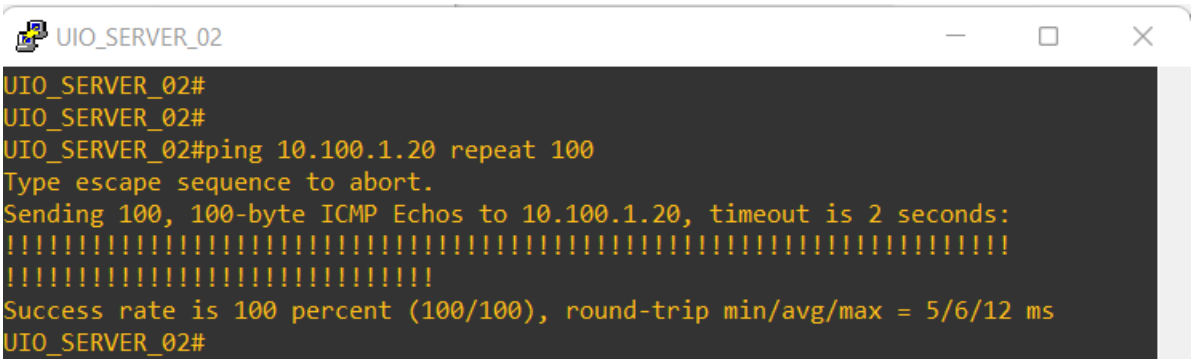


FIGURA 17 Conectividad desde SERVER_02 hacia GYE SERVER_01

SERVER_02 hacia el Centro de Datos GYE SERVER_02

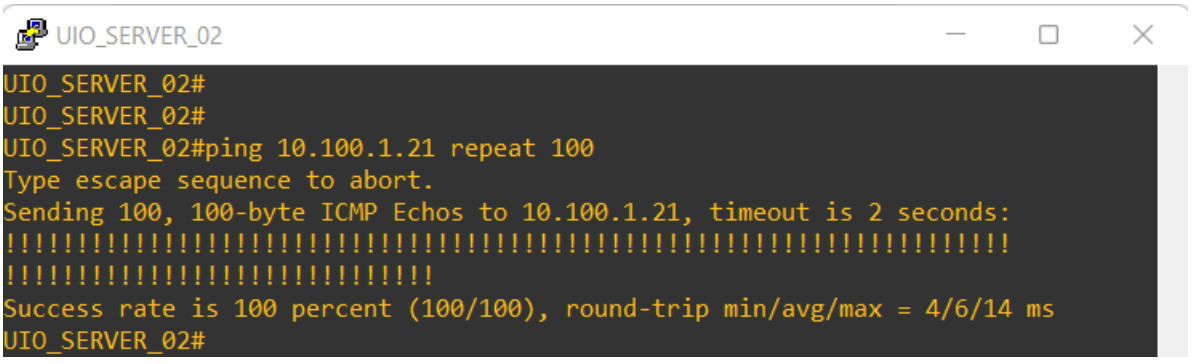


FIGURA 18 Conectividad desde SERVER_02 hacia GYE SERVER_02

- **Desde el Centro de Datos GYE**

SERVER_01 hacia el Centro de Datos UIO SERVER_01

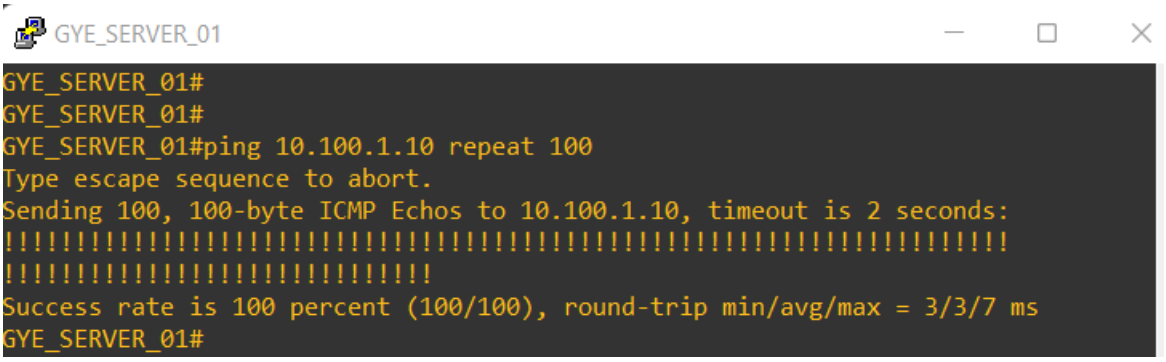


FIGURA 19 Conectividad desde SERVER_01 hacia UIO SERVER_01

SERVER_01 hacia el Centro de Datos UIO SERVER_02

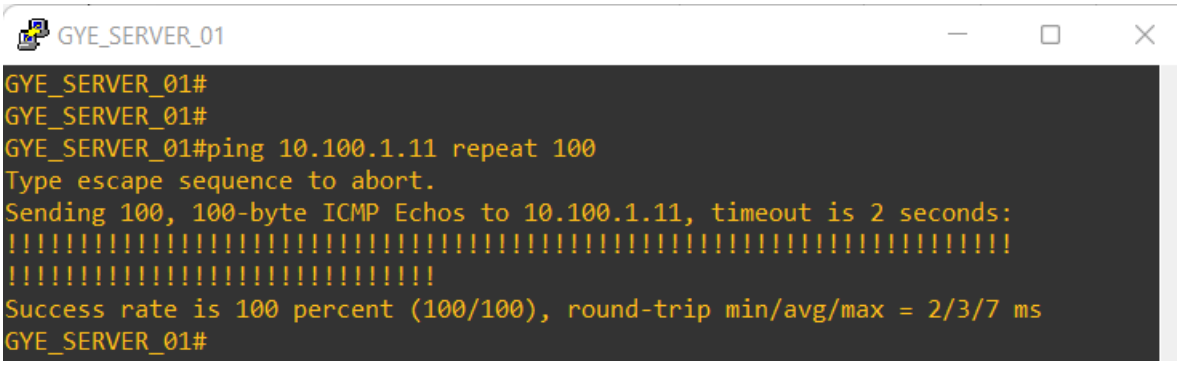


FIGURA 20 Conectividad desde SERVER_01 hacia UIO SERVER_02

SERVER_02 hacia el Centro de Datos UIO SERVER_01

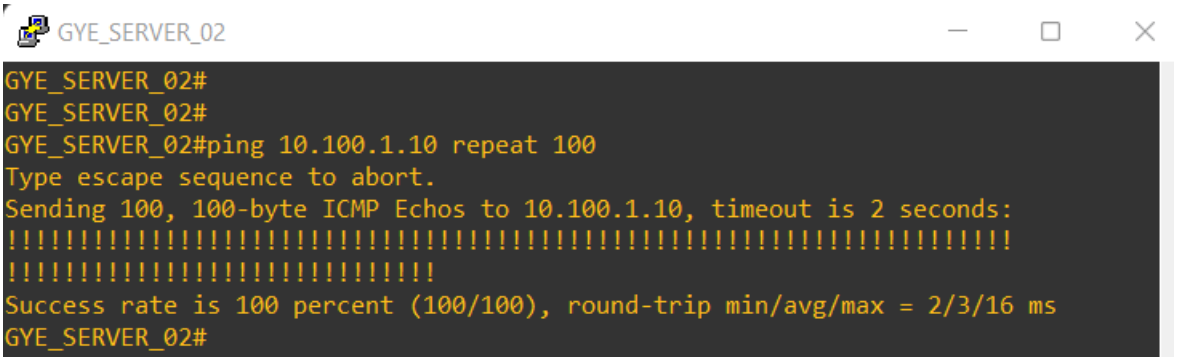


FIGURA 21 Conectividad desde SERVER_02 hacia UIO SERVER_01

SERVER_02 hacia el Centro de Datos UIO SERVER_02

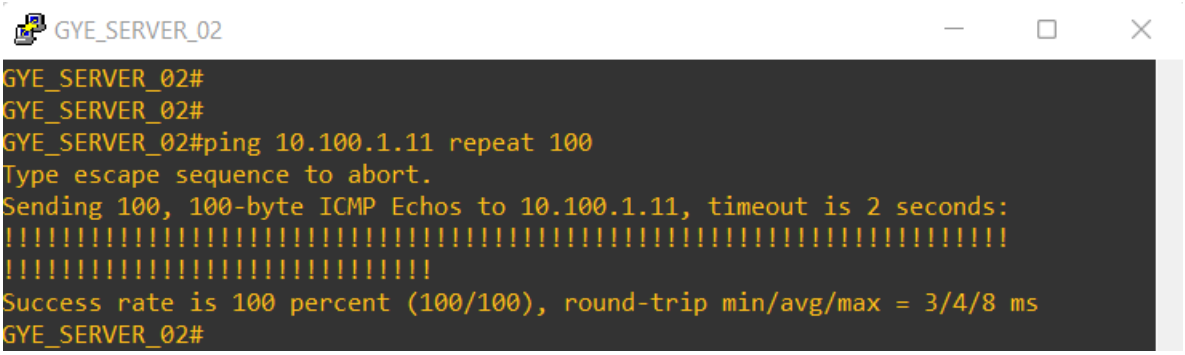


FIGURA 22 Conectividad desde SERVER_02 hacia UIO SERVER_02

En la topología propuesta, se garantiza alta disponibilidad, por lo cual se realiza pruebas de redundancia, apagando los SPINE y validando la conectividad entre los servidores:

5.2. Pruebas de alta disponibilidad

- **Desconexión UIO_SPINE_01 - Centro de Datos UIO**

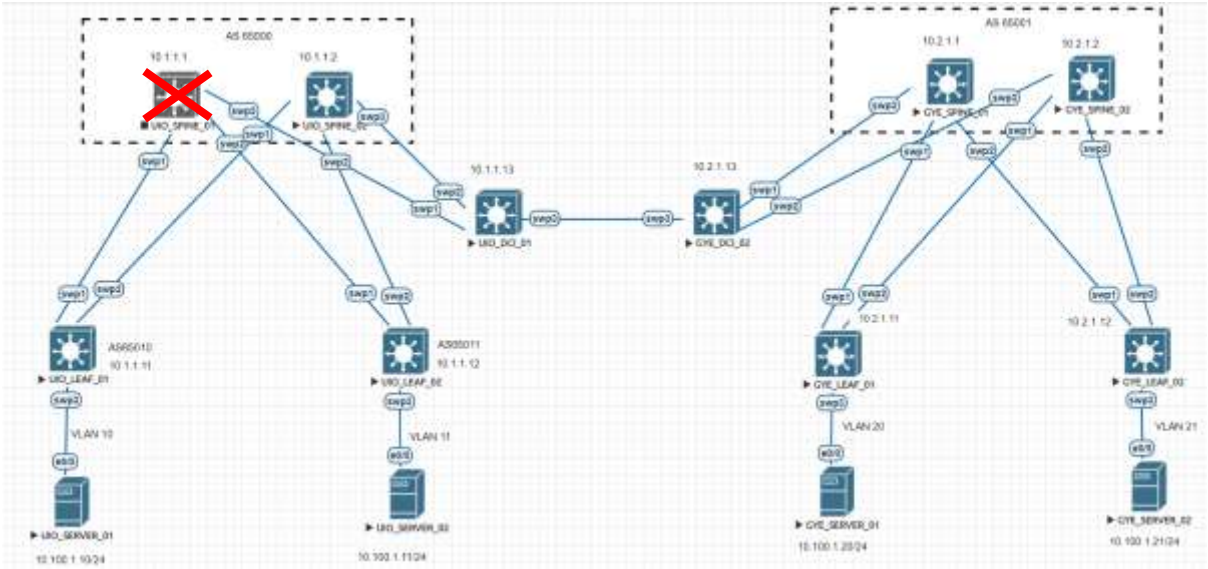


FIGURA 23 Apagado del equipo UIO_SPINE_01

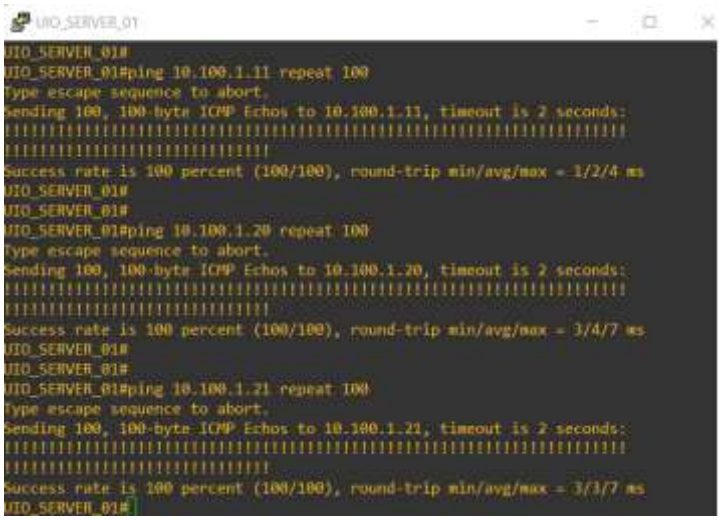


FIGURA 24 Prueba conexión desde UIO_SERVER_01 hacia el resto de servidores

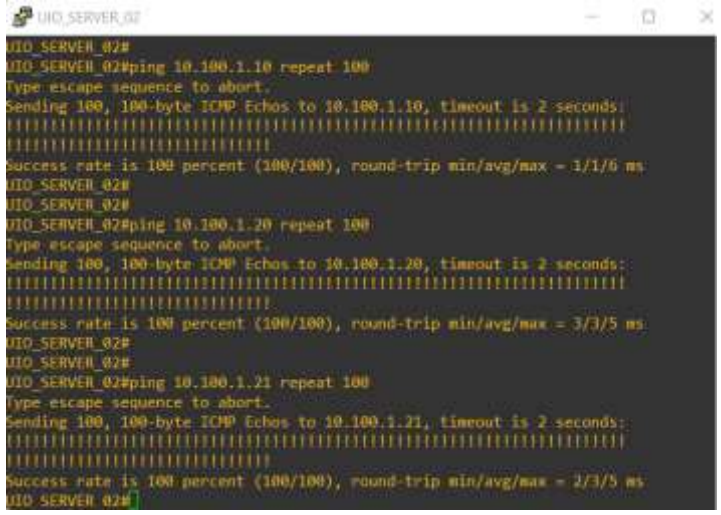


FIGURA 25 Prueba conexión desde UIO_SERVER_02 hacia el resto de servidores

..

