ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELECTRÍCA Y ELECTRÓNICA

AUTOMATIZACIÓN DE REDES UTILIZADAS PARA EOT

ANÁLISIS CONCEPTUAL DEL PROTOCOLO VXLAN PARA LA VIRTUALIZACIÓN DE CENTRO DE DATOS PARA EOT

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

ANDRES PAUL RAZO ACHIG

andres.razo@epn.edu.ec

DIRECTOR: MSc. CARLOS ROBERTO EGAS ACOSTA

carlos.egas@epn.edu.ec

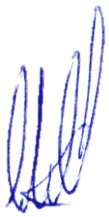
DMQ, Agosto 2022

CERTIFICACIONES

Yo, ANDRES PAUL RAZO ACHIG declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

ANDRES PAUL RAZO ACHIG

Certifico que el presente trabajo de integración curricular fue desarrollado por ANDRES PAUL RAZO ACHIG, bajo mi supervisión.



Msc. CARLOS ROBERTO EGAS ACOSTA

DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

ANDRES PAUL RAZO ACHIG

Msc. CARLOS ROBERTO EGAS ACOSTA

DEDICATORIA

A mis padres, hermano, sobrino, amigos, compañeros y profesores que con paciencia me orientaron para poner todas mis capacidades en esta carrera que he decidido seguir yo. Ellos supieron darme su confianza y apoyarme en todas mis etapas estudiantiles de mi carrera profesional que he vivido para hoy poder obtener este título que es el fruto de la confianza y apoyo moral de mi familia y demás allegados.

AGRADECIMIENTO

Mi sincero agradecimiento a Dios y a mis distinguidos maestros quienes, con paciencia, entusiasmo depositaron sus sabios conocimientos y así formaron en mi un profesional con capacidades intelectuales para ejercer con responsabilidad esta carrera y pueda llegar hacer un excelente Ingeniero.

Agradezco a la Escuela Politécnica Nacional por su enseñanza, su formación humana y profesional.

ÍNDICE DE CONTENIDO

TABLA DE ILUSTRACIONES

RESUMEN

Este trabajo de integración curricular está enfocado a realizar un análisis conceptual del protocolo VXLAN, el cual en la teoría ayuda como un extensor de una red VLAN, se tomará como punto de partida la virtualización para entender su concepto y sus diferentes aplicaciones, de igual manera se estudiará las diferentes arquitecturas de red de centros de datos y sus topologías desde las más conocidas hasta las menos conocidas, sus capacidades para escalar y para ser administradas.

Al estudiar VXLAN partiremos desde su nacimiento, su conceptualización, su estructura, su forma de difundirse en la red, su arquitectura y en la arquitectura se hablará de las redes superpuestas, y sobre puestas de igual manera se estudiará los comandos necesarios para poder configurar en los equipos.

Como parte final se implementará un prototipo el cual estará implementado con el emulador gns3 y las imágenes ISO de los Routers CSR 1000 V para realizar la captura de paquetes y poder visualizar la forma de encapsulación, demostrando de esta forma que el protocolo es funcional y que efectivamente funciona como una extensión de VLAN, en dicho prototipo se usara la topología spine and leaf, se configurara los VNI correspondientes al igual que los VNE, para formar un bridge-domain.

PALABRAS CLAVE: VTEP, VNI, VNE, Bridge-Domain, VDC, Spine, Leaf

ABSTRACT

This curricular integration work is focused on performing a conceptual analysis of the VXLAN protocol, which in theory helps as an extender of a VLAN network, virtualization will be taken as a starting point to understand its concept and its different applications, in the same way the different network architectures of data centers and their topologies will be studied from the best known to the least known, its capabilities to scale and to be managed.

When studying VXLAN we will start from its birth, its conceptualization, its structure, its way of spreading in the network, its architecture and in the architecture, we will talk about the superimposed networks, and on the same way the necessary commands will be studied to be able to configure in the equipment.

As a final part, a prototype will be implemented which will be implemented with the gns3 emulator and the iso images of the CSR 1000 V Routers to perform packet capture and be able to visualize the form of encapsulation, demonstrating in this way that the protocol is functional and that it effectively works as a VLAN extension, in this prototype the spine and leaf topology will be used, the corresponding NIVs will be configured as well as the VNE, to form a bridge-domain.

KEYWORDS: VTEP, VNI, VNE, Bridge-Domain, VDC, Spine, Leaf

1 INTRODUCCIÓN

VXLAN (*Virtual Extensible Local Area Network*) nace de una propuesta de los grandes proveedores de servicios de virtualización como son Arista, Bradcom, Intel, VMware, entre otros, los cuales desarrollaron las especificaciones necesarias para mejorar el tema de escalabilidad de VXLAN en centros virtualizados.[1] La virtualización es la clave para tener un mejor índice de utilización en un servidor, además poder mover máquinas virtuales entre servidores mientras estas se ejecutan, lo cual con llevaba a un mejor administración y un uso más eficiente de los servidores, sin tener que caer en baja disponibilidad de servicios dichas marcas se dieron cuenta que estas estaban limitadas por la subdivisión que presentan las redes pues al tratar de mover una VM(*Virtual machine*) de una red a otra esto provocaba problemas, como la nueva configuración de direcciones IP y sobre todo la duplicación de direcciones IP.[1]

En vista de todo esto se crea el protocolo VXLAN el cual es un protocolo para super poner redes específicamente las de capa 2 sobre las de capa 3 del modelo OSI consiguiendo que el tráfico de ethernet sea dirigido sobre IP y provocando una encapsulación MAC-UDP.[2] Como una solución para los centros de datos de múltiples inquilinos debido a que un administrador de red trata de tener su red lo más aislada posible y manejando un tráfico individual, actualmente esto se lo realiza con el protocolo VLAN pero cuando se trata de equipos virtualizados y de clientes que necesitan un uso mayor de VLANS, estas se ven muy limitadas, debido a que solo se pueden crear 4094 VLANS, a comparación de VXLAN la cual cuenta con 16 millones de redes virtuales.[3]

En la actualidad casi un 95% de cambios en las redes los realiza el personal de TI. No obstante, el problema más relevante que enfrentan los administradores de redes es el incremento en los costos de TI en lo que a operaciones de red se refiere[4], pues el costo de operativos puede duplicar o triplicar el costo de la red, de igual manera el incremento exponencial de los datos y dispositivos empieza a exceder sus capacidades, convirtiendo a las operaciones manuales en algo casi imposible de realizar. De la misma manera existen otros problemas como resultado de la manipulación como son: errores de configuración, incoherencias en la red, problemas en implementar cambios a gran escala e interrupciones de red.

En la actualidad la alta demanda de equipos virtuales origina problemas en direccionamiento y segmentación de la red que a través de los años se ha tratado de mitigar con los protocolos de encapsulamiento como es IEEE 802.1q como una solución[3], pero

la misma consta de la limitación en cantidad de VLANS que se pueden generar y también de falta de flexibilidad, escalabilidad.

El presente trabajo tiene como objetivo presentar un análisis conceptual del protocolo VXLAN y como ayuda a solventar problemas en la virtualización de centros de datos, además de un estudio de las redes tradicionales y redes de nueva generación.

1.1 OBJETIVO GENERAL

- Analizar conceptualmente el protocolo VXLAN para la virtualización de Centro de Datos.

1.2 OBJETIVOS ESPECÍFICOS

1. Describir los fundamentos teóricos de los centros de datos.
2. Investigar el estado actual de los protocolos VXLAN en centros de datos.
3. Validar el funcionamiento del protocolo VXLAN en un habiente emulado.

1.3 ALCANCE

El presente trabajo, consta de las siguientes fases:

A. Fase de Planteamiento

Se propone estudiar las redes tradicionales y las redes de nueva generación, también se estudiará conceptualmente el protocolo VXLAN y como este podría ayudar en el manejo de equipos que han sido virtualizados dentro de la infraestructura de centros de datos y como mejora su operabilidad.

Se estudiará los conceptos de la tecnología VXLAN, el protocolo 802.1q, además el estado actual de la virtualización de centros de datos, y se pretende abarcar el estudio de la información relacionado con mecanismos de virtualización de la recopilación de información y que tan posicionados están en la industria.

En esta fase hablaremos de lo que son las redes overlay y las redes underlay las cuales son el tema principal de donde parte el protocolo VXLAN.[3]

B. Fase de implementación

Se presentará la implementación de un prototipo sobre lo estudiado previamente, en un ambiente de emulación en el cual se pretende visualizar cuan fácil o complejo es la implementación del protocolo VXLAN y sus características principales, el uso de los comandos a utilizar en los equipos emulados para la configuración utilizando emuladores

de red. Los escenarios de pruebas en base a las ventajas que se tiene con la utilización de VXLAN y los requerimientos para evidenciar las, Tanto los escenarios de pruebas como los requerimientos dependerán de los resultados obtenidos en la fase teórica.[4]

C. Fase de análisis

Se presentarán los resultados de comparar el protocolo VXLAN con el protocolo 802.1q en infografías, además se llevará a cabo un análisis de resultados en la que se definirá en base al análisis previo los parámetros necesarios para la obtención de la mejor eficiencia al implementar este protocolo y como es que mejora el procesamiento de los centros de datos.

En este trabajo no se obtendrá un producto final demostrable.

1.4 MARCO TEÓRICO

1.4.1 CENTRO DE DATOS

Un centro de datos es una instalación física que las instituciones públicas o privadas tienen para el almacenamiento de sus aplicaciones y la información sensible. Un centro de datos está compuesto por varios equipos de red como son ruteadores, conmutadores firewalls, servidores y sistemas de almacenamiento, todo esto con el afán de administrar, manejar y difundir una cantidad masiva de información [5], [6].

1.4.2 TOPOLOGIAS DE CENTRO DE DATOS

Hoy en día se encuentran vigentes tres tipos de topologías para centros de datos, una topología hace referencia a la forma en la que se encuentran distribuidos los equipos ya sean estos nodos o Pcs físicamente.[7]

1.4.2.1 Topología centralizada

La topología centralizada es aquella que tiene separada la red LAN (*Local Área Network – Red de área local*) de la red SAN (S*torage Área Network*- Área de red de almacenamiento[1]), cada área tiene su cableado correspondiente que a su vez va a los servidores y de regreso a los conmutadores principales, se puede observar en la Figura. 1.1. Esta topología está orientada para usarse en empresas pequeñas y en centros de datos de no más de 468 metros cuadrados o 5000 pies cuadrados de área, no es una topología muy adecuada para escalamientos, en centros de datos de más área, las longitudes excesivas por tramo de cable provocan un mal funcionamiento, esto provoca congestión en las comunicaciones.[7]

[1] **Área de red de almacenamiento** es una red especializada de alta velocidad que proporciona acceso de red a dispositivos de almacenamiento, general mente compuesta por host conmutadores y elementos de almacenamiento [7]

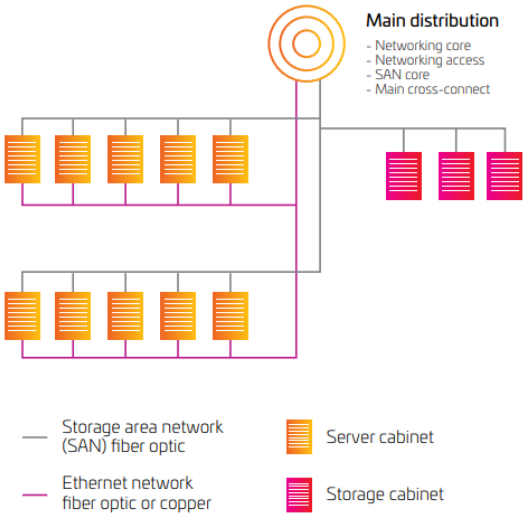


Figura. 1.1: Topología centralizada[7]

1.4.2.2 Topología dividida por zonas

Una topología dividida por zonas es una topología en la cual cada zona tiene un switch principal para conectar los servidores, dicho equipo puede ir tanto al final de la fila (*EoR-End of Row*) como a la mitad (*MoR – Middle of Row*), esta topología cuenta con las ventajas de fácil escalabilidad, replicable, imaginable de bajo costo de cableado y realiza el mejor uso de los puertos del switch como se puede evidenciar en la Figura. 1.2 [7]

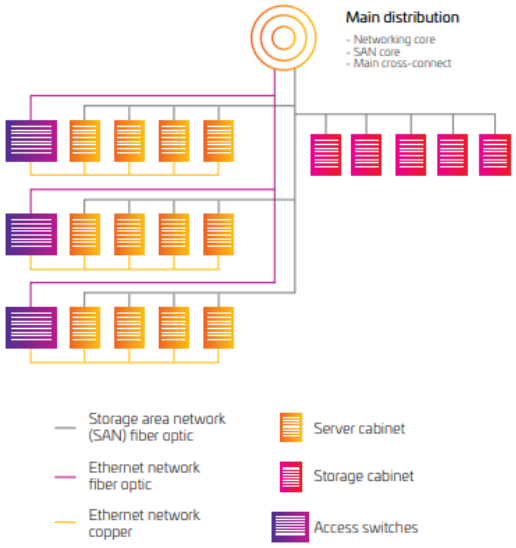


Figura. 1.2: Topología divida por zonas[7]

1.4.2.3 Topología *top of rack* (ToR)

Es una topología en la cual cada rack tendrá su propio equipo de conmutación, este a su vez se comunicará a la distribución principal y estos a la red SAN, la ventaja de esta topología es minimizar los costos por cableado, esta topología puede llegar a ser complicada de administrar cuando de centros de datos grande se trata y también

representa más costos en equipos con relación a la topología por zonas como se puede apreciar en la Figura. *1.3* [7]

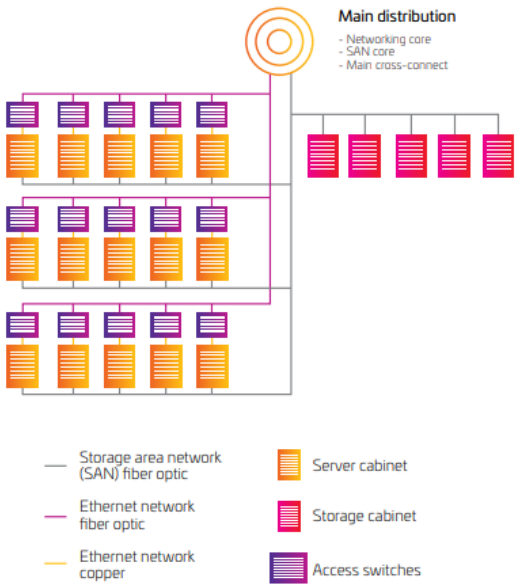


Figura. 1.3: Topología *Top of Rack* [7]

1.4.3 ARQUITECTURAS PARA CENTROS DE DATOS

Los centros de datos tienen típicamente tres partes las cuales son: arquitectura red de centro de datos, seguridad y arquitectura informática. [7]

1.4.3.1 Arquitectura de red de centro de datos

Se enfoca principalmente en la distribución y disposición de los dispositivos de red. Hay 4 tipos de arquitectura para centro de datos:

- **Arquitectura de red mallada (*Mesh Network)***: es una arquitectura que se caracteriza por su transmisión de datos predecibles al mismo tiempo que reduce la latencia, es una de las arquitecturas que se adapta de forma más rápido a los servicios en la nube, es una red totalmente redundando lo que ayuda en la disponibilidad de las aplicaciones, como se aprecia en la Figura. 1.4 [7]

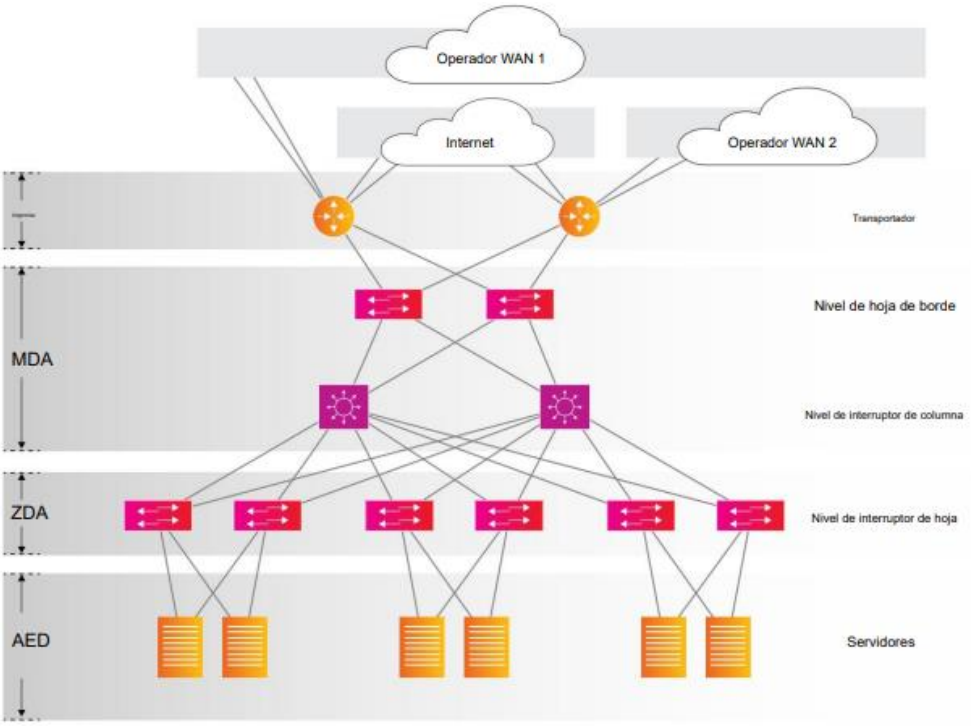


Figura. 1.4: Arquitectura de red mallada [7]

- **Arquitectura Modelo de tres niveles o multinivel**: en esta arquitectura se dispone de la capa de servidores web, de la capa aplicación y de la capa de almacenamiento, esta arquitectura debido a su distribución ayuda a su crecimiento independiente una capa de otra, como se puede apreciar en la Figura. 1.5. [8]

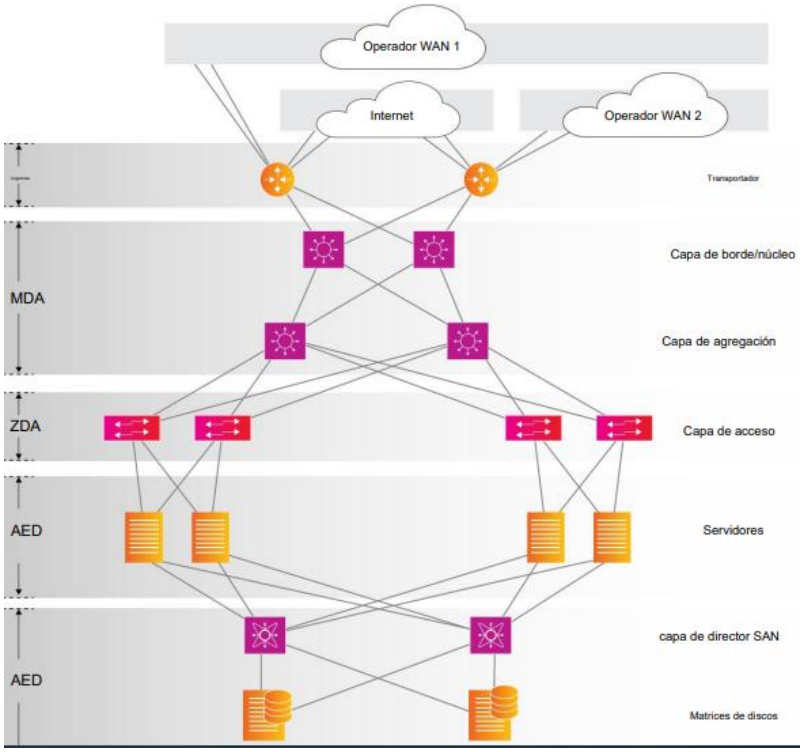


Figura. 1.5: Arquitectura Modelo de tres niveles o multinivel [7]

- **Arquitectura Mallada con punto de entrega (PoD - Point of Delivery)**, es una arquitectura modular, escalable y repetible, un PoD tiene equipos de red, almacenamiento, y aplicaciones. Cada PoD consta de una serie de conmutadores interconectados en la capa de acceso, seguido de la capa de servidores y para terminar con la capa SAN, es decir es una PoD es una arquitectura de 3 capas que a subes se interconecta con la capa de distribución principal, como se puede apreciar en la **Figura. 1.6**.

