ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

"ANÁLISIS DE LA TECNOLOGÍA MULTICAST VPN EN REDES MPLS PARA LA TRANSMISIÓN DE SERVICIOS DE VIDEO STREAMING."

Trabajo de Titulación

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

INGENIERO EN TELECOMUNICACIONES

AUTOR:

CARLOS ALEXIS MAFLA GER

Riobamba - Ecuador

2023

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

"ANÁLISIS DE LA TECNOLOGÍA MULTICAST VPN EN REDES MPLS PARA LA TRANSMISIÓN DE SERVICIOS DE VIDEO STREAMING."

Trabajo de Titulación

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

INGENIERO EN TELECOMUNICACIONES

AUTOR: CARLOS ALEXIS MAFLA GER

DIRECTOR: ING. ALBERTO LEOPOLDO ARELLANO AUCANCELA

Riobamba - Ecuador

2023

Yo, Carlos Alexis Mafla Ger, declaro que el presente Trabajo de Titulación es de mi autoría y los resultados de este son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 15 de mayo del 2023

Carlos Alexis Mafla Ger
0401439831

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE INFORMÁTICA Y ELECTRÓNICA
CARRERA TELECOMUNICACIONES

El Tribunal de Trabajo de Titulación certifica que: El Trabajo de Titulación: Tipo: Proyecto de Investigación, **"ANÁLISIS DE LA TECNOLOGÍA MULTICAST VPN EN REDES MPLS PARA LA TRANSMISIÓN DE SERVICIOS DE VIDEO STREAMING."**, realizado por el señor **CARLOS ALEXIS MAFLA GER**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el tribunal autoriza su presentación.

NOMBRE	FIRMA	FECHA
Ing. Wilson Oswaldo Baldeón López **PRESIDENTE DEL TRIBUNAL**		15-05-2023
Ing. Alberto Leopoldo Arellano Aucancela **DIRECTOR DEL TRABAJO DE TITULACIÓN**		15-05-2023
Ing. Diego Fernando Veloz Cherrez **ASESOR DEL TRABAJO DE TITULACIÓN**		15-05-2023

DEDICATORIA

A mis padres, quienes me han apoyado en todo momento y han luchado por forjar la persona que soy en la actualidad, muchos de mis logros se los debo a ustedes entre los que se incluye este, agradezco todas sus motivaciones para que alcance mis anhelos y sueños. A mi hermana quien se ha convertido en mi soporte y pilar fundamental en estos últimos años difíciles. A Eli y mis amigos, que con voces de aliento impidieron que me diera por vencido y siempre creyeron en mí.

Carlos

AGRADECIMIENTOS

Mi más sincero agradecimiento a la Escuela Superior Politécnica de Chimborazo sobre todo a la Facultad de Informática y Electrónica por permitirme formarme académicamente para ser un profesional, a cada uno de los ingenieros que han compartido sus conocimientos, en especial a maestros que colaboraron en mi etapa de crecimiento personal y profesional, agradezco por guiarme y ayudarme en todo este proceso.

Carlos

ÍNDICE DE CONTENIDO

CAPITULO III

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El crecimiento global en el uso de servicios de video streaming ha generado la necesidad de actualizar y optimizar la forma en que los proveedores de estos servicios manejan el contenido para minimizar los problemas durante su consumo. Por lo tanto, el objetivo de esta investigación fue analizar la tecnología Multicast VPN en redes MPLS para la transmisión de servicios de video streaming. La metodología implementada se basó en un enfoque cuantitativo. Se llevó a cabo una simulación experimental en la cual se evaluó el funcionamiento de los perfiles Multicast VPN y cómo cada uno de ellos interactúa con los tipos de transmisión multicast y unicast entre 2 clientes y 2 servidores. Se determinó que, antes de analizar los perfiles MVPN, es necesario realizar pruebas de ancho de banda para verificar el funcionamiento de la red. Posteriormente, se obtuvieron resultados de transmisión unicast y multicast utilizando las herramientas Ostinato y VLC Media Player. La utilización de la tecnología Multicast VPN permitió a los clientes beneficiarse de una transmisión de contenido en streaming más eficiente, segura y escalable, lo cual es especialmente importante cuando se necesita transmitir información a una audiencia dispersa geográficamente. Como conclusión, se encontró que los perfiles MVPN permitieron optimizar el envío de tráfico multicast y que la encapsulación MPLS ofrecida por algunos perfiles MVPN demostró una mayor eficiencia al transmitir servicios de video streaming. Estos hallazgos destacan la importancia de adoptar tecnologías como Multicast VPN para mejorar la calidad y la experiencia de los servicios de video streaming.

Palabras clave: <PROTOCOLOS DE COMUNICACIÓN>, <EVALUACIÓN DEL FUNCIONAMIENTO>, <VIDEO STREAMING>, <GNS3 (SOFTWARE)>, <PERFILES MULTICAST VPN>

1456-DBRA-UPT-2023

SUMMARY

The growth of users who use video streaming services worldwide every day has meant that the way in which this type of content is handled by each of the providers of said services needs to be updated and optimized so that the inconveniences to time of consumption of streaming video services are minimal, therefore, the objective of this research was to analyze multicast VPN technology in MPLS networks for the transmission of streaming video services. The implemented methodology had a quantitative approach. An experimental scenario was simulated in which the operation of the Multicast VPN profiles is evaluated and how each one of them acts with the types of multicasts and unicast transmission between 2 clients and 2 servers. Through this technology, it was possible to determine that, prior to analyzing each of the MVPN profiles, it is necessary to carry out bandwidth tests that allow verifying the throughput of the network. Subsequently, unicast and multicast transmission results were obtained with the Ostinato and VLC Media Player tools. By using Multicast VPN technology, the client can benefit from a more efficient, secure and scalable transmission of streaming content, which is especially important if information needs to be transmitted to a geographically dispersed audience. In this context, it is concluded that MVPN profiles allow optimizing the sending of multicast and unicast traffic. It is also concluded that the MPLS encapsulation offered by some MVPN profiles offers greater efficiency when transmitting streaming video services.

Keywords: <COMMUNICATION PROTOCOLS>, <PERFORMANCE EVALUATION>, <VIDEO STREAMING>, <GNS3 (SOFTWARE)>, <MULTICAST VPN PROFILES>.

MSc. Wilson G. Rojas
CI: 0602361842

INTRODUCCIÓN

En la era digital actual, la transmisión eficiente de datos es esencial para garantizar la conectividad y el intercambio de información en redes empresariales. Una de las tecnologías más utilizadas para este propósito es Multiprotocol Label Switching (MPLS), que permite el enrutamiento de paquetes de datos de manera rápida y eficiente. Dentro del contexto de las redes MPLS, el Multicast VPN (Virtual Private Network) se ha convertido en una solución cada vez más popular para la transmisión de datos en grupos selectivos, ya que combina los beneficios de la tecnología de multidifusión con las capacidades de enrutamiento de MPLS.

Multicast VPN en redes MPLS es una técnica que permite la distribución de datos a múltiples destinatarios de manera simultánea, utilizando una infraestructura de red MPLS como base. A diferencia del enrutamiento unicast, que envía una copia individual de los datos a cada receptor, el multicast envía una sola copia de los datos a múltiples destinatarios que pertenecen a un grupo específico. Esto reduce significativamente el ancho de banda utilizado y mejora la eficiencia de la red, especialmente en entornos donde se transmiten grandes volúmenes de datos a múltiples usuarios al mismo tiempo, como en aplicaciones de streaming de video en tiempo real, conferencias en línea y distribución de contenido multimedia.

La implementación de multicast VPN en redes MPLS ofrece muchas ventajas. En primer lugar, proporciona una transmisión de datos eficiente y optimizada, ya que minimiza la duplicación de paquetes y aprovecha al máximo el ancho de banda disponible. Esto es especialmente beneficioso en redes empresariales donde la eficiencia de la red es crucial para garantizar el rendimiento y la satisfacción de los usuarios.

CAPÍTULO I

1. ANTECEDENTES

Desde noviembre de 1931 el ser humano se ha visto atraído por la presentación de contenido audiovisual (Zworykin 1935, p. 15), este contenido en el pasado se mostraba en diferentes medios como la radio y la televisión analógicas . Gracias a la evolución tecnológica a lo largo de los años la distribución de contenido multimedia ha podido ir cambiando y presenta nuevas ofertas que van de la mano con el crecimiento de las redes de telecomunicaciones.

El consumo de servicios de video streaming en la actualidad es el principal causante de la necesidad de mayor ancho de banda por parte de los usuarios, ya que estos servicios generan un tráfico considerablemente mayor al resto de aplicaciones, razón por la cual las empresas que prestan servicios de video streaming se han visto en la necesidad de mejorar día a día la emisión de sus contenidos.

Los usuarios de los servicios de video streaming desean que el consumo del contenido sea lo más accesible posible (Castrillo, Estupiñán, Guardia 2011, p. 43), es decir que el contenido sea presentado como y cuando el usuario lo desee y que el mismo presente cualidades que permitan disfrutar su visualización.

Netflix en la actualidad es considerado un gigante empresarial debido a que distribuye legalmente a través de la red una cantidad muy alta de contenido multimedia como: películas, cortometrajes, series, documentales, miniseries, etc. Los mismos en el pasado eran cedidos por productoras, televisiones y grupos empresariales pero que en la actualidad son producidos por la misma compañía. Se considera que su crecimiento se debe en gran parte a su accesible y módica tarifa mensual y a la calidad de sus servicios, puntos que le han permitido alcanzar más de 20 millones de clientes sólo en Norteamérica. Los números de Netflix a nivel mundial son realmente impresionantes, tanto en el uso de tráfico como en el mercado pago es uno de los más importantes con un 30% más que su competencia directa en los que podemos encontrar a DirecTV Now, HBO Now, Amazon Prime y Hulu (Pino, Aguado 2012, p. 27).

La estimación de cisco para el año 2022 era que este se encuentre alrededor de 400 exabytes mensuales, de este tráfico la mayoría se consideraba que sería debido al consumo de video con un 70%, el 30% restante lo ocuparía el tráfico generado por los usuarios de juegos en línea, la compartición de archivos y la navegación por internet. (Index 2018, p. 65)

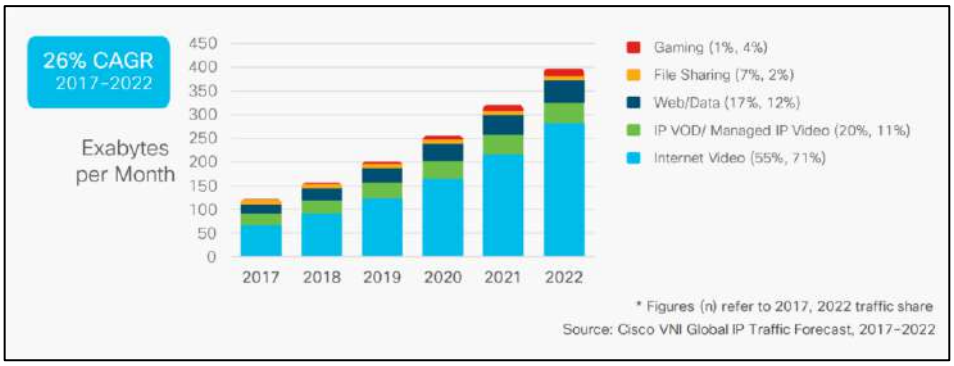


Ilustración 1-1: Cisco VNI Global IP Traffic Forecast, 2017-2022

Fuente: (Index 2018).

Para el año 2023 las estimaciones cambiaron drásticamente, debido a que las conexiones máquina a máquina M2M, utilizadas para IoT, reflejan el 50% de los dispositivos y conexiones conectados a nivel mundial. Con respecto a la transmisión de video se debe destacar que gracias a la adquisición masiva de dispositivos que permiten consumir video en ultra alta definición o 4k el tráfico enviado mediante internet crece de forma abrumadora ya que dichos dispositivos consumen el doble de la tasa de bits utilizada para transmitir un video en calidad HD y 9 veces la tasa de bits con respecto a un video en calidad SD. Debido a esto las estimaciones de tráfico para 2023 por parte de cisco, se han superado totalmente (Cisco, Internet 2020, p. 23).

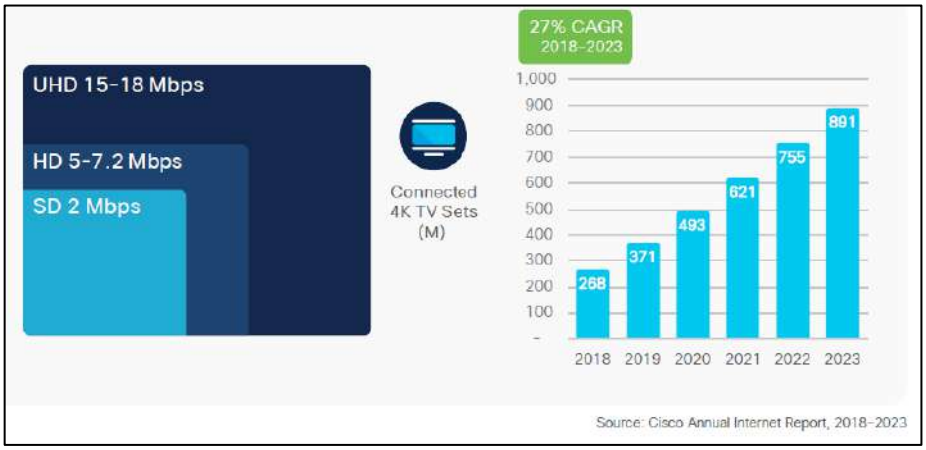


Ilustración 1-2: Predicción de consumo de video para 2023 según Cisco.

Fuente: (Cisco, Internet 2020)

Las empresas que prestan servicios de video streaming llegaron para quedarse, son consideradas como uno de los puntos fuertes en la emisión de contenido multimedia, con un crecimiento exponencial en los últimos años, buscan ahora métodos que permitan asegurar la emisión de sus contenidos, cuidando así la privacidad de la información de cada uno de sus usuarios y tratando

de resolver los problemas que se presentan al consumir el contenido multimedia como latencia y baja calidad de video recibido.

1.1. Formulación del problema

¿Es posible realizar la transmisión de servicios de video streaming mediante multicast VPN en redes MPLS?

1.2. Sistematización del problema

¿Cuáles son los protocolos que existen y que se utilizan en la tecnología multicast VPN en redes MPLS para la transmisión de servicios de video streaming?
¿Cuáles son los parámetros de rendimiento y QoS que afectan a la transmisión de servicios de video streaming en multicast VPN sobre redes MPLS?
¿Es posible diseñar un prototipo de pruebas de la tecnología multicast VPN en redes MPLS para la transmisión de servicios de video streaming?
¿Se puede evaluar el funcionamiento de la tecnología para la transmisión de servicios de video streaming en el prototipo planteado?

1.3. Justificación teórica

Las empresas que prestan servicios de video streaming en la actualidad ofrecen una gran cantidad de opciones como servicios de video bajo demanda e IPTV, la transmisión de dichos servicios es realizada a través de la red de internet y la calidad con que estos servicios lleguen a cada uno de los consumidores depende en gran parte del ancho de banda que cada uno posee, si el ancho de banda no es suficiente para la visualización de un contenido determinado, este no podrá ser reproducido o presentará intermitencias en su reproducción (Rosen, Aggarwal 2012, p. 9) .

La presente investigación se enfoca en el análisis del funcionamiento de multicast VPN en redes MPLS para la transmisión de servicios de video streaming. Al realizar la investigación bibliográfica acerca de temas similares en los repositorios digitales de las 10 principales universidades del Ecuador: Escuela Politécnica Nacional, Universidad San Francisco de Quito, Pontificia Universidad Católica del Ecuador, Universidad de las Fuerzas Armadas , Universidad de Cuenca, Universidad Politécnica Salesiana Ecuador, Universidad Técnica de Ambato y Universidad Central del Ecuador, Escuela Superior Politécnica de Chimborazo, se pudo evidenciar que aún no se han realizado investigaciones similares a pesar de ser una tecnología que fue desarrollada en 2012.

Existen investigaciones de temas relacionados como: "Estudio y diseño de redes virtuales privadas (VPN) basadas en tecnología MPLS" realizado en la Escuela Politécnica Nacional (Castillo et al. 2004, p. 4), "Análisis, diseño y simulación de una red MPLS de un portador nacional que permita comparar los servicios de VPN capa 2 y capa 3", realizada en la Escuela Superior Politécnica del Litoral y "Estudio de redes privadas virtuales basadas en la Tecnología MPLS", realizado en la Escuela Superior Politécnica del Ejército (Segarra Zambrano 2009, p. 14). Estos documentos han sido tomados como fuente de consulta para el presente análisis.

A nivel internacional existen algunos artículos científicos que tratan el tema como el realizado por Yelmo Isaías, David Larrabeiti e Ignacio Soto en la Universidad Carlos III de Madrid con el título, "Multicast Traffic Aggregation in MPLS-Based VPN Networks" (Martínez Yelmo et al. 2007, p. 23), el mismo que habla acerca de los árboles de distribución de tráfico multicast en redes VPN sobre redes IP-MPLS y también, "Performance Evaluation of MPLS in a Virtualized Service Provider Core (with/without Class of Service)" realizado por Utkarsh Shah estudiante de B. Thomas Golisano College (Shah 2017, p. 34).

Uno de los mayores inconvenientes en la transmisión de contenido audiovisual en la actualidad es la presencia de algunos problemas como latencia y baja calidad de video. Estos pueden ser resueltos al aumentar el ancho de banda, pero esto supone costos muy altos. En razón a lo anterior se puede destacar que es muy importante la investigación de nuevas tecnologías que permitan mejorar la forma en que el contenido audiovisual es distribuido por empresas que prestan dichos servicios, puesto que las predicciones a futuro indican, que la transmisión de video representará más del 50% de todo el tráfico en la red (Martínez Yelmo et al. 2007, p. 16).

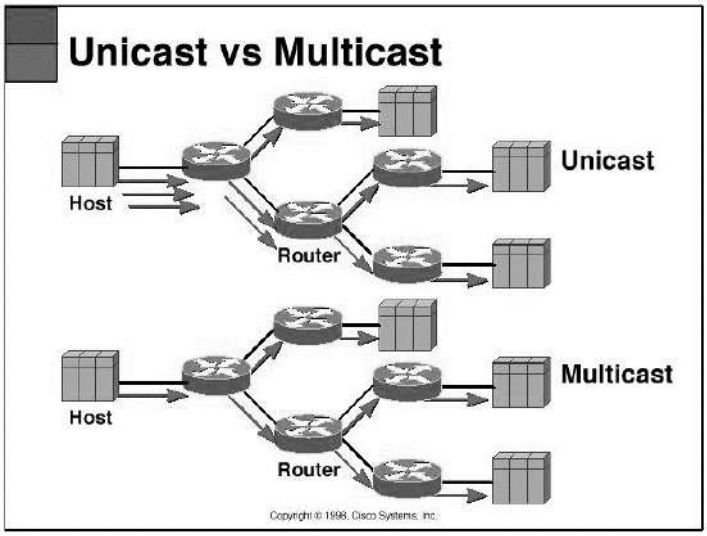


Ilustración 1-3: Representación de la transmisión Unicast vs Multicast

Fuente: (Martínez Yelmo et al. 2007)

Para el envío de datos en la capa 2 se pueden utilizar los métodos de transmisión: unicast y multicast. La principal diferencia entre los dos es que en el método unicast, el servidor debe enviar un paquete diferente por cada usuario receptor. En cambio, en el método multicast el servidor envía 1 solo paquete para todos los usuarios que lo soliciten. Esto produce que tanto el servidor como los routers necesiten mayor cantidad de recursos y la tasa de transferencia también sea mayor para la utilización del método unicast. En la actualidad se utilizan los dos métodos para la transmisión de datos sobre redes IP. Las principales redes de distribución de contenidos a nivel mundial (CDN) están empezando a utilizar transmisión multicast debido a las ventajas que esta presenta, en versiones CDN 1.0 y CDN 2.0 se utilizaba transmisión unicast, la versión CDN 3.0 utiliza multicast como su característica (Conde 2017, p. 29).

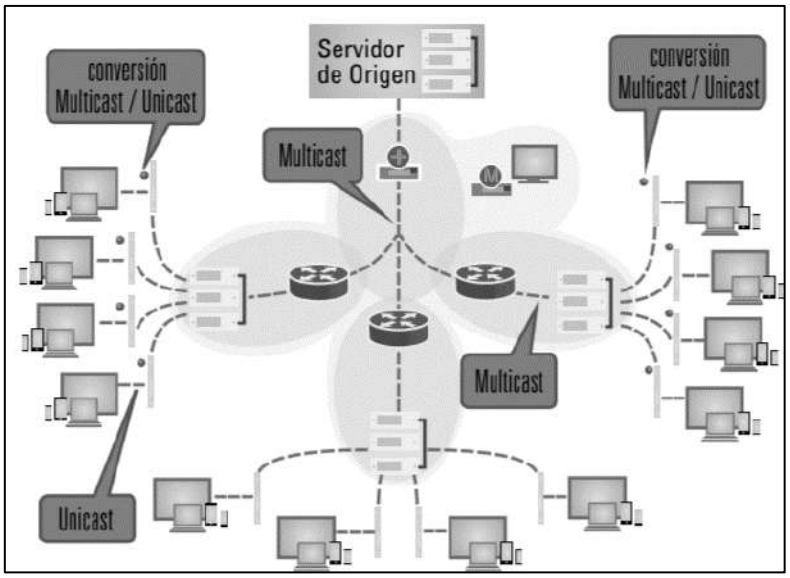


Ilustración 1-4: Optimización de la red de un operador con CDN 3.0

Fuente: (Conde 2017).

Una de las características más importantes de MPLS es permitir implementar VPN de capa 3, en Ecuador la mayoría de los proveedores de servicios de internet utilizan esta tecnología para garantizar la estabilidad de servicio a sus clientes. Estos proveedores dan servicios de VPN capa 3 para tráfico unicast, multicast VPN presenta la misma característica, pero con la diferencia de poder enviar tráfico multicast, permitiendo la utilización ingeniería de tráfico y garantizando la calidad de servicio. En redes IP se pueden implementar soluciones similares a MVPN como túneles GRE, túneles L2TP e IPSEC, pero sobre los cuales la implementación de ingeniería de tráfico es complicada. El análisis de esta tecnología pretende resolver los problemas que existen al reproducir servicios de video streaming en sitios en donde el ancho de banda no es demasiado alto, estos problemas son la latencia y la baja calidad de video con la que el servicio llega a cada uno de los consumidores (Castillo et al. 2004, p. 34).

1.4. Justificación aplicativa

Como se indicó en el apartado anterior al no existir un estudio realizado sobre esta tecnología en las universidades consultadas, el presente trabajo pretende hacer una evaluación de uno de los servicios que mayor presencia va a tener en los próximos 20 años en el internet.

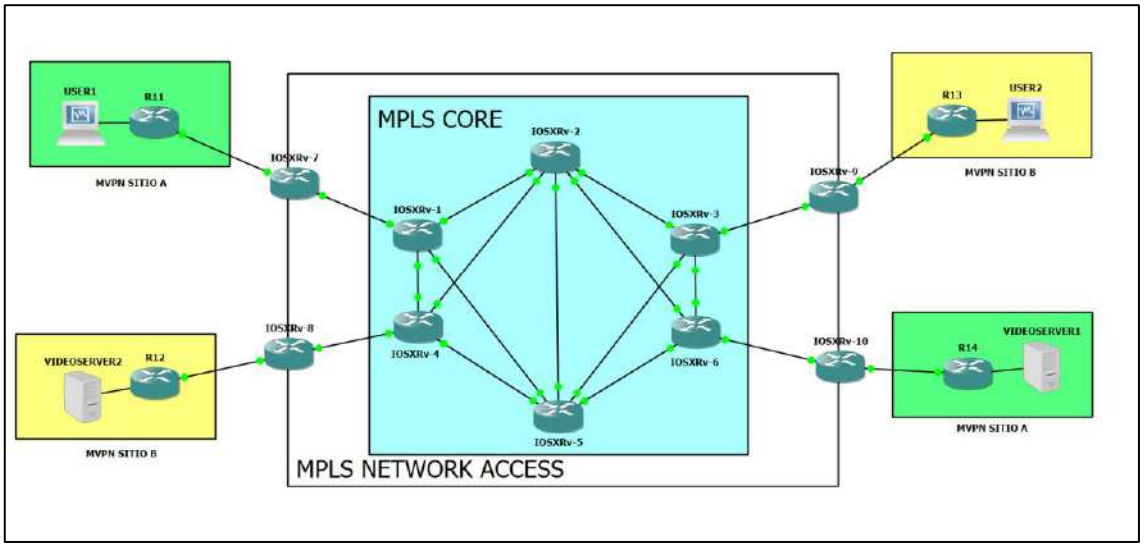


Ilustración 1-5*:* Escenario propuesto

Realizado por: Mafla, Carlos, 2022.

Para la realización del análisis de la tecnología VPN de siguiente generación en redes MPLS se propone la utilización de un escenario que permita evaluar su funcionamiento como también en donde se genere tráfico Multicast y Unicast para así permitir realizar la evaluación de parámetros de rendimiento de la red como: jitter, tasa de transferencia y paquetes perdidos, parámetros de consumo como: la cantidad procesamiento y memoria RAM en los servidores y routers. Se realizará un análisis de comportamientos de la red en diferentes prototipos, que presentan la variación de algunos parámetros como: tipos de transmisión, implementación de QoS y resolución de video transmitido.

Para la transmisión de video se utilizará el reproductor VLC que actuará como servidor, este emitirá la señal de video que será recibida en los nodos de los clientes, para su recepción en cada uno de los sitios receptores se utilizará el reproductor VLC. Se utilizará también para la generación de tráfico Unicast en el escenario planteado.

1.5. Objetivos

1.5.1. Objetivo general

Analizar la tecnología multicast VPN en redes MPLS para la transmisión de servicios de video streaming.

1.5.2. Objetivos específicos

- Analizar los protocolos que existen en la tecnología multicast VPN en redes MPLS para la transmisión de servicios de video streaming.
- Determinar los parámetros de rendimiento y QoS que afectan a la transmisión de servicios de video streaming en multicast VPN sobre redes MPLS.
- Diseñar el prototipo de pruebas de la tecnología multicast VPN en redes MPLS para la transmisión de servicios de video streaming.
- Evaluar el funcionamiento de la tecnología multicast VPN en redes MPLS para la transmisión de servicios de video streaming, mediante parámetros de latencia, calidad de servicio de video y consumo de ancho de banda.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. VPN

Es un entorno de comunicaciones en el que se controla la entrada de información y así se permite o niega el acceso entre dos puntos, los mismos que se encuentran dentro de una comunidad definida. Otra de las definiciones menciona que una VPN es una red en la que la conectividad del cliente entre múltiples sitios se implementa en una infraestructura compartida con las actividades de marketing y que es bien conocido y utilizado en el mercado de los proveedores de servicios (Pepelnjak, Guichard 2002, p. 126).

Una red privada virtual se puede definir como una red a través de la cual se interconectan sitios o puntos que se encuentran geográficamente dispersados mediante enlaces punto a punto a través de una infraestructura compartida. Para ello las redes privadas virtuales hacen uso de técnicas avanzadas de encriptación y tunneling permitiendo a las organizaciones seguridad extremo a extremo a través de una red pública como por ejemplo el Internet.

Los autores coinciden en que se trata de una tecnología de red privada que permite extender el dominio de la red local, hacia una red pública como el Internet o viceversa, como en el caso de algunos proveedores de servicios. Para lograr esto, se hace uso de técnicas avanzadas que permitan asegurar los datos transmitidos.

2.1.1. Clasificación de las VPN

Las VPN se pueden clasificar de distintas maneras, una de las clasificaciones más amplia se basa en la forma en que la información de enrutamiento se intercambia en la VPN, en esta clasificación se puede notar que existen dos modelos de VPN, una denominada igualitaria, en la cual la información de encamamiento del cliente se intercambia entre los routers de los clientes y los routers de los proveedores de servicios, y la otra denominada de superposición, en la que el proveedor de servicios proporciona solo líneas arrendadas lógicas y la información de enrutamiento se intercambia directamente entre los routers de borde (Pepelnjak, Guichard 2002, p. 152).

Otra de las clasificaciones comunes es aquella que se realiza con respecto a las formas en las que una organización puede implementar una VPN, en ésta se pueden encontrar VPN de firewall, VPN de router y de concentrador, VPN de sistema operativo, VPN de aplicación y VPN de

proveedor de servicios, cada una con características específicas que le permiten funcionar para cada uno de los ambientes en los que se encuentran implementadas (Gonzáles Morales 2006, p. 53). Tanto Pepelnjak y Gonzales coinciden en que las VPN se deben clasificar de acuerdo con la forma en que la red privada virtual maneja la información, la tecnología que usa y también que tipo de usuarios hacen uso de esta.

Las VPN de acuerdo con la tecnología que utilizan pueden clasificarse en:

- Overlay
- Peer-to-Peer
- VPN/MPLS

2.1.1.1. Tecnología VPN Overlay

Este tipo de proveedor de servicios VPN brinda servicios de red privada a los clientes a través de un circuito virtual establecido entre enrutadores centrales y, en este modelo, el proveedor de servicios no participa en el enrutamiento del cliente (Oña Piña, 2016, p. 33). Una de las topologías que se utiliza en overlay es la topología hub-and-spoke en la cual todos los lugares remotos son enlazados con un único circuito virtual al router central (Pepelnjak, Guichard 2002, p. 16).

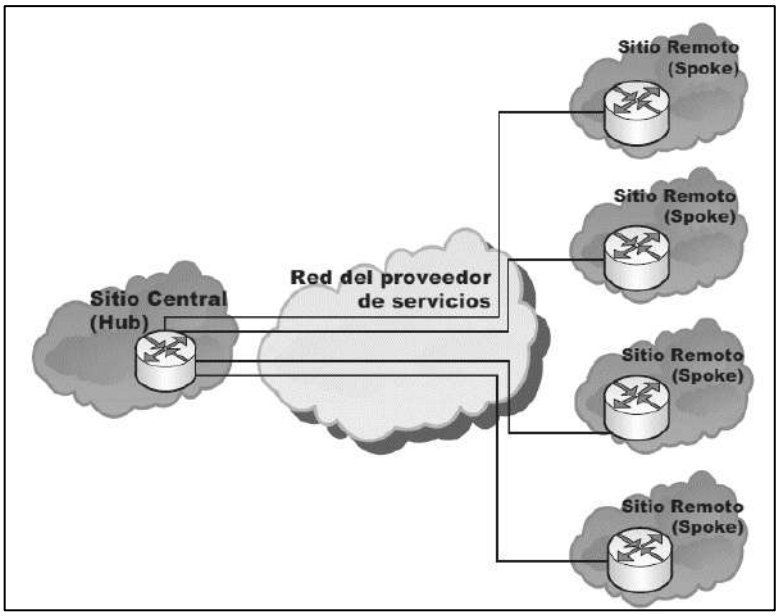


Ilustración 2-1: Representación VPN Overlay

Fuente: (Oña Piña, 2016).

En el presente trabajo se utiliza una topología híbrida, ya que en el escenario de estudio se encuentra implementado una topología hub-and-spoke y una de malla parcial.

2.1.1.2. Tecnología VPN Peer to Peer

La tecnología VPN Peer to Peer se creó para superar el problema de escalabilidad y brindar al cliente un transporte de datos óptimo a través del backbone del proveedor de servicios (Oña Piña 2016, p. 45). En la Ilustración 2-2 se puede observar que el proveedor de servicios es el que realiza el enrutamiento del cliente.

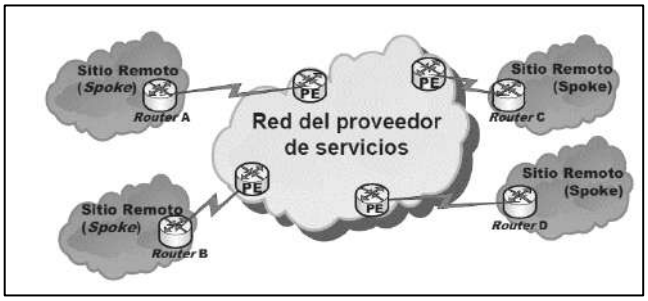


Ilustración 2-2: Representación VPN Peer-to-Peer

Fuente: (Oña Piña 2016).

Para crear las VPN Peer-to-Peer se utiliza una arquitectura en malla parcial en la que los clientes se encuentran aislados, por lo que sus datos corporativos están seguros (Pepelnjak, Guichard 2002, p. 48).

2.1.1.3. VPN MPLS

Las VPN MPLS son VPN similares a las Overlay y Peer-to-Peer, pero a diferencia de estas presentan ventajas extra como la posibilidad de implementación de transmisión Multicast y QoS, las redes de sus clientes son aprendidas por IGP en los que se puede utilizar OSPF, EIGRP, RIPv2 o rutas estáticas desde un cliente o a través de BGP desde otro routers backbone MPLS (Castillo et al. 2004, p. 67).