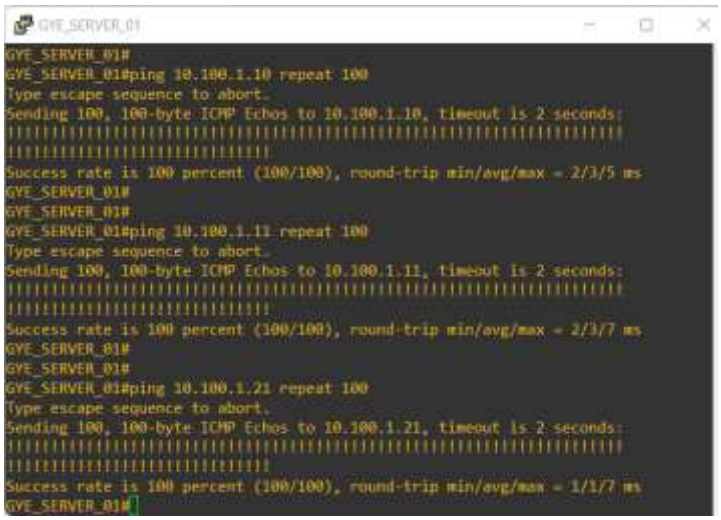


FIGURA 26 Prueba conexión desde GYE_SERVER_01 hacia el resto de servidores

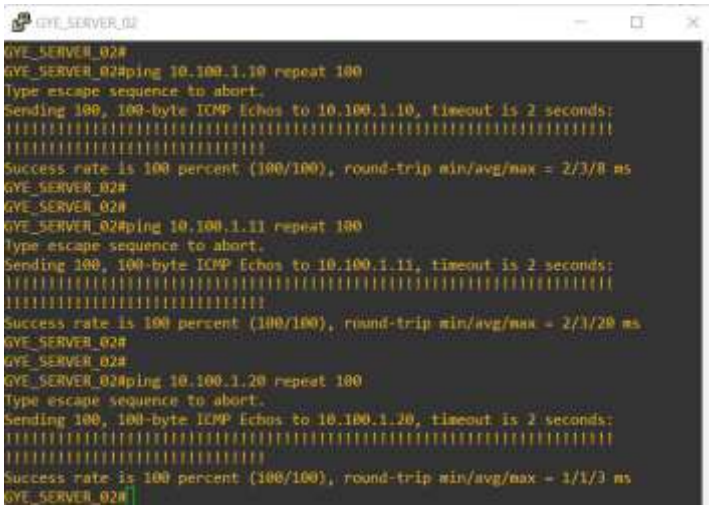


FIGURA 27 Prueba conexión desde GYE_SERVER_02 hacia el resto de servidores

- **Desconexión UIO_SPINE_02 - Centro de Datos UIO**

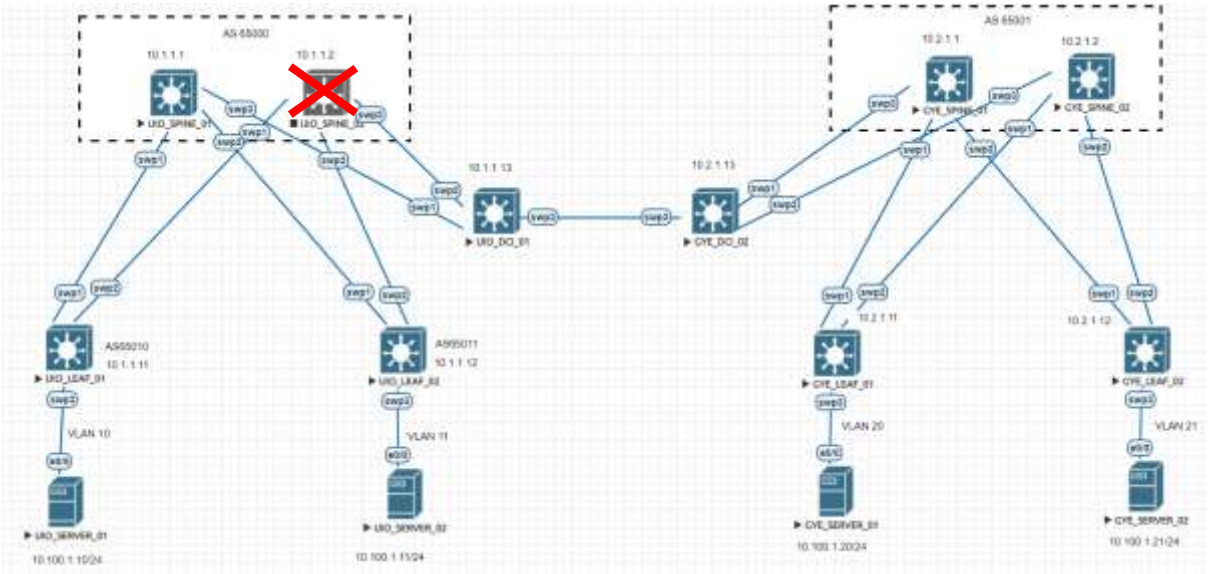


FIGURA 28 Apagado del equipo UIO_SPINE_02

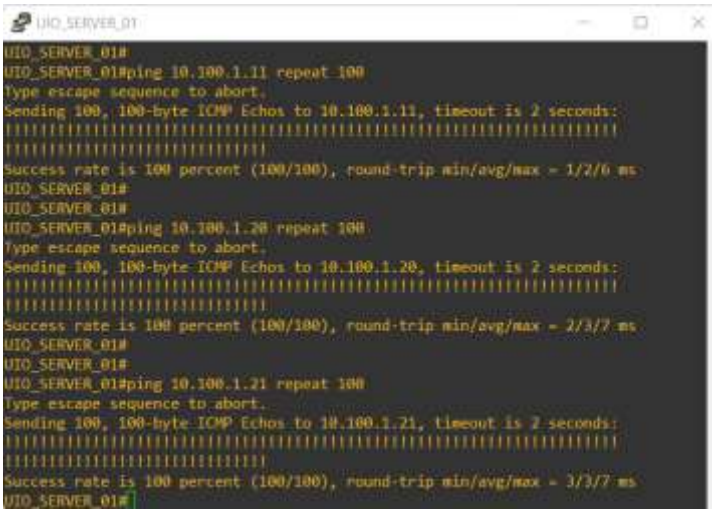


FIGURA 29 Prueba conexión desde UIO_SERVER_01 hacia el resto de servidores

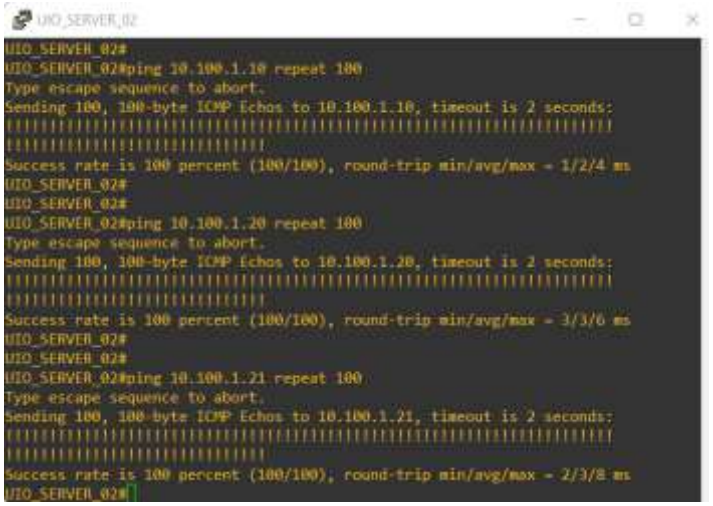


FIGURA 30 Prueba conexión desde UIO_SERVER_02 hacia el resto de servidores

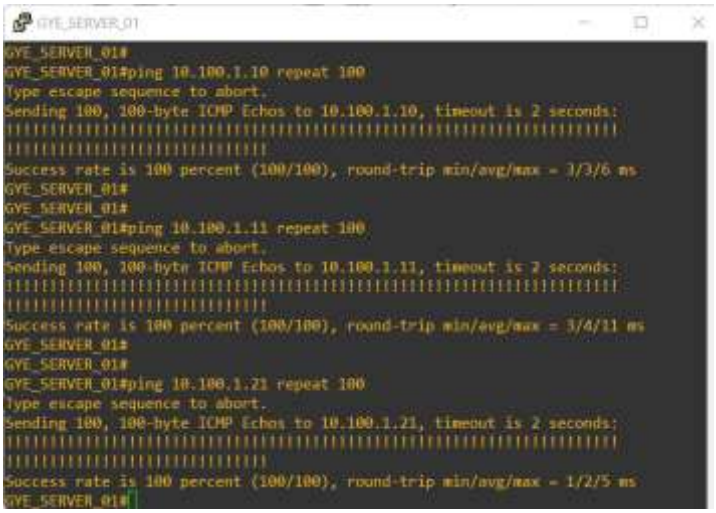


FIGURA 31 Prueba conexión desde GYE_SERVER_01 hacia el resto de servidores

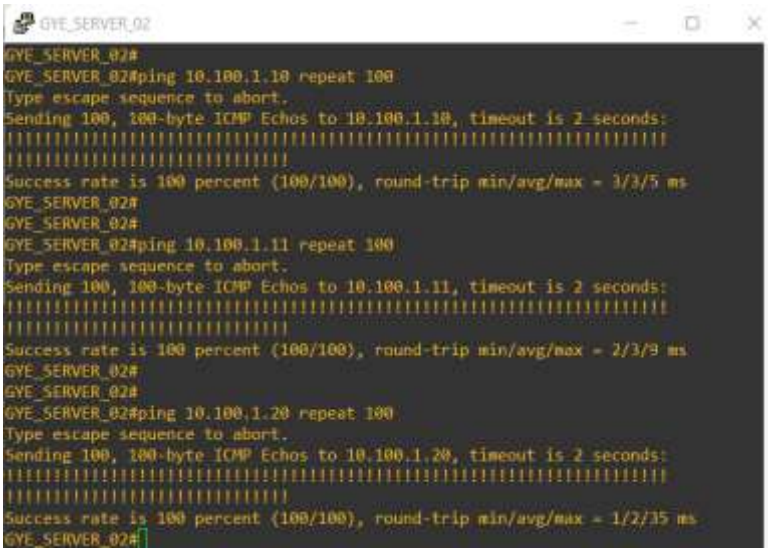


FIGURA 32 Prueba conexión desde GYE_SERVER_02 hacia el resto de servidores

- **Desconexión GYE_SPINE_01 - Centro de Datos GYE**

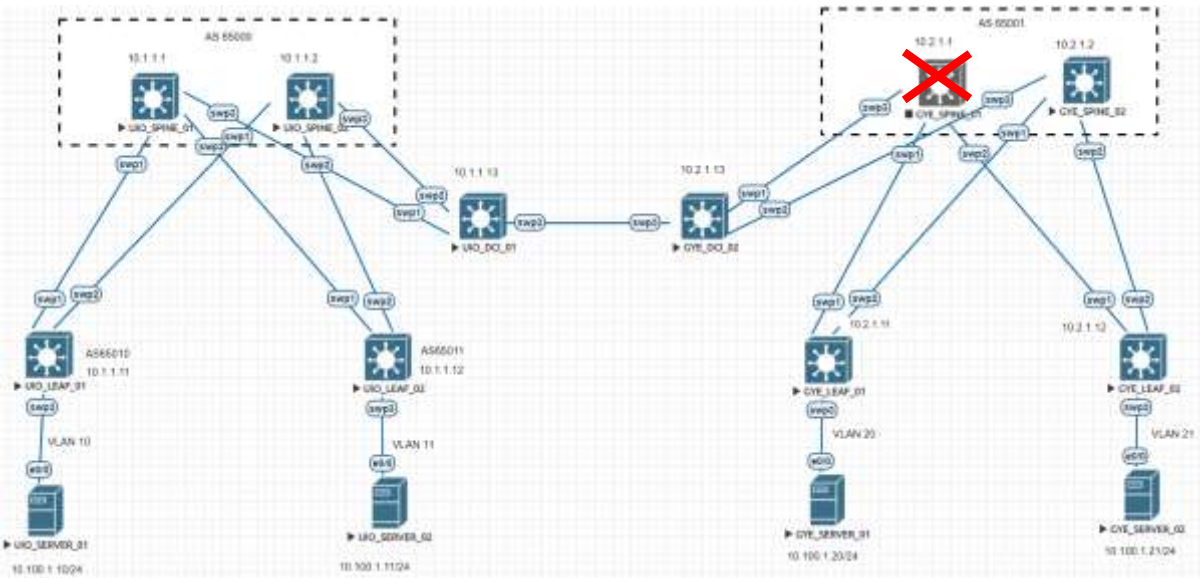


FIGURA 33 Apagado del equipo GYE_SPINE_01

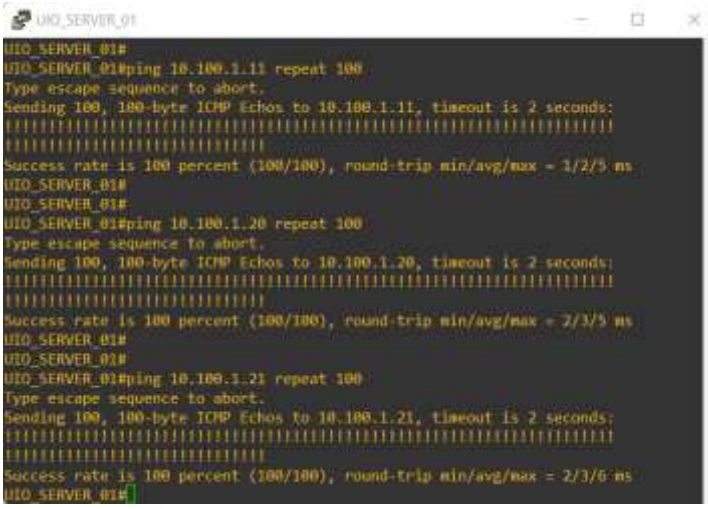


FIGURA 34 Prueba conexión desde UIO_SERVER_01 hacia el resto de servidores