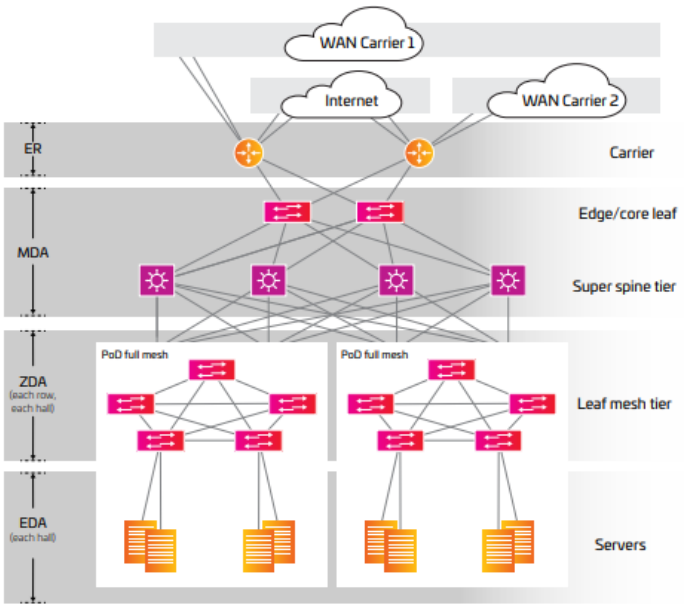


Figura. 1.6: Arquitectura Mallada con punto de entrega (PoD)[7]

- **Arquitectura de malla Super Spine**, son redes diseñadas para implementarlas en ambientes donde se necesita híper escalabilidad como los centros de datos ya que esta es ideal para servicios que manejan grandes cantidades de datos. [7]

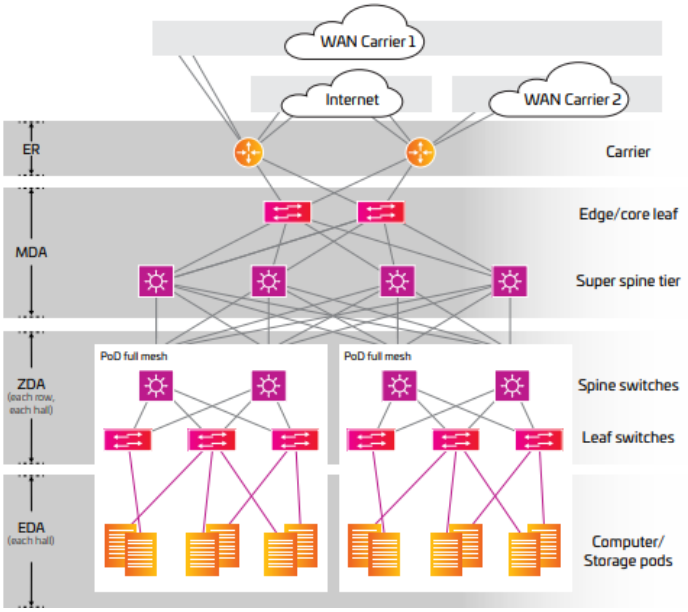


Figura. 1.7: Arquitectura de malla Super Spine [7]

1.4.3.2 Arquitectura de seguridad de centro de datos

Este tipo de arquitectura hace referencia a las buenas prácticas tanto físicas como informáticas de mitigar las amenazas de ataques y de accesos no autorizados.[9]

1.4.3.3 Arquitectura informática del centro de datos

Es la encargada de reducir los problemas de latencia y ancho de banda para la transmisión con la finalidad de reducir gastos, tener implementaciones rápidas y escalabilidad.[9]

1.4.4 VIRTUALIZACIÓN

Se la puede considerar a la virtualización como el efecto de la abstracción de los recursos de los computadores, la virtualización no es más que la creación de VM (Virtual Machine - Máquinas virtuales) que imitan el funcionamiento del hardware con la ayuda de software que a su vez comparten recursos físicos de una maquina real.[10]

La virtualización no solo se enfoca en la creación de VM también se enfoca en diferentes funciones que se encuentran en los centros de datos de los cuales se describen a continuación.[11]

1.4.4.1 Tipos de virtualización

- **Virtualización del servidor**: con lleva a utilizar un hipervisor que a su vez funciona como un emulador de un host físico en el cual se pueden colocar sistemas operativos individuales.[12] Lo que permite que varios sistemas operativos se ejecuten dentro de un servidor físico, un servidor por lo general, sin la virtualización está usando solo un 15% de su capacidad, la virtualización de un servidor implica tener una máquina virtual de alto rendimiento que viene ligado a un aumento en la productividad y servidores con costos mínimos. [11]

- **Virtualización de redes:** es la duplicación de las redes físicas en su totalidad, la cual permitirá correr las aplicaciones de igual manera que en la red física, pero con todas las prestaciones que conlleva la virtualización, en este tipo de virtualizaciones se pueden apreciar todos los equipos de red semejante a la realidad. [13]

- **Virtualización de escritorios:** son imágenes listas y configuradas de los sistemas operativos que incluyen las aplicaciones a utilizase las cuales no tiene un hardware como tal y su usuario puede acceder desde cualquier lugar ya que estas van a estar en un ambiente virtualizado. [14]

- **Virtualización de almacenamiento** o también conocido como almacenamiento definido por software (SDN - Software Defined Network), se refiere al proceso de

conceptualización del almacenamiento físico en almacenamiento lógico. Se propone como una solución a las necesidades crecientes de almacenamiento de datos, constituyendo una importante técnica para el ahorro de recursos. Se implementa adicionando una capa de software y/o hardware entre el sistema de dispositivos de almacenamiento físico y los Sistemas Operativos (S.O.) de los elementos que lo utilizan y comparten. [10]

- **Virtualización de aplicaciones:** es una manera de hacer creer a la aplicación que está ejecutándose sobre sistema operativo para lo cual se necesita agregar una capa de virtualización entre la aplicación y el sistema operativo, este tipo de virtualización se usa en conjunto con la virtualización de escritorio. [15]

1.4.4.2 Principios de la virtualización

Los diferentes principios por los que se generó la necesidad de virtualizar los equipos de red son:

- **Hardware de los servidores infrautilizados**, significa que los servidores no operan a su máxima capacidad de cómputo sino apenas usan un 15 a 20% lo que conlleva a tener una ineficiencia de 80 a 85%. [16]

- **Agotamiento de los espacios** en los centros de datos, el espacio físico que ocupa un rack es muy grande y si bien los centros de datos son amplios estos espacios tienden a agotarse todo esto debido al gran crecimiento informático que se tiene en la actualidad. [16]

- **Demanda de una mejor eficiencia energética**, en retrospectiva el consumo de energía de hace 5 años con respecto a este año en los centros de datos se han incrementado, lo que indica que se debe gestionar mejor el uso de la energía para los servidores que se tiene ya funcionando, esto conjunto con el bajo rendimiento de los servidores convencionales hacen necesario el uso de tecnologías de virtualización que ayuden a mejorar este rendimiento de cómputo y a su vez a no aumentar físicamente más servidores que representen más gastos por energía. [16]

- **Costo de administración de sistemas**, el costo de mantener una infraestructura física es grande, el técnico debe encontrarse en el centro de datos para monitorear los servidores, darle mantenimiento, cambiar piezas etc. son tareas laboriosas y que incrementan los costos de facturación, el uso de la virtualización hace que estas tareas sean realizadas por vía remota reduciendo costos operativos, por que brindan todas las facilidades para dar mantenimiento, realización de backup, actualización de software entre otras. [16]

- **Necesidad de alto rendimiento y alta disponibilidad** con los tipos de negocios que hoy en día existen, la alta disponibilidad, fiabilidad y rendimiento son características que buscan los cliente de los grandes proveedores de servicios todo esto acompañado de los servidores infrautilizados, hace más notoria la necesidad de la técnica de virtualización, para cumplir con la meta de alto rendimiento y alta disponibilidad siempre será necesario el aumento de nuevos servidores, los cuales estarán a la espera de realizar balanceo de carga o resolución de problemas, todos estos nuevos servidores se los podría virtualizar para tener una consolidación de servidores sin tener que adquirir hardware nuevo y sin caer en más gastos energéticos e infrautilización de servidores. [16]

1.4.4.3 Herramientas de virtualización

Entre las mejores herramientas de virtualización se encuentran las siguientes:

- **VirtualBox**, considerado uno de los mejores por ser de libre uso y soportado por diferentes plataformas como Windows, MAC OS, Linux, solaris, de fácil uso. [17]
- **Citrix XenServer**, destaca por ser un software de virtualización de servidores, con un entorno administrable seguro y fiable, soportado por Windows, Linux, cuenta con versiones free, versiones premium.
- **Sanboxie**, destacado por ser software para realizar pruebas de *malware*, especializado para realizar ambientes aislados sin la posibilidad de afectar al entorno físico. [18]
- **VMware Workstation Pro**, es una Plataforma muy avanzada para la virtualización tiene dos plataformas VMware player, la cual se utiliza para la virtualización de sistemas operativos y VMware Workstation la cual se utiliza para la virtualización de una maquina completa además de las características que permite la virtualización de servidores, redes entre otros. [19]
- **Cameyo**, es una plataforma que se encarga de entregar aplicaciones virtuales, permitiendo a los usuarios una forma de trabajar fácil y eficiente, está alojado en Google Cloud y Microsoft Azure. [20]
- **Parallels**, es una aplicación que admite diferentes tipos de S.O. en una sola maquina física es decir permite tener Windows y MACOS sin la necesidad de particionar el disco y reiniciar el equipo para cambiar de sistema operativo es decir como su nombre lo indica los S.O.s funcionan en paralelo. [21]

- **Xen Hipervisor**, es una herramienta de virtualización que trabaja en el nivel de más altos privilegios, es de código abierto. [17]
- **QEMU**, se popularizo por ser una plataforma *Open Source*, soportada tanto por Windows, MAC OS y Linux, aunque uno de sus contras es que no tiene interface de usuario. [17]
- **Microsoft Hyper-V Server**, es una herramienta que intenta emular a VMware, es una herramienta que permite emular sistemas Windows y algunos S.O. de código abierto.
- **KVM[2],** software de licencia abierta, capas de correr máquinas virtuales desde una imagen ISO con S.O [3]y proporcionando tarjetas de red a cada máquina virtual. [17]
- ***Aviat Design,*** software para virtualización de redes, se usa principalmente para la automatización y virtualización de las redes Wireless, proporcionado por el SAAS[4] de *Aviat Design.* [18]

1.4.5 ESTADO ACTUAL DE LA VIRTUALIZACION DE CENTROS DE DATOS

Para entender la actualidad que viven los centros de datos primero se debe definir bien un VDC (Virtual Data Center – centro virtual de Datos).

Un VDC se lo puede considerar como un contenedor de red privado, al cual se le puede agregar más y más servidores virtuales, los cuales pueden tener diferentes características ya sea de capacidad, procesamiento, sistema operativo, etc. [22]

Además de tener su propio segmento de red, protección y seguridad también cuentan con lo mejor en el campo de la conectividad, los VDC son hoy en día considerados como IaaS. [22]

Un VDC dependiendo del proveedor puede contar con las siguientes características:[23]

- Arquitectura de red definida
- Conexión a internet
- Panel de control en línea
- Integración con herramientas de respaldo
- Firewall

[2] **KVM:** *Kernel-based Virtual Machine*
[3] **S.O:** Operating System
[4] **SAAS**: *Software As A Service*

- Altamente escalable
- Flexible
- Capacidad de crear redes públicas o privadas

Como se observar todo esto hace que las empresas reduzcan de una gran manera sus costos de operación, dejando una gran responsabilidad al proveedor y mas no a ellas.

En la Tabla 1 se presenta las ventajas y desventajas presentes en los VDCs.

Tabla 1: Ventajas de VDC basada en [16][24][25][26][27][28][29][22]

Ventajas	Desventajas
Gran escalabilidad	Gran diversidad
Movilidad de datos	Distribución de recursos inadecuada
Migración de máquinas en caliente	Fallos críticos en maquina física
Ahorros en Costos	Tiempo de capacitación del personal
Reducción de costos en infraestructura y bienes raíces	Menor rendimiento del al VM comparado con la maquina física
Seguridad y menor riesgo de falla	
Aprovisionamiento rápido de VM	
Pronta recuperación ante desastres	
Velocidad	
Acceso remoto	
Gestión centralizada	
No necesita mantenimiento	

1.5 802.1 Q

Es un mecanismo que da la capacidad de crear múltiples redes sobre un mismo medio físico, sin dar lugar a tener interferencias entre las comunicaciones, fue más conocido como un mecanismo de encapsulamiento el cual se lo aplica a redes ethernet, también conocido como protocolo de trucking el cual genera un enlace punto a punto para la comunicación de las VLANS entre switches o entre switches y Routers. [30]

El protocolo 802.1Q añade una etiqueta VLAN de 4 bytes al encabezado ethernet original.

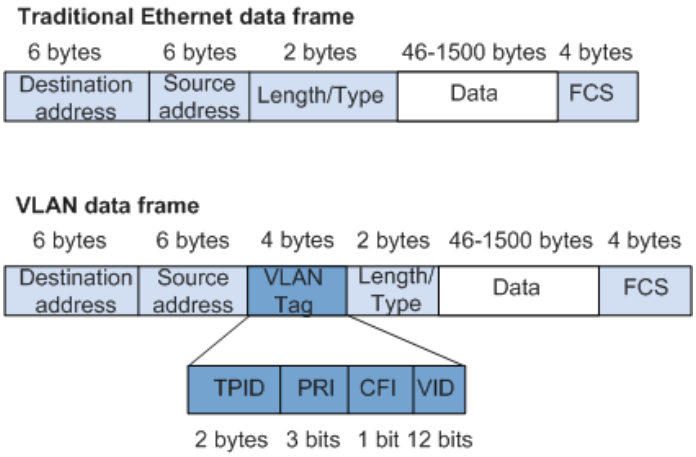


Figura. 1.8: trama 802.1Q[30]

1.6 VXLAN

De acuerdo con el RFC 7348 el cual habla de VXLAN se define a VXLAN como una tecnología de redes superpuestas, es decir el protocolo VXLAN como su nombre lo indica virtual *extensible LAN - LAN virtual extendida* la cual es capaz de crear redes virtuales de capa 2 sobre redes reales de capa 3 sin tener ningún problema para la intercomunicación.

A la red real de capa 2 que forma el protocolo VXLAN se la conoce como red overlay y a la red de capa 3 se la conoce una red underlay, una rede VXLAN puede abarcar fácilmente varias redes de capa 2 reales, y al igual que el protocolo VLAN provee segmentación de red.

1.6.1.1 Arquitectura de red

El protocolo VXLAN principalmente utiliza la arquitectura de red spine and leaf la cual consiste en una arquitectura de 2 capas donde los switches leaf se conectan a los con los switches spine a través del tunelamiento o encapsulamiento que proporciona VXLAN.

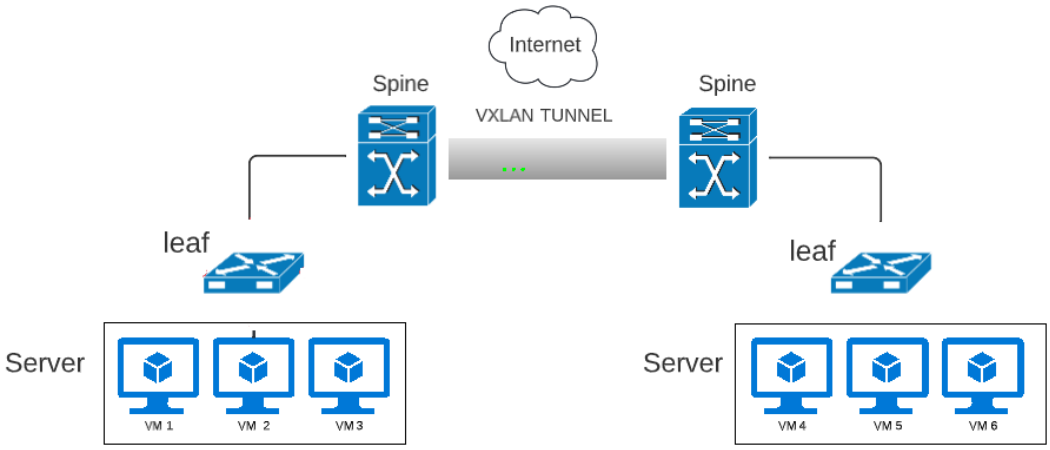


Figura. 1.9: Arquitectura VXLAN

1.7 REDES TRADICIONALES Y DE NUEVA GENERACION

1.7.1.1 Redes underlay o red subyacente

Una red subyacente o red underlay o redes tradicionales son redes físicas compuestas de todos los equipos de red necesarios para la intercomunicación y transmisión de información, para que estos equipos se ´puedan comunicar dependen de los protocolos de enrutamiento y de esta forma se obtiene un funcionamiento optimo, las redes subyacentes pueden ser tanto de capa 2 como de capa 3 como se puede observar en la Figura. *1.10*

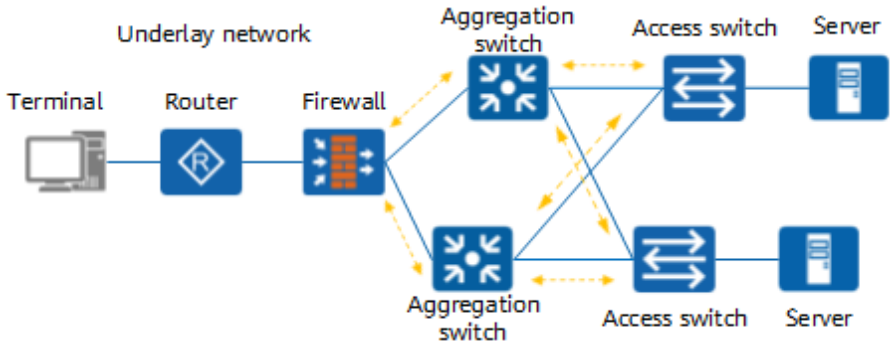


Figura. 1.10: Redes Underlay

1.7.1.2 Redes overlay

Las redes de nueva generación overlay son redes netamente lógicas virtuales que se crean a partir del concepto de la virtualización de red, estas se encuentran funcionando sobre las redes originales o también conocidas como redes subyacentes, estas redes a nivel de servicio pueden ayudar brindando servicios a un solo inquilino o de ser necesario a múltiples inquilinos.

Los equipos de una red overlay están conectados a través de enlaces lógicos a los cuales se les llamara túneles y de esta manera la red super puesta desconoce totalmente a la red subyacente como se muestra en la Figura. *1.11*.

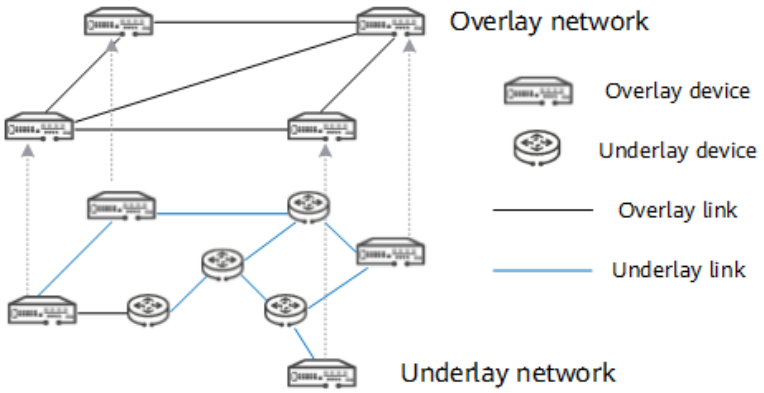


Figura. 1.11: Redes Overlay

2 METODOLOGÍA

En este capítulo se desarrollará el componente siguiendo una metodología de análisis conceptual debido a que se trabaja con definiciones, descripciones y ejemplos los cuales darán como resultado un trabajo del tipo explicativo, en el cual se rescatará la información más relevante sobre el protocolo VXLAN.

Como se habla en la anterior sección el protocolo VXLAN es la tecnología creada para generar redes sobrepuestas o redes overlay, las mismas que de acuerdo con el RFC 7348 contienen o pueden generar más redes virtuales que las VLAN en la actualidad, en esta sección se estudiara más afondo al protocolo VXLAN.

2.1 ANÁLISIS CONCEPTUAL

Que es el encapsulamiento muchas veces, es un proceso por el cual todos los datos que atraviesa una red de información deben pasar para poder llegar a su destino, este proceso genera paquetes de datos más pequeños los cuales pueden ser rastreables y verificables hay muchos tipos de encapsulamientos en las redes. Para este caso principal se centra en la encapsulación que realiza VXLAN, componentes utilidades en que lo diferencia, y como ayuda con los problemas del centro de datos.

En primera instancia se considera que VXLAN es un protocolo para la mejora en la segmentación de las redes, el cual funciona creando una capa 2 virtual superpuesta a la capa 3 del modelo ISO OSI, fue propuesto para resolver las limitantes como la segmentación de las redes virtuales de centros de datos, la movilidad de las VM en centros de datos, escalabilidad frente a tecnologías como VLAN que cuenta con 4096 redes virtuales, VXLAN cuenta con un total aproximado de 16 millones de redes virtuales.