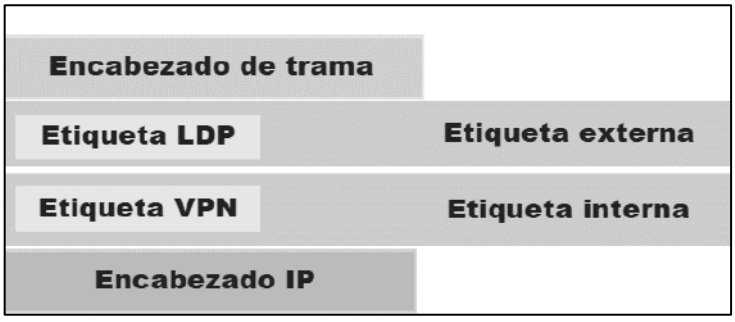


Ilustración 2-3: Representación del Stack de etiquetas para una VPN MPLS

Fuente: (Castillo et al. 2004)

La etiqueta superior del stack apunta al router de salida y utiliza LDP para enlazar los routers LSR que conmutan etiquetas de borde mediante un único túnel LSP. La segunda etiqueta identifica el interfaz de salida en el router de salida o identifica una tabla de enrutamiento donde realiza una búsqueda de enrutamiento y utiliza MP-BGP para propagar información de enrutamiento VPN y etiquetas que atraviesan el dominio (Oña Piña 2016, p. 63).

Se conocen también VPN de capa 3 o VPRN (Virtual Private Routed Network), y se caracteriza porque utiliza la capa 3 VRF (VPN / Virtual Routing and Forwarding) para realizar una tabla de de enrutamiento para cada cliente que ocupa el servicio. En la nube también es necesario el multi protocolo BGP para utilizar el servicio.

La topología VPN está directamente ligada a la función que ésta debe cumplir en cada organización y lo problemas que se requieren resolver (Gonzáles Morales 2006, p. 57). Pepelnjak coincide en que la topología de una VPN debe ser dictada por los problemas que la organización o negocio está tratando de resolver (Pepelnjak, Guichard 2002, p. 139).

2.1.2. Topología hub-and-spoke

Es la topología más común, la misma que presenta un concentrador al que se conectan las sucursales remotas para que puedan intercambiar información con el concentrador y también entre ellas, ya que no existen restricciones de seguridad explícitas (Pepelnjak, Guichard 2002, p. 140), Gonzales coincide con Pepelnjak en la definición de ésta topología, pero con el nombre de topología radial y hace énfasis en que los datos no se encuentran seguros debido a que los intercambios de información entre las sucursales siempre viajan a través del sitio central (Gonzáles Morales 2006, p. 57).

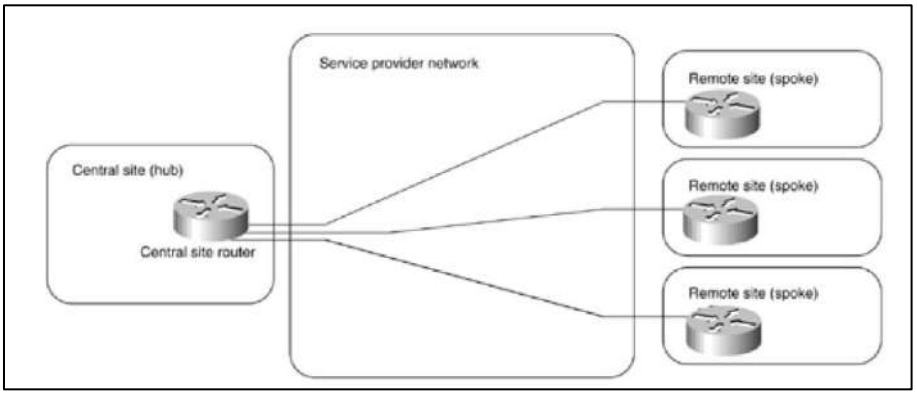


Ilustración 2-4: Representación de la topología hub and spoke

Fuente: (Pepelnjak, Guichard 2002).

2.1.2.1. Topología de malla completa o parcial

Es conocida gracias a su implementación en corporaciones que no tienen una estructura demasiado jerárquica, en esta topología las redes LAN de la compañía pueden realizar un intercambio constante de datos entre ellas (Gonzáles Morales 2006, p. 58). Se implementa también cuando la organización requiere intercambio entre los diversos puntos de la empresa y cuando las aplicaciones utilizadas en la organización necesitan una conexión punto a punto (Pepelnjak, Guichard 2002, p. 143).

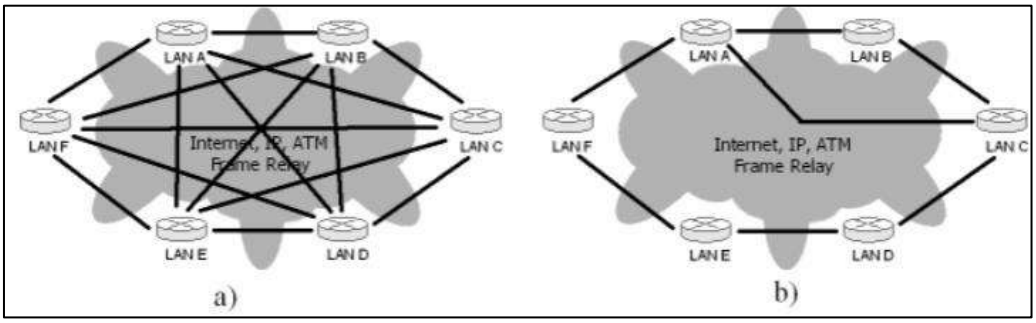


Ilustración 2-5: Representación de topologías de malla completa y parcial

Fuente: (Pepelnjak, Guichard 2002).

2.1.2.2. Topología hibrida

Aparecen cuando la VPN a implementarse es de gran tamaño, combinan las topologías hub-and-spoke y la topología de malla completa o parcial (Pepelnjak, Guichard 2002, p. 145)

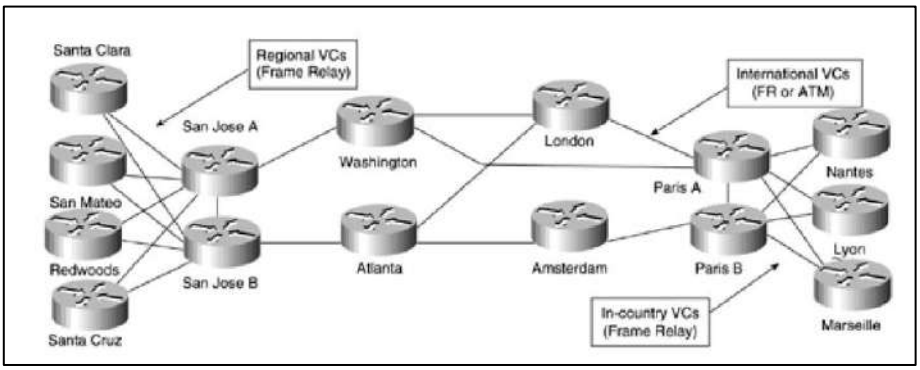


Ilustración 2-6: Representación de la topología híbrida

Fuente: (Pepelnjak, Guichard 2002).

En el presente trabajo se utiliza una topología híbrida, ya que en el escenario de estudio se encuentra implementado una topología hub-and-spoke y una de malla parcial.

2.1.2.3. Topología de acceso remoto

Consiste en un enlace punto a punto entre el usuario y la oficina remota utilizando tramas tunneling PPP intercambiadas entre el usuario remoto y el servidor VPN (Gonzáles Morales 2006, p. 59)

2.1.3. Protocolos utilizados en los VPN

2.1.3.1. Protocolo de túnel punto a punto

Es un protocolo de red que fue desarrollado por Microsoft, permite la realización de transferencias seguras entre clientes remotos y servidores en redes privadas haciendo uso de redes como el Internet (Gonzáles Morales 2006, p. 100). En la actualidad es considerado un protocolo de VPN un tanto obsoleto ya que no ofrece la seguridad que los usuarios requieren en la actualidad (Hamzeh et al. 1999).

2.1.3.2. Protocolo de Túnel de Capa 2 (L2TP)

Es un protocolo diseñado para transmitir datos y conectar de forma segura redes a través de Internet. Es soportado por la mayoría de los equipos en el mercado. Surgió de la fusión de las mejores características de los protocolos PPTP de Microsoft y L2F de Cisco (Gonzáles Morales 2006, p. 112). L2TP aísla las tramas PPP que van a ser enviadas en las redes IP. A pesar de ser un tanto más actual que PPTP no ofrece garantías en cuanto a la seguridad de la información que se transmite (Townsley, Pall 1999, p. 40).

2.1.3.3. Seguridad IP (IP Sec)

Una de las principales preocupaciones para cualquier persona que use cualquier VPN es la seguridad de sus datos cuando atraviesa la red, encriptar los datos es una forma de protegerlos. IP Sec es un conjunto de protocolos desarrollados bajo los auspicios de la IETF para lograr servicios seguros a través de redes de conmutación de paquetes IP (Bollapragada, Khalid, Wainner 2005, p. 23). IP Sec se basa en un modelo de seguridad completo, y establece la confianza y la seguridad desde una IP de origen hasta una IP de destino (Gonzáles Morales 2006, p. 125).

2.2. Métodos de transmisión de datos en redes de comunicación

2.2.1. Unicast

Ocurre cuando el envío de información se realiza desde un único emisor hacia un único receptor. Funciona de forma similar a un enlace punto a punto, tiene un efecto negativo sobre la red debido a que consume altos recursos del servidor por cada usuario que establezca comunicación (Audet et al. 2007, p. 7).

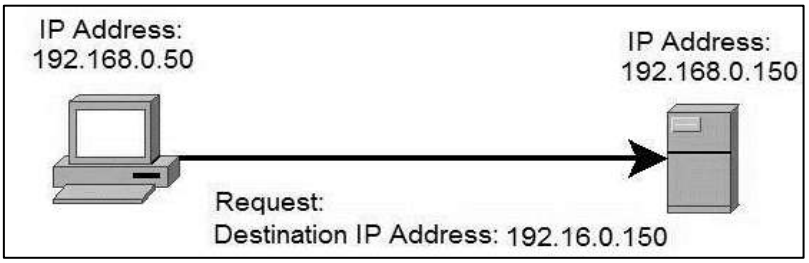


Ilustración 2-7: Representación de transmisión unicast

Fuente: (Audet et al. 2007).

2.2.2. Enrutamiento por difusión (Broadcasting)

En algunas aplicaciones, los usuarios necesitan enviar mensajes a varios o a todos los usuarios en la red. Son situaciones similares a las que ocurren cuando se realiza la distribución de informes sobre el clima, la actualización de los precios de la bolsa o la emisión de programas de radio en vivo, los mismos pueden funcionar mejor si se difunden a todas las máquinas para dejar que las personas interesadas acepten los datos. El envío simultáneo de un paquete a todos los destinos se conoce como broadcasting (Tanenbaum 2012, p. 327). Se trata de una transmisión en la que el contenido que es enviado hacia todos los puntos conectados al servidor.

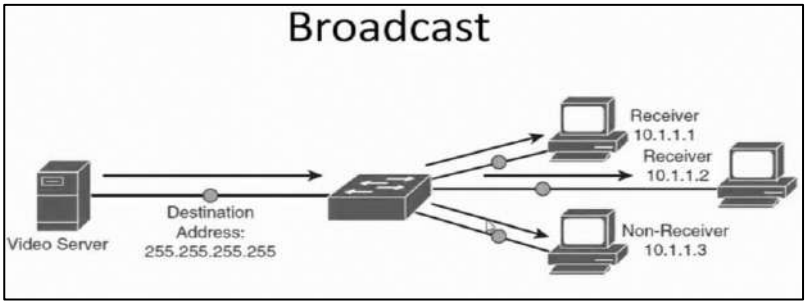


Ilustración 2-8: Representación de transmisión broadcast

Fuente: (Tanenbaum 2012).

2.2.3. Enrutamiento multidifusión (Multicast)

El proceso de enviar un mensaje a uno de tales grupos se denomina enrutamiento por multidifusión (Multicast), para esto se utiliza el algoritmo de enrutamiento por multidifusión, es decir se envían paquetes a través de árboles de expansión. La tecnología Multicast tiene como característica principal permitir una distribución eficiente de la información entre una sola fuente y múltiples receptores (Tanenbaum 2012, p. 329). El enrutamiento multidifusión es más eficiente que el enrutamiento por difusión ya que permite que el contenido enviado por el servidor llegue solo a los usuarios que lo solicitan.

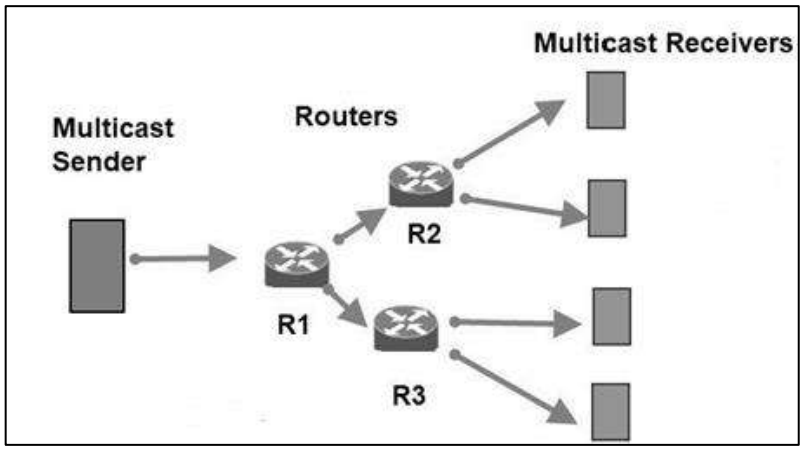


Ilustración 2-9: Representación de transmisión multicast

Fuente: (Tanenbaum 2012).

2.2.4. Enrutamiento anycast

Existe otro modelo de distribución llamado anycast, que algunas veces también es útil. En anycast, un paquete se entrega al miembro más cercano de un grupo (Tanenbaum 2012, p. 332).

En el presente estudio se utilizará enrutamiento multicast, ya que este presenta la ventaja de permitir enviar el mismo paquete hacia todos los destinos que lo soliciten, sin la necesidad de crear un paquete por cada destino, logrando un menor consumo de ancho de banda y recursos en cada uno de los equipos utilizados para la transmisión.

2.3. IP Multicast

2.3.1. Definición

Es una tecnología diseñada para reducir tráfico y a la vez entregar un solo stream de información a cientos o miles de clientes residenciales o corporativos. En la actualidad existen tres modos de transmisión: unicast, broadcast y multicast (Holbrook, Cain 2006).

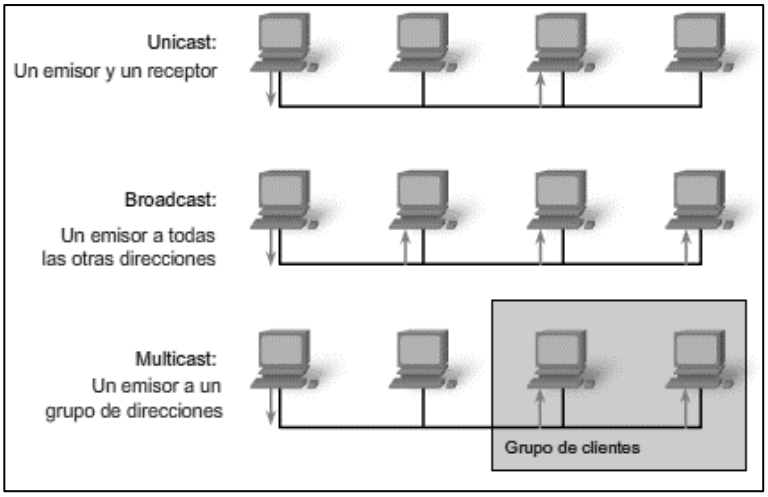


Ilustración 2-10: Representación de modos de transmisión de información

Fuente: (Holbrook, Cain 2006)

En comparación con IP unicast, IP multicast posee la capacidad de minimizar la carga de información en los hosts, tanto en el envío como en la recepción de información, reduciendo así el tráfico total de la red (Shabtay, Rodrig 2011, p. 77). En una red multicast, se utilizan routers para distribuir el contenido multicast a todos los hosts que pertenezcan a un grupo multicast en particular.

Para transmitir contenido multicast los routers usan la construcción de árboles de distribución mediante protocolos de enrutamiento multicast como PIM (Protocol Independent Multicast). A diferencia de las aplicaciones unicast que requieren que una fuente transmita una copia por cada receptor individual en el grupo (Fenner et al. 2006, p. 74).

2.3.2. Protocol Independent Multicas PIM

PIM es el protocolo multicast más desarrollado, usa la tabla de enrutamiento unicast para descubrir si el paquete multicast ha llegado a la interfaz correcta (Fenner et al. 2006, p. 87). En la actualidad se encuentran disponibles muchas variantes de PIM.x

2.3.2.1. Dense mode PIM DM

El modo denso de PIM supone que casi todas las subredes disponibles tienen al menos un receptor esperando recibir el tráfico multicast desde la fuente, por lo cual la red es inundada con el tráfico en todas las posibles ramas, luego estas ramas son cortadas cuando las ramas no expresan un interés en recibir los paquetes ya sea de en forma de un mensaje o cuando el tiempo se haya agotado (Fenner et al. 2006, p. 36). PIM DM permite a un dispositivo de enrutamiento usar cualquier protocolo de enrutamiento unicast y llevar a cabo chequeos RPF empleando la tabla de enrutamiento unicast (Adams, Nicholas, Siadak 2004, p. 58).

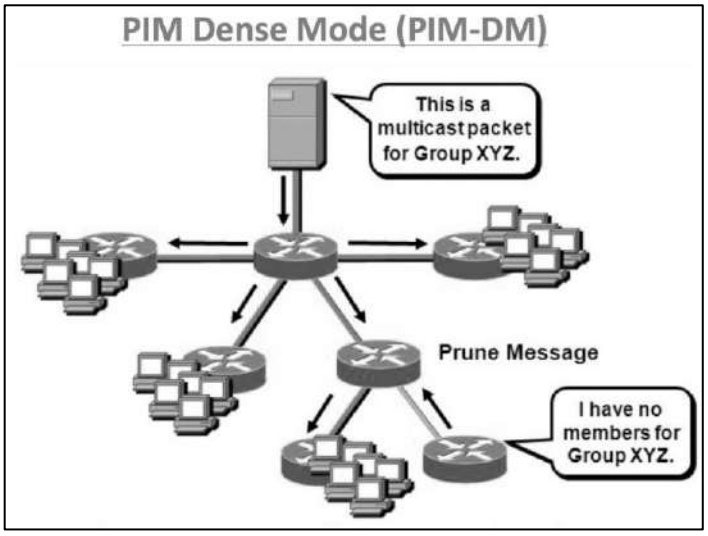


Ilustración 2-11: Representación de Multicast PIM Dense Mode

Fuente: (Fenner et al. 2006).

2.3.2.2. Sparse mode PIM DM

El modo sparse de PIM utiliza el modelo explícito de unión y juntura, donde sólo los routers con receptores activos se unirán a grupos multicast. La suposición que se tiene de este modo es que muy pocos de los posibles receptores desean los paquetes multicast de cada fuente, por lo que la red establece y envía paquetes sólo a las ramas que tienen al menos una hoja que indique por mensaje su interés en el tráfico (Fenner et al. 2006, p. 65).

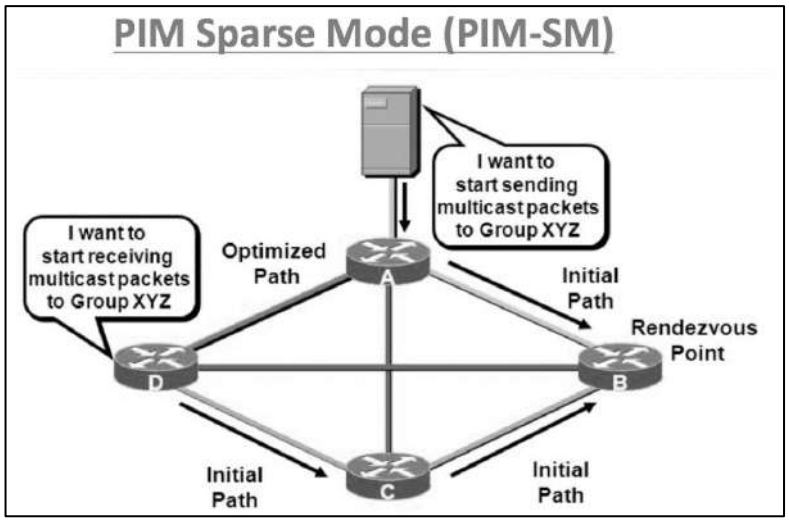


Ilustración 2-12: Representación de Multicast PIM Sparse Mode

Fuente: (Fenner et al. 2006).

2.3.2.3. PIM Multicast fuente especifica (PIM-SSM)

PIM SSM es una variación en modo disperso. Destinado a un modelo de reenvío de uno a muchos, en donde sólo se hace envío hacia adelante basándonos en rutas de árboles en la fuente (Adams, Nicholas, Siadak 2004, p. 90). Esto nos brinda varias ventajas, como el direccionamiento único a nivel mundial, la eliminación del RP y las entradas de reenvío de árbol compartido, y también para la multidifusión entre dominios.

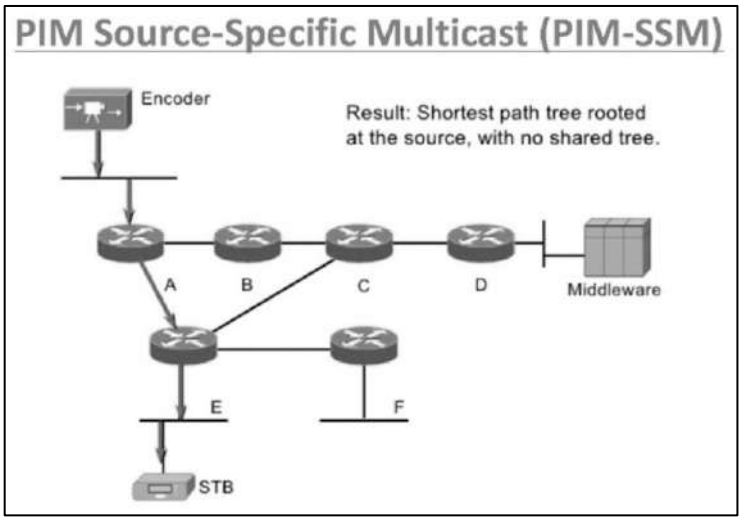


Ilustración 2-13: Representación de Multicast PIM Source Specific Mode

Fuente: (Fenner et al. 2006)

2.3.2.4. PIM Bidireccional PIM BiDir

El PIM Bidireccional PIM BiDir es una variación de PIM, en la cual se construye árboles compartidos bidireccionales que están enraizados en una dirección RP. El tráfico bidireccional no conmuta a árboles de camino más corto como PIM SM y es por tanto óptimo para el tamaño de los estados de enrutamiento en lugar de la longitud de camino. Es considerado una variación del modo disperso y lo opuesto a SSM. Por lo tanto, BiDir está destinado principalmente para muchas aplicaciones con un gran número de fuentes en donde se reenvía todo el tráfico basado solo en el árbol compartido, que está enraizado en el RP (Fenner et al. 2006, p. 45).

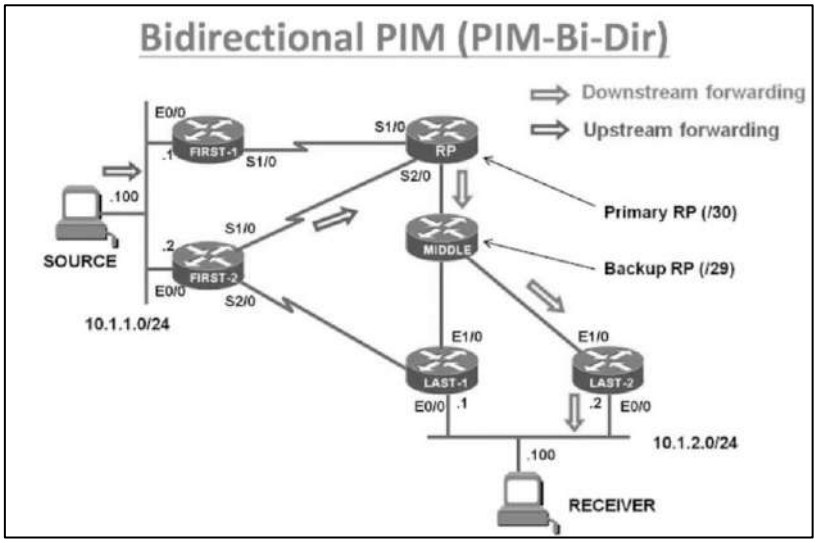


Ilustración 2-14: Representación de Multicast PIM Bidirectional Mode

Fuente: (Fenner et al. 2006)

2.4. Multiprotocol Label Switching MPLS

2.4.1. Definición

La conmutación de etiquetas multiprotocolo (MPLS) ha revolucionado redes de proveedores de servicios en los últimos años como la tecnología que permite la eficacia en la explotación multiservicio de un paquete conmutado. La conmutación de etiquetas multiprotocolo fue creada por la IETF y es un mecanismo de transporte de datos estándar que se encuentra definido en el RFC 3031. (Garcia 2008, p. 97). MPLS opera entre la capa de enlace de datos y la capa de red del modelo OSI y está diseñado para simplificar la forma en que las redes basadas en circuitos y las basadas en paquetes conviven. MPLS puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP (Castro Ullauri 2015, p.86). MPLS reduce el procesamiento de paquetes debido a que cuando un paquete ingresa a un router de la red, este es

señalizado con las etiquetas propias de la tecnología permitiendo el mejor desempeño de la red y los dispositivos que la conforman. Dentro de los principales beneficios que ofrece MPLS están el Soporte de Calidad sobre servicio (QoS), Ingeniería de Tráfico (TE), soporte para redes virtuales (VPNs) y soporte multiprotocolo (Dibildox 2006, p. 36).

2.4.1.1. Etiqueta MPLS

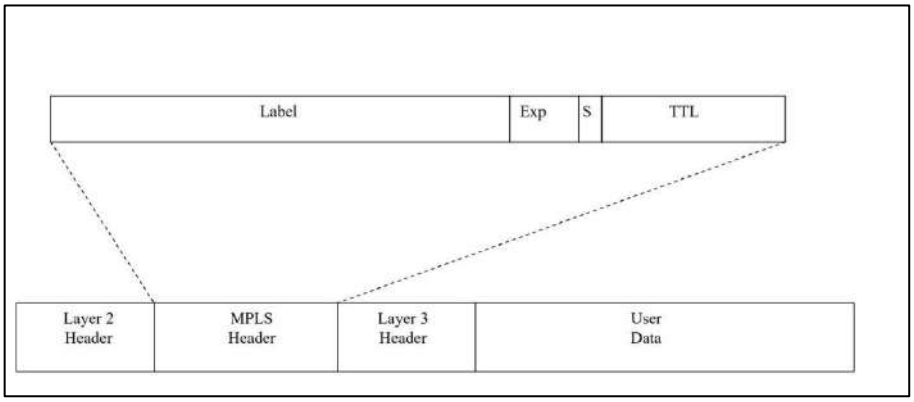


Ilustración 2-15: Componentes de la etiqueta MPLS

Fuente: (Ruela, Ricardo 2005)

En la Ilustración 15-1 se observa los componentes de la etiqueta MPLS, la misma que tiene un tamaño de 4 bytes y presenta 4 campos: Label, Exp, S, TTL, los mismos que se describen a continuación.

Tabla 2-1: Componentes de la etiqueta MPLS

Nombre	Tamaño	Descripción
Label	20 bits	Almacena el valor de la etiqueta, los valores del 0 a 15 se encuentran reservados.
EXP	3bits	Campo experimental, no se encuentra definido en ningún RFC, es utilizado por las empresas Cisco, Juniper y Huawei para definir una clase de servicio.
S	1 bit	Determina si la etiqueta en la que se encuentra es la última etiqueta en el paquete. Si se encuentra en (1), este valor indica que ésta es la última etiqueta.
TTL	8 bits	Tiempo de vida, funciona como un contador que descuenta una unidad conforme la etiqueta viaje en el datagrama MPLS, funciona de manera similar al campo TTL de la cabecera IP.

Fuente: MAFLA, 2021

Realizado por: Mafla, Carlos, 2022.

2.4.2. Arquitectura MPLS

MPLS es una solución para la conmutación multiprotocolo que presenta características como la introducción a una estructura orientada a la conexión en redes que originariamente no estaban orientadas a la conexión, integra también sin discontinuidades los niveles 2 y 3 del modelo OSI, esto permite que las funciones de control y las de enrutamiento estén conmutadas. MPLS permite también que la complejidad de los algoritmos disminuya debido a su asignación de etiquetas propias, esto contribuye a que la comunicación entre los nodos sea más optimizada. Entre sus características más importantes también se encuentran permitir introducir QoS en redes IP y optimizar el establecimiento de túneles en las VPN. (Pepelnjak, Guichard 2002, p. 258).

2.4.3. Componentes de la arquitectura MPLS

- Plano de control
- Plano de datos

2.4.3.1. Plano de control

El Plano de control de MPLS se encarga del intercambio de información de enrutamiento y de intercambio de etiquetas entre los dispositivos que se encuentran contiguos (Oña Piña 2016, p. 40).

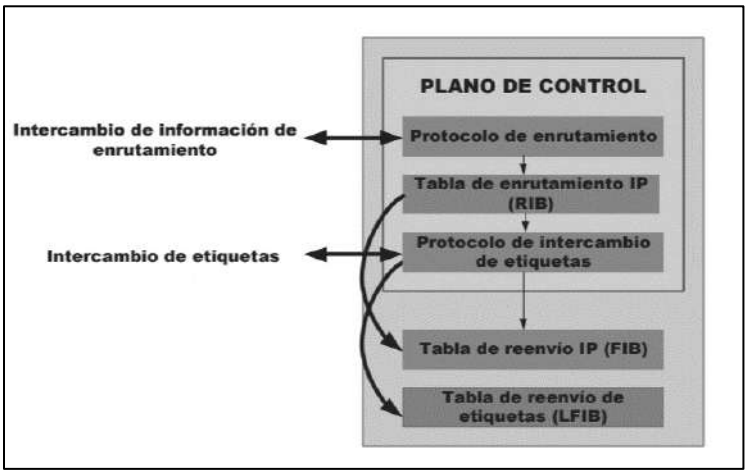


Ilustración 2-16: Representación del Plano de control MPLS

Fuente: (Oña Piña 2016)

El Plano de Control construye una tabla de enrutamiento RIB que se encuentra basada en protocolos de enrutamiento tales como: OSPF, IGRP, EIGRP, IS-IS, RIP, BGP, para la gestión de enrutamiento de capa 3. Utiliza también un protocolo de intercambio de etiquetas que sirve

para crear, mantener e intercambiar las etiquetas internas con otros dispositivos (Rosen, Aggarwal 2012, p. 56). El protocolo de intercambio permite que las etiquetas se unan a las redes aprendidas por medio de un protocolo de enrutamiento. Los protocolos de intercambio de etiquetas pueden ser: LDP, TDP, BGP (usado en VPN MPLS) y RSVP (usado por TE MPLS). El Plano de Control permite también que se construyan dos tablas de reenvío utilizadas por el Plano de Datos (Oña Piña, 2016, p. 17).

Una FIB basada en la información de la RIB, y una tabla LFIB basada en el protocolo de intercambio de etiquetas y en la información de la RIB (Román Vallejo 2011, p. 41), la misma que incluye valores de etiqueta y asociaciones con la interfaz de sal ida para cada prefijo de red.

2.4.3.2. Plano de datos

El Plano de Datos es también conocido como Plano de Reenvío y se encarga de conmutar los paquetes, independientemente del protocolo de enrutamiento o del protocolo de intercambio de etiquetas que se está utilizando (Oña Piña 2016, p. 41). Se encarga de enviar los paquetes de la interfaz correspondiente basándose en la información que encuentra en las tablas LFIB y FIB.

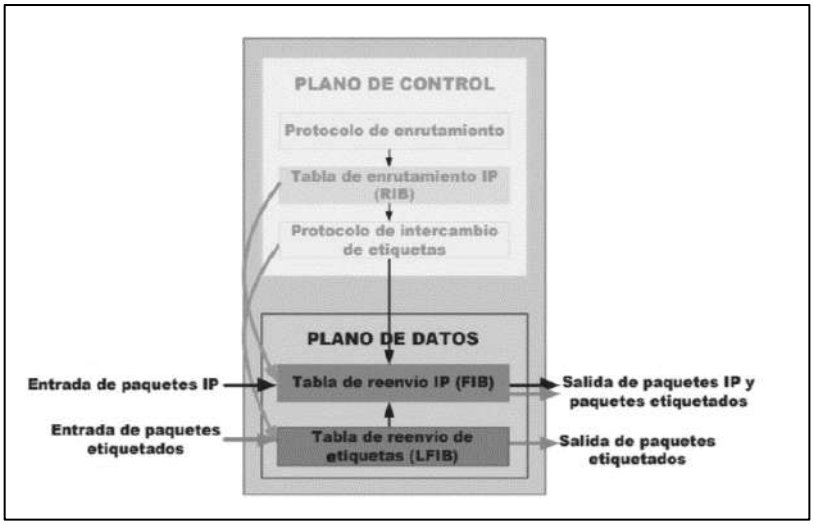


Ilustración 2-17: Representación del Plano de datos MPLS

Fuente: (Oña Piña 2016)

2.4.4. Dispositivos de MPLS

Son los que realizan la conmutación de etiquetas y el enrutamiento IP, sus nombres representan la posición que ocupan en el dominio MPLS (Oña Piña 2016, p. 42).