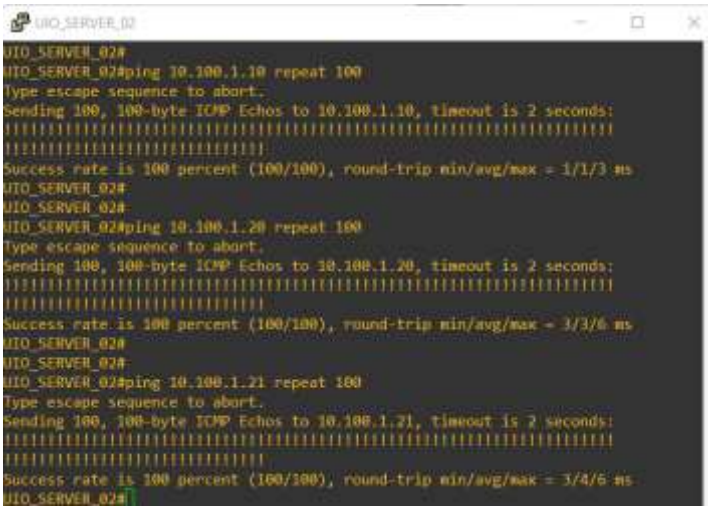


FIGURA 35 Prueba conexión desde UIO_SERVER_02 hacia el resto de servidores

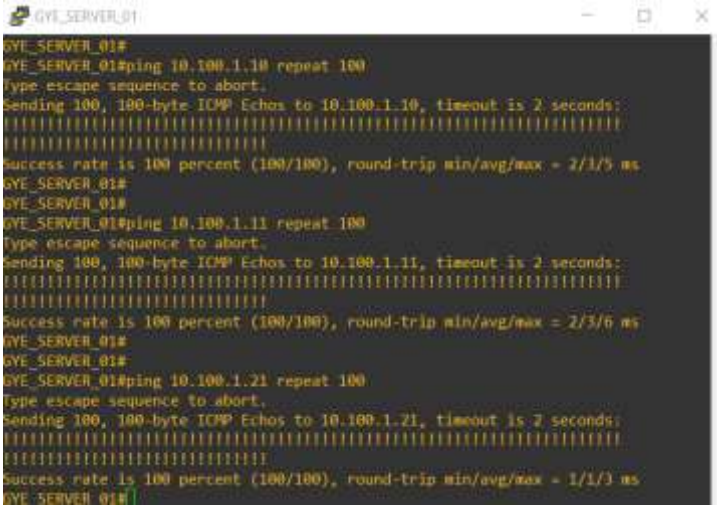


FIGURA 36 Prueba conexión desde GYE_SERVER_01 hacia el resto de servidores

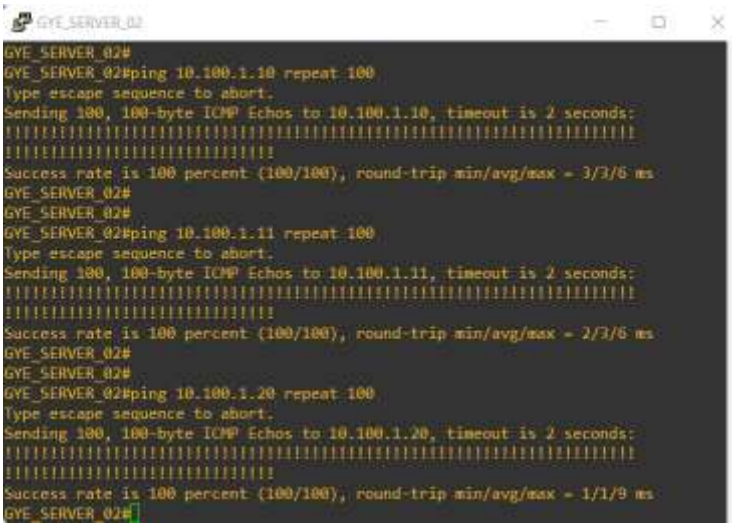


FIGURA 37 Prueba conexión desde GYE_SERVER_02 hacia el resto de servidores

- **Desconexión GYE_SPINE_02 - Centro de Datos GYE**

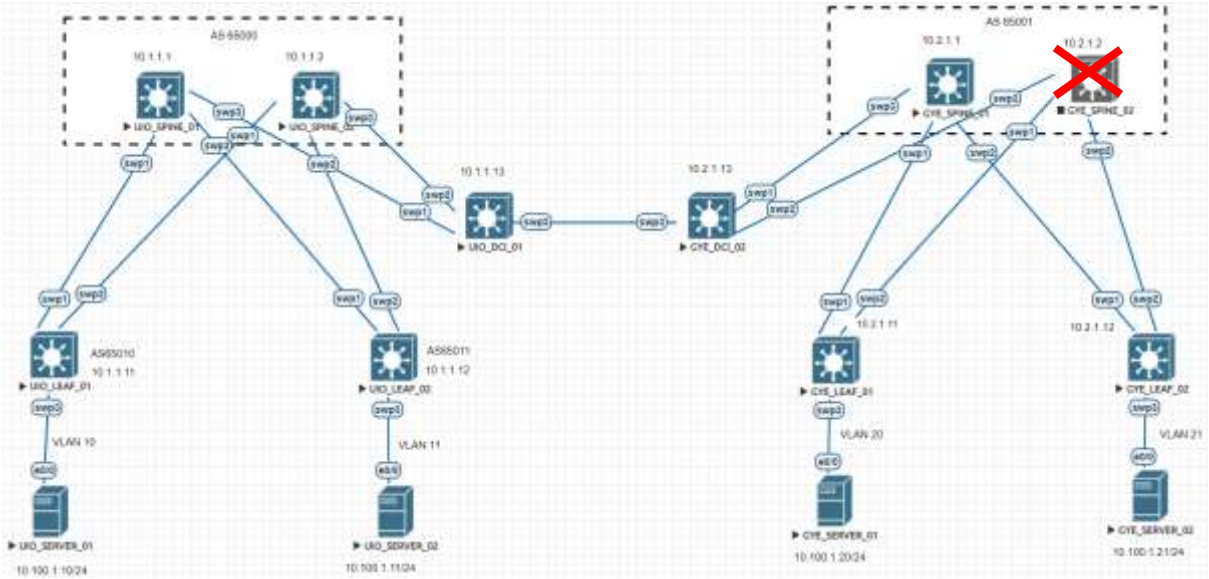


FIGURA 38 Apagado del equipo GYE_SPINE_02

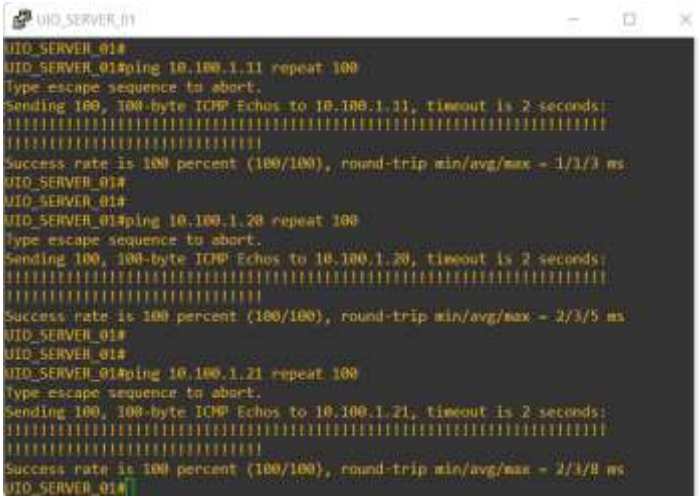


FIGURA 39 Prueba conexión desde UIO_SERVER_01 hacia el resto de servidores

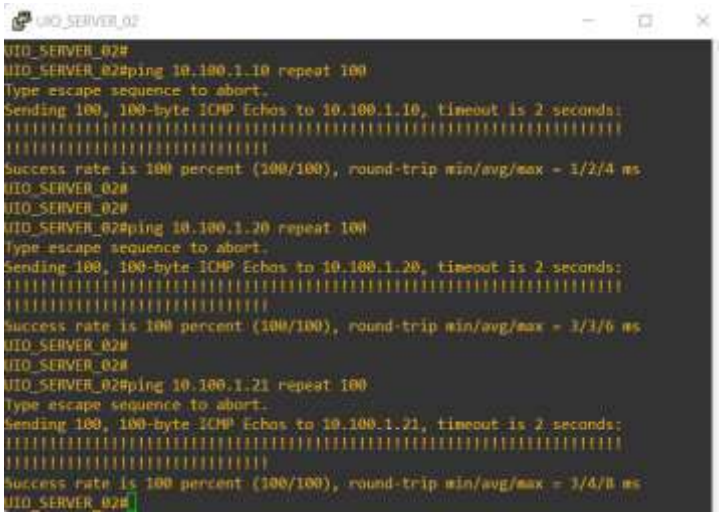


FIGURA 40 Prueba conexión desde UIO_SERVER_02 hacia el resto de servidores

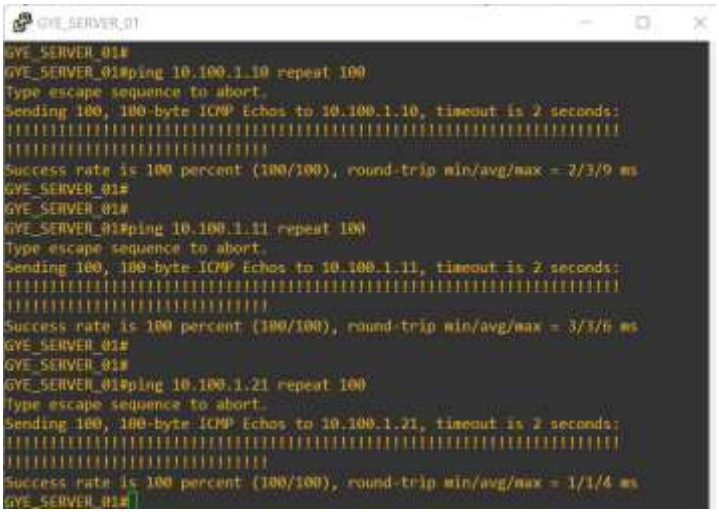


FIGURA 41 Prueba conexión desde GYE_SERVER_01 hacia el resto de servidores

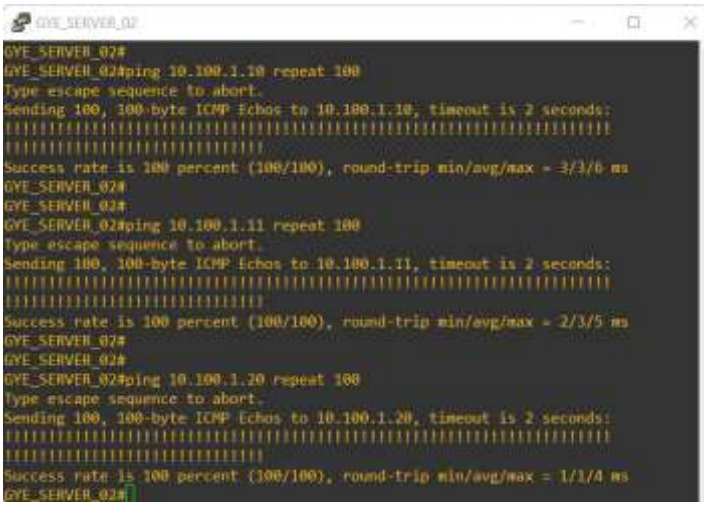


FIGURA 42 Prueba conexión desde GYE_SERVER_02 hacia el resto de servidores

5.3. Validación encapsulamiento VXLAN