2.2 COMPONENTES DE VXLAN

Las redes VXLAN tiene los siguientes componentes:

VTEP (*Virtual tunnel end point*): Considerado como punto o puntos finales e iniciales de la red VXLAN, son equipos de borde que se encargan de encapsular y des encapsular la información, los VTEP pueden ser conmutadores o servidores físicos que contienen VMs.

VNID (Virtual Network Identifier): Es un identificador que utilizan las redes VXLAN son similares a los usados en VLAN, la diferencia se encuentra en que un solo VNID puede admitir hasta 16 millones de inquilinos.

VNI (Virtual Network Instance): como su nombre lo indica instancia la red lógica que dará servicios tanta capa 2 o 3 y es un dominio de broadcast para capa 2.

Túnel VXLAN: Es el camino lógico utilizado por VXLAN para transportador a ojos de la red es como un camino directo entre un VTEP y otro.

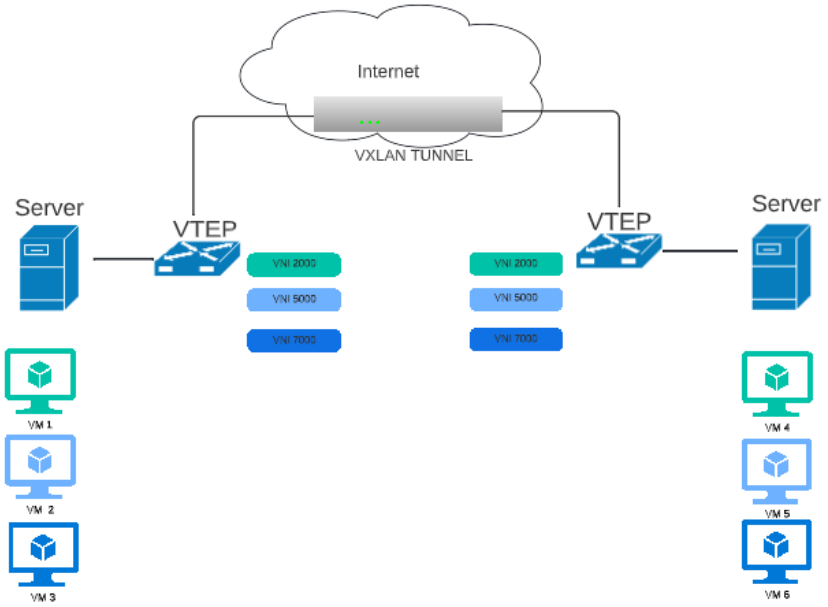


Figura. 2.12: Componentes VXLAN

2.3 FORMATO DE PAQUETE VXLAN

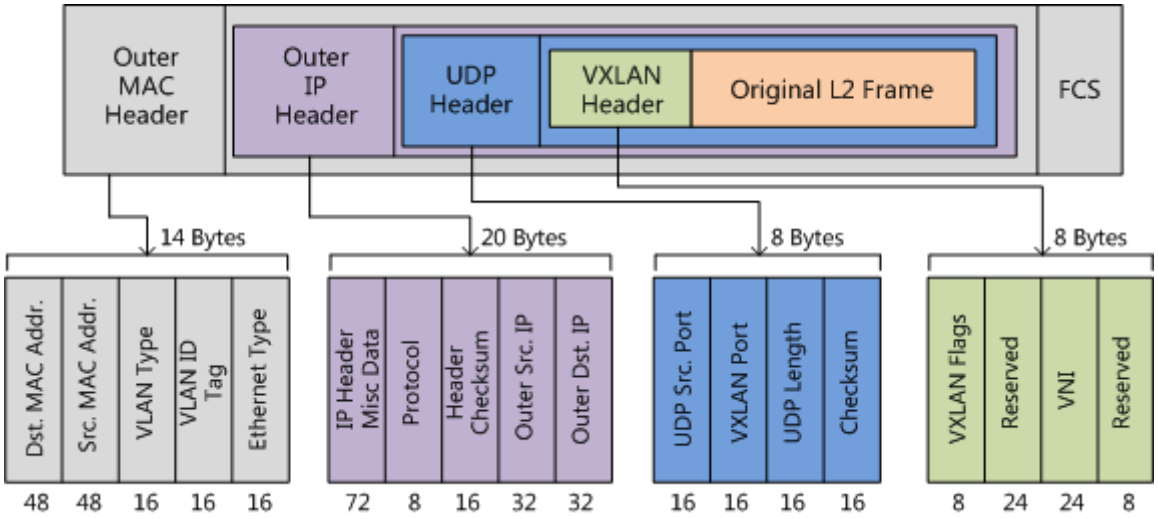


Figura. 2.13: El paquete VXLAN [31]

El paquete VXLAN es generado en los VTEP y tiene la siguiente estructura y se lo puede observar en la Figura. 2.13

2.3.1 CABECERA VXLAN

La cabecera consta de 8 Bytes los cuales están distribuidos de la siguiente manera: [31]

- 8 bits para banderas VXLAN.
- 24 bits para el identificador de red virtual VNI.
- 24/8 bits reservados.

2.3.2 CABECERA UDP

La cabecera contiene 8 Bytes los cuales están distribuidos de la siguiente manera: [31]

- 16 bits para identificar el puerto fuente.
- 16 bits para el puerto destino 4789.
- 16 para la longitud del paquete.
- 16 bits de checksum.

2.3.3 CABECERA IP

Esta cabecera está compuesta por 20 Bytes los cuales se distribuyen:[31]

- 72 bits para la cabecera IP.
- 8 para el protocolo a transportar.
- 16 de checksum.
- 32 bits para la IP del VTEP de origen.
- 32 para la dirección IP de VTEP de destino.

2.3.4 CABECERA MAC

Esta cabecera consta de 14 Bytes distribuido entre los más importantes capos de la siguiente manera:[31]

- 48 para la dirección MAC destino la cual pertenece al VTEP donde se tiene alojada la VM.
- 48 para la dirección MAC origen de igual manera.
- 16 bites que representan el tipo de VLAN que es opcional y cuando se usa lleva un valor 0x8100 y el identificador tag VLAN.
- 16 bits para definir el tipo de paquete ethernet.

2.4 METODOS DE DIFUSION DE VXLAN

2.4.1 DIFUSION UNICAST

La difusión unicast se realiza de VM a VM, las cuales se encuentran formando parte de la red superpuesta que VXLAN genera, este procedimiento se realiza con la generación del paquete VXLAN que se va a enviar en el VTEP el cual verifica primero si la VM que se va a alcanzar se encuentra primero en VNI correspondiente una vez realizado esta tarea se envía el paquete a través del túnel VXLAN.

2.4.2 DIFUSION MULTICAST

Para utilizar multicast en VXLAN en la cabera llevará el indicador VNI esta información será enviada al grupo de multidifusión de la red superpuesta, para llevar a cabo la multidifusión es necesario contener con un mapeo de las VXLAN Y VNI asociadas a dicha VXLAN.

Solo los VTEP conocen el mapeo por lo cual ellos son los encargados de generar los informes IGMP a los equipos de red unir o descartar host a los grupos de multidifusión VXLAN.

Se pueden usar protocolos de enrutamiento de multidifusión *como Protocol Independent Multicast Sparce Mode* (PIM-SM) el cual se encarga de proporcionar arboles multidifusiones eficientes dentro de la red de capa 3.

Cuando el destino ha sido alcanzado, dicho host envía su respuesta utilizando comunicación unicast, dicha respuesta es menos compleja de entregar, ya que todos los datos necesarios para su envió han sido capturados de la primera solicitud ARP enviada.

2.5 ARQUITECTURA SPINE-LEAF

Maneja una arquitectura redundante, donde cada leaf se conecta directamente y redundante mente a los spine formando una topología de 2 saltos como máximo esta es la topología más usada en los centros de datos, se observa en la Figura. 2.14

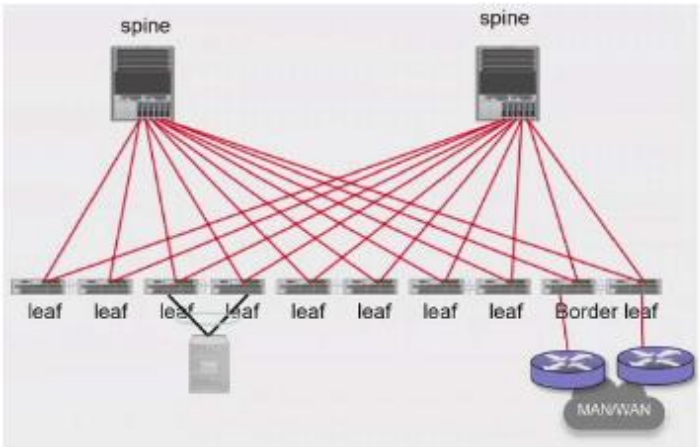


Figura. 2.14: Arquitectura Spine-leaf

Componentes de la red spine- leaf

Spine

- Es el encargado de interconectar los leafs
- Reenviar el tráfico entre los leafs (tráfico EAST-WEST)
- Funciona como un reflector para EVPN
- Solo se lo configurara como VTEP cuando sea un dispositivo de borde.
- Es considerado el punto de encuentro (RP- *Rendezvous Point*) con la red underlay

Leaf

- Son dispositivos de borde de una red VXLAN
- Realizan el procesamiento de la información es decir Encapsulamiento y desencapsulación de los paquetes VXLAN
- Interconecta los equipos finales

Leaf de borde

- Son dispositivos de borde para interconectar redes VXLAN
- Transmiten y receptan tráfico de redes exteriores y lo encapsulan en paquetes VXLAN
- utiliza protocolos de enrutamiento como IGP, EGP

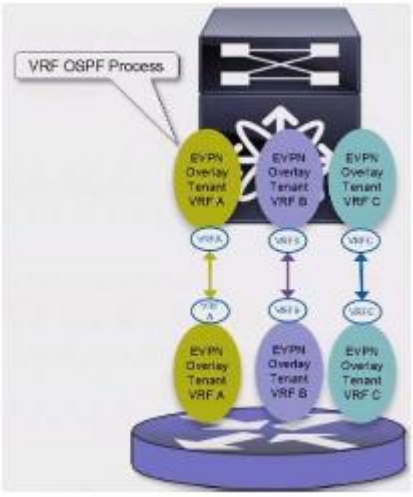


Figura. 2.15: Leaf de borde

Spine de borde

- Realiza tareas de spine y leaf de borde
- Provee de comunicación con redes externas
- Se lo debe configurar como VTEP

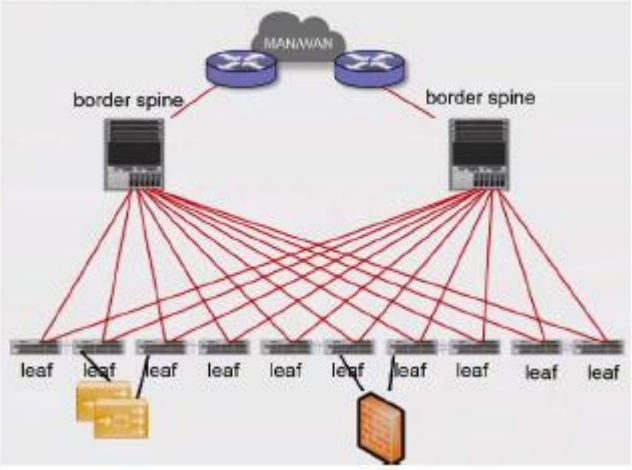


Figura. 2.16: Spine de Borde

2.6 VXLAN TUNNEL ENDPOINT

Utiliza los VXLAN tunnel Endpoint (VTEP) para la encapsulación y desencapsulación VXLAN.

Los VTEP están compuestos por dos interfaces una interfaz es para la comunicación de punto final local haciendo uso de bridging y la otra es una interfaz parea la red IP de transporte.

La interfaz que se conecta a la red de transporte cuenta con una dirección IP única la misma que es identificada por el dispositivo VTEP, el mismo que usa esa IP para encapsular las tramas ethernet y transmitir los paquetes encapsulados a la rede de transporte a través de dicha interfaz.

El dispositivo VTEP está en capacidad de descubrir otros VTEP en sus segmentos de red y sus direcciones MAC realizando mapeos a través de la interfaz.

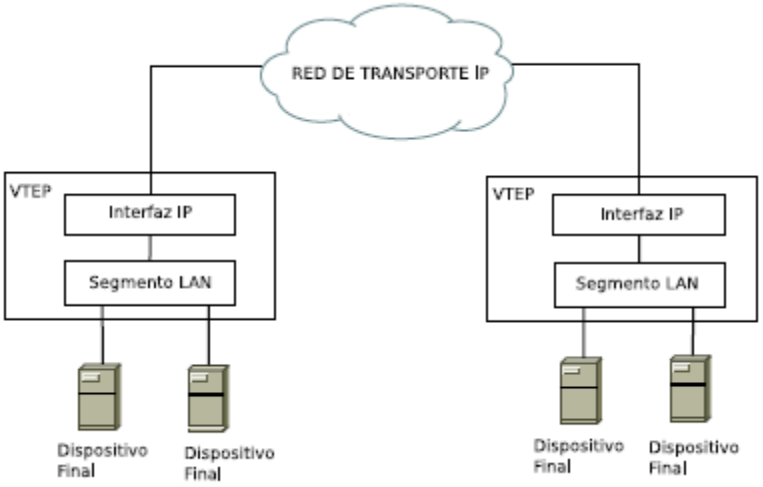


Figura. 2.17: VXLAN Tunnel endpoint

2.7 FUNCIONAMIENTO DE VXLAN

VXLAN necesita una infraestructura de red base (red underlay), con la cual pueda realizar el reenvío del plano de datos, mediante la cual brindara comunicación tanto de forma unicast como multicast a este tráfico también se lo llama BUM (tráfico de broadcast, unknown unicast y multicast), hay dos formas de formas por las que se podría emplear el tráfico BUM.

1. Cuando se usa VXLAN en modo difusión multicast en la red overlay, en el cual se debe usar el protocolo PIM (Protocolo Independiente Multicast), el cual ayuda a realizar la replicación nativa de los SPINES que distribuyen el tráfico a las VTEP.

2. Cuando no se puede usar el modo de difusión multicast, se debe hacer uso de la capacidad para replicar los VTEP ayudando así a la creación de muchas tramas BUM que se envían a cada uno de los VTEP, por obvias razones este método de difusión no es eficiente al igual que multicast cuando se trata de replicar el tráfico BUM. Sin embargo, este método no precisa cambios en la estructura de VXLAN para él envió tanto en capa 2 como en la capa 3, con lo cual se logra permitir que el VTEP siga llevando a cabo tareas de enrutamiento y puenteo, mientras usa el tunnelling VXLAN en el plano de envió de datos.

3. Un VTEP ofrece funciones de Gateway las que se van a detallar en la siguiente Figura. 2.18

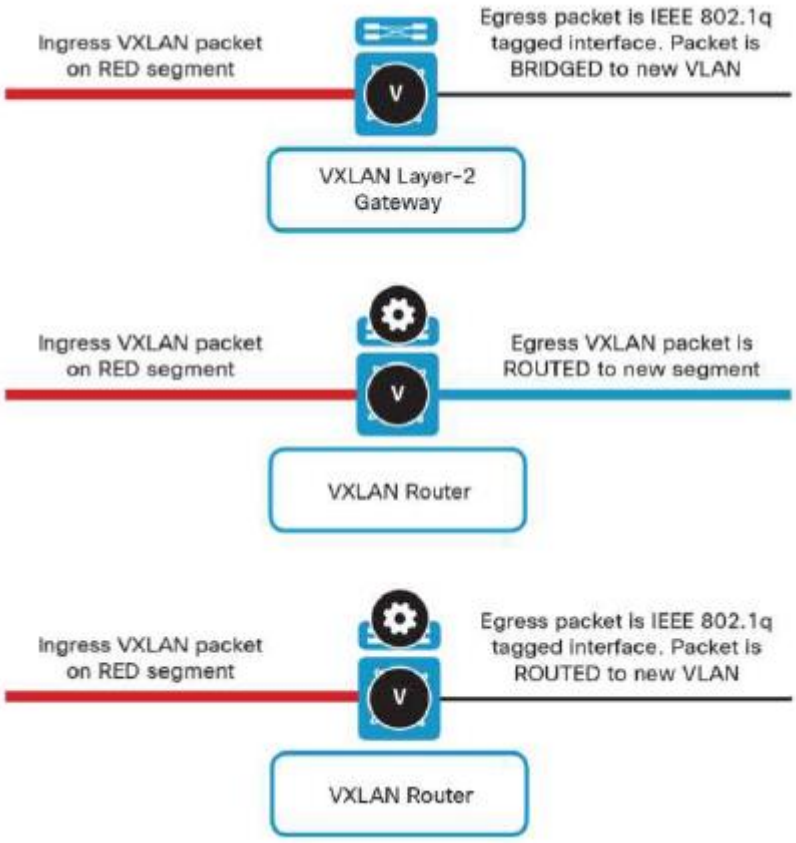


Figura. 2.18: Funcione VTEP

- Gateway de capa 2: genera un puente que nos ayuda a pasar de VXLAN a VLAN de acuerdo con el VNI y usando un bridge-domain común.
- Gateway de capa 3 (VXLAN Router): pueden realizar enrutamiento de VXLAN a VXLAN entre dos VNI por lo que no necesitan realizar desencapsulación y entre un VNI y VLAN en la cual la desencapsulación es necesaria.

2.7.1 PLANO DE CONTROL

En el plano de control de VXLAN se utilizan los protocolos, *Multi Protocol Gateway Protocol* (MP-BGP) con *Ethernet Virtual Private Network* (EVPN), juntos el plano MP-BGP EVPN distribuye la información basándose en el descubrimiento de VTEPS vecinos y conectividad en dispositivos finales para mayor escalabilidad de diseño de redes VXLAN overlay.

El plano de control introduce grandes características, reduciendo la cantidad de tráfico en la red y optimiza él envió del tráfico.

En centros de datos el uso de EVPN ayuda en la adquisición de información para la conectividad de dispositivos finales de capa 3 y capa 2, lo cual crea la oportunidad de

suprimir el protocolo ARP, además reduce el número de inundaciones de trafico de igual manera ayuda al descubrimiento de vecinos VTEP y mitigando el riego de tener datos de VTEPs dudosos en rede VXLAN.

En el plano de control de VXLAN hay prácticamente tres tipos de planos de datos como se indica en la Figura. 2.19.

- Multi-Protocol Label Switching (MPLS, draft-ietl-l2vpn-evpn)
- Provider Backbone Bridging (PBB, draft-ietf-l2vpn-pbb-evpn)
- Network Visualization Overlay (NVO, draft-ietf-bess-evpn-overlay)

Figura. 2.19: Plano de control

2.8 DESCRIPCIÓN DEL ENCAPSULAMIENTO Y DESENCAPSULAMIENTO VXLAN

Para la descripción del proceso se utilizará un ejemplo

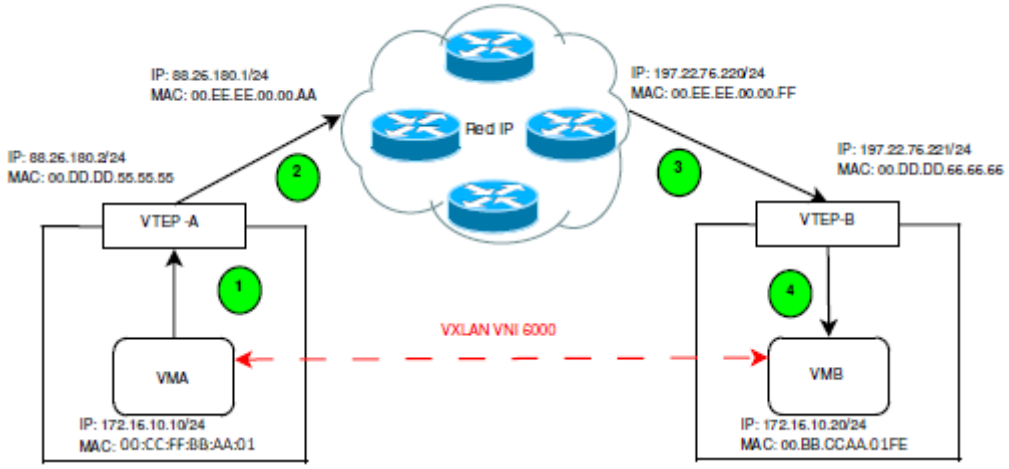


Figura. 2.20: Proceso de encapsulamiento

El cual consta de dos máquinas virtuales que trabajan en la misma subred VXLAN, a pesar de que están muy separados por varios dispositivos en la capa 3.

1. La máquina VMA va a enviar un paquete a la maquina VMB con una dirección IP 172.16.10.20, el mismo que va a ser encapsulado en la trama ethernet llevando los siguientes datos.