- LSR
- EDGE LSR

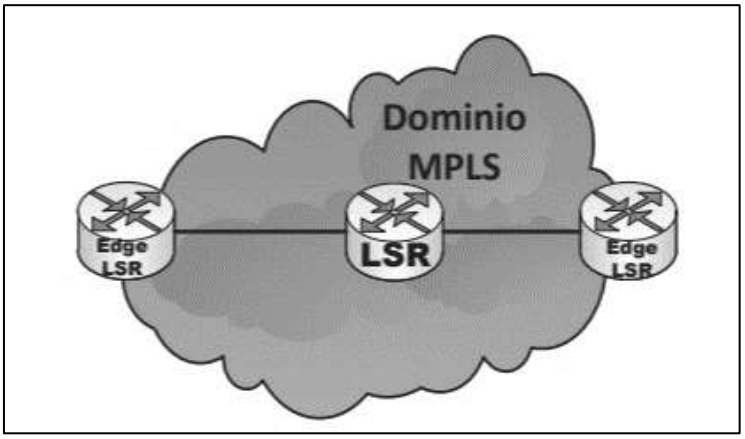


Ilustración 2-18: Representación de los Dispositivos LSR en MPLS

Fuente: (Oña Piña 2016)

2.4.4.1. LSR

Es el dispositivo que realiza la distribución de etiquetas y sus interfaces están habilitadas solo para el dominio MPLS, se encuentran orientados a la conmutación de etiquetas de los paquetes (Oña Piña 2016, p. 74). Cuando un paquete ingresa al dispositivo LSR la última etiqueta del paquete se utiliza para determinar su próximo salto.

Cada dispositivo LSR necesita de un protocolo de enrutamiento y de un protocolo de intercambio de etiquetas como LDP o TPD. El protocolo LDP permite publicar la tabla LFIB en el plano de datos, la misma que es usada para intercambiar paquetes etiquetados, un dispositivo LSR no puede reenviar paquetes que no estén etiquetados (Castillo et al. 2004, p. 24).

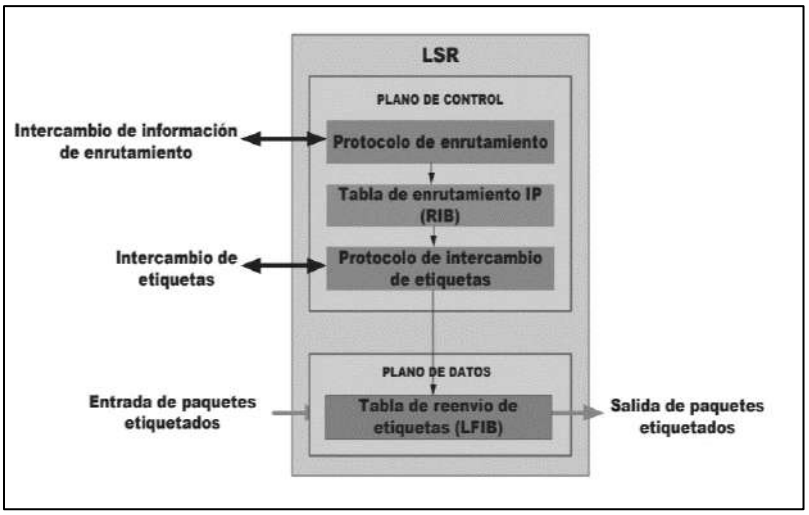


Ilustración 2-19: Representación de la Arquitectura LSR

Fuente: (Oña Piña 2016).

2.4.4.2. Edge LSR

Son dispositivos que se encuentran ubicados en la frontera del dominio MPLS (Oña Piña, 2016, p. 43), se caracterizan por poseer algunas interfaces que no están habilitadas para MPLS. Sus funciones son la distribución, inserción y extracción de etiquetas en los paquetes recibidos (Castillo et al. 2004, p. 19). Estos paquetes son reenviados dentro del dominio MPLS a través de las interfaces que han sido habilitadas para MPLS basándose en etiquetas y fuera del dominio MPLS basándose en direcciones IP de destino (Oña Piña, 2016, p. 43).

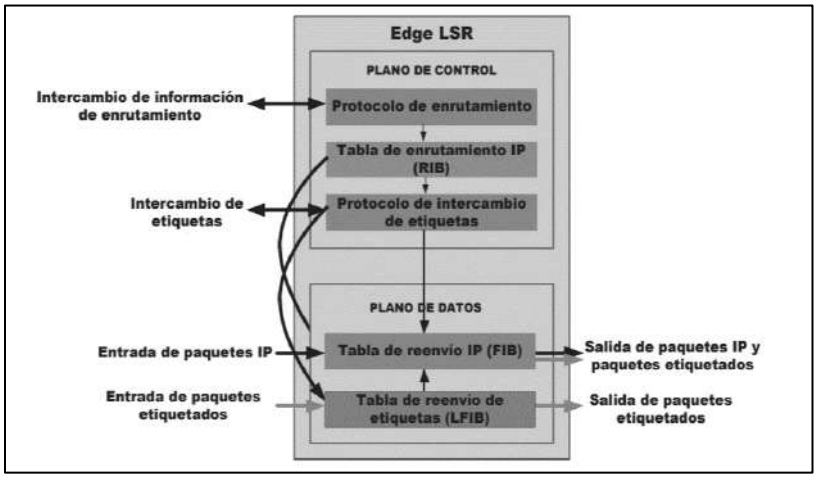


Ilustración 2-20: Representación de la Arquitectura Edge LSR

Fuente: (Oña Piña 2016).

2.4.5. MPLS VPNs

MPLS permite que el tráfico de una red privada atraviese la Internet de manera eficaz y transparente para el usuario (Dibildox 2006, p. 33), logrando así que no intervenga ningún tráfico externo y que la información que el usuario envía se mantenga segura. MPLS permite que paquetes enviados a través de túneles privados se encuentren señalizados por etiquetas que actúan como identificadores.

Las ventajas principales de implementar VPN en MPLS son: (Dibildox 2006, p. 34)

- Maximizar la capacidad de ampliación.
- Actualización transparente para el usuario.
- Uso óptimo de la red y sus recursos.
- Reducción de costos mediante consolidación de servicios.
- Seguridad y rapidez en la transferencia de información.
- Uso de tecnología de vanguardia.

2.4.5.1. Esquema VPNs MPLS

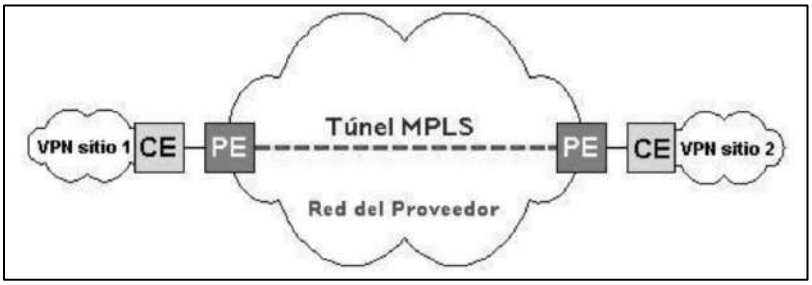


Ilustración 2-21: Esquema de una VPN MPLS

Fuente: (Dibildox 2006)

Una VPN MPLS se presenta como un canal privado que atraviesa una red conformada por los routers P; que son routers internos pertenecientes al proveedor, routers PE; que son routers de frontera del proveedor y routers CE; que son routers de frontera del cliente que solicita el servicio, como se muestra en la Ilustración 2-21. Cada VPN está asociada a una o más instancias de reenvío virtuales (VRF), dicha VRF muestra la relación que existe entre el router del cliente CE conectados al router PE de la compañía de servicio. Para prevenir que no salga ni ingrese información a la VPN cada sitio puede estar suscrito a varias VPN, pero sólo a un VRF. (Dibildox 2006, p. 18)

2.4.5.2. Servicio VPN de Capa 3

Este servicio permite prescindir de las conexiones punto a punto, ya que a diferencia de los servicios de VPN FR y ATM las VPN de Capa 3 no son orientadas a conexión.

La escalabilidad es una de las principales ventajas al utilizar VPN de Capa 3 ya que entre los enrutadores PE y CE no existe intercambio de paquetes etiquetados permitiendo así que la infraestructura del cliente no necesite ser cambiada.

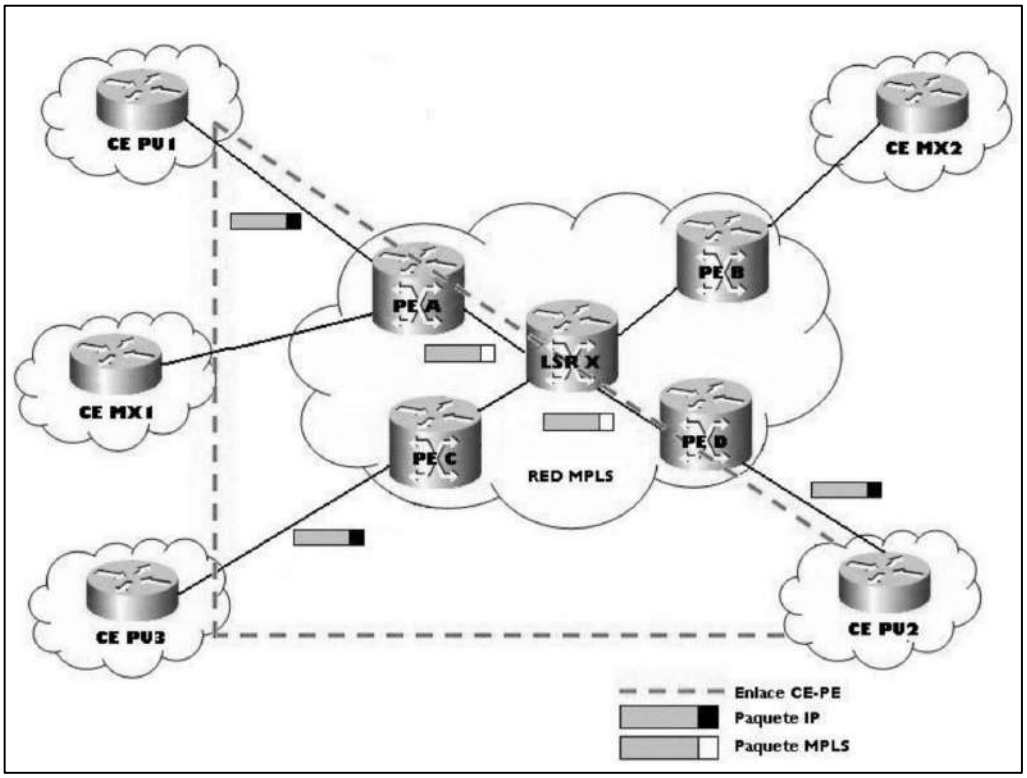


Ilustración 2-22: Arquitectura MPLS-VPN

Fuente: (Dibildox 2006)

En la Ilustración. 2-22 se muestra que los routers PU1, PU2 y PU3 sólo pueden enviar tráfico a otros routers PU, MPLS permite que los enlaces CE-PE se encuentren optimizados.

El uso del protocolo BGP es obligatorio en redes MPLS-VPN (Saxena et al. 2010, p. 28), ya que este protocolo se encarga del intercambio de prefijos y etiquetas entre dispositivos.

2.4.6. MPLS-TE

Es una de las prestaciones más importantes de MPLS, ya que permite el cálculo y la configuración de caminos a través de la red, con el fin de utilizar de manera efectiva el ancho de banda disponible (Dibildox 2006, p. 39).

Uno de los problemas que la ingeniería de tráfico en MPLS busca resolver es la congestión de enlaces; la misma que se da cuando rutas son utilizadas de manera excesiva produciendo congestión en la red.

Las VPN MPLS y TE resuelven problemas como la congestión de enlaces mediante la creación de túneles privados que atraviesan el núcleo MPLS. La ingeniería de tráfico permite reservar el ancho de banda para cada túnel en cada LSR (Dibildox 2006, p. 39).

2.5. BGP (Border Gateway Protocol)

BGP es un protocolo de enrutamiento usado para intercambiar información de enrutamiento entre diferentes redes funciona sobre TCP sobre el puerto 179, teniendo la principal característica el intercambio de paquetes IP entre distintos sistemas autónomos, BGP es un protocolo de vector de trayectoria que va teniendo actualizaciones incrementales además de soportar enrutamiento inter dominio sin clases Para ello, es necesario intercambiar dinámicamente prefijos de enrutamiento entre diferentes AS, lo que se realiza mediante el establecimiento de sesiones BGP entre AS mediante conexiones TCP. Este tipo de operación proporciona comunicación fiable y esconde todos los detalles de la red por la que se pasa (BiBing 2018, p. 28).

Un sistema autónomo es necesario para controlar la expansión de las tablas de enrutamiento, proveen una vista más estructurada del internet, segregan dominios de enrutamiento en grupos administrativos bien definidos con sus propias políticas de enrutamiento e IGPs, estos sistemas autónomos se representan con números (LACNIC XII 2016, p. 14)

2.5.1. Sesiones BGP

Solo dos enrutadores participan en una sesión BGP. Además de las sesiones entre dominios, los enrutadores fronterizos en el mismo sistema autónomo deben intercambiar información BGP para aprender las mismas rutas externas e internas. Esta regla de limitación para renunciar prefijos entre routers vecinos mediante I-BGP sirve para evitar bucles dentro de un AS. Debido a que no se puede volver a anunciar prefijos entre routers I-BGP, es necesario que exista conectividad entre

todos los routers vecinos que se comuniquen mediante IBGP dentro de un mismo AS, por lo que se utiliza un mallado total entre éstos (BiBing 2018, p. 25).

Entonces, otra diferencia es que los vecinos I-BGP no tienen que estar conectados directamente como E-BGP.

2.5.2. Mensajes BGP

Los tamaños de los mensajes oscilan entre 19 y 4096 octetos, y los mensajes se pueden enviar de forma segura mediante una función hash MD5. El encabezado es común a todos los mensajes y consta de una etiqueta (16 octetos) que contiene información de sincronización y seguridad, un campo de longitud (2 octetos) que indica la longitud total del mensaje y un campo de tipo (1 octeto) que representa el tipo de mensaje mensaje.

Existen 4 tipos de mensajes

2.5.2.1. Open

Este es el primer mensaje enviado después de establecer una conexión TCP. Su función es informar a los vecinos sobre la versión del protocolo BGP, el número AS y el identificador del proceso BGP. Además, el mensaje contiene un valor de cuánto tiempo se debe mantener la sesión (normalmente 90 segundos). Si se indica el valor 0 significa que la sesión no va a tener límite de duración. Una vez que se envía este mensaje, el proceso BGP se queda en espera de recibir un mensaje KEEPALIVE (BiBing 2018, p. 69).

2.5.2.2. Keepalive

Este mensaje se utiliza como reconocimiento del mensaje OPEN. Si la sesión está cronometrada, el proceso BGP debe enviar este mensaje periódicamente (normalmente cada 30 segundos) para indicar que se mantiene la sesión. De este modo, en el caso de que no haya modificación de la tabla de encaminamiento, los routers BGP sólo intercambian este tipo de mensaje de forma periódica, lo cual genera un tráfico de unos 5bits/s en el nivel BGP (cada mensaje tiene un tamaño mínimo de unos 19 octetos) (Universidad Politecnica de Navarra 2016, p. 85).

2.5.2.3. Notification

Este mensaje se usa para cerrar la sesión BGP y al mismo tiempo cerrar la conexión TCP. Además, se envía un código para indicar si hubo errores, como por ejemplo la recepción de un mensaje incorrecto, un problema del proceso BGP o la ausencia de mensajes KEEPALIVE durante 90 segundos (hello time). La consecuencia del cierre de la sesión BGP es la anulación de todas las rutas aprendidas en dicha sesión (Universidad Politecnica de Navarra 2016, p. 86).

2.5.2.4. Update

Este mensaje se utiliza para intercambiar información de enrutamiento, como la ruta que se eliminará, el conjunto de atributos para cada ruta, el prefijo de red disponible (longitud de red y máscara) o NLRI (información de accesibilidad de la capa de red) e información de longitud de red. Este mensaje se envía solo cuando se ha producido un cambio y su recepción activa el proceso BGP, que luego es responsable de transmitir los cambios relevantes a la tabla RIB y luego los mensajes de actualización a otros vecinos (BiBing 2018, p. 29).

2.5.3. Atributos BGP

Los atributos BGP se describen en RFC 1771. Tenemos 4 tipos:

Well-Known Mandatory: debe ser compatible con todas las implementaciones de BGP e incluirse en todas las actualizaciones de BGP.

Well-Known Discretionary: debe estar soportado en todas las implementaciones de BGP pero no tiene por qué estar incluido en todos los "updates" (actualizaciones) de BGP.

Optional Transitive: Esto no es necesario en la implementación de BGP, pero si está presente, debe pasarse sin cambios a todos los pares de BGP.

Optional Nontransitive: no es requerido en las implementaciones de BGP. Si se pasa un comando, pero no se acepta, no se pasará a los pares BGP (Romero 2016, p. 26).

BGP Attributes	
Name	**Type**
AS Path	Well-known mandatory
Local Preference	Well-known discretionary
MED	Optional nontransitive
Origin	Well-known mandatory
Next Hop	Well-known mandatory
Community	Optional transitive
Aggregator	Optional transitive
Atomic Aggregator	Well-known discretionary
Cluster List	Optional nontransitive
Originator ID	Optional nontransitive

Ilustración 2-23: Atributos BGP

Fuente: (Romero, 2016)

2.5.4. Router reflector

El concepto de route reflector se ha desarrollado para abordar el problema de escalabilidad de las sesiones iBGP de malla completa. La idea es bastante simple: hacer que uno o más altavoces iBGP actúen como enrutadores de concentración, comúnmente conocidos como route reflectors.

La introducción de route reflectors crea una jerarquía entre los altavoces iBGP agrupando un subconjunto de altavoces iBGP con cada route reflector. Los altavoces iBGP asociados con un route reflector en un grupo se denominan clientes reflector de ruta; Los hablantes de iBGP que no son clientes del mismo nivel se denominan no clientes. Tenga en cuenta que un cliente no es consciente de que está hablando con un reflector de ruta y asume que es como una configuración de malla completa (Deep Medhi 2018, p. 47).

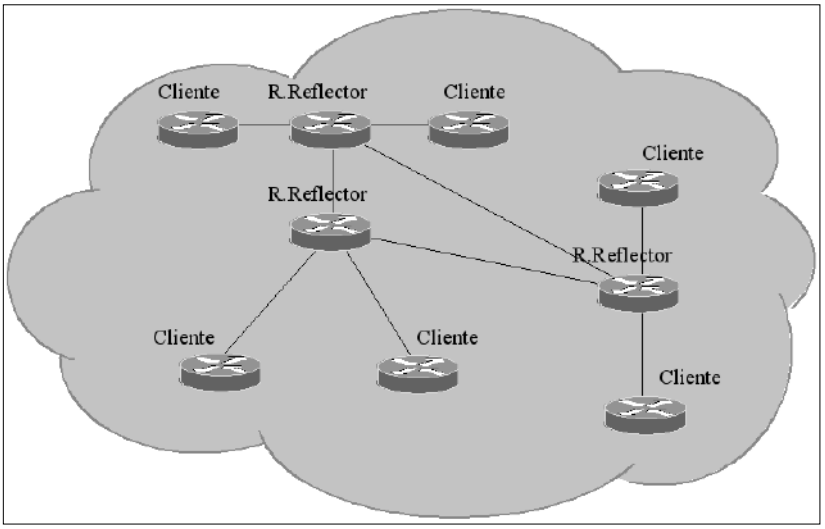


Ilustración 2- 24: Ilustración Route Reflector

Fuente: (Deep Medhi 2018)

2.5.5. Split horizon

Split Horizon es una técnica combinada con protocolos de enrutamiento de vector de distancia para evitar bucles de enrutamiento al evitar que las rutas enrutadas se envíen o anuncien de nuevo a los nodos que anuncian enrutadores. La técnica de horizonte dividido reenvía paquetes y los distribuye a todos los nodos conectados excepto al enrutador que envía la nueva actualización. Esta técnica puede evitar bucles de enrutamiento y también puede sublimar regiones donde el envenenamiento de rutas no puede evitar que ocurran bucles de enrutamiento. Esta técnica está integrada en la mayoría de los protocolos de enrutamiento por vector de distancia, incluidos RIP, IGRP, EIGRP y VPLS (Orozco 2018, p. 101)

2.5.6. BGP en MPLS

BGP (Border Gateway Protocol) es un protocolo utilizado para conectar diferentes sistemas autónomos, es el responsable de que Internet exista. La función principal de un sistema BGP es intercambiar información de accesibilidad con otros sistemas BGP en la red. Esta información de disponibilidad de la red incluye información sobre la ruta completa que debe tomar el tráfico para llegar a los sistemas autónomos de estas redes (Monte de Oca, Pantelis 2009, p. 27). Esta información es suficiente para construir un gráfico de conectividad de AS, bucles de enrutamiento que se pueden eliminar y algunas políticas de decisión de enrutamiento a nivel de AS que se pueden implementar.

Las comunidades BGP en MPLS se encargan de la distribución de información de la red de paquetes cognoscitiva (Dibildox 2006, p. 29), cuando una nueva ruta VPN ingresa a un router CE es añadida también al protocolo BGP.

Los routers PE en una red MPLS pueden obtener el prefijo IP de los routers CE por configuración estática, esto se puede ser mediante una sesión BGP con el router CE (Dibildox 2006, p .32).

BGP es el encargado de la propagación de la información de capacidad de alcance, mediante las extensiones multiprotocolo BGP, también es el encargado de realizar la distribución de la información de capacidad de alcance a los prefijos VPN, cuando esta distribución se lleva a cabo dentro del dominio IP se denomina BGP interno (IBGP) el mismo que se da por sesiones PE-PE, cuando se lleva a cabo fuera de los dominios IP se denomina BGP externo (eBGP) por medio de sesiones PE-CE (Rosen, Aggarwal 2012, p. 74).

2.6. VPN Multicast

2.6.1. Nociones de MVPN

Se define como un servicio de BGP / MPLS IP VPN que soporta multidifusión y que se establece entre los sitios remitentes y los sitios receptores (Rosen, Aggarwal 2012, p. 10). También se conoce como la aplicación de protocolos de multidifusión y técnicas de túnel VPN para lograr una alta calidad de servicio para el transporte de medios en tiempo real a través de redes IP (Lehmann Jr, Dye 2013, p. 1). Estos conceptos permiten comprender que el objetivo de la tecnología VPN Multicast "MVPN", es permitir que tráfico IP sea transportado a través de una VPN utilizando multidifusión.

2.6.2. Arquitectura MVPN

Previo a la implementación de un perfil Multicast VPN es necesario conocer los componentes básicos de los mismos, identificar si pertenecen a Multicast VPN clásica o Multicast VPN de siguiente generación y así ofrecer una orientación clara, para la utilización de un perfil MVPN determinado. Los componentes que conforman una MVPN son:

2.6.2.1. Planos Base, Planes Underlay, Underlay Signaling

En el plano de core se encuentran los árboles centrales, los mismos que pueden ser de 4 tipos:

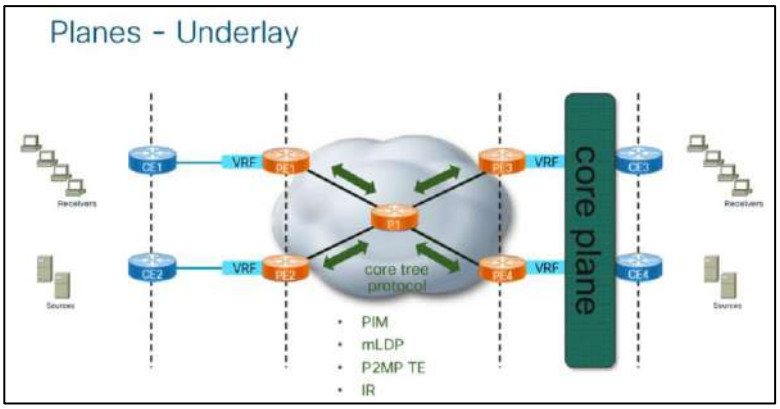


Ilustración 2-25: Planes - Underlay

Fuente:(Ghein 2019).

- PIM

Es el más conocido, pero uno de los más complejos, para su implementación es necesario recordar conceptos cómo PIM SSM, PIM Modo disperso, PIM Bidir y cómo estos funcionan en un árbol central, fue utilizado para el modelo predeterminado Rosen y se caracteriza por realizar replicación en los routers centrales del escenario en que se utiliza.

- mLDP

Es un tipo de señalización presente en MPLS, se conoce como una etiqueta LDP multipunto ya que aprovecha las etiquetas de MPLS para nutrir de extensiones adicionales al paquete que va a ser enviado. Presenta beneficios de la tecnología MPLS tales como: protección gracias a la ingeniería de tráfico de MPLS y a LFA que es un mecanismo mediante el cual el tráfico fluye temporalmente si uno de los enlaces falla. Presenta replicación de mcast en los enrutadores principales.

Ilustración 2-26: Etiqueta mLDP

Fuente:(Ghein 2019)

- TE P2MP

Este tipo de señalización ofrece un enrutamiento explícito desde la fuente mediante la creación de túneles, reserva de ancho de banda y protección FRR (Recuperación rápida del tráfico en caso

de fallas). Utiliza el protocolo RSVP que permite la reserva de recursos para realizar ingeniería de tráfico. Realiza replicación de multidifusión en los enrutadores centrales.

- IR

Esta señalización no presenta replicación de multidifusión en los enrutadores centrales, se reutilizan rutas conmutadas de etiquetas LSP MPLS de unidifusión, por lo general es usado cuando los enrutadores no entienden P2MP TE, mLDP u otros problemas de interoperabilidad. Los paquetes poseen una etiqueta MPLS adicional para que se pueda diferenciar el tráfico de unidifusión frente al de multidifusión y es necesario la distancia administrativa BGP para transportar la etiqueta mVPN MPLS.

2.6.2.2. Superposición de señalización, Overlay Signaling

En el plano de VPN se encuentran la señalización de superposición entre los routers PE-CE, los mismos que pueden ser de 2 tipos:

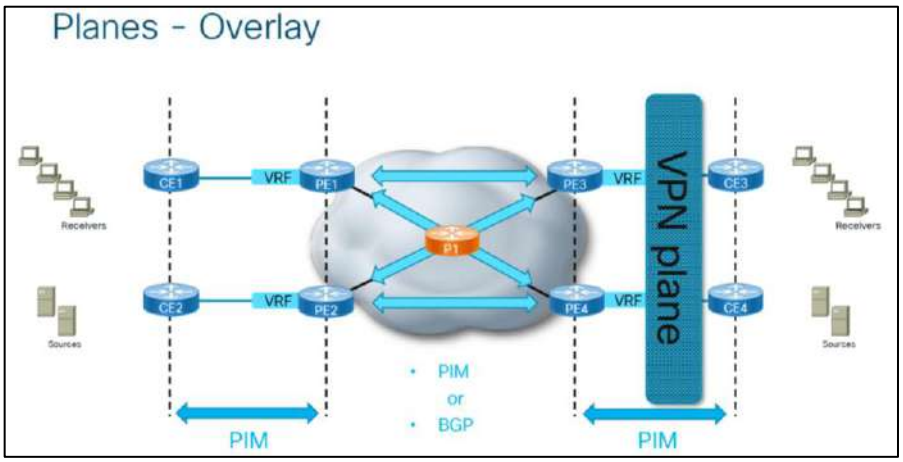


Ilustración 2- 27: Planes - Overlay

Fuente:(Ghein 2019)

- PIM

Al ser el más antiguo y más conocido es de mayor utilización a pesar de su complejidad, uno de sus beneficios es que presenta actualización periódica. La información se encuentra dirigida a un enrutador PE específico y se establecen adyacencias PIM a todos los enrutadores PE. Su escalabilidad es media.

- BGP

Su uso se implementó para mejorar el protocolo existente gracias a nuevos procedimientos que solucionan algunos de los problemas que presenta PIM. No presenta actualizaciones periódicas. La información está dirigida a todos los enrutadores PE y se crean adyacencias BGP a todos los enrutadores PE, pero probablemente solo a los Router Reflector, gracias a esto su escalabilidad es muy alta.

2.6.2.3. Encapsulación

Existen 2 formas de encapsulación de paquetes multicast:

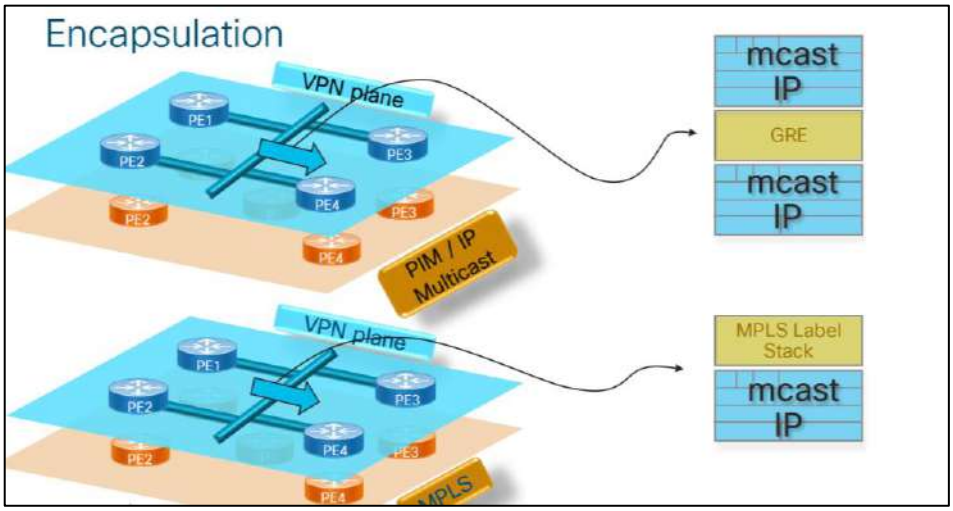


Ilustración 2-28: Encapsulación paquetes multicast

Fuente: (Ghein 2019).

- GRE

La encapsulación GRE es un protocolo de tunelización que se utiliza para encapsular y transportar diferentes tipos de paquetes de red a través de una red IP. En esencia, GRE crea un túnel virtual entre dos puntos finales, que puede ser utilizado para transportar paquetes de red de manera segura y confiable a través de una red pública o privada.

- MPLS LABEL STACK

En la encapsulación MPLS se utiliza una etiqueta para identificar el camino que debe tomar un paquete a través de la red. Cuando el paquete multicast debe ser enviado a varios destinatarios,

éste también dependerá de la señalización de superposición y la señalización de base para llegar a su destino.

2.6.3. Perfiles MVPN

2.6.3.1. Perfiles MVPN Cisco

Cisco a definido hasta la actualidad un total de 26 perfiles, numerados del 0 al 26, estos se encuentran diferenciados por las cinco posibles tecnologías que utilizan cada uno, las mismas que crean el árbol en la red central.

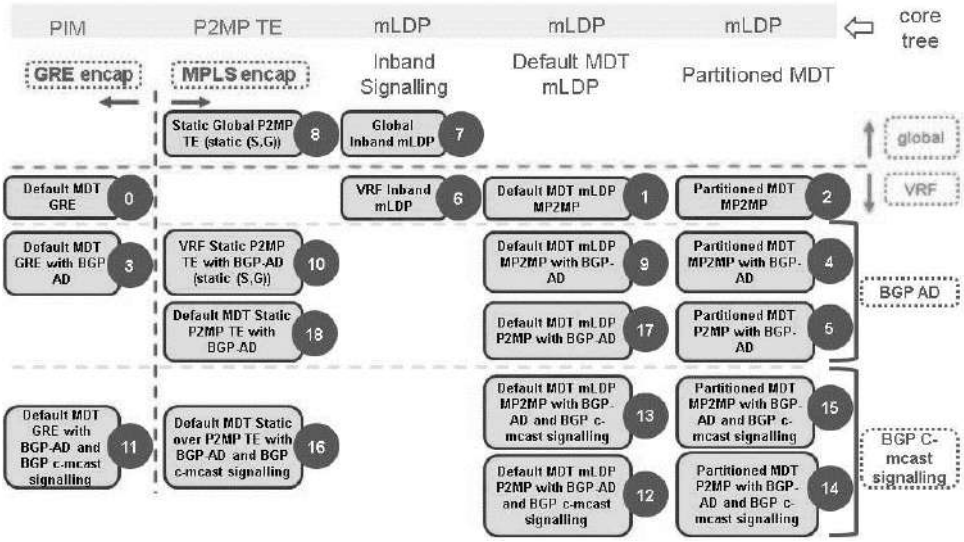


Ilustración 2-29: Descripción general de todos los perfiles MVPN posibles

Fuente: (Cisco, 2020).