Para realizar la validación del tráfico VXLAN, se ha utilizado el analizador de protocolos Wireshark, se debe tener en consideración lo siguiente para que la herramienta funcione sin inconvenientes:

Se debe asegurar que la máquina virtual en la cual se tiene el emulador tenga salida a internet, por lo cual la red asignada a la máquina debe estar correctamente nateada.

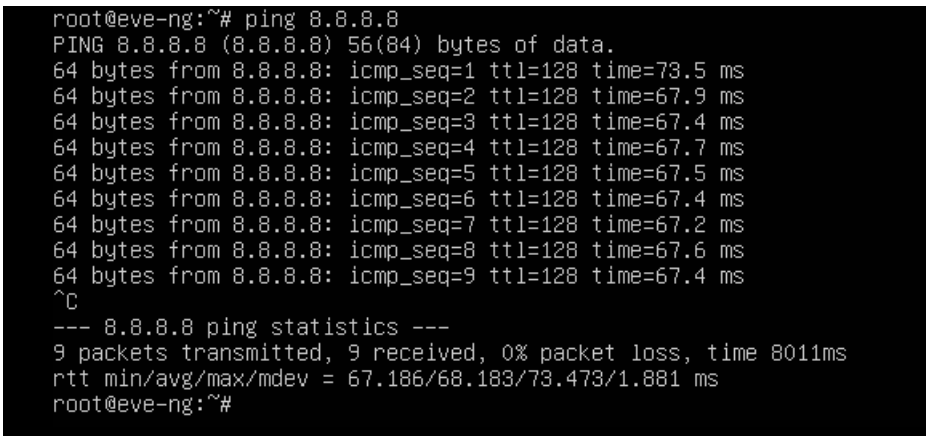


FIGURA 43 Salida de internet desde la MV EVE-NG

EVE-NG permite realizar el análisis de tráfico en cada una de las interfaces de los equipos que conforman la topología de red:

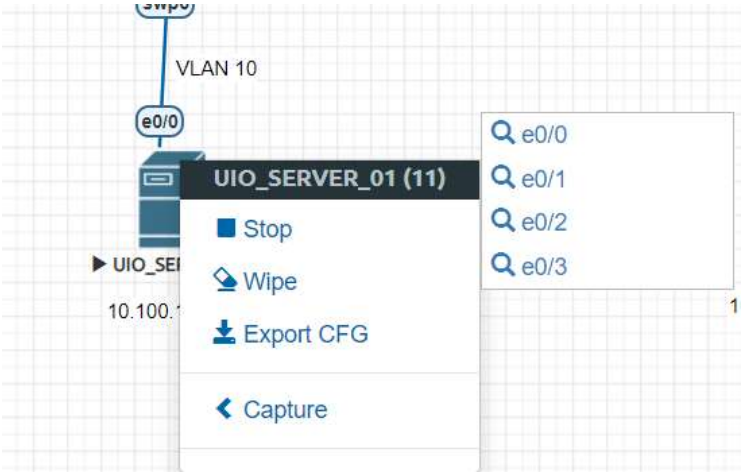


FIGURA 44 Interfaces del servidor UIO_SERVER_01

Si al momento de seleccionar la interfaz a analizar se despliega el siguiente error:

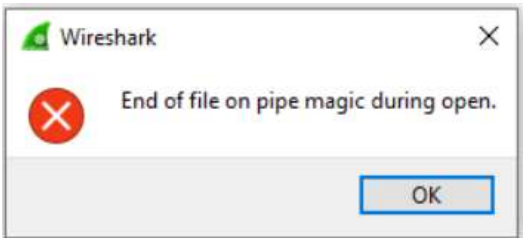


FIGURA 45 Pantalla de error de Wireshark

Es necesario editar el archivo **"wireshark_wrapper.bat"** dentro de la carpeta de programa EVE-NG. Este error se produce debido a que Wireshark no puede acceder al emulador con las claves de root que se encuentra establecidas por defecto en el archivo wireshark_wrapper.bat.