   IP de destino: 172.16.10.20

   IP de origen: 172.16.10.10

   MAC de destino: 00:BB:CC: AA:01: FE

   MAC de origen: 00:CC: FF:BB: AA:01

   La nueva trama ethernet es enviada a al VTEP-A y se le va a nombrar trama ethernet interna. Para este caso se asume que el paquete IPV4 contiene datos para el inicio de sesión en el protocolo TELNET, en ambas máquinas virtuales, en modo de ejemplo asumiremos que este paquete tiene 90 bytes y el encabezado TCP tiene 32 bytes contemplando que el encabezado TCP maneja todos los campos, VMA envía el paquete de 122 byte de longitud en IP, de la misma manera se agregan 20 bytes más que representan el encabezado IPV4.

   Por el momento ya se cuenta con 142 bytes dentro de la trama ethernet que va a ser enviado desde VMA a VTEP-A, una vez para su envío se coloca la cabecera ethernet y el FCS que suman 160 bytes más de la trama interna como se puede apreciar en la Figura. 2.21

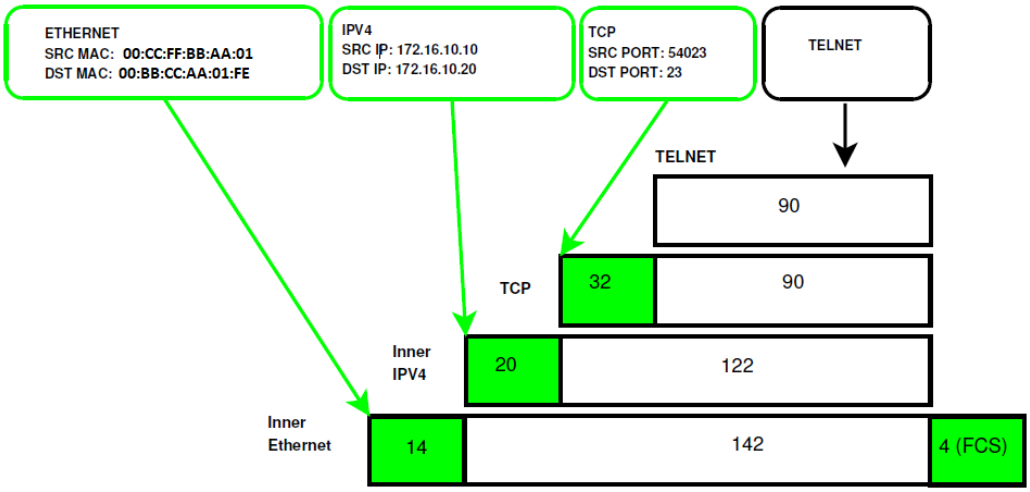


Figura. 2.21: Encapsulamiento Ethernet

2. Cuando el paquete llega al VTEP-A empezamos la encapsulación en VXLAN se agrega un encabezado de 8 bytes que contienen un VNI de 6000 (el VNI puede llegar hasta 2^{24}).

Como el FCS no es necesario para el transporte del paquete este será descartado dejando una trama de 156 bytes para sumarle los bytes de la cabecera VXLAN que son 8 bytes.

Cuando esta información entra en el VTEP-A este encapsula dichos datos en un paquete UDP, al mismo que se le llama UDP externo, como siguiente paso a este paquete UDP Externo se le agrega una cabecera IPv4 para lograr una encapsulación Ethernet normal llamada Ethernet externa.

La trama ethernet externa es entregada al Router el cual trata el paquete como in paquete IP normal encaminándole al destino ya programado, el VTEP-B.

Al momento que el VTEP-A enviar la información al Router intermedio entre el VTEP-A y el VTEP -B la trama Ethernet externa lleva:

- MAC destino: 00:EE:EE: 00:00: AA (MAC Router destino)
- MAC origen: 00:CC: FF:BB: AA:01 perteneciente al VTEP-A

Mientras que en la cabecera IPv4 externa constan los datos:

- IP destino: 197.22.76.221 perteneciente al VTEP-B
- IP origen: 88.26.180.2 perteneciente al VTEP-A

Como se observa en la Figura. 2.22

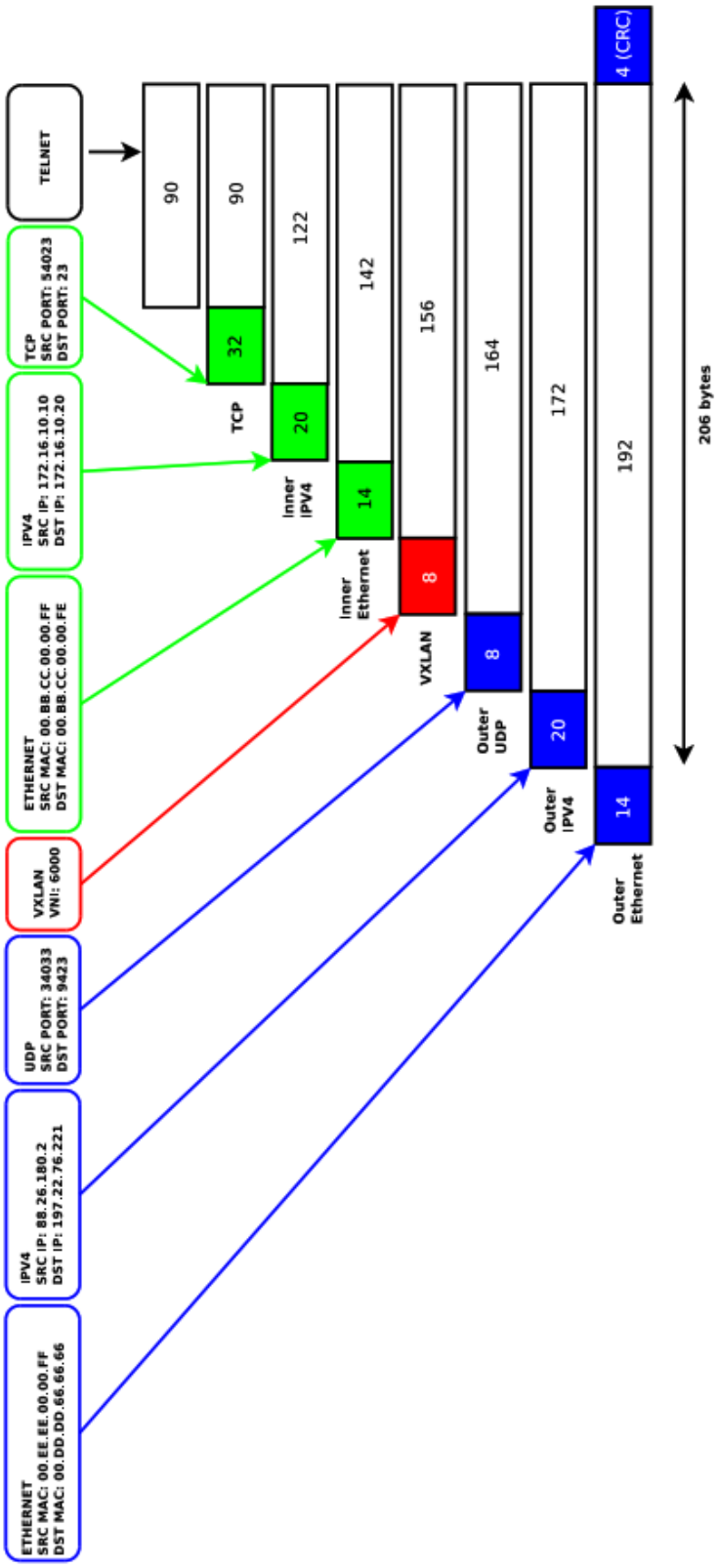


Figura. 2.22: Encapsulamiento VXLAN y Ethernet externa

3. Al salir la información del Router es necesario realizar un análisis de dichos datos antes que llegue al VTEP-B estudiaremos el ´paquete IP externo y la trama encapsulada, como observar en el paquete IP lo que ha cambiado es la dirección MAC origen y

destino estas representan el ultimo Router y VTEP-B como se observa en la Figura. 2.23

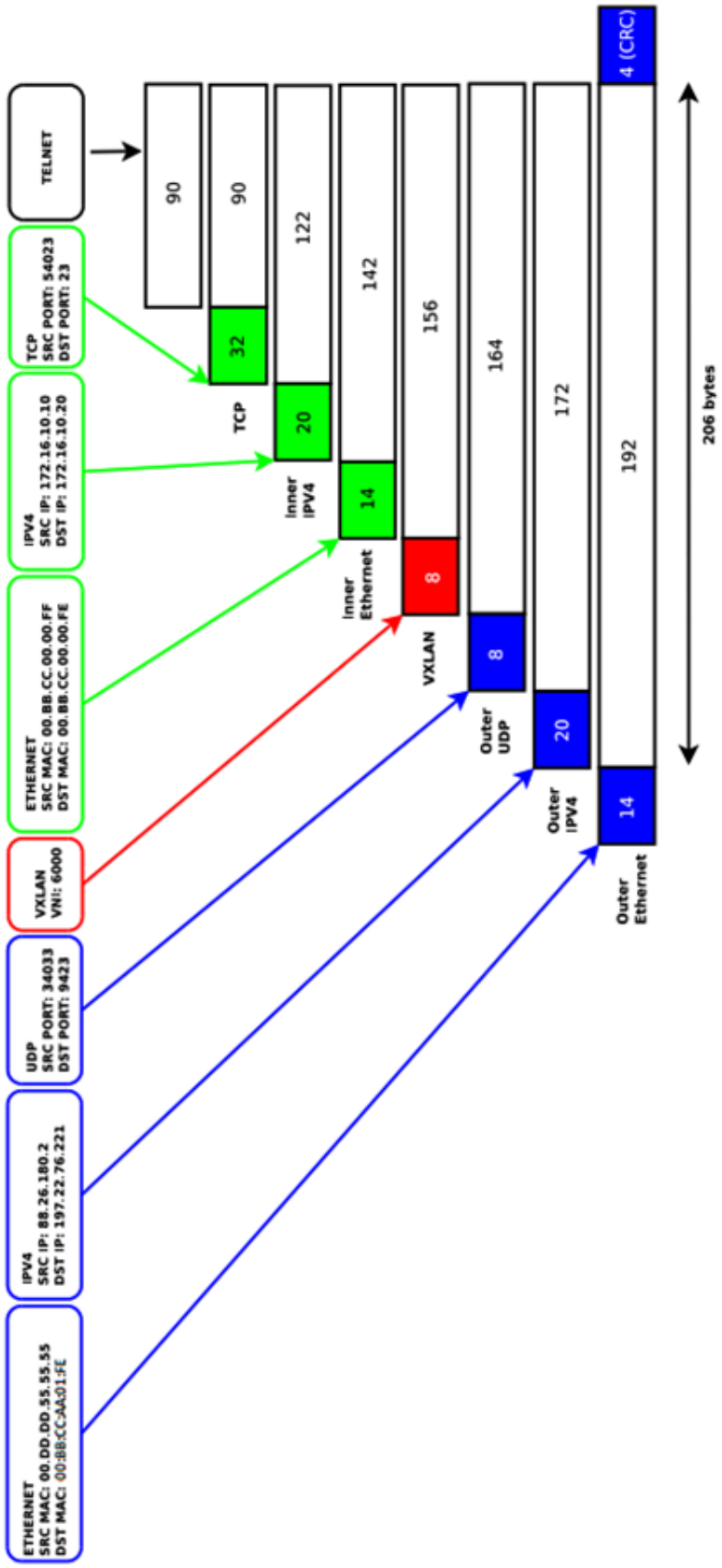


Figura. 2.23: Paquete del Router al VTEP B

4. Cuando la trama llega al VTEP-B este comienza el proceso de desencapsulamiento, quitando el paquete IPV4 externo y la cabecera UDP externa para tener acceso al VNI correspondiente el cual nos indica el valor 6000 que corresponde a una conexión a la maquina VMB ya sin los valores de capa 3 solo nos queda la información de la trama ethernet interna, la misma que será reconstruida su FCS, la podemos observar en Figura. 2.24

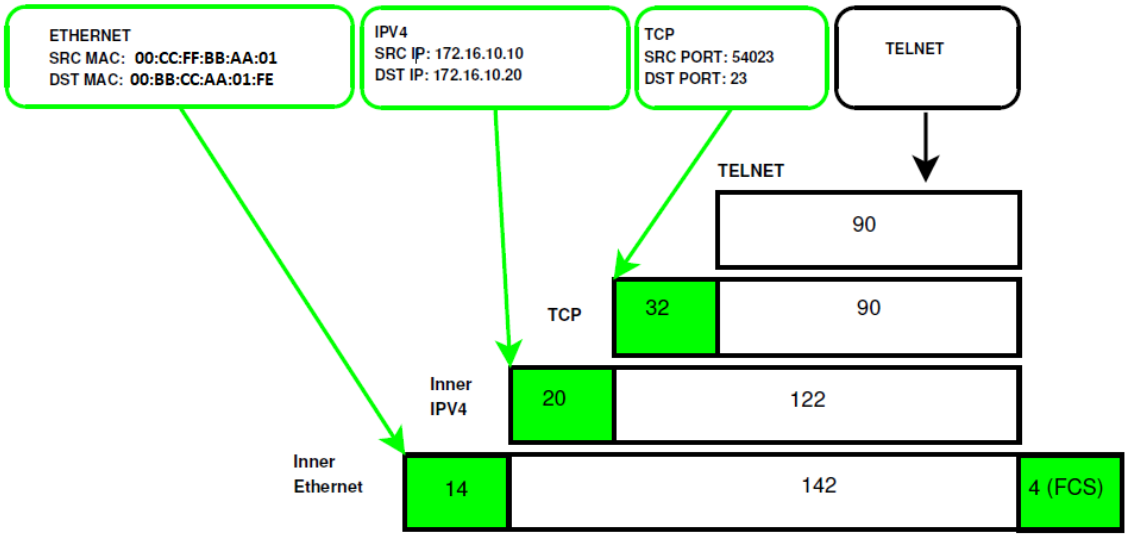


Figura. 2.24 Desencapsulamiento

Para terminar, se retira la cabecera TCP la cual nos da acceso a los datos de aplicación y los verifica posteriormente para ser entregados a la VMB.

2.9 ANÁLISIS PLANO DE CONTROL DE VXLAN

VXLAN no tiene muchas formas de escalar y de tolerar fallos como en las redes tradicionales, en VXLAN cada switch tiene una tabla de host conectados. Para que la información del host sea enviada toda la red normal mente se lo hacía por el método de inundación y aprendizaje. En una red VXLAN se debe manejar un plano de control el cual permita la conectividad a nivel de capa 2 y capa 2, en un principio no se contaba con este plano de control, pero con el pasar del tiempo de implemento extensiones de ethernet VPN al multiprotocolo BGP.

2.9.1 EVPN

EVPN es una extensión del protocolo BGP el cual permite el transporte de información a través de la red al punto final, utiliza las direcciones MAC de capa 2 y la direcciones IP de la capa 3, se usa MP-BGP para considerar las direcciones MAC e IP para distribuir los puntos finales, de esta manera se usa a las direcciones MAC como rutas.[32]

EVPN brinda la posibilidad de tener redundancia y reenvía información por varias rutas. Utilizando EVPN un solo punto final puede estar conectado a uno o varios dispositivos juntos que estén en la misma red.

EVPN maneja aprendizaje por descubrimiento de MAC lo que hace que el método de inundación sea obsoleto, EVPN diseñado para admitir distinta tecnología de encapsulación entre ellas EVPN-VXLAN, VXLAN.

2.10 EVPN EN CENTRO DE DATOS

En la actualidad los centros de datos usan EVPN-VXLAN para sus redes superpuestas.

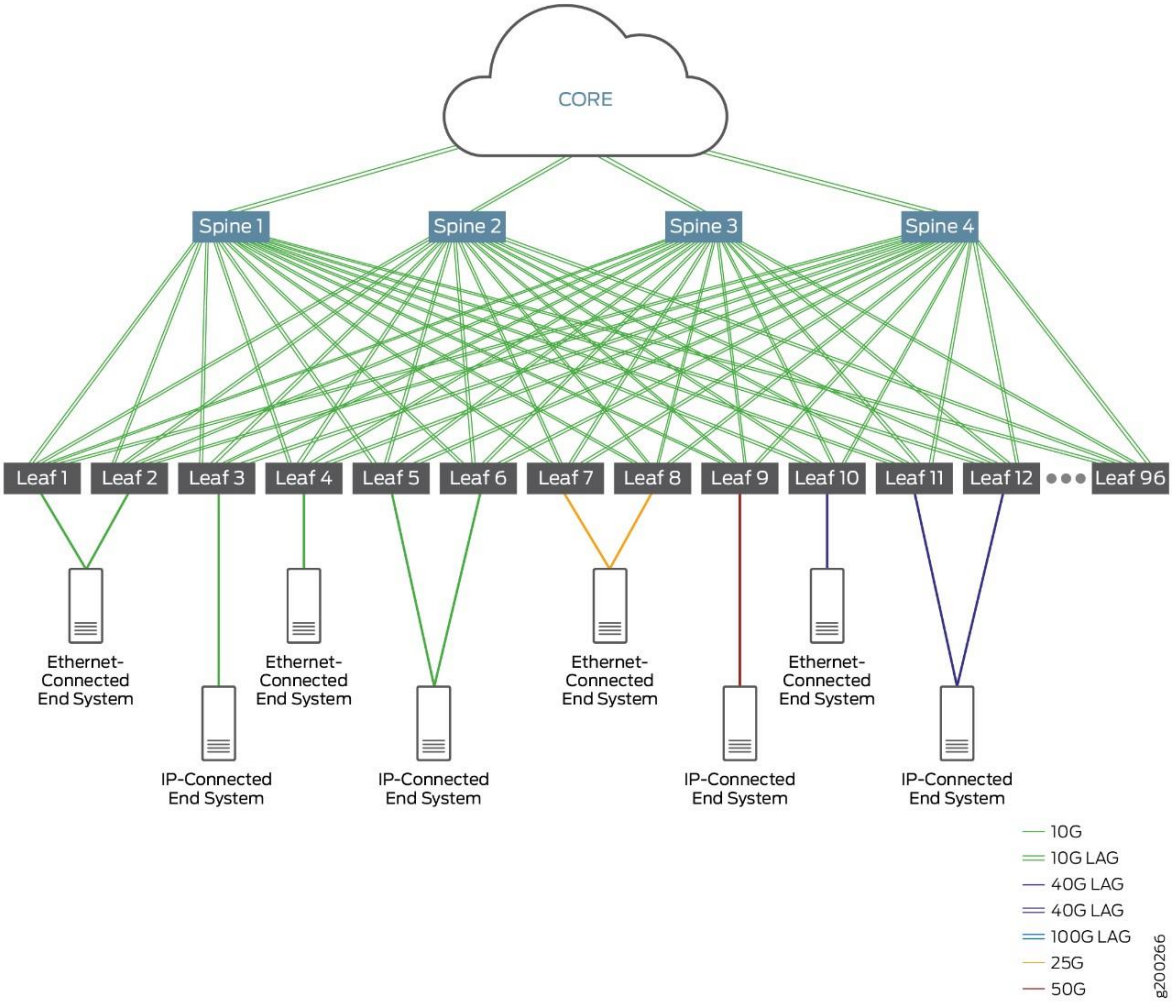


Figura. 2.25: Topología EVPN en centros de datos

En la cual todas las capas de red tradicionales se ven simplificadas a 2 simples niveles la capa spine y capa leaf, estas redes de capa red se caracterizan por ser de latencia baja, altamente disponible y bastante escalable. [32]

2.11 MEJORAS EN VXLAN

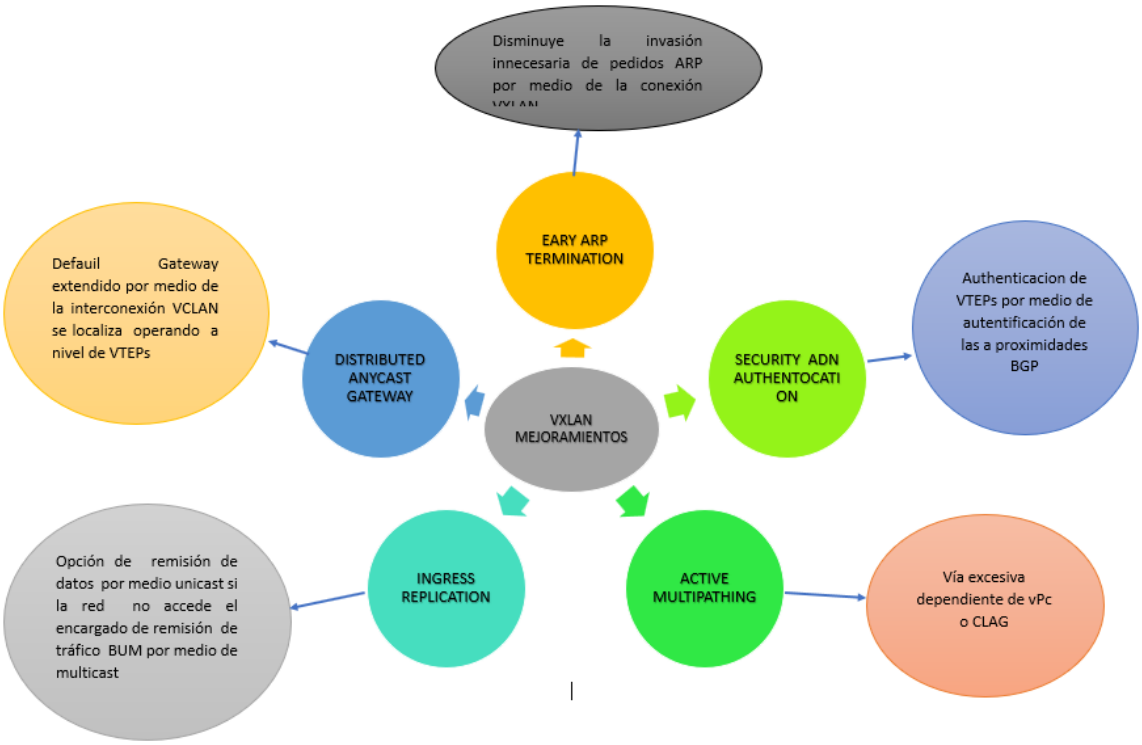


Figura. 2.26: Mejoras VXLAN

2.11.1 SEGURIDADES Y AUTENTIFICACIÓN

La autentificación para VXLAN se determina entre los residentes BGP por medio de MD5 digest. Este autoriza a cubrir los sectores BGP y oposiciones de acceso de seguridad TCP.