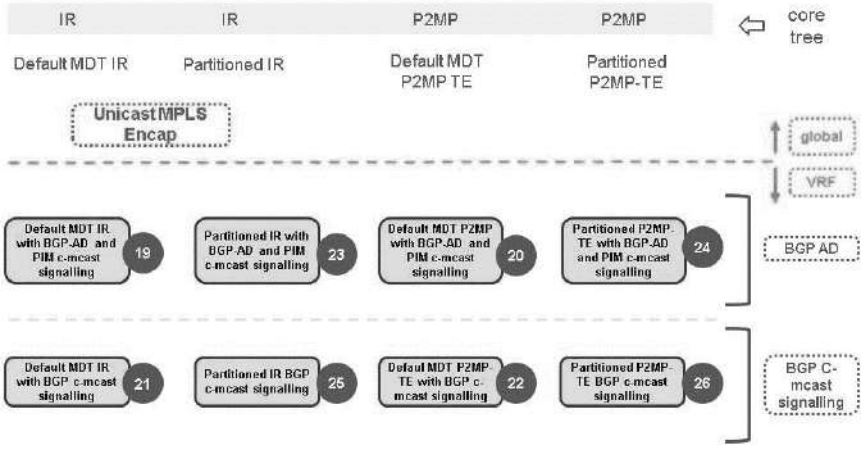


Ilustración 2-30: Descripción general de todos los perfiles MVPN posibles

Fuente: (Cisco, 2020**).**

La línea verde separa a los perfiles en dos conjuntos por su tipo de encapsulación:

- Encapsulación de enrutamiento genérico (GRE)
- Encapsulación de conmutación de etiquetas multiprotocolo (MPLS).

La línea amarilla divide los perfiles en dos conjuntos según su contexto:

- Multidifusión en el contexto global
- Multidifusión en el contexto de enrutamiento y reenvío virtual (VRF).

Hay tres conjuntos, cada uno con un nivel adicional de señalización del Border Gateway Protocol (BGP):

- Sin señalización BGP (excepto IPv4 Multicast Distribution Tree (MDT) para Rosen GRE),
- BGP Auto-Discovery (AD)
- BGP AD y BGP Señalización C-MCAST (señalización de clientes de Multicast en superposición).

Un nivel "adicional" de señalización BGP significa un nivel además de la señalización BGP que siempre se necesita para unidifusión sobre MPLS VPN.

2.6.3.2. Perfiles MVPN Juniper

Juniper menciona que existen dos formas de implementar MVPN de capa 3:

- MVPN de PIM dual
- MBGP

MVPN de PIM dual

Se le conoce también como “draft-rosen”, se encuentra configurada con túneles de proveedor de servicio y cuenta con la VPN habilitada para multidifusión y configurada para utilizar el protocolo de multidifusión independiente PIM dentro de la VPN. El sistema operativo Junos proporciona dos tipos de multidifusión “draft-rosen”(Juniper Networks 2020, p. 59)

- VPN de multidifusión Draft-rosen con túneles de proveedor de servicios que operan en modo de multidifusión de cualquier fuente (ASM).
- VPN de multidifusión Draft-rosen con túneles de proveedor de servicios que operan en modo de multidifusión específica de origen (SSM).

MBGP

Conocido como el método de configuración de MVPN de "próxima generación", su principal característica es que no requiere configuración de multidifusión en la red troncal del proveedor de servicios. Las VPN de MBGP utilizan el plano de control de BGP del sistema intra autónomo AS y el modo disperso PIM cómo plano de datos (Juniper Networks 2020, p. 25).

Se evidencia que tanto Cisco Systems y Juniper Networks dividen a los perfiles o formas de implementar Multicast VPN en dos grupos según su tipo de encapsulación, el primer grupo utiliza túneles de encapsulación genérica GRE y el segundo grupo encapsulación de conmutación de etiquetas multiprotocolo.

2.7. Streaming

2.7.1. Parámetros de transmisión de video streaming

2.7.1.1. Fotograma por segundo (FPS)

Los cuadros por segundo (FPS) miden cómo se muestra el video en movimiento. Con la forma en que nuestro cerebro agrega información faltante para crear movimiento, cuanto mayor es el FPS, más suave aparece el movimiento ante los ojos. Por ejemplo, si un video se captura y se reproduce a 24 cuadros por segundo, eso significa que cada segundo del video muestra 24 imágenes fijas distintas.

En general, el FPS mínimo necesario para evitar movimientos bruscos es de 30 fotogramas por segundo. Para contenido de alto movimiento, verá alrededor de 60 cuadros por segundo (Krings 2021, p. 53)

2.7.1.2. Buffer

Área de memoria destinada a almacenar datos por un lapso de tiempo determinado (ECURED 2018, p. 27). Los datos se almacenan en búferes a medida que se transfieren desde un dispositivo de

entrada o antes de que se envíen a un dispositivo de salida. También se puede utilizar para transferir datos entre procesos (CISET 2021, p. 85).

2.7.1.3. Latencia

Conocido como tiempo de respuesta, es una medida del tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino; Un paquete es uno de los fragmentos de datos en los que se divide la información que se va a enviar, por lo que los datos se pueden enviar más rápido y con más control dividiendo la información en paquetes (LINUBE 2017, p. 96).

2.7.1.4. Bit rate

La tasa de bits de un video es la tasa de tráfico o datos, o de manera equivalente, la cantidad de información que una computadora procesa cada segundo. Por lo tanto, cuanto mayor sea el flujo de datos al segundo, mayor será la calidad. Este tráfico se mide en kilobytes por segundo, lo que significa que cuantos más kbps, mejor será la calidad del video (Fernandez 2017, p. 31)

2.7.2. Protocolos de transmisión

2.7.2.1. Protocolo de transporte en tiempo real (RTP)

RTCP (Protocolo de transporte en tiempo real), está definido en el RFC 3550. RTCP trabaja mano a mano con RTP. RTP hace el envío de los datos, donde RTCP es utilizado para enviar los paquetes de control a los participantes en una llamada. La función principal es proporcionar retroalimentación sobre la calidad del servicio proporcionado por RTP.

Transporta estadísticas e información en forma de octetos, conteo de paquetes y tiempo de regreso. RTCP no provee algún tipo de encriptación o método de autenticación, pero estos mecanismos pueden ser implementados al usar Secure Real-time Transport Protocol (SRTP) (3CX 2018)

2.7.2.2. Protocolo de suscripción de publicación en tiempo real (RTPS)

RTPS (Protocolo de suscripción de publicación en tiempo real) es un protocolo para el mejor esfuerzo y comunicaciones pub-sub confiables sobre transportes no confiables como UDP tanto en unidifusión como en multidifusión.

RTPS ha sido estandarizado por OMG (Object Management Group) como el protocolo de interoperabilidad para implementaciones del Servicio de Distribución de Datos (DDS), un estándar ampliamente utilizado en los sectores aeroespacial y de defensa para aplicaciones en tiempo real (Eprosima 2016, p. 63).

2.7.2.3. Protocolo de mensajería en tiempo real (RMTP)

Es el Protocolo de mensajería en tiempo real como indican sus siglas RTMP (Real Time Messaging Protocol) creado por Adobe para lograr comunicación entre Flash y Adobe Air, utiliza TCP a nivel de capa de transporte con el puerto 1935 existen variaciones como RTMPT (tunelizado a través de HTTP), RTMPE (encriptado), RTMPTE (tunelizado y encriptado), RTMPS (encriptado sobre SSL) , RTMFP (viaja sobre UDP en lugar de TCP) (Campo, Chanchi, Camacho 2017, p. 85).

RTMP puede enviar y recibir paquetes por canales virtuales específicos independientes el uno del otro, permite transmisión de baja latencia, se divide en fragmentos y su tamaño es arreglado dinámicamente entre cliente y servidor. Su principal uso es en aplicaciones streaming debido a su persistente entrega y baja latencia de contenido, empresas como Twitch y Facebook utilizan este protocolo, pero con modificaciones permitiendo mayor seguridad en la información transmitida y mejor funcionamiento en la red actual.

2.7.2.4. Comunicación en tiempo real para la web (WebRTC)

WebRTC es un estándar de código abierto para la comunicación en tiempo real compatible con casi todos los navegadores modernos, incluidos Safari, Google Chrome, Firefox, Opera y otros. WebRTC admite VP8 y VP9 de alta calidad (además del antiguo H.264), así como el códec de audio Opus. En un futuro próximo, el protocolo será compatible con un nuevo códec de video AV1. Se prevé que el protocolo sustituya a la telefonía y se convierta en el pilar de los servicios de comunicación.

Una de las mayores ventajas de WebRTC es que transforma millones de navegadores en terminales de transmisión sin necesidad de instalar complementos adicionales. Además, WebRTC admite una latencia inferior a un segundo, lo que significa que no habrá más retrasos.

El protocolo utiliza una tecnología de tasa de bits adaptable, que le permite ajustar automáticamente la calidad del video y evitar caídas e interrupciones (Bychok 2020, p. 59).

2.7.2.5. Protocolo de código abierto (SRT)

SRT es un protocolo de transmisión de video de código abierto desarrollado por Haivision y Wowza. Se considera ampliamente que será un sustituto de RTMP en un futuro próximo. Al compartir las mismas ventajas, SRT está dando el siguiente paso y haciendo realidad el sueño de transmisiones en vivo estables con una latencia inferior a un segundo. Esto permite la transmisión en vivo de contenido en redes subóptimas. Sin embargo, un gran inconveniente es que la opción de reproducción no está disponible.

Los desarrolladores afirman que SRT protege sus videos en vivo de fluctuaciones, fluctuaciones del ancho de banda y pérdida de paquetes. Además, SRT es similar a FTL y WebRTC en términos de latencia inferior a un segundo, lo que permite una comunicación casi en tiempo real. Además, también se afirma que el protocolo es independiente del códec, lo que significa que es compatible con cualquier códec de audio y video moderno. Desafortunadamente SRT no es ampliamente compatible (Bychok 2020, p. 27).

2.7.2.6. Protocolo más rápido que la luz (FTL)

FTL es un protocolo de transmisión en tiempo real, admite latencia inferior a un segundo. Esto le permite interactuar y comunicarse con sus espectadores en tiempo real prácticamente sin demora. FTL es compatible con las aplicaciones de transmisión más populares, incluidas XSplit y OBS Studio. También está preintegrado en el sistema operativo Windows 10 y Xbox One. Utiliza el códec de audio Opus y el códec de video H.264 para permitir una buena combinación de calidad, reproducción fluida y baja latencia.

La desventaja de usar FTL es que su transmisión perderá algo de calidad. Mixer recomienda reducir su tasa de bits a 7 Mbps en comparación con los 10 Mbps de RTMP (Bychok 2020, p. 74).

Tabla 2-2: Protocolos de Transmisión de Video Streaming

	RMTP	**WebRTC**	**FTL**	**SRT**
Ventajas	• Estabilidad • Almacenamiento en búfer bajo • Amplio soporte de plataforma	• No se necesitan complementos • Admite nuevos códecs • Latencia ultrabaja	Latencia de menos de un segundo	• Códecs compatibles • Alta calidad • Estabilidad de la corriente • Latencia de menos de un segundo
Desventajas	• Latencia realmente alta • Posible seguridad • Códecs antiguos	• Todavía en desarrollo • Inestabilidad debido a una latencia inferior a un segundo	• Baja calidad • Soporte de plataforma débil	• Soporte de plataforma débil • Sin reproducción
Video Codec	H.264	VP8, VP9, H.264, (AV1 en proceso)	H.264	Codec-agnostic
Audio Codec	AAC	Opus	Opus	Codec-agnostic
Latencia	3-30 sec	Menos de 1 segundo	Menos de 1 segundo	Menos de 1 segundo

Fuente: (Bychok 2020).

Realizado por: Mafla, Carlos, 2022.

2.8. Software de emisión de video VLC media player

VLC media playes es un software multiplataforma gratuito y de código abierto que permite ser utilizado como servidor y como cliente para enviar y recibir video streaming unicast y multicast en una red. Soporta la mayoría de los archivos multimedia y varios protocolos de emisión. Se utiliza la versión 3.0.16 para Windows disponible en la página oficial del software.

2.8.1. Método de emisión

VLC media player permite utilizar algunos métodos de compresión de audio y video, al ser un software que soporta varios formatos de archivo, posee también algunos métodos de emisión de contenido multimedia que se detallan en la tabla 2-3.

Tabla 2-3: Comparación de los métodos de emisión disponibles en VLC

NOMBRE	DEFINICIÓN	PRESTACIONES	Protocolo de la capa de transporte
HTTP	Protocolo de transferencia de hipertexto	Transmisión de datos multimedia en tiempo real	TCP
MS-WMSP	Protocolo de transmisión HTTP de Windows Media	Transmisión de datos multimedia en tiempo real usado por Windows Media	TCP
RTSP	Protocolo de transmisión en tiempo real	Establece y controla uno o muchos flujos sincronizados de datos.	TCP UDP
RTP/MPEG	Protocolo de transporte en tiempo real	Transmisión de audio y video en tiempo real que utiliza el protocolo de comunicación Transport Stream, puede ser unicast o multicast	UDP
RTP/AVP	Protocolo de transporte en tiempo real	Transmisión de audio y video en tiempo real,	UDP
UDP	Protocolo de datagrama de usuario	Transmisión de audio y video basado en datagramas.	UDP
ICECAST	Programa para transmisión continua de medios	Software de servidor gratuito para la transmisión de multimedia. (transmisión de radio)	UDP

Realizado por: Mafla, Carlos 2022.

2.8.2. Opciones de transcodificación

VLC ofrece la opción de transcodificar el contenido, la misma consiste en transformar el audio y video a enviar a otro formato para que todos los clientes tengan acceso al contenido. Se encuentran muchos formatos para la transcodificación del contenido, como se muestra en la Ilustración 2-31.

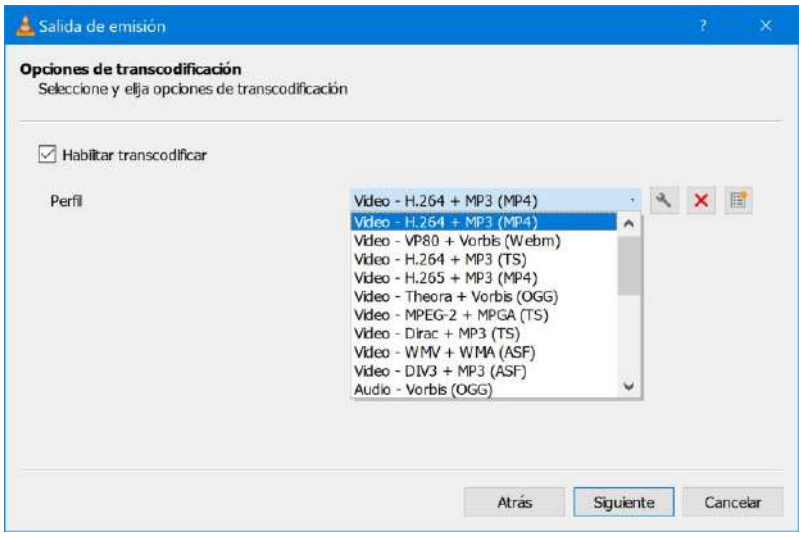


Ilustración 2-31: Opciones de emisión y recepción en VLC

Realizado por: Mafla, Carlos, 2022.

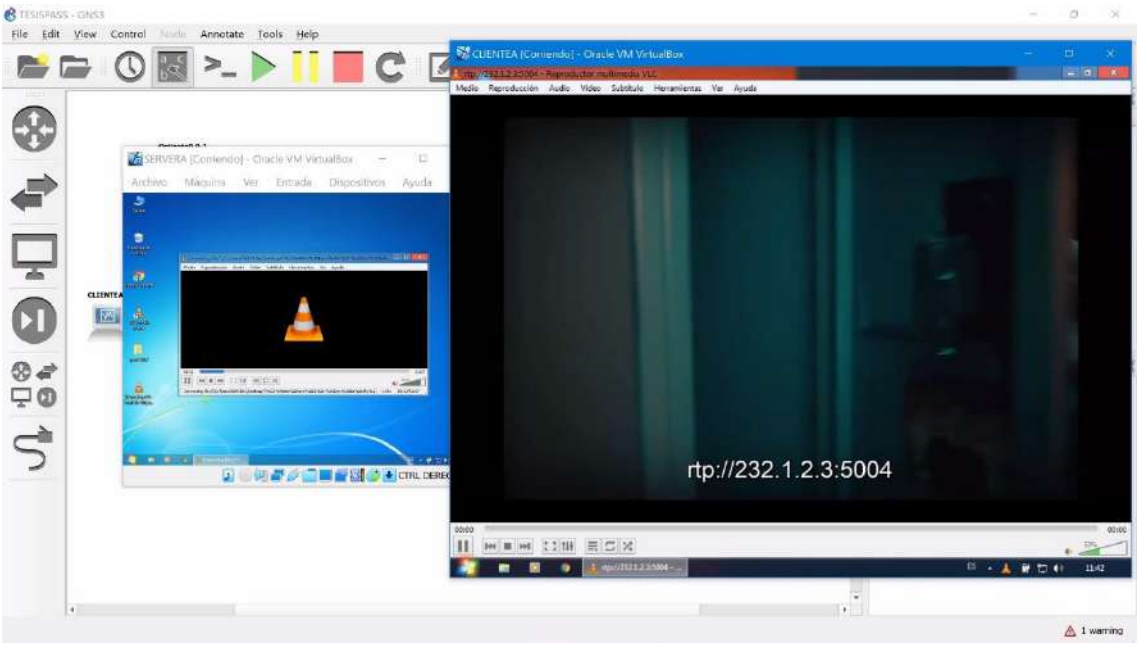


Ilustración 2-32: Recepción de video utilizando el protocolo RTP

Realizado por: Mafla, Carlos, 2022.

En la Ilustración 2-32 se puede observar la recepción de video multicast que fue emitido desde el servidor A y reproducido en el cliente A, el mismo utiliza el protocolo RTP.

2.9. Herramienta de monitoreo Wireshark

Conocido como uno de los mejores analizadores de tráfico en red, permite capturar todos los paquetes que se generan en los distintos equipos, los decodifica y ofrece la posibilidad de que estos sean analizados a detalle.

Entre sus mayores ventajas se encuentran su facilidad de ser instalado y utilizado en multitud de plataformas en las que se destacan; Windows, Linux, macOS, Solaris, GNS3, FreeBSD, NetBSD y también el soportar alrededor de unos 750 protocolos (Tene Salcán 2020, p. 39), su manejo es intuitivo debido a su excelente interfaz gráfica. Entre la información que presenta se puede destacar el número de paquetes capturados, el número de paquetes analizados, el tiempo entre paquetes, el promedio de paquetes, tamaño de paquetes, cabeceras de protocolos, número de tramas, etc. Otra de sus mayores funcionalidades es que permite obtener resúmenes generales de los análisis realizados en la red.

En resumen, Wireshark es un analizador de red que permite ser usado en múltiples plataformas y analiza el tráfico generado en la red en tiempo real, permitiendo así solucionar inconvenientes generados en la red e identificar en qué lugar ocurren.

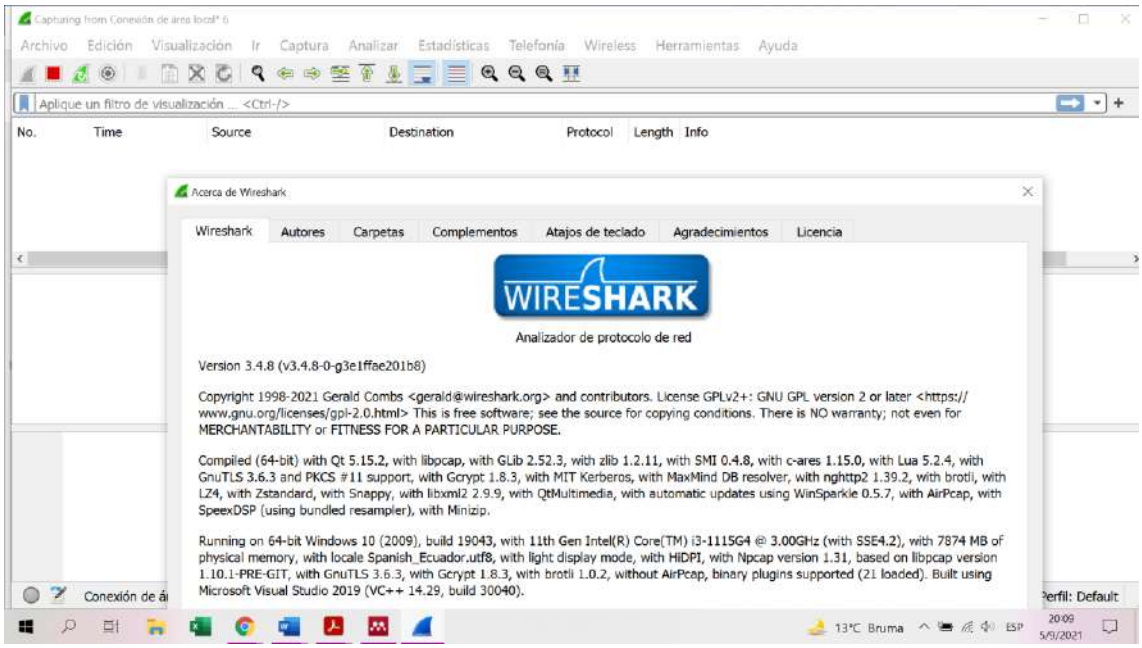


Ilustración 2-33: Herramienta de monitoreo de protocolos wireshark

Realizado por: Mafla, Carlos, 2022.

2.10. Herramienta de generación y análisis de tráfico Ostinato 0.9.1

El generador y analizador de tráfico Ostinato, presenta varias características que le permiten realizar envío de tráfico multicast. Permite configurar velocidades de transmisión, ráfagas, y número de paquetes, muestra estadísticas y velocidades de recepción. Una de sus mayores ventajas es que permite crear y configurar múltiples transmisiones y analizarlas capturando el tráfico con wireshark.

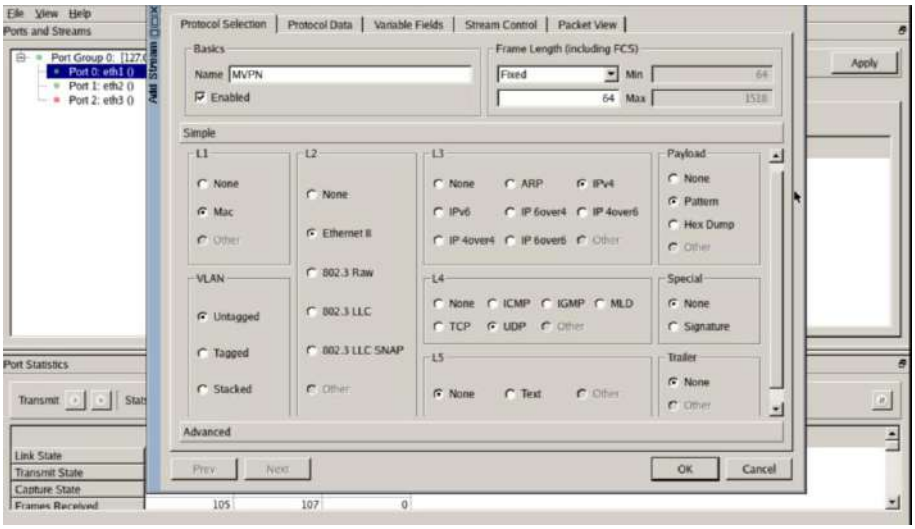


Ilustración 2-34: Analizador de tráfico Ostinato

Realizado por: Mafla, Carlos, 2022.

2.11. Herramienta de generación y análisis de tráfico Iperf/Jperf

Jperf en su versión 2.0.2 es un software que permite medir el ancho de banda y la calidad de un enlace en la red, está diseñado para funcionar en múltiples plataformas y su funcionamiento va de la mano con Java. Ofrece también su versión sin interfaz gráfica, utilizable en modo consola y que también se puede ejecutar mediante CMD de Windows denominada Iperf, las dos herramientas ofrecen opciones similares encontrándose diferenciadas por la facilidad de manejo.

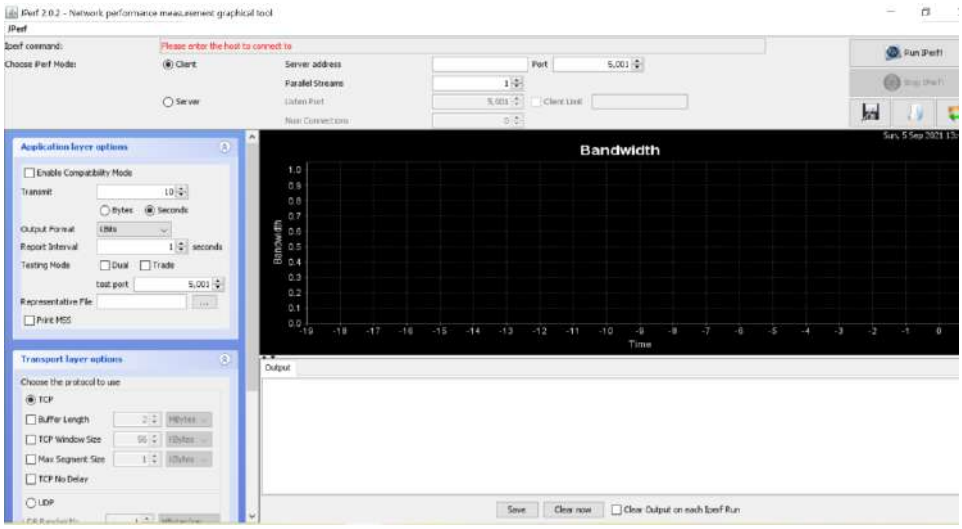


Ilustración 2-35: Software Jperf versión 2.0.2

Realizado por: Mafla, Carlos, 2022.

CAPITULO III

3. MARCO METODOLÓGICO

3.1. Implementación del escenario

Para la construcción del escenario propuesto es necesaria la creación del núcleo MPLS-VPN el mismo que simula el Core del proveedor de servicios y se encuentra formado por routers Cisco IOS-XR que permiten la creación de redes virtuales Capa 3 y la implementación de perfiles Multicast VPN. También se utilizan routers Cisco IOS-XR cómo routers PE que permiten la conexión del núcleo MPLS con routers CE que simulan ser los routers del cliente. La simulación se realiza en GNS3, un simulador gráfico de red lanzado en 2008, que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellas (Neumann 2015, p. 37).

Es necesario también la creación de 4 ubicaciones que simularán los emisores de video streaming y los receptores de estos. Para la simulación de los servidores de video streaming se utilizarán máquinas virtuales del sistema operativo Windows 7 virtualizadas en el software Virtual Box versión 6.1.26 y en cada una de ellas se empleará el software VLC versión 3.0.16 para la emisión del contenido y la recepción de este.

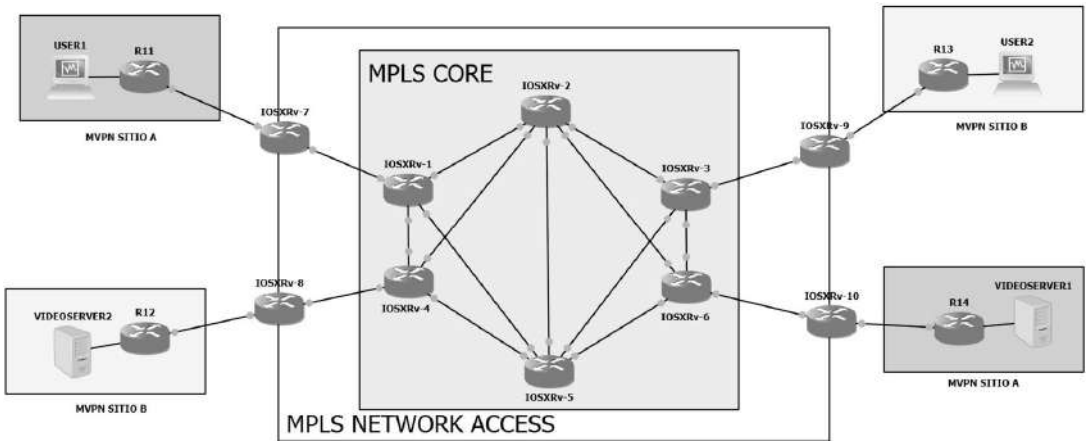


Ilustración 3-1: Escenario detallado de la red implementada

Realizado por: Mafla, Carlos 2022

Tabla 3-1: Direccionamiento IP de la red (Routers)

ROUTER	INTERFAZ	DIRECCIÓN IP	MÁSCARA
P1	GigabitEthernet0	10.10.1.1	255.255.255.0
	GigabitEthernet1	10.10.2.1	255.255.255.0
	GigabitEthernet2	10.10.3.1	255.255.255.0
	GigabitEthernet3	10.10.11.1	255.255.255.0
P2	GigabitEthernet0	10.10.1.2	255.255.255.0
	GigabitEthernet1	10.10.4.1	255.255.255.0
	GigabitEthernet2	10.10.5.1	255.255.255.0
	GigabitEthernet3	10.10.6.1	255.255.255.0
	GigabitEthernet4	10.10.7.1	255.255.255.0
P3	GigabitEthernet0	10.10.7.2	255.255.255.0
	GigabitEthernet1	10.10.8.1	255.255.255.0
	GigabitEthernet2	10.10.9.1	255.255.255.0
	GigabitEthernet3	10.10.13.1	255.255.255.0
P4	GigabitEthernet0	10.10.3.2	255.255.255.0
	GigabitEthernet1	10.10.4.2	255.255.255.0
	GigabitEthernet2	10.10.15.2	255.255.255.0
	GigabitEthernet3	10.10.12.1	255.255.255.0
P5	GigabitEthernet0	10.10.15.1	255.255.255.0
	GigabitEthernet1	10.10.2.2	255.255.255.0
	GigabitEthernet2	10.10.5.2	255.255.255.0
	GigabitEthernet3	10.10.8.2	255.255.255.0
	GigabitEthernet4	10.10.10.2	255.255.255.0
P6	GigabitEthernet0	10.10.10.1	255.255.255.0
	GigabitEthernet1	10.10.6.2	255.255.255.0
	GigabitEthernet2	10.10.9.2	255.255.255.0
	GigabitEthernet3	10.10.14.1	255.255.255.0
PE1	GigabitEthernet0	100.10.20.1	255.255.255.0
	GigabitEthernet1	10.10.11.2	255.255.255.0
PE2	GigabitEthernet0	172.20.21.1	255.255.255.0
	GigabitEthernet1	10.10.12.2	255.255.255.0
PE3	GigabitEthernet0	10.10.13.2	255.255.255.0
	GigabitEthernet1	200.10.22.1	255.255.255.0
PE4	GigabitEthernet0	10.10.14.2	255.255.255.0
	GigabitEthernet1	192.168.23.1	255.255.255.0
CE1	GigabitEthernet0	100.10.20.2	255.255.255.0
	GigabitEthernet1	100.10.30.1	255.255.255.0
CE2	GigabitEthernet0	172.20.21.2	255.255.255.0
	GigabitEthernet1	172.20.31.1	255.255.255.0
CE3	GigabitEthernet0	200.10.22.2	255.255.255.0
	GigabitEthernet1	200.10.32.1	255.255.255.0
CE4	GigabitEthernet0	192.168.23.2	255.255.255.0
	GigabitEthernet1	192.168.33.1	255.255.255.0

Realizado por: Mafla, Carlos 2022.

En la tabla 3-2 se puede observar el direccionamiento de cada una de las interfaces de los routers que conforman la red.

Tabla 3-2: Direccionamiento IP de la red (Equipos Cliente / Servidor)

COMPUTADOR	DIRECCIÓN IP	MÁSCARA	GATEWAY
SERVER A	100.10.30.2	255.255.255.0	100.10.30.1
SERVER B	172.20.31.2	255.255.255.0	172.20.31.1
CLIENTE A	200.10.32.2	255.255.255.0	200.10.32.1
CLIENTE B	192.168.33.2	255.255.255.0	192.168.33.1

Realizado por: Mafla, Carlos 2022.

En la tabla 3-3 se muestran las direccione IP que se encuentran configuradas en los equipos servidor y cliente.

Tabla 3-3: Características Servidor y Cliente

	SERVIDOR	RECEPTOR
SISTEMA OPERATIVO	WINDOWS 7 / 32 bits	WINDOWS 7 / 32 bits
PROCESADOR	Core i7 2.9 GHz	Core i7 2.9 GHz
MEMORIA RAM	1 GB	1 GB
MEMORIA DE VIDEO	200MB	200MB

Realizado por: Mafla, Carlos 2022.

La función de VPN multicast o VPN de multidifusión permite a los equipos enrutadores admitir la multidifusión a través de una VPN de capa 3, esto ayuda a que empresas que amplían los alcances de sus aplicaciones que necesitan o ocupan multidifusión utilicen proveedores de servicio que puedan brindar conexión mediante su red central de conmutación de etiquetas multiprotocolo MPLS. El escenario planteado pretende simular el funcionamiento de un proveedor de servicios de video que posee dos centrales desde donde emite su contenido. Los receptores se encuentran conectados mediante una red MPLS y también se utiliza la tecnología multicast VPN para la transmisión de contenido.

Tabla 3-4: Características Routers Utilizados

ROUTER CISCO IOS XR	
SISTEMA OPERATIVO	CISCO 6.0.1
MEMORIA RAM	3072 MB

Realizado por: Mafla, Carlos 2022.