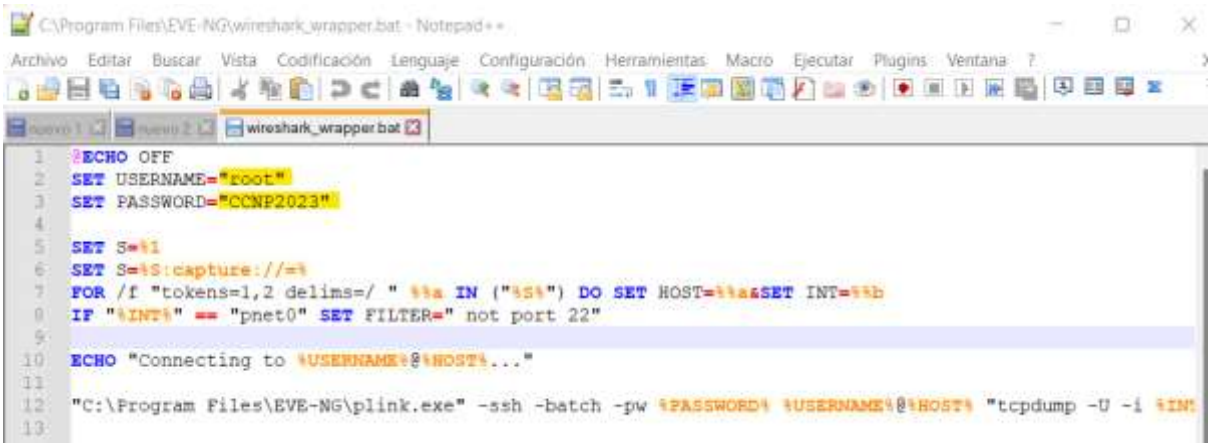


FIGURA 46 Archivo de texto de wireshark_wrapper.bat

Una vez editado el archivo mencionado, se debe reiniciar la máquina virtual, probar nuevamente salida a internet y reiniciar los equipos/servidores que conformar la topología de red y wireshark se ejecutará sin problemas.

Para la validación del tráfico VXLAN, se realizará la captura de ping entre los servidores ubicados en los Centros de Datos UIO y GYE. El análisis de tráfico se hará en las interfaces que interconectan las dos localidades en los equipos de borde DCI UIO y GYE.