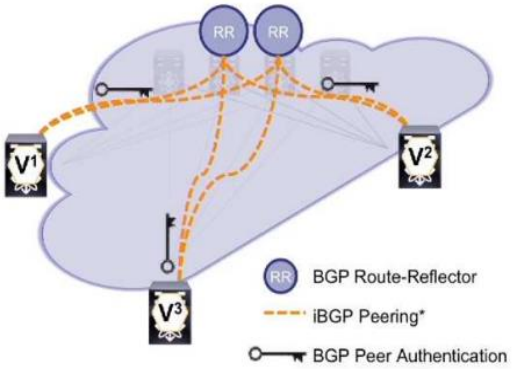


Figura. 2.27: Autenticidad usada en BGP

La autentificación fortalece la rectitud del recibimiento de la información, se puede colar códigos área de red por medio registros de control de entrada (ACL), PREFIX LIST y registros distribuidos. El comprimir y descomprimir VXLAN solo ocurre si el VTEP puede acreditar por medio de la sección BGP.

2.11.2 ANULACIÓN DE ARP

La anulación de ARP es un adelanto apto por el plano de inspección MP-BGP-EVPN para disminuir la invasión de red ocurrida por el estancamiento broadcast a inicios de solicitudes de ARP.

Cuando la anulación de ARP está autorizada por un VNI propio, sus VTEPs sostiene una tabla cache de revocación de ARP para hosts IP parecidos y direcciones MAC y acompañado en fragmentos VNI.

Como se muestra en la Figura. 2.28 Cuando un host final en un VNI remite una petición ARP para otro rumbo IP de host final su VTEP local interrumpe la petición ARP verifica la ruta IP determinada por ARP en su tabla cache de eliminación ARP Si localiza un parecido, el VTEP local remite una respuesta ARP en designación del host final lejano.

El host local en sucesión de termina la dirección MAC del host lejano en la respuesta ARP. Si el VTEP local tiene la ruta IP determinada por ARP en su tabla de revisiones ARP inmunda una petición ARP a los otros VTEP en el VNI.

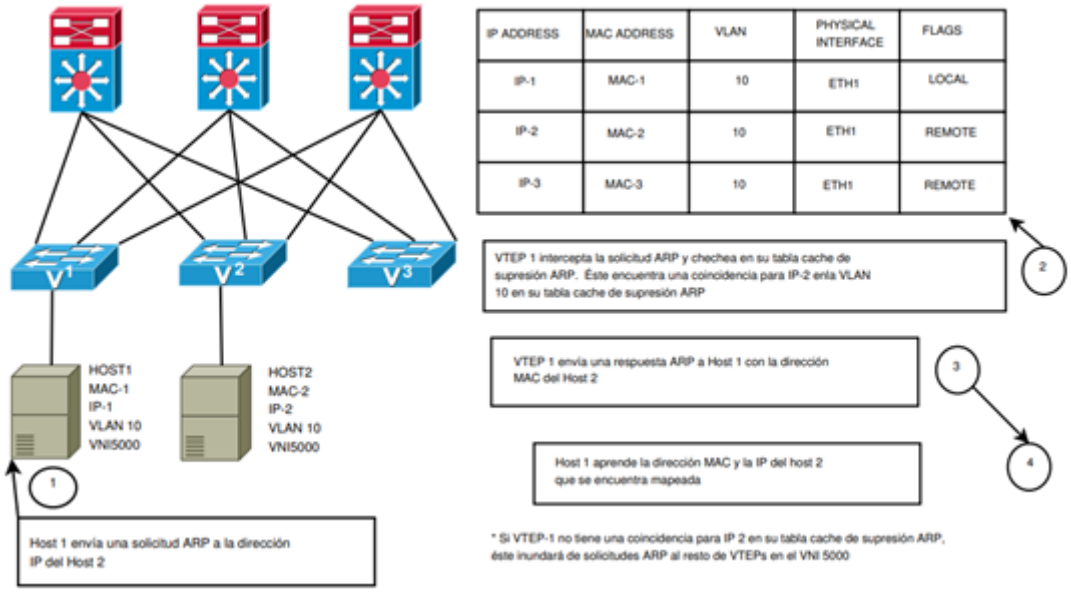


Figura. 2.28: Eliminación ARP

2.12 ANÁLISIS COMPARATIVO VLAN VS VXLAN

Tabla 2 Comparación VLAN vs VXLAN

	VXLAN	VLAN
Numero de bits para identificador	24 bits	12 bits
# de redes a crear	16 millones y mas	4094
Uso de STP	No	si
Encapsulado	MAC-in- UDP	802.1q
Manejo de VNI	SI	NO
Manejo de VNE	NO	NO
Difusión Multicast	SI	SI
Difusión Unicast	SI	SI

2.13 IMPLEMENTACIÓN DEL PROTOCOLO

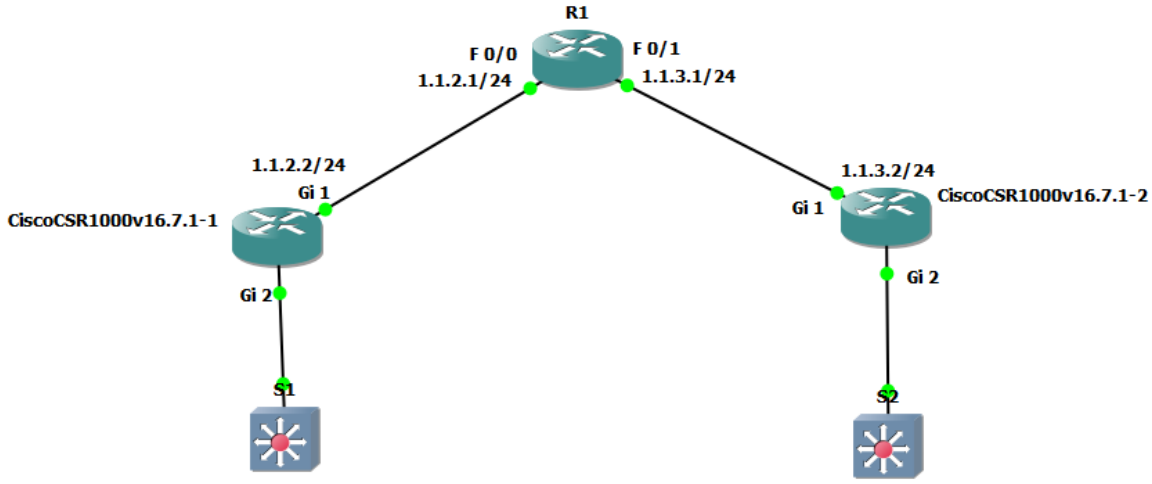


Figura. 2.29: Topología de Prototipo

Para implementar el prototipo se usa el emulador GNS3 y GNS3 VM

Las siguientes imágenes .ISO de cisco:

- Router Cisco 7200 153.13
- Router Cisco CSR1000V16.7.1
- Switch Cisco IOSvL2 15.2(4.0.55) E

Como se puede observar en la Figura. 2.30

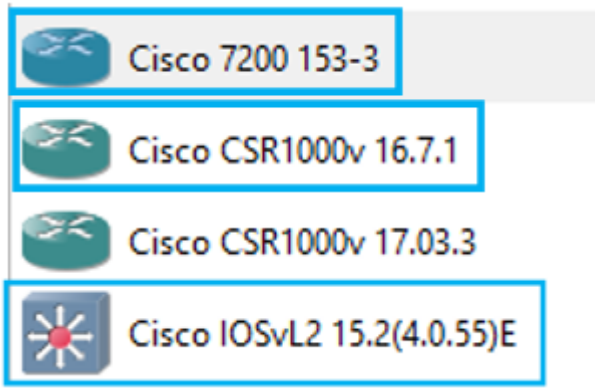


Figura. 2.30: Equipos Usados

2.13.1 GUIA PARA IMPORTACION DE IMÁGENES ISO EN GNS3

Para importar las imágenes de los diferentes equipos es necesario realizar lo siguiente.

1. En la pantalla de gns3 dar clic en la pestaña File y dirigirse al item *"Import appliance "como* se puede observar en Figura. 2.31

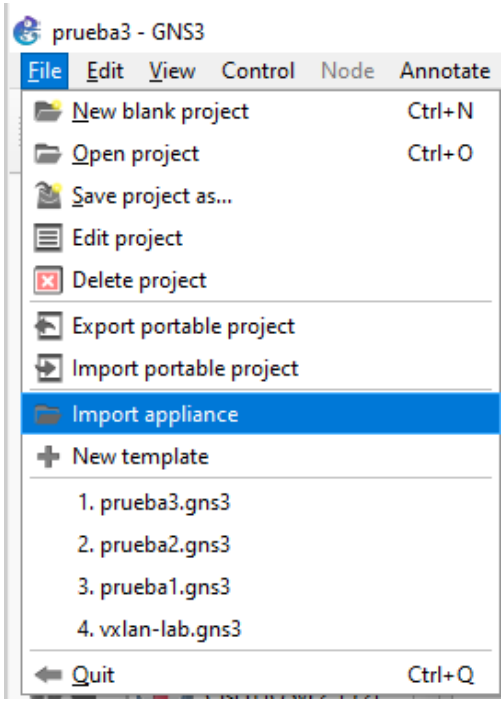


Figura. 2.31: Pestaña File

2. Para obtener los diferentes *appliance* visitamos la página web de GNS3 en ANEXO o también se puede dar clic en *"New Template*" que se visualiza en la Figura. 2.31

3. Al dar clic en "*New Template*" visualizar la siguiente Figura. 2.32

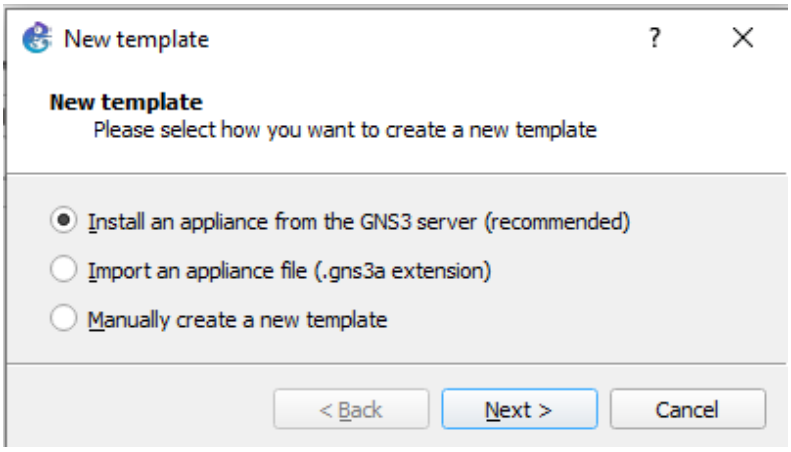


Figura. 2.32: *New Template*

4. Seleccionar instalar desde el servidor de GNS3 y clic en siguiente lo cual nos desplegara la siguiente Figura. 2.33 y seleccionara la categoría de equipo que necesite.

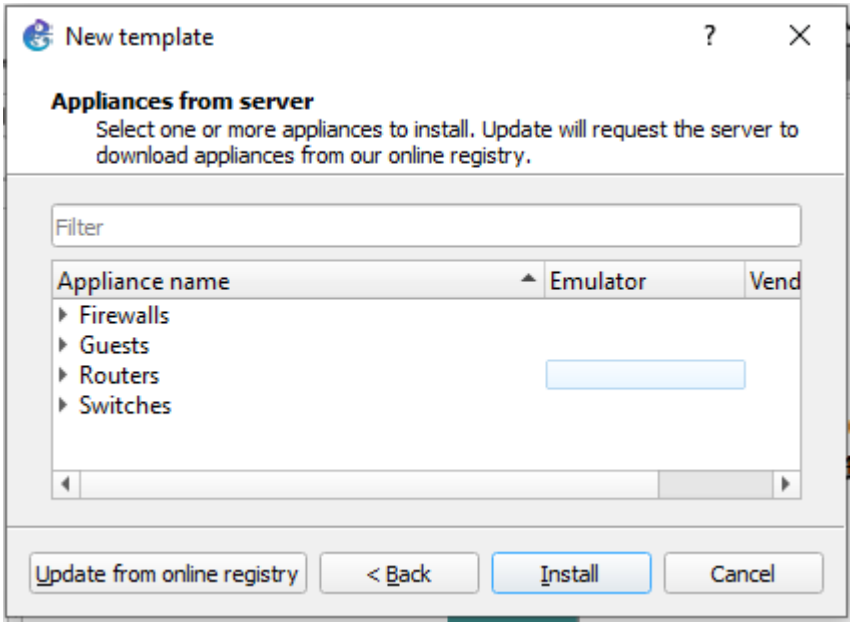


Figura. 2.33: *Appliances from server*

5. Al dar clic en una categoría se desplegará la lista de equipos integrados a gns3 y clic en instalar.

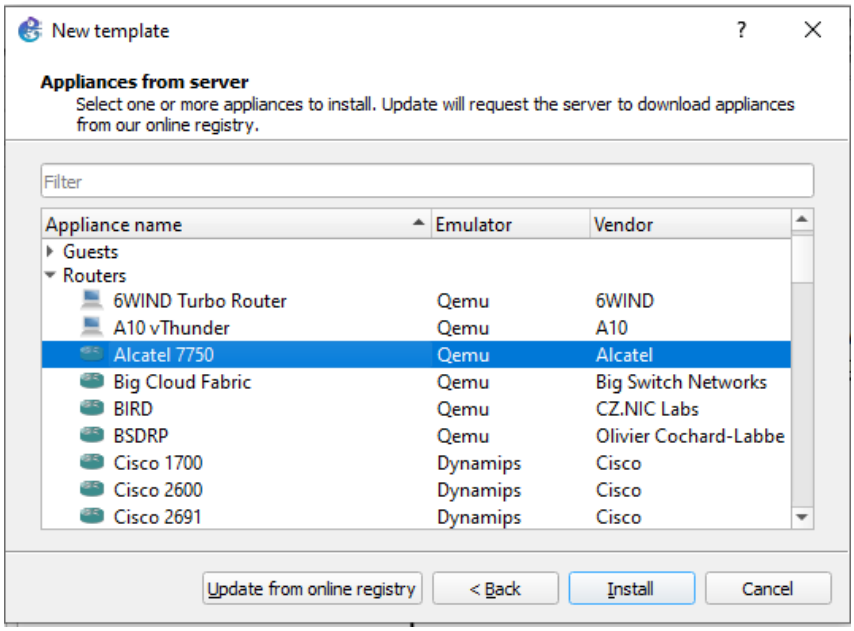


Figura. 2.34: Lista de equipos

6. Instalar el *appliance* en GNS3 VM y dar clic en next como se aprecia en la Figura. 2.35

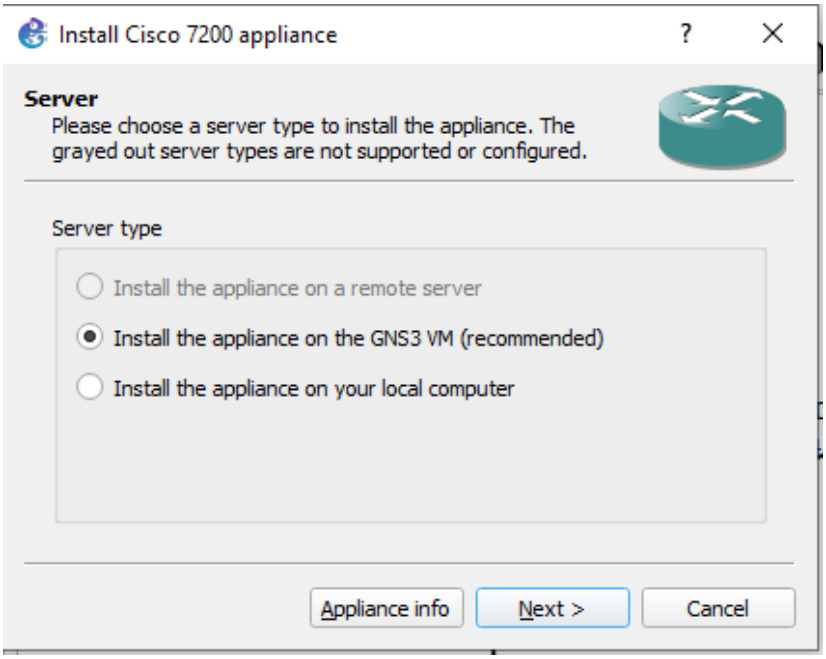


Figura. 2.35: Instalar el appliance en GNS3 VM

Para concluir con la instalación necesitará las imágenes de los sistemas operativos de cada equipo los cuales encontrará en

7. ANEXO , al cargar la .iso la maquina se mostrará en letras de color verde como muestra la Figura. 2.36 para instalar el equipo y daremos clic en siguiente.

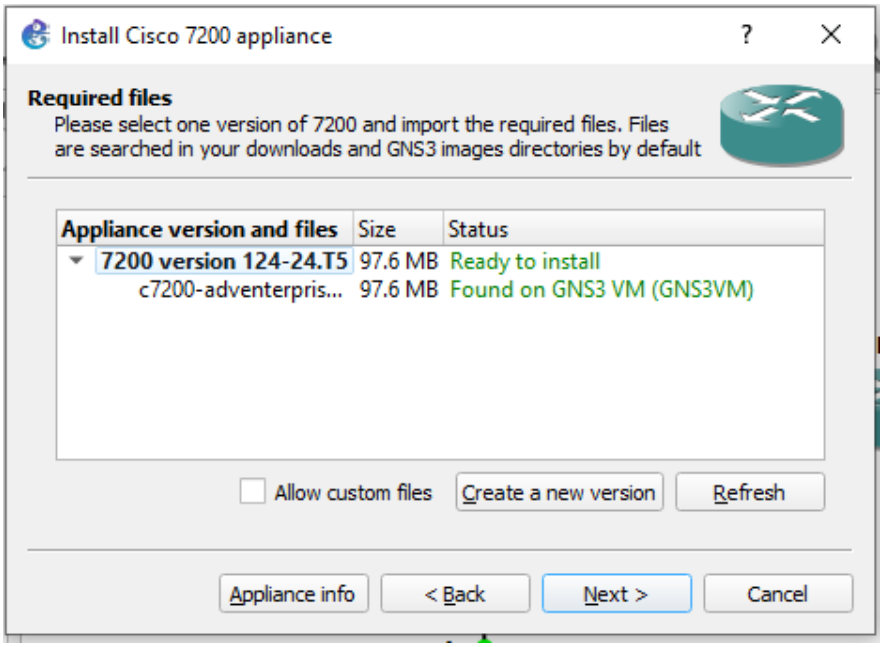


Figura. 2.36: Carga de archivos .iso

8. Al dar clic en siguiente se mostrar si quiere instalar el archivo al cual se dará clic en sí y finalizará el proceso el equipo estará en la categoría correspondiente.

2.13.2 CÓDIGOS PARA LA IMPLEMENTACIÓN DE VXLAN

En el Anexos VII se puede encontrar los comandos básicos que fueron usados en el presente documento para hacer el desarrollo del prototipo para la implementación de la red VXLAN.