Para la simulación de la tecnología Multicast VPN se utilizan routers que permitan configurar los perfiles MVPN a ser analizados, estos dispositivos son simulados en el entorno GNS3, al ser equipos que ofrecen una multitud de opciones de configuración necesitan también una gran cantidad de memoria para su funcionamiento, tal y como se puede evidenciar en la tabla 3-5.

Tabla 3-5: Características equipo utilizado para la simulación

COMPUTADOR HP ENVY X360	
PROCESADOR	I7 -7500U @ 2.9 GHz
SISTEMA OPERATIVO	Windows 10
MEMORIA RAM	16 GB

Realizado por: Mafla, Carlos 2022.

Las características del equipo utilizado para la simulación de todo el escenario planteado se muestran en la Tabla 3-6.

Tabla 3-6: Comparación de los protocolos multicast

Protocolo de Enrutamiento Multicast	**Escalabilidad**	**Protocolo de enrutamiento Unicast del que depende**	**Modo disperso**	**Modo denso**
DWMRP	No	RIP	No	Si
MOSPF	No	OSPF	No	Si
PIM DM	No	Independiente	No	Si
PIM SM	Si	Independiente	Si	No
PIM BiDir	Si	Independiente	No	No
PIM SSM	Si	Independiente	Si	No

Realizado por: Mafla, Carlos 2022.

Cómo se puede observar en la tabla 3-6 existen varios protocolos de enrutamiento multicast, cada uno presenta características particulares que les permiten estar enfocado a diferentes tipos de transmisiones. Una de las características más importantes para el funcionamiento de Multicast VPN es el árbol de distribución que cada uno de los protocolos utilizan, los protocolos analizados se diferencian en la forma que dichos árboles trabajan, por una parte, DWMRP, MOSPF, PIM DM trabajan en modo denso con árboles de distribución basados en la fuente y PIM SM, PIM SSM trabajan en modo disperso con árboles de distribución compartido. Para el presente trabajo se busca la utilización del protocolo más eficiente a la hora de enviar tráfico multicast desde un servidor hacia varios clientes, cómo lo hacen los protocolos que trabajan en modo disperso.

Los protocolos que utilizan modo disperso ofrecen también una mayor escalabilidad debido a que la memoria que se necesita en cada uno de los routers que conformar la red multicast es menor. Debido a esto se descarta también la utilización de DWMRP, MOSPF y PIM DM además que estos dependen de los mecanismos propuestos por algún protocolo de enrutamiento unicast. PIM SM y PIM SSM utilizan árboles de distribución compartidos por lo que son utilizados en redes de área extendida. PIM Bidir construye árboles de distribución compartidos bidireccionales, alcanzando su mejor funcionamiento en redes con varias fuentes y receptores dispersos. PIM SSM construye árboles basados en la fuente y conserva el modo disperso de PIM SM.

Para la simulación del escenario planteado se decidió utilizar el protocolo PIM-SM en routers CE debido a su escalabilidad y PIM SSM en el core MPLS, esto también dependerá de cada uno de

los perfiles MVPN que se implementen en el escenario ya que existen perfiles que utilizan señalizaciones diferentes a PIM en el core MPLS.

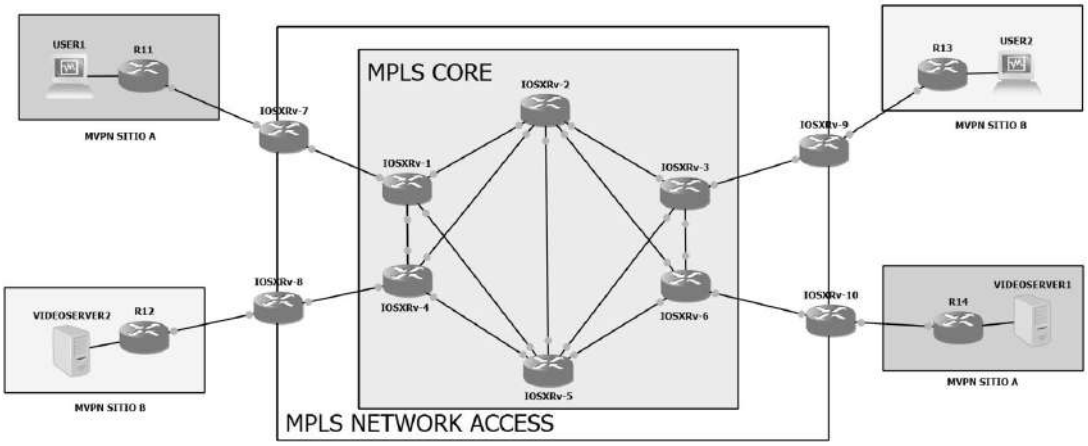


Ilustración 3-2: Esquema de los protocolos multicast en la red

Realizado por: Mafla, Carlos, 2022.

3.1.1. Análisis y comparación de los perfiles MVPN

Las VPN de multidifusión se utilizan para trasportar tráfico a través de MPLS L3VPN, los modelos o perfiles MVPN afectan la forma en la que el proveedor de servicios maneja el tráfico del cliente en su red MPLS, es decir la forma en la que el PIM del cliente atraviesa la red MPLS. Los dispositivos del cliente CE solo se encargan de ejecutar PIM SM, PIM SSM o PIM BiDir, los dispositivos PE del proveedor del servicio manejan los paquetes PIM del router del cliente, es decir que la multidifusión del cliente es similar a un salto sobre el núcleo del proveedor de servicio, como ocurre con la unidifusión MPLS L3VPN.

Los perfiles Multicast VPN se diferencian según la arquitectura MVPN que cada uno presenta, los routers P señalan un árbol a través del núcleo, el mismo que se puede señalizar con PIM o MPLS, a este proceso se le conoce como señalización sub adyacente “underlay signaling” o árbol del núcleo “core tree”, los routers PE señalan un árbol sobre el núcleo, este se puede señalizar con PIM o BGP, a este proceso se le conoce como señalización superpuesta “overlay signaling” o árbol VPN “VPN tree”. Además de estas señalizaciones los perfiles MVPN se diferencian por el tipo de encapsulación que el perfil presenta en el plano VPN, esta puede ser GRE o MPLS.

Tabla 3-7: Comparación de las opciones de Señalización Subadyacente

	PIM	**mLDP**	**P2MP TE**
Encapsulación	GRE	MPLS	MPLS
Reserva de ancho de banda	NO	NO	SI
Complejidad	Alta	Media	Alta
Actualizaciones	Periódica	Sin actualizaciones periódicas	Periódica
Enrutamiento	Sigue enrutamiento unicast	Sigue enrutamiento unicast	Permite restricción explícita de enrutamiento
Tipos de árboles	P2MP	P2MP MP2MP	P2MP

Realizado por: Mafla, Carlos 2022.

Tabla 3-8: Comparación de las opciones de Señalización Superpuesta

	PIM	**BGP**
Antiguedad	Más antiguo, bien conocido	Nueva mejora del protocol existente
Actualizaciones	Periódica	No existen actualizaciones periódicas
Escalabilidad	Media	Alta
Adyacencias	PIM a todos los routers PE	BGP a todos los routers PE, puede ser solo a Router Reflector.
Información	Dirigida a un router PE específico	Dirigida a todos los enrutadores PE

Realizado por: Mafla, Carlos 2022.

Los perfiles MVPN nacen de la combinación de:

- Tipo de servicio (IPV4 / IPV6 / VPNV4 / VPNV6)
- Señalización Superpuesta “Underlay Signaling” (PIM / MPLS)
- Señalización Subadyacente “Overlay Signaling” (PIM / BGP)
- Encapsulación (GRE / MPLS)

Tabla 3-9: Comparación de los Perfiles MVPN analizados

PERFIL	Tipo de servicio	Señalización Superpuesta	Señalización Subadyacente	Encapsulación
Perfil 0	IPV4	PIM	PIM	GRE
Perfil 1	IPV4	mLDP MP2MP	PIM	MPLS
Perfil 11	IPV4	PIM	BGP	GRE

Realizado por: Mafla, Carlos 2022.

Los perfiles elegidos para el análisis en el escenario planteado presentan diferentes tipos de señalizaciones y encapsulaciones.

3.1.2. Configuración de los perfiles Multicast VPN en el escenario planteado

Se muestran de forma general los comandos utilizados para la configuración de los perfiles multicas VPN en los routers que conforman la red planteada. Los archivos de configuración de todos los equipos de la red se muestran en el Anexo A.

3.1.2.1. Configuración del núcleo en las redes MPLS

- Configurar OSPF como protocolo IGP
- Habilitar MPLS LDP en las todas las interfaces del router

3.1.2.2. Configuración del área de acceso a la red MPLS

- Se configura OSPF como protocolo IGP
- Se habilita MPLS en la interfaz

3.1.2.3. Configuración de los routers de borde

- Se configura la red del servidor A
- Se configura la conexión hacia la red MPLS del proveedor de servicios
- Se configura las interfaces del router para que ejecuten el protocolo PIM

3.1.2.4. Configuración de los servidores de video

- Se instala el software VLC versión 3.0.16 y se configura para la emisión de video a través del protocolo RPT con dirección Multicast 232.1.2.3
- Se instala y se configura el software Jperf para generación, recepción de tráfico y análisis de este.

3.1.2.5. Configuración de los clientes

- Se instala el software VLC versión 3.0.16 y se configura para la recepción de video a través del protocolo RPT con dirección Multicast 232.1.2.3
- Se instala y se configura el software Jperf para generación, recepción de tráfico y análisis de este.

3.1.3. Consideraciones de los perfiles MVPN utilizados

3.1.3.1. Perfil 0 predeterminado MDT PIM - PIM – GRE

Este perfil empieza su funcionamiento cuando el router PE recibe un mensaje PIM, este debe ser enviado a todos los routers PE mediante un túnel PIM que será parte de la ruta virtual creada, para que esto suceda se encapsula el paquete dentro de un túnel GRE y luego se utiliza el enrutamiento PIM regular del núcleo para llevar el paquete a su destino. No existe ningún encapsulamiento MPLS cuando trabajamos con el perfil 0. En la configuración BGP se debe identificar los routers reflectores y verificar que estos tengan acceso a los árboles de distribución multicast vecinos.

3.1.3.2. Perfil 1 predeterminado MDT MLDP - PIM - MPLS

En este perfil usaremos MPLS como medio de transporte en vez de un túnel GRE y especificamos en donde queremos que se construya la raíz de nuestro árbol de distribución, así es posible que todos los routers PE puedan construir un árbol hacia dicho dispositivo central. Se ejecuta PIM desde el router de borde del cliente hasta el router de borde del proveedor. A diferencia del perfil 0 la encapsulación está dada mediante MPLS. Se debe tener presente que el valor VPN ID de la configuración debe coincidir entre todos los routers PE que quieren participar en el enrutamiento VPN de multidifusión. Al no usar BGP debemos estar completamente seguros de que dicho valor coincida, ya que es mediante esta configuración que se permite que el autodescubrimiento ocurra.

3.1.3.3. Perfil 11 MDT predeterminado PIM - BGP- GRE

Este perfil tiene como principal característica que usa BGP para la señalización a través del proveedor. Al momento de transportar los paquetes multicast usa GRE de igual forma que en el perfil 0. También usa el descubrimiento automático de BGP para encontrar los puntos finales y para la señalización de multidifusión del cliente.

3.1.4. Video para la emisión Multicast VPN

El video utilizado para la transmisión Multicast VPN del escenario planteado muestra diferentes presentaciones, con el objetivo de emitir el video en varias resoluciones y calidades, para así obtener resultados detallados del comportamiento de la red del escenario planteado para cada tipo de video emitido.

Tabla 3-10: Características de video para emisión Multicast VPN

NOMBRE	DURACIÓN (segundos)	TAMAÑO (MB)	CODEC AUDIO	CODEC VIDEO	RESOLUCIÓN
BEAUTY OF WORLD	30	2.52	MPEG AAC	H264 MPEG - 4	640x360
BEAUTY OF WORLD	30	3.10	MPEG AAC	H264 MPEG - 4	854x480
BEAUTY OF WORLD	30	5.57	MPEG AAC	H264 MPEG - 4	1280x720
BEAUTY OF WORLD	30	10	MPEG AAC	H264 MPEG - 4	1920x1080

Realizado por: Mafla, Carlos 2022.

CAPÍTULO IV

4. ANÁLISIS DE RESULTADOS

Se realizaron pruebas de ancho de banda en el escenario planteado, con cada uno de los perfiles MVPN analizados, para esto se utilizó la herramienta Jperf en su versión 2.0.2 que se encuentra instalada tanto en la máquina virtual SERVERA y CLIENTEA, esta herramienta permite medir el ancho de banda de una red mediante la generación de tráfico UDP.

Se simularon escenarios de pruebas con cada uno de los perfiles MVPN analizados, en los que se generaba emisión de tráfico multicast y unicast mediante la herramienta Ostinato, que se encuentra instalada en una máquina virtual que corre la versión de Linux Ubuntu 16.04.6, dicha máquina virtual tiene 2 puertos ethernet que permiten generar tráfico y enviarlo a través de la red del escenario planteado. La emisión de tráfico sobre el escenario planteado pudo ser evaluada mediante Wireshark, mediante su opción de análisis de streams.

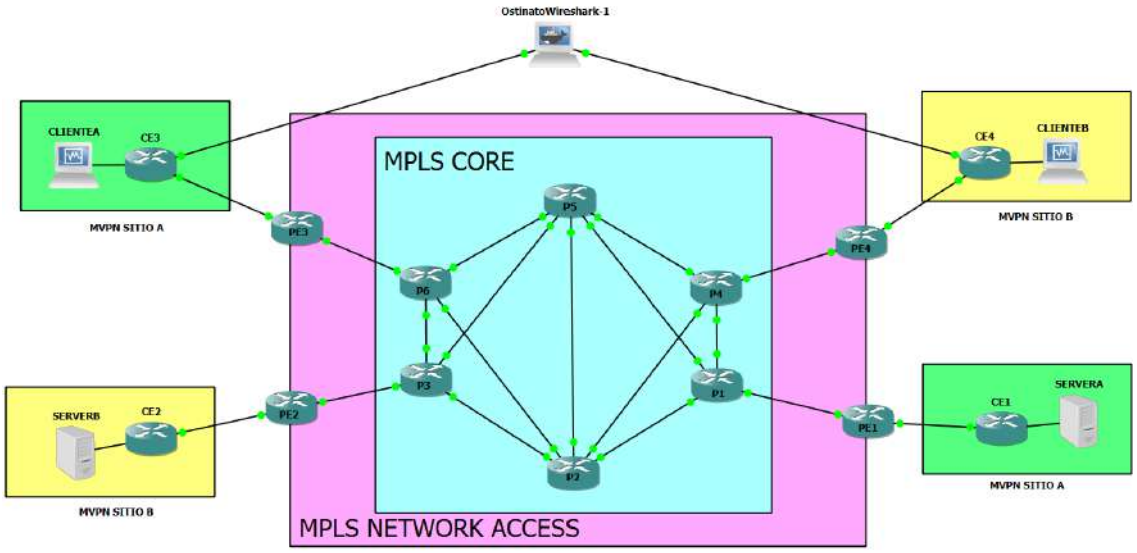


Ilustración 4-1: Generación de tráfico UDP unicast y multicast con herramienta Ostinato

Realizado por: Mafla, Carlos, 2023.

Para la generación de tráfico mediante la emisión de video se utilizó el software VLC, que se encuentra instalado en la máquina virtual SERVERA, se optó por recoger una muestra de 5 observaciones en cada uno de los perfiles analizados, cada una con una duración de 30 segundos con el objetivo de obtener una mejor comprensión y análisis de los resultados obtenidos.

Después de la generación de tráfico con las herramientas Jperf, Ostinato y VLC se obtuvieron varios datos. Es necesario utilizar medidas estadísticas que permitan entender y analizar los

resultados de mejor manera. Para cada uno de los parámetros de calidad de servicio se toma en cuenta los valores máximos, mínimo, media, mediana y desviación estándar.

4.1. Parámetros de calidad de servicio

Los parámetros de calidad de servicio que van a ser analizados en el presente trabajo pretenden informar acerca de las ventajas que ofrece la implementación de cada uno de los perfiles MVPN, también buscan mostrar los fallos o errores que ocurren en el proceso de transmisión y que estos puedan ser medidos de forma estadística.

4.1.1. Retardo

Conocido como el tiempo que tarda un paquete en llegar desde una Fuente hacia su destino, se encuentra medido en milisegundos y según la recomendación IITU Y.1541 el máximo aceptable es de 100ms (Tene Salcán, 2020, p. 48). Cuando se sobrepasa este límite equivale a una calificación de 0% y no se garantiza la calidad de transmisión.

4.1.2. Pérdida de paquetes

Como su nombre lo indica, muestra la cantidad de paquetes que debido a diferentes inconvenientes no han podido llegar a su destino, algunas de estas limitantes son el ancho de banda, congestión en la red, etc. También es necesario mencionar que debido a la utilización del protocolo UDP, no se garantizan la llegada de todos los paquetes enviados ya que no es un protocolo orientado a la conexión.

4.1.3. Jitter

Es conocido como la diferencia de retardo que presenta un paquete con respecto a otro dentro de un mismo enlace, de acuerdo a la recomendación ITU Y.1541 el jitter no debe ser mayor a 50 milisegundos (Tene Salcán, 2020, p. 74). Si este parámetro sobrepasa el tiempo mencionado equivale a una calificación de 0% y no se garantiza una calidad en la transmisión,

En la table 4-1 se puede observar los niveles de valoración que existen según los resultados que puedan ser obtenidos en las mediciones de los parámetros de calidad de servicio.

Tabla 4-1: Valoración del porcentaje de: Retardo, Pérdida de paquetes y Jitter

NIVEL DE VALORACIÓN	RETARDO		PÉRDIDA DE PAQUETES	JITTER	
	RETARDO (ms)	PORCENTAJE (%)	PORCENTAJE (%)	JITTER (ms)	PORCENTAJE (%)
EXCELENTE	0 - 20	100	0 – 2	0 – 10	100
MUY BUENO	20 - 40	80	2 – 4	10 - 20	80
BUENO	40 - 60	60	4 – 6	20 - 30	60
MALO	60 - 80	40	6 – 8	30 - 40	40
PÉSIMO	80 - 100	20	8 – 10	40 - 50	20

Fuente: (Tene Salcán 2020)

La tabla 4-2 muestra la manera en que influyen los parámetros de calidad de servicio para la percepción de usuario final.

Tabla 4-2: Percepción del usuario acerca de los parámetros de servicio

Parámetros de Calidad de Servicio	Grado de Importancia Relativa del Usuario
Packet Loss	41.7%
Burst Level	29.2%
Packet Jitter	10.7%
Packet Delay	10.6%
Bandwidth	7.8%

Fuente: (Tene Salcán 2020).

El "troughput" se define como la velocidad de transporte de datos a través de una red, este se encuentra medida en megabit por segundo y siempre debe ser menor al ancho de banda (Tanenbaum 2012, p. 74). Es la cantidad de información que fluye a través de un sistema.

Antes de realizar las pruebas correspondientes en los perfiles implementados en el escenario planteado, se realizaron pruebas de ancho de banda con la herramienta Jperf, estas pruebas permitieron establecer un ancho de banda al cual se pueda trabajar a la hora de enviar tráfico en el escenario planteado, es importante considerar que al ser un escenario simulado existen varias limitantes que impiden el funcionamiento al total de la capacidad de cada uno de los equipos simulados, esto quedó claramente evidenciado desde el momento en que se realizaron pruebas de ancho de banda en cada uno de los adaptadores de red de las máquinas virtuales simuladas en el escenario. Dichos adaptadores tienen una velocidad nominal de 1000 Mbps pero en las pruebas

realizadas no se pudo transmitir tráfico a dicha velocidad, alcanzando un ancho de banda máximo de 35 Mbps.

En la ilustración 4-2 se puede evidenciar que el enlace simulado presenta inconvenientes para trabajar con anchos de banda extremadamente altos y condiciona a que las pruebas de transmisión de video multicast sean realizadas a un ancho de banda reducido.

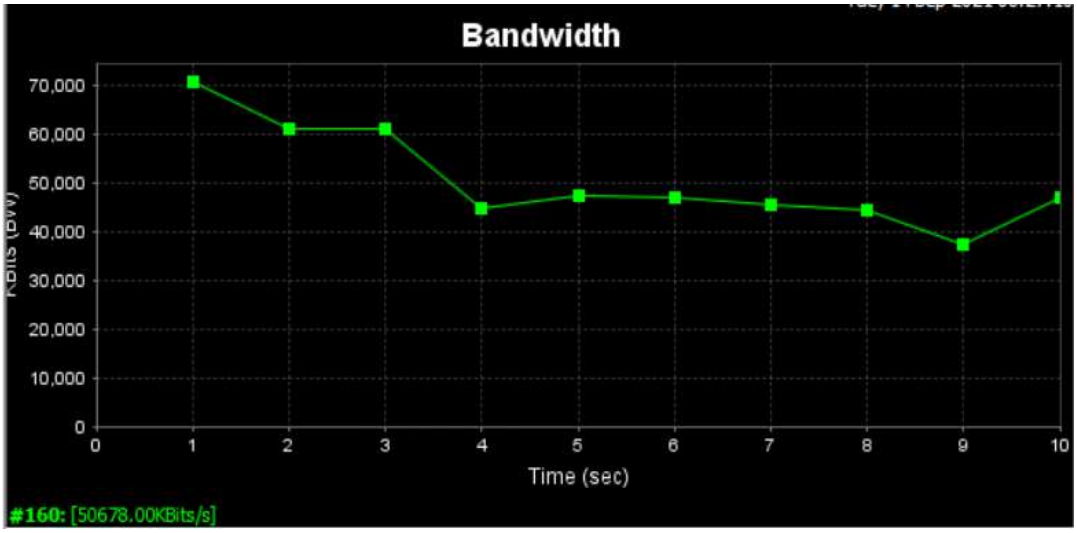


Ilustración 4-2: Prueba ancho de banda 100Mbps Jperf (Perfil 0)

Realizado por: Mafla, Carlos, 2022.

Mediante la herramienta Ostinato se realizaron 10 pruebas de envío y recepción de paquetes multicast y unicast en cada uno de los perfiles multicast VPN analizados, se utiliza la opción Packet View para visualizar la información de cada emisión y recepción cómo se puede observar en la Ilustración 4-3.

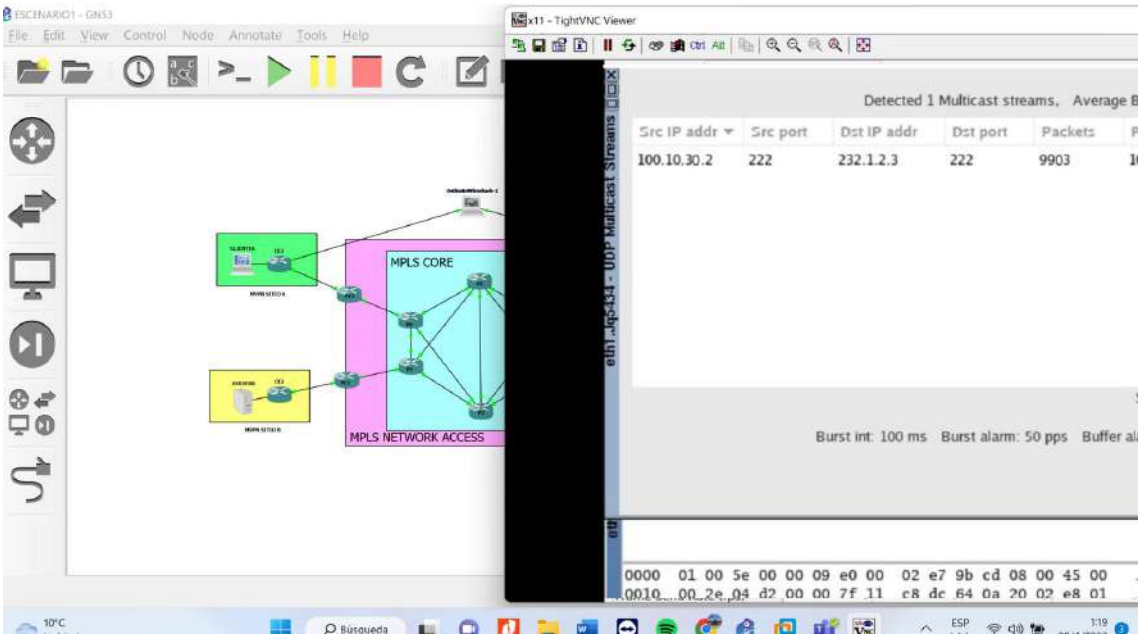


Ilustración 4-3: Envío paquetes mediante la herramienta ostinato

Realizado por: Mafla, Carlos, 2023.

4.2. Pruebas escenario 1 Perfil 0

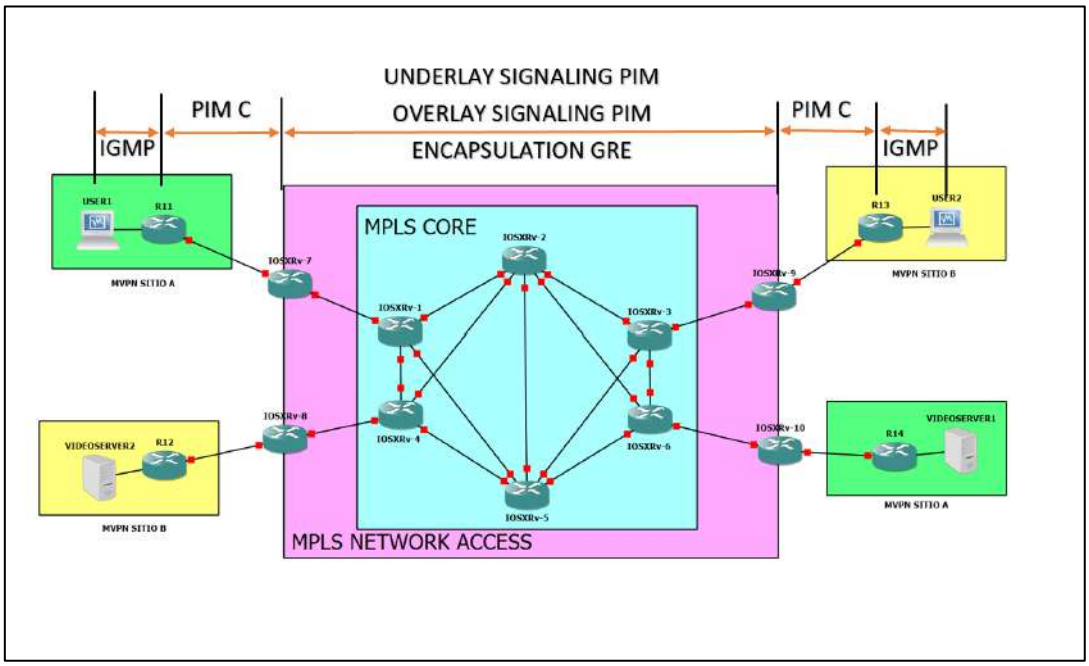


Ilustración 4-4: Escenario de pruebas con Perfil MVPN 0

Realizado por: Mafla, Carlos, 2022.

Se realizan pruebas de ancho de banda con la herramienta Jperf, enviando tráfico UDP desde SERVERA hasta CLIENTEA, permitiendo así verificar el ancho de banda que se puede utilizar para él envió de paquetes multicast y unicast. Se evidencia que el ancho de banda máximo que se

puede utilizar es de 30 Mbps, a este ancho de banda la pérdida de paquetes es menor, a diferencia de pruebas realizadas a mayores anchos de banda, cómo se puede evidenciar en las tablas 4-3, 4-4. 4-5, 4-6 y la Ilustración 4-3

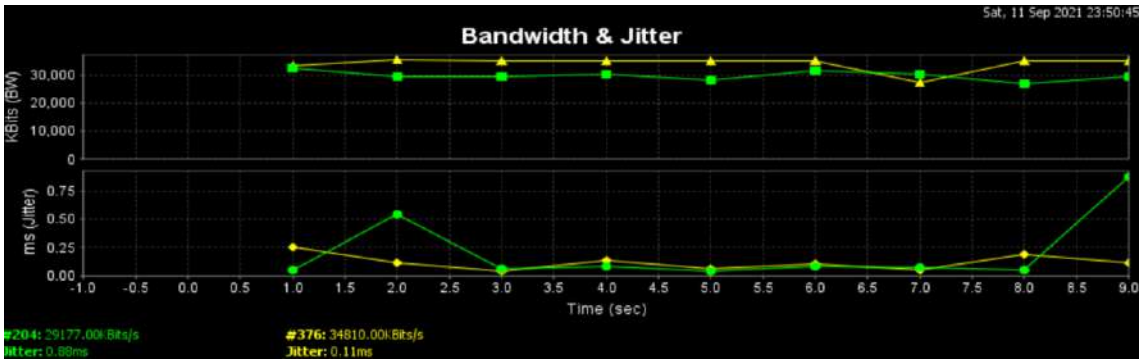


Ilustración 4-5: Comparación ancho de banda 30 Mbps y 35 Mbps Jperf

Realizado por: Mafla, Carlos, 2022.

Tabla 4-3: Pruebas ancho de banda 50Mbps con Jperf perfil 0

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	36962	250	55	456	38874
Máximo	52014	280	1014	3276	41842
Media	45150,6	268,5	657	2540(6,42%)	39560

Realizado por: Mafla, Carlos, 2022.

Tabla 4-4: Pruebas ancho de banda 30Mbps con Jperf perfil 0

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	27307	130	45	206	21666
Máximo	31164	170	116	2211	29246
Media	29267	145	96	1652(5,99%)	27564

Realizado por: Mafla, Carlos, 2022.

Tabla 4-5: Pruebas ancho de banda 20Mbps con Jperf perfil 0

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	19166	65	35	108	18920
Máximo	20358	89	64	1356	19347
Media	19675	76	58	958(5,06%)	19122

Realizado por: Mafla, Carlos, 2022.

Tabla 4-6: Pruebas ancho de banda 10Mbps con Jperf perfil 0

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	9376	23	20	65	8965
Máximo	9965	45	35	366	9257
Media	9645	39	29	265 (2,9%)	9122

Realizado por: Mafla, Carlos, 2022.

Cómo se puede observar en las tablas 4-3, 4-4, 4-5, 4-6, las pruebas de ancho de banda a 50Mbps y 30Mbps presentan una gran cantidad de paquetes perdidos, a diferencia de las pruebas de ancho de banda a 20Mbps y 10Mbps. Los valores de Jitter se muestran de forma similar, siendo muy elevados en las pruebas a 50Mbps y 30Mbps y se reducen en pruebas de ancho de banda a 20Mbps y 10Mbps.

Se genera tráfico UDP multicast y unicast con la herramienta Ostinato, el mismo que atraviesa la red del escenario planteado a una velocidad de 0,672Mbps. Al realizar 10 pruebas en el escenario planteado y utilizando el perfil Multicast VPN perfil 0 se obtuvieron los siguientes resultados.

Tabla 4-7: Generación de tráfico Multicast para el perfil MVPN 0

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9865	17	0,17%
Máximo	9983	135	1,35%
Media	9906,4	93,6	0,94%
Mediana	9887,5	112,5	1,14%
Desviación Estándar	39,86	36,23	

Realizado por: Mafla, Carlos, 2022.

Tabla 4-8: Generación de tráfico Unicast para el perfil MVPN 0

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9899	5	0,05%
Máximo	9915	38	0,38%
Media	9906,9	22,05	0,22%
Mediana	9907,5	24	0,24%
Desviación Estándar	5,12	10.43	

Realizado por: Mafla, Carlos, 2023

Cómo se puede observar en las tablas 4-7 y 4-8 el porcentaje de pérdida de paquetes es más alto que en los resultados de la transmisión del perfil 1, se observa también que la perdida de paquetes en la transmisión unicast es menor que en la transmisión multicast. Los paquetes generados con la herramienta ostinato son transmitidos por el puerto 222, y son enviados mediante transmisión multicast a la dirección 232.1.2.3, cómo se puede observar en la Ilustración 4-6. Para la generación de tráfico unicast se realiza el envío de información desde la máquina virtual SERVERB mediante la herramienta ostinato y hacia la dirección 192.168.33.2 correspondiente al CLIENTEB.