- **UIO_DCI_01**

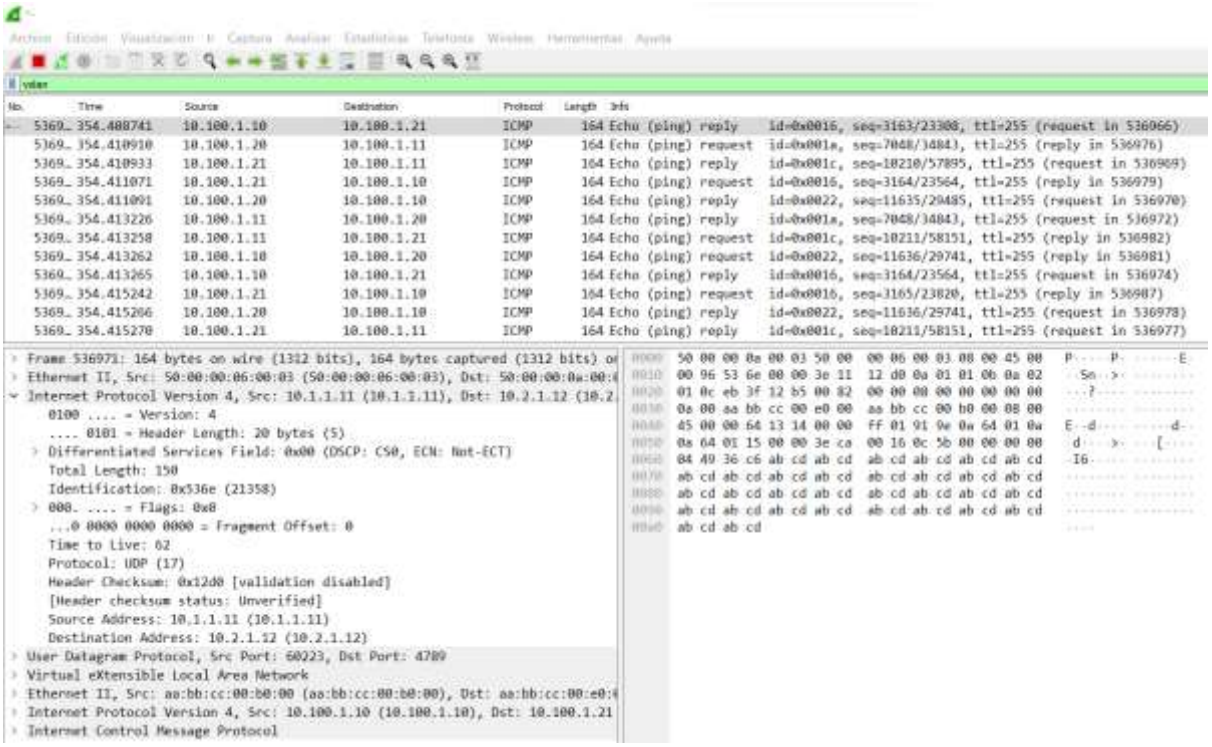


FIGURA 47 Análisis de tráfico en Wireshark desde el DCI_UIO

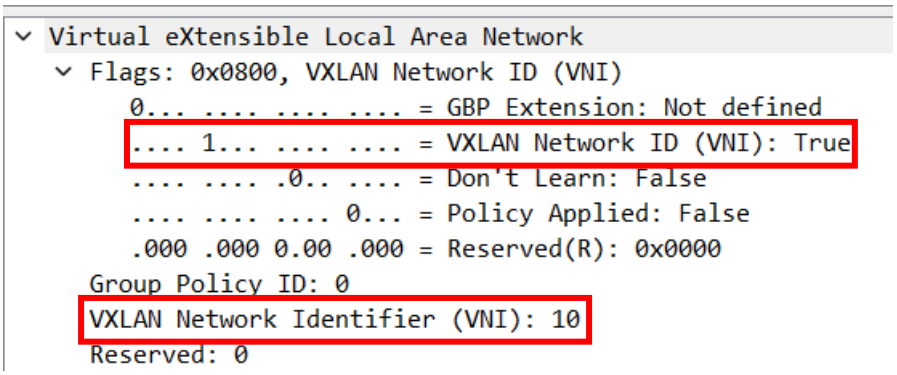


FIGURA 48 Validación de tráfico VXLAN desde DCI_UIO

- **GYE_DCI_01**

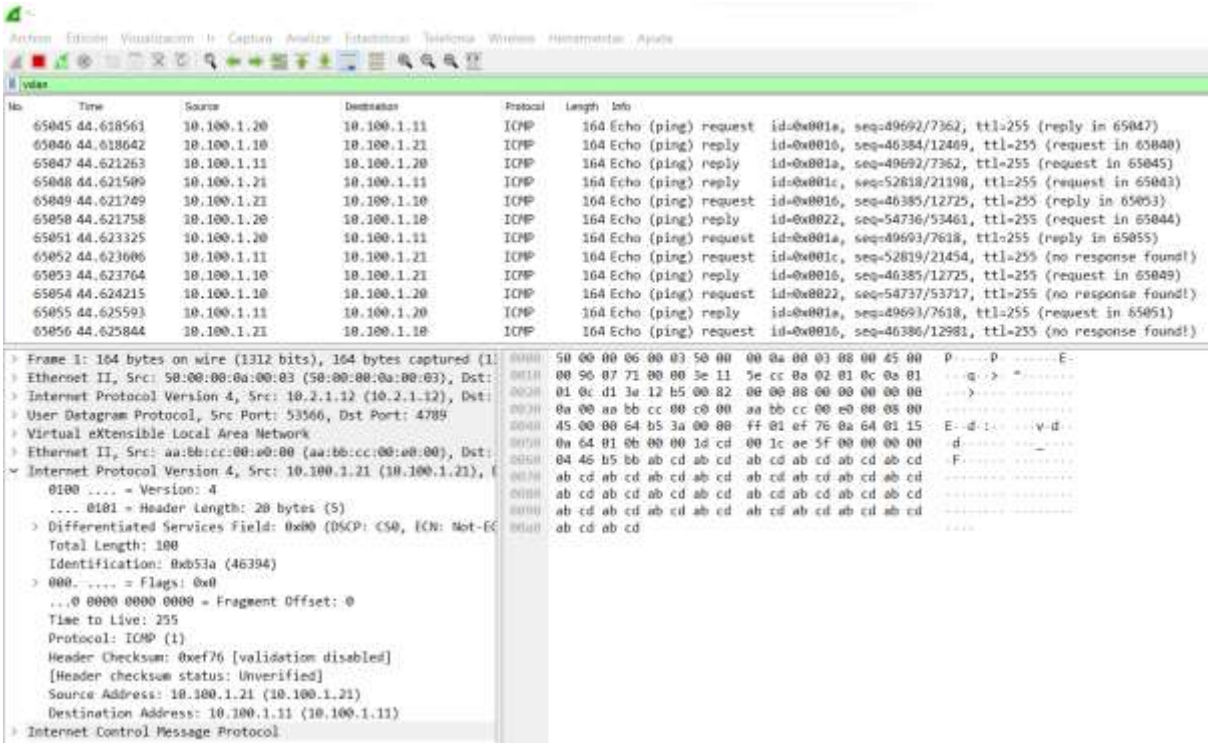


FIGURA 49 Análisis de tráfico en Wireshark desde el DCI_GYE

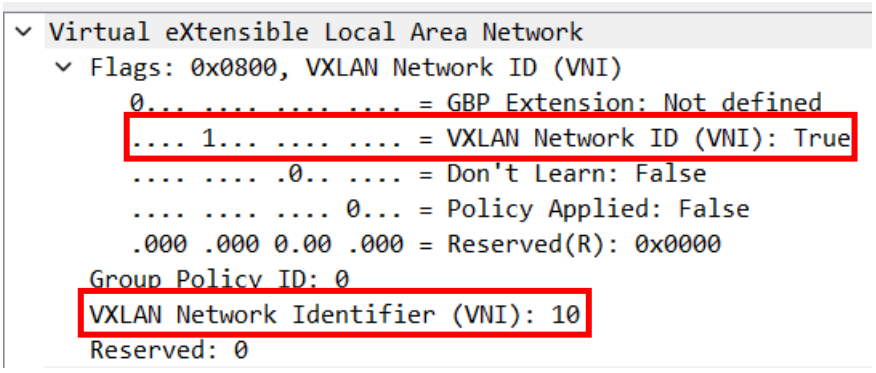


FIGURA 50 Validación de tráfico VXLAN desde DCI_GYE

CONCLUSIONES

Luego del análisis de la topología propuesta, se puede concluir que con la evolución de la tecnología en la nube y los enormes beneficios del multi-tenancy, los requisitos básicos de una arquitectura de red han cambiado por completo de una perspectiva de Centro de Datos único a Centros de Datos en múltiples ubicaciones. Esto ha requerido mejorar las arquitecturas existentes que priorizaban el tráfico norte – sur, y enfocarse en el tráfico este-oeste que continúa aumentando en los centros de data modernos.

Se valida en la emulación que, con una topología Spine and Leaf se logra la interconexión entre centros de datos separados geográficamente, brindado así también los beneficios de alta disponibilidad, latencia mejorada y ampliación de ancho de banda, soportando aplicaciones de alta demanda de usuarios.

Los beneficios de utilizar EVPN incluyen multi-inquilino, enrutamiento y puentes integrados y soporte para VXLAN. EVPN como solución L2 para DCI proporciona una convergencia más rápida cuando la VM se mueve de un DC a otro y también proporciona aprendizaje MAC remoto, lo que reduce así la inundación de unidifusión desconocida. Se concluye que el aprendizaje MAC en VXLAN es más eficiente y escalable.

Con la implementación de los prototipos VXLAN con EVPN se aprovechan beneficios importantes para clientes de centros de datos. Escalabilidad, una arquitectura basada en VXLAN-EVPN permite agregar conmutadores nuevos sin la necesidad de un rediseño de la red subyacente. Eficiencia operativa, con la expansión de operaciones de las empresas a lo largo del mundo, VXLAN-EVPN aborda los problemas que surgen debido a la distancia física entre los centros de datos; EVPN reduce la carga tanto en el plano de control como en el de datos y mejoran la eficiencia por la implementación de funciones como aprendizaje MAC remoto. Alto rendimiento, esta arquitectura proporciona el alto rendimiento requerido para satisfacer las demandas de los centros de datos modernos. Esto implica la necesidad de una rápida convergencia y agregación de enlaces, que se pueden lograr mediante el uso de una capa subyacente basada en IP de Capa 3 en combinación con una superposición de VXLAN-EVPN.

Se concluye que la emulación de una red programática tipo VXLAN-EVPN implementada a través de EVE-NG y con analizador de tráfico y protocolos WIRESHARK es totalmente factible, facilita y optimiza el trabajo del ingeniero de redes, simplificando la ejecución de tareas de configuración de la red, reduciendo los puntos de falla y se puede validar el comportamiento de los protocolos implementados, análisis de redundancias y adicionalmente, se trabajó con Cumulus Linux lo que elimina la necesidad de adquirir licencias para los equipos con los cuales se trabajó en la topología de red al ser un un sistema operativo de red abierto basado en Linux para conmutadores bare metal, lo que permitió construir de manera económica y operar de manera eficiente una topología de red como operadores de centros de datos.

Mediante las pruebas realizadas en el presente trabajo de titulación, se pudo validar que con la implementación de una topología de red Spine and Leaf basada en protocolos EVPN-VXLAN, se garantiza alta disponibilidad en los servidores implementados, la redundancia existente entre los spines, garantiza que haya una respuesta imperceptible en la conmutación cuando uno de los equipos falla, brindando continuidad en los servicios a los clientes de los centros de datos.

RECOMENDACIONES

Previo a la implementación de la topología propuesta, se debe validar que se encuentren instaladas todas las librerías necesarias para la configuración de protocolos en Cumulus Linux y EVE-NG.

Validar que el archivo wireshark_wrapper.bat de EVE-NG tenga la contraseña correcta del usuario root del emulador, con el fin de que Wireshark pueda realizar el análisis de tráfico y protocolos sin inconvenientes

Para trabajos futuros, se recomienda realizar el análisis con tecnologías IP FABRIC y explotar los beneficios que esta nueva arquitectura brindará a los centros de datos, tomando en cuenta que una arquitectura Spine and Leaf puede ser adaptada y reutilizada.

REFERENCIAS

ARUBA. (2022). *ARUBA NETWORKS*. Obtenido de www.arubanetworks.com

Ch, G. D. (2018, November). SDN-Ready WAN networks: Segment Routing in MPLS-Based Environments. In 2018 9th IEEE Annual Ubiquitous Computing. *Electronics & Mobile Communication Conference (UEMCON)*, (págs. 173 - 178).

Checkpoint. (2021). *Cyber Hub*. Obtenido de https://www.checkpoint.com/es/cyber-hub/what-is-a-data-center/

CISCO. (s.f.). *CISCO*. Obtenido de www.cisco.com

Davidson, J. (05 de 10 de 2019). *JD Networks*. Obtenido de https://jd-networks.co.uk/blog/2019/10/05/labbing-a-modern-datacentre/

Espín, E. F. (2018). *Desarrollo de una propuesta de administración y aprovisionamiento de clientes en el Data Center de Telconet de la ciudad de Quito basada en el uso de la tecnología VXLAN.* Trabajo de titulación, Centro de Posgrados, Quito.

GALLARDO, C. P. (2023). *PRUEBA DE CONCEPTO DE VXLAN-EVPN EN INFRAESTRUCTURA.* Quito.

Hernández, E. (31 de Agosto de 2020). *NET4DD*. Obtenido de https://net4dd.com/evolucion-de-la-topologia-de-data-center/

HUAWEI. (10 de Febrero de 2020). *Support Huawei.* Obtenido de https://support.huawei.com/enterprise/en/doc/EDOC1100125781/65029582/vxlan-packet-format

HUAWEI. (7 de Septiembre de 2022). *Comunidad Huawei Enterprise*. Obtenido de www.huawei.com

Jansen, D. &. (2017). *A modern, Open and Scalable Fabric VXLAN EVPN.* . San José, California: Cisco Press.

Juniper. (2020). *Juniper Netwiorks*. Obtenido de www.juniper.net

Naranjo, E. (2018). *Desarrollo de una propuesta de administración y aprovisionamiento de clientes en el Data Center de Telconet de la ciudad de Quito basado en el uso de la tecnología VXLAN.* Trabajo de titulación, Universidad de las Fuerzas Armadas ESPE, Centro de Posgrados, Quito.