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentará la aplicación práctica de la investigación realizada llevará un enfoque, hacia la configuración de equipos cisco como: Routers csr1000, Routers 7200.

3.1 RESULTADOS

3.1.1 TOPOLOGIA

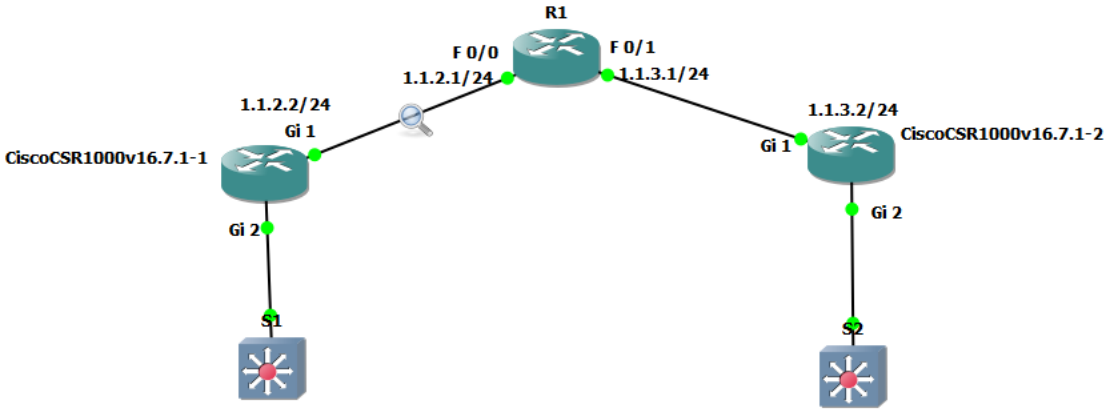


Figura. 3.37: Topología

3.1.2 CONFIGURACIÓN DE S1

En la Figura. 3.38 y la Figura. 3.39 se puede observar la configuración de la red VLAN 1 con una dirección IP 1.1.1.1. /24 al igual que su debida verificación.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#no s
*Sep  4 10:39:05.307: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Switch(config-if)#
*Sep  4 10:39:10.367: %LINK-3-UPDOWN: Interface Vlan1, changed state
*Sep  4 10:39:11.369: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Switch(config-if)#ip add
Switch(config-if)#ip address 1.1.1.1 255.255.255.0
Switch(config-if)#
```

Figura. 3.38: Configuración Switch1

```
Switch(config)#int vlan 1
Switch(config-if)#no shu
*Sep  5 07:33:58.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to
down
Switch(config-if)#
*Sep  5 07:34:04.249: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Sep  5 07:34:05.250: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to
upip add 1.1.1.1 255.255.255.0
Switch(config-if)#do show ip int bri
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
GigabitEthernet0/3     unassigned      YES unset  down                  down
GigabitEthernet1/0     unassigned      YES unset  down                  down
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
GigabitEthernet2/0     unassigned      YES unset  down                  down
GigabitEthernet2/1     unassigned      YES unset  down                  down
GigabitEthernet2/2     unassigned      YES unset  down                  down
GigabitEthernet2/3     unassigned      YES unset  down                  down
GigabitEthernet3/0     unassigned      YES unset  down                  down
GigabitEthernet3/1     unassigned      YES unset  down                  down
GigabitEthernet3/2     unassigned      YES unset  down                  down
GigabitEthernet3/3     unassigned      YES unset  down                  down
Vlan1                  1.1.1.1         YES manual up                    up
Switch(config-if)#
```

Figura. 3.39: Configuración de s1

3.1.3 CONFIGURACIÓN DE S2

De igual manera que la configuración anterior el switch 2 también contará con una interfaz VLAN 1 que se encontrará en la misma red 1.1.1.0/24, hay que notar que tanto en el switch 1 como en el switch 2 aparte de la dirección VLAN no se incluye ninguna otra dirección IP como se observa en la Figura. 3.40

```
Switch(config-if)#int vlan 1
Switch(config-if)#no shut
Switch(config-if)#ip add
Switch(config-if)#ip address 1.1.1.2 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#do show ip int bri
```

Figura. 3.40: Configuración S2

3.1.4 CONFIGURACIÓN DE R1

Para la configuración de R1 o también conocido como switch de Core, empezaremos por la interfaz *fast ethernet 0/0* a la cual se le asignara la dirección IP 1.1.2.1/24, contara con el protocolo OSPF con el identificador de proceso 1 y el identificador de área 0, sin olvidar el protocolo PIM.

Para la interfaz *fast ethernet 0/1* se asigna la dirección IP 1.1.3.1/24, al igual que la interfaz f0 contara con el protocolo OSPF con el mismo indicador de proceso y área y por último el protocolo PIM.

En la interfaz de *loopback 0* se agregará la dirección IP 1.2.3.4/32, el protocolo PIM y el protocolo OSPF, además de activar el *multicasting route*.

Como se puede apreciar en la Figura. 3.41

```
R1(config)#int f 0/0
R1(config-if)#no shut
R1(config-if)#
*Sep  5 07:26:50.879: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Sep  5 07:26:51.879: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, cha
nged state to up
R1(config-if)#ip add
R1(config-if)#ip address 1.1.2.1 255.255.255.0
R1(config-if)#ip ospf 1 ar 0
R1(config-if)#int f 0/1
R1(config-if)#no sh
R1(config-if)#
*Sep  5 07:27:54.327: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Sep  5 07:27:55.327: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, cha
nged state to up
R1(config-if)#ip ad
R1(config-if)#ip add
R1(config-if)#ip address 1.1.3.1 255.255.255.0
R1(config-if)#ip ospf 1 ar 0
R1(config-if)#ip pim sp
R1(config-if)#
*Sep  5 07:28:52.131: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 1.1.3.1 on interfac
e FastEthernet0/1
R1(config-if)#int f 0/0
R1(config-if)#ip pim sp
R1(config-if)#
*Sep  5 07:29:27.131: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 1.1.2.1 on interfac
e FastEthernet0/0
R1(config-if)#int l0
R1(config-if)#
*Sep  5 07:29:52.651: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed s
tate to up
R1(config-if)#ip add
R1(config-if)#ip address 1.2.3.4 255.255.255.255
R1(config-if)#ip pim sp
R1(config-if)#
*Sep  5 07:30:33.079: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 1.2.3.4 on interfac
e Loopback0
R1(config-if)#ip ospf 1 ar 0
R1(config-if)#ip multicast-r
```

Figura. 3.41: Configuración de interfazes en Router de core

En la Figura. 3.42 se puede aprecia como a la interfaz de *loopback 0* del Router1 se la configura como en punto de encuentro para el protocolo PIM de forma bidireccional, de igual manera se muestra la table de enrutamiento *multicast IP*.

```
R1(config)#ip pim rp-address 1.2.3.4 bidir
R1(config)#
*Sep  5 07:31:47.331: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed sta
te to up
*Sep  5 07:31:47.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed sta
te to up
R1(config)#ip pim bidir
% Ambiguous command:  "ip pim bidir"
R1(config)#ip pim bidir-e
R1(config)#ip pim bidir-enable
R1(config)#do show ip mro
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.0.1.40), 00:01:48/00:02:54, RP 1.2.3.4, flags: SJCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/1, Forward/Sparse, 00:01:48/00:02:54
```

Figura. 3.42: Ip multicast routing table

3.1.5 CONFIGURACIÓN DE CSR 1

En la Figura. 3.43 se aprecia la configuración de la interfaz *gigabit ethernet 1* misma que está conectada al switch de Core, a la cual se le asigna la dirección IP 1.1.2.2 /24, por supuesto cuenta con su configuración OSPF y PIM.

```
Router(config)#int gi 1
Router(config-if)#no shut
Router(config-if)#shut
Router(config-if)#
*Sep  5 08:05:06.617: %LINK-5-CHANGED: Interface GigabitEthernet1, changed state to administrativ
ely down
*Sep  5 08:05:07.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1, changed s
tate to downno shut
Router(config-if)#
*Sep  5 08:05:23.634: %LINK-3-UPDOWN: Interface GigabitEthernet1, changed state to up
*Sep  5 08:05:24.633: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1, changed s
tate to up
Router(config-if)#ipad
Router(config-if)#ip add
Router(config-if)#ip address 1.1.2.2 255.255.255.0
Router(config-if)#do ping 1.1.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.2.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/15/30 ms
Router(config-if)#ip pim sp
Router(config-if)#
*Sep  5 08:06:39.729: %PIM-5-NBRCHG: neighbor 1.1.2.1 UP on interface GigabitEthernet1
*Sep  5 08:06:41.470: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 1.1.2.2 on interface Gigab
itEthernet1
Router(config-if)#ip ospf 1 ar 0
Router(config-if)#
*Sep  5 08:07:10.049: %OSPF-6-DFT OPT: Protocol timers for fast convergence are Enabled.
```

Figura. 3.43: Configuración de G1 en Router CSR1

En la Figura. 3.44 se aprecia la configuración de la interface de *loopback* del CSR1, siendo asignada la dirección IP 1.2.3.1/32 de igual forma, como en casos anteriores se configura el protocolo OSPF, el protocolo PIM y el protocolo de enrutamiento *multicasting* distribuido, también podemos observar cómo se configura a la interface como punto de encuentro con el comando rp-address.

```
Router(config-if)#int l0
Router(config-if)#
*Sep  5 08:07:35.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to
 up
Router(config-if)#ip add
Router(config-if)#ip address 1.2.3.1 255.255.255.255
Router(config-if)#ip pim sp
Router(config-if)#
*Sep  5 08:08:34.371: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 1.2.3.1 on interface Loopb
ack0
Router(config-if)#ip ospf 1 ar 0
Router(config-if)#exit
Router(config)#ip mul
Router(config)#ip multicast-r
Router(config)#ip multicast-routing di
Router(config)#ip multicast-routing distributed
Router(config)#ip pim rp
% Ambiguous command:  "ip pim rp"
Router(config)#ip pim rp-add
Router(config)#ip pim rp-address 1.2.3.4
Router(config)#
```

Figura. 3.44: Configuración interfaz Loopback deL CSR1

En la Figura. 3.45 se puede apreciar la Configuración de la interfaz gigabit ehternet 2, misma que es un caso especial de Configuración, al ser uno de los puntos finales de la red VXLAN.

Lo primero que podemos observar es que esta interfaz no tiene asignada una dirección IP, al contrario, se la configura como una instancia de servicio con identificador 1, configurada sin etiquetado, además se la se la define como una interfaz NVE con identificador 1 y se le asocia al VNI 5000 el cual difundirá información a través de la IP 225.1.1.1 que pertenece al grupo multicast.

De igual manera la interfaz de *loopback* será tomada como la interface fuente.

Al configura el dominio del puente VXLAN identificado como “dominio 1”, se le asigna a la interfaz *gigabit ethernet* 2 como miembro de la VNI 5000.

```
Router(config)#int gi 2
Router(config-if)#no sh
Router(config-if)#
*Sep  5 08:11:43.671: %LINK-3-UPDOWN: Interface GigabitEthernet2, changed state to up
*Sep  5 08:11:44.672: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2, changed s
tate to up
Router(config-if)#ser
Router(config-if)#serviceins
Router(config-if)#service ins
Router(config-if)#service instance 1 e
Router(config-if-srv)#encp
Router(config-if-srv)#encap
Router(config-if-srv)#encapsulation un
Router(config-if-srv)#encapsulation untagged
Router(config-if-srv)#int nve 1
Router(config-if)#int nve 1
Router(config-if)#membe
Router(config-if)#member vni 5000 mcas
Router(config-if)#member vni 5000 mcast-group 225.1.1.1
Router(config-if)#source-
Router(config-if)#source-interface lo0
Router(config-if)#
*Sep  5 08:13:36.041: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to u
p
Router(config-if)#no shut
Router(config-if)#
*Sep  5 08:13:46.743: %LINK-3-UPDOWN: Interface nve1, changed state to up
*Sep  5 08:13:47.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface nve1, changed state to up
*Sep  5 08:13:47.874: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 1.2.3.1 on interface Tunne
l1
Router(config-if)#brid
Router(config-if)#bridge-domain 1
Router(config-bdomain)#member vni 5000
Router(config-bdomain)#member gi
Router(config-bdomain)#member gigabitEthernet 2 ser
Router(config-bdomain)#member gigabitEthernet 2 service-instance 1
Router(config-bdomain-efp)#exit
```

Figura. 3.45: Configuración de la interfaz *Gigabit ethernet* 2 del Router CSR1

3.1.6 CONFIGURACIÓN CSR2

En la Figura. 3.46 se aprecia la configuración de la interfaz *gigabit ethernet* 1 misma que está conectada al switch de Core, a la cual se le asigna la dirección IP 1.1.3.2 /24, por supuesto cuenta con su configuración OSPF y PIM.

De igual manera se aprecia la configuración de la interfaz de *loopback 0* a la cual se le asigna la dirección IP 1.2.3.2 /24 igualmente cuenta con su configuración PIM y OSPF con el identificador de proceso 1 e identificador de área 0, esta interface también está activo el *multicasting routing* distribuido y al igual que el caso anterior la dirección de *loopback* 1.2.3.4 es considerado como punto de encuentro.

```
Router(config)#int gi 1
Router(config-if)#no shut
Router(config-if)#ip ad
*Sep  5 07:55:20.177: %LINK-3-UPDOWN: Interface GigabitEthernet1, changed state to up
*Sep  5 07:55:21.177: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1, change
d state to up
Router(config-if)#ip address
Router(config-if)#ip address 1.1.3.2 255.255.255.0
Router(config-if)#do ping 1.1.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.3.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 7/47/165 ms
Router(config-if)#ip pim sp
Router(config-if)#
*Sep  5 07:56:08.461: %PIM-5-NBRCHG: neighbor 1.1.3.1 UP on interface GigabitEthernet1
*Sep  5 07:56:10.212: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 1.1.3.2 on interface Gi
gabitEthernet1ip
Router(config-if)#ip ospf 1 ar 0
Router(config-if)#
*Sep  5 07:56:41.657: %OSPF-6-DFT_OPT: Protocol timers for fast convergence are Enabled.
*Sep  5 07:56:42.060: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.2.1 on GigabitEthernet1 from LOADING
to FULL, Loading Done
Router(config-if)#int l0
Router(config-if)#
*Sep  5 07:57:17.673: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
 to up
Router(config-if)#ip add
Router(config-if)#ip address 1.2.3.2 255.255.255.255
Router(config-if)#ip pim sp
Router(config-if)#
*Sep  5 07:58:11.212: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 1.2.3.2 on interface Lo
opback0
Router(config-if)#ip ospf 1 ar 0
Router(config-if)#ip multicast-r di
Router(config)#ip pimrp-add 1.2.3.4
                   ^
% Invalid input detected at '^' marker.

Router(config)#ip pim rp-add 1.2.3.4
Router(config)#
*Sep  5 07:59:21.422: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state t
```

Figura. 3.46: Configuración de interfaz G1 Lo 0

En la Figura. 3.47 se puede apreciar la Configuración de la interfaz *gigabit ehternet* 2, misma que es un caso especial de Configuración, al ser el otro punto final de la red VXLAN.

Lo primero que podemos observar es que esta interfaz no tiene asignada una dirección IP, al contrario, se la configura como una instancia de servicio con identificador 1, configurada sin etiquetado, además se define una interfaz NVE con identificador 1 y se le asocia al VNI 5000 el cual difundirá información a través de la IP 225.1.1.1 que pertenece al grupo *multicast.*

De igual manera la interfaz de *loopback* será tomada como la interface fuente.

Al configura el dominio del puente VXLAN identificado como “dominio 1”, se le asigna a la interfaz *gigabit ethernet* 2 como miembro de la VNI 5000.

```
Router(config)#int gi 2
Router(config-if)#no sh
Router(config-if)#
*Sep  5 08:17:10.296: %LINK-3-UPDOWN: Interface GigabitEthernet2, changed state to up
*Sep  5 08:17:11.297: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2, changed s
tate to up
Router(config-if)#servi
Router(config-if)#service ins
Router(config-if)#service instance 1 e
Router(config-if)#service instance 1 ethernet
Router(config-if-srv)#encap
Router(config-if-srv)#encapsulation un
Router(config-if-srv)#encapsulation untagged
Router(config-if-srv)#ex
Router(config-if)#int nve1
Router(config-if)#no shut
Router(config-if)#
*Sep  5 08:17:56.364: %LINK-3-UPDOWN: Interface nve1, changed state to down
Router(config-if)#sour
Router(config-if)#source-i
Router(config-if)#source-interface lo0
Router(config-if)#
*Sep  5 08:18:20.212: %LINK-3-UPDOWN: Interface nve1, changed state to up
*Sep  5 08:18:21.007: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to u
p
*Sep  5 08:18:21.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface nve1, changed state to up
Router(config-if)#member vni 5000 mcast
Router(config-if)#member vni 5000 mcast-group 225.1.1.1
Router(config-if)#
*Sep  5 08:19:08.114: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 1.2.3.2 on interface Tunne
l1
Router(config-if)#no shut
Router(config-if)#bridge-domain 1
Router(config-bdomain)#member vni 5000
```

Figura. 3.47: Configuración de G2

De acuerdo con la Figura. 3.48 para terminar con la configuración a la interfaz *gigabit ethernet* 2 se la asocia a la instancia de servicio 1 y se activa el protocolo PIM bidireccional, y nuevamente establecemos la dirección IP 1.2.3.4 como dirección de encuentro.

```
Router(config-bdomain)#member gigabitEthernet 2 service-instance 1
Router(config-bdomain-efp)#exit
Router(config-bdomain)#ip pim bidir-e
Router(config-bdomain)#ip pim bidir-e
Router(config)#ip pim rp-a
Router(config)#ip pim rp-add
Router(config)#ip pim rp-address 1.2.3.4 bidir
Router(config)#
```

Figura. 3.48: Configuración Bidireccional

En la Figura. 3.49 se puede constatar cuales son los puntos finales de puente o túnel VXLAN, los cuales son la interfaz G*igabit Ethernet* con MAC 0C77.4D7C.8001 y la interfaz *Gigabit Ethernet* con dirección MAC 0C77.4D7C.0000, mismas que a su vez pertenecen a la NVE1, VNI 5000 y están configuradas como VXLAN.