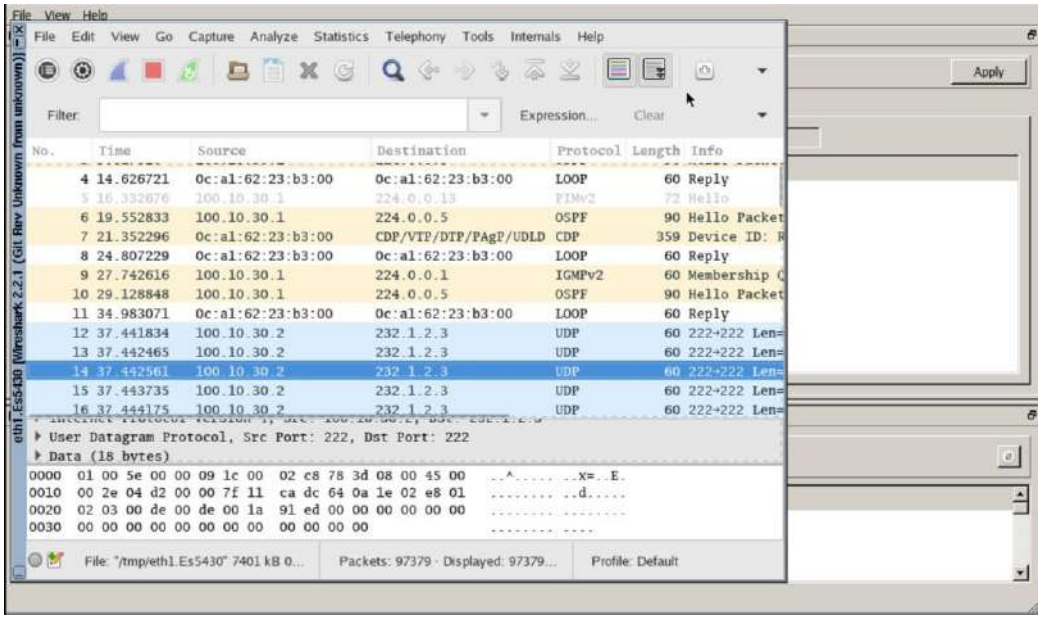


Ilustración 4-6: Generación de tráfico mediante la herramienta ostinato

Realizado por: Mafla, Carlos, 2023.

4.3. Pruebas escenario 1 Perfil 1

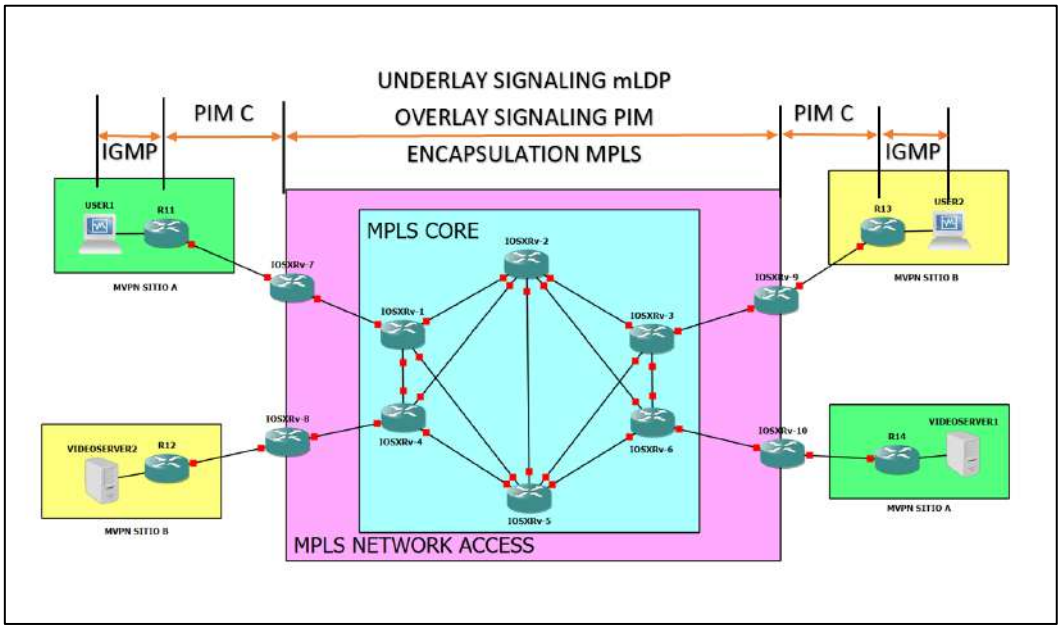


Ilustración 4-7: Escenario de pruebas con Perfil MVPN 1

Realizado por: Mafla, Carlos, 2022.

Se realizan pruebas de ancho de banda con la herramienta Jperf, enviando tráfico UDP desde SERVERA hasta CLIENTEA, para verificar el ancho de banda que se puede utilizar para realizar él envió de paquetes multicast y unicast. Se evidencia que el ancho de banda máximo que se puede utilizar es de 10Mbps, a este ancho de banda la pérdida de paquetes es mínima a diferencia de pruebas realizadas a mayores anchos de banda, cómo se puede evidenciar en las tablas 4-9, 4-10, 4-11, 4-12.

Tabla 4-9: Pruebas ancho de banda 50Mbps con Jperf perfil 1

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total, Paquetes
Mínimo	38536	191	35	342	38232
Máximo	51822	228	898	2992	41764
Media	46123	201,5	497	2140(5,44%)	39288

Realizado por: Mafla, Carlos, 2022.

Tabla 4-10: Pruebas ancho de banda 30Mbps con Jperf Perfil 1

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total, Paquetes
Mínimo	26223	129	55	219	22124
Máximo	30924	182	136	2182	29140
Media	28462	145	87	1754(6,35%)	27621

Realizado por: Mafla, Carlos, 2022.

Tabla 4-11: Pruebas ancho de banda 20Mbps con Jperf Pefil 1

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	19232	69	28	119	18834
Máximo	21359	98	72	1418	19325
Media	20198	89	66	1058(5,54%)	19102

Realizado por: Mafla, Carlos, 2022.

Tabla 4-12: Pruebas ancho de banda 10Mbps con Jperf Perfil 1

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	9364	14	16	58	8958
Máximo	9962	28	28	296	9261
Media	9616	24	22	175,4(1,92%)	9148

Realizado por: Mafla, Carlos, 2022.

Cómo se puede observar en las tablas 4-9, 4-10, 4-11, 4-12 las pruebas de ancho de banda a 50Mbps y 30Mbps presentan una gran cantidad de paquetes perdidos, a diferencia de las pruebas de ancho de banda a 20Mbps y 10Mbps. Los valores de Jitter se muestran de forma similar, siendo son muy elevados en las pruebas de 50 y 30Mbps.

Se genera tráfico UDP multicast y unicast con la herramienta Ostinato, el mismo que atraviesa la red del escenario planteado a una velocidad de 0,672Mbps. Al realizar 10 pruebas en el escenario planteado y utilizando el perfil Multicast VPN perfil 1 se obtuvieron los siguientes resultados.

Tabla 4-13: Generación de tráfico Multicast para el perfil MVPN 1

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9862	9	0,09%
Máximo	9870	51	0,51%
Media	9863,4	30,5	0,30%
Mediana	9862	28,5	0,28%
Desviación Estándar	14,56	15,83	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-14: Generación de tráfico Unicast para el perfil MVPN 1

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9890	6	0,06%
Máximo	9922	41	0,41%
Media	9905,35	23,02	0,23%
Mediana	9905	23,5	0,24%
Desviación Estándar	8,73	10,66	

Realizado por: Mafla, Carlos, 2023.

Cómo se puede observar en la tabla 4-13 y 4-14 el porcentaje de pérdida de paquetes es muy pequeño, en comparación a la misma prueba realizada con el perfil 0, el porcentaje de pérdida es menor. Se observa también que el resultado de paquetes perdidos en la transmisión unicast es menor, con respecto al obtenido en la transmisión multicast.

Los paquetes generados con la herramienta Ostinato son transmitidos por el puerto 222, y son enviados mediante transmisión multicast a la dirección 232.1.2.3. Para la generación de tráfico unicast se realiza el envío de información desde la máquina virtual SERVERB mediante la herramienta ostinato y hacia la dirección 192.168.22.3 correspondiente a CLIENTEB.

4.4. Pruebas escenario 1 Perfil 11

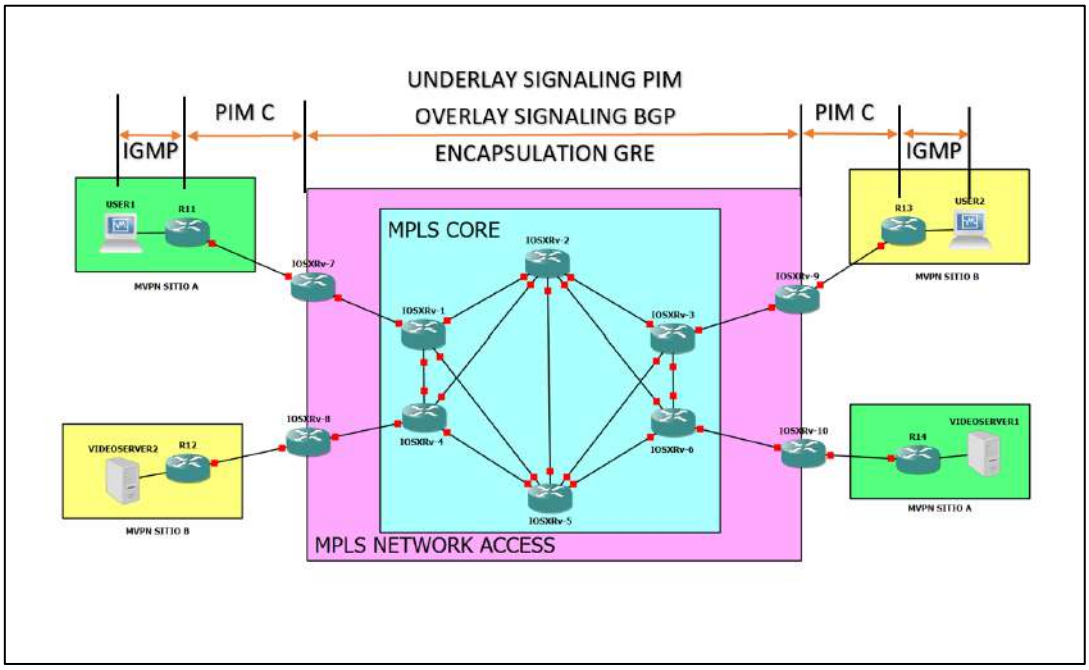


Ilustración 4-8: Escenario de pruebas con Perfil MVPN 11

Realizado por: Mafla, Carlos, 2022.

Se realizan pruebas de ancho de banda con la herramienta Jperf, enviando tráfico UDP desde SERVERA hasta CLIENTEA, para verificar el ancho de banda que se puede utilizar para él envió de paquetes multicast y unicast. Se evidencia que el ancho de banda máximo que se puede utilizar es de 10Mbps, a este ancho de banda la pérdida de paquetes es mínima a diferencia de pruebas realizadas a mayores anchos de banda, cómo se puede evidenciar en las tablas 4-15, 4-16, 4-17, 4-18.

Tabla 4-15: Pruebas ancho de banda 50Mbps con Jperf perfil 11

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	36962	250	55	456	38874
Máximo	52014	280	1014	3276	41842
Media	45150,6	268,5	657	2540(6,42%)	39560

Realizado por: Mafla, Carlos, 2022.

Tabla 4-16: Pruebas ancho de banda 30Mbps con Jperf perfil 11

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	26223	129	55	219	22124
Máximo	30924	182	136	2182	29140
Media	28462	145	87	1754(6,35%)	27621

Realizado por: Mafla, Carlos, 2022.

Tabla 4-17: Pruebas ancho de banda 20Mbps con Jperf perfil 11

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	19232	69	28	119	18834
Máximo	21359	98	72	1418	19325
Media	20198	89	66	1058(5,54%)	19102

Realizado por: Mafla, Carlos, 2022.

Tabla 4-18: Pruebas ancho de banda 100Mbps con Jperf perfil 11

	Ancho de banda (Kbps)	Latencia(ms)	Jitter (ms)	Paquetes perdidos	Total Paquetes
Mínimo	9476	29	28	83	8972
Máximo	9929	62	49	428	9193
Media	9588	48	37	307 (3,3%)	9092

Realizado por: Mafla, Carlos, 2022.

Cómo se puede observar en las tablas 4-15, 4-16, 4-17, 4-18, las pruebas de ancho de banda a 50Mbps y 30Mbps presentan una gran cantidad de paquetes perdidos, a diferencia de las pruebas de ancho de banda a 20Mbps y 10Mbps. Los valores de Jitter se muestran de forma similar, siendo muy elevados en las pruebas a 50Mbps y 30Mbps y se reducen en pruebas de ancho de banda a 20Mbps y 10Mbps.

Se genera tráfico UDP multicast y unicast con la herramienta Ostinato, el mismo que atraviesa la red del escenario planteado a una velocidad de 0,672Mbps. Al realizar 10 pruebas en el escenario planteado y utilizando el perfil Multicast VPN perfil 11 se obtuvieron los siguientes resultados.

Tabla 4-19: Generación de tráfico Multicast para el perfil MVPN 11

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9855	14	0,14%
Máximo	9986	145	1,45%
Media	9922,6	77,4	0,78%
Mediana	9930	70	0,70%
Desviación Estándar	44,05	39,2	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-20: Generación de tráfico Unicast para el perfil MVPN 11

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9896	6	0,05%
Máximo	9919	43	0,37%
Media	9908,2	23,5	0,24%
Mediana	9908,5	24,5	0,23%
Desviación Estándar	5,32	14,15	

Realizado por: Mafla, Carlos, 2023.

Cómo se puede observar en la tabla 4-19 y 4-20 el porcentaje de pérdida de paquetes es muy pequeño, en comparación a la misma prueba realizada con el perfil 0 y el perfil 1 el porcentaje de pérdida es mayor.

Los paquetes generados con la herramienta ostinato son enviados y recibidos por el puerto 222, y son enviados mediante transmisión Multicast a la dirección 232.1.2.3. Para la generación de tráfico unicast se realiza el envío de información desde la máquina virtual SERVERB mediante la herramienta ostinato y hacia la dirección 192.168.22.3 correspondiente a CLIENTEB.

Los resultados muestran que el perfil MVPN que menor pérdida de paquetes presenta es el perfil 1, el mismo utiliza señalización superpuesta mLPD, señalización subyacente PIM y encapsulación MPLS. Debido a su rendimiento el perfil 1 será utilizado para la realización de las pruebas de emisión de video multicast con la herramienta VLC.

4.5. Pruebas de generación de tráfico unicast vs multicast con 5 clientes

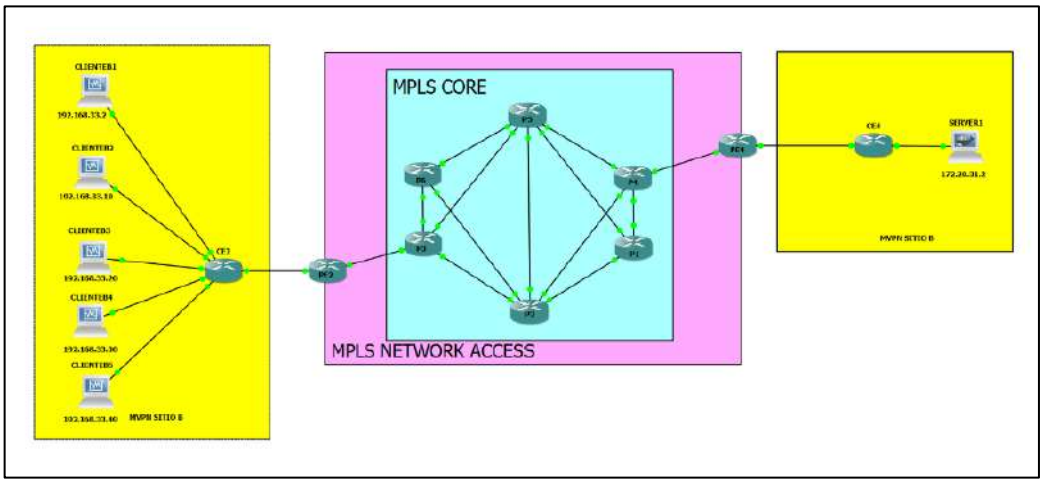


Ilustración 4-9: Pruebas generación de tráfico unicast y multicast 5 clientes

Realizado por: Carlos Mafla 2023

Debido a que se obtuvo resultados similares en la generación de tráficos multicast y unicast con un servidor y un cliente se realizan pruebas con el perfil 1 y con una cantidad de 5 clientes en total.

Tabla 4-21: Generación de tráfico Multicast para el perfil 1 CLIENTE1B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9865	39	0,39%
Máximo	9888	103	1,04%
Media	9876,3	72,7	0,74%
Mediana	9878	76,5	0,77%
Desviación Estándar	7,66	24,91	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-22: Generación de tráfico Multicast para el perfil 1 CLIENTE2B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9863	35	0,35%
Máximo	9885	89	0,90%
Media	9872,5	66,2	0,67%
Mediana	9872,5	74	0,75%

Desviación Estándar	7,59	21,20	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-23: Generación de tráfico Multicast para el perfil 1 CLIENTE3B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9867	29	0,29%
Máximo	9891	68	0,69%
Media	9880,2	50,2	0,51%
Mediana	9882,5	53,5	0,54%
Desviación Estándar	9,44	14,19	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-24: Generación de tráfico Multicast para el perfil 1 CLIENTE4B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9821	24	0,24%
Máximo	9891	61	0,62%
Media	9864,2	54,5	0,67%
Mediana	9865	56	0,75%
Desviación Estándar	6,83	13,8	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-25: Generación de tráfico Multicast para el perfil 1 CLIENTE5B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9865	23	0,23%
Máximo	9902	55	0,55%
Media	9890,2	40,8	0,41%
Mediana	9890	41,5	0,54%
Desviación Estándar	9,44	12,6	

Realizado por: Mafla, Carlos, 2023**.**

En el servidor se realiza el envío de paquetes hacia la dirección multicast 232.1.2.3 mediante la herramienta ostinato y por el puerto 222, se genera un solo stream que viaja hacia los clientes mediante la tecnología multicast VPN del perfil 1.

Para la generación de tráfico unicast se realiza el envío de información desde la máquina virtual SERVERB mediante la herramienta ostinato, con un stream por cada cliente al que se desea enviar la información, se configura cada stream con la dirección ip hacia la que va dirigido y se obtuvieron los siguientes resultados.

Tabla 4-26: Generación de tráfico Unicast para el perfil 1 CLIENTE1B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9893	34	0,34%
Máximo	9916	93	0,94%
Media	9903,5	67,04	0,68%
Mediana	9906	82	0,82%
Desviación Estándar	5,57	23,1	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-27: Generación de tráfico Unicast para el perfil 1 CLIENTE2B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9888	33	0,33%
Máximo	9897	95	0,96%
Media	9894,7	68,5	0,69%
Mediana	9897	72	0,73%
Desviación Estándar	3,4	19,20	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-28: Generación de tráfico Unicast para el perfil 1 CLIENTE3B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9892	33	0,33%
Máximo	9918	88	0,88%
Media	9932,4	60,4	0,61%
Mediana	9918	62,5	0,63%
Desviación Estándar	11,12	20,14	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-29: Generación de tráfico Unicast para el perfil 1 CLIENTE4B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9898	32	0,32%
Máximo	9907	94	0,95%
Media	9926,8	58,2	0,59%
Mediana	9924	59	0,59%
Desviación Estándar	11,12	20,14	

Realizado por: Mafla, Carlos, 2023.

Tabla 4-30: Generación de tráfico Unicast para el perfil 1 CLIENTE5B

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9892	33	0,33%
Máximo	9918	88	0,89%
Media	9932,4	60,4	0,61%
Mediana	9918	62,5	0,63%
Desviación Estándar	11,12	20,14	

Realizado por: Mafla, Carlos, 2023.

Se observó que los valores de porcentaje de paquetes perdidos se mantienen en las pruebas realizadas con los 5 clientes en la generación de tráfico Unicast, en cambio estos porcentajes de pérdida van disminuyendo paulatinamente en la transmisión Multicast.

Tabla 4-31: Generación de tráfico Multicast GLOBAL

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	9865	34,3	0,34%
Máximo	9988	86,7	0,87%
BW	0,671Mbps	10Mbps	6,71%

Realizado por: Mafla, Carlos, 2023.

Tabla 4-32: Generación de tráfico Unicast GLOBAL

	Paquetes generados	Paquetes perdidos	Porcentaje de perdida de paquetes
Mínimo	49470	236	0,48%
Máximo	49565	565	1,13%
BW	3,35Mbps	10Mbps	33,5%

Realizado por: Mafla, Carlos, 2023.

Al realizar una comparación con la sumatoria del total de paquetes generados en cada una de las generaciones de tráfico se observó que la cantidad de paquetes enviados en la transmisión unicast es mucho mayor a la cantidad de paquetes enviados en la transmisión multicast.

También se observó que el porcentaje de pérdida de paquetes en la transmisión unicast va ascendiendo conforme se aumenta el número de clientes que solicitan la transmisión.

4.6. Pruebas emisión de video en transmisión mediante la herramienta VLC

Se realizan pruebas de emisión de video con la herramienta VLC media player, para la transmisión multicast desde la máquina virtual SERVER A se emiten cada uno de los videos con diferentes resoluciones y características mostradas en la tabla 11-2. La emisión utiliza el protocolo RTP y la dirección multicast 232.1.2.3. Desde la máquina virtual CLIENTE A se recepta la transmisión multicast gracias a la herramienta VLC, esta herramienta permite también mostrar las estadísticas

de la emisión, como se muestra en la Ilustración 9-3, las mismas que serán utilizadas para realizar el respectivo análisis.

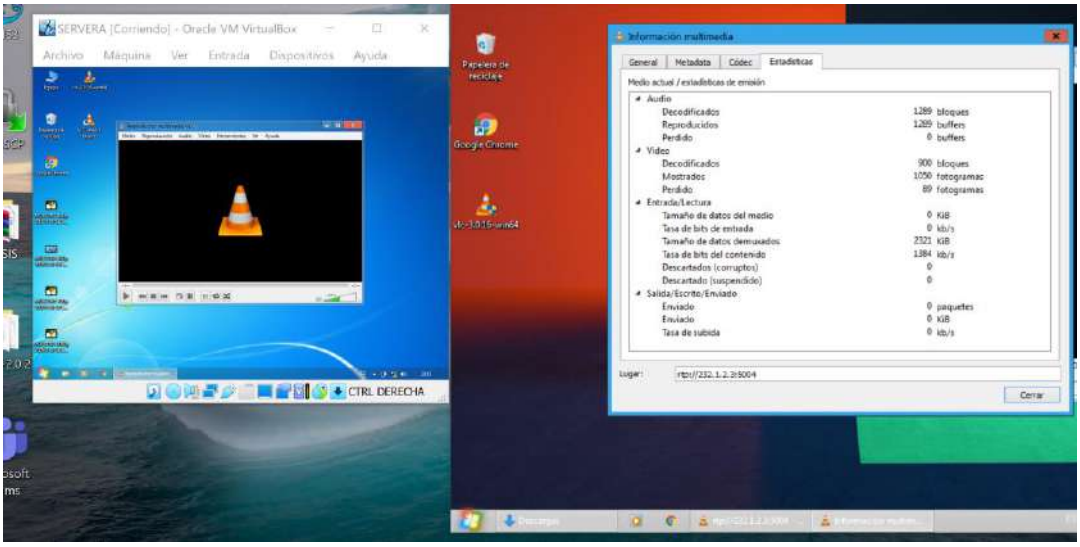


Ilustración 4-10: Emisión y recepción multicast mediante VLC media player

Realizado por: Mafla, Carlos, 2022.

Para la transmisión unicast, desde la máquina virtual SERVERB se emiten cada uno de los videos con las diferentes resoluciones y características mostradas en la tabla 3-10. La emisión utiliza el protocolo HTTP al ser una emisión unicast, desde la máquina CLIENTEB se abre el flujo de red proveniente desde la ip del servidor 172.20.31.2, cómo se muestra en la Ilustración 4-10.

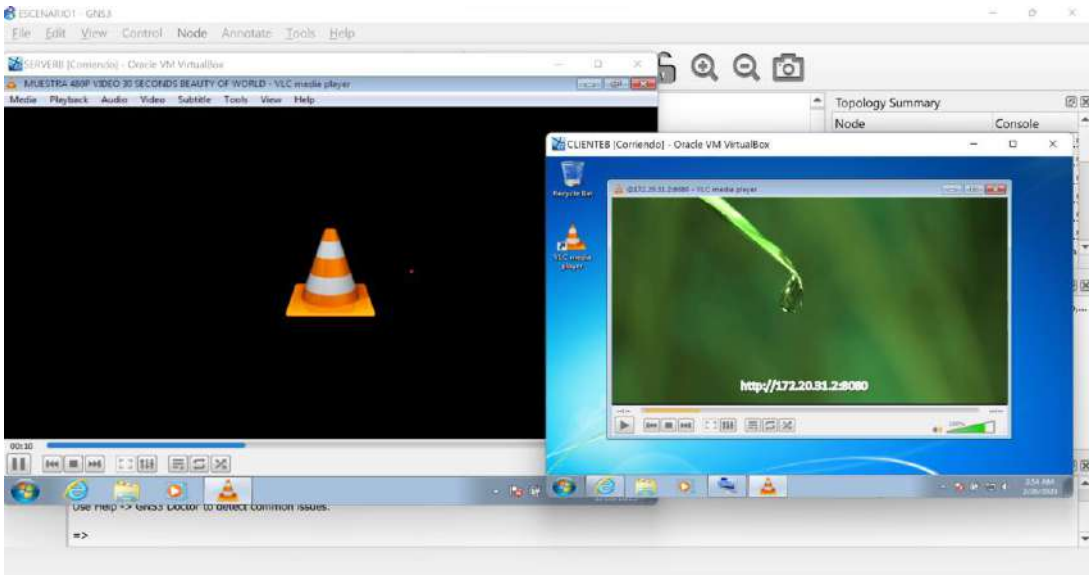


Ilustración 4-11: Emisión y recepción unicast mediante VLC media player

Realizado por: Mafla, Carlos, 2023.

4.6.1. Emisión de video 360p

La emisión de video multicast a una resolución de 360p presenta muy pocos buffers de información de audio perdidos, y los fotogramas de video perdidos son mínimos también, tal como se puede observar en las ilustraciones, debido a esto no se observa pérdida de calidad en la reproducción del video en las máquinas virtuales de los clientes. Se observa que existen menos buffers y fotogramas perdidos en la emisión unicast.

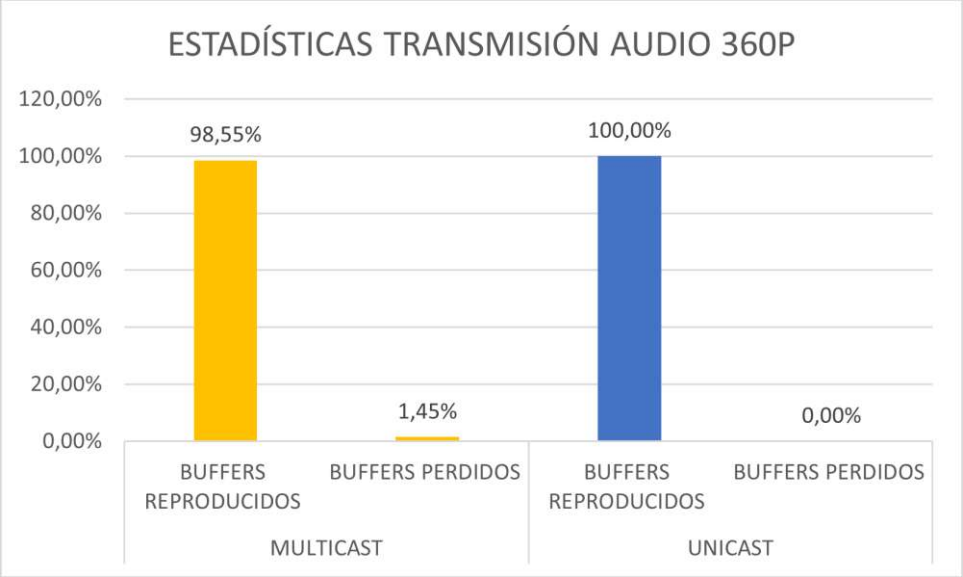


Ilustración 4-12: Estadísticas de transmisión de audio a 360p

Realizado por: Mafla, Carlos, 2023.

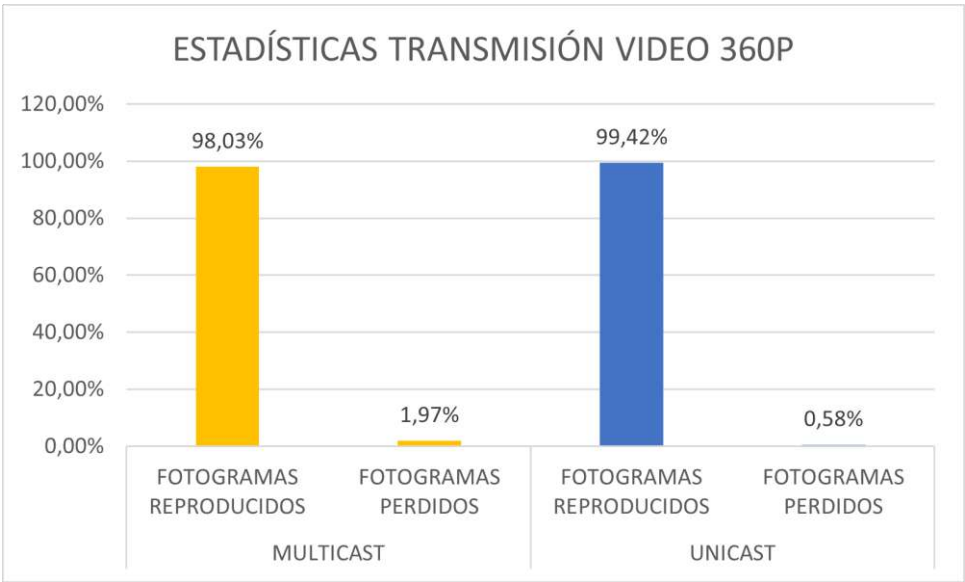


Ilustración 4-13: Estadísticas de transmisión de video a 360p

Realizado por: Mafla, Carlos, 2023.

4.6.2. Emisión de video 480p

La emisión de video multicast a una resolución de 480p presenta muy pocos buffers de información de audio perdidos, y los fotogramas de video perdidos son pocos también, tal como se puede observar en las ilustraciones, debido a esto no se observa pérdida de calidad en la reproducción del video en las máquinas virtuales de los clientes. Se empieza a observar una mayor diferencia en el porcentaje de fotogramas perdidos en la transmisión unicast con respecto a la transmisión multicast.

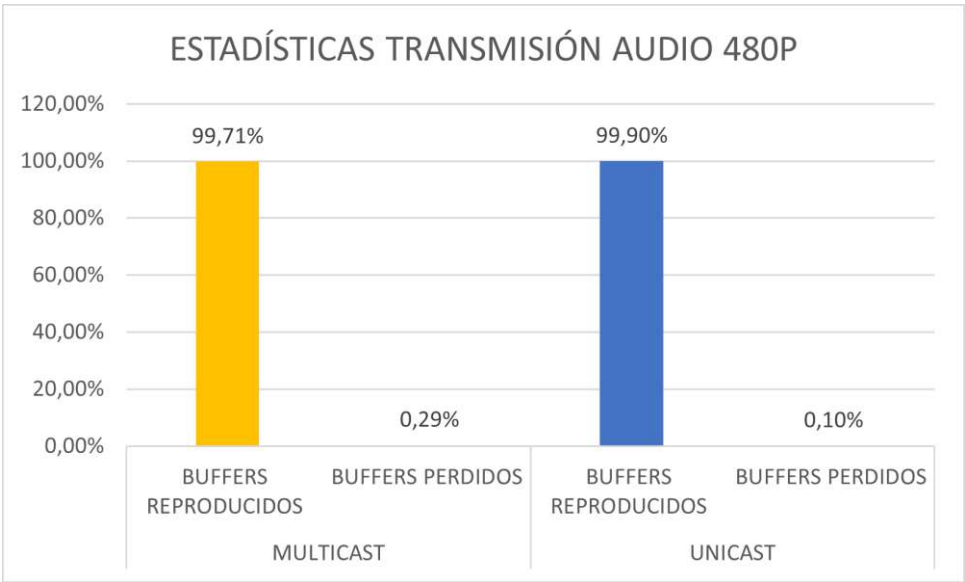


Ilustración 4-14: Estadísticas de transmisión de audio a 480p

Realizado por: Mafla, Carlos, 2023.

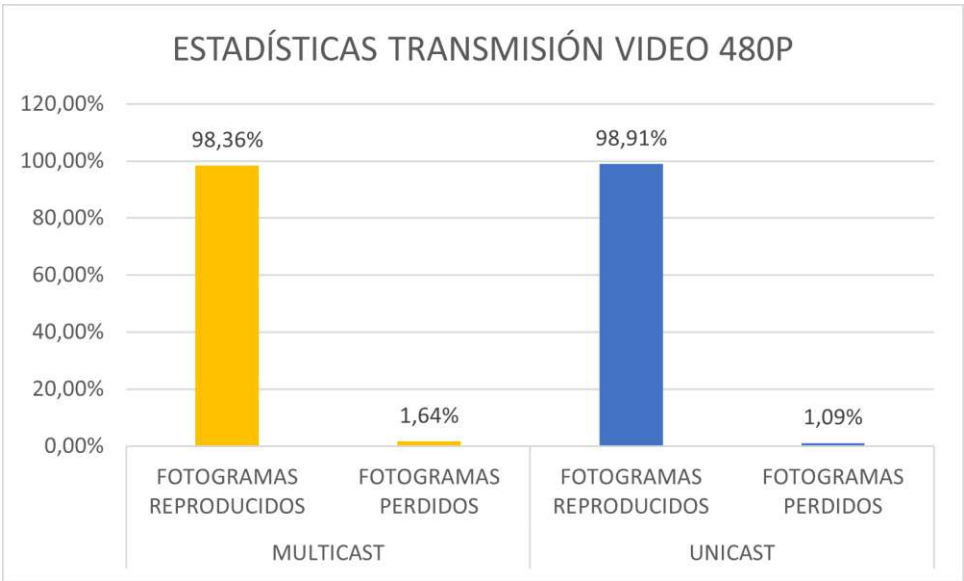


Ilustración 4-15: Estadísticas de transmisión de video a 480p

Realizado por: Mafla, Carlos, 2023.