Naranjo, E. F. (Octubre, 2017). 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.*

ORACLE. (Septiembre de 2014). *Gestión de virtualización de red y recursos de red.* Obtenido de https://docs.oracle.com/cd/E56339_01/html/E53790/gnmug.html

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

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

Salazar-Chacón, G., & Marcillo Parra, D. (2023). Infrastructure-as-Code in Open-Networking: Git, Ansible, and Cumulus-Linux Case Study. *13th Annual Computing an Communication Workshop and Conference (CCWC)* (pág. 6). Quito: IEEE.

Salinero, M. (8 de Abril de 2019). *laSalle Blogging*. Obtenido de https://blogs.salleurl.edu/es/protocolos-de-routing-i-switching-en-los-data-centers

TkmE Enviromental and Power Monitoring. (2017). *TkmE Enviromental and Power Monitoring.* Obtenido de https://www.tkme.net/como-funciona-un-data-center/

Zárate, S. E. (2017). *Análisis de Arquitecturas Modernas de Data Center.* Colombia.

ANEXOS

Configuraciones de los equipos

UIO-SPINE-01

```
cumulus@UIO-SPINE-01:~$ net show configuration commands
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65000
net add interface swp1-3 ipv6 nd ra-interval 5
net del interface swp1-3 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
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 neighbor swp3 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 add dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
```

```
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
net add interface swp1-3
net add loopback lo ip address 10.1.1.1/32
net add hostname UIO-SPINE-01
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
net commit
```

UIO-SPINE-02

```
cumulus@UIO-SPINE-02:~$ net show configuration commands
net del all
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65000
net add interface swp1-3 ipv6 nd ra-interval 5
net del interface swp1-3 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
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 neighbor swp3 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 add dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
net add interface swp1-3
net add loopback lo ip address 10.1.1.2/32
net add hostname UIO-SPINE-02
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
net commit
```

GYE-SPINE-01

```
cumulus@GYE-SPINE-01:~$ net show configuration commands
net del all
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65001
net add interface swp1-3 ipv6 nd ra-interval 5
net del interface swp1-3 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
net add bgp router-id 10.2.1.1
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 neighbor swp3 interface peer-group fabric
net add bgp ipv4 unicast network 10.2.1.1/32
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 add dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
net add interface swp1-3
net add loopback lo ip address 10.2.1.1/32
net add hostname GYE-SPINE-01
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
net commit
```

GYE-SPINE-02

```
cumulus@GYE-SPINE-02:~$ net show configuration commands
net del all
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65001
net add interface swp1-3 ipv6 nd ra-interval 5
net del interface swp1-3 ipv6 nd suppress-ra
```

```
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
net add bgp router-id 10.2.1.2
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 neighbor swp3 interface peer-group fabric
net add bgp ipv4 unicast network 10.2.1.2/32
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 add dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
net add interface swp1-3
net add loopback lo ip address 10.2.1.2/32
net add hostname GYE-SPINE-02
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
net commit
```

UIO-LEAF-01

```
cumulus@UIO-LEAF-01:~$ net show  configuration commands
net del all
```

```
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65010
net add interface swp1-2 ipv6 nd ra-interval 5
net del interface swp1-2 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
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 dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
net add vxlan vni-10 vxlan id 10
net add bridge bridge ports swp3,vni-10
net add bridge bridge vids 10
net add bridge bridge vlan-aware
net add interface swp1-2
net add interface swp3 bridge access 10
net add loopback lo ip address 10.1.1.11/32
```

```
net add vxlan vni-10 bridge access 10
net add vxlan vni-10 stp bpduguard
net add vxlan vni-10 stp portbpdufilter
net add vxlan vni-10 vxlan local-tunnelip 10.1.1.11
net add hostname UIO-LEAF-01
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
net commit
```

UIO-LEAF-02

```
cumulus@UIO-LEAF-02:~$ net show configuration commands
net del all
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65011
net add interface swp1-2 ipv6 nd ra-interval 5
net del interface swp1-2 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
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 dns nameserver ipv4 10.0.2.3
```

```
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
net add vxlan vni-10 vxlan id 10
net add bridge bridge ports swp3,vni-10
net add bridge bridge vids 11
net add bridge bridge vlan-aware
net add interface swp1-2
net add interface swp3 bridge access 11
net add loopback lo ip address 10.1.1.12/32
net add vxlan vni-10 bridge access 11
net add vxlan vni-10 stp bpduguard
net add vxlan vni-10 stp portbpdufilter
net add vxlan vni-10 vxlan local-tunnelip 10.1.1.12
net add hostname UIO-LEAF-02
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
 net commit
```

GYE-LEAF-01

```
cumulus@GYE-LEAF-01:~$ net show  configuration commands
net del all
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65020
net add interface swp1-2 ipv6 nd ra-interval 5
net del interface swp1-2 ipv6 nd suppress-ra
```

```
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
net add bgp router-id 10.2.1.11
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 10.2.1.11/32
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 dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
net add vxlan vni-10 vxlan id 10
net add bridge bridge ports swp3,vni-10
net add bridge bridge vids 20
net add bridge bridge vlan-aware
net add interface swp1-2
net add interface swp3 bridge access 20
net add loopback lo ip address 10.2.1.11/32
net add vxlan vni-10 bridge access 20
net add vxlan vni-10 stp bpduguard
net add vxlan vni-10 stp portbpdufilter
net add vxlan vni-10 vxlan local-tunnelip 10.2.1.11
net add hostname GYE-LEAF-01
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
 net commit
```

GYE-LEAF-02

```
cumulus@GYE-LEAF-02:~$ net show configuration commands
net del all
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65021
net add interface swp1-2 ipv6 nd ra-interval 5
net del interface swp1-2 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
net add bgp router-id 10.2.1.12
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 10.2.1.12/32
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 dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
```

```
net add vxlan vni-10 vxlan id 10
net add bridge bridge ports swp3,vni-10
net add bridge bridge vids 21
net add bridge bridge vlan-aware
net add interface swp1-2
net add interface swp3 bridge access 21
net add loopback lo ip address 10.2.1.12/32
net add vxlan vni-10 bridge access 21
net add vxlan vni-10 stp bpduguard
net add vxlan vni-10 stp portbpdufilter
net add vxlan vni-10 vxlan local-tunnelip 10.2.1.12
net add hostname GYE-LEAF-02
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
 net commit
```

UIO-DCI-01

```
cumulus@UIO-DCI-01:~$ net show configuration commands
net del all
net add time zone Etc/UTC
net add time ntp server 0.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 1.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 2.cumulusnetworks.pool.ntp.org iburst
net add time ntp server 3.cumulusnetworks.pool.ntp.org iburst
net add time ntp source eth0
net add snmp-server listening-address localhost
net add bgp autonomous-system 65012
net add interface swp1-3 ipv6 nd ra-interval 5
net del interface swp1-2 ipv6 nd suppress-ra
net add routing defaults datacenter
net add routing service integrated-vtysh-config
net add routing log syslog informational
net add bgp router-id 10.1.1.13
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 neighbor swp3 interface peer-group fabric
        net add bgp ipv4 unicast network 10.1.1.13/32
        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 dns nameserver ipv4 10.0.2.3
        net add ptp global slave-only no
        net add ptp global priority1 255
        net add ptp global priority2 255
        net add ptp global domain-number 0
        net add ptp global logging-level 5
        net add ptp global path-trace-enabled no
        net add ptp global use-syslog yes
        net add ptp global verbose no
        net add ptp global summary-interval 0
        net add ptp global time-stamping
        net add interface swp1-3
        net add loopback lo ip address 10.1.1.13/32
        net add hostname UIO-DCI-01
        net add dot1x radius accounting-port 1813
        net add dot1x radius authentication-port 1812
        net add dot1x eap-reauth-period 0
        net add dot1x mab-activation-delay 30
net commit
```

GYE-DCI-02

```
        net del all
        net add time zone Etc/UTC
        net add snmp-server listening-address localhost
        net add bgp autonomous-system 65022
        net add interface swp1-3 ipv6 nd ra-interval 5
        net del interface swp1-2,4 ipv6 nd suppress-ra
        net add routing defaults datacenter
        net add routing service integrated-vtysh-config
        net add routing log syslog informational
        net add bgp router-id 10.2.1.13
        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 neighbor swp3 interface peer-group fabric
net add bgp ipv4 unicast network 10.2.1.13/32
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 dns nameserver ipv4 10.0.2.3
net add ptp global slave-only no
net add ptp global priority1 255
net add ptp global priority2 255
net add ptp global domain-number 0
net add ptp global logging-level 5
net add ptp global path-trace-enabled no
net add ptp global use-syslog yes
net add ptp global verbose no
net add ptp global summary-interval 0
net add ptp global time-stamping
net add interface swp1-3
net add loopback lo ip address 10.2.1.13/32
net add hostname GYE-DCI-02
net add dot1x radius accounting-port 1813
net add dot1x radius authentication-port 1812
net add dot1x eap-reauth-period 0
net add dot1x mab-activation-delay 30
net commit
```

Código referenciado de (Davidson, 2019)