```
Router(config-bdomain)#do show bridge-do
Bridge-domain 1 (2 ports in all)
State: UP                    Mac learning: Enabled
Aging-Timer: 300 second(s)
    GigabitEthernet2 service instance 1
    vni 5000
   AED MAC address    Policy  Tag       Age  Pseudoport
   0   0C77.4D7C.0000 forward dynamic   297  GigabitEthernet2.EFP1

Router(config-bdomain)#do show bridge-do
Bridge-domain 1 (2 ports in all)
State: UP                    Mac learning: Enabled
Aging-Timer: 300 second(s)
    GigabitEthernet2 service instance 1
    vni 5000
   AED MAC address    Policy  Tag       Age  Pseudoport
   0   0C77.4D7C.8001 forward dynamic   300  GigabitEthernet2.EFP1
   0   0C48.572B.8001 forward dynamic   300  nve1.VNI5000, VxLAN
                                            src: 1.2.3.1 dst: 1.2.3.2
   0   0C77.4D7C.0000 forward dynamic   293  GigabitEthernet2.EFP1
   0   0C48.572B.0000 forward dynamic   257  nve1.VNI5000, VxLAN
                                            src: 1.2.3.1 dst: 1.2.3.2

Router(config-bdomain)# ip pim bidir-e
```

Figura. 3.49: Tabla MAC

3.1.7 CAPTURA DE PAQUETES ENVIADOS A TRAVÉS DE LA RED VXLAN PROTOTIPADA

Para realizar esta tarea fue necesaria la herramienta Wireshark la cual es un complemento de la herramienta GNS3.

Se procede a monitorear las interfaces antes y después de cada Router CSR con el fin de comprobar la teoría, es decir la forma de la trama antes de Router y después del Router, al Router CSR en la teoría se lo conoce como VTEP, para este caso práctico los títulos dirán antes y después del VTEP.

3.1.7.1 Antes del VTEP

Al referirnos con antes del VTEP, se refiere al tramo de red entre el switch S1 y el Router CSR. Como se puede apreciar en la Figura. 3.50 en este caso en particular se ha seleccionado un mensaje ICMP cuyo origen es la dirección 1.1.1.2 y su destino es 1.1.1.1.

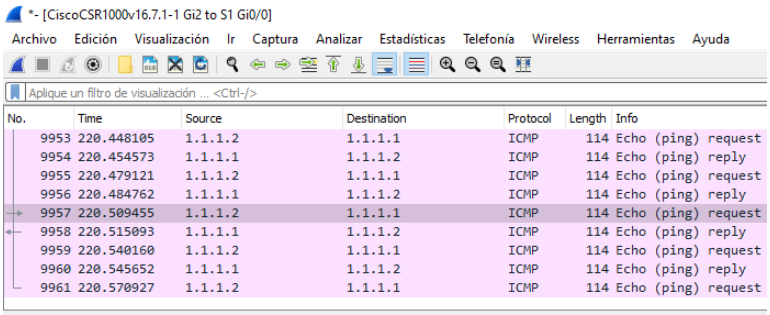


Figura. 3.50: Captura de paquetes en VTEP 1

En la Figura. 3.51 se puede evidenciar que toda la información sobre el mensaje ICMP, es encapsulada en el protocolo IP el cual a su vez tiene como datos la dirección IP origen y la dirección IP destino y está a su vez será encapsulada en la trama ethernet la cual lleva de datos las direcciones MAC origen y destino.

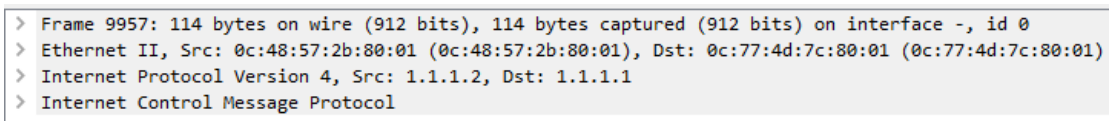


Figura. 3.51: Trama de información antes del VTEP1

Como se puede observar en la Figura. 3.52 se trata de una trama de 114 bytes con un tipo de encapsulación ethernet que indica quién tiene datos de tramas IP, trama icmp y datos.

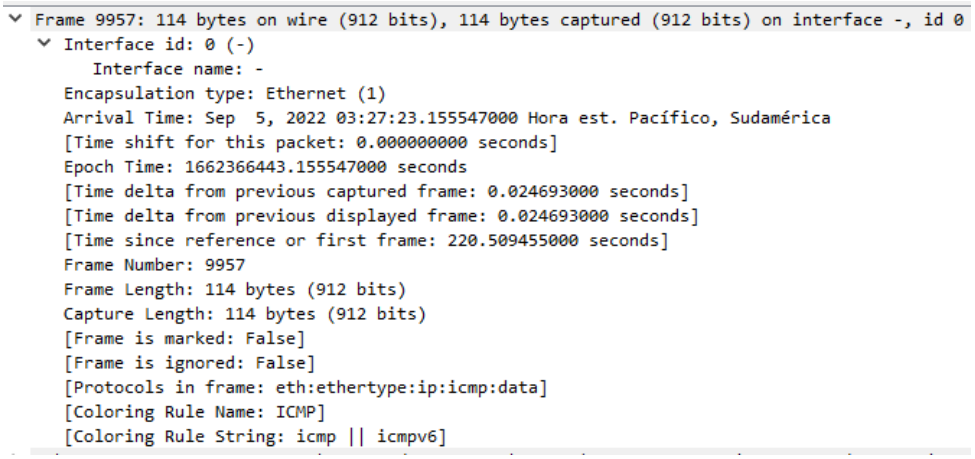


Figura. 3.52: Información de Trama

En la **Figura. 3.53** se puede observar la cabecera ethernet interna que contiene la dirección MAC origen y destino.

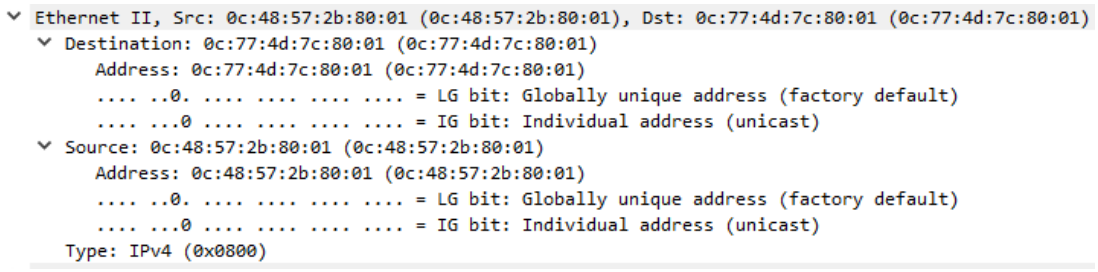


Figura. 3.53: Encabezado Ethernet

En la Figura. 3.54 se observa la cabecera IP más en detalle la cual indica la dirección IP origen destino, además del tipo de protocolo que transporta.

```
Internet Protocol Version 4, Src: 1.1.1.2, Dst: 1.1.1.1
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
   Total Length: 100
   Identification: 0x2bcd (11213)
   Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 255
   Protocol: ICMP (1)
   Header Checksum: 0x8bc7 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 1.1.1.2
   Destination Address: 1.1.1.1
```

Figura. 3.54: Encabezado IP

En la Figura. 3.55 logramos identificar el mensaje ICMP en el cual podemos verificar el tipo de mensaje y cuál es un mensaje eco request con un tamaño de datos de 72 bytes.

```
Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0x29f0 [correct]
   [Checksum Status: Good]
   Identifier (BE): 0 (0x0000)
   Identifier (LE): 0 (0x0000)
   Sequence Number (BE): 11213 (0x2bcd)
   Sequence Number (LE): 52523 (0xcd2b)
   [Response frame: 9958]
   Data (72 bytes)
      Data: 0000000000392854abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd…
      [Length: 72]
```

Figura. 3.55: Cabecera ICMP

3.1.8 DESPUÉS DEL VTEP1

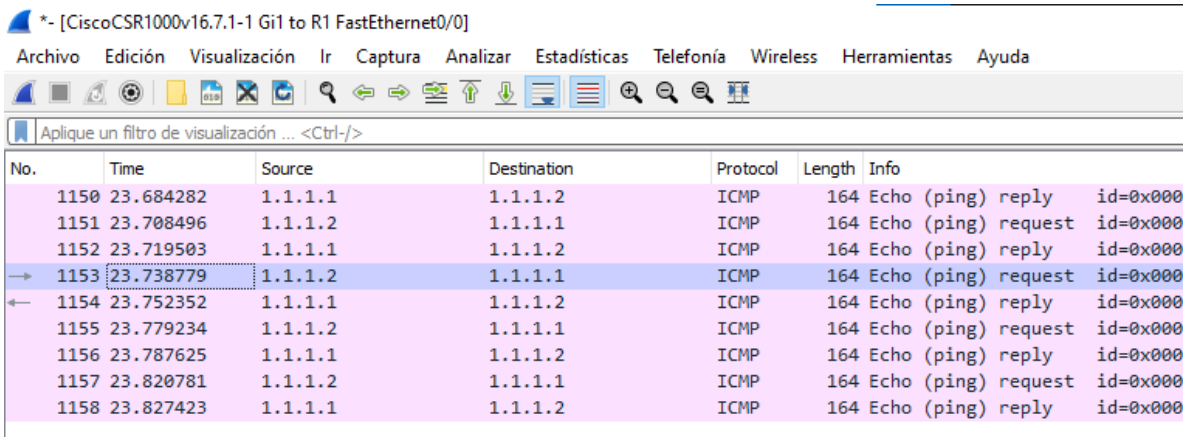


Figura. 3.56: Captura de paquete despues del VTEP 1

Como se observar en la Figura. 3.57 una vez la información atraviesa el dispositivo VTEP, se añade la cabecera ethernet, la cabecera IP, la cabecera UDP, el cual usará el puerto 64168 como puerto fuente, así como puerto destino 4789, además debe ser añadida la cabecera IP con dirección IP origen 1.2.3.2 y dirección destino 1.2.3.1 todo esto a su vez encapsulado como dato de la cabecera ethernet externa la cual indica la dirección MAC origen del VTEP y MAC destino del siguiente salto, es decir esta trama buscara en base a su dirección MAC el dispositivo de Core y de ahí partirá al VTEP correspondiente.

```
> Frame 1153: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0
> Ethernet II, Src: ca:01:0e:34:00:08 (ca:01:0e:34:00:08), Dst: 0c:30:a7:80:00:00 (0c:30:a7:80:00:00)
> Internet Protocol Version 4, Src: 1.2.3.2, Dst: 1.2.3.1
> User Datagram Protocol, Src Port: 64168, Dst Port: 4789
> Virtual eXtensible Local Area Network
> Ethernet II, Src: 0c:48:57:2b:80:01 (0c:48:57:2b:80:01), Dst: 0c:77:4d:7c:80:01 (0c:77:4d:7c:80:01)
> Internet Protocol Version 4, Src: 1.1.1.2, Dst: 1.1.1.1
> Internet Control Message Protocol
```

Figura. 3.57: Trama despues del VTEP1

En la Figura. 3.58, Al ANALIZAR LA TRAMA obtenida podemos identificar, en su cabecera se encuentran los tipos de protocolos que lleva encapsulado como son: Ethernet, IP, UDP, VXLAN, Ethernet, IP, ICMP.

```
v Frame 1153: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0
  > Interface id: 0 (-)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep  5, 2022 03:28:21.496476000 Hora est. Pacífico, Sudamérica
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1662366501.496476000 seconds
    [Time delta from previous captured frame: 0.019276000 seconds]
    [Time delta from previous displayed frame: 0.019276000 seconds]
    [Time since reference or first frame: 23.738779000 seconds]
    Frame Number: 1153
    Frame Length: 164 bytes (1312 bits)
    Capture Length: 164 bytes (1312 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:vxlan:eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
```

Figura. 3.58: Analisis de la trama

En la siguiente **Figura. 3.59** podemos observar el encabezado ethernet el cual nos muestra la dirección MAC origen del actual dispositivo y la dirección MAC destino que en este caso representa el dispositivo de Core.

```
v Ethernet II, Src: ca:01:0e:34:00:08 (ca:01:0e:34:00:08), Dst: 0c:30:a7:80:00:00 (0c:30:a7:80:00:00)
  v Destination: 0c:30:a7:80:00:00 (0c:30:a7:80:00:00)
      Address: 0c:30:a7:80:00:00 (0c:30:a7:80:00:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: ca:01:0e:34:00:08 (ca:01:0e:34:00:08)
      Address: ca:01:0e:34:00:08 (ca:01:0e:34:00:08)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Figura. 3.59: Trama Ethernet

En la siguiente Figura. 3.60, en la cabecera IP podemos observar la dirección IP origen y destino las cuales representan la parte derecha de la topología es decir pertenecen a la interfaz fast Ethernet 1 del Router de Core y a la interfaz Gigabit 1 del Router CSR2, esto lo hace con el fin de saber hacia dónde dirigir paquete el switch de Core

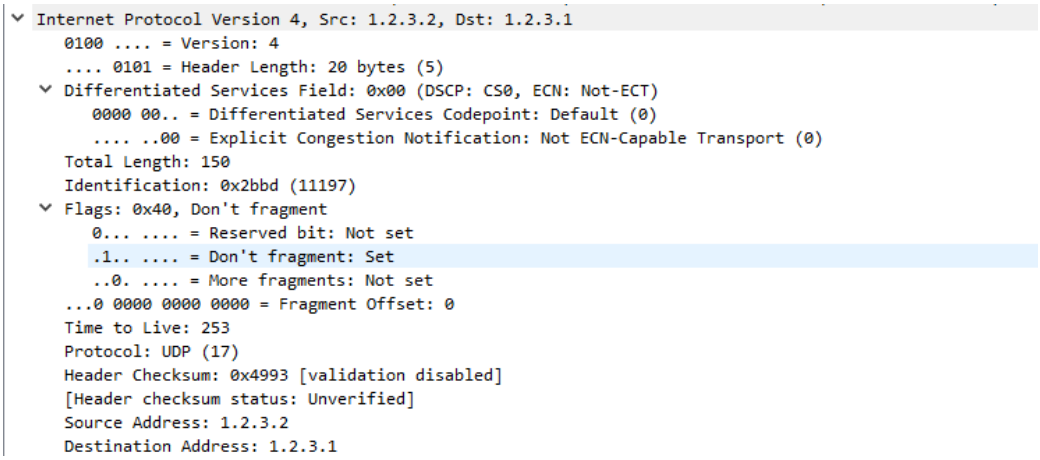


Figura. 3.60: Encabezado IP

En la Figura. 3.61 se puede observar el encabezado UDP el cual lleva el puerto origen y el puerto destino.

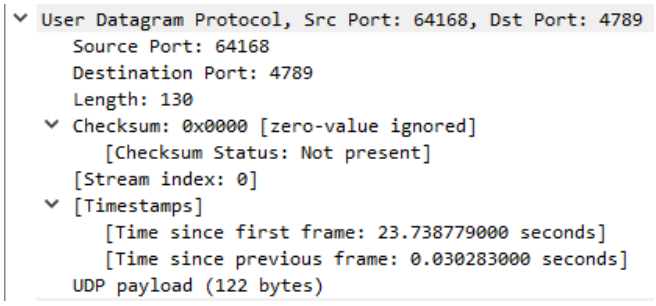


Figura. 3.61: Datagrama UDP

En la Figura. 3.62 se puede observar el encabezado VXLAN el cual lleva consigo el identificador de red VNI asociado al identificador 5000.

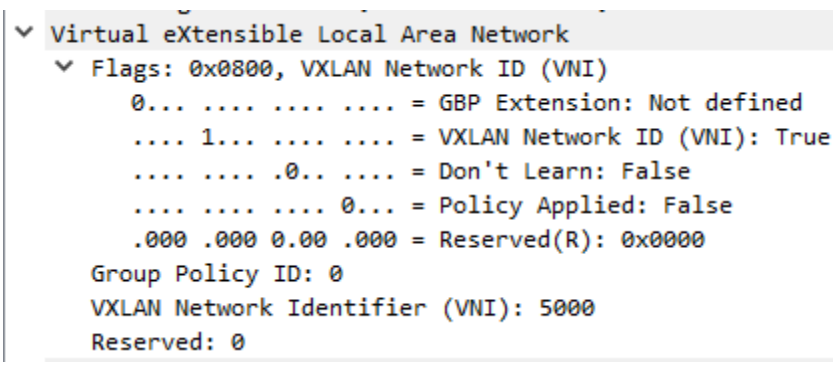


Figura. 3.62: Encabezado VXLAN

A partir de aquí se mantienen los mismos encabezados ya analizados en la sección antes del VTEP.

3.1.9 ANALISIS DE PAQUETES ANTES DEL VTEP 2

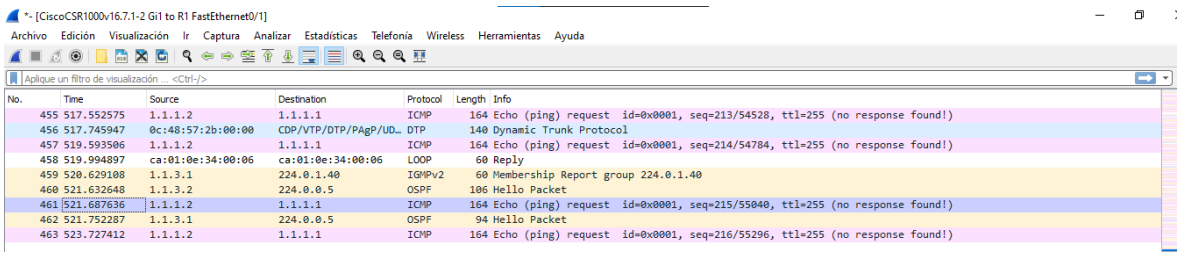


Figura. 3.63: Captura de paquetes antes del VTEP 2

Como podemos observar en la Figura. 3.64 la cabecera ethernet externa nos trae la dirección MAC origen la cual pertenece al Router de Core y como destino trae una dirección de multicast pues al traer la información a donde realmente apunta es a la MAC del grupo de multicast.

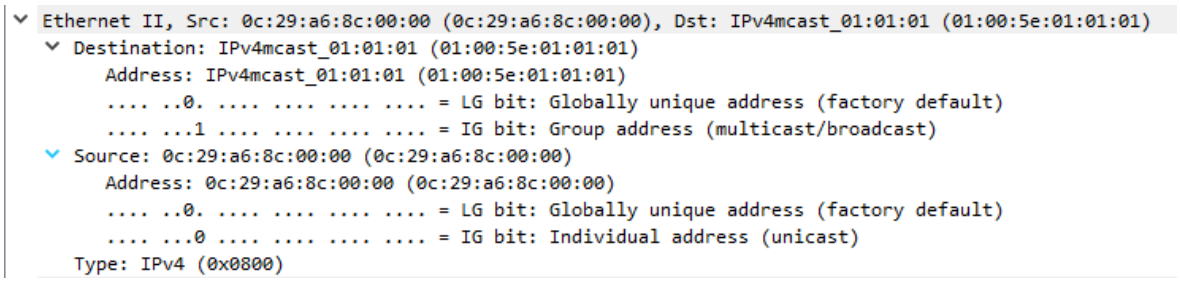


Figura. 3.64: Encabezado Ethernet externo

En la Figura. 3.65 podemos apreciar como el Router de Core a enrutado el paquete hacia la dirección IP que representa el punto de encuentro, una vez el paquete entre al VTEP este va a enrutar el paquete hacia el destino correspondiente.

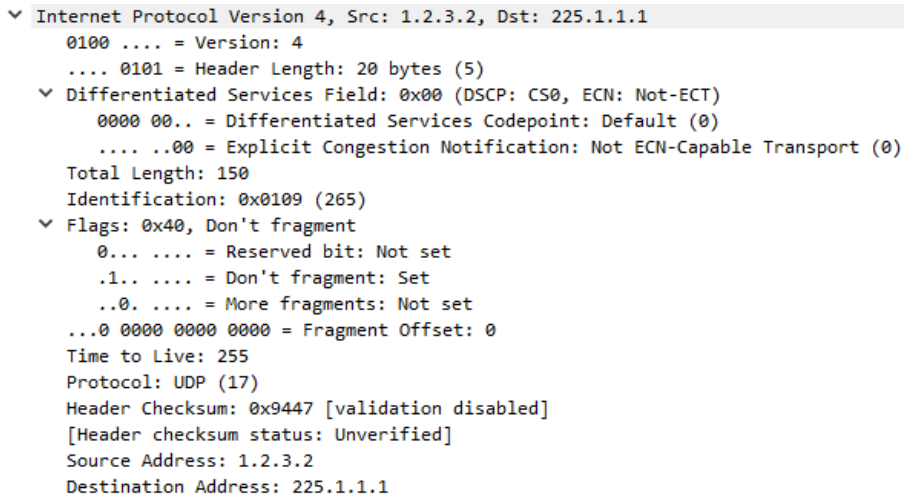


Figura. 3.65: Encabezado IP externo

En la Figura. 3.66 se observa el datagrama UDP con los puertos origen y destino.

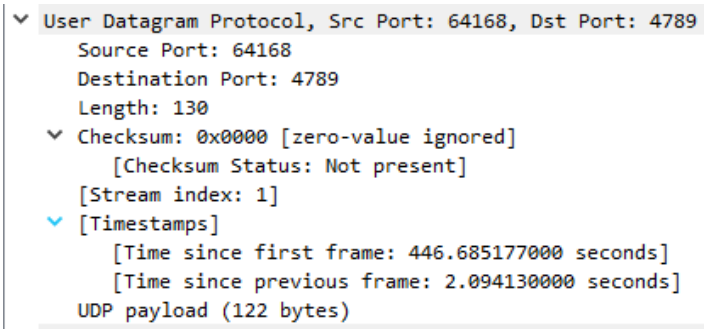


Figura. 3.66: Datagrama UDP

En la Figura. 3.67 se visualiza la cabecera VXLAN que como se trató antes maneja lo que es el VNI 5000.

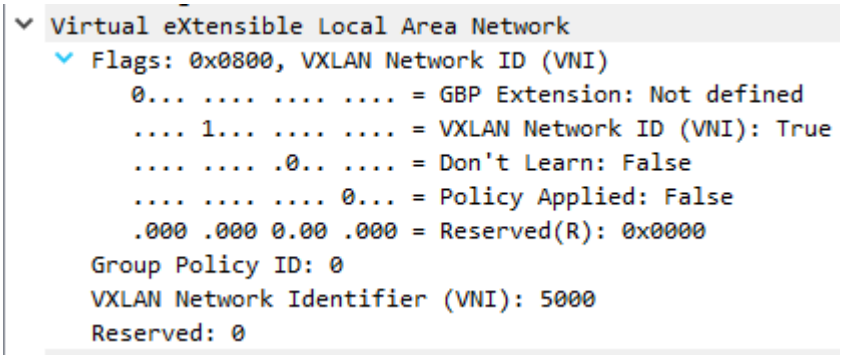


Figura. 3.67: Encabezado VXLAN

En la Figura. 3.68 se observa la cabecera ethernet en la cual se tiene la dirección MAC origen y destino en base a la cual el Router va a decidir a qué dispositivo se enruta la información.

```
Ethernet II, Src: 0c:48:57:2b:80:01 (0c:48:57:2b:80:01), Dst: 0c:77:4d:7c:80:01 (0c:77:4d:7c:80:01)
  Destination: 0c:77:4d:7c:80:01 (0c:77:4d:7c:80:01)
      Address: 0c:77:4d:7c:80:01 (0c:77:4d:7c:80:01)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: 0c:48:57:2b:80:01 (0c:48:57:2b:80:01)
      Address: 0c:48:57:2b:80:01 (0c:48:57:2b:80:01)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Figura. 3.68: Encabezado ethernet

En la Figura. 3.69 se muestra la cabecera IP interna en la cual el Router puede identificar desde que endpoint perteneciente al dominio viene la información y también para enrutar la información a la interfaz correcta.