4.6.3. Emisión de video 720p

La emisión de video multicast a una resolución de 720p presenta buffers de información de audio perdidos un tanto altos, los fotogramas de video perdidos son bajos, representando un 3% con respecto a todos los fotogramas mostrados. Al presentar una cantidad de fotogramas enviados muy alta no se observa pérdida de calidad en la reproducción del video en las máquinas virtuales de los clientes. Se mantiene la tendencia y existe menos pérdidas tanto en buffers de audio y fotogramas de video.

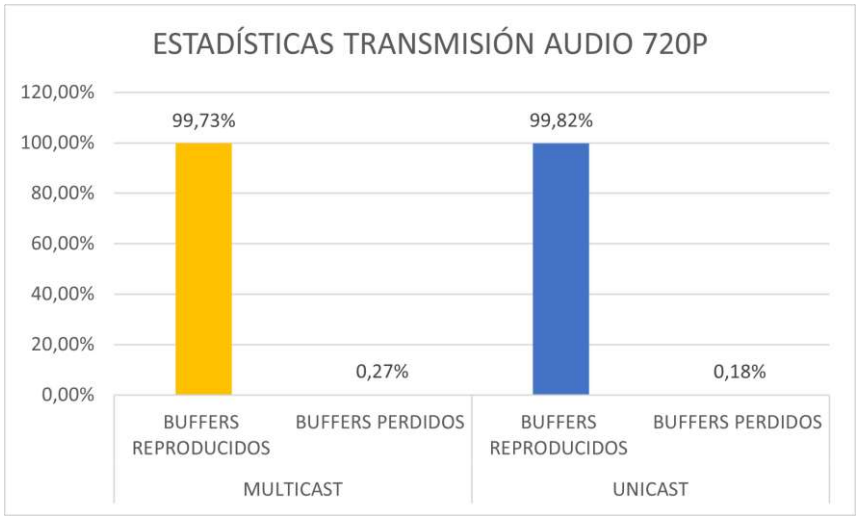


Ilustración 4-16: Estadísticas de transmisión de video a 720p

Realizado por: Mafla, Carlos, 2023.

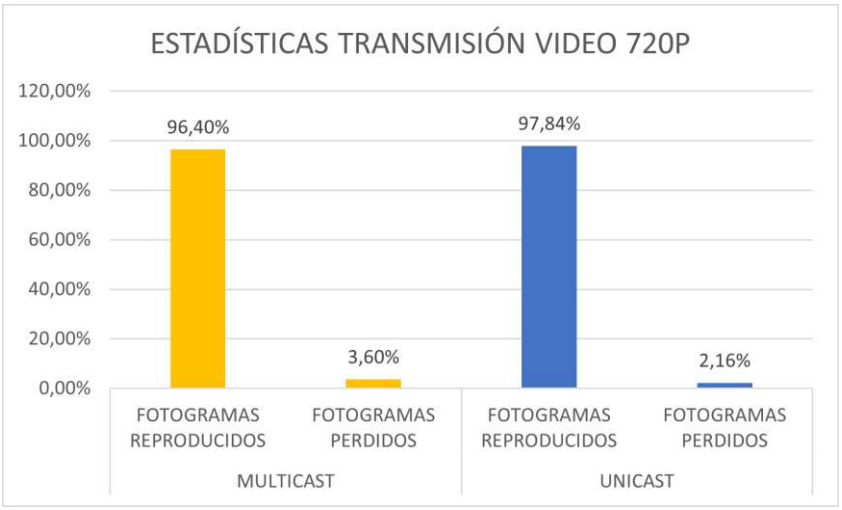


Ilustración 4-17: Estadísticas de transmisión de audio a 720p

Realizado por: Mafla, Carlos, 2023.

4.6.4. Emisión de video 1080p

La emisión de video multicast a una resolución de 1080p presenta un número elevado de fotogramas de video perdidos, los buffers de audio perdidos son bajos. Esto se ve evidenciado al momento de visualizar el video, el mismo empieza a mostrar cortes y pérdida de la calidad de imagen. En la transmisión unicast se notan menos problemas de calidad de señal al momento de la reproducción.

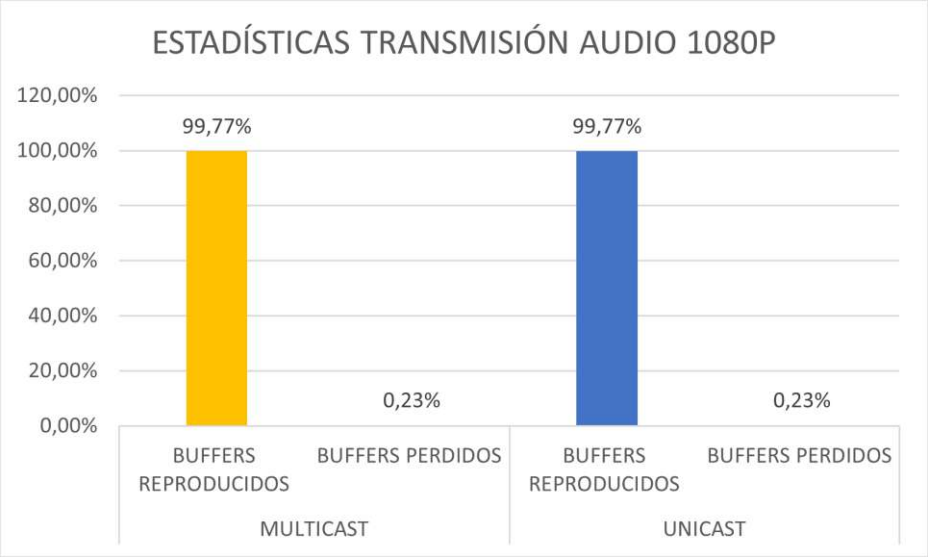


Ilustración 4-18: Estadísticas de transmisión de audio 1080p

Realizado por: Mafla, Carlos, 2023.

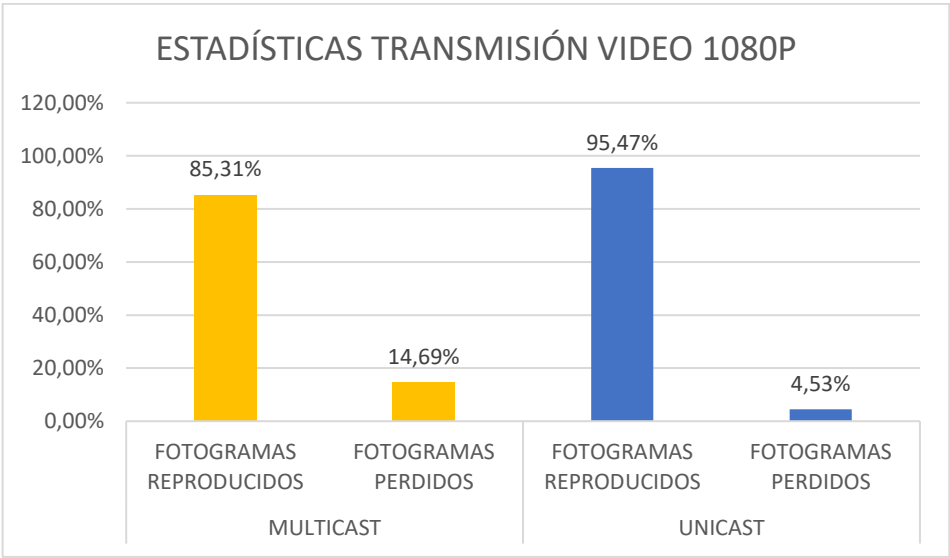


Ilustración 4-19: Estadísticas de transmisión de video a 1080p

Realizado por: Mafla, Carlos, 2023.

CONCLUSIONES

- Se evidenció que Multicast VPN en redes MPLS es una tecnología que utiliza varios protocolos para la transferencia de información, estos se utilizan de diferentes maneras en las distintas marcas de dispositivos para lograr que la información se transmita de manera eficiente haciendo uso de diferentes señalizaciones y encapsulamientos que permiten manejar de manera óptima el tráfico generado dentro de una red MPLS.

- Se observó que existen varios parámetros de rendimiento y calidad de servicio, tales como: latencia, jitter, pérdida de paquetes y ancho de banda; los mismos que presentan una serie de valoraciones de percepción por parte del usuario final y ayuda a evidenciar el funcionamiento de la forma de transmisión que se utilice.

- Se diseñó el prototipo de pruebas para la tecnología Multicas VPN, el mismo que a lo largo del estudio debió ser modificado para obtener resultados más precisos a la hora de transmitir tráficos unicast y multicast, permitiendo así observar las principales diferencias y ventajas que presenta cada uno de estos tipos de transmisión.

- Se observó que la encapsulación MPLS presenta mejores resultados para la transmisión de paquetes UDP multicast que la encapsulación GRE. Al utilizar el perfil 1 que ofrece encapsulación MPLS se obtuvo un porcentaje 0,05% menor de pérdida de paquetes. También se observó que la transmisión multicast maneja de una manera más eficiente la información que se desea transmitir a un número alto de clientes, sin embargo, se pudo evidenciar que la transmisión unicast funciona de manera ideal cuando la transmisión es de uno a uno.

- La tecnología Multicast VPN permite que un mismo flujo de datos sea transmitido a múltiples destinatarios al mismo tiempo, lo que es especialmente útil en entornos de transmisión de vídeo en directo, conferencias en línea y otras aplicaciones que requieren la distribución eficiente de contenido a un gran número de usuarios, llegando a ser similar a cuando se realiza una transmisión unicast.

RECOMENDACIONES

- Simular en el escenario generaciones de tráfico mucho más realistas, para esto se puede hacer uso de generadores de tráfico mucho más robustos, que ofrecen prestaciones que asemejan mucho más el tráfico generado al tráfico real en una red, uno de los mayores inconvenientes para el uso de estos generadores es la cantidad de recursos que necesitan.

- Si se desea realizar pruebas de emisión de video multicast a resoluciones mucho más altas como 2k, 4k o 8k es necesario la utilización de equipos físicos, ya que las máquinas virtuales simuladas no permiten la emisión de este tipo de tráfico debido a su baja memoria de video y también a que no cuentan con una tarjeta gráfica dedicada.

- Antes de la implementación de perfiles Multicast VPN, definir estrictamente el tráfico multicast que va a ser generado, ya que existen perfiles Multicast VPN que son idóneos para diversos tipos de tráficos, cómo es el caso de la señalización superpuesta P2MP TE que es la más adecuada para la emisión de video desde uno hacia varios puntos.

- Las pruebas realizadas consumieron el 100% de los recursos prestados por el computador en el que se realizaron todas las simulaciones, ocasionando varios fallos del sistema y errores de funcionamiento, debido a esto se recomienda dimensionar el escenario a ser simulado, todos los equipos que se van a utilizar en el mismo y los recursos que la máquina de simulación ofrece.

GLOSARIO

AS	AUTONOMOS SISTEM
BGP	BORDER GATEWAY PROTOCOL
CPU	UNIDAD CENTRAL DE PROCESAMIENTO
EGP	EXTERIOR GATEWAY PROTOCOL
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
IETF	INTERNET ENGINEERING TASK FORCE
IGMP	INTERNET GROUP MANAGEMENT PROTOCOL
IGP	INTERIOR GATEWAY PROTOCOL
IGRP	INTERIOR GATEWAY ROUTING PROTOCOL
IOS	INTERNET OPERATING SYSTEM
IP	PROTOCOLO DE INTERNET
IPV4	PROTOCOLO DE INTERNET VERSION 4
IS-IS	INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM
ISP	INTERNET SERVICE PROVIDER
ITU	UNIÓN INTERNACIONAL DE TELECOMUNICACIONES
LAN	LOCAL AREA NETWORK
MPEG	MOVING PICTURE EXPERTS GROUP
MPLS	MULTIPROTOCOL LABEL SWITCHING
OSI	OPEN SYSTEM INTERCONNECTION
OSPF	OPEN SHORTEST PATH FIRST
PIM SM-DM	PIM SPARSE MODE – DENSE MODE
PIM	PROTOCOL INDEPENDENT MULTICAST
PIM-DM	PIM – DENSE MODE
PIN-SM	PIM – SPARSE MODE
QoS	CALIDAD DE SERVICIO
RAM	RANDOM ACCESS MEMORY
RP	RENDEZVOUS POINT
RPM	REVERSE PATH MULTICASTING
RTP	REAL TIME PROTOCOL
TCP	TRANSMISSION CONTROL PROTOCOL
TTL	TIME TO LIVE
UDP	USER DATAGRAM PROTOCOL
VPN	VIRTUAL PRIVATE NETWORK

BIBLIOGRAFÍA

3CX,. ¿Qué es RTCP – 2018. Real Time Transport Protocol? Online. 2018. [Accessed 13 September 2021]. Retrieved from: https://www.3cx.es/voip-sip/rtcp/

ADAMS, ANDREW, NICHOLAS, JONATHAN AND SIADAK, WILLIAM, *Protocol independent multicast-dense mode (PIM-DM-*2004*.): Protocol specification (revised)*.

AUDET, FRANCOIS, JENNINGS, CULLEN, PERREAULT, S, YAMAGATA, I, MIYAKAWA, S, NAKAGAWA, A, ASHIDA, H, PENNO, R, BOUCADAIR, M AND SIVAKUMAR, S. Network address translation (NAT) behavioral requirements for unicast UDP. *Network*. 2007.

BOLLAPRAGADA, VIJAY, KHALID, MOHAMED AND WAINNER, SCOTT, *IPSec VPN Design*. Cisco Press. 2005. ISBN 0134384164.

BYCHOK, ALEXANDER. Comparación de protocolos de transmisión: RTMP, WebRTC, FTL, SRT - Blog de Restream. Online. May 2020. [Accessed 13 September 2021]. Retrieved from: https://restream.io/blog/streaming-protocols/

CAMPO, WILMAR, CHANCHI, GABRIEL AND CAMACHO, MARTA. Uso de técnicas de emulación en la construcción de un modelo de tráfico para un servicio multimedia. *SciELO*. Online. June 2017. Vol. 18, no. 2. [Accessed 13 September 2021]. Retrieved from: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-77432017000200209

CASTILLO, COSIOS, RICHARD, EDUARDO, LOACHAMÍN, SIMBAÑA AND XAVIER, WILSON. *Estudio y diseño de redes virtuales privadas (VPN) basadas en tecnología MPLS*. . 2004. QUITO/EPN/2004.

CASTRILLO, DIEGO, ESTUPIÑÁN, OSCAR AND GUARDIA, MARÍA LUISA GARCÍA. El impacto del vídeo on-line en la industria de televisión de pago en España. *Derecom*. 2011. No. 7, pp. 9.

CASTRO ULLAURI, EMILENI SOLANGE. Diseño y simulación de una red MPLS para interconectar estaciones remotas utilizando el emulador GNS3. Online. 2015. [Accessed 2 September 2021]. Retrieved from:

http://dspace.ups.edu.ec/handle/123456789/10297

CISCO, THE AND INTERNET, ANNUAL. Cisco Annual Internet Report (2018–2023). *Computer Fraud & Security*. 2020. Vol. 2020, no. 3, pp. 4–4. DOI 10.1016/s1361-3723(20)30026-9.

CISET. Buffer, memoria temporal. Online. 2021. [Accessed 13 September 2021]. Retrieved from: https://www.ciset.es/glosario/417-buffer?dt=1631561429405

CONDE, LUÍS ENRIQUE. Conde L. Impactos de la implementación de las Content Delivery Network. Revista TONO. Etecsa. Año 2016. - Buscar con Google. Online. January 2017. [Accessed 20 May 2019]. Retrieved from: http://www.revistatonoetecsa.cu/sites/default/files/pdf_articulo/evoluciondelascontent.pdf

DIBILDOX, LM. Investigación de redes VPN con tecnología MPLS. Online. 2006. [Accessed 4 August 2021]. Retrieved from: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/

ECURED. Buffer - EcuRed. Online. 2018. [Accessed 13 September 2021]. Retrieved from: https://www.ecured.cu/Buffer

EPROSIMA. RTPS. Online. 2016. [Accessed 13 September 2021]. Retrieved from: https://www.eprosima.com/index.php/resources-all/whitepapers/rtps

FENNER, BILL, HANDLEY, MARK, KOUVELAS, ISIDOR AND HOLBROOK, HUGH. Protocol independent multicast-sparse mode (PIM-SM): protocol specification (revised). . 2006.

FERNANDEZ, YUBAL. Qué es el Bitrate de un vídeo y cómo saberlo en Windows 10 y macOS. Online. 2017. [Accessed 13 September 2021]. Retrieved from: https://www.xataka.com/basics/que-es-el-bitrate-de-un-video-y-como-saberlo-en-windows-10-y-macos

GARCIA, MARTHA ODILIA TAPASCO. *MPLS, el presente de las redes IP*. . 2008. Universidad Tecnológica de Pereira. Facultad de Ingenierías Eléctrica ….

GHEIN, LUC DE. mVPN Deployment Models. *Cisco live*. 2019.

GONZÁLES MORALES, ALEXANDRO. Redes privadas virtuales. . 2006.

HAMZEH, KORY, PALL, GRUEEP, VERTHEIN, WILLIAM, TAARUD, JEFF, LITTLE, W AND ZORN, GLEN. *Point-to-point tunneling protocol (PPTP)*. 1999

HOLBROOK, HUGH AND CAIN, BRAD,. *Source-specific multicast for IP*. 2006.

INDEX, CISCO VISUAL NETWORKING. Forecast and Trends, 2017–2022. *Cisco Systems*. 2018. pp. 1–7.

JUNIPER NETWORKS. Multiprotocol BGP MVPNs Overview - TechLibrary - Juniper Networks. *Descripción general de MVPN multiprotocolo BGP*. Online. 3 June 2020. [Accessed 25 September 2020]. Retrieved from: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/mcast-mvpn-overview.html

KRINGS, EMILY. FPS for Live Streaming: Advanced Guide to Video Frame Rates in 2021. Online. June 2021. [Accessed 13 September 2021]. Retrieved from: https://www.dacast.com/blog/frame-rate-fps/

LEHMANN JR, L CURTIS AND DYE, THOMAS A. *Applying multicast protocols and VPN tunneling techniques to achieve high quality of service for real time media transport across IP networks*. . 2 July 2013. Google Patents.

LINUBE. Latencia: qué es, cómo se mide y cómo puedes reducirla - Blog de Linube. Online. 2017. [Accessed 13 September 2021]. Retrieved from: https://linube.com/blog/latencia-ping-que-es/

LUC DE GHEIN. mVPN Profiles - Cisco. *mVPN Profiles ID 116321*. Online. 2 August 2013. [Accessed 25 September 2020]. Retrieved from: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/multicast-vpn/116321-technote-mvpn-00.html

MARTÍNEZ YELMO, ISAÍAS, LARRABEITI LÓPEZ, DAVID, SOTO CAMPOS, IGNACIO AND PACYNA, PIOTR. Multicast traffic aggregation in MPLS-based VPN networks. . 2007.

MONTE DE OCA, VÍCTOR MARTÍN AND PANTELIS, PABLO FEDERICO. BGP.

Análisis y simulación. . 2009.

NEUMANN, JC. The book of GNS3: build virtual network labs using Cisco, Juniper, and more. Online. 2015. [Accessed 4 August 2021]. Retrieved from: https://books.google.com/books?hl=es&lr=&id=9wcvDwAAQBAJ&oi=fnd&pg=PR5&dq=gns3&ots=aEKg5pU-N2&sig=L6y0q1zpwdgiBjkaS9mspcYNFbU

OÑA PIÑA, GLADYS DIANA. *Diseño y comparación de redes de acceso MPLS y Metro Ethernet integradas a un backbone MPLS para un proveedor de servicios y realización de un prototipo base*. . 2016. Quito, 2016.

PEPELNJAK, IVAN AND GUICHARD, JIM. *MPLS and VPN architectures*. Cisco press. ISBN 1587050811.

PINO, CRISTINA DEL AND AGUADO, ELSA. Comunicación y tendencias de futuro en el escenario digital: el universo "sisomo" y el caso de la plataforma Netflix. In: *I Congreso Internacional de la Red Iberoamericana de Narrativas Audiovisuales (Red INAV). Málaga-Sevilla, 23-25 de mayo de 2012. Editores: Virginia Guarinos, María Jesús Ruiz (pp. 1497-1508). Sevilla: Universidad de Sevilla, Secretariado de Recursos Audio*. 2012.

ROMÁN VALLEJO, MARÍA FERNANDA. *Estudio y diseño de una red metro Ethernet sobre MPLS (Multiprotocol Label Switching) para el transporte de voz, datos y video para la Empresa Eléctrica Quito SA*. . 2011. QUITO/EPN/2011.

ROSEN, ERIC C AND AGGARWAL, RAHUL. Multicast in mpls/bgp ip vpns. . 2012.

RUELA, J AND RICARDO, M. MPLS-Multiprotocol Label Switching. Online. 2005. [Accessed 4 August 2021]. Retrieved from: https://web.fe.up.pt/~jruela/Apontamentos/MPLS.pdf

SAXENA, VP, GOEL, A, GUPTA, V, COMPUTER, OP Sahu - International Journal of and, undefined, 2010. Importance of Multicast Virtual Private Networks based on RFC 2547. *Citeseer*. Online. 2010. Vol. 2, no. 8, pp. 975–8887. [Accessed 4 August 2021]. Retrieved from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.4470&rep=rep1&type=pdf

SEGARRA ZAMBRANO, ANA LUCÍA. *Estudio de redes privadas virtuales basadas en la*

Tecnología MPLS. . 2009. SANGOLQUÍ/ESPE/2009.

SHABTAY, LIOR AND RODRIG, BENNY. *IP multicast in VLAN environment*. . 12 April 2011. Google Patents.

SHAH, UTKARSH. Performance Evaluation of MPLS in a Virtualized Service Provider Core (with/without Class of Service). . 2017.

TANENBAUM, ANDREW S. *Redes de computadoras*. Pearson educación. ISBN 9702601622. 2012.

TENE SALCÁN, DIOSELINA ISABEL. Análisis y evaluación de los protocolos de enrutamiento multicast sobre multiprotocolo Label Switching aplicado a la provisión del servicio de IPTV. Online. 8 January 2020. [Accessed 5 September 2021]. Retrieved from: http://dspace.espoch.edu.ec/handle/123456789/14079

TOWNSLEY, W MARK AND PALL, GURDEEP SINGH. Layer Two Tunneling Protocol" L2TP". . 1999.

ZWORYKIN, VLADIMIR K. *Method of and apparatus for producing images of objects*. . November 1935. Google Patents.

ANEXOS

ANEXO A: CONFIGURACIÓN DE LOS ROUTERS

Configuración del núcleo en las redes MPLS

ROUTER PROVIDER P1

Se configura OSPF como protocolo IGP

```
router opsf 10
router-id 1.1.1.1
area 0
int g0/0/0/0
network point-to-point
exit
int g0/0/0/1
network point-to-point
exit
int g0/0/0/2
network point-to-point
exit
int g0/0/0/3
network point-to-point
exit
int lo0
passive
exit
```

Se habilita MPLS LDP en las todas las interfaces del router

```
conf t
router ospf 10
mpls ldp
router-id loopback 0
mpls ldp auto-config
router ospf 10
mpls ldp auto-config
```

Configuración del área de acceso a la red MPLS

ROUTER PROVIDER EDGE 1 PE-1

Se configura OSPF como protocolo IGP

router opsf 10

router-id 5.5.5.5

area 0

int g0/0/0/0

network point-to-point

exit

int g0/0/0/1

network point-to-point

exit

int lo0

passive

exit

Se habilita MPLS en la interfaz

conf t

router ospf 10

mpls ldp

router-id loopback 0

mpls ldp auto-config

router ospf 10

mpls ldp auto-config

Configuración de los routers de borde

ROUTER CUSTOMER EDGE 1 CE-1

conf t

int g0/0/0/0

ip add 100.10.20.2 255.255.255.0

no shut

exit

int g0/1

ip add 100.10.30.1 255.255.255.0

no shut

exit

Configuración de la conexión hacia la red MPLS del proveedor de servicios

ip route 0.0.0.0 0.0.0.0 10.10.20.1

Configuración de las interfaces del router para que ejecuten el protocolo PIM

conf t

multicast-routing

address-family ipv4
interface all enable
exit
Configuración de los perfiles MVPN
Perfil 0 default MDT-GRE
ROUTER PE1
router bgp 100
bgp router-id 5.5.5.5
address-family ipv4 unicast
address-family vpnv4 unicast
neighbor 6.6.6.6
remote-as 100
update-source Loopback0
address-family ipv4 unicast
next-hop-self
address-family vpnv4 unicast
next-hop-self
conf t
interface tunnel-ip 10
tunnel mode gre ipv4
ipv4 address 10.1.1.1 255.255.255.0
tunnel source 10.10.10.2
tunnel destination 10.10.12.2
exit
router ospf 10
router-id 5.5.5.5
area 0
interface tunnel-ip 10
interface Loopback 0
commit
CONFIGURACION MVPN PERFIL
conf t
multicast-routing
address-family ipv4
interface Loopback0
enable
interface GigabitEthernet0/0/0/2

enable
mdt source Loopback0
vrf one
address-family ipv4
mdt source Loopback0
rate-per-route
interface all enable
accounting per-prefix
mdt default ipv4 232.100.1.1
mdt data 232.100.100.0/24
router pim
address-family ipv4
interface Loopback0
enable
interface GigabitEthernet0/0/0/2
vrf one
address-family ipv4
rpf topology route-policy rpf-for-one
interface GigabitEthernet0/1/0/0
enable
end
ROUTER PE2
router bgp 100
bgp router-id 6.6.6.6
address-family ipv4 unicast
address-family vpnv4 unicast
neighbor 5.5.5.5
remote-as 100
update-source Loopback0
address-family ipv4 unicast
next-hop-self
address-family vpnv4 unicast
next-hop-self
conf t
interface tunnel-ip 10
tunnel mode gre ipv4
ipv4 address 10.1.1.2 255.255.255.0

```
tunnel source 10.10.12.2
tunnel destination 10.10.10.2
exit
router ospf 10
router-id 6.6.6.6
area 0
interface tunnel-ip 10
interface Loopback 0
commit
conf t
multicast-routing
address-family ipv4
interface Loopback0
enable
interface GigabitEthernet0/0/0/2
enable
mdt source Loopback0
vrf one
address-family ipv4
mdt source Loopback0
rate-per-route
interface all enable
accounting per-prefix
mdt default ipv4 232.100.1.1
mdt data 232.100.100.0/24
router pim
address-family ipv4
interface Loopback0
enable
interface GigabitEthernet0/0/0/2
vrf one
address-family ipv4
rpf topology route-policy rpf-for-one
interface GigabitEthernet0/1/0/0
enable
end
```

ANEXO B EMISIÓN DE VIDEO CON VLC MEDIA PLAYER

Para la emisión de video multicast se utilizó el software VLC en su versión 3.0.16, previamente instalado en la máquina virtual del servidor. El primer paso para la emisión de video multicast es ejecutar el programa y dirigirse al menú “Medio”, y luego elegir la opción “Emitir” como se muestra en la Ilustración B-1

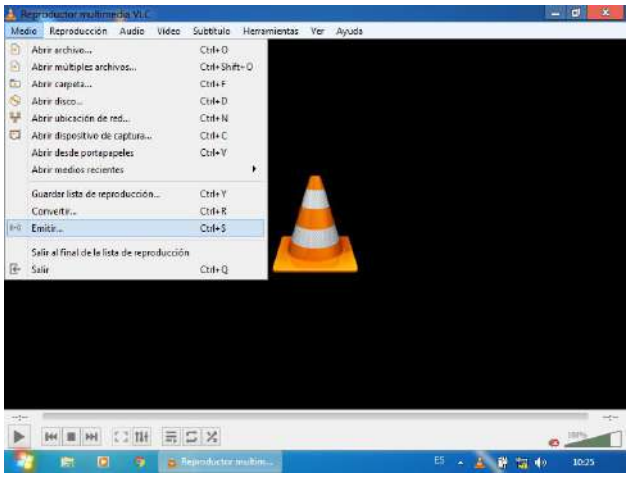


Ilustración B-1: Opción emitir VLC media player

Realizado por: Mafla, Carlos, 2022.

En la siguiente pantalla elegimos la opción “Añadir” y seleccionamos el archivo de video previamente cargado en la máquina virtual del servidor. Para configurar los parámetros de la emisión elegimos la opción “Emitir” cómo se muestra en la Ilustración B-2.

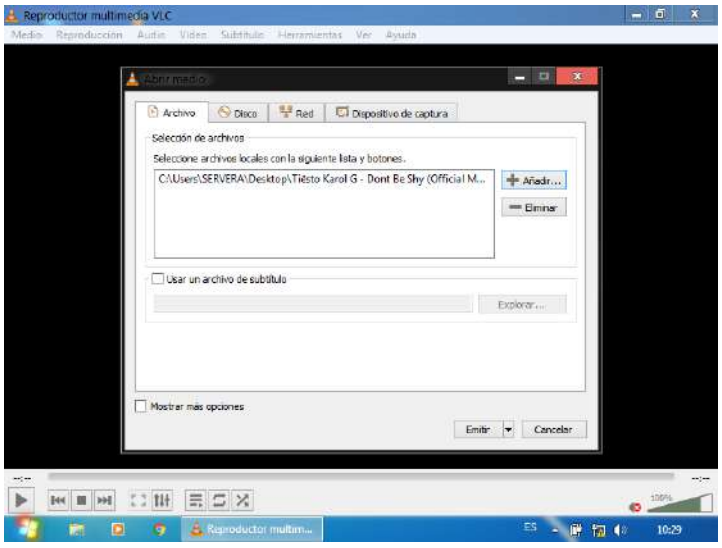


Ilustración B-2: Añadir archivo local de video para ser emitido en VLC media player

Realizado por: Mafla, Carlos, 2022.

El siguiente paso es añadir el método de emisión más adecuado de los ofrecidos por VLC media player, para el presente estudio se utiliza el método de emisión RTP/MPEG Transport Stream, cómo se observa en la Ilustración B-3.

Luego configuramos la dirección multicast, el puerto y asignamos un nombre aleatorio a la emisión. En este caso la dirección multicast que se usa es la 232.100.1.1 con el puerto 5001 y el nombre mvpn, cómo se muestra en la Ilustración B-3.

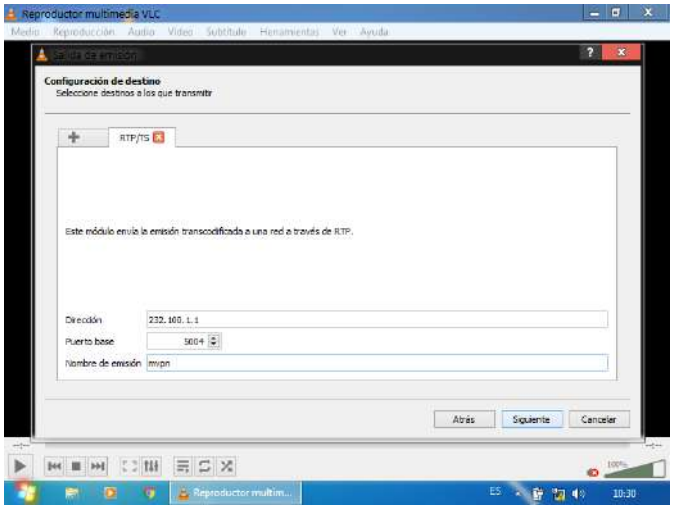


Ilustración B-3: Configuración tipo de emisión multicast VLC

Realizado por: Mafla, Carlos, 2022.

Para la emisión de la muestra de video en mensaje unicast, configuramos la dirección unicast de la máquina que emite la información, cómo se puede observar en la Ilustración B-4.

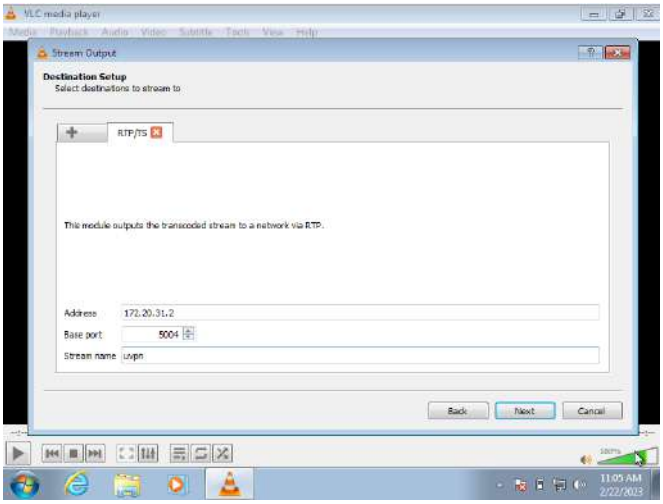


Ilustración B-4: Configuración tipo de emisión unicast VLC

Realizado por: Mafla, Carlos, 2023.

En la pantalla siguiente se habilita las opciones de transcodificación y se elige el formato más adecuado de acuerdo con el tipo de video a emitirse.

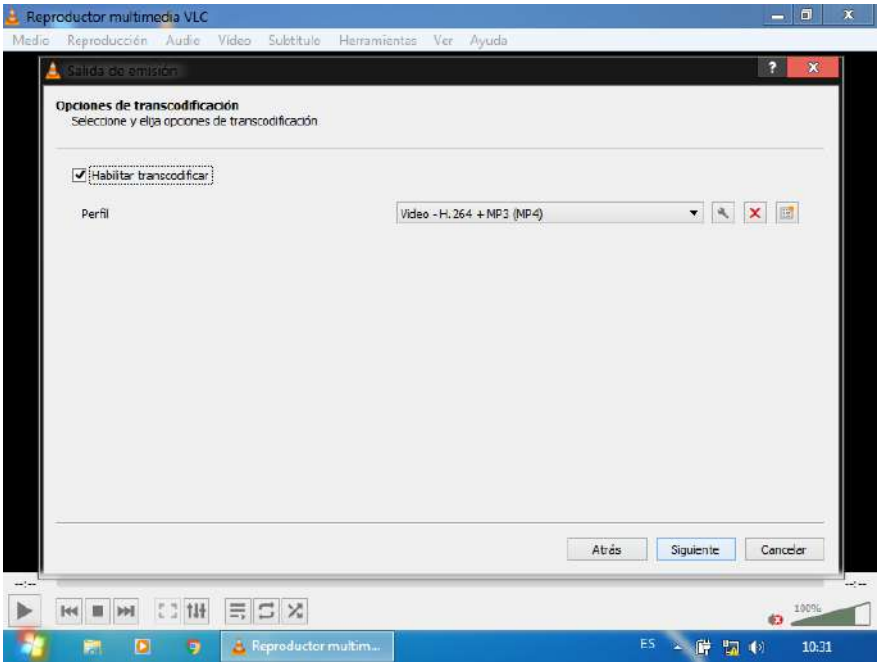


Ilustración B-5: Configuración opciones de transcodificación VLC media player

Realizado por: Mafla, Carlos, 2022.

Finalmente se visualizan los parámetros finales de la emisión y se configura de forma manual el tiempo de vida útil "ttl", este se configura con un valor 100 para que pueda viajar por toda la red del escenario planteado cómo se muestra en la Ilustración B-6.

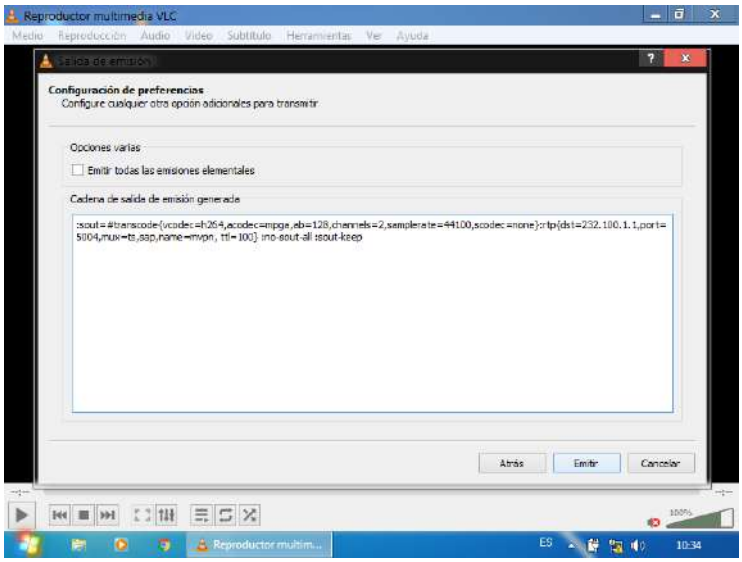


Ilustración B-6: Parámetros de emisión de video multicast mediante VLC

Realizado por: Mafla, Carlos, 2022.

Finalmente se selecciona la opción “Emitir” para que empiece la emisión multicast.

Para la emisión unicast se visualizan los parámetros finales y se configura de forma manual el tiempo de vida de útil “ttl”, este se configura con un valor 100 para que pueda viajar por toda la red del escenario planteado cómo se muestra en la Ilustración B-7.

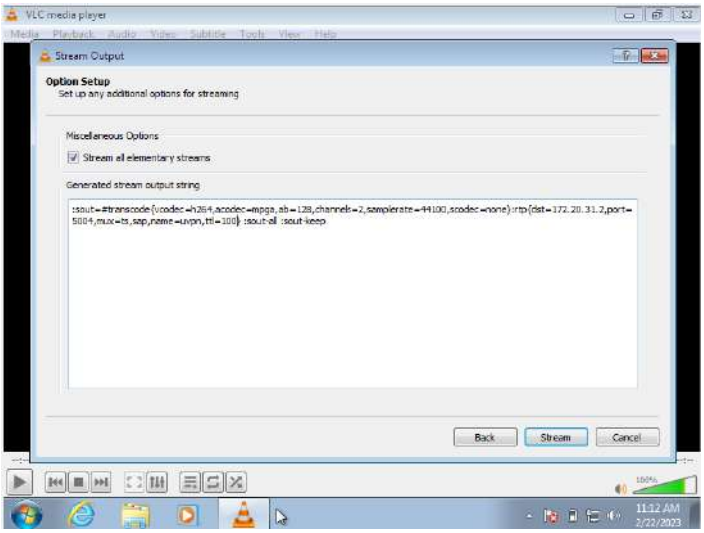


Ilustración B-7: Parámetros de emisión de video unicast mediante VLC

Realizado por: Mafla, Carlos, 2023.

Finalmente se selecciona la opción “Emitir” para que empiece la emisión unicast.

RECEPCIÓN DE VIDEO CON VLC MEDIA PLAYER

En la máquina virtual del cliente, se instala previamente VLC media player versión 3.0.16 para realizar la recepción de video. Se ejecuta VLC media player y se dirige al menú “Medio”, luego se elige la opción “Abrir ubicación de red” cómo se muestra en la Ilustración B-8.

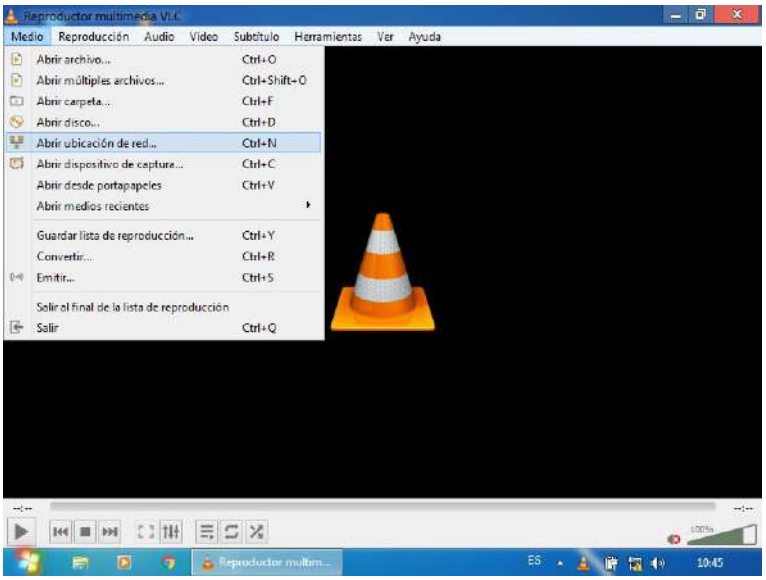
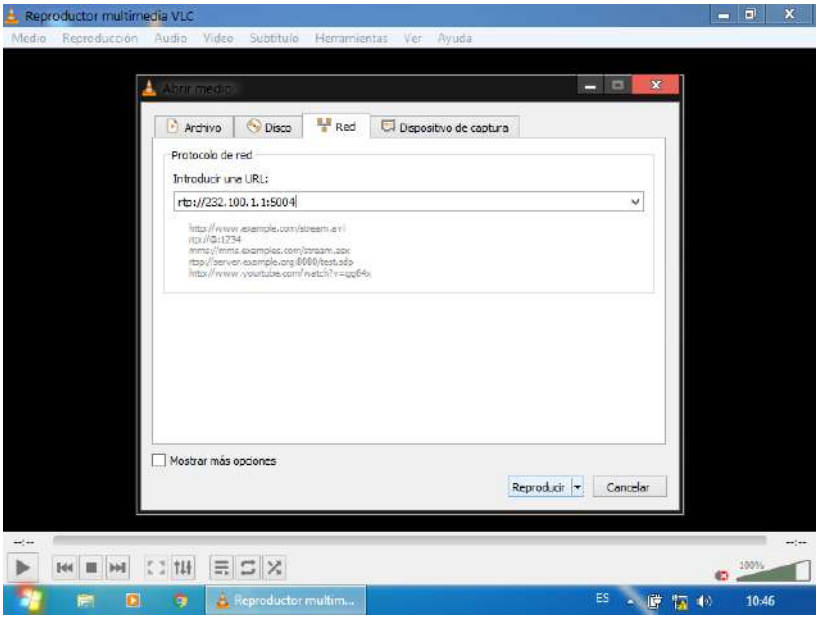


Ilustración B-8: Opción Abrir ubicación de red VLC media player

Realizado por: Mafla, Carlos, 2022.

En la siguiente pantalla se elige configura la dirección de emisión multicast, el puerto y el tipo de emisión que debe ser similar al seleccionado en el emisor, para este caso "rtp://232.100.1.1:5004" como se observa en la Ilustración B-9.



IlustraciónB-9: Configuración de parámetros de recepción de emisión Multicast

Realizado por: Mafla, Carlos, 2022.

Para la recepción de la emisión unicast se configura la dirección de emisión, el puerto y el tipo de emisión que debe ser similar al seleccionado en el emisor, para este caso "rtp://172.20.31.2:5004" como se observa en la Ilustración B-10.

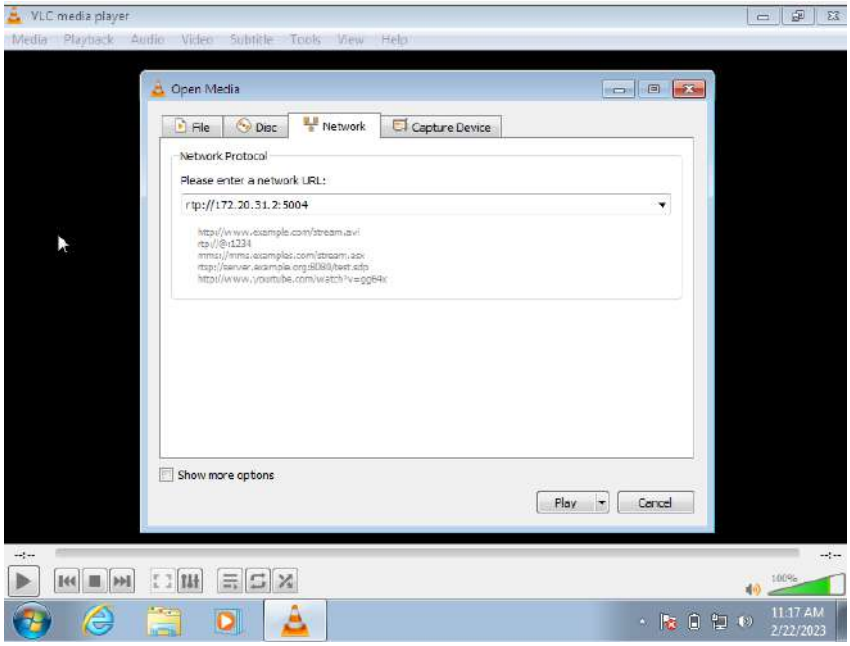


Ilustración B-10: Configuración de parámetros de recepción de emisión Unicast con VLC

Realizado por: Mafla, Carlos, 2023.

ANEXO C: GENERACIÓN DE TRÁFICO CON JPERF

Jperf en su versión 2.0.2 se instala previamente en cada una de las máquinas virtuales correspondientes al servidor y el cliente. Las máquinas deben tener Java previamente instalado para poder ejecutar la herramienta con su interfaz gráfica.

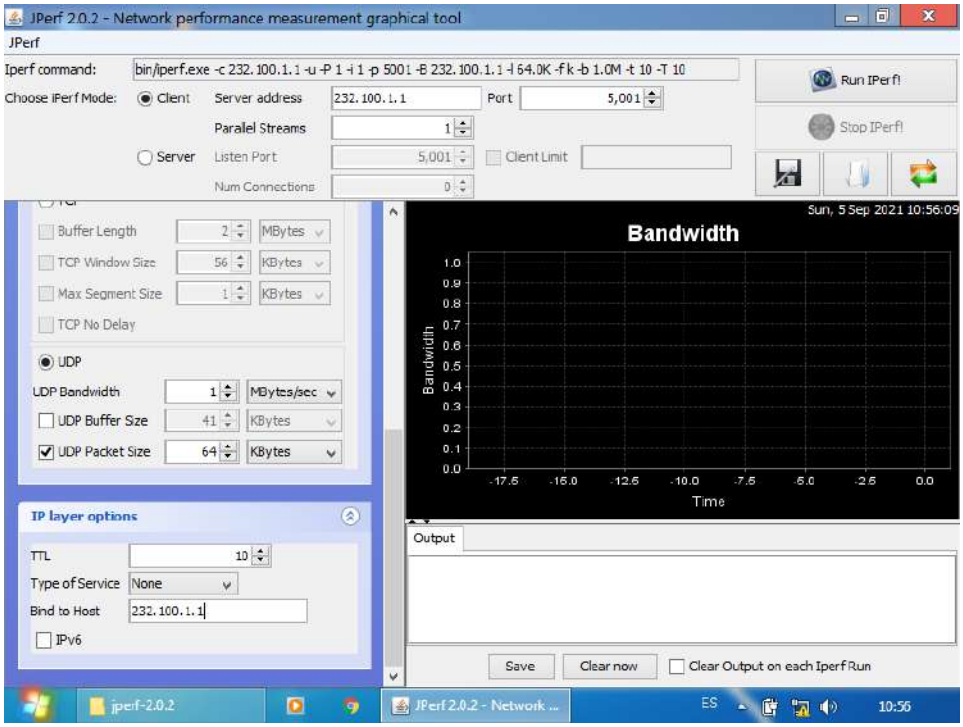


Ilustración C-1: Configuración de herramienta Jperf en la máquina Cliente A

Realizado por: Mafla, Carlos, 2022.

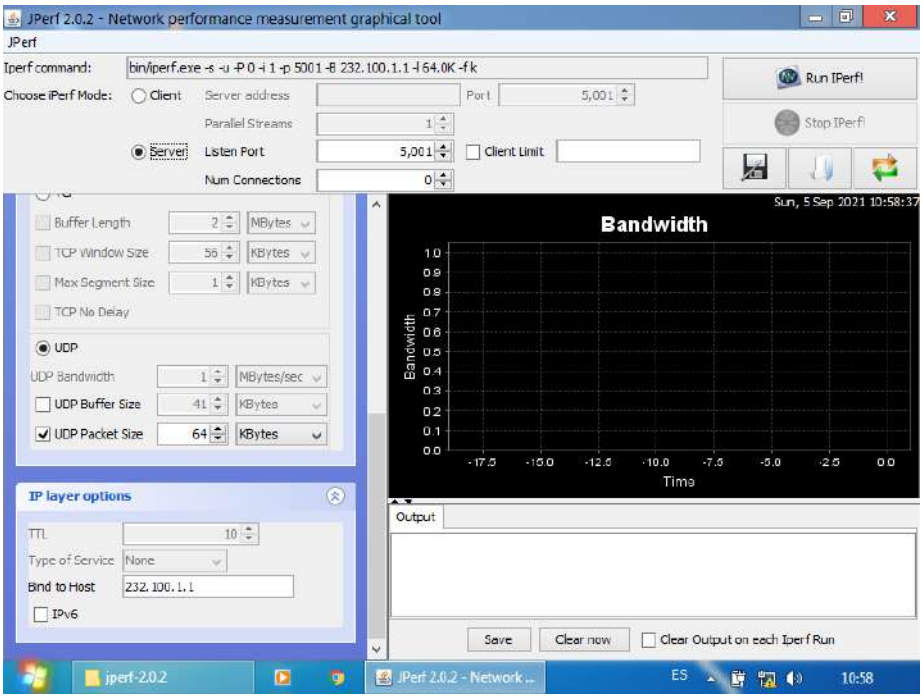


Ilustración C-2: Configuración de la herramienta Jperf en la máquina virtual Server A

Realizado por: Mafla, Carlos, 2022.

ANEXO D: GENERACIÓN TRÁFICO HERRAMIENTA OSTINATO

Una vez que se ha instalado ostinato en GNS3 se procede a iniciar y en su la pantalla de bienvenida se selecciona el grupo de puertos que se va a utilizar, para la generación de tráfico multicast y unicast en todo el escenario se utilizarán los dos primeros puertos eth0 y eth1, en el primero se transmitirán paquetes IP de multidifusión, mientras que en el segundo puerto se generarán peticiones IGMP para solicitar la recepción de la transmisión de multidifusión.

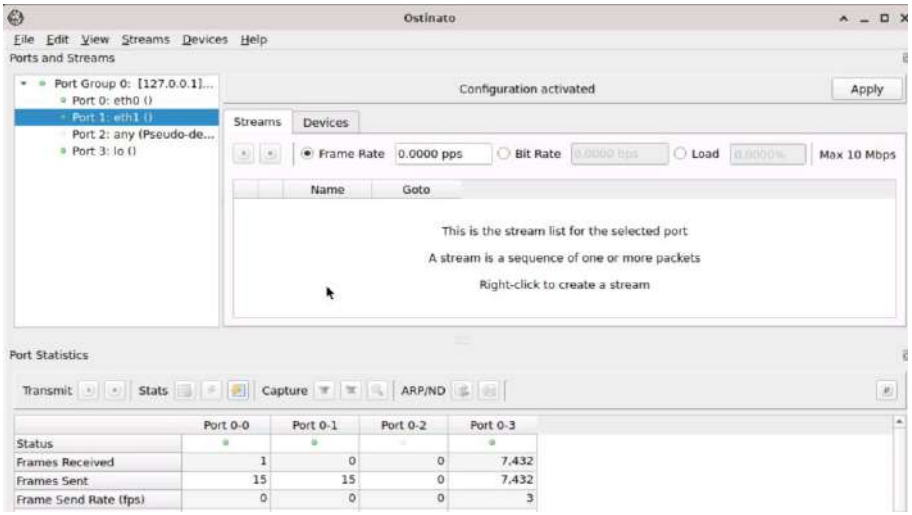


Ilustración D-1: Transmisión de paquetes IP de multidifusión

Realizado por: Mafla, Carlos, 2022.

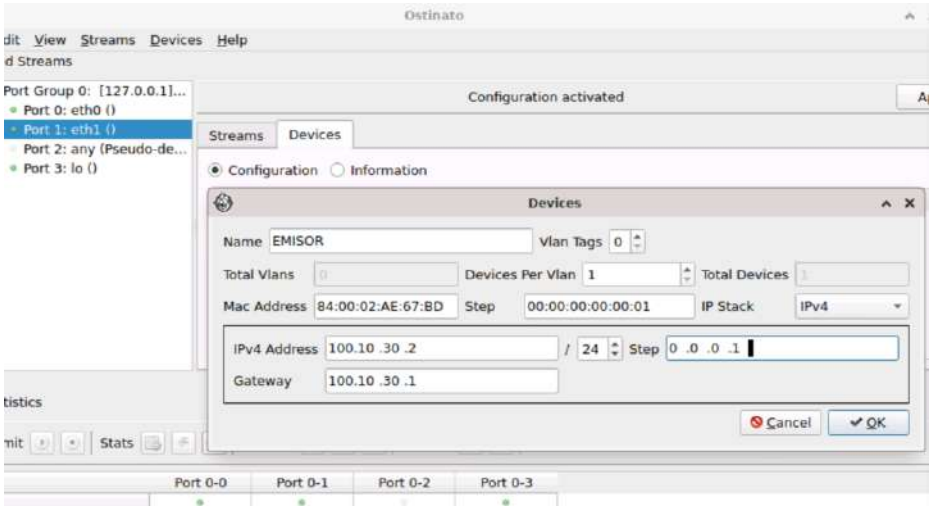


Ilustración D-2: Configuración EMISOR de la transmisión de multidifusión

Realizado por: Mafla, Carlos, 2022.

Se procede a añadir los dispositivos en cada uno de los puertos, en el primero se configura el dispositivo EMISOR de paquetes multicast, el mismo posee la misma ip del dispositivo SERVER A como se puede observar en la Ilustración D-2.

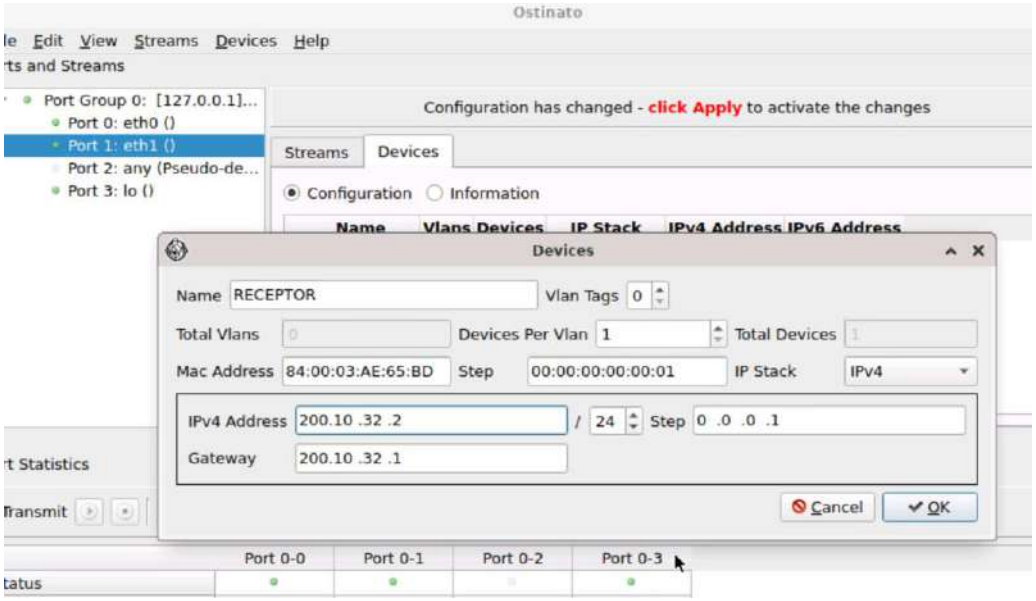


Ilustración D-3: Generación de tráfico multicast

Realizado por: Mafla, Carlos, 2022.

Para la transmisión de paquetes unicast y multicast se configuran los protocolos del paquete generado mediante la herramienta ostinato cómo se puede apreciar en la Ilustración D-4.

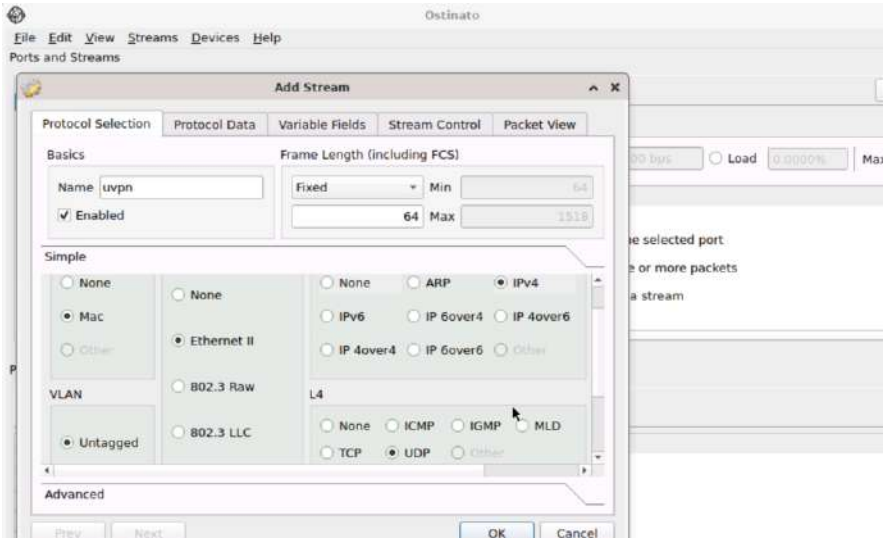


Ilustración D-4: Selección de protocolos tráfico unicast y multicast.

Realizado por: Mafla, Carlos, 2023.

Para la transmisión de paquetes unicast y multicast se configuran las direcciones de los equipos de emisión y recepción de los mensajes cómo se puede observar en la Ilustración D-5.

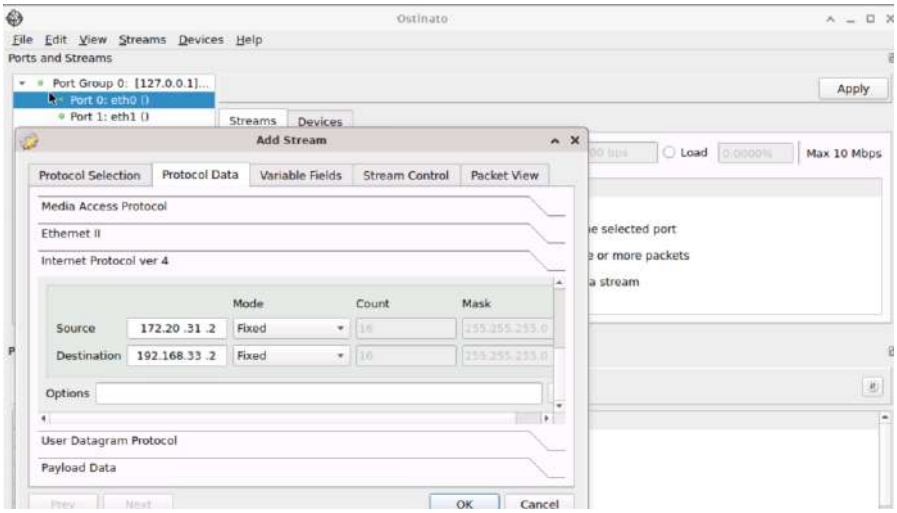


Ilustración D-5: Configuración de direcciones para tráfico unicast.

Realizado por: Mafla, Carlos, 2023.

Como destino de Media Access Protocol se utiliza la mac 01:00:5E:00:00:09 correspondiente al grupo de multidifusión IP y como fuente se utiliza la mac asignada al dispositivo receptor.

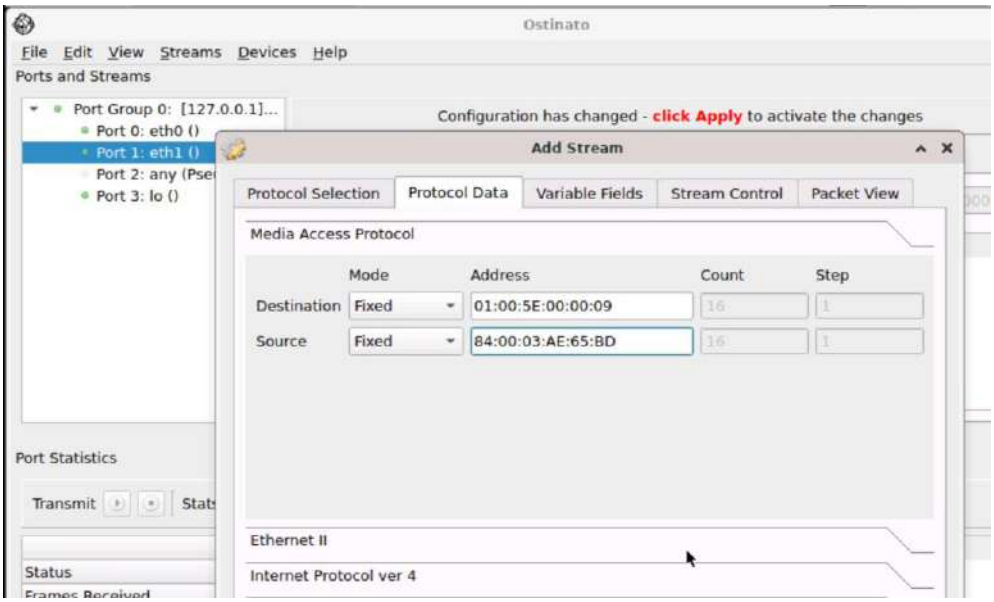


Ilustración D-6: Configuración de transmisión del paquete IP

Realizado por: Mafla, Carlos, 2022.

En el apartado protocolo se elige un puerto de origen y destino para el tráfico, en este caso se configura el puerto 222 cómo se puede observar en la Ilustración D-7.

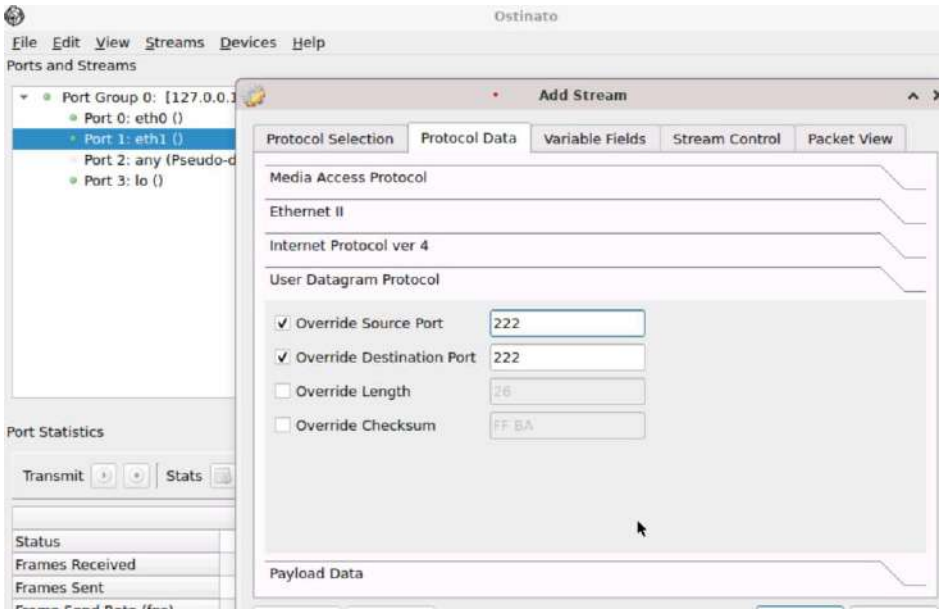


Ilustración D.7: Configuración puerto transmisión y recepción.

Realizado por: Mafla, Carlos, 2023.

Finalmente se configuran las opciones de control del stream, el número y la velocidad a la que se decide enviar los paquetes, éste se puede configurar en paquetes por segundo o bits por segundo cómo se puede observar en la Ilustración D-8.

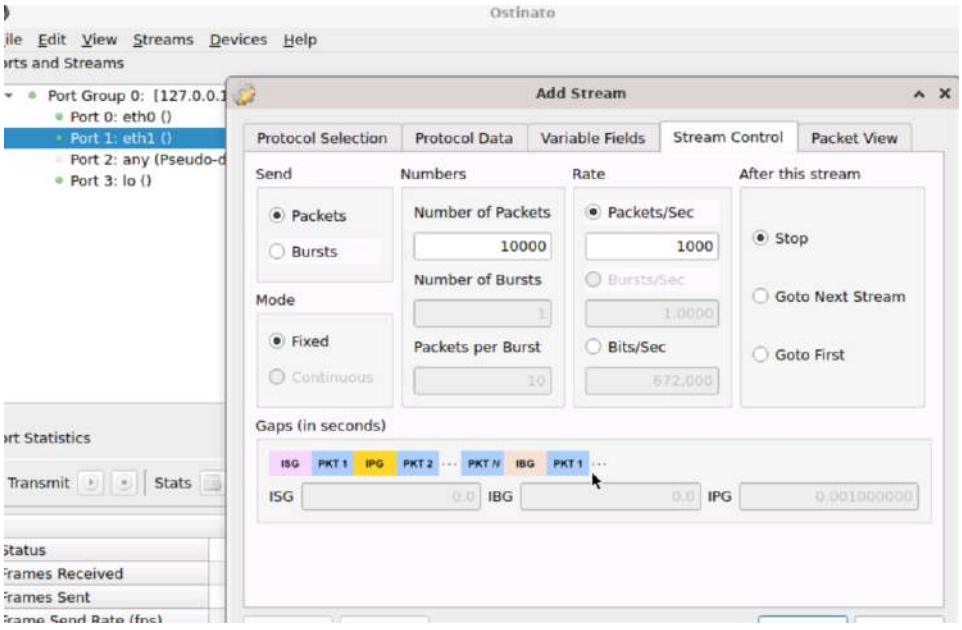


Ilustración D.8: Configuración opciones stream.

Realizado por: Mafla, Carlos, 2023.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 17 / 07 / 2023

INFORMACIÓN DEL AUTOR
Nombres – Apellidos: Carlos Alexis Mafla Ger
INFORMACIÓN INSTITUCIONAL
Facultad: Informática y Electrónica
Carrera: Telecomunicaciones
Título a optar: Ingeniero en Telecomunicaciones
f. Analista de Biblioteca responsable: Ing. Fernanda Arévalo M.

1456-DBRA-UPT-2023