```
Internet Protocol Version 4, Src: 1.1.1.2, Dst: 1.1.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 100
    Identification: 0x4ef7 (20215)
  Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x689d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 1.1.1.2
    Destination Address: 1.1.1.1
```

Figura. 3.69: Cabecera IP

3.1.10 DESPUES DEL VTEP 2

*- [CiscoCSR1000v16.7.1-2 Gi2 to S2 Gi0/0]

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayu

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
850	826.835206	1.1.1.2	1.1.1.1	ICMP	114	Echo (ping) r
851	827.864611	0c:48:57:2b:00:00	Spanning-tree-(for-…	STP	60	RST. Root = 3
852	828.988815	1.1.1.2	1.1.1.1	ICMP	114	Echo (ping) r
853	830.065127	0c:48:57:2b:00:00	Spanning-tree-(for-…	STP	60	RST. Root = 3
854	831.143311	1.1.1.2	1.1.1.1	ICMP	114	Echo (ping) r
855	832.158681	0c:48:57:2b:00:00	Spanning-tree-(for-…	STP	60	RST. Root = 3
856	833.242679	1.1.1.2	1.1.1.1	ICMP	114	Echo (ping) r
857	834.278231	0c:48:57:2b:00:00	Spanning-tree-(for-…	STP	60	RST. Root = 3
858	835.320175	1.1.1.2	1.1.1.1	ICMP	114	Echo (ping) r

Figura. 3.70: Paquete capturado despues del VTEP2

Una vez que la información a pasado por el Router vtep2 y procesado toda la información en base a la tabla de direcciones MAC procede a desencapsular la trama enviada llenando la dirección MAC destino con la información correcta ,al igual que la direccion ip como se observa en la Figura. 3.71.

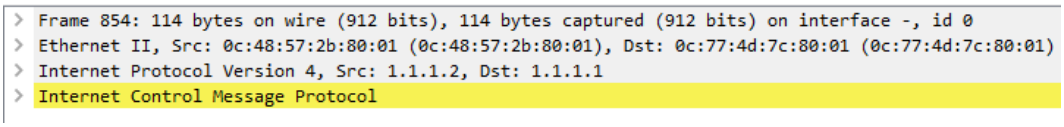


Figura. 3.71: Estructura de la trama después del VTEP2

Como podemos visualizar en la Figura. 3.66 se encuentran las diferentes direcciones MAC tanto de origen como de destino originales.

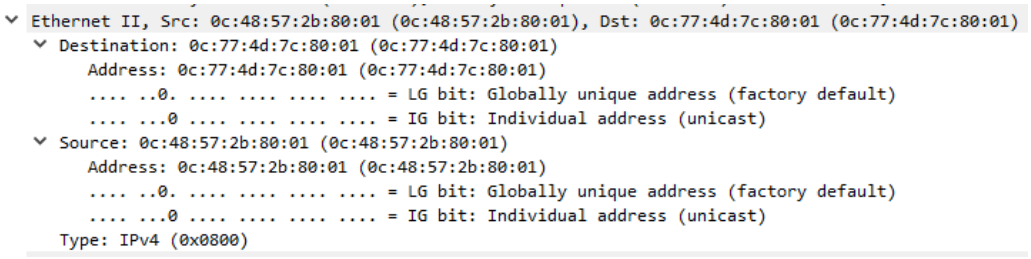


Figura. 3.72: Encabezado ethernet en VTEP 2

Como se observa en la Figura. 3.73 al analizar el protocolo IP notamos que este tiene las direcciones IP originales de los equipos terminales.

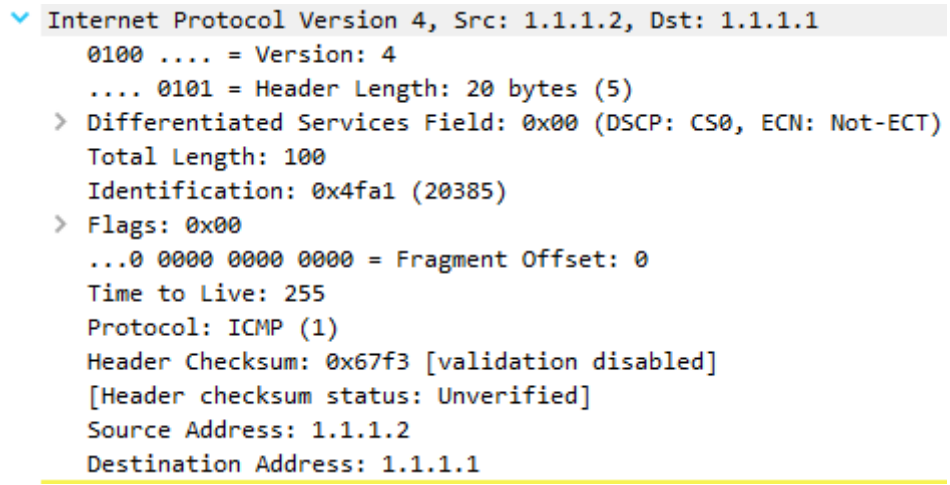


Figura. 3.73: Encabezado IP Después desencapsular en VTEP2

3.2 CONCLUSIONES

- Las redes LAN virtuales extendidas son una gran oportunidad, si bien por el momento no son tan conocidas, crean grandes impactos al brindar una amplia escalabilidad, disponibilidad para los centros de datos, además de brindar la posibilidad de comunicar lejanos sitios de trabajo al solo adquirir dos dispositivos de borde y poder reutilizar toda la infraestructura ya instalada.

- Con la implementación del prototipo se pudo constatas que las Virtual Extensible LAN realizan un encapsulado del datagrama UDP sobre ethernet posibilitando de esta manera la transmisión a través del túnel que se genera al configurar las redes VXLAN.

- Con el prototipo se identifica que si bien las Virtual Extensibles LAN (VXLAN) fueron creadas para extender las redes VLAN, esto no quiere decir que estas se encuentren totalmente desvinculadas de estas pues para lograr la implementación el prototipo fue necesaria la creación de una interface VLAN a la cual los dos switches leaf estarían conectadas, esto quiere decir que si bien aún se usarían VLAN el número de conexiones virtuales a través le nos VNE y de los varios VNI que soporta aumentaría de forma exponencial la cantidad de equipos a transmitir.

3.3 RECOMENDACIONES

- Antes de empezar a implementar un prototipo, verificar que cuente con todas las imágenes iso de los equipos, verificar si estos cuentan con la licencia necesaria para poder ejecutar los comando que se necesita, algunos iso vienen con el uso restringido de las funciones.

- Para la instalación del emulador de red GNS3 es importante conocer sobre el uso de los hipervisores como son VMware y Virtual box ya que la herramienta cuenta con una máquina virtual que si bien no es muy indispensable de instalar si es recomendable hacerlo, en vista que esta máquina ya viene optimizada para poder ejecutar varias emulaciones de equipos en ella, realizando de esta manera una doble optimización de los recursos de la maquina física.

- Para la red se deber tener muy en cuanta al momento de al momento de configurar visualizar las interfaces que se han levantado, en el caso de VXLAN que los túneles estén habilitados caso contrario no se tendrá comunicación, además de esto verificar los comandos a usar en la página oficial pues estos pueden estar sujetos a cambios o ajustes que si bien no es gran cosa nos puede desorientar al momento de configurar.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] "VXLAN: Scaling Data Center Capacity Virtual Extensible LAN (VXLAN) Overview".

[2] "VXLAN | Blogs La Salle | Campus Barcelona." https://blogs.salleurl.edu/es/vxlan (accessed May 29, 2022).

[3] "rfc7348." https://datatracker.ietf.org/doc/html/rfc7348 (accessed Jan. 16, 2022).

[4] E. F. Naranjo and G. D. Salazar Ch, "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," *2017 IEEE 2nd Ecuador Technical Chapters Meeting, ETCM 2017*, vol. 2017-January, pp. 1–6, Jan. 2018, doi: 10.1109/ETCM.2017.8247505.

[5] "¿Qué es un Centro de Datos? - Definición de TechTarget.com." https://www.techtarget.com/searchdatacenter/definition/data-center (accessed May 31, 2022).

[6] "¿Qué es un centro de datos? - cisco." https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html (accessed May 31, 2022).

[7] CommScope, "Chapter 3: Data Center topologies and architectures", Accessed: May 31, 2022. [Online]. Available: www.commscope.com

[8] "¿Qué es la arquitectura de tres niveles? IBM." https://www.ibm.com/cloud/learn/three-tier-architecture (accessed Jun. 13, 2022).

[9] "What is data center architecture? | FS Community." https://community.fs.com/blog/what-is-data-center-architecture.html (accessed Jun. 13, 2022).

[10] Yenisleidy Fernández Romero and Karen García Pombo, "Virtualización," *3 de septiembre, 2011*, pp. 61–73, 2011. Accessed: May 29, 2022. [Online]. Available: https://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/2281/1/Virtualizaci%C3%B3n.pdf

[11] "Los fundamentos de la virtualización de IT | Preemo." https://preemo.com/es/los-fundamentos-de-la-virtualizaci%C3%B3n (accessed jun. 01, 2022).

[12] "5 tipos de virtualización exitosa en los departamentos de TI | icorp Blog." http://www.icorp.com.mx/blog/tipos-de-virtualizacion/ (accessed jun. 02, 2022).

[13] "¿En qué consisten la tecnología de virtualización y las máquinas virtuales? | VMware | LATAM." https://www.vmware.com/latam/solutions/virtualization.html (accessed Jun. 02, 2022).

[14] "¿Qué son los escritorios virtuales? | Glosario de VMware | ES." https://www.vmware.com/es/topics/glossary/content/virtual-desktops.html (accessed jun. 02, 2022).

[15] "¿Qué es la virtualización de aplicaciones? | Glossary de VMware | LATAM." https://www.vmware.com/latam/topics/glossary/content/application-virtualization.html (accessed Jun. 02, 2022).

[16] E. Villar and J. Gómez, “\376\377\000M\000e\000m\000o\000r\000i\000a\000_\000P\000F\000C”, Accessed: May 29, 2022. [Online]. Available: http://www.adminso.es

[17] S. Talens-Oliag, “Herramientas de virtualización libres para sistemas GNU/Linux Congreso Internet del Mediterráneo,” 2010, Accessed: jun. 11, 2022. [Online]. Available: http://user-mode-linux.sourceforge.net/

[18] “Software de virtualización. Los 11 mejores | Ayuda Ley Protección Datos.” https://ayudaleyprotecciondatos.es/2021/05/17/software-de-virtualizacion/ (accessed jun. 11, 2022).

[19] “Descargar VMware Workstation Pro | LATAM.” https://www.vmware.com/latam/products/workstation-pro/workstation-pro-evaluation.html (accessed Jun. 11, 2022).

[20] “Soporte de Cameyo - Siempre gratis. Estamos aquí para ayudar.” https://cameyo.com/support/ (accessed jun. 11, 2022).

[21] “Instalar Windows en MAC: Parallels Desktop 17 Virtual Machine para MAC.” https://www.parallels.com/es/products/desktop/ (accessed Jun. 11, 2022).

[22] “¿Data Center Virtual o Tradicional? Ventajas y Características.” https://www.nephosit.com/data-center-virtual-o-tradicional-ventajas-y-caracteristicas/ (accessed jun. 11, 2022).

[23] “Virtual Data Center - Grandes Clientes - Movistar.” https://www.movistar.es/grandes-empresas/soluciones/fichas/virtual-data-center/ (accessed jun. 11, 2022).

[24] “Virtualización: Qué es, para qué sirve y ventajas | OpenWebinars.” https://openwebinars.net/blog/virtualizacion-que-es-para-que-sirve-y-ventajas/ (accessed jun. 11, 2022).

[25] “Beneficios de la Virtualización de Servidores con VMware.” https://www.beservices.es/beneficios-virtualizacion-servidores-vmware-n-5445-es (accessed jun. 11, 2022).

[26] “Data center virtual.” https://www.clarocloud.com.ec/portal/ec/cld/productos/infraestructura/datacenter-virtual/#!/ (accessed Jun. 11, 2022).

[27] “Consolidación del Data Center: ¿Qué es virtualización y qué beneficios tiene?” https://www.orbit.es/consolidacion-del-data-center-que-es-la-virtualizacion-y-que-beneficios-tiene/ (accessed jun. 11, 2022).

[28] “Data Center y virtualización - www.seditel.eu.” https://www.seditel.eu/data-center-y-virtualizacion (accessed jun. 11, 2022).

[29] “Virtual Data Center versus Infraestructura tradicional - Servicios en la Nube, Infraestructura TI seguridad informática.” https://garatucloud.com/virtual-data-center-versus-infraestructura-tradicional/ (accessed jun. 11, 2022).

[30] “IEEE 802.1Q Frame Format - Huawei.” https://support.huawei.com/enterprise/br/doc/EDOC1100088104 (accessed Aug. 10, 2022).

[31] “华为CloudEngine 12800交换机VXLAN技术白皮书 - 华为企业业务.” https://e.huawei.com/cn/material/networking/dcswitch/361290eaffa542b0adc309ebe5a4955b (accessed Aug. 11, 2022).

[32] “¿Qué es EVPN-VXLAN en una red empresarial? | Juniper Networks EE. UU.” https://www.juniper.net/us/en/research-topics/what-is-evpn-vxlan.html (accessed Aug. 27, 2022).

5 ANEXOS

ANEXO I

Portal web para descargas del proveedor GNS3

https://gns3.com/marketplace/appliances

ANEXO II

Portal web para descargas del proveedor Cisco

https://software.cisco.com/download/home/284364978/type/282046477/release/Amsterdam-17.3.4a

ANEXO III

Codificación de VLAN en s1

S1(config-if)#int vlan 1

S1(config-if)#no shut

S1(config-if)#ip add

S1(config-if)#ip address 1.1.1.1 255.255.255.0

S1(config-if)#no shut

S1(config-if)#do show ip int bri

Codificación de VLAN en s2

S2(config-if)#int vlan 1

S2(config-if)#no shut

S2(config-if)#ip add

S2(config-if)#ip address 1.1.1.2 255.255.255.0

S2(config-if)#no shut

S2(config-if)#do show ip int bri

ANEXO IV

Configuración de Router 1

```
R1#enable

R1#conf t

R1(config)#int f 0/0

R1(config-if)#no shut

R1(config-if)#

R1(config-if)#ip add

R1(config-if)#ip address 1.1.2.1 255.255.255.0

R1(config-if)#ip ospf 1 ar 0

R1(config-if)#int f 0/1

R1(config-if)#no sh

R1(config-if)#ip

R1(config-if)#ip add 1.1.3.1 255.255.255.0

R1(config-if)#ip ospf 1 ar 0

R1(config-if)#ip  pim sp

R1(config-if)#

R1(config-if)#int f 0/0

R1(config-if)#ip pim sp

R1(config-if)#

R1(config-if)#int l0

R1(config-if)#ip address 1.2.3.4 255.255.255.255

R1(config-if)#ip pim sp

R1(config-if)#ip ospf 1 ar 0

R1(config-if)#ip multicast-r

R1(config)#ip pim rp-add
```

```
R1(config)#ip pim rp-address 1.2.3.4 bidir

R1(config)#ip pim bidir-enable

R1(config)#do show ip mro
```

ANEXO V

Configuración CSR1

CSR1>enable

CSR1#conf t

CSR1(config)# int gi 1

CSR1(config-if)#no shut

CSR1(config-if)#ip address 1.1.2.2 255.255.255.0

CSR1(config-if)#do ping 1.1.2.1

CSR1(config-if)#ip pim sp

CSR1(config-if)#ip ospf 1 ar 0

CSR1(config-if)#int l0

CSR1(config-if)#ip address 1.2.3.1 255.255.255.255

CSR1(config-if)#ip pim sp

CSR1(config-if)#ip ospf 1 ar 0

CSR1 (config-if)#exit

CSR1 (config)#ip multicast-routing distributed

CSR1 (config)#ip pim rp-address 1.2.3.4

CSR1 (config)#do show ip ro

CSR1 (config)#do ping 1.2.3.4

CSR1 (config)#int gi 2

CSR1 (config-if)#no sh

CSR1(config-if)#service instance 1 ethernet

CSR1(config-if-srv)#encapsulation untagged

CSR1 (config-if)#int nve 1

CSR1 (config-if)#member vni 5000 mc

CSR1 (config-if)#member vni 5000 mcast-group 225.1.1.1

CSR1 (config-if)#source-interface lo0

CSR1 (config-if)#no shut

CSR1 (config-if)#bridge-domain 1

CSR1 (config-bdomain)#member vni 5000

CSR1 (config-bdomain)#member gigabitEthernet 2 service-instance 1

CSR1 (config-bdomain-efp)#exit

CSR1 (config-bdomain)#exit

CSR1 (config)#do show bridge-domain

CSR1 (config)#ip pim bidir-enable

CSR1 (config)#ip pim rp-address 1.2.3.4 bidir

ANEXO VI

Configuración CSR2

Router(config)#int gi 1

Router(config-if)#no shut

Router(config-if)#ip address 1.1.3.2 255.255.255.0

Router(config-if)#do ping 1.1.3.1

Router(config-if)#ip pim sp

Router(config-if)#ip ospf 1 ar 0

Router(config-if)#int l0

Router(config-if)#ip address 1.2.3.2 255.255.255.255

Router(config-if)#ip pim sp

Router(config-if)#ip ospf 1 ar 0

Router(config-if)#ip multicast-r di

Router(config)#ip pim rp-add 1.2.3.4

Router(config)#do show ip ospf nei

Router(config)#int gi 2

Router(config-if)#no sh

Router(config-if)#service instance 1 ethernet

Router(config-if-srv)#encapsulation untagged

Router(config-if-srv)#ex

Router(config-if)#int nve1

Router(config-if)#no shut

Router(config-if)#source-interface lo0

Router(config-if)#member vni 5000 mcast-group 225.1.1.1

Router(config-if)#no shutdown

Router(config-if)#bridge-domain 1

```
Router(config-bdomain)#member vni 5000
Router(config-bdomain)#member gigabitEthernet 2 service-instance 1
Router(config-bdomain-efp)#exit
Router(config-bdomain)#exit
Router(config)#ip pim bidir-enable
Router(config)#ip pim rp-address 1.2.3.4 bidir
```

ANEXO VII

Tabla 3: Comandos básicos para configurar VXLAN

Command or Action		Objective
Enable multicast-routing and bidirectional PIM. Static RP is used for simplicity		
1	IP multicast-routing distributed	activamos el ruteo multicast
2	IP PIM bidir-enable	activamos el protocolo de multicast independiente
3	IP PIM rp-address [IP] bidir	asignamos una dirección IP para el tráfico bidireccional
OSPF is used to provide reachability		
4	Router ospf 1	activamos ospf en el Router
5	Router-ID [IP address]	asignamos una dirección IP
6	interface Loopback0	seleccionamos la interfaz de *loopback*
7	IP address [IP address][subnet mask]	asociamos una dirección IP y su respectiva submascara de red
8	IP PIM [mode]	modo de operación de PIM
9	IP ospf [ID process] area [area ID]	asociamos un ID de proceso y el área donde se va a ejecutar
Associate VNI 4096 with mcast-group		
10	interface [nve#]	definimos una red virtual extendida y un ID
11	no IP address	
12	member VNI [1-16millon] mcast-group [IP multicast group]	asociamos un Identificador de red virtual y una IP para el grupo multicast
13	source-interface [interface lo0]	interfaz fuente
L3 interface towards core		
14	interface[type interface #]	Identificamos el tipo de interface hacia el Core

15	IP address [IP address][subnet mask]	asignamos dirección IP Y submascara de red
16	IP PIM [mode]	modo de operación de PIM
17	IP ospf [ID process] area [area ID]	asociamos un ID de proceso y el área donde se va a ejecutar
18	negotiation auto	
LAN interface from where we want to extend L2 via VXLAN across the L3 network		
19	interface [type interface #]	definimos la interface desde donde va el puente VXLAN
20	service instance [ID] [type interface]	asociamos a un ID y el tipo de interface
21	encapsulation [mode]	definimos modo de encapsulación
22	bridge-domain [ID]	definimos ID del puente
23	member VNI [ID]	Identificamos que VNI va a tener acceso a ese puente
24	member [interface] service-instance [ID]	asociamos la interfaz y el ID a la VNI